Peer review 2020

op basis van de Benchmark IBP in het mbo 2019

IBPDOC32a

REGIEGROEP IBP IN HET MBO

Kennisnet SURF saMBO-ICT

Verantwoording

Productie

Kennisnet / saMBO-ICT

Auteur

Martijn Bijleveld

Versie 1.0, mei 2020

Met dank aan

Aeres	MBO Utrecht
Alfa College	Onderwijsgroep Tilburg
Aventus	Rijn IJssel
Cibap	ROC De Leijgraaf
Citaverde College	ROC Kop van Noord Holland
Clusius College	ROC Midden Nederland
Curio	ROC Nijmegen
Da Vinci College	ROC van Amsterdam
Deltion College	ROC van Twente
Drenthe College	Scalda
Friesland College	SG De Rooi Pannen
Gilde Opleidingen	Sint Lucas
Graafschap College	Summa College
Grafisch Lyceum Utrecht	SVO
Hoornbeeck College	VISTA
Landstede	Zadkine
MBO Rijnland	Zone college

Sommige rechten voorbehouden

Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, aanvaarden de auteur(s), redacteur(s) en uitgever van Kennisnet geen aansprakelijkheid voor eventuele fouten of onvolkomenheden.

Creative commons

Naamsvermelding 3.0 Nederland
(CC BY 3.0)

De gebruiker mag:

- Het werk kopiëren, verspreiden en doorgeven
- Remixen – afgeleide werken maken

Onder de volgende voorwaarde:

- Naamsvermelding – De gebruiker dient bij het werk de naam van Kennisnet te vermelden (maar niet zodanig dat de indruk gewekt wordt dat zij daarmee instemt met uw werk of uw gebruik van het werk).

Inhoudsopgave

1. Inleiding

In 2019 is voor de 5e keer de Benchmark IBP/E uitgevoerd. Deze benchmark is een belangrijk instrument om te beoordelen hoe de mbo-sector ervoor staat op het gebied van informatiebeveiliging en privacy. Ook in 2019 hebben we als mbo-sector weer een stap vooruit gezet: alle onderdelen komen uit op een gemiddelde volwassenheid van 2,5. Een bescheiden stap voorwaarts, die duidelijk maakt dat we nog steeds in beweging zijn.

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

De resultaten van deze benchmark zijn binnen het Netwerk IBP in het mbo uitvoerig besproken. Zie hiervoor de rapportage van de benchmark 2019: www.sambo-ict.nl/ibpdoc11e.

2. Het belang van de peer review

We hebben geconstateerd dat de benchmark, als zelfassessment, een zekere mate van onnauwkeurigheid kent. Er zitten verschillen in de mate van aandacht waarmee het assessment wordt ingevuld. Ook kennis en ervaring van de invullers speelt een rol. Het wordt in deze fase belangrijk om ook over de representativiteit uitspraken te kunnen doen. Een belangrijk instrument daarbij is de peer review, waarbij instellingen elkaars assessment beoordelen. Een van de aanbevelingen vanuit de Benchmark IBP/E 2019 was om de peer review structureel in te zetten, als een logische vervolgstap op de benchmark.

3. Scenario's voor de peer review

De peer review is in 2018 voor het eerst ingezet met 10 mbo-instellingen en is in 2019 herhaald. Aan deze laatste editie hebben 11 instellingen deelgenomen. De deelname bleef beperkt omdat deze eerste twee edities van de peer review vrij tijdsintensief waren. Er werd veel aandacht besteed aan formele rapportages, waarin ook weer feedback vanuit de onderzochte instelling werdt meegenomen. De bevindingen werden vervolgens persoonlijk gepresenteerd. Voor het doel dat wij ermee voor ogen hebben is deze grondige aanpak wellicht wat zwaar aangezet. Daarom heeft de Regiegroep een voorstel gedaan voor een nieuwe aanpak van de peer review, die voor elke instelling haalbaar zou moeten zijn. De uitgangspunten daarvan zijn:

- De 10 te reviewen statements worden centraal vastgesteld en tijdig gecommuniceerd.
- Voor deze 10 statements wordt de bewijslast uitvoerig beschreven en toegelicht in een servicedocument.
- De review moet in een dagdeel worden afgerond, de documentatie en/of onderbouwing van de bewijslast moet door de ontvangende instelling daarom goed worden voorbereid en op dat tijdslot worden afgestemd.
- Rapportage van de bevindingen gebeurt via een standaard digitaal formulier, waarbij de toelichting tot het hoogstnoodzakelijke wordt beperkt, er is verder geen documentatie of nazorg vereist.
- De gegevens uit het formulier worden centraal verzameld, geanalyseerd en (geanonimiseerd) gerapporteerd.
- Er worden drie scenario's aangeboden:
    - peer-carrousel
    - peer review bijeenkomst
    - expert review / vaststelling

3.1 Peer-carrousel

De deelnemende instellingen worden door de organisatie in een carrousel ingedeeld, waarbij rekening wordt gehouden met de reisafstand. Instelling A bezoekt instelling B, B bezoekt C enzovoort. Binnen de vastgestelde periode maken de instellingen zelf de afspraken voor het peer review bezoek. De bewijslast wordt ter plekke beoordeeld, vastgesteld en eventueel voorzien van opmerkingen. Het reviewen kost een dagdeel; gereviewd worden kost eveneens een dagdeel.

3.2 Peer review bijeenkomst

De deelnemers aan deze centrale bijeenkomst komen in Utrecht bij elkaar. Er zijn twee ronden; in de ene ronde word je gereviewd, in de andere ronde voer je zelf de review uit. De indeling van de peers wordt bij de start van de dag door de organisatie bekend gemaakt. Er is gedurende de dag ondersteuning aanwezig mocht-ten er vragen zijn met betrekking tot de uitvoering van de review en de interpretatie van de bewijslast.

3.3 Expert review

Instellingen die geen tijd kunnen of willen vrijmaken om zelf als reviewer op te treden kunnen gebruikmaken van de expert review. Daarbij voert een externe expert de review op locatie uit. De kosten hiervan zijn voor rekening van de instelling.

Bij enkele mbo-instellingen was de benchmark al ingevuld door een externe expert. Deze assessments worden beoordeeld en vastgesteld door een externe auditor (expert vaststelling).

4. Selectie van statements

Voor de bovengenoemde drie scenario's werden twee sets van statements geselecteerd. Set A was bedoeld voor de peer review bijeenkomst, met statements waarvan de bewijslast op afstand beoordeeld kan worden, bijvoorbeeld aan de hand van documenten. Set B bevat ook statements die bijvoorbeeld door waarneming ter plaatse of een interview kunnen worden vastgesteld. Zie hieronder.

A: 10 statements voor de peer review bijeenkomst										
1.1	5.1.1	Beleidsregels voor informatiebeveiliging	P	3,1	0	8	34	14	0
1.7	8.2.1	Classificatie van informatie	P	2,5	6	24	18	8	0
1.16	15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	E	3,1	0	5	41	10	0
1.17	16.1.1	Verantwoordelijkheden en procedures.	E	3,0	0	13	32	11	0
2.2	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	P	2,2	5	35	15	1	0
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	P-E	2,0	10	35	11	0	0
5.2	9.1.2	Toegang tot netwerken en netwerkdiensten	P-E	2,5	9	16	27	4	0
5.9	9.4.2	Beveiligde inlogprocedures	P-E	2,5	7	21	23	4	1
5.18	9.4.3	Systeem voor wachtwoordbeheer		2,7	7	12	26	11	0
P.5		Bewaartermijnen		2,0	8	39	8	1	0

B: 10 statements voor de peer carrousel en de expert review									
1.1	5.1.1	Beleidsregels voor informatiebeveiliging	P	3,1	0	8	34	14	0
1.17	16.1.1	Verantwoordelijkheden en procedures.	E	3,0	0	13	32	11	0
2.2	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	P	2,2	5	35	15	1	0
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	P-E	2,0	10	35	11	0	0
3.5	11.1.3	Kantoren, ruimten en faciliteiten beveiligen	E	2,4	8	20	26	2	0
4.5	12.3.1	Back-up van informatie	P	3,2	1	8	30	15	2
4.8	12.6.1	Beheer van technische kwetsbaarheden		2,7	5	15	27	9	0
4.13	16.1.5	Respons op informatiebeveiligingsincidenten	E	3,1	3	5	33	14	1
5.18	9.4.3	Systeem voor wachtwoordbeheer		2,7	7	12	26	11	0
P.5		Bewaartermijnen		2,0	8	39	8	1	0

