



Mbo benchmark IBP/E 2019

Martijn Bijleveld en Leo Bakker

| | | | | | | | | |
|-------------|---|-------------|-------------|-------------|-------------|-------------|--|--|
| | Diverse beveiligingsincidenten, examenfraude | | | | | | | |
| | Taskforce Informatiebeveiliging en Privacy Framework IB 1.0 | | | | | | | |
| | Start masterclasses informatiebeveiliging en privacy | | | | | | | |
| | Toetsingskader IB 1.0 | | | | | | | |
| | Benchmark IB 2015 | | | | | | | |
| | Compliancekader Privacy | | | | | | | |
| | Toetsingskader Privacy 1.0 | | | | | | | |
| | Toetsingskader IB 2.0 | | | | | | | |
| | Benchmark IBP 2016 | | | | | | | |
| | Toetsingskader IB 3.0 | | | | | | | |
| | Benchmark IBP 2017 | | | | | | | |
| | Toetsingskader Examinering | | | | | | | |
| | Benchmark IBP 2018 | | | | | | | |
| | Peer review 2018 | | | | | | | |
| | Framework IBP 2.0 | | | | | | | |
| | Toetsingskader Examinering 3.0 | | | | | | | |
| | Toetsingskader Privacy 3.0 | | | | | | | |
| | Peer review 2019 | | | | | | | |
| | | | | | | | | |
| 2014 | | 2015 | 2016 | 2017 | 2018 | 2019 | | |

IBP Benchmark mbo 2019

| | 2015 | 2016 | 2017 | 2018 |
|--|------------|------------|------------|------------|
| Cluster 1: Beleid en organisatie | 1,7 | 1,8 | 2,0 | 2,4 |
| Cluster 2: Personeel, studenten en gasten | 1,7 | 1,7 | 1,9 | 2,3 |
| Cluster 3: Ruimtes en apparatuur | 2,1 | 2,2 | 2,3 | 2,5 |
| Cluster 4: Continuïteit | 2,0 | 2,1 | 2,3 | 2,5 |
| Cluster 5: Vertrouwelijkheid en integriteit | 2,0 | 2,0 | 2,2 | 2,4 |
| Cluster 6: Controle en Logging | 1,6 | 1,6 | 1,8 | 2,1 |
| Totaal score Informatiebeveiliging in de mbo sector | 1,9 | 1,9 | 2,1 | 2,4 |
| Totaal score Privacy in de mbo sector | - | 1,5 | 1,9 | 2,3 |
| Totaal score Examinering in de mbo sector | - | - | - | 2,1 |
| Deelnamepercentage | 29% | 46% | 77% | 95% |

2015.....

Verplichte zelfregulering: waarom?

Kennisnet

saMBO-ICT

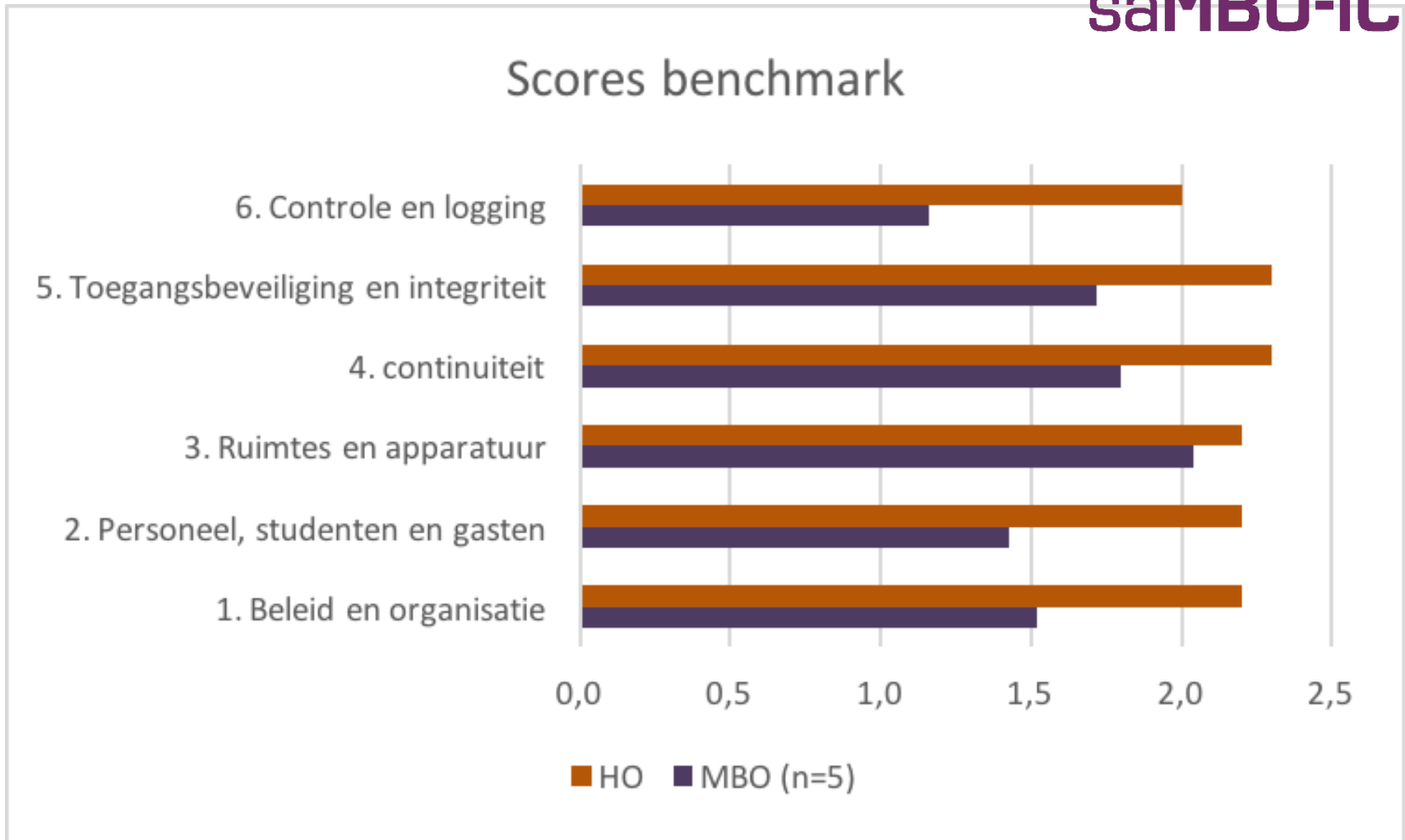
Organisatie (ROC):

Benchmark een instrument waarmee bestuur/management in staat zijn te meten of de organisatie 'in control' is op gebied van informatieveiligheid.

