****

**Benchmark informatiebeveiliging, privacy en examinering in de mbo sector 2019**

 **IBPDOC11e**

**Verantwoording**

**Productie**

Kennisnet / saMBO-ICT

**Auteur**

Martijn Bijleveld

Versie 1.1, december 2019

**Met dank aan**

**Afbeelding met tekst

Automatisch gegenereerde beschrijving**

**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**

[](http://www.google.nl/url?sa=i&source=images&cd=&cad=rja&uact=8&ved=0CAgQjRw&url=http://creativecommons.org/about/downloads&ei=ViUYVb6yHcbWPPKhgMAM&psig=AFQjCNFD0SQUbum02GpIZCKN9_e8blqrwQ&ust=1427732182559562)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](#_Toc27421373)

[1. De Benchmark IBP/E in het mbo 4](#_Toc27421374)

[1.1 Inleiding 4](#_Toc27421375)

[1.2 Eindresultaat Benchmark IBP/E mbo 2019 4](#_Toc27421376)

[1.3 Representativiteit 5](#_Toc27421377)

[1.4 Ontwikkeling resultaten van de Benchmark IBP/E 5](#_Toc27421378)

[2. Achtergronden toetsingskaders 6](#_Toc27421379)

[2.1 Verklaring tabellen 6](#_Toc27421380)

[2.2 Informatiebeveiliging, Privacy en Examinering 7](#_Toc27421381)

[2.3 Volwassenheidsniveaus: het CMM-model 7](#_Toc27421382)

[2.4 Bewijslast 8](#_Toc27421383)

[3. Resultaten Benchmark IBP/E mbo 2019 9](#_Toc27421384)

[3.1 Resultaten Informatiebeveiliging (cluster 1-6) 9](#_Toc27421385)

[3.2 Resultaten Privacy (Pluscluster 7) 11](#_Toc27421386)

[3.3 Resultaten Examinering (Pluscluster 8) 12](#_Toc27421387)

[4. Nadere analyse Informatiebeveiliging 15](#_Toc27421388)

[4.1 De invloed van de nieuwe statements 15](#_Toc27421389)

[4.2 Ranking in vier groepen van 15 instellingen 16](#_Toc27421390)

[4.3 De hoogst en laagst scorende statements 18](#_Toc27421391)

[5. Conclusies en aanbevelingen 19](#_Toc27421392)

[Bijlage 1: Scores Informatiebeveiliging 22](#_Toc27421393)

[Beleid en organisatie 22](#_Toc27421394)

[Personeel, studenten en gasten 22](#_Toc27421395)

[Ruimtes en apparatuur 23](#_Toc27421396)

[Continuïteit 23](#_Toc27421397)

[Vertrouwelijkheid en integriteit 24](#_Toc27421398)

[Controle en logging 24](#_Toc27421399)

[Bijlage 2: ranking IB in 4 groepen 25](#_Toc27421400)

[Bijlage 3: Respons vragenlijst 29](#_Toc27421401)

[Inhoudelijke verbeterpunten van de toetsingskaders 29](#_Toc27421402)

[Procesmatige verbeterpunten rondom de benchmark 30](#_Toc27421403)

[Verbetering van de resultaten van de Benchmark IBP/E 30](#_Toc27421404)

[Uitvoering van de peer review 31](#_Toc27421405)

[Bijlage 4: Framework ibp in het mbo 32](#_Toc27421406)

# De Benchmark IBP/E in het mbo

## Inleiding

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

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

De benchmark is dit jaar voor de vijfde keer afgenomen, een lustrumjaar en alleen al daarom reden voor een feestje. We kijken terug op een succesvolle periode waarin veel werk is verzet en er veel is bereikt. Het toetsingskader IB heeft inmiddels alweer een update ondergaan en is uitgebreid met 31 nieuwe statements, waardoor nu de gehele ISO 27001 norm wordt afgedekt. Tegelijkertijd is het privacykader op de schop genomen en is daarmee weer helemaal in lijn met de AVG. En tot slot is het toetsingskader examinering vrijwel helemaal herschreven en opnieuw ingedeeld. Het sluit daarmee beter aan op de examineringsprocessen zoals beschreven in de procesarchitectuur examinering.

Dit lustrumjaar is ook bijzonder omdat we hebben bereikt dat alle 59 mbo-instellingen tenminste een keer hebben meegedaan aan de benchmark. Het aantal deelnemers was dit jaar opnieuw erg hoog: 56 van de 59 instellingen hebben deelgenomen aan de onderdelen Informatiebeveiliging en Privacy en 50 instellingen hebben het examineringskader ingevuld. Net als vorig jaar zitten we daarmee op een totale deelname van 95%.

## Eindresultaat Benchmark IBP/E mbo 2019

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. Dat is een belangrijk vaststelling, omdat we als sector een ambitieniveau van 3 hebben afgesproken. Onze doelstelling is om dat ambitieniveau van 3 in 2020 te behalen en de komende tijd zal nog veel discussie volgen over hoe we dat kunnen realiseren.

Afbeelding met schermafbeelding

Automatisch gegenereerde beschrijving

## Representativiteit

Aan de eerste benchmark in 2015 namen 19 mbo instellingen deel, oftewel 29% van de instellingen, bij de tweede benchmark in 2016 groeide dat percentage naar 46%; in 2017 gingen we naar 77% en in 2018 deed een recordaantal van 95% van de mbo-instellingen mee. Dit jaar hebben we ingezet op een deelname van 100%, maar door omstandigheden waren drie instellingen niet in staat om de benchmark in te vullen. Evengoed deden 56 van de 59 instellingen mee; opnieuw een zeer goede score van 95%. We hebben dit jaar ook de mijlpaal bereikt dat alle instellingen tenminste een keer hebben deelgenomen.

Nu alle instellingen ‘aan boord’ zijn is de vervolgvraag in hoeverre de scores van de zelfassessments representatief zijn. Er zitten verschillen in de mate van aandacht waarmee het assessment wordt ingevuld. Zo zijn er instellingen die fors inzetten op het normenkader en daar tientallen mensdagen in investeren terwijl er ook instellingen deelnemen waarbij het assessment bij wijze van spreken vanachter het bureau in een dag moet worden afgerond. Het wordt in deze fase belangrijk om ook over deze meer kwalitatieve representativiteit uitspraken te kunnen doen. Een belangrijk instrument daarbij is de peer review, waarbij instellingen elkaars assessment beoordelen. Bij de aanbevelingen aan het einde van dit document meer daarover.

## Ontwikkeling resultaten van de Benchmark IBP/E

De benchmark is uitgevoerd op basis van de vernieuwde toetsingskaders Informatiebeveiliging, Privacy en Examinering. Het toetsingskader Informatiebeveiliging is dit jaar uitgebreid met 31 nieuwe statements en het dekt daarmee de ISO 27001 norm volledig af. Dit toetsingskader is onderverdeeld in zes clusters. Cluster 1 gaat vooral over beleidsmaatregelen, cluster 2 over personeel (bewustwording), cluster 3 over ruimten en apparatuur (veel ICT gerelateerde zaken), cluster 4 betreft vooral de continuïteit van de bedrijfsvoering (vooral ten aanzien van de ICT infrastructuur), cluster 5 gaat over toegang tot data (vertrouwelijkheid) en de integriteit ervan en cluster 6 tot slot gaat over controle en monitoring.

Dit jaar is voor de vierde keer het pluscluster Privacy gescoord. Dit cluster bevat aanvullende statements met betrekking tot onder andere de rechtmatigheid van de gegevensverwerking in het kader van de AVG en de hantering van bewaartermijnen. Het onderdeel examinering is vorig jaar voor het eerst afgenomen en het betreffende toetsingskader is daarna weer grondig aangepast. Daarom is het voor examinering niet goed mogelijk om een vergelijking met vorig jaar te maken.

Hieronder een samenvatting van de resultaten:

Afbeelding met schermafbeelding

Automatisch gegenereerde beschrijving

**Bron: Benchmark IBP/E mbo 2019, Kennisnet en saMBO-ICT (december 2019)**

We zien over de gehele linie een groei. Vooral examinering maakt een sprong vooruit, maar zoals al eerder opgemerkt zijn die twee edities voor examinering niet goed met elkaar te vergelijken. Op alle toetsingskaders wordt dit jaar gemiddeld een 2,5 gescoord.

