De Benchmark IBP-E

en het NBA Volwassenheidsmodel Informatiebeveiliging

1. De resultaten van de Benchmark IBP-E
2. Het toetsingskader als stuurinstrument
   -ervaringen vanuit Zadkine (Richard de Koning)
3. Het NBA Volwassenheidsmodel Informatiebeveiliging
4. Het NBA Volwassenheidsmodel als gids voor informatiebeveiliging
   -ervaringen vanuit COG / ROC A12 (Henk Links & Ludo Cuijpers)
5. De overstap naar het NBA-model als toetsingskader voor de benchmark IB

Samantha Rodolf (VISTA College, vz Regiegroep IBP)
Martijn Bijleveld (MBO Digitaal, adviseur IBP)

28-01-2022
Conferentie MBO Digitaal

mbo digitaal

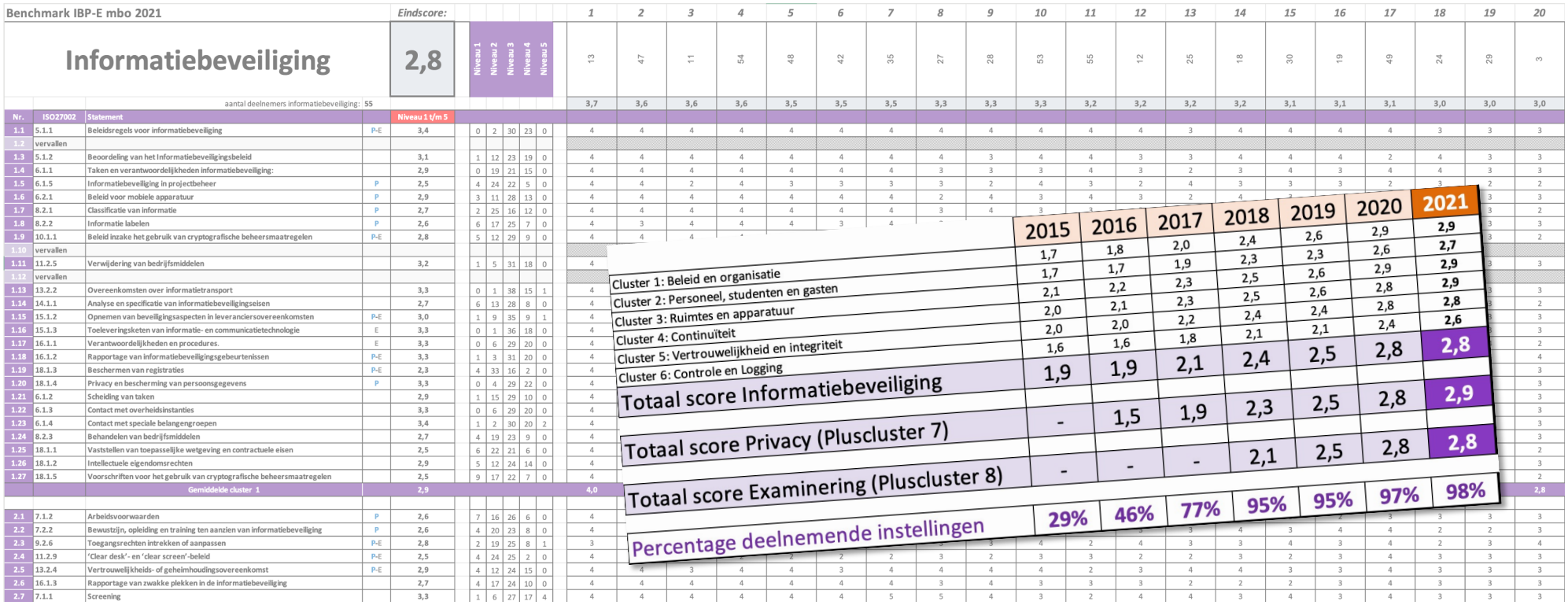
Toetsingskader en benchmark: tweeledig doel

- Verantwoording
  - Intern
  - Naar elkaar
  - Externe stakeholders
- Intern stuurinstrument
  - Risicobeheersing
  - Roadmap IBP
  - Jaarplan IBP

Toetsingskader informatiebeveiliging		
Cluster	**1**	**Beleid en organisatie**
Statement	**1.4**	**Taken en verantwoordelijkheden informatiebeveiliging**
Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.		
Toelichting Alle verantwoordelijkheden voor informatiebeveiliging behoren duidelijk te zijn gedefinieerd en gedocumenteerd als onderdeel van het IBP-beleid. Dat betekent dat voor belangrijke processen als het beheren van de netwerkinfrastructuur, het beheren van toegangsrechten of het maken van back-ups de (eind)verantwoordelijkheden zijn belegd en gedocumenteerd, in overeenstemming met het beleid.		
Bewijsvoering Het IBP-beleid omvat de governance van de informatiebeveiliging, met een beschrijving van alle functies en rollen, bijvoorbeeld aan de hand van het 3-lines of defence model.		
2 Overleg het IBP-beleid met betrekking tot de governance, waarin functies, rollen en verantwoordelijkheden duidelijk zijn beschreven.		
3 Overleg een overzicht met namen, functies en rollen en check voor enkele medewerkers, bijvoorbeeld door middel van een interview, of deze hun taken op basis van dit overzicht/beleid uitvoeren.		
Document	Model informatiebeveiliging en privacy beleid IBPDOC6	
Zie ook	1.1	

mbo digitaal

Resultaten Benchmark IBP-E 2021



Benchmark IBP-E mbo 2021 — Eindscore: 2,8

Informatiebeveiliging

aantal deelnemers informatiebeveiliging: 55

Nr.	ISO27002	Statement		Niveau 1 t/m 5	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
										13	47	11	54	48	42	35	27	28	53	55	12	25	18	30	19	49	24	29	3
										3,7	3,6	3,6	3,6	3,5	3,5	3,5	3,3	3,3	3,3	3,2	3,2	3,2	3,2	3,1	3,1	3,1	3,0	3,0	3,0
1.1	5.1.1	Beleidsregels voor informatiebeveiliging	P-E	3,4	0	2	30	23	0	4	4	4	4	4	4	4	4	4	4	4	4	3	4	4	4	4	3	3	3
1.2	vervallen																												
1.3	5.1.2	Beoordeling van het Informatiebeveiligingsbeleid		3,1	1	12	23	19	0	4	4	4	4	4	4	4	4	3	4	4	3	3	4	4	4	2	4	3	3
1.4	6.1.1	Taken en verantwoordelijkheden informatiebeveiliging:		2,9	0	19	21	15	0	4	4	4	4	4	4	4	3	3	3	4	3	2	3	4	3	4	4	3	3
1.5	6.1.5	Informatiebeveiliging in projectbeheer	P	2,5	4	24	22	5	0	4	4	2	4	3	3	3	3	2	4	3	2	4	3	3	3	2	3	2	2
1.6	6.2.1	Beleid voor mobiele apparatuur	P	2,9	3	11	28	13	0	4	4	4	4	4	4	4	2	4	3	4	3	2	4	3	3	3	3	3	3
1.7	8.2.1	Classificatie van informatie	P	2,7	2	25	16	12	0	4	4	4	4	4	4	4	3	4	3	3	3	3	4	3	3	3	3	3	2
1.8	8.2.2	Informatie labelen	P	2,6	6	17	25	7	0	4	3	4	4	4	3	4	3	3	3	3	3	3	3	3	3	3	3	3	3
1.9	10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	P-E	2,8	5	12	29	9	0	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	2
1.10	vervallen																												
1.11	11.2.5	Verwijdering van bedrijfsmiddelen		3,2	1	5	31	18	0	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	3
1.12	vervallen																												
1.13	13.2.2	Overeenkomsten over informatietransport		3,3	0	1	38	15	1	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	3
1.14	14.1.1	Analyse en specificatie van informatiebeveiligingseisen		2,7	6	13	28	8	0	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	2
1.15	15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	P-E	3,0	1	9	35	9	1	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	3
1.16	15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	E	3,3	0	1	36	18	0	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	3
1.17	16.1.1	Verantwoordelijkheden en procedures.	E	3,3	0	6	29	20	0	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	2
1.18	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	P-E	3,3	1	3	31	20	0	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4
1.19	18.1.3	Beschermen van registraties	P-E	2,3	4	33	16	2	0	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	3
1.20	18.1.4	Privacy en bescherming van persoonsgegevens	P	3,3	0	4	29	22	0	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	3
1.21	6.1.2	Scheiding van taken		2,9	1	15	29	10	0	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	3
1.22	6.1.3	Contact met overheidsinstanties		3,3	0	6	29	20	0	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	3
1.23	6.1.4	Contact met speciale belangengroepen		3,4	1	2	30	20	2	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	3
1.24	8.2.3	Behandelen van bedrijfsmiddelen		2,7	4	19	23	9	0	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	3
1.25	18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen		2,5	6	22	21	6	0	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	2	2
1.26	18.1.2	Intellectuele eigendomsrechten		2,9	5	12	24	14	0	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	3
1.27	18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen		2,5	9	17	22	7	0	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	2	2
		Gemiddelde cluster 1		2,9						4,0																		2,8	
2.1	7.1.2	Arbeidsvoorwaarden	P	2,6	7	16	26	6	0	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	3
2.2	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	P	2,6	4	20	23	8	0	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	3
2.3	9.2.6	Toegangsrechten intrekken of aanpassen	P-E	2,8	2	19	25	8	1	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	3
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	P-E	2,5	4	24	25	2	0	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	3
2.5	13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	P-E	2,9	4	12	24	15	0	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	3
2.6	16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging		2,7	4	17	24	10	0	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	3
2.7	7.1.1	Screening		3,3	1	6	27	17	4	4	4	4	4	4	4	5	5	4	3	2	4	4	3	4	3	4	3	3	3