Sector (MBO):

Voor een beeld van de volwassenheid van de hele sector is een vorm van benchmarking noodzakelijk opdat kan worden vastgesteld of er sprake is van een normale distributie van risico's.

Assessment / benchmark 2015



IBP Benchmark mbo 2019

- 2015 Benchmark IB : 19 instellingen
- 2016 Benchmark IB en P : 30/20 instellingen
- 2017 Benchmark IB en P : 47/31 instellingen
- 2018 Benchmark IB, P en E : 57/56/43 instellingen
- 2019 Benchmark IB, P en E : 100%.....

| | 2015 | 2016 | 2017 | 2018 |
|--|------------|------------|------------|------------|
| Cluster 1: Beleid en organisatie | 1,7 | 1,8 | 2,0 | 2,4 |
| Cluster 2: Personeel, studenten en gasten | 1,7 | 1,7 | 1,9 | 2,3 |
| Cluster 3: Ruimtes en apparatuur | 2,1 | 2,2 | 2,3 | 2,5 |
| Cluster 4: Continuïteit | 2,0 | 2,1 | 2,3 | 2,5 |
| Cluster 5: Vertrouwelijkheid en integriteit | 2,0 | 2,0 | 2,2 | 2,4 |
| Cluster 6: Controle en Logging | 1,6 | 1,6 | 1,8 | 2,1 |
| Totaal score Informatiebeveiliging in de mbo sector | 1,9 | 1,9 | 2,1 | 2,4 |
| Totaal score Privacy in de mbo sector | - | 1,5 | 1,9 | 2,3 |
| Totaal score Examinering in de mbo sector | - | - | - | 2,1 |
| Deelnamepercentage | 29% | 46% | 77% | 95% |

| | 2015 | 2016 | 2017 | 2018 |
|--|------------|------------|------------|------------|
| Cluster 1: Beleid en organisatie | 1,7 | 1,8 | 2,0 | 2,4 |
| Cluster 2: Personeel, studenten en gasten | 1,7 | 1,7 | 1,9 | 2,3 |
| Cluster 3: Ruimtes en apparatuur | 2,1 | 2,2 | 2,3 | 2,5 |
| Cluster 4: Continuïteit | 2,0 | 2,1 | 2,3 | 2,5 |
| Cluster 5: Vertrouwelijkheid en integriteit | 2,0 | 2,0 | 2,2 | 2,4 |
| Cluster 6: Controle en Logging | 1,6 | 1,6 | 1,8 | 2,1 |
| Totaal score Informatiebeveiliging in de mbo sector | 1,9 | 1,9 | 2,1 | 2,4 |
| Totaal score Privacy in de mbo sector | - | 1,5 | 1,9 | 2,3 |
| Totaal score Examinering in de mbo sector | - | - | - | 2,1 |
| Deelnamepercentage | 29% | 46% | 77% | 95% |

Informatiebeveiliging ranking 1-15

2,9

Niveau 1

Niveau 2

Niveau 3

Niveau 4

Niveau 5

aantal deelnemers aan informatiebeveiliging: 15

| Nr. | ISO27002 | Statement | Niveau 1 t/m 5 | | | | | |
|------|----------|---|----------------|---|----|----|---|---|
| 1.1 | 5.1.1.1 | Beleidsregels voor informatiebeveiliging | 3,1 | 1 | 2 | 7 | 4 | 1 |
| 1.2 | 5.1.1.2 | Beleidsregels voor informatiebeveiliging | 2,5 | 2 | 5 | 7 | 1 | 0 |
| 1.20 | 18.1.4 | Privacy en bescherming van persoonsgegevens | 3,1 | 0 | 4 | 6 | 4 | 1 |
| 1.21 | 6.1.2 | Scheiding van taken | 3,1 | 0 | 1 | 12 | 2 | 0 |
| | | Gemiddelde cluster 1 | 2,8 | | | | | |
| 2.1 | 7.1.2 | Arbeidsvoorwaarden | 2,7 | 1 | 3 | 11 | 0 | 0 |
| 2.2 | 7.2.2 | Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging | 2,2 | 1 | 10 | 4 | 0 | 0 |
| 2.7 | 7.1.1 | Screening | 3,0 | 1 | 2 | 8 | 4 | 0 |
| | | Gemiddelde cluster 2 | 2,7 | | | | | |
| | | Gemiddelde cluster 3 | 3,0 | | | | | |
| 4.1 | 12.1.2 | Wijzigingsbeheer | 3,1 | 0 | 3 | 7 | 5 | 0 |
| | | Gemiddelde cluster 4 | 3,1 | | | | | |
| 5.1 | 9.1.1 | Beleid voor toegangsbeveiliging | 3,0 | 0 | 5 | 7 | 1 | 2 |
| | | Gemiddelde cluster 5 | 3,0 | | | | | |
| 6.1 | 9.2.5 | Beoordeling van toegangsrechten van gebruikers | 2,5 | 0 | 8 | 7 | 0 | 0 |
| | | Gemiddelde cluster 6 | 2,5 | | | | | |