# Achtergronden toetsingskaders

## Verklaring tabellen

Afbeelding met schermafbeelding

Automatisch gegenereerde beschrijving

Een toelichting op de kolommen, van links naar rechts:

* Kolom Nr.: het nummer van het statement, dit is opgebouwd uit het clusternummer en een volgnummer. Als de kleur donkerpaars is, dan is dit statement -ten opzichte van de vorige versie van het toetsingskader- samengevoegd met een ander statement. In vorige versies waren enkele ISO-statements namelijk uitgesplitst, dat is in de nieuwe versie ongedaan gemaakt. De vervallen statements zijn licht gearceerd.  
  Volgnummers in een oranje vakje (zie afbeelding onder) duiden op een nieuw statement dat deze editie voor het eerst wordt beoordeeld.
* Kolom ISO 27002: het nummer van het statement volgens de ISO-norm, in verband met eenvoudige referentie naar de ISO norm.
* Kolom Statement: de korte omschrijving van het statement, volgens de ISO-norm.
* Kolom P/E: deze kolom bevat een P en/of een E wanneer het statement is opgenomen in het gemeenschappelijke normenkader privacy en/of examinering.
* Kolom met scores: bovenin het gemiddelde van alle scores op de statements en daarmee de gemiddelde score voor het gehele onderdeel (in dit voorbeeld Informatiebeveiliging). In de rijen daaronder de gemiddelden per statement.
* Kolommen Niveau 1 t/m Niveau 5: de verdeling van de aantallen voor elk van de 5 niveaus. De meest gekozen waarde (modus) is lichtpaars gearceerd.
* Voor elk van de clusters wordt het gemiddelde berekend in de donkerpaarse rij (zie afbeelding hieronder) en deze worden (gewogen) gemiddeld tot het eindresultaat, bovenaan in die kolom.

Afbeelding met schermafbeelding

Automatisch gegenereerde beschrijving

## Informatiebeveiliging, Privacy en Examinering

Deze Benchmark heeft betrekking op de onderdelen Informatiebeveiliging, Privacy en Examinering en hoewel we ze als afzonderlijke onderdelen invullen en beoordelen, kunnen ze niet los van elkaar gezien worden. Zo moet voor een goede bescherming van de privacy de informatiebeveiliging op orde zijn. Ook voor de examinering geldt een dergelijke afhankelijkheid. In principe geldt dat voor alle statements uit het IB-kader, maar daarbinnen zijn wel specifieke aandachtpunten te benoemen. Zo zijn er 34 statements uit het toetsingskader informatiebeveiliging benoemd die extra aandacht behoeven voor een goede bescherming van de privacy en 20 statements die cruciaal zijn voor een goede beveiliging van het examineringsproces. Deze statements uit het IB-kader zijn herkenbaar aan respectievelijk de letter P en/of de letter E in de betreffende kolom, zie hieronder.

Afbeelding met schermafbeelding

Automatisch gegenereerde beschrijving

## Volwassenheidsniveaus: het CMM-model

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

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

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



## Bewijslast

De oude toetsingskaders leunden zwaar op het kunnen tonen van documenten als bewijslast. Het produceren van de gevraagde documenten werd in sommige gevallen bijna een doel op zich. Bij de update van de toetsingskaders in 2019 zijn nieuwe vormen van bewijslast toegevoegd. Als bewijslast kan worden gebruikgemaakt van:

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

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

# Resultaten Benchmark IBP/E mbo 2019

Binnen de mbo-sector hebben we aangegeven dat niveau 2 de baseline is (minimum niveau voor alle statements) en dat volwassenheidsniveau 3 het ambitieniveau is dat in 2020 bereikt zou moeten worden. Voor sommige statements, bijvoorbeeld in het kader van examinering zou al eerder een hoger niveau (3 of zelfs 4) gewenst zijn. De 10 best scorende instellingen hebben dit jaar het gemiddelde ambitieniveau van 3 behaald.

Er is in de voorgaande periode door veel instellingen ingezet op het ontwikkelen, laten vaststellen en het communiceren van beleid. Niet alleen omdat dit vaak als ‘laaghangend fruit’ wordt bestempeld, maar ook omdat dit de fundering is voor veel van de maatregelen die in het kader van de overige clusters gerealiseerd moeten worden. Cluster 1; “Beleid en organisatie”, doet het daarom gemiddeld genomen goed. Ook de meer technische, beheersmatige clusters zoals “Ruimten en apparatuur” en “Continuïteit” (waaronder bijvoorbeeld het maken van back-ups) scoren relatief goed; de meeste instellingen hebben die technische zaken wel op orde.

Het cluster “Controle en logging” blijft door de jaren heen een punt van zorg en we zien ook nu nog geen significante ontwikkeling voorwaarts. Het beeld is dat er wel van alles wordt gelogd, maar dat we die informatie niet gebruiken om veiligheidsrisico’s vroegtijdig op te sporen en te beperken.

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

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

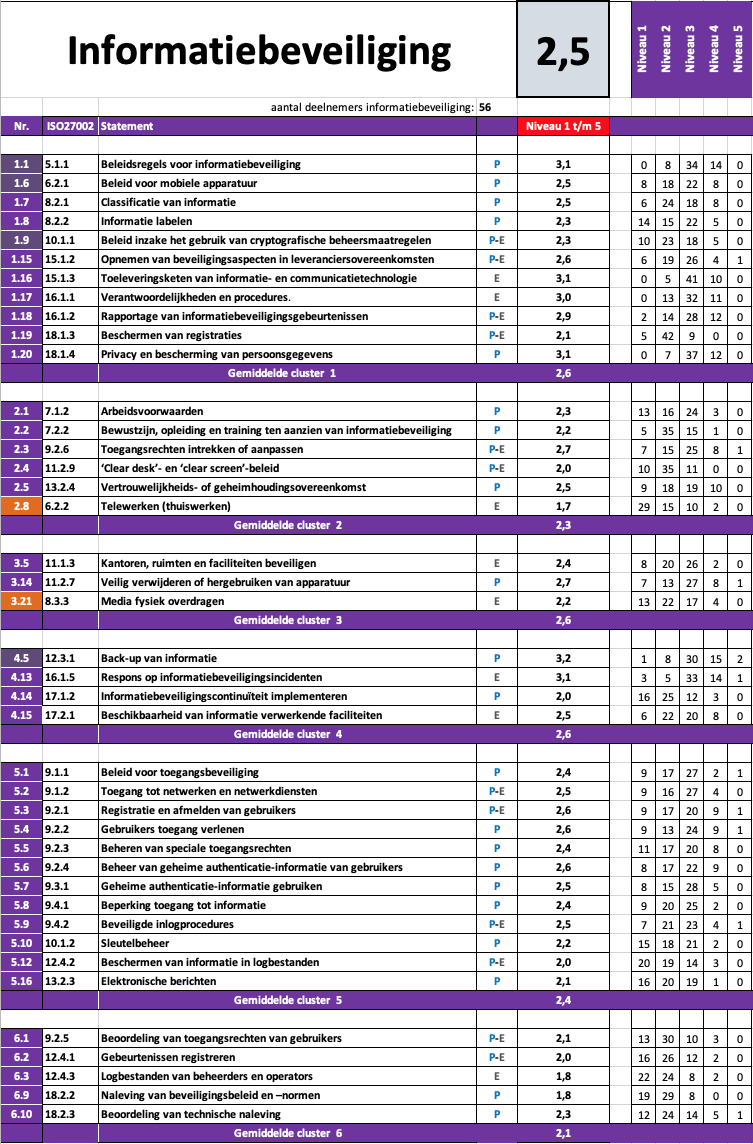
## Resultaten Informatiebeveiliging (cluster 1-6)

Zoals gezegd laten we in dit overzicht over Informatiebeveiliging niet alle 108 statements zien. In plaats daarvan is er een keuze gemaakt voor die statements die voorkomen in het Gemeenschappelijk normenkader Privacy en -Examinering. Dat zijn dus de IB-statements die vanuit privacy- en/of examineringsoogpunt extra aandacht behoeven en waarvan we binnen de sector de baseline op 3 hebben bepaald. De volledige set met statements en scores mb.t. Informatiebeveiliging is opgenomen in bijlage 1.

In de kolommen met de 5 niveaus staat steeds het aantal instellingen met het betreffende volwassenheidsniveau. Voor de “beleidsregels voor informatiebeveiliging” bijvoorbeeld hebben 8 instellingen zich ingeschaald op niveau 3, 34 instellingen zitten op niveau 3 en 14 instellingen op niveau 4. (Voor een toelichting op deze volwassenheidsniveaus, zie bijlage 3).

De onderstaande tabel laat zien dat de clusters “1. Beleid en organisatie” en de meer technisch georiënteerde clusters “3. Ruimten en apparatuur” en “4. Continuïteit” voorop lopen met ieder een gemiddelde volwassenheidsscore van 2,6. Cluster 2; “Personeel, studenten en gasten” blijft daarbij wat achter. Vooral het “clear desk en clear screen-beleid” verdient aandacht en het is duidelijk dat we nog moeten wennen aan het nieuwe statement 2.8 met betrekking tot “telewerken”. Cluster 6 met betrekking tot “Controle en logging” verdient in zijn geheel meer aandacht de komende periode.

