Benchmark informatiebeveiliging, privacy en examinering in het mbo 2021

IBPDOC11g

REGIEGROEP IBP IN HET MBO
Kennisnet SURF mbo digitaal

Verantwoording

Productie

Kennisnet & MBO Digitaal

Auteur

Martijn Bijleveld

Versie 1.1, januari 2022

Met dank aan

	Naam	Instelling		Naam	Instelling
1	Hans Thalen	Aeres/Nordwin	29	Gerard Jans	Onderwijsgroep Noord
2	Remko Willemstein	Albeda	30	Joel de Bruijn	Onderwijsgroep Tilburg
3	Peter van der Zee	Alfa College	31	Michel Broersen	Regio College
4	Fung Yee Poon	Aventus	32	Maarten Veldhuis	Rijn IJssel
5	Niels Dutij	Cibap	33	Henk Links	ROC A12
6	Natascha Enklaar	Clusius College	34	Jorrit van der Heijden	ROC De Leijgraaf
7	Joris Weel	Curio	35	Gerrit Haakma	ROC Friese Poort
8	Manfred Tjapkes	Da Vinci College	36	Wietse de Graaf	ROC Horizon College
9	Helma de Boer	Deltion College	37	John Dijkman	ROC Kop van Noord-Holland
10	Hilbert van der Duim	Drenthe College	38	René van der Mark	ROC Midden Nederland
11	Klaske Bouma	Friesland College	39	Niels Dutij	ROC Nijmegen
12	Wim Triepels	Gilde Opleidingen	40	Niels Dutij	ROC Rivor
13	Claartje Uitterhoeve	Graafschap College	41	Leendert van Ingen	ROC Ter AA
14	Paul Rehm	Grafisch Lyceum Rotterdam	42	Theo Kuilboer	ROC Top
15	Paul 't Lam	Grafisch Lyceum Utrecht	43	Niels Hilhorst	ROC van Amsterdam/Flevoland
16	Jan Schrevel	Hoornbeeck College	44	Lotte Swaters	ROC van Twente
17	Peter Udo	Hout en Meubileringscollege	45	Marco Anceaux	Scalda
18	Gerry van der Schoot	Koning Willem I College	46	Harrie van de Graaf	SG De Rooi Pannen
19	Bert Lammers	Landstede	47	Erwin Huggers	SintLucas
20	René Bosman	Lentiz Onderwijsgroep	48	Esther ter Avest	Soma College
21	Ralph Kronieger	LIS	49	Ton Hoppener	STC-Group
22	Kees-Jan van 't Hof	MBO Amersfoort	50	Frank Verkamman	Summa College
23	Marjolein Rombouts	MBO Utrecht	51	Adriaan Noteboom	SVO
24	Niels Dutij	mboRijnland	52	Samantha Rodolf-Lejeune	VISTA college
25	Roy Prins	Mediacollege Amsterdam	53	Martijn van Hoorn	Yuverta
26	Jelle van Baggem	Nimeto Utrecht	54	Richard de Koning	Zadkine
27	Gert Fokkema	Noorderpoort	55	Niek Bunskoek	Zone.college
28	Rob van Bruggen	Nova College			

Sommige rechten voorbehouden

Inhoudsopgave

1. De Benchmark IBP-E in het mbo

1.1 Inleiding

Sinds 2014 speelt het onderwerp informatiebeveiliging een belangrijke rol binnen de mbo-sector, naar aanleiding van enkele ernstige informatiebeveiligingsincidenten. Na overleg met OCW kreeg de sector het mandaat om het onderwerp informatiebeveiliging zelf te gaan regelen. De Taskforce Informatiebeveiliging werd opgericht en ging van start met een duidelijk opdracht. Er werd een toetsingskader Informatiebeveiliging geadopteerd vanuit het hoger onderwijs, op basis van het ISO 27001 normenkader. Er werd scholing voor functionarissen vanuit de instellingen georganiseerd en er werd een Framework opgezet met diverse handreikingen en modeldocumenten. Vanaf 2015 werd jaarlijks een benchmark uitgevoerd. Aanvankelijk alleen op het gebied van informatiebeveiliging maar in 2016 werd het toetsingskader uitgebreid met een cluster waarin specifieke statements op het gebied van privacy waren opgenomen. In 2018 werd opnieuw een cluster toegevoegd met aanvullende statements op het gebied van examinering. De naam Benchmark IBP-E heeft dus betrekking op het gecombineerde zelfassessment met betrekking tot Informatiebeveiliging (IB), Privacy (P) en Examinering (E). De benchmark is dit jaar voor de zevende keer afgenomen.

Deze benchmarks hebben een tweeledig doel. Enerzijds geven ze een goed beeld van de stand van zaken in de mbo-instellingen met betrekking tot de volwassenheid van de IBP-organisatie: belangrijk voor de sector zelf maar ook voor de verantwoording richting OCW. Anderzijds geven de benchmarks de instelling zelf ook een helder overzicht van de mate waarin de maatregelen rond IBP succesvol zijn geïmplementeerd en leveren ze een roadmap op voor de instelling om mee aan de slag te gaan.

Het belang van de benchmark wordt in het mbo door alle instellingen onderschreven, getuige het feit dat alle 56 mbo-instellingen tenminste een keer hebben meegedaan aan de benchmark. Dit jaar hebben 55 van de 56 instellingen deelgenomen aan de onderdelen Informatiebeveiliging en Privacy en 51 instellingen hebben het examineringskader ingevuld. Daarmee zitten we op een totale deelname van 98%, een heel mooi resultaat.

1.2 Het netwerk IBP in het mbo

Belangrijke factor voor het succes van de benchmark is het Netwerk IBP in het mbo, waarin alle instellingen vertegenwoordigd zijn. Binnen dit hechte netwerk weten de 150 deelnemende IBP-ers elkaar goed te vinden en worden ervaringen en best-practices gedeeld. Er zijn diverse werkgroepen rondom belangrijke thema's als verwerkersovereenkomsten en awareness. Het netwerk komt 4 keer per jaar bijeen en heeft daarnaast een online teams-omgeving. Het wordt aangestuurd door de Regiegroep IBP, waarin 10 vertegenwoordigers van de instellingen zijn afgevaardigd, aangevuld met IBP-ondersteuners vanuit MBO Digitaal, Kennisnet, de MBO Raad en SURF. Activiteiten zoals deze benchmark en de peer review worden gecoördineerd door de regiegroep en daarmee zijn de mbo's zelf eigenaar: een heel krachtige aanpak.

1.3 Belangrijke ontwikkelingen in 2021

Bij de start van schooljaar 2021-2022 kreeg ROC Mondriaan te maken met een ransomware-aanval en daarmee werd voor het eerst ook een mbo-instelling op grote schaal geraakt. Alle systemen werden offline gehaald en één voor één opnieuw opgebouwd. De eerste maanden van het schooljaar kon er zeer beperkt ict worden ingezet en het is een groot compliment waard dat het onderwijs desondanks doorgang kon vinden. Deze cyberaanval heeft veel losgemaakt in het mbo en de lessons learned zijn op operationeel, tactisch en strategisch niveau gedeeld binnen de netwerken van MBO Digitaal.

De coronasituatie heeft ook in 2021 extra inzet gevraagd op het gebied IBP: de instellingen worden steeds afhankelijker van ict en de betrouwbaarheid, integriteit en vertrouwelijkheid van informatie zijn daarbij belangrijke aandachtspunten.
Via een korte enquête onder de invullers van de benchmark hebben we gepeild in hoeverre de aandacht voor IBP is veranderd. Ruim driekwart van de respondenten geeft aan dat de aandacht voor IBP in 2021 is toegenomen en bij ongeveer de helft heeft die toegenomen aandacht in sterke mate te maken met het incident bij ROC Mondriaan. Zie verder bijlage 2.
Verder is al in 2020 een discussie op gang gekomen over een nieuw toetsingskader voor het onderdeel Informatiebeveiliging: het Volwassenheidsmodel Informatiebeveiliging van de NBA. In 2021 is hierover tijdens de netwerkbijeenkomsten veel gesproken en we hebben dat nieuwe model ook op grote schaal beproefd tijdens de afgelopen benchmarkperiode. De bevindingen zijn geëvalueerd en de regiegroep IBP heeft op basis hiervan besloten om met ingang van 2022 de benchmark informatiebeveiliging uit te voeren op basis van het NBA-model als toetsingskader. Meer hierover in hoofdstuk 5.

1.4 Eindresultaat Benchmark IBP-E mbo 2021

Toen we 7 jaar geleden begonnen met deze benchmark hebben we het doel gesteld om als sector qua volwassenheid in 2020 gemiddeld op 3,0 uit te komen. Dat is ook in 2021 niet helemaal gelukt; de onderdelen Informatiebeveiliging en Examinering blijven op een 2,8 en Privacy stijgt licht naar een 2,9. Een bescheiden stap voorwaarts, die laat zien dat het -gemiddeld genomen- nog best een uitdaging is om op ons ambitieniveau van 3,0 te komen.

Totaal score Informatiebeveiliging	2,8
Totaal score Privacy	2,9
Totaal score Examinering	2,8
Percentage deelnemende instellingen	98%

1.5 Representativiteit

Aan de eerste benchmark in 2015 namen 19 mbo-instellingen deel, oftewel 29% van de instellingen. Bij de tweede benchmark in 2016 groeide dat percentage naar 46%; in 2017 gingen we naar 77% en vanaf 2018 doen -steeds op 1 of 2 instellingen na- alle mbo's mee. Ook dit jaar hebben we ingezet op een deelname van 100%, maar door de nasleep van de cyberaanval was ROC Mondriaan niet in staat om de benchmark in te vullen. De rest van onze mbo's hebben allemaal deelgenomen, wat laat zien dat het onderwerp sterk leeft en dat de mbo's gezamenlijk verantwoording willen afleggen: intern, naar elkaar toe en richting externe stakeholders, zoals OCW. Ook dit jaar werden, naar aanleiding van onder andere het incident bij ROC Mondriaan Kamervragen gesteld over cyberveiligheid binnen de onderwijssector. De resultaten van onze Benchmark IBP-E worden daarbij aangehaald en er gaan stemmen op voor extern toezicht. Het is daarom belangrijk om de betrouwbaarheid van de benchmark als instrument aan te tonen, vandaar dat we al enkele jaren inzetten op de peer review, waarbij instellingen elkaars assessment beoordelen.

1.6 Ontwikkeling van de scores van de Benchmark IBP-E

De benchmark wordt uitgevoerd op basis van de toetsingskaders Informatiebeveiliging, Privacy en Examinering. Het toetsingskader Informatiebeveiliging is onderverdeeld in zes clusters. Cluster 1 gaat vooral over beleidsmaatregelen, cluster 2 over personeel (bewustwording), cluster 3 over ruimten en apparatuur (veel ICT gerelateerde zaken), cluster 4 betreft vooral de continuïteit van de bedrijfsvoering (vooral ten aanzien van de ICT-infrastructuur), cluster 5 gaat over toegang tot data (vertrouwelijkheid) en de integriteit ervan en cluster 6 tot slot gaat over controle en logging.

Dit jaar is voor de zesde keer het pluscluster Privacy gescoord. Dit cluster bevat aanvullende statements met betrekking tot onder andere de rechtmatigheid van de gegevensverwerking in het kader van de AVG en de hantering van bewaartermijnen.
Het onderdeel examinering is in 2021 voor de vierde keer afgenomen.
Hieronder een samenvatting van de resultaten.

	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%**

Bron: Benchmark IBP-E mbo 2021, Kennisnet en MBO Digitaal (december 2021)

We zien een bescheiden groei in drie clusters van het onderdeel Informatiebeveiliging: cluster 2; Personeel, studenten en gasten, cluster 4; Continuïteit en cluster 6; Controle en logging. Daarnaast groeit het pluscluster Privacy met 0,1 naar 2,9.

2. Achtergronden toetsingskaders

2.1 De drie toetsingskaders

Voor de Benchmark IBP-E worden drie toetsingskaders gebruikt:

- **Toetsingskader Informatiebeveiliging** (IBPDOC3), totaal 101 statements, onderverdeeld in 6 clusters:
  1. Beleid en organisatie (24 statements)
  2. Personeel, studenten en gasten (10 statements)
  3. Ruimten en apparatuur (20 statements)
  4. Continuïteit (17 statements)
  5. Toegangsbeveiliging en integriteit (19 statements)
  6. Controle en logging (11 statements)
- **Toetsingskader Privacy** (IBPDOC7)
  - 21 statements
- **Toetsingskader Examinering** (IBPDOC8)
  - 18 statements

Het toetsingskader Informatiebeveiliging is gebaseerd op de ISO27002-norm. Van de 114 ISO-statements zijn er 101 overgenomen en voorzien van een vertaalslag naar de mbo-praktijk. Hieronder een voorbeeld van een statement uit het toetsingskader Informatiebeveiliging.

