**Benchmark informatiebeveiliging, privacy en examinering in de mbo sector 2018**

 **IBPDOC11d**

**Verantwoording**

**Productie**

Kennisnet / saMBO-ICT

**Auteurs**

Leo Bakker (Kennisnet)

Ludo Cuijpers (Kennisnet, ROC Leeuwenborgh)

Versie 1.0, december 2018

**Met dank aan**

****

**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

[Verantwoording 2](#_Toc533079071)

[1. Conclusies IBP*E* benchmark 2018 4](#_Toc533079072)

[1.1 Inleiding 4](#_Toc533079073)

[1.2 Representativiteit 5](#_Toc533079074)

[1.3 Benchmark ibpe 2018 en algemene bevindingen ibp in het mbo 5](#_Toc533079075)

[1.4 Gedetailleerde bevindingen informatiebeveiliging 6](#_Toc533079076)

[1.5 Benchmark privacy 11](#_Toc533079077)

[1.6 Benchmark Examinering 12](#_Toc533079078)

[1.7 Samenvatting benchmark in de afgelopen jaren 13](#_Toc533079079)

[1.8 Aanbevelingen 13](#_Toc533079080)

[1.8.1 Bewaartermijnen 13](#_Toc533079081)

[1.8.2 Controle en logging 13](#_Toc533079082)

[1.8.3 Uitvoeren DPIA’s 13](#_Toc533079083)

[1.8.4 Aangeven ambitie niveau 13](#_Toc533079084)

[1.8.5 Governance 14](#_Toc533079085)

[1.8.6 Toetsingskader 4.0 14](#_Toc533079086)

[1.8.7 Peer review 14](#_Toc533079087)

[1.8.8 IBP Jaarplan 14](#_Toc533079088)

[1.8.9 Masterclasses 15](#_Toc533079089)

[1.8.10 Internal audit IBP 15](#_Toc533079090)

[2. Resultaten ibp benchmark 16](#_Toc533079091)

[2.1 Toelichting op de tabellen 16](#_Toc533079092)

[2.2 Wat gaat goed en wat gaat minder goed? 18](#_Toc533079093)

[2.3 Beleid en organisatie 19](#_Toc533079094)

[2.4 Personeel, studenten en gasten 20](#_Toc533079095)

[2.5 Ruimtes en apparatuur 21](#_Toc533079096)

[2.6 Continuïteit 22](#_Toc533079097)

[2.7 Vertrouwelijkheid en integriteit 23](#_Toc533079098)

[2.8 Controle en Logging 24](#_Toc533079099)

[Bijlage 1: Framework 2.0 informatiebeveiliging en privacy in het mbo 25](#_Toc533079100)

# Conclusies IBP*E* benchmark 2018

## Inleiding

In 2014 is een Taskforce Informatiebeveiliging en privacy van start gegaan met een duidelijke opdracht, zoals in het Verantwoordingsdocument IBPDOC1 van het Framework ibp in het mbo is beschreven. Er is in de afgelopen jaren heel veel tot stand gebracht met betrekking tot ibp in het mbo en de benchmarks hebben hierin een belangrijke rol gespeeld. Deze benchmarks hebben een tweeledig doel. Enerzijds geven ze een goed beeld van de stand van zaken in de mbo instellingen met betrekking tot ibp, belangrijk voor de sector zelf maar ook voor 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.

Intussen ligt dan alweer de vierde Benchmark ibp in het mbo voor u. Het afgelopen jaar is een belangrijk jaar in deze geweest omdat in mei 2018 de AVG is ingevoerd. Dat heeft alle mbo instellingen duidelijk tot extra activiteiten aangezet en dat blijkt ook uit de Benchmark 2018. Als sector hebben we daarmee naast de informatiebeveiliging nu ook de privacy in onze sector echt op de kaart gezet. Daarnaast is in 2018 ook nog eens het toetsingskader Examinering in de benchmark opgenomen waarmee ook de eerste stappen gezet zijn om digitaal examinering ook op een hoger beveiligingsniveau te brengen.

Op tactisch niveau is ook afgelopen jaar weer een groot aantal documenten in het framework kader opgeleverd, reden waarom dit Framework moest worden herzien en nu een versie 2.0 kent (zie bijlage 1). Ook is er afgelopen jaar weer volop geschoold in de masterclasses informatiebeveiliging en privacy waar een vijftigtal mbo instellingen aan hebben deelgenomen. Nieuw waren daarbij de trainingen voor de FG’s. Alle mbo instellingen hebben d.d. eind 2018 een FG aangesteld.