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



## Resultaten Privacy (Pluscluster 7)

Er is sinds de eerste versie van het toetsingskader privacy (in 2017) veel ervaring opgedaan met dit toetsingskader. Na de inwerkingtreding van de AVG moest het daaraan worden aangepast, waarbij meteen een aantal andere wijzigingen konden worden doorgevoerd. Uitgangspunt was echter dat er zoveel mogelijk wordt aangesloten bij het bestaande toetsingskader en de gehanteerde systematiek, waarbij wijzigingen alleen worden doorgevoerd indien deze noodzakelijk zijn. Dat heeft geleid tot dit nieuwe toetsingskader Privacy versie 3.0 (zie ibpdoc7).

De gemiddelde score komt uit op 2,5 en dat is een verbetering van 0,2 ten opzichte van vorig jaar.

Afbeelding met schermafbeelding

Automatisch gegenereerde beschrijving

Een belangrijk statement als P.5, met betrekking tot de bewaartermijnen blijft hier bij achter. Veel instellingen hebben op dit gebied, ook met terugwerkende kracht, nog veel werk te verzetten. Complicerend daarbij is dat de administratieve softwarepakketten dit aspect vaak nog niet ‘by design’ ondersteunen, hoewel daar inmiddels wel beweging in zit.

Verder blijft het uitvoeren van DPIA’s (P.21) een struikelblok. De mbo-instellingen hebben behoefte aan een modelaanpak en saMBO-ICT en Kennisnet zetten gezamenlijk stappen in die richting.

Voor wat betreft gegevensverwerkingen ten behoeve van onderzoek (P.6) is op veel instellingen nog niets geregeld. Toch wordt (onderzoeks)data steeds belangrijker in het mbo; denk aan de diverse practoraten die worden opgericht. Daarbij wordt het thema data-ondersteund onderwijs steeds belangrijker en ook vanuit die ontwikkeling neemt de behoefte aan onderzoeksdata toe.

**Gemeenschappelijk normenkader IB - Privacy**

Afbeelding met teken

Automatisch gegenereerde beschrijvingOm een goede bescherming van de privacy te kunnen waarborgen moet -bij wijze van randvoorwaarde- de informatiebeveiliging op orde zijn. In principe geldt dat voor alle statements, maar daarbinnen zijn wel specifieke aandachtpunten te benoemen. Zo zijn er 34 statements uit het toetsingskader informatiebeveiliging geselecteerd die extra aandacht behoeven voor een goede bescherming van de privacy. De baseline van deze statement hebben we vastgesteld op 3.

Het onderstaande overzicht toont de volwassenheidsscores voor deze 34 gemeenschappelijke statements. Het gemiddelde komt uit op 2,4 en is daarmee lager dan de baseline van 3 en zelfs lager dan de gemiddelde score voor het gehele IB-kader. Van de 59 instellingen hebben 11 het vereiste niveau van 3 of hoger behaald. Al met al een uitkomst die het komende jaar extra aandacht vraagt.

Afbeelding met schermafbeelding

Automatisch gegenereerde beschrijving

## Resultaten Examinering (Pluscluster 8)

In 2018 is voor het eerst ook examinering meegenomen in de benchmark. Er is bij die editie veel kritiek geweest op de omschrijving van de statements en de bewijsvoering. Reden voor Regiegroep om dit toetsingskader in 2019 in samenwerking met het Servicepunt Examinering van de MBO Raad, aangevuld een groep van materiedeskundigen vanuit de instellingen, grondig te herzien. Dat heeft geleid tot een volledig herzien toetsingskader examinering (IBPDOC8). De volgorde, nummering, en inhoud van de statements zijn daarbij gewijzigd waardoor er geen goede vergelijking gemaakt kan worden met de resultaten van 2018. Het gemiddelde van dit cluster komt uit op een 2,5, wat gezien mag worden als een goede start.

Afbeelding met schermafbeelding

Automatisch gegenereerde beschrijving

Bij het beoordelen van dit kader kwam bij veel instellingen het beeld naar boven dat er al lang gewerkt wordt volgens de beschreven normen. We hebben het hier dan ook over processen die ook vanuit andere wet- en regelgeving solide georganiseerd moeten zijn. Veel beleid is vastgelegd in het examenreglement en veel procedures zijn helder beschreven in het handboek examinering. Toch ontbreken er, vooral waar het gaat over de digitale examinering, nog procedures en richtlijnen. De minst scorende statements hebben dan ook te maken met het continuïteitsplan (E.4), de ict-faciliteiten (E.12) en het digitale examenmateriaal (E.13).

**Gemeenschappelijk normenkader IB – Examinering**

Afbeelding met schermafbeelding

Automatisch gegenereerde beschrijvingOm de vertrouwelijkheid en integriteit van de examinering te waarborgen moet de informatiebeveiliging goed op orde zijn. In principe moeten alle statements uit het toetsingskader IB op orde zijn, maar daarbinnen zijn 20 statements benoemd die extra aandacht behoeven voor een goede bescherming van het examineringsproces. De baseline voor deze statements hebben we vastgesteld op 3.

Het onderstaande overzicht toont de volwassenheidsscores voor deze 20 gemeenschappelijke statements. Het gemiddelde komt uit op 2,4 en is daarmee lager dan de baseline van 3 en zelfs lager dan de gemiddelde score voor het gehele IB-kader. Van de 59 instellingen hebben 9 het vereiste niveau van 3 of hoger behaald. Dat betekent dat fors moet worden ingezet op verbetering van de processen die ten grondslag liggen aan deze statements.

Afbeelding met schermafbeelding

Automatisch gegenereerde beschrijving

Opvallend laag wordt gescoord op statement 2.8; Telewerken. Dit statement heeft betrekking op het thuiswerken, in opdracht (of met instemming) van de organisatie. Dit zou van toepassing kunnen zijn op de constructie van examens of de correctie van het gemaakte examenwerk. Andere kwetsbaarheden zitten ‘m -niet geheel onverwacht- in cluster 6 met betrekking tot controle en logging. Tot slot nog een aandachtspunt met betrekking tot het clear desk en clear screen beleid: dit statement wordt zowel vanuit examinerings- als privacy-oogpunt als extra kritisch bestempeld en we scoren er als sector slechts een 2,0. Van de 59 instellingen hebben er 45 dit niet- of niet goed geregeld. Opnieuw een belangrijk aandachtspunt voor het komende IBP-jaar.

# Nadere analyse Informatiebeveiliging

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

* De invloed van de 31 nieuwe statements die in 2019 zijn toegevoegd
* De ranking van de resultaten in vier groepen van 15 instellingen
* De hoogst- en de laagst scorende statements

## De invloed van de nieuwe statements

In 2019 zijn 31 statements aan het toetsingskader Informatiebeveiliging toegevoegd. Een voor de hand liggende vraag is dan: in hoeverre hebben die nieuwe statements de resultaten van de benchmark beïnvloed? Daarvoor hebben we de gemiddelde score berekend van de benchmark IB met en zonder de nieuwe statements. Dat blijkt voor het gemiddelde niet significant uit te maken.

Als we ons beperken tot de gemiddelde score van uitsluitend de nieuwe statements dan valt deze wel iets lager uit, maar nogmaals: dit heeft dus geen significante uitwerking op het gemiddelde overall, dat blijft 2,5.

Afbeelding met schermafbeelding

Automatisch gegenereerde beschrijving

## Ranking in vier groepen van 15 instellingen

We hebben in deze rapportage de instellingen gerangschikt naar hun gemiddelde totaalscore op het IB-kader en deze -evenals vorige edities- onderverdeeld in vier groepen. De eerste groep bestaat uit de 15 hoogst scorende instellingen voor wat betreft het toetsingskader Informatiebeveiliging. De tweede groep bevat 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 en de vierde groep de mbo instellingen met de ranking 46 tot en met 56. In deze laatste groep zijn de drie instellingen die niet hebben deelgenomen dus buiten beschouwing gelaten.

We hebben binnen deze groepen ook steeds het gemiddelde bepaald van die statements uit het gemeenschappelijk normenkader Privacy en -Examinering. Dat zijn dus de IB-statements die vanuit privacy- en/of examineringsoogpunt extra aandacht behoeven en waarvan we binnen de sector de baseline op 3 hebben bepaald.