Privacy

2,3

Niveau 1

Niveau 2

Niveau 3

Niveau 4

Niveau 5

aantal deelnemers aan Privacy: 56

| Nr. | Statement | Niveau 1 t/m 5 | | | | | |
|------|---|----------------|----|----|----|----|---|
| P.1 | Privacy-beleid | 2,9 | 1 | 14 | 32 | 9 | 0 |
| P.2 | Functionaris gegevensbescherming | 3,4 | 0 | 5 | 24 | 26 | 1 |
| P.3 | Doelbepaling, doelbinding, grondslag, grond bij minderjarigen en dataminimalisatie. | 2,2 | 10 | 29 | 13 | 4 | 0 |
| P.4 | Registratieplicht | 2,3 | 10 | 21 | 22 | 2 | 1 |
| P.5 | Bewaartermijnen | 1,7 | 21 | 31 | 3 | 1 | 0 |
| P.6 | Verwerking t.b.v. onderzoek | 1,6 | 28 | 20 | 8 | 0 | 0 |
| P.7 | Verwerking van bijzondere persoonsgegevens | 2,2 | 12 | 24 | 19 | 1 | 0 |
| P.8 | Geautomatiseerde besluitvorming | 1,8 | 31 | 11 | 7 | 4 | 2 |
| P.9 | Informatiebeveiliging | 2,5 | 0 | 35 | 15 | 6 | 0 |
| P.10 | Verwerkersovereenkomsten (in toetsingskader Bewerkersovereenkomst) | 2,6 | 1 | 25 | 27 | 3 | 0 |
| P.11 | Transparantie privacy-beleid | 2,8 | 1 | 15 | 35 | 5 | 0 |
| P.12 | Informatieplicht verwerkingen | 2,5 | 2 | 27 | 23 | 4 | 0 |
| P.13 | Rechten betrokkene | 2,6 | 3 | 21 | 29 | 3 | 0 |
| P.14 | Arbeidsvoorwaarden | 2,4 | 6 | 28 | 18 | 4 | 0 |
| P.15 | Bewustzijn, opleiding en training ten aanzien van privacy | 2,1 | 11 | 32 | 12 | 1 | 0 |
| P.16 | Verwijderen van persoonsgegevens | 2,2 | 9 | 29 | 16 | 1 | 1 |
| P.17 | Datakwaliteit | 2,3 | 2 | 39 | 11 | 4 | 0 |
| P.18 | Datalek | 3,0 | 2 | 11 | 29 | 12 | 2 |
| P.19 | Toegang tot bijzondere persoonsgegevens | 2,2 | 9 | 32 | 11 | 3 | 1 |
| P.20 | Privacy in informatiesystemen | 1,9 | 13 | 37 | 6 | 0 | 0 |
| P.21 | Gegevensbeschermingseffectbeoordeling (DPIA) | 1,8 | 21 | 28 | 6 | 1 | 0 |
| P.22 | Naleving van privacy beleid en –normen | 1,9 | 10 | 44 | 2 | 0 | 0 |
| P.23 | Rapportage van privacy-gebeurtenissen | 2,5 | 7 | 20 | 26 | 2 | 1 |
| P.24 | Gebeurtenissen registreren | 2,0 | 10 | 34 | 12 | 0 | 0 |
| | | 2,3 | | | | | |

Examinering

2,1

Niveau 1

Niveau 2

Niveau 3

Niveau 4

Niveau 5

aantal deelnemers examinering: 43

| Nr. | Statement | Niveau 1 t/m 5 | | | | | |
|------|---|----------------|----|----|----|---|---|
| E.1 | Beleidsregels examinering | 2,0 | 17 | 11 | 13 | 1 | 1 |
| E.2 | Richtlijnen bij constatering fraude bij digitale examens | 2,4 | 5 | 20 | 13 | 5 | 0 |
| E.3 | Procesaanpassing bij digitale examens m.b.t. examenfraude | 2,0 | 10 | 23 | 6 | 3 | 0 |
| E.4 | Procedure ontwikkelen examinering in beveiligde omgeving | 2,5 | 4 | 16 | 18 | 4 | 0 |
| E.5 | Procedure voorbereiden en afnemen examens | 2,5 | 9 | 10 | 17 | 5 | 1 |
| E.6 | Eindevaluatie examenproces en de integriteit van resultaten | 2,2 | 15 | 11 | 11 | 6 | 0 |
| E.7 | Gedragcodes, inclusief richtlijnen | 2,3 | 7 | 18 | 15 | 3 | 0 |
| E.8 | Extra ondersteuning bij examens. | 2,7 | 1 | 19 | 16 | 7 | 0 |
| E.9 | Trainingen en vaardigheden m.b.t fraude bij digitale examens (fout) | 1,6 | 24 | 13 | 6 | 0 | 0 |
| E.10 | Beveiligde examenruimte | 2,0 | 13 | 19 | 9 | 1 | 0 |
| E.11 | Faciliteiten voor examen | 2,0 | 16 | 15 | 10 | 2 | 0 |
| E.12 | Hanteren van digitaal examenmateriaal | 2,1 | 12 | 17 | 10 | 3 | 0 |
| E.13 | Continuïteitsplan | 1,7 | 25 | 8 | 9 | 1 | 0 |
| E.14 | Toekennen examens aan deelnemers | 2,6 | 7 | 11 | 16 | 6 | 1 |
| E.15 | Hergebruik examenvragen | 1,8 | 20 | 15 | 4 | 1 | 2 |
| E.16 | Vernietigen examenmateriaal | 2,0 | 11 | 22 | 7 | 3 | 0 |
| | | 2,1 | | | | | |

Algemene conclusies:

1. Doelstelling van een score 2 is gehaald
2. Technische zaken goed op orde
3. Bewustwording (personeel) is aandachtspunt
4. Cluster 6, monitoring en logging blijft achter
5. Bewaartermijnen en DPIA's nog een probleem
6. Peer Review kan helpen
7. Privacy heeft inhaalslag gemaakt
8. Examinering op 2.1, maar daar moet nog veel werk verzet worden