Twee sets van 10 statements, inclusief de gemiddelde score uit de Benchmark IBP/E 2019. De vijf rechter kolommen geven de spreiding van de scores aan, van links naar rechts niveau 1 t/m niveau 5.

De nieuwe aanpak van de peer review resulteerde in 41 aanmeldingen, 9 voor de peer carrousel, 13 voor de peer review dag en 19 aanmeldingen voor een expert review. De reviews zouden starten vanaf medio maart.

5. Online peer review

Door de coronasituatie moesten de plannen echter worden aangepast. De fysieke bezoeken konden niet doorgaan en er werd een nieuwe uitvraag gestart voor een online aanpak van de peer review. Daarbij werd gekozen voor de set statements die waren bedoeld voor de peer review dag, omdat deze immers geschikt zijn voor beoordelen op afstand.

Aan deze online peer review hebben 34 mbo-instellingen deelgenomen;

- Peer review: 16
- Expert review: 12
- Expert vaststelling: 6

De reviews vonden plaats tussen 6 april en 8 mei.

6. Resultaten peer review 2020

Het gemiddelde volwassenheidsniveau voor de benchmark IBP/E 2019 kwam uit op 2,5 voor de gehele mbo-sector. De deelnemers aan de peer review scoorden samen gemiddeld een 2,6 voor de benchmark. In dat opzicht is de groep deelnemers aan de peer review representatief voor de mbo-sector.
De gemiddelde score van de deelnemende instellingen op de onderzochte statements was een 2,7.

De reviewers beoordeelden voor elk van de 10 statements de bewijslast die door de onderzochte instelling was aangeleverd. Via het vooraf ingevulde formulier (zie bijlage) werd aangegeven of het opgegeven volwassenheidsniveau al dan niet kon worden vastgesteld. Daarbij kon eventueel worden aangegeven dat het statement

mogelijk te laag was beoordeeld (voor de vaststelling heeft dat verder geen gevolgen; het statement blijft daarmee gewoon vastgesteld). In de tabel hieronder zijn de resultaten weergegeven.

Nr.	ISO	Omschrijving	Gem. score	% vastgesteld	% mogelijk te laag
1.1	5.1.1	Beleidsregels voor informatiebeveiliging	3,3	91	16
1.7	8.2.1	Classificatie van informatie	2,7	97	16
1.16	15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	3,3	94	10
1.17	16.1.1	Verantwoordelijkheden en procedures	3,1	100	12
2.2	7.2.2	Bewustzijn, opleiding en training t.a.v. informatiebeveiliging	2,2	97	9
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	2,0	97	9
5.2	9.1.2	Toegang tot netwerken en netwerkdiensten	2,5	91	7
5.9	9.4.2	Beveiligde inlogprocedures	2,7	82	7
5.18	9.4.3	Systeem voor wachtwoordbeheer	2,9	91	6
P.5	privacy	Bewaartermijnen	2,0	97	12
		totaal	**2,7**	**94**	**10**

De uitkomst van de peer review is dat 94% van de onderzochte statements kon worden vastgesteld. Dat is een heel goed resultaat, waarmee kan worden onderbouwd dat de Benchmark 2019 correct en waarheidsgetrouw werd ingevuld en daarmee een bruikbaar instrument is om de volwassenheid op het gebied van IBP te meten. Bij 10% van de onderzochte statements gaf de reviewer aan dat op basis van de beoordeelde bewijslast het statement mogelijk hoger beoordeeld had kunnen worden.
Bij bovengenoemde uitkomsten zijn twee kanttekeningen te maken:

1. Bij de selectie van statements is rekening gehouden met de vorm van de bewijslast: vanwege de beoordeling op afstand ging het daarbij vaak om documenten. Een waarneming ter plaatse of een interview zou vermoedelijk iets vaker kunnen leiden tot interpretatieverschillen.
2. Vanwege de beperkingen qua bewijslast konden IB-clusters 2, 3 en 6 niet worden meegenomen, het toetsingskader is dus niet in de volle breedte onderzocht.