**Ranking 1-15**

Binnen deze groep van 15 toppers voldoen er 11 aan de gemiddelde baseline van 3,0 die we ons voor 2020 ten doel hebben gesteld en dat is een compliment waard. Toch is ook binnen deze groep verbetering nodig op het gebied van controle en logging; het eindresultaat van je beveiliging wordt immers bepaald door de zwakste schakel.

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

**Ranking 16-30**

Deze groep van 15 instellingen scoort gemiddeld tussen 2,8 en 2,4 en is daarmee goed op koers naar ons ambitieniveau van 3.

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

**Ranking 31-45**

Het gemiddelde beweegt zich hier tussen 2,4 en 2,0. Nog net buiten de gevarenzone, maar in het licht van de ambitie voor 2020 is volwassenheidsniveau 3 nog erg ver weg.

|  |  |
| --- | --- |
| Cluster 1: Beleid en organisatie | 2,2 |
| Cluster 2: Personeel, studenten en gasten | 2,0 |
| Cluster 3: Ruimtes en apparatuur | 2,3 |
| Cluster 4: Continuïteit | 2,3 |
| Cluster 5: Vertrouwelijkheid en integriteit | 2,2 |
| Cluster 6: Controle en Logging | 1,9 |
| Informatiebeveiliging totaal | **2,2** |
|  |  |
| Gemeenschappelijk normenkader Privacy | **2,2** |
| Gemeenschappelijk normenkader Examinering | **2,1** |

**Ranking 46-56**

Deze 11 instellingen bevinden zich in de gevarenzone omdat ze niet voldoen aan de huidige baseline van 2, die toch gezien moet worden als een absoluut minimum. Het is in het belang van deze instellingen, maar ook de sector als geheel, om samen met de invullers te onderzoeken tegen welke achtergrond deze scores tot stand zijn gekomen en zo nodig -en indien gewenst- ondersteuning aan te bieden vanuit Kennisnet en/of saMBO-ICT. Het negeren van deze situatie kan gevolgen hebben voor het mandaat dat wij als sector hebben gekregen om onze verantwoording via zelfassessments te regelen.

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

## De hoogst en laagst scorende statements

Verder is er binnen het toetsingskader Informatiebeveiliging een top 15 samengesteld van hoogst en laagst scorende statements.

**De 15 hoogst scorende statements uit het IB-kader**

Afbeelding met schermafbeelding

Automatisch gegenereerde beschrijving

Wat hier opvalt is dat er geen statement uit cluster 2 (Personeel, studenten en gasten) of 6 (Controle en logging) in voorkomt. Vooral die laatste is natuurlijk een bevestiging van wat we al weten: er is werk te doen in cluster 6.

**De 15 laagst scorende statements uit het IB-kader**

Afbeelding met schermafbeelding

Automatisch gegenereerde beschrijving

Hier zien we het omgekeerde van wat we in de eerste tabel hebben vastgesteld: cluster 6 (Controle en logging) is hier oververtegenwoordigd. Opnieuw een illustratie van de noodzaak tot actie op dit gebied.

# Conclusies en aanbevelingen

Er zijn in deze rapportage een aantal zaken naar voren gekomen die wij als sector zouden moeten oppakken. Hieronder een samenvatting van de belangrijkste bevindingen, suggesties en aanbevelingen. Daarin is de feedback meegenomen die bij de invullers van de benchmark is opgehaald in de vorm van een korte vragenlijst (zie bijlage 3).

Het toetsingskader Informatiebeveiliging

Het nieuwe toetsingskader Informatiebeveiliging is in veel opzichten een verbetering ten opzichte van de oude versies, maar er zijn ook knelpunten gesignaleerd.

De beschrijving van de bewijslast op niveau 2 en 3 was bedoeld om de instellingen te helpen bij de concretisering van soms abstracte beheersingsdoelstellingen, maar deze zijn soms te letterlijk en onnodig strak geïnterpreteerd. De nuance: *pas toe of leg uit* is niet goed overgekomen. Dat heeft de score op een aantal statements beïnvloed.

Er is dus meer duiding en instructie nodig en het belang hiervan moet onder de aandacht van de instellingen worden gebracht (aan de instructiebijeenkomsten die voorafgaand aan deze editie van de benchmark werden georganiseerd hebben 10 van de 59 instellingen deelgenomen).

Mogelijk zijn er ook andere vormen van instructie mogelijk, meer just-in-time, bijvoorbeeld door video- of geluidsfragmenten met toelichtingen aan de statements te koppelen.

Daarbij kunnen misverstanden en misinterpretaties worden voorkomen door een aantal redactionele aanpassingen, vooral met betrekking tot de hierboven genoemde beschrijving van de bewijslast.

Door het toevoegen van nieuwe statements is getracht om de ISO-norm volledig af te dekken. Enkele nieuwe statements lijken echter niet van toepassing op de meeste onderwijsinstellingen, bijvoorbeeld met betrekking tot softwareontwikkeling. Hoewel je hier kunt redeneren dat de betreffende instellingen deze risico’s hebben uitbesteed door een goede SLA, NDA en/of verwerkersovereenkomst, komt dit op velen gekunsteld over.

In verband met bovenstaande zou je ook nog kunnen overwegen om een aantal statements optioneel te maken, eventueel afhankelijk van de specifieke situatie van de instelling.

Naar aanleiding van bovenstaande bevindingen is een werkgroep m.b.t. de doorontwikkeling van de toetsingskaders opgericht die aan de slag gaat met bovengenoemde zaken.

Betrouwbaarheid van de benchmark

Door interpretatieverschillen zoals hierboven beschreven ontstaat een onnauwkeurigheid in de beoordeling, die nooit helemaal weggenomen kan worden, maar waar wel verbetering mogelijk is.

Verder kan de beoordeling van de benchmark bewust en onbewust beïnvloed worden door de situatie. Als er in de voorgaande periode veel is geïnvesteerd in ibp-maatregelen kan er een druk worden gevoeld om dat ook in de uitkomsten van de benchmark terug te laten komen. Omgekeerd komt het voor dat de benchmark bewust wat lager wordt ingevuld als signaal naar het management van de betreffende instelling.

Tot slot verschillen instellingen in de mate van aandacht waarmee het assessment wordt ingevuld en er zijn verschillen in kennis en ervaring van de functionarissen die belast zijn met het uitvoeren van het assessment.

De peer review

Hierboven zijn een aantal oorzaken geschetst die kunnen leiden tot onderlinge interpretatieverschillen en afwijkingen. De peer review is een instrument om daar zicht op te krijgen en daarin een verbeterslag te kunnen maken.

De peer review is in 2018 voor het eerst ingezet en is dit jaar herhaald. Er hebben 11 instellingen deelgenomen aan deze editie. Elk van de instellingen heeft daarbij 10 statements uit de benchmark 2018 geselecteerd, die door de peer-auditors zijn onderzocht. De uitkomst was dat de scores op gemiddeld 4 van de 10 statements niet konden worden vastgesteld. Dat is een grote afwijking en daarvoor zijn in de evaluatie twee oorzaken genoemd. In de eerste plaats hebben de instelling zelf een selectie van 10 statements gemaakt en in veel gevallen is daarbij gekozen voor statements waarbij twijfel bestond over de juistheid van de score. Een andere belangrijke oorzaak is de eerder genoemde onduidelijkheid over de interpretatie van de bewijslast. Bij de peer review komt dat versterkt naar voren omdat de auditors de instructie hebben ontvangen om zo feitelijk als mogelijk te beoordelen. Daarmee krijgt de in het toetsingskader beschreven bewijslast nog meer gewicht en het is de vraag of de peer review op deze manier meet wat wij willen weten.

Een ander punt van zorg is dat de peer review erg tijdsintensief is. Er wordt veel aandacht besteed aan formaliteiten; zo worden er uitvoerige rapportages opgeleverd, waarin ook weer feedback vanuit de onderzocht instelling wordt meegenomen. De bevindingen worden vervolgens persoonlijk gepresenteerd. De peer review in zijn huidige opzet is een mooie manier om zorgvuldig en objectief te leren beoordelen en te ervaren wat het werk van een auditor inhoudt. Voor het doel dat wij ermee voor ogen hebben is dat wellicht wat zwaar aangezet en mogelijk hebben wij meer aan een aanpak zonder al te veel ‘overhead’. Tijdens de Netwerkbijeenkomst IBP van 12 december 2019 is de aanpak van de peer review besproken en is een werkwijze voorgesteld die nader zal worden uitgewerkt. Uitgangspunten:

* De peer review is een onlosmakelijk onderdeel van de benchmark en zou snel na uitvoering van het assessment breed moeten worden uitgevoerd.
* Uitgangspunt is dus dat alle deelnemers aan de benchmark deelnemen aan de peer review.
* De tijdsinvestering voor de instellingen wordt beperkt tot het hoogstnoodzakelijke.
* De 10 te reviewen statements worden centraal, door een werkgroep vastgesteld.
* De bewijslast (documenten, interviews, waarnemingen ter plaatse) worden door de ontvangende instelling goed voorbereid.
* De peer auditors reviewen de statements in maximaal een dag en noteren de bevindingen in een standaard formulier.
* Op deze manier wordt de tijdsinvestering beperkt tot 2-3 dagen per instelling (1 dag voorbereiden, 1 dag bezoeken, een dag bezocht worden)
* Dat is nog steeds een forse tijdsinvestering, maar in verhouding tot de vorige variant een grote verbetering.
* De tijdsinvestering kan verder worden beperkt door de werkbezoeken/interviews achterwege te laten en sec het bewijsmateriaal te beoordelen op bijvoorbeeld een centraal georganiseerde peer review bijeenkomst. De werkbezoeken voegen echter dusdanig veel toe dat daar voorlopig niet voor wordt gekozen.

