NETWERK IBP IN HET MBO
Kennisnet SURF saMBO-ICT

Benchmark IBP/E in het mbo 2019

Met dank aan jullie allen!

En in het bijzonder:

- Co Klerkx (ROC van Amsterdam/Flevoland)
- Marjolein Rombouts (MBO Utrecht)
- Martijn van Hoorn (Citaverde College)
- Martin Deiman (Aeres)
- Rene Dol (Deltion College)
- Theo Kuilboer (ROC Top)
- Willem Flink (Hoornbeeck College)

➢ Ludo Cuijpers

NETWERK IBP IN HET MBO
Kennisnet SURF saMBO-ICT

Benchmark IBP/E in het mbo 2019

- Update toetsingskader IB
  - 31 nieuwe statements
  - bewijslast
  - beschrijving volwassenheidsniveaus
- Update toetsingskader Privacy
  - Aanpassingen WBP > AVG
  - Beschrijvingen statements en bewijslast
- Update toetsingskader Examinering
  - Beschrijving statements en bewijslast
  - Beter in lijn met PE

NETWERK IBP IN HET MBO
Kennisnet SURF saMBO-ICT

Eindresultaat Benchmark IBP/E 2019

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

NETWERK IBP IN HET MBO

Kennisnet SURF saMBO-ICT

Informatiebeveiliging 2,5

aantal deelnemers informatiebeveiliging: 56

Nr.	ISO27002	Statement		Niveau 1 t/m 5	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5
1.1	5.1.1	Beleidsregels voor informatiebeveiliging	P	3,1	0	8	34	14	0
1.6	6.2.1	Beleid voor mobiele apparatuur	P	2,5	8	18	22	8	0
1.7	8.2.1	Classificatie van informatie	P	2,5	6	24	18	8	0
1.8	8.2.2	Informatie labelen	P	2,3	14	15	22	5	0
1.9	10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	P-E	2,3	10	23	18	5	0
1.15	15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	P-E	2,6	6	19	26	4	1
1.16	15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	E	3,1	0	5	41	10	0
1.17	16.1.1	Verantwoordelijkheden en procedures.	E	3,0	0	13	32	11	0
1.18	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	P-E	2,9	2	14	28	12	0
1.19	18.1.3	Beschermen van registraties	P-E	2,1	5	42	9	0	0
1.20	18.1.4	Privacy en bescherming van persoonsgegevens	P	3,1	0	7	37	12	0
		Gemiddelde cluster 1		2,6					
2.1	7.1.2	Arbeidsvoorwaarden	P	2,3	13	16	24	3	0
2.2	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	P	2,2	5	35	15	1	0
2.3	9.2.6	Toegangsrechten intrekken of aanpassen	P-E	2,7	7	15	25	8	1
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	P-E	2,0	10	35			
2.5	13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	P	2,5	9	18			
2.8	6.2.2	Telewerken (thuiswerken)	E	1,7	29	15			
		Gemiddelde cluster 2		2,3					
3.5	11.1.3	Kantoren, ruimten en faciliteiten beveiligen	E	2,4	8	20			
3.14	11.2.7	Veilig verwijderen of hergebruiken van apparatuur	P	2,7	7	13			
3.21	8.3.3	Media fysiek overdragen	E	2,2	13	22			
		Gemiddelde cluster 3		2,6					
4.5	12.3.1	Back-up van informatie	P	3,2	1	8			
4.13	16.1.5	Respons op informatiebeveiligingsincidenten	E	3,1	3	5			
4.14	17.1.2	Informatiebeveiligingscontinuïteit implementeren	P	2,0	16	25			
4.15	17.2.1	Beschikbaarheid van informatie verwerkende faciliteiten	E	2,5	6	22			
		Gemiddelde cluster 4		2,6					
5.1	9.1.1	Beleid voor toegangsbeveiliging	P	2,4	9	17			
5.2	9.1.2	Toegang tot netwerken en netwerkdiensten	P-E	2,5	9	16			
5.3	9.2.1	Registratie en afmelden van gebruikers	P-E	2,6	9	17			
5.4	9.2.2	Gebruikers toegang verlenen	P	2,6	9	13			
5.5	9.2.3	Beheren van speciale toegangsrechten	P	2,4	11	17			
5.6	9.2.4	Beheer van geheime authenticatie-informatie van gebruikers	P	2,6	8	17			
5.7	9.3.1	Geheime authenticatie-informatie gebruiken	P	2,5	8	15			
5.8	9.4.1	Beperking toegang tot informatie	P	2,4	9	20			
5.9	9.4.2	Beveiligde inlogprocedures	P-E	2,5	7	21			
5.10	10.1.2	Sleutelbeheer	P	2,2	15	18			
5.12	12.4.2	Beschermen van informatie in logbestanden	P-E	2,0	20	19	14	3	0
5.16	13.2.3	Elektronische berichten	P	2,1	16	20	19	1	0
		Gemiddelde cluster 5		2,4					
6.1	9.2.5	Beoordeling van toegangsrechten van gebruikers	P-E	2,1	13	30	10	3	0
6.2	12.4.1	Gebeurtenissen registreren	P-E	2,0	16	26	12	2	0
6.3	12.4.3	Logbestanden van beheerders en operators	E	1,8	22	24	8	2	0
6.9	18.2.2	Naleving van beveiligingsbeleid en –normen	P	1,8	19	29	8	0	0
6.10	18.2.3	Beoordeling van technische naleving	P	2,3	12	24	14	5	1
		Gemiddelde cluster 6		2,1					