Bijzonder is wel het gegeven dat vrijwel alle instellingen in 2018 aan de Benchmark hebben deelgenomen, slechts een drietal instellingen is het niet gelukt dit te doen, maar 95% dus wel. Daarmee hebben we een heel goed beeld van de sector mbo weten te realiseren en hiermee kan de sector zeker als voorloper binnen het onderwijs beschouwd worden.

## Representativiteit

Aan de eerste IBP benchmark (2015) hebben 19 mbo instellingen deelgenomen. Bij de tweede benchmark (2016) waren dat al 30 mbo instellingen die deelnamen. In 2017 hebben 47 van de 61 mbo instellingen deelgenomen, dat is 77%. Dit jaar hebben we een deelnamepercentage van 95% (57 van de 60 mbo instellingen).

## Benchmark ibp*e* 2018 en algemene bevindingen ibp in het mbo

De benchmark is uitgevoerd op basis van het vastgestelde toetsingskaders informatiebeveiliging, privacy en examinering.

De toets informatiebeveiliging is uitgevoerd op de 6 clusters die afgeleid zijn van het ISO 27001/2 normenkader. De opzet van de benchmark is gelijk aan die van het Hoger Onderwijs. Alle maatregelen uit het toetsingskader zijn in een zestal clusters verdeeld om het geheel overzichtelijk te maken. Cluster 1 gaat vooral over beleidsmaatregelen, cluster 2 over personeel (bewustwording), cluster drie 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 (vertrouwelijkheid) en integriteit van de data en tot slot cluster 6 dat gaat over controle en monitoring.

Naast deze clusters is dit jaar voor de derde keer een check uitgevoerd op een pluscluster Privacy.

Voor de eerste keer is het cluster Examinering getoetst.

Een samenvatting van de resultaten, de gemiddelde scores van alle mbo instellingen van alle statements (onderzochte onderwerpen) per cluster:



Bron: Benchmark ibp in het mbo 2018, Kennisnet en saMBO-ICT (december 2018)

Als mbo sector hebben wij ons een gemiddelde score van 2 tot doel gesteld. Deze doelstelling is gehaald.

De “technische” clusters (ruimten en apparatuur, continuïteit, vertrouwelijkheid en integriteit) scoren een ruime 2. Dat mocht ook verwacht worden gezien het feit dat de instellingen in het mbo de technische zaken wel op orde hebben. Waar het vaak nog aan ontbreekt is de documentatie hiervan maar de maatregelen zijn over het algemeen wel getroffen. Dat is een pluspunt in de benchmark. Wel is het cluster “Controle en logging” nog steeds onder de maat. Dit heeft ook de afgelopen periode nog steeds geen prioriteit gehad, daar moet in de komende jaren in het kader van ‘in control zijn’ en ook op het gebied van incident management nog veel aan gebeuren.

De AOC’s en vakscholen wijken niet af van deze uitslag. Op sommige onderdelen is de score 0,1 hoger of lager. Gezien de kleine omvang kan dit veroorzaakt worden door “toevallige” deelscores van instellingen.

## Gedetailleerde bevindingen informatiebeveiliging



Momenteel zijn er in Nederland 60 mbo instellingen. AOC Oost en Groene Welle zijn dit jaar gefuseerd met als nieuwe naam Zone.college.

Om inzicht te krijgen in de stand van zaken op het gebied van informatiebeveiliging binnen de mbo sector zijn deze 60 instellingen verdeeld in 4 kwartielen van ieder 15 instellingen.

De eerste groep zijn de 15 hoogst scorende instellingen in het toetsingskader Informatiebeveiliging.

De tweede groep de mbo instellingen met de ranking 16 tot en met 30.

De derde groep de mbo instellingen met de ranking 31 tot en met 45.

De vierde groep de mbo instellingen met de ranking 46 tot en met 57 en de drie mbo instellingen die niet deelgenomen hebben. Er is geen score aan 3 instellingen toegekend, te weten Wellantcollege, ROC van Twente en STC-group. Alle 3 de instellingen hebben aangegeven volgend jaar mee te zullen doen. ROC van Twente heeft in het verleden één keer meegedaan, voor de STC-group en het Wellantcollege zal dat dan de eerste keer zijn.