Toetsingskader informatiebeveiliging					REGIEGROEP IBP IN HET MBO Kennisnet SURF saMBO-ICT
Cluster	**2**	**Personeel, studenten en gasten**			AVG art. 24
Statement	**2.6**	**Rapportage van zwakke plekken in de informatiebeveiliging**			ISO 16.1.3
Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.					
Toelichting Alle gebruikers van de informatiesystemen behoren eventuele kwetsbaarheden zo snel mogelijk aan het contactpunt te rapporteren om informatiebeveiligingsincidenten te voorkomen. De procedure hiervoor is eenvoudig en toegankelijk.					
Bewijsvoering Er een Responsible disclosure beleid binnen de onderwijsinstelling.					
2 Overleg een vastgesteld beleid, bijvoorbeeld een responsible disclosure beleid, waarin beschreven staat dat medewerkers, studenten en contractanten verplicht zijn om zwakke plekken in de beveiliging direct te melden bij de daarvoor aangewezen contactpunten.					
3 Overleg een bewijsstuk, bijvoorbeeld een printscreen, waaruit blijkt dat het responsible disclosure beleid instellingsstellingsbreed is gecommuniceerd.					
Document	Responsible disclosure model mbo (IBPDOC27)				

2.2 Verklaring tabellen

De resultaten van deze benchmark worden gerapporteerd in diverse tabellen, zie het onderstaande voorbeeld:

Benchmark IBPE mbo 2021				*Eindscore:*						
Informatiebeveiliging				**2,8**		Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5
		aantal deelnemers informatiebeveiliging:	**55**							
Nr.	**ISO27002**	**Statement**		**Niveau 1 t/m 5**						
1.1	5.1.1	Beleidsregels voor informatiebeveiliging	P-E	3,4		0	2	30	23	0
1.2	vervallen									
1.3	5.1.2	Beoordeling van het Informatiebeveiligingsbeleid		3,1		1	12	23	19	0
1.4	6.1.1	Taken en verantwoordelijkheden informatiebeveiliging:		2,9		0	19	21	15	0
1.5	6.1.5	Informatiebeveiliging in projectbeheer	P	2,5		4	24	22	5	0
1.6	6.2.1	Beleid voor mobiele apparatuur	P	2,9		3	11	28	13	0

Een toelichting op de kolommen, van links naar rechts:

- Kolom Nr.: het nummer van het statement, dit is opgebouwd uit het clusternummer en een volgnummer. De vervallen statements zijn licht gearceerd.
- Kolom ISO 27002: het nummer van het statement volgens de ISO-norm, in verband met eenvoudige referentie naar de ISO-norm.
- Kolom Statement: de korte omschrijving van het statement, volgens de ISO-norm.
- Kolom P/E: deze kolom bevat een P en/of een E wanneer het statement is opgenomen in het gemeenschappelijke normenkader privacy en/of examinering.
- Kolom met scores: bovenin het gemiddelde van alle scores op de statements en daarmee de gemiddelde score voor het gehele onderdeel (in dit voorbeeld Informatiebeveiliging). In de rijen daaronder de gemiddelden per statement.
- Kolommen Niveau 1 t/m Niveau 5: de verdeling van de aantallen voor elk van de 5 niveaus.
- Voor elk van de clusters wordt het gemiddelde berekend in de donkerpaarse rij (zie afbeelding hieronder) en deze worden (gewogen) gemiddeld tot het eindresultaat, bovenaan in die kolom.

6.9	18.2.2	Naleving van beveiligingsbeleid en –normen	P	2,7		6	14	23	12	0
6.10	18.2.3	Beoordeling van technische naleving	P	2,5		8	13	30	4	0
6.11	vervallen									
6.12	12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen		2,4		12	17	19	7	0
6.13	16.1.6	Lering uit informatiebeveiligingsincidenten		3,1		1	9	30	14	1
6.14	18.2.1	Onafhankelijke beoordeling van informatiebeveiliging		3,0		1	11	31	12	0
		Gemiddelde cluster 6		2,6						

2.3 Samenhang IB, P en E

Deze Benchmark heeft betrekking op de onderdelen Informatiebeveiliging, Privacy en Examinering en hoewel we ze als afzonderlijke onderdelen invullen en beoordelen, kunnen ze niet los van elkaar gezien worden. Zo moet voor een goede bescherming van de privacy de informatiebeveiliging op orde zijn. Ook voor de examinering geldt een dergelijke afhankelijkheid. In principe geldt dat voor alle statements uit het IB-kader, maar daarbinnen zijn wel specifieke aandachtpunten te benoemen. Zo zijn er 36 statements uit het toetsingskader informatiebeveiliging benoemd die extra aandacht behoeven voor een goede bescherming van de privacy en 24 statements die cruciaal zijn voor een goede beveiliging van het examineringsproces. Deze statements uit het IB-kader zijn herkenbaar aan respectievelijk de letter P en/of de letter E in de betreffende kolom, zie hieronder.

2.1	7.1.2	Arbeidsvoorwaarden	P
2.2	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	P
2.3	9.2.6	Toegangsrechten intrekken of aanpassen	P-E
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	P-E
2.5	13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	P-E
2.6	16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging	
2.7	7.1.1	Screening	
2.8	6.2.2	Telewerken (thuiswerken)	E
2.9	7.2.3	Disciplinaire procedure	
2.10	vervallen		
2.11	7.2.1	Directieverantwoordelijkheden	

Bij de diverse updates van het toetsingskader zijn er statements vervallen, deze nummers worden niet hergebruikt en de regel wordt gearceerd weergegeven.

2.4 Volwassenheidsniveaus: het CMM-model

Om het volwassenheidsniveau van de informatiebeveiliging te meten wordt gebruikgemaakt van het Capability Maturity Model (CMM). Zie de toelichting hieronder.

Volwassenheidsniveau 1 *Ad hoc*	Beheersingsmaatregelen zijn niet of gedeeltelijk gedefinieerd en/of worden op inconsistente wijze uitgevoerd. Grote afhankelijkheid van individuen.
Volwassenheidsniveau 2 *Opzet, bestaan en beperkte werking*	Beheersingsmaatregelen zijn aanwezig en worden op consistente en gestructureerde, maar op informele wijze uitgevoerd.
Volwassenheidsniveau 3 *Uitgebreide werking*	Beheersingsmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar en wordt getoetst.
Volwassenheidsniveau 4 *PDCA-cyclus*	De effectiviteit van de beheersingsmaatregelen wordt periodiek geëvalueerd.
Volwassenheidsniveau 5 *Externe goedkeurende verklaring*	De beheersingsmaatregelen zijn verankerd in het integrale risicomanagement raamwerk, waarbij continu gezocht wordt naar verbetering.

In de drie toetsingskaders (IB, P en E) is de bewijslast uitgewerkt voor de niveaus 2 en 3. Deze uitwerking is bedoeld als richtlijn en helpt de instelling bij de concrete vertaling van de ISO-norm naar praktische en aantoonbare maatregelen.

② Overleg het IBP-beleid, voorzien van versiebeheer, dat goedgekeurd is door het CvB en de OR.
③ Overleg een bewijsstuk dat het IBP-beleid breed is gecommuniceerd binnen de organisatie, bijvoorbeeld door een printscreen van een intranetpagina.

Niveau 4 is van toepassing als de maatregel op niveau 3 aantoonbaar is opgenomen in een PDCA-cyclus.

2.5 Bewijslast

Afhankelijk van het statement kan voor de bewijslast gebruikgemaakt worden van:

- documenten
- interviews
- waarneming ter plaatse
- re-performance; het stap voor stap doornemen van een proces

Een cluster als *Beleid en organisatie* leunt zwaar op de aanwezigheid van (beleids)documenten, terwijl bij het cluster *Ruimten en apparatuur* de waarneming ter plaatse in veel gevallen veel meer voor de hand ligt. De bewijslast die beschreven wordt in de toetsingskaders is overigens bedoeld als richtlijn: pas toe of leg uit.

3. Resultaten Benchmark IBP-E mbo 2021

In de hiernavolgende paragrafen tonen we achtereenvolgens de scores voor de onderdelen:

- Informatiebeveiliging (par. 3.1)
  - omwille van het overzicht beperken wij ons tot presentatie van de statements uit de gemeenschappelijke normenkaders Privacy en Examinering; statements dus die in een breder perspectief van belang zijn en daarom extra aandacht vragen
- Privacy (par 3.2)
  - inclusief het gemeenschappelijk normenkader IB - Privacy
- Examinering (par. 3.3)
  - inclusief het gemeenschappelijk normenkader IB - Examinering

3.1 Resultaten Informatiebeveiliging (cluster 1-6)

We laten in dit overzicht over Informatiebeveiliging niet alle 101 statements zien. In plaats daarvan is er een keuze gemaakt voor die statements die voorkomen in het gemeenschappelijk normenkader Privacy en -Examinering. Dat zijn dus de IB-statements die vanuit privacy- en/of examineringsoogpunt extra aandacht behoeven. De in dit overzicht weergegeven gemiddelden zijn overigens wel gebaseerd op de complete set. De volledige set met statements en scores mb.t. Informatiebeveiliging is opgenomen in bijlage 1.

Benchmark IBPE mbo 2021

Informatiebeveiliging

Eindscore: **2,8**

aantal deelnemers informatiebeveiliging: **55**

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
1.5	6.1.5	Informatiebeveiliging in projectbeheer	P	2,5	4	24	22	5	0
1.6	6.2.1	Beleid voor mobiele apparatuur	P	2,9	3	11	28	13	0
1.7	8.2.1	Classificatie van informatie	P	2,7	2	25	16	12	0
1.8	8.2.2	Informatie labelen	P	2,6	6	17	25	7	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
1.20	18.1.4	Privacy en bescherming van persoonsgegevens	P	3,3	0	4	29	22	0
		Gemiddelde cluster 1; Beleid en organisatie		**2,9**					
2.1	7.1.2	Arbeidsvoorwaarden	P	2,6	7	16	26	6	0
2.2	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	P	2,6	4	20	23	8	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
		Gemiddelde cluster 2; Personeel, studenten en gasten		**2,7**					
3.5	11.1.3	Kantoren, ruimten en faciliteiten beveiligen	E	2,6	4	14	36	1	0
3.14	11.2.7	Veilig verwijderen of hergebruiken van apparatuur	P	3,1	2	5	34	12	2
3.21	8.3.3	Media fysiek overdragen	E	2,6	6	19	23	7	0
		Gemiddelde cluster 3; Ruimtes en apparatuur		**2,9**					
4.5	12.3.1	Back-up van informatie	P	3,3	1	4	28	20	2
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
		Gemiddelde cluster 4; Continuïteit		**2,9**					
5.1	9.1.1	Beleid voor toegangsbeveiliging	P	2,7	3	18	29	4	1
5.2	9.1.2	Toegang tot netwerken en netwerkdiensten	P-E	2,9	3	12	29	11	0
5.3	9.2.1	Registratie en afmelden van gebruikers	P-E	3,0	5	8	27	14	1
5.4	9.2.2	Gebruikers toegang verlenen	P	2,9	3	9	33	9	1
5.5	9.2.3	Beheren van speciale toegangsrechten	P	2,9	2	13	29	11	0
5.6	9.2.4	Beheer van geheime authenticatie-informatie van gebruikers	P	3,1	1	8	31	15	0
5.7	9.3.1	Geheime authenticatie-informatie gebruiken	P	3,1	1	7	32	15	0
5.8	9.4.1	Beperking toegang tot informatie	P	2,7	2	16	32	5	0
5.9	9.4.2	Beveiligde inlogprocedures	P-E	3,0	1	12	30	11	1
5.10	10.1.2	Sleutelbeheer	P	2,7	4	16	30	5	0
5.12	12.4.2	Beschermen van informatie in logbestanden	P-E	2,4	8	21	21	5	0
5.16	13.2.3	Elektronische berichten	P-E	2,5	4	19	31	1	0
5.27	14.3.1	Bescherming van testgegevens	P	2,1	13	26	14	1	0
		Gemiddelde cluster 5; Vertrouwelijkheid en integriteit		**2,8**					
6.1	9.2.5	Beoordeling van toegangsrechten van gebruikers	P-E	2,5	4	25	20	5	1
6.2	12.4.1	Gebeurtenissen registreren	P-E	2,4	7	21	26	1	0
6.3	12.4.3	Logbestanden van beheerders en operators	E	2,1	13	23	17	2	0
6.9	18.2.2	Naleving van beveiligingsbeleid en –normen	P	2,7	6	14	23	12	0
6.10	18.2.3	Beoordeling van technische naleving	P	2,5	8	13	30	4	0
		Gemiddelde cluster 6; Controle en logging		**2,6**					

Noot: de getoonde gemiddelden van de clusters zijn bepaald op basis van de complete set en niet op basis van de selectie van statements in dit overzicht.