IBP Benchmark mbo 2019

| | 2015 | 2016 | 2017 | 2018 |
|--|------------|------------|------------|------------|
| | 1,7 | 1,8 | 2,0 | 2,4 |
| Cluster 1: Beleid en organisatie | 1,7 | 1,7 | 1,9 | 2,3 |
| Cluster 2: Personeel, studenten en gasten | 2,1 | 2,2 | 2,3 | 2,5 |
| Cluster 3: Ruimtes en apparatuur | 2,0 | 2,1 | 2,2 | 2,4 |
| Cluster 4: Continuïteit | 1,6 | 1,6 | 1,8 | 2,1 |
| Cluster 5: Vertrouwelijkheid en integriteit | | | | 2,4 |
| Cluster 6: Controle en Logging | 1,9 | 1,9 | 2,1 | |
| Totaal score Informatiebeveiliging in de mbo sector | | | | 2,3 |
| Totaal score Privacy in de mbo sector | - | 1,5 | 1,9 | 2,1 |
| Totaal score Examinering in de mbo sector | - | - | - | 2,1 |
| Deelnamepercentage | 29% | 46% | 77% | 95% |

Nieuwe ronde, 'nieuwe' kaders

- Update Toetsingskader IB, versie 3.0
- Update Privacykader 3.0
- Update Examineringskader 3.1
- Spreadsheet
- Doorklikbare Word-documenten

Update toetsingskaders

Informatiebeveiliging

- ISO 27002 helemaal afdekken
- Nieuwe vormen van bewijsvoering

Privacy

- Aanpassingen WBP > AVG
- Beschrijvingen statements en bewijslast

Examinering

- Verwerken feedback werkveld
- Beter in lijn met PE

Update toetsingskader IB

Met dank aan de leden van de werkgroep Toetsingskader 4.0

| | |
|----------------------------|-------------------------|
| Ludo Cuijpers (voorzitter) | Kennisnet |
| Wim Arendse | Zadkine |
| Bert Barske | Drenthe College |
| Henk Bax | S.G. de Rooi Pannen |
| Martijn Bijleveld | saMBO-ICT |
| Bart Bosma | SURFnet |
| Paula Cartigny | ROC Nijmegen |
| Niels Dutij | Cibap |
| Elly Dingemanse | Kennisnet |
| Elke van Essen | Kien |
| Samantha Lejeune | Vista College |
| Fung Yee Poon | Aventus |
| Daniël Rense | Meerkring |
| Rene Ritzen | SURFnet |
| Leander Versleijen | Movare |
| Jurrian Wijffels | Fontys Hogescholen |
| Rene Zaal | Novacollege |
| Frits van Zadelhoff | Koning Willem I College |

Update toetsingskader IB

- nieuwe statements
- bewijslast
- beschrijving volwassenheidsniveaus
- spreadsheet

Nieuwe statements IB

- 30 statements toegevoegd
- 7 statements vervallen (opnieuw geclusterd)
- totaal 108 statements IB (cluster 1-6)

1.23

6.1.4

NIEUW: Contact met speciale belangengroepen

Er behoren passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en professionele organisaties te worden onderhouden.

Lidmaatschap van speciale belangengroepen behoort te worden overwogen als middel om:

- Kennis te verbeteren over "best practices" en op de hoogte te blijven van relevante beveiligingsinformatie.
- Ervoor te zorgen dat de kennis van informatiebeveiliging actueel en volledig is.

Het IBP-beleid bevat een richtlijn "Lidmaatschap IBP-netwerken".

- ② Overleg een richtlijn: "Lidmaatschap IBP-netwerken".
- ③ Overleg een lijst met daadwerkelijke deelname aan de bijeenkomsten van bijvoorbeeld het IBP-netwerk mbo, SCIRT en SCIPR.

| Nr. | ISO27002 | Statement |
|------|-----------|---|
| 1.1 | 5.1.1 | Beleidsregels voor informatiebeveiliging |
| 1.2 | vervallen | Zie nr 1.1 (5.1.1) |
| 1.3 | 5.1.2 | Beoordeling van het Informatiebeveiligingsbeleid |
| 1.4 | 6.1.1 | Taken en verantwoordelijkheden informatiebeveiliging: |
| 1.5 | 6.1.5 | Informatiebeveiliging in projectbeheer |
| 1.6 | 6.2.1 | Beleid voor mobiele apparatuur: |
| 1.7 | 8.2.1 | Classificatie van informatie |
| 1.8 | 8.2.2 | Informatie labelen |
| 1.9 | 10.1.1 | Beleid inzake het gebruik van cryptografische beheersmaatregelen |
| 1.10 | vervallen | Zie nr. 1.9 (10.1.1) |
| 1.11 | 11.2.5 | Verwijdering van bedrijfsmiddelen |
| 1.12 | 13.2.1 | Beleid en procedures voor informatietransport: |
| 1.13 | 13.2.2 | Overeenkomsten over informatietransport |
| 1.14 | 14.1.1 | Analyse en specificatie van informatiebeveiligingseisen |
| 1.15 | 15.1.2 | Opnemen van beveiligingsaspecten in leveranciersovereenkomsten |
| 1.16 | 15.1.3 | Toeleveringsketen van informatie- en communicatietechnologie |
| 1.17 | 16.1.1 | Verantwoordelijkheden en procedures. |
| 1.18 | 16.1.2 | Rapportage van informatiebeveiligingsgebeurtenissen |
| 1.19 | 18.1.3 | Beschermen van registraties |
| 1.20 | 18.1.4 | Privacy en bescherming van persoonsgegevens |
| 1.21 | 6.1.2 | Scheiding van taken |
| 1.22 | 6.1.3 | Contact met overheidsinstanties |
| 1.23 | 6.1.4 | Contact met speciale belangengroepen |
| 1.24 | 8.2.3 | Behandelen van bedrijfsmiddelen |
| 1.25 | 18.1.1 | Vaststellen van toepasselijke wetgeving en contractuele eisen |
| 1.26 | 18.1.2 | Intellectuele eigendomsrechten |
| 1.27 | 18.1.3 | Voorschriften voor het gebruik van cryptografische beheersmaatregelen |