	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%

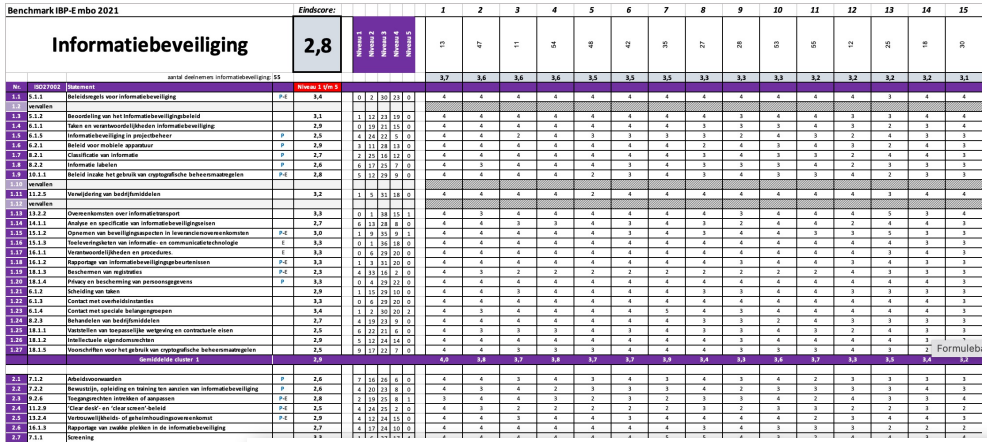
mbo digitaal

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%**

mbo digitaal

Resultaten Benchmark IBP-E 2021 - Informatiebeveiliging



Benchmark IBP-E mbo 2021 — Eindscore: 2,8

Informatiebeveiliging

aantal deelnemen informatiebeveiliging: 55

Nr.	ISO27002	Statement		Niveau 1 t/m 5	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
					13	47	11	54	48	42	35	27	28	53	55	12	25	18	30
					3,7	3,6	3,6	3,6	3,5	3,5	3,5	3,3	3,3	3,3	3,2	3,2	3,2	3,2	3,1
1.1	5.1.1	Beleidsregels voor informatiebeveiliging	P-E	3,4	0	2	30	23	0	4	4	4	4	4	4	4	4	3	4	4
1.2	vervallen																			
1.3	5.1.2	Beoordeling van het Informatiebeveiligingsbeleid		3,1	1	12	23	19	0	4	4	4	4	4	3	4	4	3	3	4	4
1.4	6.1.1	Taken en verantwoordelijkheden informatiebeveiliging:		2,9	0	19	21	15	0	4	4	4	4	4	3	3	4	3	2	3	4
1.5	6.1.5	Informatiebeveiliging in projectbeheer	P	2,5	4	24	22	5	0	4	4	2	4	3	3	3	3	2	4	3	3
1.6	6.2.1	Beleid voor mobiele apparatuur	P	2,9	3	21	28	13	0	4	4	4	4	4	4	2	4	3	2	4	3
1.7	8.2.1	Classificatie van informatie	P	2,7	2	25	16	12	0	4	4	4	4	4	3	3	4	3	2	4	4
1.8	8.2.2	Informatie labelen	P	2,6	6	17	25	7	0	4	3	4	4	4	3	3	3	4	2	3	3
1.9	10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	P-E	2,8	5	12	29	9	0	4	4	4	4	2	3	4	3	4	2	3	3
1.10	vervallen																				
1.11	11.2.5	Verwijdering van bedrijfsmiddelen		3,2	1	5	31	18	0	4	4	4	4	2	4	4	4	4	3	4	4
1.12	vervallen																				
1.13	13.2.2	Overeenkomsten over informatietransport		3,3	0	1	38	15	1	4	3	4	4	4	4	3	4	4	4	5	3	4
1.14	14.1.1	Analyse en specificatie van informatiebeveiligingseisen		2,7	6	13	28	8	0	4	4	3	3	4	3	2	4	4	2	4	4	3
1.15	15.1.2	Opnemen van beveiligingsaspecten in leverancieovereenkomsten	P-E	3,0	1	9	35	9	1	4	4	4	4	4	3	4	4	3	3	5	3	3
1.16	15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	E	3,3	0	1	36	18	0	4	4	4	4	4	4	4	4	4	4	3	3	3
1.17	16.1.1	Verantwoordelijkheden en procedures	E	3,3	0	6	29	20	0	4	4	4	4	4	4	4	4	4	4	3	4	3
1.18	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	P-E	3,3	1	3	31	20	0	4	4	4	4	4	3	4	4	3	4	3	3	3
1.19	18.1.3	Beschermen van registraties	P-E	2,3	4	33	16	2	0	4	3	2	2	2	2	2	2	4	3	3	3	3
1.20	18.1.4	Privacy en bescherming van persoonsgegevens	P	3,3	0	4	29	22	0	4	4	4	4	4	4	4	4	4	4	4	4	3
1.21	6.1.2	Scheiding van taken		2,9	1	15	29	10	0	4	4	3	4	4	4	3	3	4	3	3	3	3
1.22	6.1.3	Contact met overheidsinstanties		3,3	0	6	29	20	0	4	4	4	4	4	4	4	4	4	4	4	4	3
1.23	6.1.4	Contact met speciale belangengroepen		3,4	1	2	30	20	2	4	3	4	4	4	5	4	3	4	4	4	4	3
1.24	8.2.3	Behandelen van bedrijfsmiddelen		2,7	4	19	23	9	0	4	4	4	4	4	3	3	2	4	3	3	3	3
1.25	18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen		2,5	6	22	21	6	0	4	3	3	3	4	3	3	4	3	2	4	3	3
1.26	18.1.2	Intellectuele eigendomsrechten		2,9	5	12	24	14	0	4	4	4	4	4	4	3	4	4	4	4	3	3
1.27	18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen		2,5	9	17	22	7	0	4	4	3	3	4	4	3	3	4	3	2	2	2
		Gemiddelde cluster 1		2,9						4,0	3,8	3,7	3,8	3,7	3,7	3,9	3,4	3,3	3,6	3,7	3,3	3,5	3,4	3,2
2.1	7.1.2	Arbeidsvoorwaarden	P	2,6	7	16	26	6	0	4	4	3	4	3	4	3	4	2	3	3	3	3
2.2	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	P	2,6	4	20	23	8	0	4	3	4	2	3	3	3	3	3	3	4	3	3
2.3	9.2.6	Toegangsrechten intrekken of aanpassen	P-E	2,8	3	19	25	8	1	3	4	4	3	2	3	2	3	3	4	2	4	3
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	P-E	2,5	4	24	25	2	0	4	3	2	2	2	2	3	2	3	3	2	2	3
2.5	13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	P-E	2,9	4	12	24	15	0	4	4	3	4	4	3	4	4	2	3	4	4	3
2.6	16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging		2,7	4	17	24	10	0	4	4	4	4	4	3	4	3	3	3	2	2	2
2.7	7.1.1	Screening																				
2.8	6.2.2	Telewerken (thuiswerken)																				
2.9	7.2.3	Disciplinaire procedure																				
2.10	vervallen																					
2.11	7.2.1	Directieverantwoordelijkheden																				
		Gemiddelde cluster 2																				
3.1	vervallen																					
3.2	8.3.2	Verwijderen van media																				
3.3	11.1.1	Fysieke beveiligingszone																				
3.4	11.1.2	Fysieke toegangsbeveiliging																				
3.5	11.1.3	Kantoren, ruimten en faciliteiten beveiligen																				
3.6	11.1.4	Beschermen tegen bedreigingen van buitenaf																				
3.7	11.1.5	Werken in beveiligde gebieden																				
3.8	11.1.6	Laad- en losplaatsen																				
3.9	11.2.1	Plaatsing en bescherming van apparatuur																				
3.10	11.2.2	Nutsvoorzieningen																				
3.11	11.2.3	Beveiliging van bekabeling																				
3.12	11.2.4	Onderhoud van apparatuur																				
3.13	11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein																				
3.14	11.2.7	Veilig verwijderen of hergebruiken van apparatuur																				
3.15	12.4.4	Kloksynchronisatie																				
3.16	8.1.1	Inventariseren van bedrijfsmiddelen																				
3.17	8.1.2	Eigendom van bedrijfsmiddelen																				
3.18	8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen																				
3.19	8.1.4	Teruggeven van bedrijfsmiddelen																				
3.20	8.3.1	Beheer van verwijderbare media																				
3.21	8.3.3	Media fysiek overdragen																				
		Gemiddelde cluster 3																				
4.1	12.1.2	Wijzigingsbeheer																				
4.2	12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen																				

