Peer review 2021

op basis van de Benchmark IBP in het mbo 2020

IBPDOC32b

REGIEGROEP IBP IN HET MBO

Kennisnet SURF saMBO-ICT

Verantwoording

Productie

Kennisnet / saMBO-ICT

Auteur

Martijn Bijleveld

Versie 1.1, maart 2021

Met dank aan

Alfa College	Helicon Opleidingen	ROC Mondriaan
Aventus	Lentiz Onderwijsgroep	ROC Nijmegen
Cibap	MBO Utrecht	ROC Rivor
Citaverde College	mboRijnland	ROC van Amsterdam/Flevoland
Clusius College	Mediacollege Amsterdam	ROC van Twente
Curio	Noorderpoort	Scalda
Da Vinci College	Onderwijsgroep Noord	SG De Rooi Pannen
Deltion College	Rijn IJssel	Soma College
Drenthe College	ROC A12	Summa College
Friesland College	ROC De Leijgraaf	VISTA college
Gilde Opleidingen	ROC Horizon College	Wellantcollege
Graafschap College	ROC Kop van Noord-Holland	Zadkine
Grafisch Lyceum Utrecht	ROC Midden Nederland	Zone.college

Sommige rechten voorbehouden

Inhoudsopgave

1. Inleiding

In het najaar van 2020 is voor de 6e 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. Toen we 6 jaar geleden begonnen met deze benchmark hebben we het doel gesteld om als sector qua volwassenheid in 2020 gemiddeld minimaal op 3,0 uit te komen. Dat is niet helemaal gelukt; alle onderdelen komen in 2020 uit op een gemiddelde volwassenheid van 2,8. Evengoed is het weer een flinke stap voorwaarts ten opzichte van de 2,5 van 2019.

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

Zie verder de rapportage van de benchmark 2020: http://www.sambo-ict.nl/ibpdoc11f.

2. Het belang van de peer review

De bovengenoemde benchmark IBP-E is een zelfassessment en het is belangrijk om over de representativiteit uitspraken te kunnen doen. Ons instrument daarvoor is de peer review, waarbij instellingen elkaars assessment beoordelen, of het kunnen laten beoordelen door een externe auditor. Met ingang van 2020 zetten we de peer review structureel in, als een logische vervolgstap op de benchmark. In 2020 namen 33 van de 56 benchmarkdeelnemers deel, dit jaar 39 van de 57. Tot nu toe hebben 45 mbo-instellingen ten minste een keer deelgenomen aan de peer review en dat is een heel mooi resultaat. Onze ambitie is dat alle benchmarkdeelnemers meedoen met de peer review en vanuit de regiegroep hebben we een aantal scenario's ontwikkeld waarmee dat qua tijdsinvestering voor iedere instelling haalbaar zou moeten zijn.

3. Aanpak van de peer review

Het invullen van de Benchmark IBP-E is al een flinke klus voor de mbo-instellingen en de peer review komt daar nog eens achteraan. We hebben daarom binnen de regiegroep gezocht naar een balans tussen haalbaarheid en representativiteit. Uitkomst daarvan was een aanpak met 10 te reviewen statements, waarbij de administratieve last tot een absoluut minimum wordt beperkt. Daarbij kan de

mbo-instelling kiezen voor een scenario waarbij uitsluitend de eigen benchmark wordt gereviewd, in dat geval door een externe auditor.
De aanpak is als volgt:

- De 10 te reviewen statements worden centraal vastgesteld en snel na afronding van de Benchmark IBP-E gecommuniceerd.
- Voor deze 10 statements wordt de bewijslast uitvoerig beschreven en toegelicht in een servicedocument.
- De ontvangende instelling verzamelt de documentatie en/of onderbouwing van de bewijslast en stelt deze ter beschikking aan de reviewer.
- Tijdens een online meeting wordt de bewijslast besproken met de reviewer.
- 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.
- Het door de instelling gescoorde volwassenheidsniveau kan wel/niet worden vastgesteld, waarbij nog aangegeven kan worden dat het statement eventueel te laag beoordeeld is. In dat laatste geval is het oordeel nog steeds 'vastgesteld'.
- De gegevens uit het formulier worden centraal verzameld, geanalyseerd en (geanonimiseerd) gerapporteerd.
- Er worden drie scenario's aangeboden:
    - peer carrousel
    - expert review
    - expert vaststelling

3.1 Peer carrousel

De deelnemende instellingen worden door de organisatie in een carrousel ingedeeld; instelling A reviewt instelling B, B reviewt C enzovoort. Binnen de peer review periode maken de instellingen zelf de afspraken voor de (online) overlegmomenten. De bewijslast wordt op afstand besproken, beoordeeld en eventueel voorzien van opmerkingen.

Deelnemers peer carrousel (23)	
Alfa College	Rijn IJssel
Clusius College	ROC Horizon College
Curio	ROC Kop van Noord-Holland
Da Vinci College	ROC van Amsterdam/Flevoland
Drenthe College	ROC van Twente
Friesland College	Scalda
Gilde Opleidingen	Summa College
Graafschap College	VISTA college
Helicon Opleidingen	Wellantcollege
Lentiz Onderwijsgroep	Zadkine
Mediacollege Amsterdam	Zone.college
Onderwijsgroep Noord	

3.2 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 auditor de review uit. De kosten hiervan zijn voor rekening van de instelling.