| | | |
|------|--------|--|
| 2.1 | 7.1.2 | Arbeidsvoorwaarden |
| 2.2 | 7.2.2 | Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging |
| 2.3 | 9.2.6 | Toegangsrechten intrekken of aanpassen |
| 2.4 | 11.2.9 | 'Clear desk'- en 'clear screen'-beleid |
| 2.5 | 13.2.4 | Vertrouwelijkheids- of geheimhoudingsovereenkomst |
| 2.6 | 16.1.3 | Rapportage van zwakke plekken in de informatiebeveiliging |
| 2.7 | 7.1.1 | Screening |
| 2.8 | 6.2.2 | Telewerken (thuiswerken) |
| 2.9 | 7.1.3 | Disciplinaire procedure |
| 2.10 | 7.3.1 | Beëindiging of wijziging van verantwoordelijkheden van het dienstverband |
| 3.2 | 8.3.2 | Verwijderen van media |
| 3.3 | 11.1.1 | Fysieke beveiligingszone |
| 3.4 | 11.1.2 | Fysieke toegangsbeveiliging |
| 3.5 | 11.1.3 | Kantoren, ruimten en faciliteiten beveiligen |
| 3.6 | 11.1.4 | Beschermen tegen bedreigingen van buitenaf |
| 3.7 | 11.1.5 | Werken in beveiligde gebieden |
| 3.8 | 11.1.6 | Laad- en loslocatie |
| 3.9 | 11.2.1 | Plaatsing en bescherming van apparatuur |
| 3.10 | 11.2.2 | Nutsvoorzieningen |
| 3.11 | 11.2.3 | Beveiliging van bekabeling |
| 3.12 | 11.2.4 | Onderhoud van apparatuur |
| 3.13 | 11.2.6 | Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein |
| 3.14 | 11.2.7 | Veilig verwijderen of hergebruiken van apparatuur |
| 3.15 | 12.4.4 | Kloksynchronisatie |
| 3.16 | 8.1.1 | Inventariseren van bedrijfsmiddelen |
| 3.17 | 8.1.2 | Eigendom van bedrijfsmiddelen |
| 3.18 | 8.1.3 | Aanvaardbaar gebruik van bedrijfsmiddelen |
| 3.19 | 8.1.4 | Teruggeven van bedrijfsmiddelen |
| 3.20 | 8.3.1 | Beheer van verwijderbare media |
| 3.21 | 8.3.3 | Media fysiek overdragen |

| | | |
|------|-----------|---|
| 4.1 | 12.1.2 | Wijzigingsbeheer |
| 4.2 | 12.1.4 | Scheiding van ontwikkel-, test- en productieomgevingen |
| 4.3 | 12.2.1 | Beheersmaatregelen tegen malware |
| 4.4 | vervallen | Zie nr 4.3 (12.2.1) |
| 4.5 | 12.3.1 | Back-up van informatie |
| 4.6 | vervallen | Zie nr 4.5 (12.3.1) |
| 4.7 | 12.5.1 | Software installeren op operationele systemen |
| 4.8 | 12.6.1 | Beheer van technische kwetsbaarheden |
| 4.9 | 12.6.2 | Beperkingen voor het installeren van software |
| 4.10 | 14.2.6 | Beveiligde ontwikkelomgeving |
| 4.11 | 15.2.2 | Beheer van veranderingen in dienstverlening van leveranciers |
| 4.12 | 16.1.4 | Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen |
| 4.13 | 16.1.5 | Respons op informatiebeveiligingsincidenten |
| 4.14 | 17.1.2 | Informatiebeveiligingscontinuïteit implementeren |
| 4.15 | 17.2.1 | Beschikbaarheid van informatie verwerkende faciliteiten |
| 4.16 | 12.1.1 | Gedocumenteerde bedieningsprocedures |
| 4.17 | 12.1.3 | Capaciteitsbeheer |
| 4.18 | 17.1.1 | Informatiebeveiligingscontinuïteit plannen |
| 4.19 | 17.1.3 | Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren |

| | | |
|------|--------|--|
| 6.4 | 14.2.7 | Uitbestede software testen |
| 6.5 | 14.2.8 | Testen van systeembeveiliging |
| 6.6 | 14.2.9 | Systeemacceptatietests |
| 6.7 | 15.2.1 | Monitoring en beoordeling van dienstverlening van leveranciers |
| 6.8 | 16.1.7 | Verzamelen van bewijsmateriaal |
| 6.9 | 18.2.2 | Naleving van beveiligingsbeleid en -normen |
| 6.10 | 18.2.3 | Beoordeling van technische naleving |
| 6.11 | 7.2.1 | Directieverantwoordelijkheden |
| 6.12 | 12.7.1 | Beheersmaatregelen betreffende audits van informatiesystemen |
| 6.13 | 16.16 | Lering uit informatiebeveiligingsincidenten |
| 6.14 | 18.2.1 | Onafhankelijke beoordeling van informatiebeveiliging |

| | | |
|------|-----------|---|
| 5.1 | 9.1.1 | Beleid voor toegangsbeveiliging |
| 5.2 | 9.1.2 | Toegang tot netwerken en netwerkdiensten |
| 5.3 | 9.2.1 | Registratie en afmelden van gebruikers |
| 5.4 | 9.2.2 | Gebruikers toegang verlenen |
| 5.5 | 9.2.3 | Beheren van speciale toegangsrechten |
| 5.6 | 9.2.4 | Beheer van geheime authenticatie-informatie van gebruikers |
| 5.7 | 9.3.1 | Geheime authenticatie-informatie gebruiken |
| 5.8 | 9.4.1 | Beperking toegang tot informatie |
| 5.9 | 9.4.2 | Beveiligde inlogprocedures |
| 5.10 | 10.1.2 | Sleutelbeheer |
| 5.11 | vervallen | Zie nr 5.10 (10.1.2) |
| 5.12 | 12.4.2 | Beschermen van informatie in logbestanden |
| 5.13 | vervallen | niet relevant (13.1.1; Beheersmaatregelen voor netwerken) |
| 5.14 | 13.1.2 | Beveiliging van netwerkdiensten |
| 5.15 | 13.1.3 | Scheiding in netwerken |
| 5.16 | 13.2.3 | Elektronische berichten |
| 5.17 | 14.1.3 | Transacties van toepassingen beschermen |
| 5.18 | 9.4.3 | Systeem voor wachtwoordbeheer |
| 5.19 | 9.4.4 | Speciale systeemhulpmiddelen gebruiken |
| 5.20 | 9.4.5 | Toegangsbeveiliging op programmabroncode |
| 5.21 | vervallen | niet relevant (14.1.2) |
| 5.22 | 14.2.1 | Beleid voor beveiligd ontwikkelen |
| 5.23 | 14.2.2 | Procedures voor wijzigingsbeheer met betrekking tot systemen |
| 5.24 | 14.2.3 | Technische beoordeling van toepassingen na wijzigingen bedieningsplatform |
| 5.25 | vervallen | niet relevant (14.2.4) |
| 5.26 | vervallen | niet relevant (14.2.5) |
| 5.27 | 14.3.1 | Bescherming van testgegevens |
| 5.28 | vervallen | niet relevant (15.1.1) |