- Lichte groei in cluster 2, 4 en 6
- Extra aandacht in 2021 voor cluster 6; Controle en logging
- Ambitieniveau 3,0 nog niet behaald

	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**

mbo digitaal

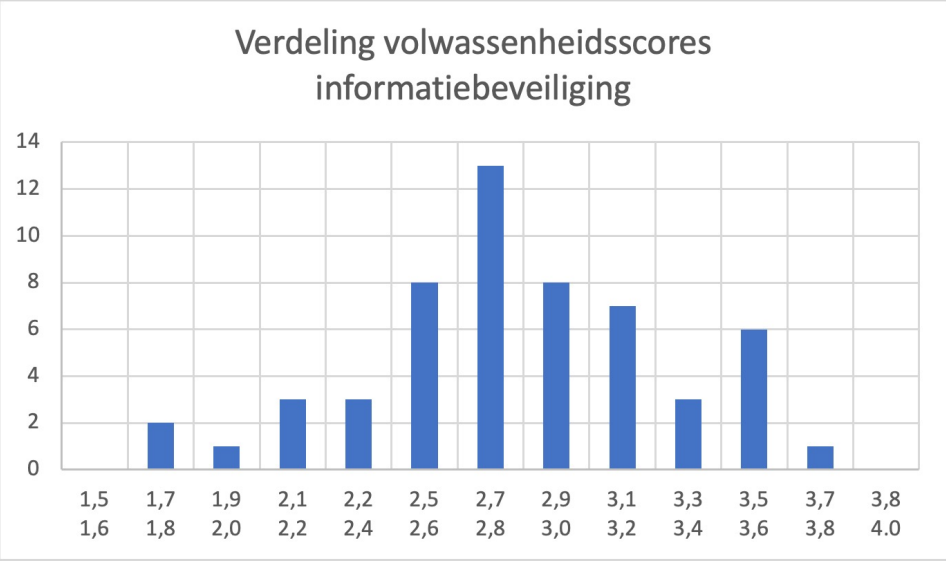
Grote verschillen in volwassenheid IB

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**



mbo digitaal

Resultaten Benchmark IBP-E 2021 - Privacy

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							

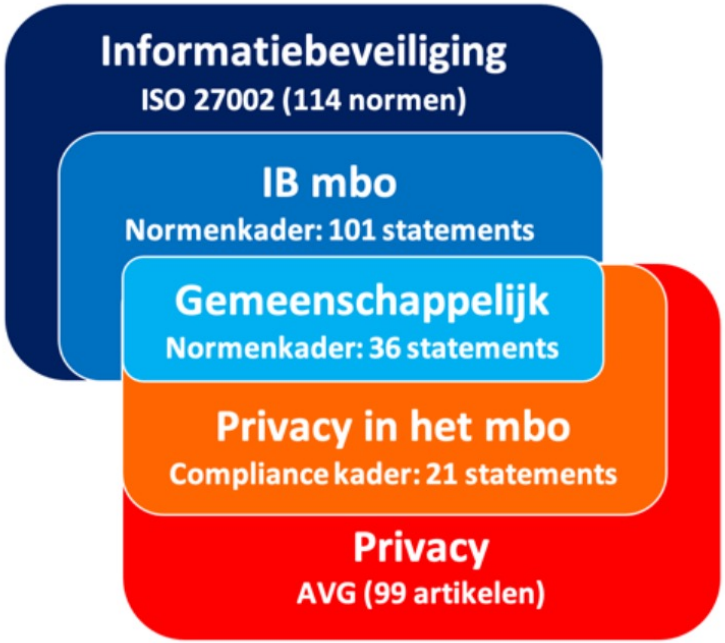
- Aandachtspunten
  - P5 Bewaartermijnen: beleid is er (N2), naleving (N3) problematisch.
  - P6 Verwerking t.b.v. onderzoek

mbo digitaal

Gemeenschappelijk normenkader IB - Privacy

Minimaal niveau 3, streefniveau 4

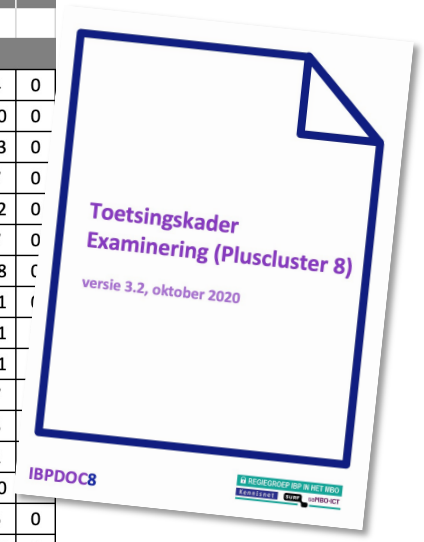
Benchmark IBPE mbo 2021				Eindscore:						
Gemeenschappelijk normenkader IB-Privacy				**2,8**						
		aantal deelnemers informatiebeveiliging:	55			Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5
Nr.	ISO27002	Statement		Niveau 1 t/m 5						
1.1	5.1.1	Beleidsregels voor informatiebeveiliging	P-E	3,4		0	2	30	23	0
1.5	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		13	17	16	10	0



mbo digitaal

Resultaten Benchmark IBP-E 2021 - Examinering

Benchmark IBPE mbo 2019		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	
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	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