Doel is dus om met deze light variant van de peer review een voor alle instellingen haalbaar scenario te bieden, zodat de peer review een vast onderdeel kan worden van de benchmark. De Regiegroep communiceert dit voorstel begin 2020 naar de instellingen.

Overige ondersteuning

Er blijft behoefte aan standaard (beleids)documenten, handreikingen enzovoort. Het is dus belangrijk om het Framework te blijven vernieuwen. Daarnaast kan ook worden gedacht aan een platform waar instellingen onderling hun documenten met elkaar kunnen delen.

Er zijn op dit moment 11 instellingen die volgens de benchmark zoals die nu is ingevuld, niet voldoen aan de baseline van 2, die gezien moet worden als een minimum. In overleg met deze instellingen zouden wij vanuit saMBO-ICT/Kennisnet kunnen onderzoeken tegen welke achtergrond deze scores tot stand zijn gekomen. Als daar behoefte aan is kan er mogelijk ondersteuning op maat worden geboden.

Er zijn een aantal statements die sector-breed structureel achterblijven en waaruit je zou kunnen opmaken dat daar meer ondersteuning nodig is. Het gaat dan bijvoorbeeld over het uitvoeren van DPIA’s, over een aantal statements met betrekking tot het personeel en vooral de statements uit cluster 6 met betrekking tot controle en logging. De Regiegroep heeft al zaken in gang gezet op het gebied van een model-aanpak voor DPIA’s en zou ook op deze andere punten moeten onderzoeken welke concrete ondersteuning kan worden ingezet.

Tenslotte

We kijken bij deze lustrum-editie van de benchmark terug op een periode waarin er veel is bereikt. Alle mbo-instellingen zijn inmiddels aangehaakt bij de benchmark en een gemiddelde volwassenheid van 2,5 op de clusters informatiebeveiliging, privacy en examinering is een mooie prestatie. Tegelijkertijd hebben we als sector voor 2020 een ambitieniveau van 3,0 afgesproken en die doelstelling gaan we hoogstwaarschijnlijk niet halen.

Het is belangrijk om dat ambitieniveau van 3 te laten herbevestigen door onze bestuurders. Dat zou dan moeten resulteren in een breed gedragen opdracht om focus en versnelling op ibp te krijgen. Daarmee kan de *Regiegroep ibp in het mbo*, samen met de mbo-instellingen aan de slag, bijvoorbeeld door het in gang zetten van (scholings)activiteiten op het gebied van controle en logging (cluster 6), een gezamenlijke DPIA-aanpak of het laten auditen van onze examenleveranciers. Dat kan overigens niet allemaal uit de bestaande middelen die saMBO-ICT en Kennisnet hiervoor beschikbaar hebben, dus het betekent ook een discussie over (prioritering van) middelen.

Waar mogelijk zou ook de samenwerking met de andere onderwijssectoren gezocht moeten worden. De samenwerking met het HO wordt steeds hechter, vooral door de samenwerking met SURF, maar ook het PO/VO biedt aanknopingspunten. Zo is de coöperatie SIVON met veel ambitie van start gegaan, met mogelijk veel raakvlakken op het gebied van informatiebeveiliging en privacy.

De resultaten van deze benchmark hebben wij besproken op 12 december 2019, tijdens de *Netwerkbijeenkomst ibp in het mbo*. Er hadden zich voor deze bijeenkomst 60 ibp-ers aangemeld en er kwamen er 70 naar Utrecht. Met wat extra stoelen en improviseren paste het allemaal net. Dit is een illustratie van de enorme betrokkenheid van de mbo-instellingen en het is voor ons als Regiegroep een bevestiging van het belang om dit netwerk te blijven ondersteunen. We zijn trots op dit netwerk, dankbaar voor het vertrouwen en gemotiveerd om samen met de instellingen de volgende stap voorwaarts te zetten.

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

Bart Bosma (SURF)

Bram Bogers (Onderwijsgroep Tilburg)

Co Klerkx (ROC van Amsterdam / Flevoland)

Fung Yee Poon (Aventus)

Henk Links (COG)

Leo Bakker (Kennisnet)

Martijn Bijleveld (saMBO-ICT)

Martijn van Hoorn (Citaverde)

Peter Vermeijs (MBO Raad)

Richard de Koning (Zadkine)

Samantha Rodolf-Lejeune (VISTA college)

Willem Flink (Hoornbeeck)