Bewijslast

- documenten
- interview
- waarneming ter plaatse
- re-performance

Bewijslast: documenten

| | |
|--|--------------------------------|
| Cluster: | 1 Beleid en Organisatie |
| Toetsingskader 4.0 nummer: 1.1 | ISO-27002 nummer: 5.1.1 |
| Controledoelstelling: Beleidsregels voor informatiebeveiliging Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd en goedgekeurd door het College van Bestuur. | |

Bewijslast: interview

| | |
|--|---|
| Cluster: | 2 Personeel, studenten en gasten |
| Toetsingskader 4.0 nummer: 2.4 | ISO-27002 nummer: 11.2.9 |
| Controledoelstelling: 'Clear desk'- en 'clear screen'-beleid Er behoort een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatie verwerkende faciliteiten te worden ingesteld. | |

Bewijslast: waarneming ter plaatse

| | |
|---|--------------------------------|
| Cluster: | 3 Ruimten en apparatuur |
| Toetsingskader 4.0 nummer: 3.3 | ISO-27002 nummer: 11.1.1 |
| Controledoelstelling: Fysieke beveiligingszone Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten. | |

Bewijslast: re-performance

| | |
|---|-----------------------|
| Cluster: | 4 Continuïteit |
| Toetsingskader 4.0 nummer: 4. | ISO-27002 nummer: 8. |
| Controledoelstelling: Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiliging incidenten. | |

Beschrijving bewijsvoering

- uitsluitend niveau 2 en 3
- niveau 4 = opgenomen in pdca cyclus
- niveau 5 = externe accountant

Er is een awarenesscampagne en introductie- /scholingsprogramma opgesteld voor de huidige en de toekomstige medewerkers. Dit plan kan jaarlijks worden bijgesteld als gevolg van actuele ontwikkelingen op het IBP-gebied. De evidence is gebaseerd op het hebben van een gedefinieerd scholingsplan met begroting en omschreven doelgroep is.

② Overleg een document waar de awareness (algemeen) en de scholing (doelgroepen) in het kader van IBP is beschreven en vastgesteld.

③ Overleg een begroting in het kader van de awareness campagne, geef een overzicht van de financiële realisatie en toon de gemeten resultaten aan.

③ Overleg een lijst waaruit aangetoond kan worden dat 90% van de doelgroep, heeft deelgenomen aan de IBP-scholing.