mbo digitaal

Gemeenschappelijk normenkader IB - Examinering

Minimaal niveau 3, streefniveau 4

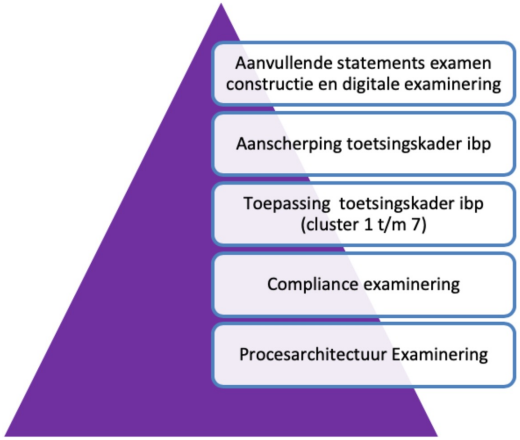
Benchmark IBPE mbo 2021

Gemeenschappelijk normenkader IB-Examinering

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
1.9	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



mbo digitaal

Peer review 2021

- Betrouwbaarheid zelfassessment aantonen
- 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**

mbo digitaal

Zadkine: toetsingskader als stuurinstrument

ZADKINE

Richard de Koning
IVP Manager

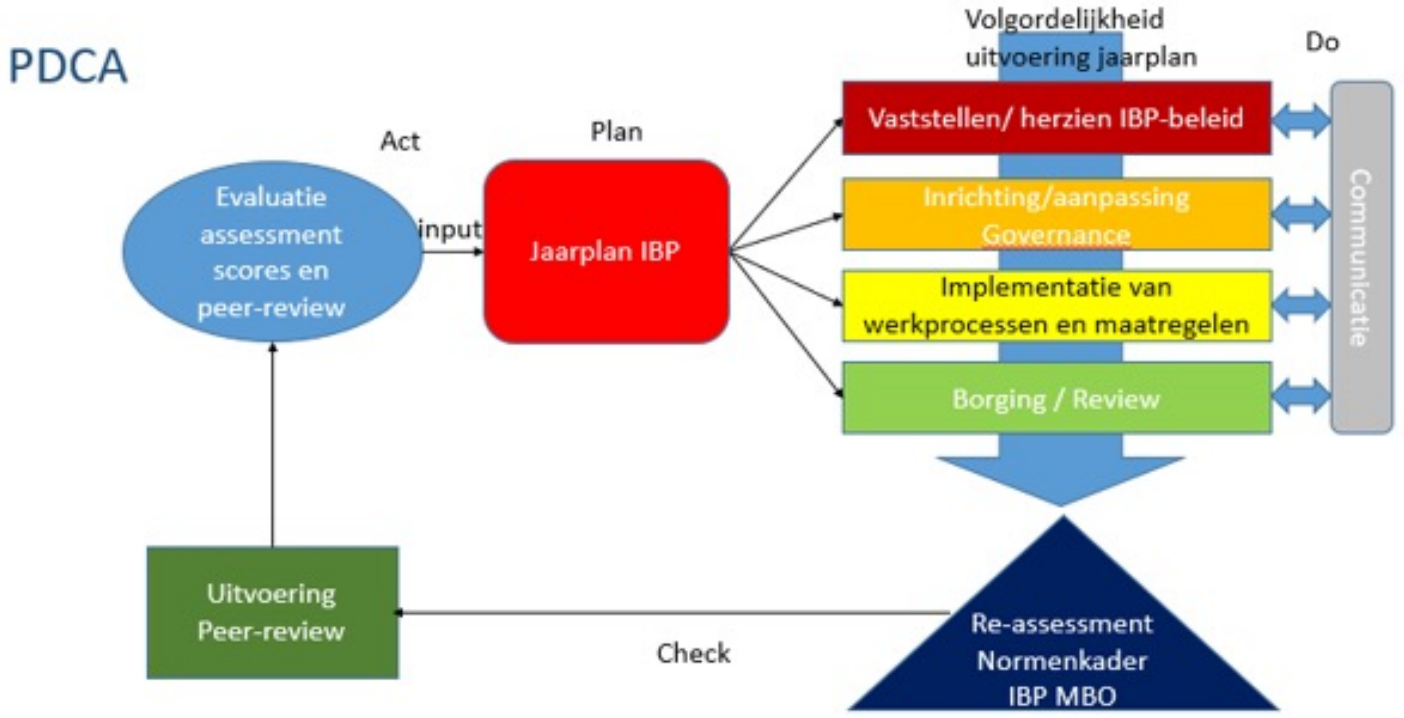
Doelstellingen

- Risico's en bedreigingen beter in beeld krijgen en houden
- Bevordering van de cyberweerbaarheid en bekendheid met IVP/IBP organisatie
- Gemiddeld volwassenheidsniveau 3 op toetsingskader IB
- Onze instelling voldoet blijvend aan AVG-wetgeving
- Aantoonbare continue verbetering