Bovenstaand zijn de 9 statements toegevoegd die voor elke mbo instellingen op orde zouden moeten zijn. Een volwassenheidsniveau 3 is voor deze statements wenselijk.









## Benchmark privacy

Dit jaar is er naast informatiebeveiliging, voor de derde keer getoetst op privacy. De benchmark is uitgevoerd op basis van het vastgestelde toetsingskader privacy[[1]](#footnote-1).

De gemiddelde score van de benchmark privacy bedraagt 2,3. Dit is een verbetering van 0,4 t.o.v. het vorige jaar.

* Op 1 mbo instelling na hebben nu alle deelnemers een informatiebeveiliging en privacy beleid dat goedgekeurd is.
* Alle mbo instellingen hebben inmiddels een FG’er.
* De implementatie van bewaartermijnen is slecht.
* De uitvoer van DPIA’s is onder de maat.

Al met al een lichte vooruitgang, maar zeker geen reden om tevreden achterover te leunen.



## Benchmark Examinering

Voor de eerste maal is er ook een benchmark examinering uitgevoerd. 43 instellingen hebben gegevens aangeleverd. Er is veel kritiek geweest op de bewijsvoering. Reden voor saMBO-ICT om dit toetsingskader in 2019 te herzien. De resultaten zijn toch opgenomen in dit document, met de kanttekening dat deze resultaten gezien moeten worden als een opmaat voor het volgend jaar.



## Samenvatting benchmark in de afgelopen jaren



## Aanbevelingen

De onderstaande aanbevelingen zijn aangegeven door de 57 instellingen die deelgenomen hebben aan de benchmark. De aanbevelingen zijn alleen geordend, maar tekstueel niet aangepast.

### Bewaartermijnen

* Praktische handreiking/stappenplan voor implementatie van bewaartermijnen. In hoeverre kan MBO-breed het gesprek met hoofdleveranciers MBO (bijv. van Eduarte) aangegaan worden voor ondersteuning hiervan door de systemen?
* Bewaartermijnen: hoe pak je dit verantwoord aan gezien de hoeveelheid applicaties waar je mee te maken hebt. Je wil niet gegevens verwijderen die niet meer terug te draaien zijn.

### Controle en logging

* Praktische handreiking hoe om te gaan met controle/logging. XX heeft op dit moment de persoonsgegevens geclassificeerd a.d.h.v. BIV classificatie in de verwerkersregisters. Hoe nu de volgende stap te maken naar beveiligingsniveaus?
* De aandachtspunten t.a.v. “controle en logging” en “incidentmanagement” staan nadrukkelijk genoemd in de tekst en horen in de aanbevelingen terug te komen. Dat geldt ook voor de DPIA’s en de bewaartermijnen.
* Gezamenlijk kijken of er een mogelijkheid is het logging deel op een hoger niveau te krijgen (ik ben al meerdere keren met leveranciers in overleg geweest maar of de oplossing voldoet niet of is niet te betalen).

### Uitvoeren DPIA’s

* Handreiking wanneer DPIA’s uit te voeren binnen MBO? Op welke applicaties/processen standaard, wanneer bij wijzigingen?
* Wat ik in onze organisatie merk, maar ook van andere organisaties hoor is, dat privacy by design, het direct betrekken van de IBP-deskundigen bij de voorbereiding van projecten nauwelijks gebeurd. Pas op een heel laat moment worden we betrokken, met alle risico’s en frustraties die hierbij horen. Als dit beter zou verlopen, zouden enkel andere zwakke punten uit de benchmark waarschijnlijk ook direct geadresseerd zijn.
* PIA best practices: hoe pak je dit aan.

### Aangeven ambitie niveau

* Het zou helpen als de sector/saMBO-ICT het ambitieniveau per deelgebied (informatiebeveiliging, privacy, examinering) aan gaat geven. Dit scheelt veel interne discussie bij het krijgen van projectbudget per instelling. Bij mijn projectaanvraag miste ik een duidelijke uitspraak vanuit de sector. Daarom heb ik gekozen om op benchmarkniveau 2019 te komen (wat moeilijk mikken is).

### Governance

* Duidelijkheid omtrent proces- en systeem eigenaren en wat hun taken en verantwoordelijkheden zijn op het gebied van IBP-beleid.
* Draag zorg voor een duidelijke IBP-organisatiestructuur, inclusief de bijbehorende taken. Alle actoren dienen hun eigen rol te kennen en daar naar te handelen. Denk daarbij ook aan de rol van een proces- of applicatie-eigenaar. Deze groep is zich vaak niet bewust van zijn of haar rol en bijbehorende eigenaarschap als het gaat over informatiebeveiliging of privacy.
* De “mens” blijft een zwakke schakel. Een permanente bewustwordingscampagne helpt het risico verminderen.