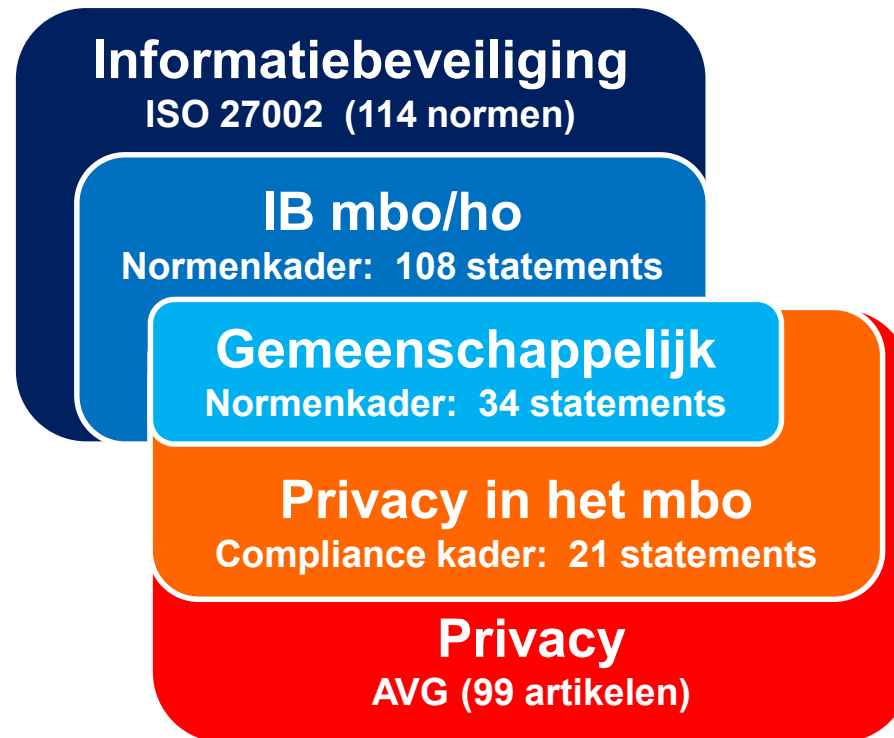
Spreadsheet

| | A | B | C | D | F | G |
|----|---|------------------|--|---|--|---|
| 1 | Cluster 1: Beleid en organisatie | | | | | |
| 2 | | | | | 1 Niveau 1: Adhoc | De onderwijsinstelling kan de beheersmaatregel op volgende manier aantonen: 1. D.m.v. een vastgesteld document OF een ondertekend gespreksverslag waarin de procedure/methode wordt toegelicht. De proceseigenaar en de auditor ondertekenen het verslag. 2. De werking wordt getoetst door waarneming terplaatse en/of aanvullende vragen aan medewerkers. |
| 3 | | | | | 2 Niveau 2: Opzet, bestaan en beperkte werking | |
| 4 | | | | | 3 Niveau 3: Werking | |
| 5 | | | | | 4 Niveau 4: PDCA-cyclus | |
| 6 | | | | | 5 Niveau 5: Externe goedkeurende verklaring | |
| 7 | Nr. | ISO 27002 | Cluster 1: Beleid en organisatie <small>(tekst conform beheersmaatregel ISO 27002:2013)</small> | Toelichting | Bewijsvoering op niveau 2 en 3 | Gehanteerd document |
| 8 | 1.1 AVG | 5.1.1 | Beleidsregels voor informatiebeveiliging Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd en goedgekeurd door het College van Bestuur. | Er is beleid voor informatiebeveiliging door het College van Bestuur vastgesteld, op basis van inzicht in risico's, kritieke bedrijfsprocessen en toewijzing van verantwoordelijkheden en uitgangspunten. Dit beleid is goedgekeurd door de OR van de mbo instelling en wordt gedeeld met alle betrokken en externe partijen. Privacy toets: Hanteer als uitgangspunt het model Informatiebeveiliging en Privacy Beleid. Indien gebruik wordt gemaakt van een eigen beleidsplan controleer dan de volgende onderdelen op aanwezigheid en juistheid: 1. Verantwoording 2. Compliance 3. Governance Bijlage 1: Ondersteunende documenten en richtlijnen | Inhoudsopgave IBP-beleid: 1. Verantwoording 2. Compliance 3. Governance 4. Afhandelen van informatiebeveiligingsincidenten en datalekken Bijlage: Ondersteunende documenten en richtlijnen 2 Overleg het IBP-beleid, voorzien van versiebeheer, dat goedgekeurd is door het CvB en de OR. 3 Overleg een printscreen van een intranetpagina waar een link staat naar het IBP-beleid. | Model Informatiebeveiligings- en Privacy-beleid voor de mbo sector (IBPDO6) |
| 10 | 1.2 | 5.1.1.2 | <i>Vervolgzie 1.1 (5.1.1)</i> | | | |
| 12 | 1.3 | 5.1.2 | Beoordeling van het informatiebeveiligingsbeleid Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is. | Het IBP-beleid wordt minimaal één keer per jaar, of zodra zich belangrijke wijzigingen voordoen, beoordeeld en zo nodig bijgesteld. Belangrijke wijzigingen zijn bijvoorbeeld een (de)fusie of samenwerking met nieuwe ICT-dienstenleverancier. Het functioneren van de informatiebeveiliging wordt jaarlijks gerapporteerd aan het bestuur en de OR. | Het IBP-beleid is onderdeel van de jaarplancyclus. 2 Overleg een IBP-beleid, voorzien van versiebeheer, dat goedgekeurd is door het CvB en de OR. 3 Overleg een document waaruit blijkt dat het IBP-beleid in het vorige jaar is geëvalueerd. | Model Informatiebeveiligings- en Privacy-beleid voor de mbo sector (IBPDO6) |
| 15 | 1.4 | 6.1.1 | Taken en verantwoordelijkheden informatiebeveiliging Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen. | Alle verantwoordelijkheden voor informatiebeveiliging behoren duidelijk te zijn gedefinieerd en gedocumenteerd als onderdeel van het IBP-beleid. Toewijzing vindt plaats in overeenstemming met het beleid. Verantwoordelijkheden worden waar nodig aangevuld met meer gedetailleerde besluiten. Bevoegdheden zijn duidelijk gedefinieerd en gedocumenteerd. | Het IBP-beleid bevat het hoofdstuk Governance, waar alle functies en rollen duidelijk zijn beschreven, bijvoorbeeld aan de hand van het 3-lines of defence model. 2 Overleg het IBP-beleid met daarin opgenomen het hoofdstuk Governance, waar alle functies en rollen duidelijk zijn beschreven. 3 Overleg een ingevulde lijst met namen met functies en rollen. Check middels interviews of de aangewezen medewerkers hun taken op basis van hun rol daadwerkelijk uitvoeren. | Model Informatiebeveiligings- en Privacy-beleid voor de mbo sector (IBPDO6) |
| 18 | 1.5 | 6.1.5 | Informatiebeveiliging in projectbeheer Informatiebeveiliging behoort aan de orde te komen in projectbeheer, ongeacht het soort project. | Informatiebeveiliging moet geïntegreerd zijn in alle projecten (niet alleen ICT) van de organisatie om ervoor te zorgen dat informatiebeveiligingsrisico's, indien mogelijk, worden geïdentificeerd en aangepakt als deel van een project. Dit geldt in het algemeen voor elk project ongeacht het karakter, bijv. een project voor een proces voor kernactiviteiten, ICT, 'facility management' en andere ondersteunende processen. | Neem IBP als hoofdstuk op in projectdocumentatie en als agendapunt bij projectvergaderingen. Informatiebeveiliging en Privacy in projectbeheer wordt getoetst d.m.v. respectievelijk een BIV-classificatie en een DPIA. 2 Overleg het gehanteerde format DPIA met de daarin gestelde eisen ten aanzien van informatiebeveiliging en het format BIV classificatie. 3 Overleg een overzicht van uitgevoerde DPIA's inclusief BIV-classificaties. 3 Overleg een overzicht van niet uitgevoerde DPIA's met opgave van reden. | Handleiding uitvoeren Data Protection Impact Assessment (DPIA) (IBPDO38) |

Update toetsingskader Privacy

- Aanpassingen WBP > AVG
- Beschrijvingen statements en bewijslast
- Spreadsheet

Overlappende statements



Overlappende statements

Extra aandacht Privacy in IB cluster:

1. 9 van de 21 statements
2. 5 van de 7 statements
3. 2 van de 15 statements
4. 2 van de 15 statements
5. 12 van de 17 statements
6. 4 van de 10 statements

2.2

7.2.2

Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging: Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.

