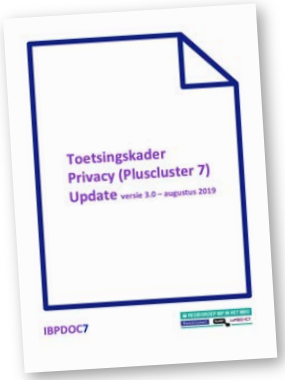
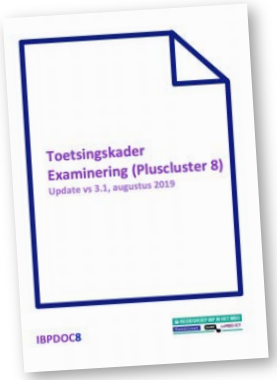
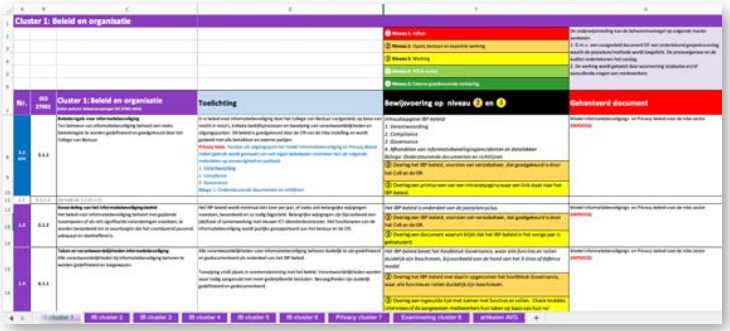
Toetsingskaders IB, P en E

in vogelvlucht door de statements







Wat is er nieuw

- Informatiebeveiliging
- ISO 27002 helemaal afdekken
- Nieuwe vormen van bewijsvoering

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

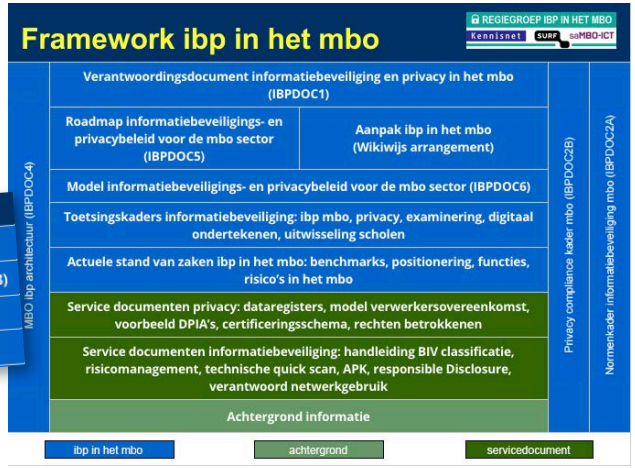
- Examinering
- Verwerken feedback werkveld
- Beter in lijn met PE

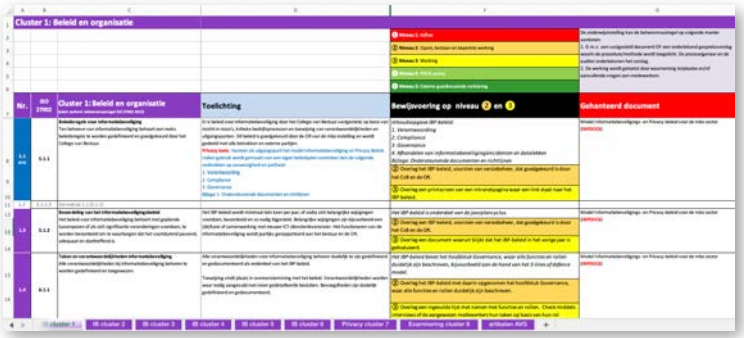
Update toetsingskader IB

- Nieuwe statements (van 85 > 108)
- Bewijslast
  - documenten
  - interview
  - waarneming ter plaatse
  - re-performance
- Beschrijving volwassenheidsniveau's
  - niveau 2 en 3 beschreven
  - niveau 4: pdca
  - niveau 5: externe audit

Framework IBP

- Via saMBO-ICT.nl > netwerken > IBP





NETWERK IBP IN HET MBO
Kennisnet SURF saMBO-ICT

Cluster 1: Beleid en organisatie

Nr.	ISO27002	Statement	
1.1	5.1.1	Beleidsregels voor informatiebeveiliging	P
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	P
1.7	8.2.1	Classificatie van informatie	P
1.8	8.2.2	Informatie labelen	P
1.9	10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	P-E
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	P-E
1.16	15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	E
1.17	16.1.1	Verantwoordelijkheden en procedures.	E
1.18	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	P-E
1.19	18.1.3	Beschermen van registraties	P-E
1.20	18.1.4	Privacy en bescherming van persoonsgegevens	P
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	18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	

NETWERK IBP IN HET MBO
Kennisnet SURF saMBO-ICT

Cluster 2: Personeel, studenten en gasten

2.1	7.1.2	Arbeidsvoorwaarden	P
2.2	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	P
2.3	9.2.6	Toegangsrechten intrekken of aanpassen	P-E
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	P-E
2.5	13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	P
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)	E
2.9	7.1.3	Disciplinaire procedure	
2.10	7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	

Cluster 3: Ruimtes en apparatuur

3.1	vervallen	Zie nr 1.6 (6.2.1)	
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	E
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	P
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	E