Deelnemers expert review (9)
Deltion College
Grafisch Lyceum Utrecht
MBO Utrecht
Noorderpoort
ROC De Leijgraaf
ROC Midden Nederland
ROC Mondriaan
SG De Rooi Pannen
Soma College

3.3 Expert vaststelling

Bij een aantal mbo-instellingen is de benchmark ingevuld door een externe expert/auditor. Deze benchmarks worden via een steekproef van 4 statements vastgesteld door een externe auditor. Als de vier statements in orde zijn dan wordt het de peer review als geheel (10 statements) vastgesteld. Als een van de statements niet kan worden vastgesteld dan worden alle 10 statements onderzocht, zoals bij de normale expert-review.

Deelnemers expert vaststelling (7)
Aventus
Cibap
Citaverde College
mboRijnland
ROC A12
ROC Nijmegen
ROC Rivor

4. Selectie van statements

Bij de peer review worden 10 statements van de benchmark IBP onderzocht. Het merendeel van de statements is afkomstig uit het IB cluster, bij deze editie waren 2 statements afkomstig uit het pluscluster Privacy. De regiegroep selecteert deze statements, waarbij rekening wordt gehouden met een goede spreiding over de zes IB-clusters. Verder wordt ermee rekening gehouden dat de statements niet teveel op niveau 1 gescoord zijn (dan valt er immers niets te reviewen). Tot slot geldt in deze corona-tijd dat de bewijslast online gedeeld kan worden en daarmee op afstand beoordeeld kan worden.

Nr.	ISO 27002	Omschrijving
1.18	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen
2.8	6.2.2	Telewerken (thuiswerken)
3.2	8.3.2	Verwijderen van media
5.4	9.2.2	Gebruikers toegang verlenen
5.10	10.1.2	Sleutelbeheer
6.1	9.2.5	Beoordeling van toegangsrechten van gebruikers
6.9	18.2.2	Naleving van beveiligingsbeleid en –normen
6.13	16.1.6	Lering uit informatiebeveiligingsincidenten
P.13	privacy	Procedures rechten van de betrokkenen
P.18	privacy	Datalekken en beveiligingsincidenten

Het gemiddelde volwassenheidsniveau voor de benchmark IBP/E 2020 kwam uit op 2,8 voor de gehele mbo-sector. De gemiddelde score van de deelnemende instellingen op de bovenstaande onderzochte statements was 2,9.

5. Resultaten peer review 2021

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
1.18	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**

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

6. Conclusie

Aan de peer review 2021 hebben 39 van de 57 benchmarkdeelnemers meegedaan. Daarbij werd 95% van de onderzochte statements vastgesteld. Dat is een heel goed resultaat, waarmee kan worden onderbouwd dat de Benchmark IBP 2020 correct en waarheidsgetrouw werd ingevuld en daarmee een bruikbaar instrument is om de volwassenheid op het gebied van IBP te meten.

De reacties vanuit de deelnemers aan de peer review waren wederom positief. Vooral de efficiënte aanpak, met een minimum aan overhead wordt gewaardeerd. Maar ook de gesprekken tussen de instellingen worden vaak als heel waardevol ervaren, het gaat vaak over meer dan alleen sec de beoordeling van de statements.

Hopelijk kunnen we bij de volgende editie van de peer review weer fysiek afspreken, dan kan er nog meer van elkaar worden geleerd. Bovendien is dan de keuze aan statements groter, met rijkere vormen van bewijsvoering, zoals interviews en waarneming ter plaatse. En we gaan voor 100% deelname, want eigenlijk is elke instelling het aan zichzelf verplicht om het zelfassessment op deze manier objectief te laten bevestigen.

7. Bijlagen

Peer review 2021

Selectie van statements ten behoeve van de online peer review

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

Nr.	ISO	Omschrijving	Benchmark 2020	Bevinding peer review	Beoordeelde bewijslast	Eventuele toelichting beoordeling	Consensus
1.18	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	2	Vastgesteld	IBP Beleid 3.11 en 3.12	In het beleid staat het melden en registreren van incider	Ja
2.8	6.2.2	Telewerken (thuiswerken)	2	Vastgesteld, mogelijk te laag beoordeeld	Privacyveilig thuiswerken, Screenshots van publicatie	Informatie is breed gedeeld en op diverse momenten on	Ja
3.2	8.3.2	Verwijderen van media	2	Vastgesteld	Afdanken en hergebruiken digitale medis		Ja
5.4	9.2.2	Gebruikers toegang verlenen	2	Vastgesteld	Toegangsbeleid Digitaal V2.0		Ja
5.10	10.1.2	Sleutelbeheer	3	Niet vastgesteld	Leencontract	Er dient in bredere zin nog invulling gegeven te worden a	Ja
6.1	9.2.5	Beoordeling van toegangsrechten van gebruikers	1	Vastgesteld	Geen	Men is bezig met de opzet van de Soll-matrices	Ja
6.9	18.2.2	Naleving van beveiligingsbeleid en –normen	3	Vastgesteld, mogelijk te laag beoordeeld	IBP Benchmark, Verbeterplan en opvolging	Goed uitgewerkt verbeterplan en gedocumenteerde ma	Ja
6.13	16.1.6	Lering uit informatiebeveiligingsincidenten	3	Vastgesteld	Waarneming ter plaatse van incident + verbeteractie		Ja
P.13	privacy	Procedures rechten van de betrokkenen	2	Vastgesteld	Privacyverklaring_2021	Document was al actief in september 2020, derhalve kar	Ja
P.18	privacy	Datalekken en beveiligingsincidenten	2	Vastgesteld, mogelijk te laag beoordeeld	Procedure datalekken incidentenregister op sharepoint		Ja

Voorbeeld van het invulformulier voor de peer review