	2019
Cluster 1: Beleid en organisatie	2,6
Cluster 2: Personeel, studenten en gasten	2,3
Cluster 3: Ruimtes en apparatuur	2,6
Cluster 4: Continuïteit	2,6
Cluster 5: Vertrouwelijkheid en integriteit	2,4
Cluster 6: Controle en Logging	2,1
Totaal Informatiebeveiliging	2,5

NETWERK IBP IN HET MBO

Kennisnet SURF saMBO-ICT

1. Beleid en organisatie

Informatiebeveiliging				2,5		Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5
aantal deelnemers informatiebeveiliging: 56										
Nr.	ISO27002	Statement		Niveau 1 t/m 5						
1.1	5.1.1	Beleidsregels voor informatiebeveiliging	P	3,1		0	8	34	14	0
1.6	6.2.1	Beleid voor mobiele apparatuur	P	2,5		8	18	22	8	0
1.7	8.2.1	Classificatie van informatie	P	2,5		6	24	18	8	0
1.8	8.2.2	Informatie labelen	P	2,3		14	15	22	5	0
1.9	10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	P-E	2,3		10	23	18	5	0
1.15	15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	P-E	2,6		6	19	26	4	1
1.16	15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	E	3,1		0	5	41	10	0
1.17	16.1.1	Verantwoordelijkheden en procedures.	E	3,0		0	13	32	11	0
1.18	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	P-E	2,9		2	14	28	12	0
1.19	18.1.3	Beschermen van registraties	P-E	2,1		5	42	9	0	0
1.20	18.1.4	Privacy en bescherming van persoonsgegevens	P	3,1		0	7	37	12	0
		Gemiddelde cluster 1		2,6						
5.10	10.1.2	Sleutelbeheer	P	2,2		15	18	21	2	0
5.12	12.4.2	Beschermen van informatie in logbestanden	P-E	2,0		20	19	14	3	0
5.16	13.2.3	Elektronische berichten	P	2,1		16	20	19	1	0
		Gemiddelde cluster 5		2,4						
6.1	9.2.5	Beoordeling van toegangsrechten van gebruikers	P-E	2,1		13	30	10	3	0
6.2	12.4.1	Gebeurtenissen registreren	P-E	2,0		16	26	12	2	0
6.3	12.4.3	Logbestanden van beheerders en operators	E	1,8		22	24	8	2	0
6.9	18.2.2	Naleving van beveiligingsbeleid en –normen	P	1,8		19	29	8	0	0
6.10	18.2.3	Beoordeling van technische naleving	P	2,3		12	24	14	5	1
		Gemiddelde cluster 6		2,1						