### Toetsingskader 4.0

* Classificeren, labelen incl. bewaartermijnen van gegevens.
* Duidelijkheid omtrent verwerker zijn en uitwisseling van gegevens met andere partijen. Zie hiervoor scholen die samenwerken, CJB, Intergrip, onderzoeken, centraal aanmelden etc.
* Awareness, Awareness, Awareness. Zorgen dat IBP een gewoon onderdeel wordt van de bedrijfs- en onderwijsvoering.
* Aanpassen beschrijving volwassenheidsniveaus aan “leg uit of pas toe”.
* Zoals aangegeven zouden we een doorzoekbare kennisbank/FAQ met praktische voorbeelden, gerangschikt op categorie erg fijn vinden.
* Voor de interviews voor het invullen van de benchmark, heb ik het toetsingskader in stukken uiteen gesplitst, zodat ik (zonder de totale tekst als ballast) de juiste personen de juiste vragen kon stellen. Dat waren niet altijd de proceseigenaren. Er zou m.i. iets voor te zeggen zijn om het hele toetsingskader in één vragenlijst te stoppen die al een ordening kent naar proceseigenaren. Door de nummering kan bij de resultaten weer de volledige aansluiting worden gevonden met de eerdere benchmarks. Hiermee wordt het ook meer een lijnverantwoordelijkheid dan een IBP-feestje.
* Als ik kijk waar ik de meeste vragen over krijg, is het de uitwisseling van gegevens met externen. Dat is inmiddels niet meer vanzelfsprekend, maar levert veel vragen en onzekerheid op. Ik zou er voor zijn gemeenschappelijk een IBPDOC op te stellen met aanwijzingen/aanbevelingen over het delen van informatie. Het doorstroomdossier (al dan niet digitaal) is een van de heikele punten.
* De huidige ambitie was volwassenheidsniveau voor de sector op niveau 2. Wat is onze ambitie voor de sector? Wat zou de ambitie moeten zijn per instelling. Volstaat op sommige gebieden een “niveau 1”- niveau? Herformuleren ambitie.
* Updaten toetsingskaders aan huidige standaarden.
* De aanbevelingen van 2017 bevatten o.a. "aanpassen van de toetsingskaders", wellicht dat dit nog opgepakt kan worden? Soms mogen zaken echt wel verdwijnen; iets minder op detailniveau.

### Peer review

* Uitvoer geven aan peer-review door minimaal 20 collega instellingen onderling.
* Gaan we deze systematiek ook gebruiken voor de interne controle verantwoording?
* Voor de peer review trainingen aansluiten op Norea, Isaca en de methodiek van de VNG (Ensia).
* Als aanbeveling wil ik meegeven dat de MBO's er naar streven een 100% deelname aan de peer-review. Er kan dan via site van saMBO een "regionale intekenlijst" komt, waarmee instituten elkaar kunnen vinden zonder dat er grote afstanden gereisd hoeven te worden.
* Om de inzet van peer review te stimuleren (is namelijk naar onze ervaring super zinvol !), koppels maken van ROC's die elkaar reviewen m.b.v. vaste agenda en zoals nu een deel vaste statements en een deel keuze statements.

### IBP Jaarplan

* Is er iemand vanuit het netwerk met een best practise van een IBP jaarplan, die we als format kunnen gebruiken?
* Een belangrijke aanbeveling lijkt mij om te komen tot een samenwerking met de studentenadministratiesystemen. Waar wij als MBO instellingen verder komen in een hoger niveau op IBP lijkt de systemen soms wat achter te blijven op het gebied van AVG. Wij hebben ze juist heel hard nodig als we de boel op orde willen krijgen.