# Bijlage 1: Scores Informatiebeveiliging

## Beleid en organisatie



## Personeel, studenten en gasten

Afbeelding met schermafbeelding

Automatisch gegenereerde beschrijving

## Ruimtes en apparatuur

Afbeelding met schermafbeelding

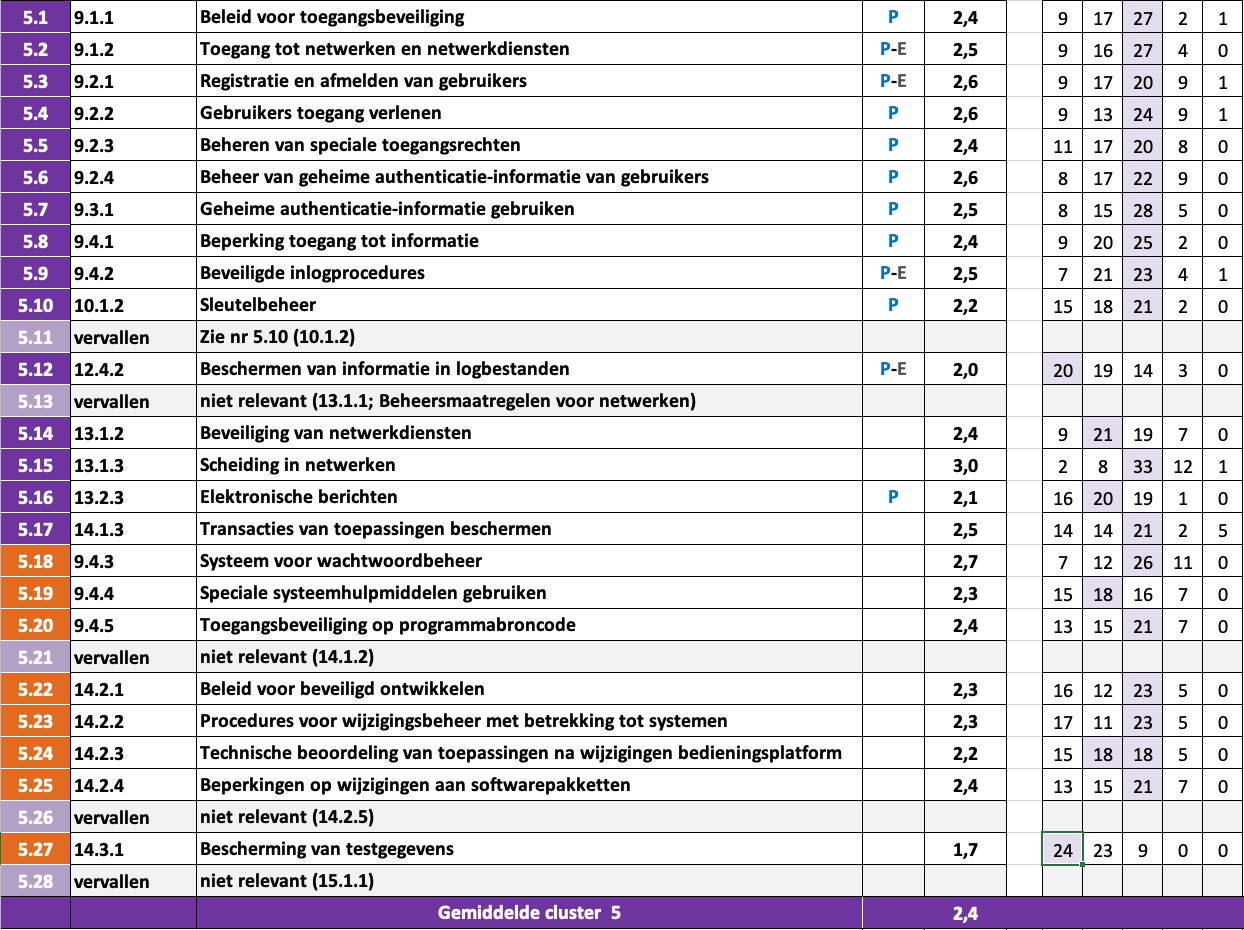
Automatisch gegenereerde beschrijving

## Continuïteit

Afbeelding met schermafbeelding

Automatisch gegenereerde beschrijving

## Vertrouwelijkheid en integriteit

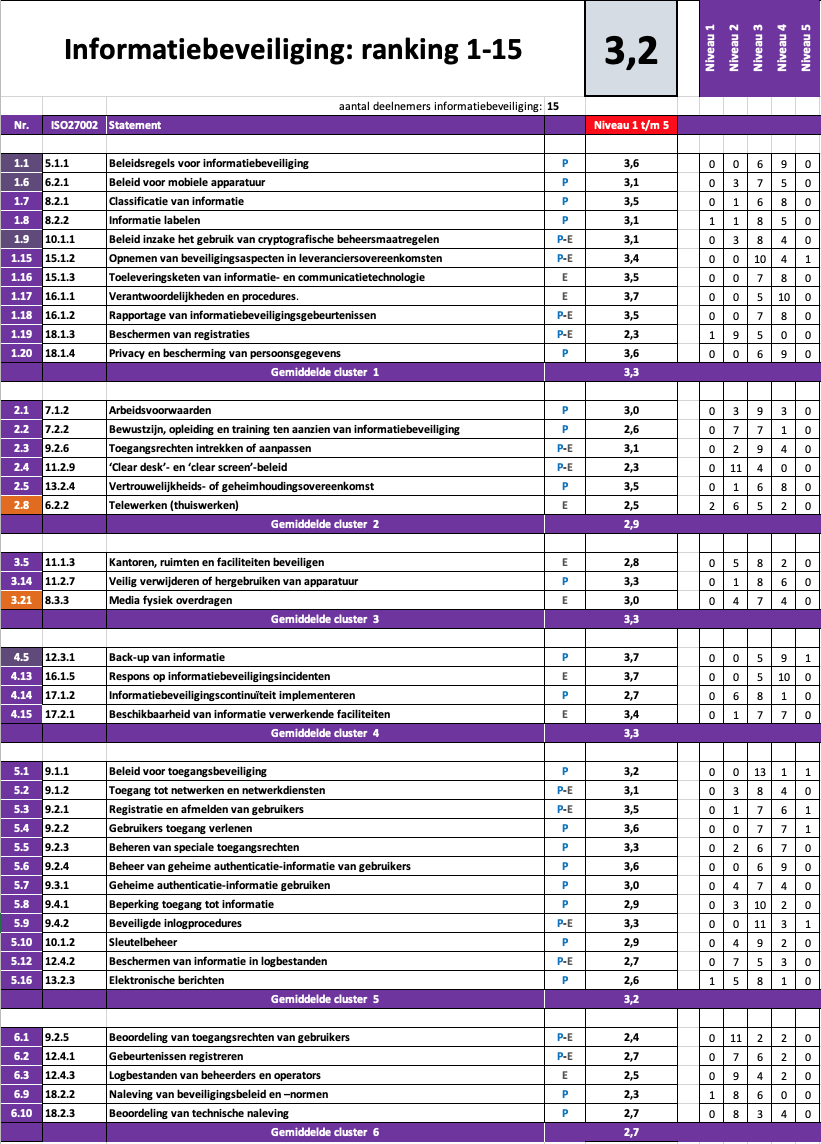


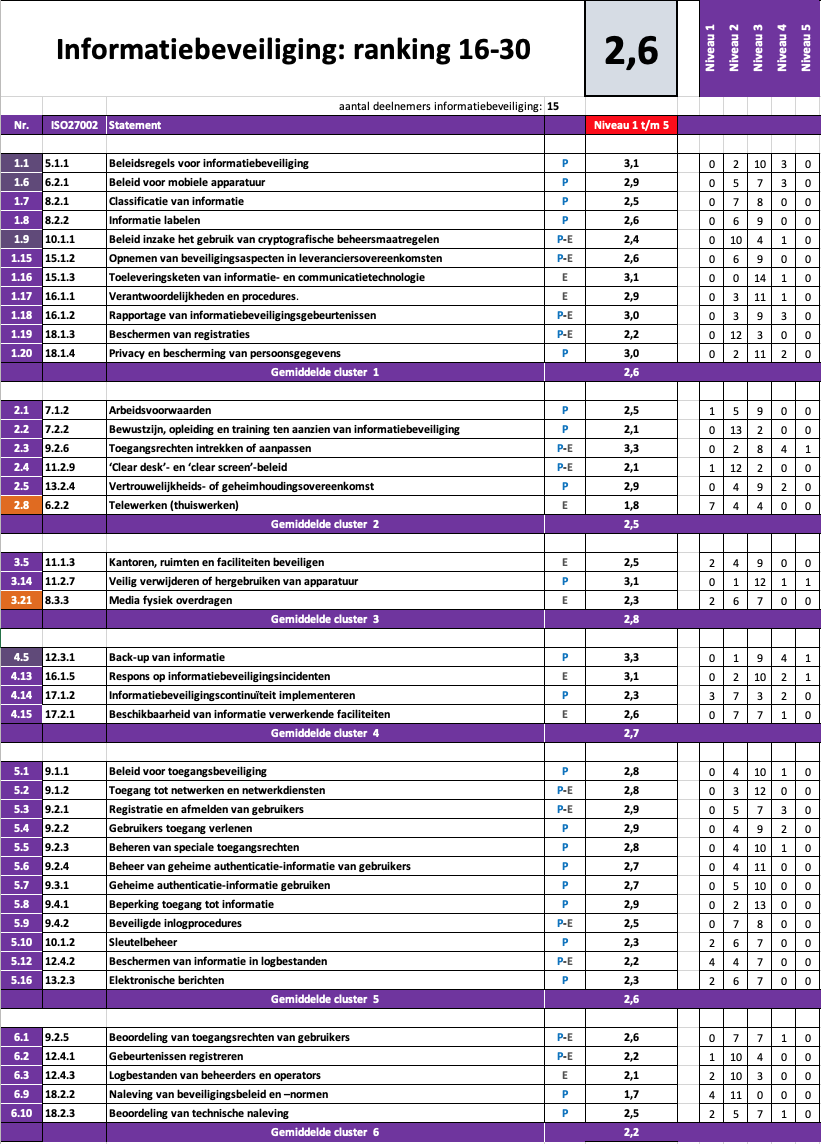
## Controle en logging

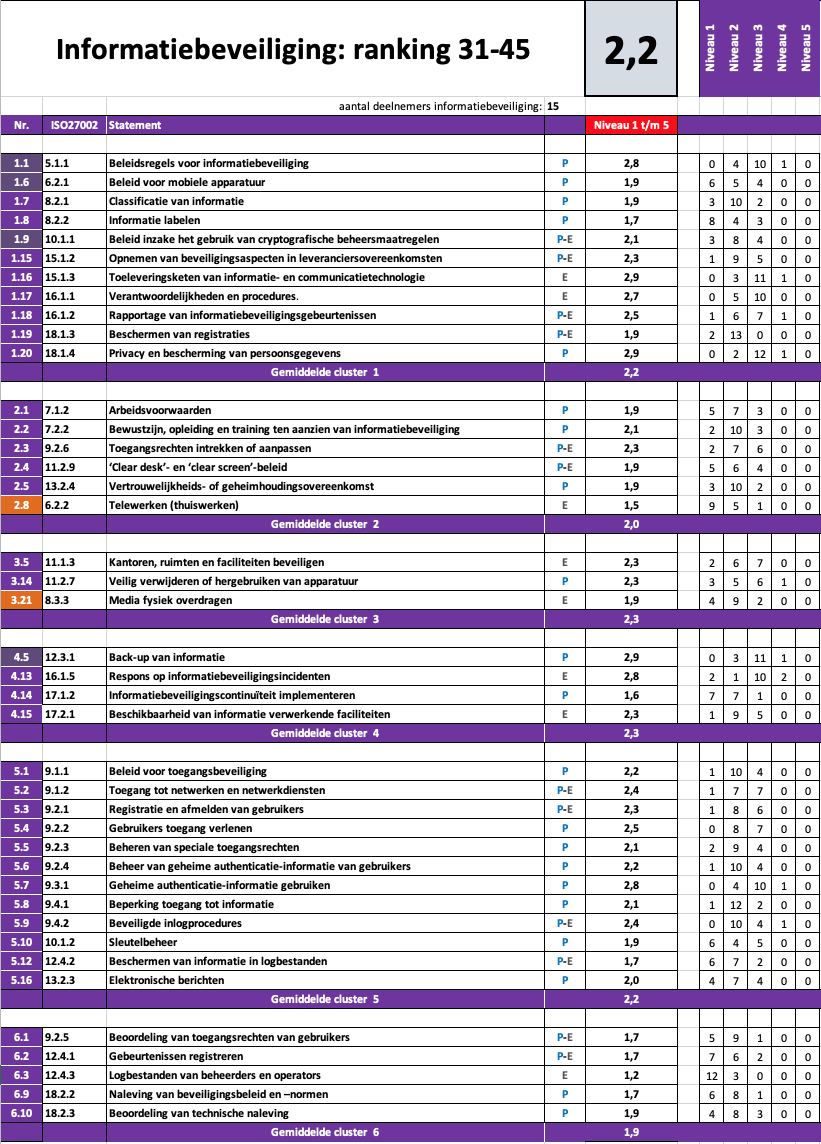
Afbeelding met schermafbeelding

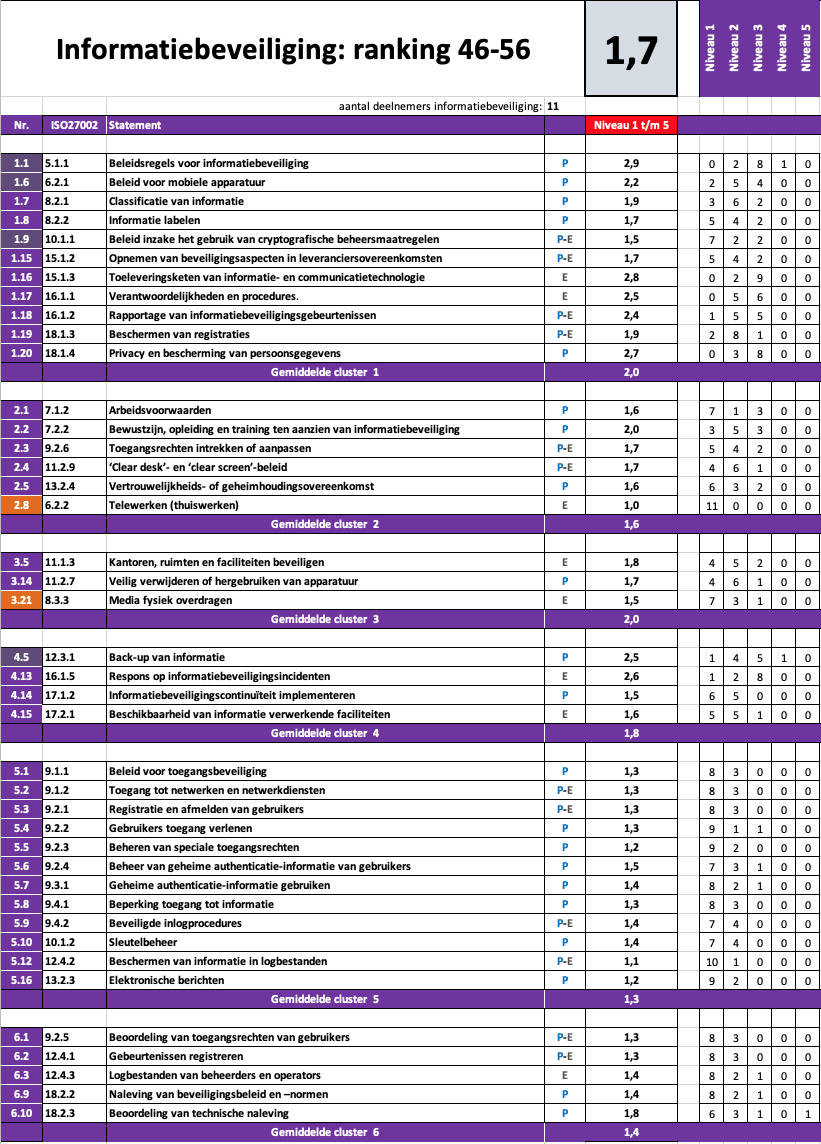
Automatisch gegenereerde beschrijving

# Bijlage 2: ranking IB in 4 groepen









# Bijlage 3: Respons vragenlijst

Na afloop van de invulperiode is er begin december 2019 een enquête uitgezet onder de respondenten met de volgende vier vragen.

1. Welke suggestie heb jij ter verbetering van het toetsingskader (IB, P en/of E)?  
   *Wat is het belangrijkste inhoudelijke verbeterpunt en op welke manier kunnen we dat realiseren*
2. Welke suggestie heb jij ter verbetering van het proces rondom de benchmark IBP/E?  
   *Wat is het belangrijkste procesmatige verbeterpunt en op welke manier kunnen we dat realiseren*
3. Welke suggestie heb jij ter verbetering van de resultaten van de benchmark IBP/E?  
   *Wat hebben we nodig om als instelling en/of mbo-sector op het gewenste volwassenheidsniveau 3 te komen?*
4. Welke suggestie heb jij met betrekking tot de uitvoering van de peer review?  
   *Hoe kunnen we de peer review een structurele plaats geven als instrument om de kwaliteit/objectiviteit van de benchmark te verbeteren? Of moeten we dat op een andere manier doen?*

Hieronder een opsomming van de gegeven antwoorden.

## Inhoudelijke verbeterpunten van de toetsingskaders

* Voeg een handleiding toe met tips om een en ander in te vullen.
* De toelichting kan nog wat duidelijker. Er blijven bij het invullen toch nog wel vragen over wat er nu precies bedoeld wordt.
* Meer clusteren wat betrekking heeft op elkaar, eventueel samenvoegen in 1 document.
* De mogelijkheid om Niet van toepassing in te kunnen vullen. Meer rekening houden met kleine scholen deze hebben een veel meer bescheiden organisatie."