7. Conclusie

De vaststelling van 94% van de onderzochte statements laat zien dat de Benchmark IBP/E als instrument werkt. Daarbij waren de reacties vanuit de deelnemers zeer positief. Vooral de efficiënte aanpak, met een minimum aan overhead werd gewaardeerd. Het belang van de peer review wordt binnen het IBP netwerk breed onderschreven. Dat betekent dat we de peer review vanaf nu als vast onderdeel van de benchmarkcyclus gaan inpassen. De tijd tussen het invullen van de benchmark en de uitvoering van de peer review zal daarbij worden verkort. En hopelijk kunnen we bij de volgende editie weer fysiek bij elkaar komen, waardoor een grotere spreiding van statements over het toetsingskader mogelijk wordt, met rijkere vormen van bewijsvoering, zoals interviews en waarneming ter plaatse. Dat komt bovendien het leereffect ten goede, wat ook een belangrijk aspect is van dit proces.
Belangrijk aandachtspunt is dat de statements in het toetsingskader goed zijn beschreven: de bewijslast moet duidelijk richting geven, zonder daarbij te dwingend te zijn. Binnen het netwerk IBP is een werkgroep gestart met deze redactionele update van het toetsingskader, die voor de nieuwe editie van de benchmark gereed zal zijn.

8. Bijlagen

Peer review 2020

Selectie van statements ten behoeve van de online peer review

Naam instelling	
Naam medewerker	
E-mail	
Functie	
Datum audit	
Type audit	Online peer review
Naam auditor	
Instelling	
E-mail	
Functie	

Nr.	ISO	Omschrijving	Benchmark 2019	Bevinding peer review	Beoordeelde bewijslast	Eventuele toelichting beoordeling	Akkoord
1.1	5.1.1	Beleidsregels voor informatiebeveiliging	3	Vastgesteld	IBP beleid en verslag vergadering MT (incl. CvB)	IBP beleid is beschikbaar voor medewerkers	Ja
1.7	8.2.1	Classificatie van informatie	4	Vastgesteld	IBP beleid verwijst naar classificatie	Dataregisters medewerkers en studenten akkoord	Ja
1.16	15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	4	Vastgesteld	VWO van Eduarte, HR2day gecontroleerd	Ovezicht VWO's beschikbaar	Ja
1.17	16.1.1	Verantwoordelijkheden en procedures.	3	Vastgesteld, mogelijk te laag beoordeeld	IBP beleid, procedure datalekken, intranet verwijz.	Instelling voldoet aan de wettelijke AVG eisen	Ja
2.2	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	3	Vastgesteld	Collectief ontwikkelprogramma schooljaar 19-20	Presentielijsten gecontroleerd	Ja
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	2	Vastgesteld	Awarenessonderdelen zijn gecontroleerd	Clear Desk/Screen is opgenomen in Baseline IBP	Ja
5.2	9.1.2	Toegang tot netwerken en netwerkdiensten	3	Vastgesteld	IBP beleid, plus afgeleide provisioning		Ja
5.9	9.4.2	Beveiligde inlogprocedures	3	Niet vastgesteld	MFA is nog niet gestart.	IBP beleid verwijst wel naar MFA	Ja
5.18	9.4.3	Systeem voor wachtwoordbeheer	2	Vastgesteld	Wachtwoordbeheer is opgenomen in Baseline IBP	Beleid wordt daadwerkelijk uitgevoerd.	Ja
P.5	privacy	Bewaartermijnen	2	Vastgesteld	IBP beleid, 3 lines of defence, bewaartermijnen	DSP is leidend. Implementatie voorzichtig gestart	Ja

Voorbeeld van het invulformulier voor de peer review