Er is de afgelopen jaren door veel instellingen ingezet op het ontwikkelen, laten vaststellen en het communiceren van beleid. Cluster 1; “Beleid en organisatie”, doet het daarom gemiddeld genomen goed. Cluster 2; “Personeel, Studenten en Gasten” blijft daarbij iets achter maar groeit wel licht ten opzichte van 2020.
De meer technische, beheersmatige clusters zoals cluster 3; “Ruimten en apparatuur” en cluster 4; “Continuïteit” (waaronder bijvoorbeeld het maken van back-ups) scoren door de jaren heen relatief goed; waarbij we dit jaar in cluster 4; “Continuïteit” een lichte groei zien.
Cluster 6; “Controle en logging” bleef door de jaren heen altijd wat achter maar we zien dat deze nu iets bijtrekt, van 2,4 naar 2,6. Daar zal de toegenomen aandacht naar aanleiding van recente ransomware aanvallen in de sector zeker aan hebben bijgedragen.

De toename in volwassenheid per statement was in 2021 maximaal 0,2. Voor de onderstaande statements nam de volwassenheid met 0,2 toe ten opzichte van 2020.

1.26	**18.1.2**	**Intellectuele eigendomsrechten**		**2,9**
2.6	**16.1.3**	**Rapportage van zwakke plekken in de informatiebeveiliging**		**2,7**
2.8	**6.2.2**	**Telewerken (thuiswerken)**	**E**	**2,7**
3.13	**11.2.6**	**Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein**		**2,9**
4.2	**12.1.4**	**Scheiding van ontwikkel-, test- en productieomgevingen**		**2,9**
4.19	**17.1.3**	**Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren**		**2,4**
5.2	**9.1.2**	**Toegang tot netwerken en netwerkdiensten**	**P-E**	**2,9**
5.7	**9.3.1**	**Geheime authenticatie-informatie gebruiken**	**P**	**3,1**
6.1	**9.2.5**	**Beoordeling van toegangsrechten van gebruikers**	**P-E**	**2,5**
6.9	**18.2.2**	**Naleving van beveiligingsbeleid en –normen**	**P**	**2,7**
6.12	**12.7.1**	**Beheersmaatregelen betreffende audits van informatiesystemen**		**2,4**
6.13	**16.1.6**	**Lering uit informatiebeveiligingsincidenten**		**3,1**
6.14	**18.2.1**	**Onafhankelijke beoordeling van informatiebeveiliging**		**3,0**

De IB-statements die gemiddeld het sterkst stegen in volwassenheid (+0,2)

3.2 Resultaten Privacy (Pluscluster 7)

De gemiddelde score voor het privacy-cluster komt uit op 2,9 en dat is een verbetering van 0,1 ten opzichte van vorig jaar.

Benchmark IBPE mbo 2021		*Eindscore:*						
	Privacy	**2,9**		**Niveau 1**	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
	aantal deelnemers privacy:	55						
Nr.	**Statement**	**Niveau 1 t/m 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	2
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							

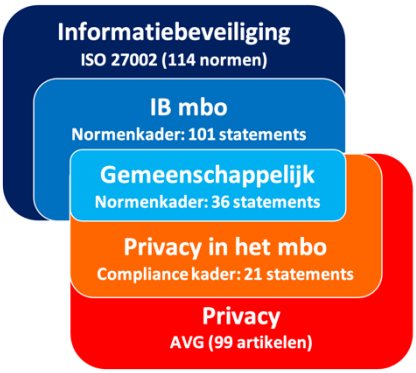
Een belangrijk statement als P.5, met betrekking tot de bewaartermijnen blijft ook dit jaar nog achter. Veel instellingen hebben op dit gebied, met terugwerkende kracht, nog veel werk te verzetten. De administratieve softwarepakketten ondersteunen dit aspect steeds vaker ‘by design’ voor nieuwe gegevens, maar voor de oude gegevens is vaak veel handwerk vereist om deze gegevens op te ruimen.
Voor wat betreft gegevensverwerkingen ten behoeve van onderzoek (P.6) is bij veel instellingen nog steeds weinig tot niets geregeld. Toch wordt (onderzoeks)data steeds belangrijker in het mbo; denk aan de diverse practoraten en de toenemende rol van data-ondersteund onderwijs: ontwikkelingen van waaruit de behoefte aan onderzoeksdata toeneemt.

Een aantal statements groeiden met 0,2 of 0,3 wat sterker dan gemiddeld, te weten:

- P.9 Informatiebeveiliging
- P.11 Transparant over privacy
- P.15 Bewustzijn, opleiding en training ten aanzien van privacy
- P.20 Privacy by design en privacy by default
- P.22 Controle naleving beleid

Gemeenschappelijk normenkader IB - Privacy

Om een goede bescherming van de privacy te kunnen waarborgen moet -bij wijze van randvoorwaarde- de informatiebeveiliging op orde zijn. In principe geldt dat voor alle statements, maar daarbinnen zijn wel specifieke aandachtpunten te benoemen. Zo zijn er 36 statements uit het toetsingskader informatiebeveiliging geselecteerd die extra aandacht behoeven voor een goede bescherming van de privacy. De baseline van deze statement hebben we vastgesteld op 3, het ambitieniveau is hier 4.
Het onderstaande overzicht toont de volwassenheidsscores voor deze 36 gemeenschappelijke statements. Het gemiddelde komt uit op 2,8 en is daarmee lager dan de baseline van 3 en gelijk aan het gemiddelde van 2,8 voor het gehele IB-kader.



Benchmark IBPE mbo 2021 — *Eindscore:*

Gemeenschappelijk normenkader IB-Privacy — **2,8**

aantal deelnemers informatiebeveiliging: 55

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
1.5	6.1.5	Informatiebeveiliging in projectbeheer	P	2,5	4	24	22	5	0
1.6	6.2.1	Beleid voor mobiele apparatuur	P	2,9	3	11	28	13	0
1.7	8.2.1	Classificatie van informatie	P	2,7	2	25	16	12	0
1.8	8.2.2	Informatie labelen	P	2,6	6	17	25	7	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
1.18	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
1.20	18.1.4	Privacy en bescherming van persoonsgegevens	P	3,3	0	4	29	22	0
2.1	7.1.2	Arbeidsvoorwaarden	P	2,6	7	16	26	6	0
2.2	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	P	2,6	4	20	23	8	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
3.14	11.2.7	Veilig verwijderen of hergebruiken van apparatuur	P	3,1	2	5	34	12	2
4.5	12.3.1	Back-up van informatie	P	3,3	1	4	28	20	2
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
5.1	9.1.1	Beleid voor toegangsbeveiliging	P	2,7	3	18	29	4	1
5.2	9.1.2	Toegang tot netwerken en netwerkdiensten	P-E	2,9	3	12	29	11	0
5.3	9.2.1	Registratie en afmelden van gebruikers	P-E	3,0	5	8	27	14	1
5.4	9.2.2	Gebruikers toegang verlenen	P	2,9	3	9	33	9	1
5.5	9.2.3	Beheren van speciale toegangsrechten	P	2,9	2	13	29	11	0
5.6	9.2.4	Beheer van geheime authenticatie-informatie van gebruikers	P	3,1	1	8	31	15	0
5.7	9.3.1	Geheime authenticatie-informatie gebruiken	P	3,1	1	7	32	15	0
5.8	9.4.1	Beperking toegang tot informatie	P	2,7	2	16	32	5	0
5.9	9.4.2	Beveiligde inlogprocedures	P-E	3,0	1	12	30	11	1
5.10	10.1.2	Sleutelbeheer	P	2,7	4	16	30	5	0
5.12	12.4.2	Beschermen van informatie in logbestanden	P-E	2,4	8	21	21	5	0
5.16	13.2.3	Elektronische berichten	P-E	2,5	4	19	31	1	0
5.27	14.3.1	Bescherming van testgegevens	P	2,1	13	26	14	1	0
6.1	9.2.5	Beoordeling van toegangsrechten van gebruikers	P-E	2,5	4	25	20	5	1
6.2	12.4.1	Gebeurtenissen registreren	P-E	2,4	7	21	26	1	0
6.9	18.2.2	Naleving van beveiligingsbeleid en –normen	P	2,7	6	14	23	12	0
6.10	18.2.3	Beoordeling van technische naleving	P	2,5	8	13	30	4	0

Een aantal statements die voor de borging van de privacy van belang zijn scoren aanmerkelijk lager dan gewenst, zeker als je bedenkt dat hier het ambitieniveau minimaal 3, bij voorkeur niveau 4 is. De laagst scorende statements (<2,5) uit dit overzicht:

- 1.19 Beschermen van registraties (2,3)
- 4.14 Informatiebeveiligingscontinuïteit implementeren (2,4)
- 5.12 Beschermen van informatie in logbestanden (2,4)
- 5.27 Bescherming van testgegevens (2,1)
- 6.2 Gebeurtenissen registreren (2,4)

Voor een goede bescherming van de privacy verdienen deze statements uit het IB-deel dus extra aandacht.

3.3 Resultaten Examinering (Pluscluster 8)

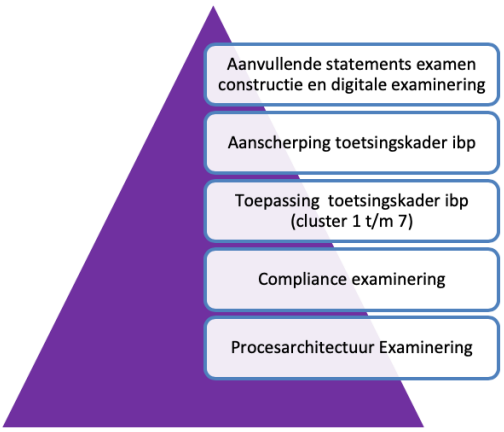
De gemiddelde score voor het cluster Examinering komt uit op 2,8 en dat is daarmee gelijk gebleven ten opzichte van vorig jaar.

Benchmark IBPE mbo 2021		Eindscore:						
	Examinering	2,8		Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5
	aantal deelnemers examinering: 51							
Nr.	Statement	Niveau 1 t/m 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	0
E.10	Extra ondersteuning bij (digitale) examens	3,3		1	4	25	21	0
E.11	Beveiligde examenruimtes	2,5		7	18	19	7	0
E.12	Het beheren en documenteren van ict-faciliteiten voor examinering	2,4		9	17	22	3	0
E.13	Hanteren van digitaal examenmateriaal	2,4		7	18	24	2	0
E.14	Toewijzen examens aan studenten	2,8		2	17	22	10	0
E.15	Kopieerbeveiliging examenvragen i.v.m. mogelijk hergebruik	2,4		10	15	21	5	0
E.16	Voorbereiden op vaststellen diplomabesluit door de examencommissie	3,4		1	4	22	20	4
E.17	Borgen dat diploma en overige waardedocumenten rechtmatig, veilig en correct worden aangemaakt en afgedrukt	3,3		1	7	20	23	0
E.18	Eindevaluatie examenproces en de integriteit van de resultaten	2,9		3	12	24	12	0

Op het gebied van de examinering is veel beleid vastgelegd in het examenreglement en veel procedures zijn helder beschreven in het handboek examinering. Toch ontbreken er, vooral waar het gaat over de digitale examinering, nog procedures en richtlijnen. Het statement E.1 met betrekking tot het beleidsplan beveiliging examinering scoort met een 2,3 het laagst, maar groeit wel met 0,2 ten opzichte van vorig jaar. Ook E.2 m.b.t. gedragscodes en richtlijnen voor de afname stijgt met 0,2, evenals statement E.5 met betrekking tot het archiveren en vernietigen van examenmateriaal.