* Je kan zien dat het geschreven is door verschillende mensen. Hoofdstuk 3 en 4 heeft voor elk statement dezelfde evidence voor niveau 2 en 3. Dat is jammer. Hier valt ook op dat voor niveau 3 steeds sprake is van een auditor. Dit ligt te dicht bij niveau 5.
* Er lijken toch nog dubbelingen te zijn, bijvoorbeeld 3.2 Verwijderen van media en 3.14 Veilig verwijderen of hergebruiken van apparatuur. Of 4.18 en 4.19 Informatiebeveiligingscontinuïteit plannen, respectievelijk verifiëren, beoordelen en evalueren. Het lijkt mij dat deze samengevoegd kunnen worden, maar mogelijk is dat niet gedaan om aan te blijven sluiten bij de algemene standaard.
* We hebben gemerkt dat op basis van het hebben van dataregisters er dan wel erg veel statements zijn die dan direct score 3 opleveren.
* Vond het een goede stap om relaties aan te geven tussen verschillende statements. Misschien ook statements prioriteren? Bv wij doen niks met eigen ontwikkeling van software. Maar wordt even hard gewogen als een statement waar wij wel iets in doen. Statements optioneel maken?
* Niet alle statements zijn even duidelijk hoe het bedoeld wordt en/of sluiten aan bij de eigen onderwijsinstelling. Maar dat zal je toch houden.
* Een aantal uitwerkingen kloppen niet met de statements. Daarnaast zijn een aantal onderdelen eenzijdig ingevuld, bijvoorbeeld scholing deelname aan ibp netwerkdag, dit zou breder kunnen.
* De aanpassingen in de beschrijvingen in het toetsingskader (met name de bewijsvoering voor de niveaus 2 en 3) en de bijbehorende manier om de bewijsvoering vast te leggen in het document zijn erg prettig. Een nadere uitwerking van volwassenheidsniveau 4 zou kunnen helpen af en toe ook deze score gefundeerd vast te leggen
* Duidelijker maken wat niveau 4 inhoudt. Onze (foute..?) interpretatie is dat het door "onafhankelijke ogen" controleren van het PROCES een niveau 4 oplevert (bijv. steekproefsgewijs controleren admin-accounts). Echter blijkt die controle in niveau 3 te zitten en hoeft die niet perse door een onafhankelijk iemand te worden uitgevoerd. Niveau 4 lijkt meer te maken te hebben met het evalueren van het BELEID. Vind ik niet sterk.....
* Teveel stukken moeten goedgekeurd worden door de directie. Wij leggen alleen stukken op strategisch niveau voor aan de directie, op tactisch niveau bij de CIO en operationeel niveau bij de manager I&A.