mbo digitaal

ZADKINE

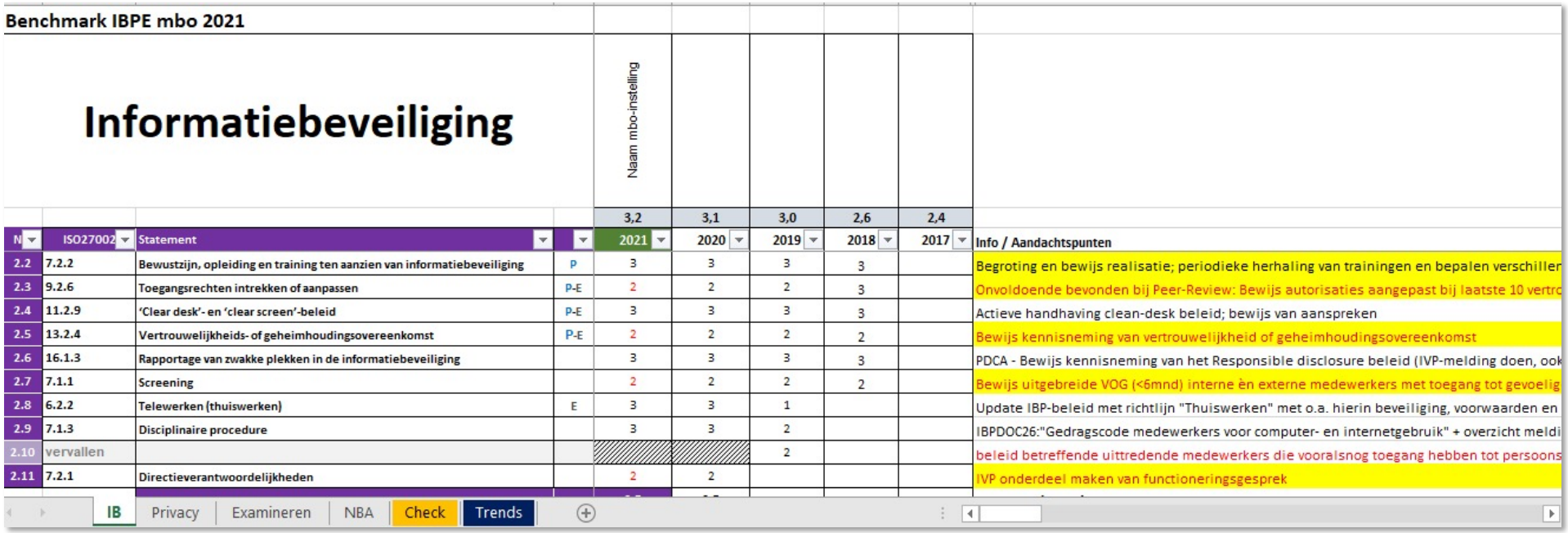
Benchmark geïntegreerd in Jaarplan



mbo digitaal

ZADKINE

IB statements > verbetermaatregelen



Benchmark IBPE mbo 2021

Informatiebeveiliging

				Naam mbo-instelling					
				3,2	3,1	3,0	2,6	2,4	
N	ISO27002	Statement		2021	2020	2019	2018	2017	Info / Aandachtspunten
2.2	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	P	3	3	3	3		Begroting en bewijs realisatie; periodieke herhaling van trainingen en bepalen verschiller
2.3	9.2.6	Toegangsrechten intrekken of aanpassen	P-E	2	2	2	3		Onvoldoende bevonden bij Peer-Review: Bewijs autorisaties aangepast bij laatste 10 vertro
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	P-E	3	3	3	3		Actieve handhaving clean-desk beleid; bewijs van aanspreken
2.5	13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	P-E	2	2	2	2		Bewijs kennisneming van vertrouwelijkheid of geheimhoudingsovereenkomst
2.6	16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging		3	3	3	3		PDCA - Bewijs kennisneming van het Responsible disclosure beleid (IVP-melding doen, ook
2.7	7.1.1	Screening		2	2	2	2		Bewijs uitgebreide VOG (<6mnd) interne èn externe medewerkers met toegang tot gevoelig
2.8	6.2.2	Telewerken (thuiswerken)	E	3	3	1			Update IBP-beleid met richtlijn "Thuiswerken" met o.a. hierin beveiliging, voorwaarden en
2.9	7.1.3	Disciplinaire procedure		3	3	2			IBPDOC26:"Gedragscode medewerkers voor computer- en internetgebruik" + overzicht meldi
2.10	vervallen					2			beleid betreffende uittredende medewerkers die vooralsnog toegang hebben tot persoons
2.11	7.2.1	Directieverantwoordelijkheden		2	2				IVP onderdeel maken van functioneringsgesprek

IB | Privacy | Examineren | NBA | Check | Trends

mbo digitaal

ZADKINE

Monitoren maatregelen

Nr.	ISO27002	Statement	2020	Eigenaar	Type Verbeteractie	Status
6.1	9.2.5	Beoordeling van toegangsrechten van gebruikers	2	Systeem/proceseigenaren	2. Autorisatiematrixen	
P.6		Verwerking t.b.v. onderzoek	3	O&K	5. Procesbeschrijving	Gereed
P.14		Geheimhouding	2	HRM	1. Updaten HR-cyclus	
P.15		Bewustzijn, opleiding en training ten aanzien van privacy	3	IVP	4. Instructie - Basistraining IVP	Gereed
P.16		Bewijs van vernietiging persoonsgegevens	2	Systeem/proceseigenaren	5. Procesbeschrijving	
E.1		Beleidsplan beveiliging examinering	2	Stuurgroep Examinering (O&K)	3. Progr. Examenprocessen	Loopt
E.2		Gedragscodes en richtlijnen afname examens	2	Stuurgroep Examinering (O&K)	1. Updaten HR-cyclus	Loopt
E.5		Archiveren en vernietigen examenmateriaal	2	Stuurgroep Examinering (O&K)	3. Progr. Examenprocessen	Loopt
E.8		Voorkomen van examenfraude	2	Stuurgroep Examinering (O&K)	3. Progr. Examenprocessen	Loopt
E.9		Procedure voorbereiden en afnemen examens	2	Stuurgroep Examinering (O&K)	3. Progr. Examenprocessen	Loopt

mbo digitaal

ZADKINE

Monitoren maatregelen n.a.v. DPIA's

	Categorie	Dreiging	Omschrijving				Beoogde maatregel				Eigenaar	Type Verbeteractie	Status
WO 07	Mens onopzettelijk	Vertrouwelijkheid van gegevens	[redacted]	4	3	12	[redacted]	2	3	6	M&C	4. Instructie - Basistraining IVP	Loopt
WO 08	Mens opzettelijk	Vertrouwelijkheid van gegevens		4	3	12		1	3	3	M&C	4. Instructie - Basistraining IVP	Loopt
WO 09	Organisatie	Vertrouwelijkheid van gegevens		4	3	12		2	3	6	M&C	2. Autorisatiematrices, rollen, eigenaars	Loopt
WO 12	Organisatie	Integriteit van gegevens		4	3	12		1	1	1	M&C	6. Standaardeisen nieuwe software - uitfaseren systeem	Loopt
IDM 05	Mens - opzettelijk	Vertrouwelijkheid		4	4	16		3	4	12	IM-IT	7. Pentest (kwetsbaarheidsonderzoek)	Plannen
												6. Standaardeisen nieuwe	

IBPE Benchmark | DPIA's | AP-meldingen | Typen Verbeteracties

mbo digitaal

ZADKINE

NBA statements > Prioriteren voor Jaarplan

Domein	NBA-ID	Statement	Cluster	2021	Eigenaar	Informatie	Prio Jaarplan
Bestuur	GO.01	Strategie	1	2	CvB (IVP)	Vertaling Missie, strategie (nog niet vastgesteld)	JA
(Governance)	GO.02	Beleid	1	5	CvB (IVP)		
	GO.03	Planning / Roadmap	1	4	IVP(IM-IT)	Integraal project- en projectportfolio nodig; roadmap	
	GO.04	Architectuur	1	2	IM-IT	EIAM publiceren en goedkeuren door het (senior) management; MORA-HORA impl	JA
	GO.05	Onafhankelijke toetsing	6	3	CvB (IVP/IM-IT)	Beter vastleggen/noteren; Afspraken maken Auditcommissie	
Organisatie	OR.01	Eigenaarschap, rollen, verantwoording en verantwoordelijkheid	1	2	CvB (IVP/IM-IT)	Intentieverklaring nodig+ 3 van de 4 oppakken (zie statement)	JA
(Organisation)	OR.02	Functiescheiding	5	3	CvB	functiescheiding implementeren en vaststellen; matrix definiëren en periodiek controleren (d.m.v. GRC tooling)	JA
Risicobeheer	RM.01	Informatie risico- management framework	1	2	FP&C (CvB en IVP)	Enkel voor IVP en ICT; niet organisatiebreed	
(Risk Management)	RM.02	Risicobeoordeling	1	2	FP&C (CvB en IVP)	DPIA's, Cybersec. Threat Analysis en verbeteroverzicht; ambitie naar 3	JA
	RM.03	Plan voor behandeling en beperking van risico's (inclusief risicoacceptatie)	1	2	FP&C (CvB en IVP)	DPIA's; mit.maatregelen worden inconsistent toegpast, onvoldoende aangepakt	JA
Personeelsbeheer	HR.01	Werving	2	2	HRM	Vragen en afstemmen bij HRM	
(Human Resources)	HR.02	Certificering, training en scholing	2	2	HRM	Vragen en afstemmen bij HRM	
	HR.03	Afhankelijkheid van individuen	2	1	CvB (HRM)	Nagaan bij CvB en HRM ('vlootschouw')	JA
	HR.04	Verandering of beeindiging van functie	2	2	HRM	Processen voor overdracht, controle bij functiewijziging	JA

IB | Privacy | Examineren | NBA | Check | Trends

mbo digitaal

Volwassenheidsmodel Informatiebeveiliging

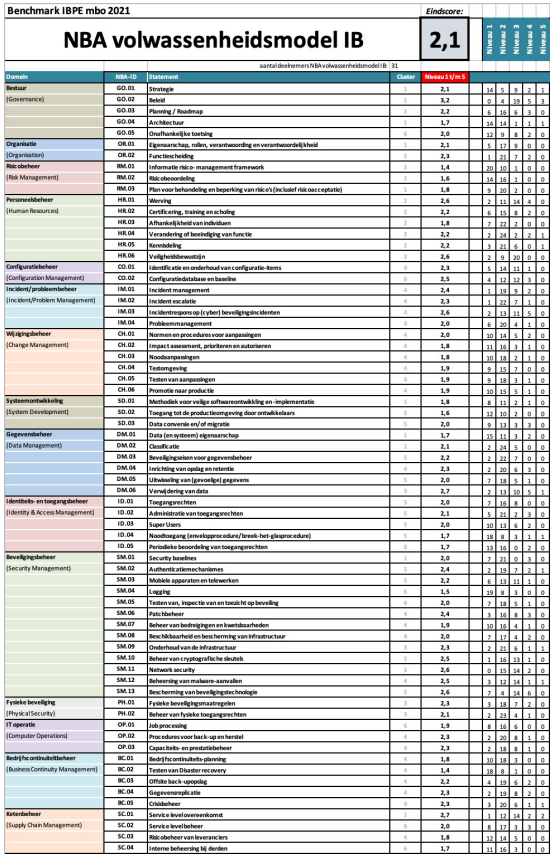
NBA: Koninklijke Nederlandse Beroepsorganisatie van Accountants
NOREA: Beroepsorganisatie van IT-auditors