Gemeenschappelijk normenkader IB – Examinering

Om de vertrouwelijkheid en integriteit van de examinering te waarborgen moet de informatiebeveiliging goed op orde zijn. In principe moeten alle statements uit het toetsingskader IB op orde zijn, maar daarbinnen zijn 24 statements benoemd die extra aandacht behoeven voor een goede bescherming van het examineringsproces. De baseline voor deze statements hebben we vastgesteld op 3 en het ambitieniveau op 4).
Het onderstaande overzicht toont de volwassenheidsscores voor deze 24 gemeenschappelijke statements. Het gemiddelde komt uit op 2,8 en is daarmee gelijk aan de gemiddelde score voor het gehele IB-kader, maar lager dan de baseline van 3.



Benchmark IBPE mbo 2021				*Eindscore:*						
Gemeenschappelijk normenkader IB-Examinering				**2,8**		Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5
		aantal deelnemers informatiebeveiliging:	**55**							
Nr.	**ISO27002**	**Statement**		**Niveau 1 t/m 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
4.15	17.2.1	Beschikbaarheid van informatie verwerkende faciliteiten	E	2,9		2	13	27	13	0
5.2	9.1.2	Toegang tot netwerken en netwerkdiensten	P-E	2,9		3	12	29	11	0
5.3	9.2.1	Registratie en afmelden van gebruikers	P-E	3,0		5	8	27	14	1
5.9	9.4.2	Beveiligde inlogprocedures	P-E	3,0		1	12	30	11	1
5.12	12.4.2	Beschermen van informatie in logbestanden	P-E	2,4		8	21	21	5	0
5.16	13.2.3	Elektronische berichten	P-E	2,5		4	19	31	1	0
6.1	9.2.5	Beoordeling van toegangsrechten van gebruikers	P-E	2,5		4	25	20	5	1
6.2	12.4.1	Gebeurtenissen registreren	P-E	2,4		7	21	26	1	0
6.3	12.4.3	Logbestanden van beheerders en operators	E	2,1		13	23	17	2	0

Een aantal statements die voor de borging van de examinering van belang zijn scoren aanmerkelijk lager dan gewenst, zeker als je bedenkt dat hier het ambitieniveau minimaal 3, bij voorkeur niveau 4 is. De laagst scorende statements (<2,5) uit het gemeenschappelijk normenkader IB-Examinering:

1.19 Beschermen van registraties (2,3)
5.12 Beschermen van informatie in logbestanden. (2,4)
6.2 Gebeurtenissen registreren (2,4)
6.3 Logbestanden van beheerders en operators (2,1)

De eerste drie komen ook terug als knelpunt vanuit het gemeenschappelijk normenkader IB-Privacy, dus op deze gebieden is echt verbetering noodzakelijk.

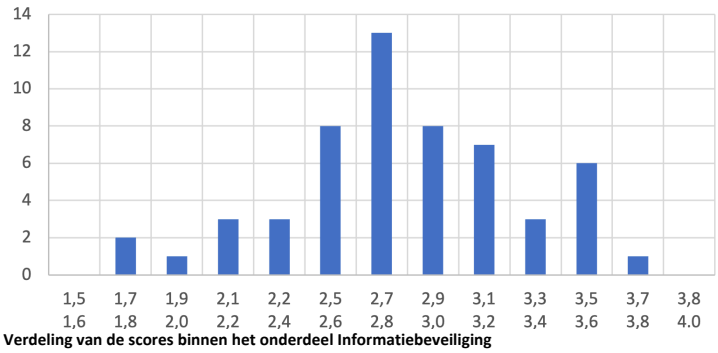
4. Nadere analyse Informatiebeveiliging

We hebben in deze rapportage een aantal aspecten met betrekking tot het onderdeel informatiebeveiliging verder uitgewerkt of uitgesplitst.

- De verdeling van de scores
- De ranking van de resultaten in vier groepen van 14 instellingen
- De hoogst- en de laagst scorende statements

4.1 De verdeling van de scores

Als we kijken naar de verdeling van de scores binnen het onderdeel informatiebeveiliging dan zien we grote verschillen in volwassenheid tussen de instellingen. 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 2,0 niet en 21 van de 55 instellingen voldoen aan het binnen de sector overeengekomen ambitieniveau van 3,0.



Verdeling van de scores binnen het onderdeel Informatiebeveiliging

4.2 Ranking instellingen in groepen

We hebben in deze rapportage de instellingen gerangschikt naar hun gemiddelde totaalscore op het IB-kader en deze -evenals vorige edities- onderverdeeld in vier groepen. De eerste groep bestaat uit de 14 hoogst scorende instellingen voor wat betreft het toetsingskader Informatiebeveiliging. De tweede groep bevat de mbo-instellingen met de ranking 15 tot en met 28. De derde groep de mbo-instellingen met de ranking 29 tot en met 42 en de vierde groep de mbo-instellingen met de ranking 43 tot en met 55.

Ranking 1-14

Deze groep van 14 toppers zit met een gemiddelde volwassenheid van 3,4 ruim boven het ambitieniveau van 3,0. Het gemiddelde van deze instellingen zit tussen 3,2 en 3,7.

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

Ranking 15-28

Deze groep van 14 instellingen scoort gemiddeld precies ons ambitieniveau van 3,0. Het gemiddelde beweegt zich tussen 2,8 en 3,1.

Cluster 1: Beleid en organisatie	3,0
Cluster 2: Personeel, studenten en gasten	2,8
Cluster 3: Ruimtes en apparatuur	3,1
Cluster 4: Continuïteit	3,1
Cluster 5: Vertrouwelijkheid en integriteit	2,9
Cluster 6: Controle en Logging	2,7
Informatiebeveiliging totaal*	**3,0**

Ranking 29-42

De instellingen scoren hier gemiddeld tussen de 2,6 en 2,8. Met een gemiddelde van 2,7 goed op koers naar het ambitieniveau van 3,0.

Cluster 1: Beleid en organisatie	2,7
Cluster 2: Personeel, studenten en gasten	2,6
Cluster 3: Ruimtes en apparatuur	2,8
Cluster 4: Continuïteit	2,7
Cluster 5: Vertrouwelijkheid en integriteit	2,7
Cluster 6: Controle en Logging	2,4
Informatiebeveiliging totaal*	**2,7**

Ranking 43-55

Deze 13 instellingen zitten gemiddeld genomen maar net boven de baseline van 2, die toch gezien moet worden als een absoluut minimum. Het gemiddelde beweegt zich in deze groep tussen 2,6 en 1,7. Het is in het belang van deze instellingen, maar ook de sector als geheel, om samen te kijken op welke manier ondersteuning kan worden geboden.

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

4.3 De hoogst en laagst scorende statements

Verder is er binnen het toetsingskader Informatiebeveiliging een ranking gemaakt van hoog naar laag scorende statements.

De 15 hoogst scorende statements uit het IB-kader

1.1	5.1.1	Beleidsregels voor informatiebeveiliging	P-E	3,4		0	2	30	23	0
1.23	6.1.4	Contact met speciale belangengroepen		3,4		1	2	30	20	2
1.20	18.1.4	Privacy en bescherming van persoonsgegevens	P	3,3		0	4	29	22	0
3.15	12.4.4	Kloksynchronisatie		3,3		1	3	30	19	2
4.5	12.3.1	Back-up van informatie	P	3,3		1	4	28	20	2
1.16	15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	E	3,3		0	1	36	18	0
2.7	7.1.1	Screening		3,3		1	6	27	17	4
1.13	13.2.2	Overeenkomsten over informatietransport		3,3		0	1	38	15	1
1.18	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	P-E	3,3		1	3	31	20	0
3.10	11.2.2	Nutsvoorzieningen		3,3		1	7	25	20	2
4.13	16.1.5	Respons op informatiebeveiligingsincidenten	P-E	3,3		0	6	29	19	1
1.17	16.1.1	Verantwoordelijkheden en procedures	E	3,3		0	6	29	20	0
1.22	6.1.3	Contact met overheidsinstanties		3,3		0	6	29	20	0
4.3	12.2.1	Beheersmaatregelen tegen malware		3,2		2	6	25	22	0
1.11	11.2.5	Verwijdering van bedrijfsmiddelen		3,2		1	5	31	18	0

Wat hier opvalt is dat er vooral statements uit de clusters 1, 3 en 4 in voorkomen.

De 15 laagst scorende statements uit het IB-kader

4.18	17.1.1	Informatiebeveiligingscontinuïteit plannen		2,5		10	13	26	6	0
1.25	18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen		2,5		6	22	21	6	0
1.27	18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen		2,5		9	17	22	7	0
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	P-E	2,5		4	24	25	2	0
4.14	17.1.2	Informatiebeveiligingscontinuïteit implementeren	P	2,4		12	17	16	10	0
5.12	12.4.2	Beschermen van informatie in logbestanden	P-E	2,4		8	21	21	5	0
6.2	12.4.1	Gebeurtenissen registreren	P-E	2,4		7	21	26	1	0
6.12	12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen		2,4		12	17	19	7	0
4.19	17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren		2,4		10	21	18	6	0
6.8	16.1.7	Verzamelen van bewijsmateriaal		2,4		11	17	23	4	0
1.19	18.1.3	Beschermen van registraties	P-E	2,3		4	33	16	2	0
6.7	15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers		2,2		10	26	15	4	0
6.3	12.4.3	Logbestanden van beheerders en operators	E	2,1		13	23	17	2	0
5.27	14.3.1	Bescherming van testgegevens	P	2,1		13	26	14	1	0
2.11	7.2.1	Directieverantwoordelijkheden		2,0		19	20	13	3	0

Hier zien we dat vooral cluster 6; Controle en logging is oververtegenwoordigd. Controle en logging blijft ook in 2022 een aandachtspunt.

5. Naar een nieuw toetsingskader IB

Het huidige toetsingskader informatiebeveiliging werd binnen het hoger onderwijs ontwikkeld en wordt sinds 2015 gebruikt binnen het mbo. In 2019 stapte het hoger onderwijs over naar een nieuw toetsingskader voor informatiebeveiliging, op basis van het NBA-volwassenheidsmodel voor informatiebeveiliging. In het mbo hebben we er toen voor gekozen die overstap nog niet te maken, omdat we op dat moment hadden bereikt dat (vrijwel) alle instellingen deelnamen aan de benchmark en we dat commitment niet op het spel wilden zetten.

Inmiddels zijn we twee jaar verder en zijn we gemiddeld genomen flink gegroeid in volwassenheid. Veel instellingen gebruiken het toetsingskader IB niet alleen voor de benchmark, maar ook als basis voor hun roadmap IB, voor het plannen en bewaken van te nemen maatregelen. Het huidige toetsingskader, dat sterk gericht is op technische maatregelen en minder op de governance van de informatiebeveiliging sluit daar steeds minder goed bij aan. Ook de huidige situatie met clouddiensten, waarbij het accent meer komt te liggen op leveranciersmanagement, krijgt in het huidige toetsingskader onvoldoende aandacht. In 2020 is er binnen het netwerk IBP een discussie op gang gekomen over de mogelijke overstap naar dit nieuwe toetsingskader en in 2021 hebben we het op grote schaal getest. Eind 2021 is er door het netwerk IBP besloten om het NBA Volwassenheidsmodel IB met ingang van 2022 te gaan gebruiken als toetsingskader informatiebeveiliging voor de Benchmark IBP-E. Hieronder meer informatie over dit NBA-model.

5.1 NBA Volwassenheidsmodel voor Informatiebeveiliging

Het Volwassenheidsmodel voor Informatiebeveiliging is ontwikkeld door de Nederlandse Beroepsorganisatie voor Accountants (NBA). Het is geen norm (zoals ISO 27001) maar een hulpmiddel voor interne- en externe auditors om de volwassenheid in kaart te brengen. De statements zijn heel geschikt om te dienen als toetsingskader informatiebeveiliging voor de onderwijssector.
Naast de meting waar de organisatie staat op het gebied van informatiebeveiliging geeft het model ook handvatten wat er moet gebeuren om het gewenste niveau van informatiebeveiliging te bereiken, rekening houdend met de risico's. Het NBA-model is daarmee veel meer dan een toetsingskader voor de benchmark IB; het is voor de individuele instelling daarnaast een gids om beter in control te komen op het gebied van cyberveiligheid.