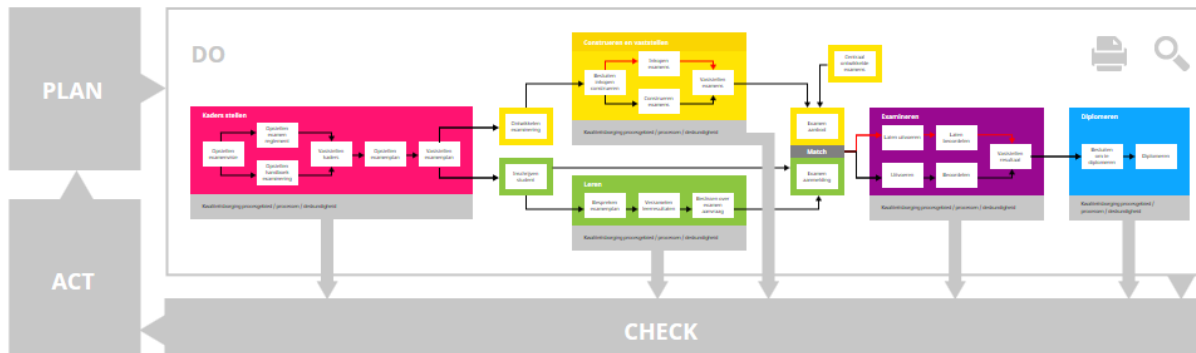
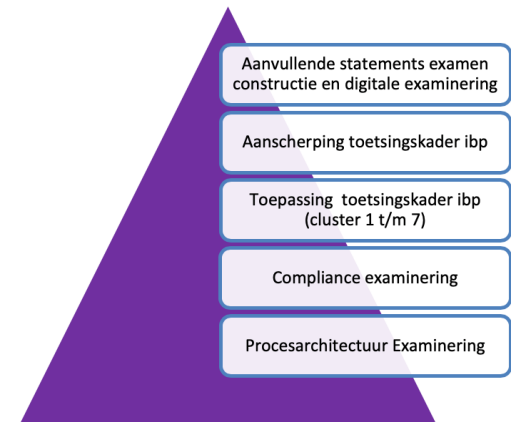
Privacy toets: hetzelfde geldt voor opleiding en training ten aanzien van privacy.

Update toetsingskader Privacy

| Nr. | Statement |
|------|---|
| P.1 | Privacy-beleid |
| P.2 | Functionaris gegevensbescherming |
| P.3 | Rechtmatige verwerking van persoonsgegevens |
| P.4 | Register van verwerkingsactiviteiten (dataregister) |
| P.5 | Bewaartermijnen |
| P.6 | Verwerking t.b.v. onderzoek |
| P.7 | Verwerking van bijzondere persoonsgegevens |
| P.8 | Geautomatiseerde besluitvorming |
| P.9 | Informatiebeveiliging |
| P.10 | Verwerkersovereenkomsten |
| P.11 | Transparant over privacy |
| P.12 | Informereren over verwerkingen |
| P.13 | Procedures rechten van de betrokkenen |
| P.14 | Geheimhouding |
| P.15 | Bewustzijn, opleiding en training ten aanzien van privacy |
| P.16 | Bewijs van vernietiging persoonsgegevens |
| P.17 | Dataclassificatie |
| P.18 | Datalekken en beveiligingsincidenten |
| P.19 | Vervallen, zie P.7, P.9 en P.17 |
| P.20 | Privacy by design en privacy by default |
| P.21 | Data Protection Impact Assessment (DPIA) |
| P.22 | Controle naleving beleid |
| P.23 | Vervallen, zie P.2, P.11, P.12, P.18 en IB1.18 |
| P.24 | Vervallen, zie IB6.2 |

Update toetsingskader Examinering

- Verwerken feedback werkveld
- Beter in lijn met PE



Overlappende statements

Extra aandacht Examinering in IB cluster:

1. 6 van de 21 statements
2. 3 van de 7 statements
3. 2 van de 15 statements
4. 2 van de 15 statements
5. 4 van de 17 statements
6. 3 van de 10 statements

1.16

15.1.3

Toeleveringsketen van informatie- en communicatietechnologie

Overeenkomsten met leveranciers behoren eisen te bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.

Toelichting examineren:

Door toenemende inkoop van examens is het van belang om de beveiliging van deze informatie(keten) en, indien van toepassing, de privacyaspecten te waarborgen in de vorm van een (verwerkers)overeenkomst, met speciale focus op de beveiligingsparagraaf.

Update toetsingskader Examinering

| Nr. | Statement |
|------|---|
| E.1 | Beleidsplan beveiliging examinering |
| E.2 | Gedragscodes en richtlijnen afname examens |
| E.3 | Trainingen en vaardigheden m.b.t. richtlijnen |
| E.4 | Continuïteitsplan |
| E.5 | Archiveren en vernietigen examenmateriaal |
| E.6 | Richtlijn inkoop, construeren en vaststellen examens in een beveiligde omgeving |
| E.7 | Richtlijnen bij constatering van onregelmatigheden die tot fraude kunnen leiden bij examens |
| E.8 | Voorkomen van examenfraude |
| E.9 | Procedure voorbereiden en afnemen examens |
| E.10 | Extra ondersteuning bij (digitale) examens |
| E.11 | Beveiligde examenruimtes |
| E.12 | Het beheren en documenteren van ict-faciliteiten voor examinering |
| E.13 | Hanteren van digitaal examenmateriaal |
| E.14 | Toewijzen examens aan studenten |
| E.15 | Kopieerbeveiliging examenvragen i.v.m. mogelijk hergebruik |
| E.16 | Vorbereiden op vaststellen diplomabesluit door de examencommissie |
| E.17 | Borgen dat diploma en overige waardedocumenten rechtmatig, veilig en correct worden aangemaakt en afgedrukt |
| E.18 | Eindevaluatie examenproces en de integriteit van de resultaten |

Framework ibp in het mbo



ibp in het mbo

achtergrond

- Toetsingskaders Informatiebeveiliging**
- Spreadsheet toetsingskaders (IBPDOc40)
- Toetsingskader informatiebeveiliging (IBPDOc3)
- Toetsingskader Privacy (IBPDOc7)
- Toetsingskader Examinering (IBPDOc8)

Aan de slag met de Benchmark

Kick-off: 3 oktober 2019,
aansluitend training toetsingskaders

Deadline: 15 november 2019

Presentatie: 12 december 2019



Bedankt voor uw aandacht

Martijn Bijleveld, Leo Bakker, Kennisnet

E-mail: m.bijleveld@kennisnet.nl