1.1	5.1.1	Beleidsregels voor informatiebeveiliging	P	3,1		0	8	34	14	0
1.6	6.2.1	Beleid voor mobiele apparatuur	P	2,5		8	18	22	8	0
1.7	8.2.1	Classificatie van informatie	P	2,5		6	24	18	8	0
1.8	8.2.2	Informatie labelen	P	2,3		14	15	22	5	0
1.9	10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	P-E	2,3		10	23	18	5	0
1.15	15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	P-E	2,6		6	19	26	4	1
1.16	15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	E	3,1		0	5	41	10	0
1.17	16.1.1	Verantwoordelijkheden en procedures.	E	3,0		0	13	32	11	0
1.18	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	P-E	2,9		2	14	28	12	0
1.19	18.1.3	Beschermen van registraties	P-E	2,1		5	42	9	0	0
1.20	18.1.4	Privacy en bescherming van persoonsgegevens	P	3,1		0	7	37	12	0
		Gemiddelde cluster 1		2,6						

NETWERK IBP IN HET MBO

Kennisnet SURF saMBO-ICT

2. Personeel, studenten en gasten

Informatiebeveiliging — 2,5

aantal deelnemers informatiebeveiliging: 56

Nr.	ISO27002	Statement		Niveau 1 t/m 5	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5
1.1	5.1.1	Beleidsregels voor informatiebeveiliging	P	3,1	0	8	34	14	0
1.6	6.2.1	Beleid voor mobiele apparatuur	P	2,5	8	18	22	8	0
1.7	8.2.1	Classificatie van informatie	P	2,5	6	24	18	8	0
1.8	8.2.2	Informatie labelen	P	2,3	14	15	22	5	0
1.9	10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	P-E	2,3	10	23	18	5	0
1.15	15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	P-E	2,6	6	19	26	4	1
1.16	15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	E	3,1	0	5	41	10	0
1.17	16.1.1	Verantwoordelijkheden en procedures.	E	3,0	0	13	32	11	0
1.18	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	P-E	2,9	2	14	28	12	0
1.19	18.1.3	Beschermen van registraties	P-E	2,1	5	42	9	0	0
1.20	18.1.4	Privacy en bescherming van persoonsgegevens	P	3,1	0	7	37	12	0
		Gemiddelde cluster 1		2,6					
2.1	7.1.2	Arbeidsvoorwaarden	P	2,3	13	16	24	3	0
2.2	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	P	2,2	5	35	15	1	0
2.3	9.2.6	Toegangsrechten intrekken of aanpassen	P-E	2,7	7	15	25	8	1
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	P-E	2,0	10	35	11	0	0
2.5	13.2.4	Ve							
2.8	6.2.2	Te							
3.5	11.1.3	Ka							
3.14	11.2.7	Ve							
3.21	8.3.3	M							
4.5	12.3.1	Ba							
4.13	16.1.5	Re							
4.14	17.1.2	In							
4.15	17.2.1	Be							
5.1	9.1.1	Be							
5.2	9.1.2	Toegang tot netwerken en netwerkdiensten	P-E	2,5	9	16	27	4	0
5.3	9.2.1	Registratie en afmelden van gebruikers	P-E	2,6	9	17	20	9	1
5.4	9.2.2	Gebruikers toegang verlenen	P	2,6	9	13	24	9	1
5.5	9.2.3	Beheren van speciale toegangsrechten	P	2,4	11	17	20	8	0
5.6	9.2.4	Beheer van geheime authenticatie-informatie van gebruikers	P	2,6	8	17	22	9	0
5.7	9.3.1	Geheime authenticatie-informatie gebruiken	P	2,5	8	15	28	5	0
5.8	9.4.1	Beperking toegang tot informatie	P	2,4	9	20	25	2	0
5.9	9.4.2	Beveiligde inlogprocedures	P-E	2,5	7	21	23	4	1
5.10	10.1.2	Sleutelbeheer	P	2,2	15	18	21	2	0
5.12	12.4.2	Beschermen van informatie in logbestanden	P-E	2,0	20	19	14	3	0
5.16	13.2.3	Elektronische berichten	P	2,1	16	20	19	1	0
		Gemiddelde cluster 5		2,4					
6.1	9.2.5	Beoordeling van toegangsrechten van gebruikers	P-E	2,1	13	30	10	3	0
6.2	12.4.1	Gebeurtenissen registreren	P-E	2,0	16	26	12	2	0
6.3	12.4.3	Logbestanden van beheerders en operators	E	1,8	22	24	8	2	0
6.9	18.2.2	Naleving van beveiligingsbeleid en –normen	P	1,8	19	29	8	0	0
6.10	18.2.3	Beoordeling van technische naleving	P	2,3	12	24	14	5	1
		Gemiddelde cluster 6		2,1					