Voordelen van het NBA-model

1. Het model is met 69 maatregelen een stuk compacter dan het huidige toetsingskader.
2. Het is minder gericht op technische beheersmaatregelen, in plaats daarvan is er meer aandacht voor governance, leveranciersmanagement en risicomanagement.
3. Het model nodigt uit om per statement een risico-afweging te maken en het vereiste volwassenheidsniveau daarop af te stemmen.
4. Voor elk statement zijn de volwassenheidsniveaus 1-5 gedetailleerd beschreven, wat het model praktisch toepasbaar en objectief toetsbaar maakt.
5. Het model wordt door de beroepsgroep breed geaccepteerd, waardoor interne- en externe auditors en accountants betrokken kunnen worden bij het assessment.
6. De SURFaudit benchmark in het hoger onderwijs is eveneens (sinds 2019) gebaseerd op dit model en dat biedt mogelijkheden voor samenwerking met het ho en SURF op dit gebied.

Overigens bevatten de statements van het NBA-model verwijzingen naar diverse normen, waaronder de ISO 27001/2. Op die manier is een relatie te leggen met het huidige ISO-gebaseerde toetsingskader informatiebeveiliging. Zo kunnen er op clusterniveau vergelijkingen met voorgaande jaren worden gemaakt en kan bestaande bewijslast om de volwassenheidsniveaus aan te tonen worden hergebruikt voor het nieuwe toetsingskader.

5.2 Pilot met het NBA-model

Om ervaring op te doen met dit nieuwe model hebben 31 mbo-instellingen bij deze editie van de Benchmark IBP-E ook de benchmark Informatiebeveiliging volgens het NBA-model ingevuld. Het gaat daarbij bij om 69 statements, verdeeld over 15 domeinen, waarbij de volwassenheid eveneens wordt gescoord op niveau 1-5. In de tabel hieronder de domeinen van het NBA-model, met het aantal statements per domein en de gemiddelde score.

				aantal	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	**Bedrijfscontinuiteïtbeheer**	(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%**

Scores voor de 15 domeinen van het NBA-model. Totaalscore op basis van het gewogen gemiddelde.

Wat opvalt is dat de gemiddelde volwassenheidsscore volgens deze nieuwe meetlat terugvalt van 2,8 naar 2,1. In paragraaf 5.4 gaan we daar verder op in.

5.3 De hoogst en laagst scorende NBA-statements

Ook bij deze benchmark volgens het NBA-toetsingskader hebben we gekeken naar de hoogst en laagst scorende statements.

De 10 hoogst scorende statements uit het NBA-kader

GO.02	**Beleid**	1	**3,2**		0	4	19	5	3	
SC.01	**Service level overeenkomst**	1	**2,7**		1	12	14	2	2	
DM.06	**Verwijdering van data**	3	**2,7**		2	13	10	5	1	
HR.01	**Werving**	2	**2,6**		2	11	14	4	0	
IM.03	**Incidentrespons op (cyber) beveiligingsincidenten**	4	**2,6**		2	13	11	5	0	
SM.13	**Bescherming van beveiligingstechnologie**	5	**2,6**		7	4	14	6	0	
HR.06	**Veiligheidsbewustzijn**	2	**2,6**		2	9	20	0	0	
SM.11	**Network security**	5	**2,6**		0	15	14	2	0	
SM.12	**Beheersing van malware-aanvallen**	4	**2,5**		3	12	14	1	1	
CO.02	**Configuratiedatabase en baseline**	6	**2,5**		4	12	12	3	0	

De tien hoogst scorende NBA-statements. Kolommen vlnr: NBA-ID, naam statement, cluster (vorig TK), gemiddelde score, verdeling niveau 1-5.

De 10 hoogst scorende statements komen we ook tegen (zij het soms in een iets andere vorm) in het huidige ISO-gebaseerde toetsingskader en doen het daar ook relatief goed. Met stip op 1: het statement *Beleid*. Dit statement komt in grote lijnen overeen met statement 1.1 uit het huidige kader, dat daar uitkomt op een 3,4.

De 10 laagst scorende statements uit het NBA-kader

Voor de 10 laagst scorende statements geldt dat deze niet (of niet op deze manier) voorkomen in het huidige ISO-gebaseerde toetsingskader en/of dat er ook in het huidige kader al slecht op gescoord wordt. Dit zijn blinde vlekken van het huidige toetsingskader, die maken dat er in de vergelijking met het huidige toetsingskader aanvankelijk beduidend lager gescoord wordt volgend deze nieuwe meetlat (zie de volgende paragraaf).

GO.04	Architectuur	1	1,7		14	14	1	1	1	
DM.01	Data (en systeem) eigenaarschap	1	1,7		15	11	3	2	0	
SC.04	Interne beheersing bij derden	6	1,7		11	16	3	0	0	
ID.05	Periodieke beoordeling van toegangsrechten	6	1,7		13	16	0	2	0	
ID.04	Noodtoegang (envelopprocedure/breek-het-glasprocedure)	5	1,7		18	8	3	1	1	
SD.02	Toegang tot de productieomgeving door ontwikkelaars	5	1,6		12	10	2	0	0	
RM.02	Risicobeoordeling	1	1,6		14	16	1	0	0	
SM.04	Logging	6	1,5		19	8	3	0	0	
RM.01	Informatie risico- management framework	1	1,4		20	10	1	0	0	
BC.02	Testen van Disaster recovery	4	1,4		18	8	1	0	0	

De tien laagst scorende NBA-statements. Kolommen vlnr: NBA-ID, naam statement, cluster (vorig TK), gemiddelde score, verdeling niveau 1-5.

5.4 Vergelijking NBA met het huidige ISO-toetsingskader

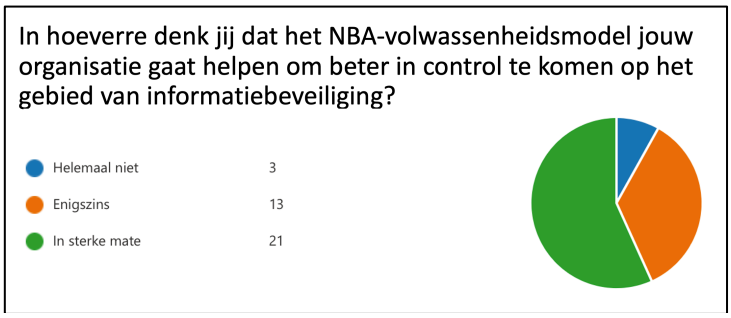
De pilot met het nieuwe toetsingskader was bedoeld om het NBA-model te kunnen vergelijken met het bestaande toetsingskader IB, ook gelet op de uitkomsten van beide benchmarks. De ervaring leert dat een derde van de NBA-statements zonder meer wordt afgedekt door bestaande bewijslast uit het huidige toetsingskader 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, vooral 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, het is vooral een belangrijk signaal richting de IBP-ers van 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. Deze meer actieve rol van het CvB bij het onderwerp informatiebeveiliging wordt de komende periode een belangrijke succesfactor.

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**

5.5 Besluit overstap NBA-model

In december 2021 zijn in het Netwerk IBP de ervaringen met het NBA-model geëvalueerd, onder andere aan de hand van een enquête onder de contactpersonen van de Benchmark IBP (zie bijlage 2). Vrijwel alle respondenten zijn van mening dat het nieuwe NBA-volwassenheidsmodel gaat helpen om beter in control te komen op het gebied van informatiebeveiliging.



Ook hebben we gevraagd of, en op welke manier we zouden moeten overstappen op het nieuwe NBA-toetsingskader. Een grote meerderheid van de respondenten heeft daarop aangegeven in 2022 over te willen stappen op het nieuwe NBA-model.

De uitkomsten van deze enquête zijn besproken tijdens de bijeenkomst van het Netwerk IBP in het mbo, op 9 december 2021 en ook bij die gelegenheid zijn aanbevelingen en feedback opgehaald uit het netwerk. Op basis hiervan heeft de regiegroep IBP het besluit genomen om met ingang van 2022 definitief over te stappen op het nieuwe NBA-toetsingskader voor Informatiebeveiliging.

6. Conclusies en aanbevelingen

Tot slot gaan we in dit hoofdstuk in op de belangrijkste bevindingen, suggesties en aanbevelingen.

Ambitieniveau van 3,0 wordt niet gehaald

Hoewel we kleine stapjes vooruitzetten behalen we ons gemiddelde ambitieniveau van 3,0 ook in 2021 niet. Het blijkt toch een hele uitdaging om die laatste stap te zetten en dat heeft er ook mee te maken dat - naarmate de volwassenheid hoger is- het relatief meer inspanning vergt om deze verder te verhogen. Tot slot worden instellingen ook meer bewust-onbekwaam: risico's zijn beter in beeld, maar dat leidt niet tot een verhoging (in enkele individuele gevallen zelfs tot een verlaging) van de volwassenheidsscores.

Grote verschillen in volwassenheid: versterk de samenwerking

We zien we grote verschillen in volwassenheid tussen de instellingen (zie paragraaf 4.1). De top 10 scoort gemiddeld een volwassenheidsniveau van 3,5 en de laatste 10 een 2,1 gemiddeld. Kleine instellingen hebben steeds meer moeite om aan de toenemende eisen op cyberveiligheid te voldoen. Binnen het netwerk IBP is veel bereidheid om te delen en elkaar te helpen dus daar ligt zeker een kans om samen te werken. Vanuit MBO Digitaal willen we daarom nog sterker inzetten op samenwerken. Ook onderzoeken we de mogelijkheden om expertise te bundelen en laagdrempelig aan te bieden aan instellingen met ondersteuningsbehoefte. Ook in de samenwerking met SURF wordt nagedacht over een gezamenlijk Security Expertise Centrum.

Versterking van clusters 5 en 6: MFA en SOC/SIEM

Cluster 6 met betrekking tot controle en logging is met 0,2 licht gegroeid ten opzichte van vorig jaar. Dat was te verwachten na de toegenomen aandacht na recente ransomware-aanvallen in de sector. De eerste mbo's zijn aangesloten op SURFsoc en een aantal instellingen kiest voor eigen SOC/SIEM oplossingen. Vanuit OCW is de ambitie uitgesproken om alle mbo's op een SOC aan te sluiten en dat zal richting MBO Digitaal en SURF veel vragen gaan opleveren. We zullen vanuit MBO Digitaal in overleg met OCW en SURF kijken naar een goede aanpak die ook past bij kleinere instellingen.
Multifactor authenticatie (MFA) wordt steeds vaker toegepast, ook voor studenten. Vanuit de hack bij ROC Mondriaan kwam naar voren dat zelfs via het compromitteren van een studentenaccount veel informatie kon worden verzameld door de hackers over mogelijke kwetsbaarheden in het netwerk. Binnen het netwerk IBP delen de instellingen hun ervaringen bij de implementatie van MFA.

De peer review geeft zicht op betrouwbaarheid

De peer review is een belangrijk instrument om de betrouwbaarheid van de benchmark te kunnen onderbouwen. Aan de peer review 2021 hebben 39 benchmarkdeelnemers meegedaan en daarbij werd 95% van de onderzochte statements vastgesteld. Zie verder www.mbodigitaal.nl/ibpdoc32b. De peer review wordt in 2022 voor de derde keer op grote schaal uitgevoerd, opnieuw in twee scenario's:

1. Online peer-carrousel
   Instelling A reviewt instelling B, B reviewt C enzovoort.
2. Online expert review
   Daarbij voert een externe expert de review uit. De kosten hiervan zijn voor rekening van de instelling.