### Masterclasses

* In de aanbevelingen van vorig jaar staat een mogelijke training voor proceseigenaren. Een van de rode draden van dit hele jaar is dat het aanwijzen van proceseigenaren bij veel instellingen problematisch is. Misschien moeten we daar een aanbeveling voor formuleren.
* Praktische masterclass/bijeenkomst hoe om te gaan met: foto’s, uitwisseling externe partijen, niet meewerkende leveranciers.
* Masterclass uitvoeren peer review (gesprekstechnieken, rapportage).
* Masterclass privacy (stond ook al voor 2018).
* Veel aanbevelingen lijken mij nog steeds van toepassing en doorlopend, bijvoorbeeld de trainingen en masterclasses en het aanpassen van de toetsingskaders aan nieuwe ontwikkelingen. Wellicht is het interessant om ook de jurisprudentie op de AVG in de gaten te houden en te kunnen implementeren in bijeenkomsten.
* Betere toelichting/toetsingskader voor Examinering.

###  Internal audit IBP

* Het is wenselijk om met een aanpak te komen om binnen een mbo instelling een internal audit IBP te kunnen uitvoeren.

# Resultaten ibp benchmark

## Toelichting op de tabellen

Alle tabellen zijn op dezelfde manier opgebouwd. Een korte toelichting:



Kolom 1, Nr. Geeft het nummer van het statement weer. Deze nummering is gelijk aan de nummering van het Hoger Onderwijs / MBO normenkader. Het eerste cijfer staat voor het cluster, het tweede cijfer voor het statement nummer.

Kolom 2. ISO27002 Geeft het nummer van de norm uit ISO27002. Een zestal normen zijn gesplitst in 12 statements. Dus 79 normen uit het ISO normenkader zijn gekoppeld aan 85 statements uit het HO/MBO normenkader.





Niveau 1, 2, 3, 4 en 5 verwijzen naar de volwassenheidsniveaus (maturity levels).

Het Normenkader informatiebeveiliging mbo wordt gebruikt om de volwassenheid van informatiebeveiliging te meten bij de mbo instellingen. Hiervoor wordt een 5-punts schaal gehanteerd gebaseerd op het Capability Maturity Model (CMM). Het CMM model is gebaseerd op procesvolwassenheid, de 5 niveaus zijn in de onderstaande tabel weergegeven.

|  |  |
| --- | --- |
| **CMM niveau** | **Omschrijving**  |
| niveau**1** | Initieel, ad hoc: De processen zijn ad hoc georganiseerd, erg afhankelijk van individuele personen**Ad hoc** |
| niveau**2** | Herhaalbaar, maar intuïtief: Er wordt op een vaste manier gewerkt**Beleid is gemaakt en goedgekeurd en bij een kleine groep bekend (opzet en bestaan).**  |
| niveau**3** | Gedefinieerd proces: De processen zijn gedocumenteerd en bekend bij betrokkenen**Beleid is bij alle betrokken medewerkers, studenten en externen bekend (werking).** |
| niveau**4** | Beheerd en meetbaar: De processen worden beheerd, zitten in een verbetercyclus en zijn meetbaar (PDCA).**IBP is onderdeel geworden van de PDCA cyclus.** |
| Niveau**5** | Geoptimaliseerd: Er wordt als vanzelfsprekend verbeterd en volgens best practices gewerkt. **IBP is toekomstbestendig, effectief en efficiënt.** |

Bij ieder volwassenheidsniveau is de score weergegeven van de deelnemende mbo instellingen aan de benchmark.

“Niveau 2” is rood omkaderd als een mogelijke baseline voor de sector.

De modale klasse (klasse met de hoogste frequentie dichtheid) is weergegeven in geel. Indien 2 klassen dezelfde dichtheid hebben is de hoogste klasse geel gearceerd.

Het gemiddelde cijfer (2018) is het rekenkundige gemiddelde van de individuele waarnemingen.

## Wat gaat goed en wat gaat minder goed?

**Best scorende statements uit alle clusters.**



In tegenstelling tot vorig jaar is cluster 1 (beleid) goed vertegenwoordigd. Cluster 2 (personeel) en 6 (monitoring) ontbreken.

**Slechts scorende statements uit alle clusters.**



Cluster 3 kent geen statement dat zeer slecht scoort. Cluster 6, beleid, komt viermaal voor.

**2.2 (Bewustzijn, etc.) scoort te slecht**. Trainingen en campagnes moeten nu opgepakt zijn.

## Beleid en organisatie



## Personeel, studenten en gasten



## Ruimtes en apparatuur



## Continuïteit



## Vertrouwelijkheid en integriteit



## Controle en Logging



Bijlage 1: Framework 2.0 informatiebeveiliging en privacy in het mbo



1. IBPDOC7: Toetsingskader privacy: cluster 7 [↑](#footnote-ref-1)