Cluster 4: Continuïteit

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	P
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	E
4.14	17.1.2	Informatiebeveiligingscontinuïteit implementeren	P
4.15	17.2.1	Beschikbaarheid van informatie verwerkende faciliteiten	E

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	

Cluster 5: Toegangsbeveiliging

5.1	9.1.1	Beleid voor toegangsbeveiliging	P
5.2	9.1.2	Toegang tot netwerken en netwerkdiensten	P-E
5.3	9.2.1	Registratie en afmelden van gebruikers	P-E
5.4	9.2.2	Gebruikers toegang verlenen	P
5.5	9.2.3	Beheren van speciale toegangsrechten	P
5.6	9.2.4	Beheer van geheime authenticatie-informatie van gebruikers	P
5.7	9.3.1	Geheime authenticatie-informatie gebruiken	P
5.8	9.4.1	Beperking toegang tot informatie	P
5.9	9.4.2	Beveiligde inlogprocedures	P-E
5.10	10.1.2	Sleutelbeheer	P
5.11	vervallen	Zie nr 5.10 (10.1.2)	
5.12	12.4.2	Beschermen van informatie in logbestanden	P-E
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	P
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)	

NETWERK IBP IN HET MBO
Kennisnet SURF saMBO-ICT

Cluster 6: Controle en logging

6.1	9.2.5	Beoordeling van toegangsrechten van gebruikers	P-E
6.2	12.4.1	Gebeurtenissen registreren	P-E
6.3	12.4.3	Logbestanden van beheerders en operators	E
6.4	14.2.7	Uitbestede softwareontwikkeling	
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	P
6.10	18.2.3	Beoordeling van technische naleving	P

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	

Update toetsingskader Privacy

- Aanpassingen WBP > AVG
- Beschrijvingen statements en bewijslast

Update toetsingskader Privacy

- Overlappende statements met IB

1.1	5.1.1	Beleidsregels voor informatiebeveiliging	P
1.6	6.2.1	Beleid voor mobiele apparatuur	P
1.7	8.2.1	Classificatie van informatie	P
1.8	8.2.2	Informatie labelen	P
1.9	10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	P-E
1.15	15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	P-E
1.18	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	P-E
1.19	18.1.3	Beschermen van registraties	P-E
1.20	18.1.4	Privacy en bescherming van persoonsgegevens	P
2.1	7.1.2	Arbeidsvoorwaarden	P
2.2	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	P
2.3	9.2.6	Toegangsrechten intrekken of aanpassen	P-E
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	P-E
2.5	13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	P
3.14	11.2.7	Veilig verwijderen of hergebruiken van apparatuur	P

4.5	12.3.1	Back-up van informatie	P
4.14	17.1.2	Informatiebeveiligingscontinuïteit implementeren	P
5.1	9.1.1	Beleid voor toegangsbeveiliging	P
5.2	9.1.2	Toegang tot netwerken en netwerkdiensten	P-E
5.3	9.2.1	Registratie en afmelden van gebruikers	P-E
5.4	9.2.2	Gebruikers toegang verlenen	P
5.5	9.2.3	Beheren van speciale toegangsrechten	P
5.6	9.2.4	Beheer van geheime authenticatie-informatie van gebruikers	P
5.7	9.3.1	Geheime authenticatie-informatie gebruiken	P
5.8	9.4.1	Beperking toegang tot informatie	P
5.9	9.4.2	Beveiligde inlogprocedures	P-E
5.10	10.1.2	Sleutelbeheer	P
5.12	12.4.2	Beschermen van informatie in logbestanden	P-E
5.16	13.2.3	Elektronische berichten	P
6.1	9.2.5	Beoordeling van toegangsrechten van gebruikers	P-E
6.2	12.4.1	Gebeurtenissen registreren	P-E
6.9	18.2.2	Naleving van beveiligingsbeleid en –normen	P
6.10	18.2.3	Beoordeling van technische naleving	P

NETWERK IBP IN HET MBO
Kennisnet SURF saMBO-ICT

Update toetsingskader Privacy

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	Informeren 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

Update toetsingskader Examinering

- Overlappende statements met IB

Nr.	ISO27002	Statement	
1.9	10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	P-E
1.15	15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	P-E
1.16	15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	E
1.17	16.1.1	Verantwoordelijkheden en procedures.	E
1.18	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	P-E
1.19	18.1.3	Beschermen van registraties	P-E
2.3	9.2.6	Toegangsrechten intrekken of aanpassen	P-E
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	P-E
2.8	6.2.2	Telewerken (thuiswerken)	E
3.5	11.1.3	Kantoren, ruimten en faciliteiten beveiligen	E
3.21	8.3.3	Media fysiek overdragen	E
4.13	16.1.5	Respons op informatiebeveiligingsincidenten	E
4.15	17.2.1	Beschikbaarheid van informatie verwerkende faciliteiten	E
5.2	9.1.2	Toegang tot netwerken en netwerkdiensten	P-E
5.3	9.2.1	Registratie en afmelden van gebruikers	P-E
5.9	9.4.2	Beveiligde inlogprocedures	P-E
5.12	12.4.2	Beschermen van informatie in logbestanden	P-E
6.1	9.2.5	Beoordeling van toegangsrechten van gebruikers	P-E
6.2	12.4.1	Gebeurtenissen registreren	P-E
6.3	12.4.3	Logbestanden van beheerders en operators	E

Update toetsingskader Examinering

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	Voorbereiden 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

Aan de slag met de Benchmark!

Deadline: 15 november 2019

Presentatie: 12 december 2019