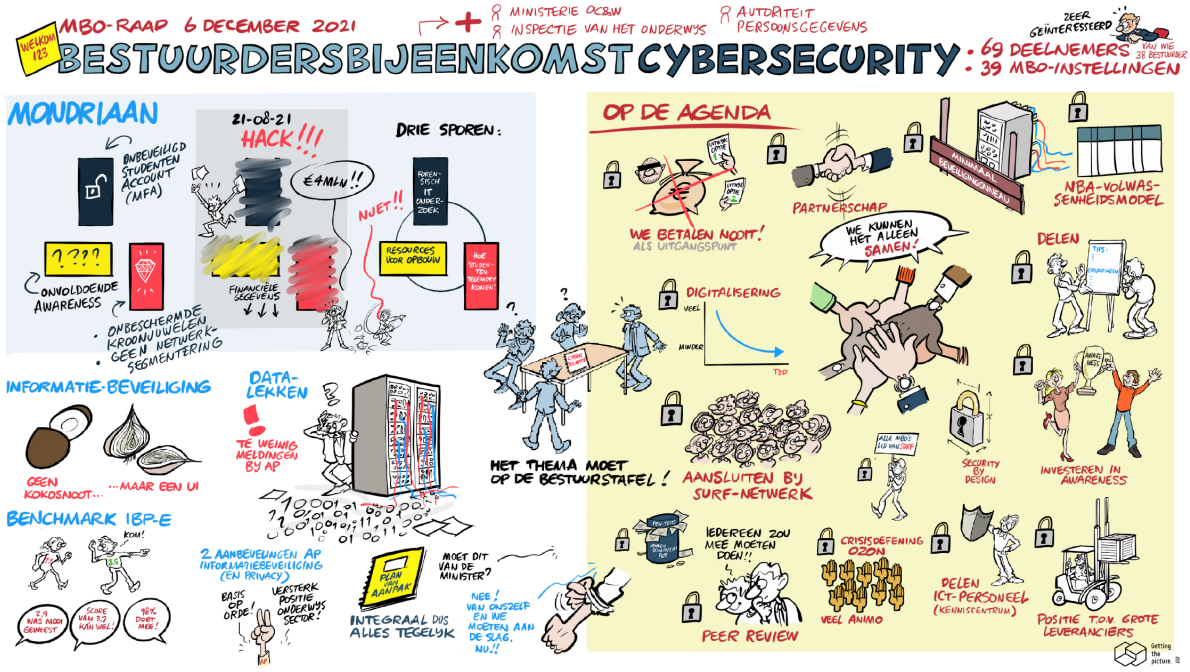
De set van 10 statements is door de regiegroep IBP bepaald en het proces is inmiddels opgestart. De reviews worden in januari en februari 2022 door de instellingen uitgevoerd en de rapportage is begin maart '22 gereed. Aan deze editie van de peer review doen 35 instellingen mee; minder dan op gerekend maar verklaarbaar vanwege de overstap naar het NBA-model.
Overigens wordt het door deze overstap naar het NBA-model ook mogelijk om de reviews in de toekomst (deels) door een onafhankelijke auditor te laten uitvoeren. Op die manier kunnen we nog beter de betrouwbaarheid van de benchmark aantonen.

Het nieuwe NBA-model informatiebeveiliging: ondersteuning en training

Nu het besluit is genomen om met ingang van dit jaar de Benchmark IB af te nemen op basis van het NBA-toetsingskader is het belangrijk om het trainingsprogramma hiervoor door te zetten en het ook te gaan richten op nieuwe doelgroepen. De 2-daagse masterclasses die in het kader van de NBA-pilot in het najaar van 2021 zijn georganiseerd worden in 2022 voortgezet. Daarbij wordt ook een 1-daagse variant aangeboden. Ook komen er trainingen voor lijnmanagers, omdat ook zij met het nieuwe model te maken krijgen. Waar mogelijk werken we samen met SURF, dat is immers de winst van de overstap naar dit nieuwe model dat ook in het ho wordt gebruikt.
Omdat het NBA-model niet alleen voor de benchmark van belang is, maar ook heel geschikt is als intern instrument voor risicobeheersing, zullen we vanuit MBO Digitaal ook inzetten op ondersteuning op dat gebied. Dat kan bijvoorbeeld door het aanbieden van een modelaanpak voor het beheren van de roadmap op het gebied van informatiebeveiliging, inclusief passende software-ondersteuning (bijvoorbeeld m.b.v. Excel, Sharepoint). Ook het delen van ervaringen over dit onderwerp binnen het netwerk IBP krijgt aandacht.

Bestuurlijke betrokkenheid wordt nog belangrijker

De bestuurlijke aandacht voor informatiebeveiliging werd al eerder als succesfactor genoemd. Het NBA-volwassenheidsmodel is sterk gebaseerd op een risicoafweging per statement, om op basis daarvan het vereiste volwassenheidsniveau te bepalen en de daarbij passende maatregelen te nemen. Voor die risico-afweging is de actieve rol van het bestuur cruciaal. Cyberveiligheid is geen ict-feestje maar raakt de hele organisatie. Ook eventuele sectorbrede afspraken, bijvoorbeeld over het elkaar kunnen bijstaan in tijden van cybercrisis kunnen alleen op bestuurlijk niveau gemaakt worden. Begin december hebben we vanuit MBO Digitaal een bestuurdersbijeenkomst over cyberveiligheid georganiseerd, zie hieronder het visuele verslag.



Ook in 2022 zetten we vanuit MBO Digitaal en de MBO Raad in op het informeren en betrekken van bestuurders bij dit onderwerp; via themabijeenkomsten en de reguliere vergadermomenten zoals de regiobijeenkomsten en de algemene ledenvergadering.

Plan van aanpak cyberveiligheid in het mbo

Naar aanleiding van Kamervragen heeft de minister toegezegd met de koepels in gesprek te gaan over wat nodig is in de onderwijssector om weerbaarder te worden tegen cyberaanvallen. Vanuit MBO Digitaal / MBO Raad stemmen we hierover af met de koepels Vereniging Hogescholen (VH) en de Universiteiten van Nederland (UNL) en met SURF. Ons plan van aanpak cyberveiligheid mbo dient als uitgangspunt voor de gesprekken met OCW hierover, die in het eerste kwartaal van 2022 worden gepland. We zien in ons plan veel

parallellen met de roadmap van SURF in het kader van de Innovatiezone Cyberveiligheid en sluiten daarbij zoveel mogelijk aan.

Samenwerken aan cyberveiligheid

We hebben een bewogen 2021 achter de rug waarin cyberveiligheid opnieuw veel aandacht heeft gekregen. Op de valreep kregen we nog te maken met de Log4J kwetsbaarheid, waarvoor veel applicaties en leveranciers moesten worden onderzocht. Op deze manier werd weer eens duidelijk hoe belangrijk het is om snel informatie te delen en goed samen te werken in tijden van crisis.
In 2021 hebben opnieuw vrijwel alle mbo's deelgenomen aan de benchmark IBP-E en we hebben met elkaar besloten om over te gaan naar een nieuw toetsingskader voor informatiebeveiliging. De invoering daarvan betekent een flinke tijdsinvestering voor de individuele instellingen en dat we hiervoor de handen op elkaar hebben gekregen laat zien dat we een hecht netwerk zijn, verantwoordelijk voor elkaar, beseffend dat we de vraagstukken op het gebied van IBP alleen samen onder controle krijgen.

Namens de Regiegroep IBP in het mbo wensen wij allen een mooi nieuw IBP-jaar toe.

Bram Bogers (Onderwijsgroep Tilburg)
Klaske Bouma (Friesland College)
Niels Hilhorst (ROC van Amsterdam)
Martijn van Hoorn (Yuverta)
Ralph Kronieger (Mediacollege Amsterdam)
Henk Links (ROC A12 / COG)
Wim Nijenhuis (NOVA College)
Fung Yee Poon (Aventus)
Samantha (S.R.Y.) Rodolf – Lejeune (VISTA College)
Jozien Winterman - Ensing (ROC van Twente)

Bart Bosma (SURF)
Peter Vermeijs (MBO Raad)
Martijn Bijleveld (MBO Digitaal / Kennisnet)

Bijlage 1: Scores Informatiebeveiliging

Beleid en organisatie

Nr.	ISO27002	Statement		Niveau 1 t/m 5						
1.1	5.1.1	Beleidsregels voor informatiebeveiliging	P-E	3,4		0	2	30	23	0
1.2	vervallen									
1.3	5.1.2	Beoordeling van het Informatiebeveiligingsbeleid		3,1		1	12	23	19	0
1.4	6.1.1	Taken en verantwoordelijkheden informatiebeveiliging:		2,9		0	19	21	15	0
1.5	6.1.5	Informatiebeveiliging in projectbeheer	P	2,5		4	24	22	5	0
1.6	6.2.1	Beleid voor mobiele apparatuur	P	2,9		3	11	28	13	0
1.7	8.2.1	Classificatie van informatie	P	2,7		2	25	16	12	0
1.8	8.2.2	Informatie labelen	P	2,6		6	17	25	7	0
1.9	10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	P-E	2,8		5	12	29	9	0
1.10	vervallen									
1.11	11.2.5	Verwijdering van bedrijfsmiddelen		3,2		1	5	31	18	0
1.12	vervallen									
1.13	13.2.2	Overeenkomsten over informatietransport		3,3		0	1	38	15	1
1.14	14.1.1	Analyse en specificatie van informatiebeveiligingseisen		2,7		6	13	28	8	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
1.20	18.1.4	Privacy en bescherming van persoonsgegevens	P	3,3		0	4	29	22	0
1.21	6.1.2	Scheiding van taken		2,9		1	15	29	10	0
1.22	6.1.3	Contact met overheidsinstanties		3,3		0	6	29	20	0
1.23	6.1.4	Contact met speciale belangengroepen		3,4		1	2	30	20	2
1.24	8.2.3	Behandelen van bedrijfsmiddelen		2,7		4	19	23	9	0
1.25	18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen		2,5		6	22	21	6	0
1.26	18.1.2	Intellectuele eigendomsrechten		2,9		5	12	24	14	0
1.27	18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen		2,5		9	17	22	7	0
		Gemiddelde cluster 1		2,9						

Personeel, studenten en gasten

2.1	7.1.2	Arbeidsvoorwaarden	P	2,6		7	16	26	6	0
2.2	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	P	2,6		4	20	23	8	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
2.6	16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging		2,7		4	17	24	10	0
2.7	7.1.1	Screening		3,3		1	6	27	17	4
2.8	6.2.2	Telewerken (thuiswerken)	E	2,7		4	12	33	6	0
2.9	7.2.3	Disciplinaire procedure		2,7		4	16	25	10	0
2.10	vervallen									
2.11	7.2.1	Directieverantwoordelijkheden		2,0		19	20	13	3	0
		Gemiddelde cluster 2		2,7						

Ruimtes en apparatuur

3.1	vervallen									
3.2	8.3.2	Verwijderen van media		3,1		1	6	38	8	2
3.3	11.1.1	Fysieke beveiligingszone		2,7		4	14	30	7	0
3.4	11.1.2	Fysieke toegangsbeveiliging		2,6		4	17	30	4	0
3.5	11.1.3	Kantoren, ruimten en faciliteiten beveiligen	E	2,6		4	14	36	1	0
3.6	11.1.4	Beschermen tegen bedreigingen van buitenaf		3,1		2	8	29	15	1
3.7	11.1.5	Werken in beveiligde gebieden		2,6		3	20	26	6	0
3.8	11.1.6	Laad- en loslocatie		2,6		4	20	24	7	0
3.9	11.2.1	Plaatsing en bescherming van apparatuur		2,7		4	16	27	8	0
3.10	11.2.2	Nutsvoorzieningen		3,3		1	7	25	20	2
3.11	11.2.3	Beveiliging van bekabeling		3,0		2	11	27	15	0
3.12	11.2.4	Onderhoud van apparatuur		3,1		0	8	34	12	1
3.13	11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein		2,9		2	13	30	10	0
3.14	11.2.7	Veilig verwijderen of hergebruiken van apparatuur	P	3,1		2	5	34	12	2
3.15	12.4.4	Kloksynchronisatie		3,3		1	3	30	19	2
3.16	8.1.1	Inventariseren van bedrijfsmiddelen		3,1		3	8	25	19	0
3.17	8.1.2	Eigendom van bedrijfsmiddelen		3,1		2	7	30	16	0
3.18	8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen		3,0		1	12	26	16	0
3.19	8.1.4	Teruggeven van bedrijfsmiddelen		3,0		0	11	31	13	0
3.20	8.3.1	Beheer van verwijderbare media		2,5		7	16	29	3	0
3.21	8.3.3	Media fysiek overdragen	E	2,6		6	19	23	7	0
		Gemiddelde cluster 3		2,9						