M.i.v. 2022 gebruikt als nieuw toetsingskader voor het onderdeel Informatiebeveiliging.

mbo digitaal

NBA-volwassenheidsmodel Informatiebeveiliging

- Minder gericht op technische maatregelen
- Sterker gericht op de governance van de informatiebeveiliging
- Beter toegerust op gebruik clouddiensten
- Risico-gebaseerde aanpak
- Geaccepteerd model (NOREA), dus mogelijkheid om interne/externe auditors te betrekken
- Als *Volwassenheidsmodel* beter geschikt als intern stuurinstrument



Benchmark IBPE mbo 2021

Eindscore:

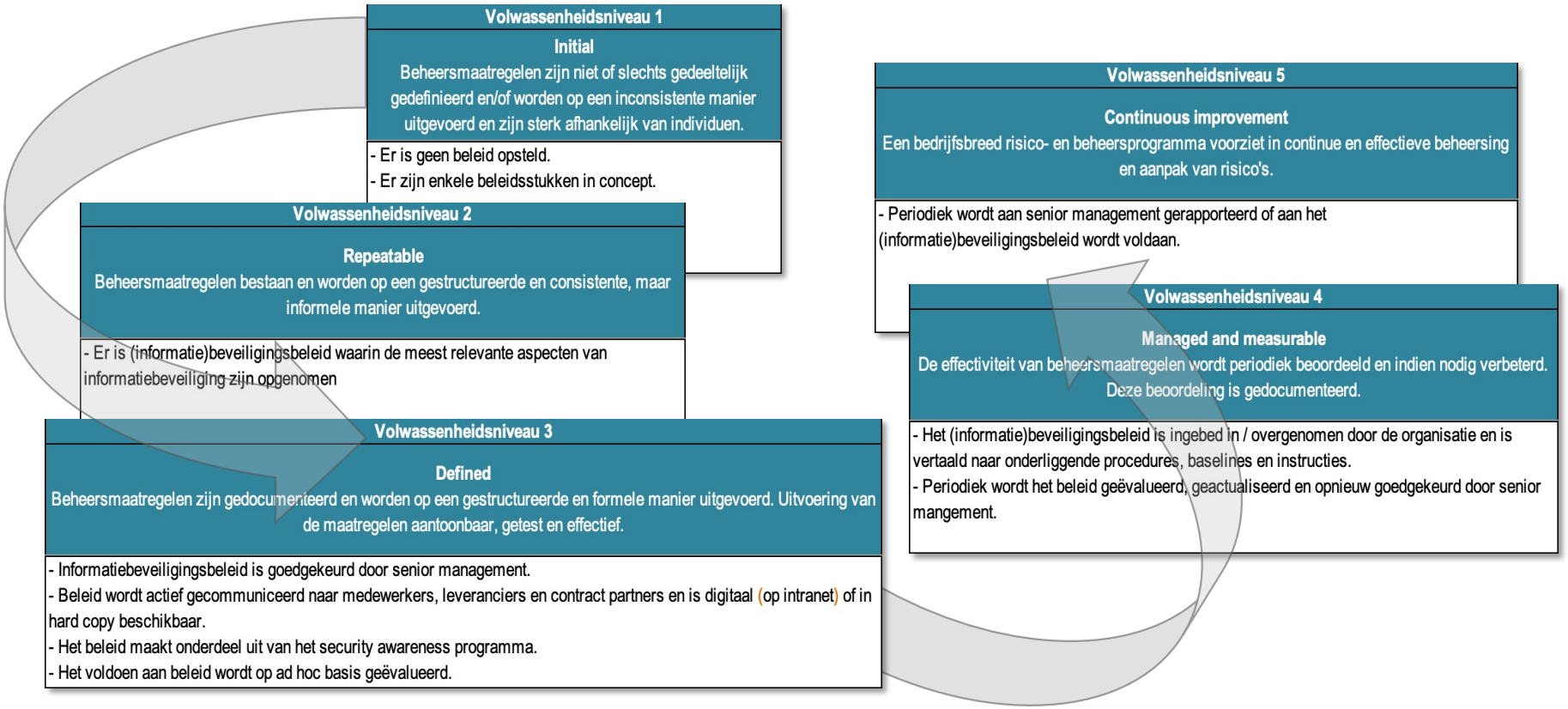
NBA volwassenheidsmodel IB — **2,1**

aantal deelnemers NBA volwassenheidsmodel IB: 31

Domein	NBA-ID	Statement	Cluster	Niveau 1 t/m 5		Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5
Bestuur	GO.01	Strategie	1	2,1		14	5	9	2	1
(Governance)	GO.02	Beleid	1	3,2		0	4	19	5	3
	GO.03	Planning / Roadmap	1	2,2		6	16	6	3	0
	GO.04	Architectuur	1	1,7		14	14	1	1	1
	GO.05	Onafhankelijke toetsing	1	2,0		12	9	8	2	0
Organisatie	OR.01	Eigenaarschap, rollen, verantwoording en verantwoordelijkheid	1	2,1		5	17	9	0	0
(Organisation)	OR.02	Functiescheiding	1	2,3		1	21	7	2	0
Risicobeheer	RM.01	Informatie risico- management framework	1	1,4		20	10	1	0	0
(Risk Management)	RM.02	Risicobeoordeling	1	1,6		14	16	1	0	0
	RM.03	Plan voor behandeling en beperking van risico's (inclusief risicoacceptatie)	1	1,8		8	20	2	0	0
Personeelsbeheer	HR.01	Werving	2	2,6		2	11	14	4	0
(Human Resources)	HR.02	Certificering, training en scholing	2	2,2		6	15	8	2	0
	HR.03	Afhankelijkheid van individuen	2	1,8		7	22	2	0	0
	HR.04	Verandering of beëindiging van functie	2	2,2		2	24	2	2	1
	HR.05	Kennisdeling	2	2,2		3	21	6	0	1
	HR.06	Veiligheidsbewustzijn	2	2,6		2	9	20	0	0
Configuratiebeheer	CO.01	Identificatie en onderhoud van configuratie-items	4	2,3		3	14	11	1	0
(Configuration Management)	CO.02	Configuratiedatabase en baseline	4	2,5		4	12	12	3	0
Incident/probleembeheer	IM.01	Incident management	4	2,4		1	19	9	2	0
(Incident/Problem Management)	IM.02	Incident escalatie	4	2,3		1	22	7	1	0
	IM.03	Incidentrespons op (cyber) beveiligingsincidenten	4	2,6		2	13	11	5	0
	IM.04	Probleemmanagement	4	2,0		8	20	4	1	0
Wijzigingsbeheer	CH.01	Normen en procedures voor aanpassingen	4	2,0		10	14	5	2	0
(Change Management)	CH.02	Impact assessment, prioriteren en autoriseren	4	1,8		11	16	3	1	0
	CH.03	Noodaanpassingen	4	1,8		10	18	2	1	0
	CH.04	Testomgeving	4	1,9		9	15	7	0	0
	CH.05	Testen van aanpassingen	4	1,9		9	18	3	1	0
	CH.06	Promotie naar productie	4	1,9		10	15	5	1	0
Systeemontwikkeling	SD.01	Methodiek voor veilige softwareontwikkeling en -implementatie	1	1,8		8	11	2	1	0
(System Development)	SD.02	Toegang tot de productieomgeving door ontwikkelaars	5	1,6		12	10	2	0	0
	SD.03	Data conversie en/of migratie	5	2,0		9	13	3	3	0
Gegevensbeheer	DM.01	Data (en systeem) eigenaarschap	1	1,7		15	11	3	2	0
(Data Management)	DM.02	Classificatie	1	2,1		2	24	5	0	0
	DM.03	Beveiligingseisen voor gegevensbeheer	5	2,2		2	22	7	0	0
	DM.04	Inrichting van opslag en retentie	6	2,3		2	20	6	3	0
	DM.05	Uitwisseling van (gevoelige) gegevens	5	2,0		7	18	5	1	0