2.1	7.1.2	Arbeidsvoorwaarden	P	2,3	13	16	24	3	0
2.2	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	P	2,2	5	35	15	1	0
2.3	9.2.6	Toegangsrechten intrekken of aanpassen	P-E	2,7	7	15	25	8	1
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	P-E	2,0	10	35	11	0	0
2.5	13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	P	2,5	9	18	19	10	0
2.8	6.2.2	Telewerken (thuiswerken)	E	1,7	29	15	10	2	0
		Gemiddelde cluster 2		2,3					

NETWERK IBP IN HET MBO

Kennisnet SURF saMBO-ICT

Informatiebeveiliging

Nr.	ISO27002	Statement		Niveau 1 t/m 5 (totaal: 2,5)	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5
		aantal deelnemers informatiebeveiliging: 56							
1.1	5.1.1	Beleidsregels voor informatiebeveiliging	P	3,1	0	8	34	14	0
1.6	6.2.1	Beleid voor mobiele apparatuur	P	2,5	8	18	22	8	0
1.7	8.2.1	Classificatie van informatie	P	2,5	6	24	18	8	0
1.8	8.2.2	Informatie labelen	P	2,3	14	15	22	5	0
1.9	10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	P-E	2,3	10	23	18	5	0
1.15	15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	P-E	2,6	6	19	26	4	1
1.16	15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	E	3,1	0	5	41	10	0
1.17	16.1.1	Verantwoordelijkheden en procedures.	E	3,0	0	13	32	11	0
1.18	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	P-E	2,9	2	14	28	12	0
1.19	18.1.3	Beschermen van registraties	P-E	2,1	5	42	9	0	0
1.20	18.1.4	Privacy en bescherming van persoonsgegevens	P	3,1	0	7	37	12	0
		Gemiddelde cluster 1		2,6					
2.1	7.1.2	Arbeidsvoorwaarden	P	2,3	13	16	24	3	0
2.2	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	P	2,2	5	35	15	1	0
2.3	9.2.6	Toegangsrechten intrekken of aanpassen	P-E	2,7	7	15	25	8	1
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	P-E	2,0	10	35	11	0	0
2.5	13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	P	2,5	9	18	19	10	0
2.8	6.2.2	Telewerken (thuiswerken)	E	1,7	29	15	10	2	0
		Gemiddelde cluster 2		2,3					
3.5	11.1.3	Kantoren, ruimten en faciliteiten beveiligen	E	2,4	8	20	26	2	0
3.14	11.2.7	Veilig verwijderen of hergebruiken van apparatuur	P	2,7	7	13	27	8	1
3.21	8.3.3	Media fysiek overdragen	E	2,2	13	22	17	4	0
		Gemiddelde cluster 3		2,6					
4.5	12.3.1	Back-up van informatie	P	3,2	1	8	30	15	2
4.13	16.1.5								
4.14	17.1.2								
4.15	17.2.1								
5.1	9.1.1								
5.2	9.1.2								
5.3	9.2.1								
5.4	9.2.2								