## Procesmatige verbeterpunten rondom de benchmark

* De beschikbare tijd, na publicatie van het nieuwe toetsingskader (met veel nieuwe statements), was te kort. Daardoor zijn we in volwassenheid gedaald ten opzichte van het oude toetsingskader.
* Bekendmaking nieuwe punten toetsingskader naar voren halen zodat hier op tijd op geacteerd kan worden.
* Niet over deze benchmark, maar toch: heb oog voor de veelheid van (ook andere) benchmarks in de MBO sector; laat e.e.a. met elkaar samengaan en motiveer op hoog overlegniveau het nut ervan. Anders bestaat in mijn beleving de kans dat deze en/of andere benchmarks gaan sneuvelen om de (te) simpele reden van de grote hoeveelheid.
* We hebben Smile aangeschaft waarin de scores nu ook staan. Maar misschien kunnen de scores gekoppeld worden. Of kan de benodigde evidence daar ook beter beschreven worden.
* Voor de onderwijsinstellingen die nog in een beginstadium bevinden is het lastig om de vragenlijst me de statements in te voeren. Immers schort het aan het informatieniveau en organisatiegraad/capaciteit om ook daadwerkelijk een correct beeld van alle statements te krijgen.
* Consistentie van de inhoud; niet te veel statements erbij of eraf halen van jaar tot jaar. Daardoor verandert het cijfer ook ineens. Leek je eerst op de goede weg, door de nieuwe statements of juist het verwijderen ervan blijk je er ineens minder goed of juist beter voor te staan. Dat vertroebelt het zicht op de progressie.
* Wij gaan voor de verbeteringen het komend jaar de teksten van het toetsingskader gebruiken om de verbeteringen te realiseren en om de bijbehorende bewijsvoering vast te leggen. Hiervoor moeten we de teksten wel splitsen naar actoren. Een kenmerk voor het type afdeling dat in de regel verantwoordelijk is voor een bepaald item zou die actie eenvoudiger maken.
* Ik vond de wijze waarop we dit jaar de excel en het word document naast elkaar moesten gebruiken niet praktisch.
* (ook) gebruik gaan maken van Smile (is volgens mij ook al de bedoeling).

## Verbetering van de resultaten van de Benchmark IBP/E

* Sommige antwoorden zijn niet realistisch. Wijs daar de deelnemers op.
* Uniformering? Gedragscode bij AP.
* Planmatig aan de slag.
* Geduld, je moet ook nog de mensen, besturen meekrijgen.
* Standaard overzicht van alle documentatie die je nodig hebt. Standaard overzicht in welke processen welke documenten moeten zitten. (bijvoorbeeld bij in dienst melding)
* Mbo-instellingen vragen om voorbeeld-documenten en die centraal beschikbaar stellen. Bronvermelding is dan wel zo aardig. Template voor gespreksverslag helpt ook.
* Voorbeeld beleidstukken waarnaar wordt verwezen in de individuele punten uit de IBP-benchmark. Lijst maken van alle benodigde beleidstukken per punt/vraag uit het toetsingskader en per vraag een voorbeeld document voor zover niet aanwezig. Deze kunnen dan worden omgeschreven naar de specifieke instelling en ondertekend worden door het bestuur. Als kleine organisatie is de administratieve last om alle documenten op orde te krijgen te groot om de benodigde stappen te maken.
* Uitvoering van een plan van aanpak voor de Security Officer en de FG. Het plan bevat detail-aanbevelingen naar aanleiding van de benchmark, waaronder: handhaving en controle op autorisaties en beleid, scholing en awareness, wijzigingsbeheer, aandacht voor bewaartermijnen, organiseer forensisch onderzoek indien nodig vanwege strafrechtelijk onderzoek, en DPIA's uitvoeren voor de belangrijkste systemen.
* Het kiezen van 10 statements in de peer review nogmaals ten het licht aan houden. Wat zegt het als van die 10 statements er 8 afgekeurd kunnen worden? Meer statements is automatisch veel meer werk, zitten we ook niet op te wachten. Echte oplossing weet ik niet, maar vind het wel een pijnpunt. Overigens mogelijk niet echt een verbetering qua score, maar wel in het aangeven van een reëler beeld.
* Veel tijd
* Zitten al op nivo 3 behalve qua examinering. Ik moet daar nog wat aan bewustwording doen bij de proceseigenaar en hoger management.
* Veel ligt aan onze organisatie zelf. wellicht kan geholpen worden om de awareness op dit gebied bij het dagelijks bestuur van de organisatie te verhogen (voorlichtingscampagne?)
* Meer voorbeelddocumenten, -procesbeschrijvingen
* Denk dat peer audit review kan helpen om meer eenheid in 'interpretaties van de actuele stand van zaken' te krijgen.

## Uitvoering van de peer review

* Peer review eenduidiger uitvoeren. Het is een assessment en geen audit. Dus ook mondelinge toelichting is akkoord.
* Peer review op een eerder moment in het jaar.
* De complete uitvoering, inclusief voorbereiding, verzamelen van evidence, het bezoek met interviews, en vooral de uitwerking in de vorm van een rapport kost erg veel tijd. Vereenvoudigen van het formele proces is mogelijk: niet standaard presenteren/verdedigen van de bevindingen. Als het rapport kwalitatief in orde is bevonden, is dit vaak niet nodig. Eventuele vragen/opmerkingen kunnen efficiënter behandeld worden.
* Zeker geen uitbreiding van het aantal te beoordelen statements.
* Eerder uitvoeren.
* De top 3 beste instellingen elk jaar door saMBO-ICT en/of externe auditor laten beoordelen.
* Ik heb er voorkeur voor om laagdrempelig te beginnen met collegiale toetsing. Het is dan mogelijk om van elkaar te leren, maar ook om kritisch naar elkaar te kijken.
* Ik heb meegedaan aan de eerste masterclass peer review en vond het toen erg vervelend dat het format zo strikt werd gehanteerd. Ik moest elke zin op een specifieke manier opstellen. Dat hielp mijn niet, terwijl ik het wel waardevol en leerzaam vond om bij anderen te kijken hoe het daar ging en ook om anderen bij ons te laten kijken en vragen te laten stellen.
* Zowel de benchmark als een peer review qua timing inpassen in de cyclus van de school, dit is voor iedere school anders.
* De norm moet zo min mogelijk interpretabel zijn. Heb het gevoel dat er met "twee maten" gemeten kan worden. Voorbeeld: als je 5 dingen moeten opleveren om op statement op niveau 3 te scoren, is 4 dingen voldoende voor niveau 3 of moet het toch 5 zijn.
* De peerreview is een goed middel voor de controle van het zelfassessment. Echter wordt over het invullen van de benchmark gezegd dat de beoordeling inhoudelijk moet kloppen. Bij de peerreview wordt echter letterlijk gecontroleerd of alle documenten en processen aanwezig zijn. Het sluit daardoor op dit moment niet goed aan, bij de wijze van invullen van de Benchmark.
* Duidelijkheid geven over het al dan niet verplichte karakter van de evidence. Wij hanteren pas toe of leg uit principe. De peer reviewers dachten er anders over.
* Een zeer heldere en realistische planning geven van het hele traject. dit jaar niet meegedaan wegens resource problemen. Helder in kaart brengen wat de meerwaarde is van de peer review voor de deelnemende instellingen; dit kan helpen om de hierboven genoemde resources te claimen.
* Wellicht beter aan externe onafhankelijke partijen?

# Bijlage 4: Framework ibp in het mbo

De Regiegroep ibp in het mbo onderhoudt een documentenbibliotheek met diverse modeldocumenten. Dit Framework ibp in het mbo is beschikbaar via [www.sambo-ict.nl/framework-ibp](http://www.sambo-ict.nl/framework-ibp).

Ook de toetsingskaders die voor deze benchmark zijn gebruikt zijn te vinden in het Framework. Het betreft de volgende documenten:

* [Toetsingskader Informatiebeveiliging (ibpdoc3)](http://www.sambo-ict.nl/ibpdoc3)
* [Toetsingskader Privacy (ibpdoc7)](http://www.sambo-ict.nl/ibpdoc7)
* [Toetsingskader Examinering (ibpdoc8)](http://www.sambo-ict.nl/ibpdoc8)
* [Spreadsheet met de toetsingskaders IB, P en E (ibpdoc40)](http://www.sambo-ict.nl/ibpdoc40)