	DM.06	Verwijdering van data	3	2,7		2	13	10	5	1
Identiteits- en toegangsbeheer	ID.01	Toegangsrechten	5	2,0		7	16	8	0	0
(Identity & Access Management)	ID.02	Administratie van toegangsrechten	5	2,1		5	21	2	3	0
	ID.03	Super Users	5	2,0		10	13	6	2	0
	ID.04	Noodtoegang (envelopprocedure/breek-het-glasprocedure)	5	1,7		18	8	1	1	1
	ID.05	Periodieke beoordeling van toegangsrechten	5	1,7		11	16	5	2	0
Beveiligingsbeheer	SM.01	Security baselines	1	2,0		7	21	0	3	0
(Security Management)	SM.02	Authenticatiemechanismes	5	2,4		2	19	7	2	1
	SM.03	Mobiele apparaten en telewerken	5	2,2		6	13	11	1	0
	SM.04	Logging	6	1,5		19	8	3	0	0
	SM.05	Testen van, inspectie van en toezicht op beveiling	6	2,0		7	18	5	1	0
	SM.06	Patchbeheer	4	2,4		3	16	8	3	0
	SM.07	Beheer van bedreigingen en kwetsbaarheden	6	1,9		10	16	4	1	0
	SM.08	Beschikbaarheid en bescherming van infrastructuur	6	2,0		7	17	4	2	0
	SM.09	Onderhoud van de infrastructuur	3	2,3		2	21	6	1	1
	SM.10	Beheer van cryptografische sleutels	5	2,5		1	16	13	1	0
	SM.11	Network security	5	2,6		0	15	14	2	0
	SM.12	Beheersing van malware-aanvallen	6	2,5		3	12	14	1	1
	SM.13	Bescherming van beveiligingstechnologie	5	2,6		7	4	14	6	0
Fysieke beveiliging	PH.01	Fysieke beveiligingsmaatregelen	3	2,3		3	18	7	2	0
(Physical Security)	PH.02	Beheer van fysieke toegangsrechten	3	2,1		2	23	4	1	0
IT operatie	OP.01	Job processing	6	1,9		8	16	6	0	0
(Computer Operations)	OP.02	Procedures voor back-up en herstel	6	2,3		2	20	8	1	0
	OP.03	Capaciteits- en prestatiebeheer	6	2,3		2	18	8	1	0
Bedrijfscontinuïteitbeheer	BC.01	Bedrijfscontinuïteits-planning	6	1,8		10	18	3	0	0
(Business Continuity Management)	BC.02	Testen van Disaster recovery	6	1,4		18	8	1	0	0
	BC.03	Offsite back-uppolicy	6	2,2		4	19	6	2	0
	BC.04	Gegevensreplicatie	6	2,3		2	19	8	2	0
	BC.05	Crisisbeheer	6	2,3		3	20	6	1	1
Ketenbeheer	SC.01	Service levelovereenkomst	1	2,7		1	12	14	2	2
(Supply Chain Management)	SC.02	Service levelbeheer	6	2,0		8	17	3	3	0
	SC.03	Risicobeheer van leveranciers	6	1,8		12	14	5	0	0
	SC.04	Interne beheersing bij derden	6	1,7		11	16	3	0	0

mbo digitaal

Beschrijving volwassenheidsniveaus: onderdeel NBA-model



mbo digitaal

Pilot NBA-model als nieuw 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	**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%**

mbo digitaal

Vergelijking scores huidig- en NBA-toetsingskader

- Statements NBA zijn via ISO27002 gemapt op huidige toetsingskader
- Vergelijking met scores oud/nieuw op clusterniveau
  - op basis van 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**

mbo digitaal

ROC A12: Ervaringen met het NBA-model als gids

ROC A 12

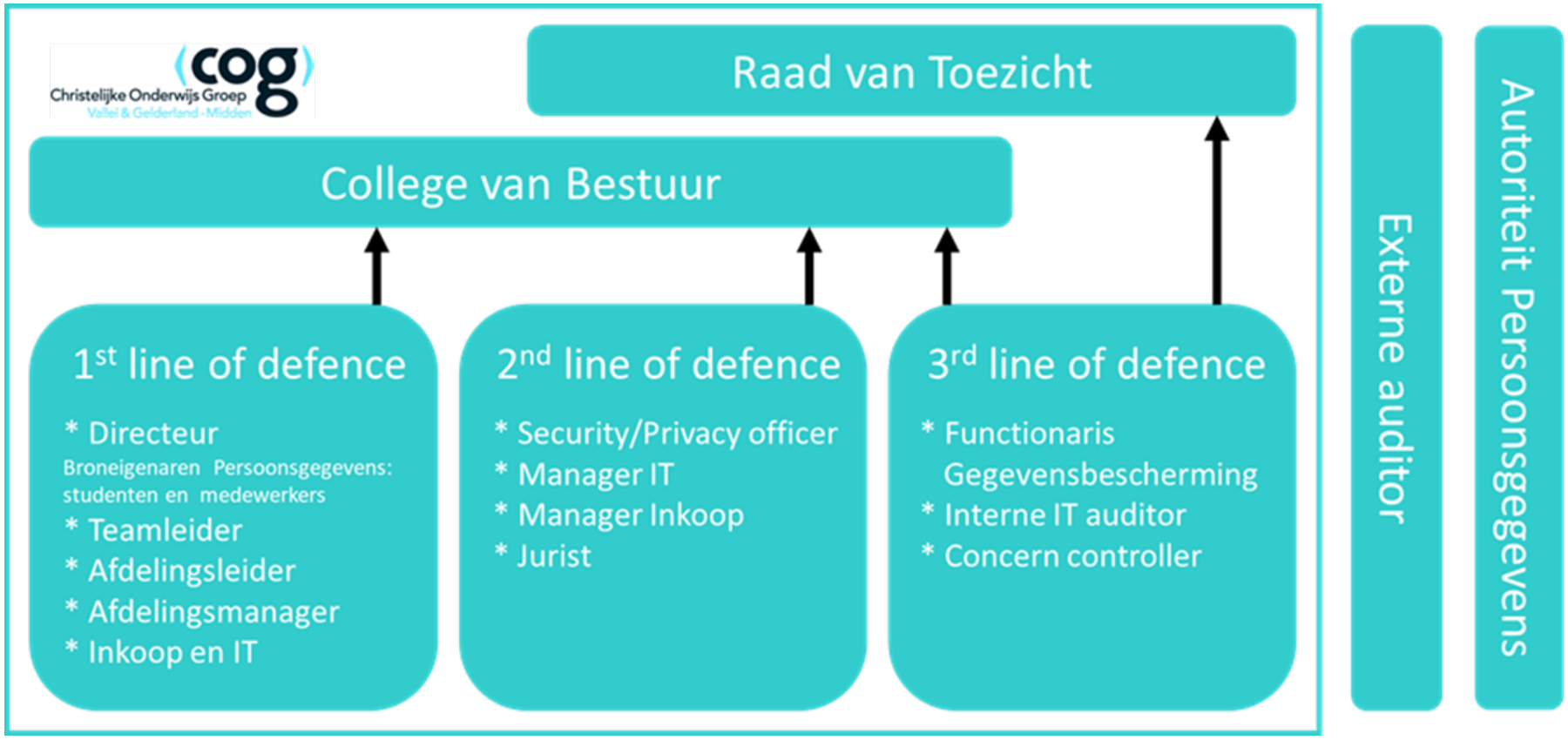
Henk Links
Security Privacy Officer

Ludo Cuijpers
IT Auditor

Het NBA volwassenheidmodel helpt ons om te zien waar we staan met betrekking tot de informatiebeveiliging. Het is onderdeel van ons risicoraamwerk waarmee we -met afgewogen risico's- tot een roadmap komen en zo concreet aan de slag gaan om onze informatiebeveiliging naar een hoger niveau brengen.