Continuïteit

4.1	12.1.2	Wijzigingsbeheer		2,7		3	17	27	7	1
4.2	12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen		2,9		2	12	31	8	2
4.3	12.2.1	Beheersmaatregelen tegen malware		3,2		2	6	25	22	0
4.4	vervallen									
4.5	12.3.1	Back-up van informatie	P	3,3		1	4	28	20	2
4.6	vervallen									
4.7	12.5.1	Software installeren op operationele systemen		3,2		3	3	31	17	1
4.8	12.6.1	Beheer van technische kwetsbaarheden		3,0		1	12	27	14	1
4.9	12.6.2	Beperkingen voor het installeren van software		2,9		1	17	22	15	0
4.10	14.2.6	Beveiligde ontwikkelomgeving		3,0		3	11	26	13	2
4.11	15.2.2	Beheer van veranderingen in dienstverlening van leveranciers		2,5		7	20	20	8	0
4.12	16.1.4	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen		3,2		2	7	27	18	1
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
4.16	12.1.1	Gedocumenteerde bedieningsprocedures		2,7		6	15	21	13	0
4.17	12.1.3	Capaciteitsbeheer		2,9		3	8	34	9	1
4.18	17.1.1	Informatiebeveiligingscontinuïteit plannen		2,5		10	13	26	6	0
4.19	17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren		2,4		10	21	18	6	0
		Gemiddelde cluster 4		2,9						

Vertrouwelijkheid en integriteit

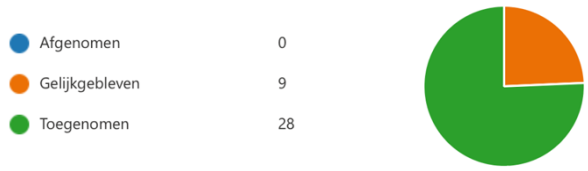
5.1	9.1.1	Beleid voor toegangsbeveiliging	P	2,7		3	18	29	4	1
5.2	9.1.2	Toegang tot netwerken en netwerkdiensten	P-E	2,9		3	12	29	11	0
5.3	9.2.1	Registratie en afmelden van gebruikers	P-E	3,0		5	8	27	14	1
5.4	9.2.2	Gebruikers toegang verlenen	P	2,9		3	9	33	9	1
5.5	9.2.3	Beheren van speciale toegangsrechten	P	2,9		2	13	29	11	0
5.6	9.2.4	Beheer van geheime authenticatie-informatie van gebruikers	P	3,1		1	8	31	15	0
5.7	9.3.1	Geheime authenticatie-informatie gebruiken	P	3,1		1	7	32	15	0
5.8	9.4.1	Beperking toegang tot informatie	P	2,7		2	16	32	5	0
5.9	9.4.2	Beveiligde inlogprocedures	P-E	3,0		1	12	30	11	1
5.10	10.1.2	Sleutelbeheer	P	2,7		4	16	30	5	0
5.11	vervallen									
5.12	12.4.2	Beschermen van informatie in logbestanden	P-E	2,4		8	21	21	5	0
5.13	vervallen	niet relevant (13.1.1; Beheersmaatregelen voor netwerken)								
5.14	13.1.2	Beveiliging van netwerkdiensten		3,0		2	11	27	15	0
5.15	13.1.3	Scheiding in netwerken		3,2		3	5	27	19	1
5.16	13.2.3	Elektronische berichten	P-E	2,5		4	19	31	1	0
5.17	14.1.3	Transacties van toepassingen beschermen		3,0		6	9	28	3	9
5.18	9.4.3	Systeem voor wachtwoordbeheer		3,1		0	8	31	16	0
5.19	9.4.4	Speciale systeemhulpmiddelen gebruiken		2,6		10	12	24	9	0
5.20	vervallen									
5.21	vervallen									
5.22	vervallen									
5.23	14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen		2,8		4	12	28	11	0
5.24	vervallen									
5.25	vervallen									
5.26	vervallen									
5.27	14.3.1	Bescherming van testgegevens	P	2,1		13	26	14	1	0
5.28	vervallen	niet relevant (15.1.1)								
		Gemiddelde cluster 5		2,8						

Controle en logging

6.1	9.2.5	Beoordeling van toegangsrechten van gebruikers	P-E	2,5		4	25	20	5	1
6.2	12.4.1	Gebeurtenissen registreren	P-E	2,4		7	21	26	1	0
6.3	12.4.3	Logbestanden van beheerders en operators	E	2,1		13	23	17	2	0
6.4	vervallen									
6.5	vervallen									
6.6	14.2.9	Systeemacceptatietests		2,7		6	18	21	9	1
6.7	15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers		2,2		10	26	15	4	0
6.8	16.1.7	Verzamelen van bewijsmateriaal		2,4		11	17	23	4	0
6.9	18.2.2	Naleving van beveiligingsbeleid en –normen	P	2,7		6	14	23	12	0
6.10	18.2.3	Beoordeling van technische naleving	P	2,5		8	13	30	4	0
6.11	vervallen									
6.12	12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen		2,4		12	17	19	7	0
6.13	16.1.6	Lering uit informatiebeveiligingsincidenten		3,1		1	9	30	14	1
6.14	18.2.1	Onafhankelijke beoordeling van informatiebeveiliging		3,0		1	11	31	12	0
		Gemiddelde cluster 6		2,6						

Bijlage 2: Respons vragenlijst

Vraag 1: Is in het algemeen binnen jouw organisatie de aandacht voor IBP in 2021 veranderd?



Gelijk gebleven (9x geantwoord)

- Er mag meer aandacht voor zijn. De gedachte onderwijs komt eerst is er nog sterk maar de gedachte AVG is onderdeel van het onderwijs moet nog komen.
- Net gefuseerd, is het te moeilijk om deze vraag te beantwoorden.
- Meestal gelijk, we merken dat we ook wel kritischer zijn als er zaken niet genoeg worden opgepakt. Het E deel hebben we nu kritischer beoordeeld omdat er steeds meer digitaal wordt afgenomen en men het centrale proces wel goed op orde heeft, maar de decentrale processen nog onvoldoende.
- Door Corona is er wel veel aandacht geweest voor IBP in het kader van online/hybride onderwijs. Maar voor de andere processen en onderdelen was dit niet het geval.
- Ivm Corona stond IBP niet hoog op de lijst van prioriteiten, al droeg landelijk nieuws daar weer wel aan bij.
- Binnen onze organisatie al langer veel aandacht voor.
- We hebben veel wijzigingen in het management.
- Werk nu minder dan een jaar in het mbo, en moet dit een beetje inschatten nu.

Toegenomen (28x geantwoord)

- Het gaat niet snel en het is een lange weg.
- Er zijn een groot aantal risico beperkende maatregelen genomen of gepland.
- Voor zover het er nu uitziet lijkt de bewustwording voor IBP te zijn verbeterd. Signalen geven aan dat het college van bestuur er meer aandacht voor heeft gekregen. Hopelijk blijft dit zo en is dit geen incidentele opleving.
- Meer fte beschikbaar. Landelijke aandacht doet goed.
- Het nieuwe strategische beleid IBP en benchmark NBA versterken elkaar. De eerste stappen voor meer participatie in de organisatie op de verschillende deelonderwerpen zijn nu gezet.
- RVT stelt ook vragen. Komt met name door de hacks die voorgaande periode geweest zijn.
- Met name IB is nadrukkelijker onder de aandacht gebracht van onze IT-afdeling
- Meer aandacht en tijd voor beveiliging, waarschijnlijk door de gebeurtenissen bij UM en Mondriaan
- Vooral vanuit Raad van Bestuur en Raad van Toezicht wordt steeds meer belang gehecht aan de staat van IT-governance en informatiebeveiliging van de organisatie.
- Vooral door Universiteit Maastricht, ROC Mondriaan en andere security-incidenten in het onderwijs.
- Vanwege de recente hacks, vooral die bij Mondriaan, staat IBP hoog op de agenda bij het bestuur.
- Door de ontwikkelingen om ons heen denk bijv. aan Mondriaan.
- De aandacht wordt vergroot door de recente hacks. Maastricht is geen incident gebleken en het onderwijs is laaghangend fruit voor de hack-sector (zie Mondriaan en Han-college).
- Dat heeft alles te maken met de recente aanvallen.
- Zelf meer "lawaai" gemaakt, mede door NBA. Diverse casussen in het land, andere grote veranderingen op ICT gebied afgerond waardoor ruimte op de agenda.
- Met name voor cybersecurity vanwege een grote phishing incident en de hacks bij andere instellingen.
- Door een bewustwordingstraject met verplichte e-learning is het meer gaan leven.
- Meer aandacht voor awareness/pentests etc.
- Hack Mondriaan heeft geholpen.
- Nav de vorige benchmark willen we aandacht geven aan de 1.0 scores. Daarna ook door externen laten kijken (testen) hoe we qua beveiliging ervoor staan.

Vraag 2: In hoeverre hebben recente cyberaanvallen in onze sector invloed gehad (UvA/HvA/HAN/ROC Mondriaan) invloed gehad op de aandacht voor IBP binnen jouw organisatie?

Helemaal niet (2x geantwoord)

- Het is bij ons nog echt 'trekken' om de aandacht op dit onderwerp te krijgen. Governance in het geheel staat nog in de kinderschoenen.

Enigszins (16x geantwoord)

- Op een kleine groep veel invloed, maar op een grote groep weinig.
- B.v. door versnelde invoering van 2FA voor alle medewerkers, dus niet alleen de sleutelfiguren. En ook wordt er vooruit gekeken naar de studenten op dat vlak. Wat dat betreft hebben we nu het momentum.
- Zeker vanuit bestuur vaak de vraag of onze organisatie dit ook kan overkomen en wat we eraan kunnen doen.
- SOC/SIEM of MDR staat op de agenda, evenals het 3-lines model.
- We zijn zeker gealarmeerd over deze aanvallen en dit leidt ook wel tot meer urgentie om maatregelen te nemen. In dat opzicht zijn die aanvallen dan toch ergens goed voor.
- Vervroegd invoeren van MFA.
- Er is meer bewustwording dat privacy/security als schil zeer belangrijk is voor onder meer de continuïteit. Daardoor komt er ook meer budget beschikbaar om dit zo goed mogelijk te regelen.
- Mede op basis van Mondriaan, Maastricht en ook onze eigen 'aanval' hebben het urgentiebesef verhoogd.
- Hier zonder stond het ook wel op de bril, er was bijv. al een sessie met alle betrokkenen gepland maar er was wel hierdoor momentum om snel acties op te pakken.
- De hacks op de andere instellingen hebben wel enige invloed, maar een grote phishing aanval (alle medewerkers kregen een phishing mail via het account van een collega) had meer impact. Het veroorzaakte heel veel paniek onder de medewerkers omdat hen ook direct raakte.
- Wel op de hoogte van de Cyber aanvallen. Maar dat dit betekend dat er meer geïnvesteerd moet worden in mensen en voorzieningen is nog niet doorgedrongen.
- Als uit een benchmark blijkt dat jouw organisatie nog niet op orde is, moet je daar aandacht aan gaan geven. De recente cyberaanvallen bevestigen dat.
- CvB en directie hebben contacten bij Mondriaan hierdoor komt het nu dichtbij.

In sterke mate (19x geantwoord)

- Het CvB vraagt bij iedere hack wat wij hebben gedaan om te voorkomen dat het bij ons kan gebeuren.
- No pain no gain.... het komt op deze manier wel erg dicht bij.
- Ook omdat de Raad van Toezicht hierin is geïnteresseerd.
- Dit kan ons ook gebeuren.
- Besef van eigen kwetsbaarheid is gegroeid en gevoel van urgentie daaraan iets te moeten doen
- Beetje jammer dat dit de wake-up call is. En tegelijk ben ik er erg blij mee.
- We zijn niet onkwetsbaar, dat dringt nu ook door in de hoogste regionen van de organisatie.
- Er wordt de vraag aan mij gesteld "kan dit ons ook overkomen" We werken samen met Mondriaan.
- Het is niet meer de vraag of je gehackt wordt maar wanneer. Dat vraagt om een volwassener beleid op het gebied van IBP-E. Het NBA-model kan daarbij ondersteunen. Maar er zijn ook nog blinde vlekken merk ik.
- Men ziet de bui echt wel hangen inmiddels.
- Van elk lek proberen we de belangrijkste zaken mee te nemen. Zo bijvoorbeeld de offline backup na de lek bij Maastricht. Dit hebben we nu goed ingeregeld.
- Digitalisering krijgt meer aandacht, daaruit volgt al bredere aandacht. IBP is niet alleen gericht op hacks en hackers, maar de aanvallen leiden wel tot extra aandacht.

Vraag 3: Hebben jullie de benchmark IB volgens het NBA-model ingevuld?

Zo ja: wat zijn je eerste ervaringen met het NBA-model?