We focussen daarmee niet op hoe we scoren op de statements maar zien wel dat we hoger scoren... we groeien dus in onze volwassenheid en worden daarmee weerbaarder en minder kwetsbaar voor eventuele aanvallen.

IBP beleid


Christelijke Onderwijs Groep
Vallei & Gelderland - Midden
Raad van Toezicht
College van Bestuur
1st line of defence
* Directeur
Broneigenaren Persoonsgegevens: studenten en medewerkers
* Teamleider
* Afdelingsleider
* Afdelingsmanager
* Inkoop en IT
2nd line of defence
* Security/Privacy officer
* Manager IT
* Manager Inkoop
* Jurist
3rd line of defence
* Functionaris Gegevensbescherming
* Interne IT auditor
* Concern controller
Externe auditor
Autoriteit Persoonsgegevens

Waar we staan en onze ambitie…

4 Human resources	4.6 Veiligheidsbewustzijn			
	Huidige volwassenheidsniveau	3	Gewenste volwassenheidsniveau	5

Risico

Mensen die zich onvoldoende bewust zijn van informatiebeveiligingsrisico's begrijpen de mogelijke gevolgen van hun acties niet en kunnen die niet bij het uitvoeren van hun taken betrekken.

Doel

Er is een security-awareness programma om gebruikers bewust te maken van hun verantwoordelijkheid om de vertrouwelijkheid, beschikbaarheid en integriteit van informatie (middelen) te beschermen.

mbo digitaal

ROC A 12

Volwassenheidsniveau 1

(a) Er zijn geen security-awareness activiteiten gedefinieerd of uitgevoerd.

Volwassenheidsniveau 2

(a) Security-awareness activiteiten worden uitgevoerd op afdelingsniveau.

Volwassenheidsniveau 3

(a) Er is een security-awareness programma opgenomen in het informatiebeveiligingsplan en wordt organisatiebreed uitgevoerd.
(b) Het programma is in lijn met het (informatie)beveiligingsbeleid.

Volwassenheidsniveau 4

Aanvullend:
(a) security-awareness activiteiten bevatten een verplicht e-learning programma dat succesvol moet worden volbracht, inclusief online examen.
(b) Afronding van e-Learning modules door medewerkers wordt bewaakt en gerapporteerd aan het senior management.

Volwassenheidsniveau 5

Aanvullend:
(a) De effecten van de security-awareness activiteiten worden gemonitord.
(b) Correlatie van beveiligingsincidenten als gevolg van gebrek aan awareness leidt tot aanpassing van de beveiliging-awareness activiteiten.

4 Human resources	4.6 Veiligheidsbewustzijn	
	Huidige volwassenheidsniveau 3	Gewenste volwassenheidsniveau 5
Beleidseigenaar	<hoofd HRM>	
1. Aanpak	Niels Dutij (Functionaris voor Gegevensbescherming) Ondersteuning door Henk Links (ISO) en Ludo Cuijpers (IT auditor)	
2. Product	Scholingprogramma in gebruik d.m.v. een e-learning tool (Privacy bekwaam)	
3. Planning en (mogelijke) kosten	Februari t/m mei 2022	
Beleidsuitvoerder	1e lijn	

Alle leidinggevende medewerkers van de COG hebben in 2020 deelgenomen aan een voorlichting betreffende de AVG en de aanpak van de AVG binnen de COG.

In 2022 worden alle medewerkers van de COG getraind op het gebied van informatiebeveiliging en privacy d.m.v. de e-learning modules van Privacy Bekwaam.

Voornemen is om tweemaal per jaar een awareness campagne te voeren naar aanleiding van actuele onderwerpen (bijvoorbeeld: phishing).

mbo digitaal

ROC A 12

IBP ROADMAP 2022-2024

- 01 Governance
- 04 Human Resource
- 11 Security management
- 14 Business Continuity Management
- 15 Supply Chain Management
- 10 Identity & Access management

mbo digitaal

ROC A 12

IBP ROADMAP 2022-2024

NBA domeinen	2021			2022												2023	2024
	Okt.	Nov.	Dec.	Jan.	Feb.	Mrt.	Apr.	Mei	Juni	Juli	Aug.	Sept	Okt.	Nov.	Dec.		
01 Governance *Extra: Decentrale IBP assessments*	Documenten afgerond	Decentrale IBP assessments		Architectuur						Internal Audit				Decentrale IBP assessments		External audit	External audit
04 Human Resources	Management Training				Training medewerkers m.b.v. e-learning tool (Privacy Bekwaam)				Beleid			Training nieuwe medewerkers en awareness campagne					
11 Security Management	Inventarisatie	Implementatie en testen															
14 Business Continuity Management	Beleid, implementatie en testen																
15 Supply Chain Management				Beleid, implementatie en testen													
10 Identity & Access Management				Beleid en implementatie													
Extra: Toegang tot ons netwerk door relaties											Beleid en implementatie						
02 Organisation							Eigenaarschap										
08 System Development 2												Beleid en implementatie					
09 Data Management 2												Beleid en implementatie					
05 Configuration Management 1													Beleid en implementatie				
06 Incident/Problem Management 1													Beleid en implementatie				
07 Change management 1													Beleid en implementatie				
12 Physical Security 1													Beleid en implementatie				
03 Risk management																DPIA's	
13 Computer Operations																Beleid	

mbo digitaal

Overstap naar NBA-model als toetsingskader

- Statements passen beter bij de onderwijspraktijk
- Beter geschikt als intern stuurinstrument
- Mogelijkheid om interne en externe auditors te betrekken
- We sluiten op deze manier weer aan bij het HO
  en trekken verder samen op met SURF

mbo digitaal

Enquête contactpersonen benchmark

In hoeverre gaat het NBA-volwassenheidsmodel jouw organisatie helpen om beter in control te komen op het gebied van informatiebeveiliging?

Helemaal niet	3
Enigszins	13
In sterke mate	21

mbo digitaal

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

mbo digitaal

Besluit overstap NBA-model, met randvoorwaarden

- Het opleidingstraject wordt in 2022 voortgezet. Naast de tweedaagse masterclasses wordt een eendaagse variant toegevoegd. Er worden in 2022 ook informatiesessies voor lijnmanagers aangeboden.
- We blijven ook in 2022 inzetten op het informeren van bestuurders bij deze ontwikkelingen, door hiervoor aandacht te vragen tijdens regiobijeenkomsten en algemene ledenvergaderingen.
- We informeren onze belangrijkste stakeholders over deze overstap en de te verwachten (aanvankelijke) daling van de gemiddelde volwassenheidsscore in vergelijking met het huidige toetsingskader.
- Het onderhoud van het toetsingskader en het bepalen van de baseline en het ambitieniveau doen we samen met het ho, binnen de Maturity werkgroep van SURF.
- Voor de laagst scorende statements uit het NBA-kader wordt onderzocht welke vormen van ondersteuning en kennisuitwisseling kunnen worden geboden; handreikingen, informatiebijeenkomsten, etc.
- In 2022 wordt het Framework IBP geactualiseerd en uitgebreid met handreikingen die zijn toegesneden op het werken met het NBA-model.
- We onderzoeken de mogelijkheden om externe auditors in te zetten, bijvoorbeeld bij de review van de assessments.
- Instellingen die het oude toetsingskader ter vergelijking willen blijven gebruiken worden hierbij gefaciliteerd. Het oude invulformat blijft beschikbaar.
- We blijven inzetten op samenwerking tussen instellingen, zodat kennis en ervaringen gedeeld kunnen worden. Vooral voor de kleinere instellingen is dit cruciaal.

mbo digitaal

Vragen en discussie