- Ik ben van mening dat het NBA-model de mbo-instellingen gaat helpen met de betrouwbaarheid van de informatiebeveiliging op de scholen. Door het NBA-model is het mogelijk de niveaus te laten bevestigen door de accountants.
- Met name onze IT-jongens vinden het NBA-toetsingskader veel beter aansluiten bij de praktijk.
- Hier en daar dezelfde "scope"-issues als bij het oude kader. Soms is de volgorde niet even logisch (wijziging, escalatie/crisis/calamiteit en business-continuity b.v.).
- Eerste ervaring is dat het meer een IT breed risicomanagement kader is. Ook dit kader is heel multi-interpretabel. Er zit geen specifiek privacy normenkader meer in, wat gaan we daarmee doen?
- Het kader is duidelijk, prettig dat het minder statements zijn. Voor aantal statements moeten we nieuwe stukken schrijven.
- Goed. Wel afwijkend, voornamelijk ook in terminologie (we hadden net de termen uit het vorige model bij ons ingevoerd zodat we allemaal over hetzelfde praten). Maar ook op changemanagement, problemmanagement en datamanagement is er weer genoeg te doen... Stukje over ontwikkeling dacht ik kwijt te zijn met die toetsingskader, maar zit er toch nog wel in.
- Het is veel overzichtelijker dan het ISO-kader.
- Wennen maar over het algemeen goed te scoren. Hogere scores lijken ook echt iets toe te voegen.
- Het was behoorlijk zoeken naar hoe je naar de statements kijkt en wat 'voldoende' bewijsvoering betekent. Desalniettemin voelde de statement als logisch en relevant.
- De vraagstelling is prettiger en beter geschikt voor intern gebruik. Het is duidelijker voor de eigenaren van de verschillende processen waarom de vragen worden gesteld.
- Examen en privacy zijn ondervertegenwoordigd, volwassenheid model is vergelijkbaar met ISO 27001, echter meer concreet dan de invulling die we volgens sa mbo it gebruikte
- Positief. Het NBA-model trekt de toetsing van informatiebeveiliging uit de technische IT-hoek/afdeling en stelt veel meer de informatiebeveiliging binnen alle geledingen van de organisatie aan de orde.
- Gaat ons nog veel papierwerk opleveren.

Zo nee: waarom niet?

- Compliance heeft dit jaar voor het eerst proces begeleid rondom benchmark (op verzoek CvB). Focus lag 100% op huidige ISO-toetsingskader. Masterclass is al wel gevolgd door mij (SO), maar nog niet door Compliance (deze maand).
- Keuze: concentreren op benchmark, niet tegelijk meerdere zaken, inzet uren.
- Geen ervaring, dus, met nba.
- Te weinig tijd tussen de cursus en de deadline. We zijn wel bezig een eerste scan te doen. Dat lukt redelijk.
- Zover zijn we hier nog niet.
- Voor nu een te grote tijdsinvestering. Bevindingen met het model vanuit de informatie die we hebben gekregen zijn goed.
- Te weinig tijd. Ik vul hem later in.
- Er was onvoldoende tijd om mezelf hierin voldoende te verdiepen zodat ik deze met de juiste gegevens kon vullen. Hopelijk worden er nog trainingen georganiseerd waarbij ik de gelegenheid heb om voldoende kennis en kunde op te doen om bij de volgende benchmark wel het NBA-toetsingskader met de juiste informatie in te vullen.
- Te weinig tijd en nog onvoldoende voorbereid op het model.
- Onvoldoende tijd voor.
- Tijdsgebrek: De vacature voor IBP-Coördinator is nog niet ingevuld.
- Nog niet alle leden NBA-training gevolgd.
- We aan één school gevraagd om enkele vragen in te vullen volgens NBA. Ik ben zelf wel druk bezig met het invullen voor de organisatie - Dus wel ervaring opgedaan maar we hebben alleen het oude model ingeleverd. Ik ben bezig om dit te gebruiken voor onze eigen baseline.
- Te kort op de masterclass. Daar pas echt de benodigde kennis opgedaan. Plus in onze grote organisatie hebben we met veel mensen te maken die tot voor kort niets deden met benchmarks. Je hebt maar een kans om het goed op de rit te krijgen. Dit gaan wij komende jaar doen d.m.v. IBP-governance waarbij we voor NBA dan de juiste mensen erbij betrekken.

Vraag 4. Gaat het NBA-model je helpen om beter in control te komen?

Helemaal niet (3x geantwoord)

- Benchmark is iets wat een keer per jaar wordt ingevuld, het gaan gebruiken als besturingssysteem is iets wat nog moet komen.
- Kan de vorige vraag niet beantwoorden omdat ik geen kennis heb van/over NBA.
- Hoezo zijn we met de benchmark niet/onvoldoende in control? Geen ervaring, onvoldoende kennis, kan deze vraag eigenlijk niet beantwoorden, maar moest iets invullen. Heb ook niet de indruk dat de instellingen zijn meegenomen in het besluit. Ook daarom vind ik mezelf onvoldoende inhoudelijk op de hoogte om deze vraag te kunnen beantwoorden.

Enigszins (13x geantwoord)

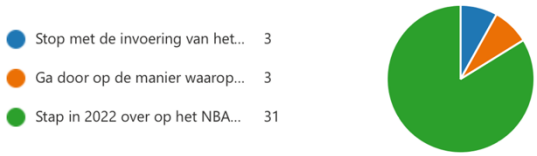
- Bij de sambo-ict benchmark waren er lastige en/of irrelevante items. Bij de NBA is dit ook zo.
- Het NBA-kader helpt niet per se om 'beter' in control te komen. Het helpt wel om het breder bekend en gedragen te krijgen.
- Het is goed om een algemeen beeld te vormen en de onderdelen te inventariseren waar je nog (te) weinig maatregelen voor hebt ingericht. Het vraagt om veel meer detaillering om echt een goed oordeel te kunnen geven over een bepaald onderdeel.
- Doordat de middelen beperkt zijn, zullen we onze tijd efficiënt moeten inzetten en kunnen we dus niet optimaal gaan voor een ''top'' eindresultaat. Voordeel is wel dat we dat nu in beeld kunnen brengen.
- Kan over het NBA-model eigenlijk nog heel weinig zeggen. Vermoed dat met de nadruk op risico inschattingen de kans aanwezig is dat we beter zicht krijgen waar de meeste aandacht qua informatiebeveiliging naartoe moet gaan.
- Hangt ook af van de betrokkenheid van het seniormanagement.
- Hangt af van de opstelling van de bestuurder. Als die serieus aan de slag gaat met risicomanagement dan is dat een win.
- Het is 'slechts' een model en dus een hulpmiddel. Het 'in control zijn' is nooit alleen het resultaat van een model.
- We hebben het nog niet ingevuld. Dus hebben we nog geen goed beeld.
- Nog geen ervaring met NBA.

In sterke mate (21x geantwoord)

- Je merkt dat heel veel nog niet is beschreven en dat geeft het NBA-kader aan. Fijn dat iets in de hoofden zit maar daar kan een ander weinig mee.
- Organisatie meer betrekken bij dit kader.
- Het scherpt alles weer aan, dat is altijd goed.
- Het biedt allerlei mogelijkheden om IBP te laten samenwerken met de processen in de organisatie, vooral om dat het compacter is en daardoor de aansluiting met de organisatie beter te maken is.
- De statements en de lijstjes bij de scores lezen bijna als een handleiding om de organisatie te verbeteren. Je kan bij wijze van spreken elke week een statement pakken en deze stap voor stap verbeteren. Het kader is duidelijk in de eisen die gesteld worden, terwijl het oude kader vooral vragen opriep.
- De concrete producten die benoemd worden als richtlijn voor het jaarplan.
- Het geeft duidelijke handvatten en zet het bestuur in haar rol om te sturen op doelstellingen.
- Beter geschikt voor bewustwording van de eigenaren.
- Het NBA-model is veel meer organisatie gericht.
- Verantwoordelijkheden worden duidelijker en hoger in de organisatie gelegd.
- We gaan van een groot aantal losse, meer technische, items naar een meer integrale benadering met verantwoordelijkheden en eigenaren. Dat levert naar verwachting een betere verantwoordelijkheidsverdeling en eigenaarschap waar het hoort te liggen.

- Door de goede voorlichting.
- Ik heb de masterclass NBA gevolgd. Daarbij is mij duidelijk geworden, dat het model beter past bij de inschatting van de risico's bij informatiebeveiliging.
- Het zorgt ervoor dat de aandacht erop blijft vanuit het eigenaarschap en daarmee komt en blijft het meer op de agenda.

Vraag 5: 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 (3x geantwoord)

- Model maakt weinig uit, het gaat om de echte verbetering en het voorkomen van een verkeerde scope, 90 of meer procent van de hacks begint bij Social engineering, modellen houden dit niet tegen.
- Ik zie niet waarom de huidige benchmark niet voldoet en waarom we moeten breken met wat dankzij de benchmark in gang is gezet. Dit jaar kreeg ik bijv. antwoorden terug met ideeën waar collega's mee aan de slag willen om volgend jaar hoger te kunnen scoren. Twee modellen naast elkaar: onzin. Waarom de benchmark niet verbeteren? Zo hou je een groot deel van de geschiedenis/trends.

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 (3x geantwoord)

- Eerst massa creëren, niet verplichten...

Stap in 2022 over op het NBA-toetsingskader voor de benchmark en stop met het huidige ISO-toetsingskader (31x geantwoord)

- Ook steeds gedacht dat dit de bedoeling was en dan niet op twee gedachten blijven hinken.
- Zoals eerder aangegeven drukt het NBA kader je meer met de neus op de feiten en des te meer dat de accountant dit model ook kan toetsen.
- Nu we het momentum hebben zorgen dat zo spoedig mogelijk zo veel mogelijk instellingen overgaan.
- We zullen dan wel oog moeten hebben voor (extra) ondersteuning.
- Maar maak wel een vertaalslag in de score, zodat je wel een vergelijking kunt maken met voorgaande jaren.
- Zou ook mooi zijn als er dan voor P en E aansluiting komt.
- Persoonlijk zou ik overstappen op de NBA-toetsingskader. Intern gaan we dat in elk geval wel doen.
- Dit kan wat mij betreft dan alleen als men al vroeg in het jaar de gelegenheid heeft om de masterclass te kunnen volgen en er vanuit de werkgroep voldoende ondersteuning gegeven kan worden zodat het NBA-toetsingskader wel met de juiste kennis ingevuld kan worden.
- In ieder geval de keuze voor 1 toetsingskader. Dat toetsingskader wat in Nederland het meest breed gedragen is.
- Helaas ontbreekt optie 4: Stap over op het NBA-toetsingskader, maar verlies het ISO-toetsingskader niet uit het oog. Certificeringen worden steeds belangrijker, en dat kan niet met NBA. Wel met ISO. ;-)
- Ik denk dat het NBA beter is.
- Twee toetsingskaders is simpelweg te veel werk.
- Scheelt enorm veel tijd in dubbel werk.
- Het goed invullen van een toetsingskader kost al de nodige tijd en capaciteit. Van 2 toetsingskaders dus nog meer.
- 2x kaders is 2x zoveel werk en 4x zoveel discussie, toelichting etc.
- Beide is te arbeidsintensief.
- Dubbel invullen is zonde van de tijd. Het NBA-model is het meest passend.
- Niet te lang blijven hangen in het oude. De vernieuwing is ruim van tevoren aangekondigd.
- Er moet zsm duidelijkheid komen of en vanaf wanneer we als mbo-sector over gaan. Dit moet ik ook rapporteren naar onze RvB.
- Belangrijk om een keuze te maken en niet beide of meerdere modellen te hanteren. Elke model heeft z'n voor- en nadelen en is sowieso niet perfect. Maak nu de keuze over te stappen of niet.

- Twee kaders is 2 keer het werk.
- Twee modellen is halfslachtig, maak een keuze.
- Ik denk dat we weinig keus hebben en is de beslissing voor de overstap naar het NBA al genomen.
- Er is dit jaar voldoende ruimte geboden om kennis te maken en twee modellen naast elkaar blijven hanteren is niet efficiënt en effectief. Het versnelt de stap naar een grotere volwassenheid en bevordert ook de kwaliteitscirkel (PDCA) op basis waarvan het geen losse acties zijn, maar dat het onderwijs meer in control is.
- Als we dit met zijn allen willen, dan moeten we er ook vol voor gaan.
- Als het NBA het nieuwe kader wordt, dan gaan we de roadmap baseren op het NBA. De score van de ISO wordt dan bijzaak.