5.5	9.2.3	Beheren van speciale toegangsrechten	P	2,4	11	17	20	8	0
5.6	9.2.4	Beheer van geheime authenticatie-informatie van gebruikers	P	2,6	8	17	22	9	0
5.7	9.3.1	Geheime authenticatie-informatie gebruiken	P	2,5	8	15	28	5	0
5.8	9.4.1	Beperking toegang tot informatie	P	2,4	9	20	25	2	0
5.9	9.4.2	Beveiligde inlogprocedures	P-E	2,5	7	21	23	4	1
5.10	10.1.2	Sleutelbeheer	P	2,2	15	18	21	2	0
5.12	12.4.2	Beschermen van informatie in logbestanden	P-E	2,0	20	19	14	3	0
5.16	13.2.3	Elektronische berichten	P	2,1	16	20	19	1	0
		Gemiddelde cluster 5		2,4					
6.1	9.2.5	Beoordeling van toegangsrechten van gebruikers	P-E	2,1	13	30	10	3	0
6.2	12.4.1	Gebeurtenissen registreren	P-E	2,0	16	26	12	2	0
6.3	12.4.3	Logbestanden van beheerders en operators	E	1,8	22	24	8	2	0
6.9	18.2.2	Naleving van beveiligingsbeleid en –normen	P	1,8	19	29	8	0	0
6.10	18.2.3	Beoordeling van technische naleving	P	2,3	12	24	14	5	1
		Gemiddelde cluster 6		2,1					

3. Ruimtes en apparatuur

3.5	11.1.3	Kantoren, ruimten en faciliteiten beveiligen	E	2,4	8	20	26	2	0
3.14	11.2.7	Veilig verwijderen of hergebruiken van apparatuur	P	2,7	7	13	27	8	1
3.21	8.3.3	Media fysiek overdragen	E	2,2	13	22	17	4	0
		Gemiddelde cluster 3		2,6					

NETWERK IBP IN HET MBO

Kennisnet SURF saMBO-ICT

Informatiebeveiliging 2,5

aantal deelnemers informatiebeveiliging: 56

Nr.	ISO27002	Statement		Niveau 1 t/m 5	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5
1.1	5.1.1	Beleidsregels voor informatiebeveiliging	P	3,1	0	8	34	14	0
1.6	6.2.1	Beleid voor mobiele apparatuur	P	2,5	8	18	22	8	0
1.7	8.2.1	Classificatie van informatie	P	2,5	6	24	18	8	0
1.8	8.2.2	Informatie labelen	P	2,3	14	15	22	5	0
1.9	10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	P-E	2,3	10	23	18	5	0
1.15	15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	P-E	2,6	6	19	26	4	1
1.16	15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	E	3,1	0	5	41	10	0
1.17	16.1.1	Verantwoordelijkheden en procedures.	E	3,0	0	13	32	11	0
1.18	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	P-E	2,9	2	14	28	12	0
1.19	18.1.3	Beschermen van registraties	P-E	2,1	5	42	9	0	0
1.20	18.1.4	Privacy en bescherming van persoonsgegevens	P	3,1	0	7	37	12	0
		Gemiddelde cluster 1		2,6					
2.1	7.1.2	Arbeidsvoorwaarden	P	2,3	13	16	24	3	0
2.2	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	P	2,2	5	35	15	1	0
2.3	9.2.6	Toegangsrechten intrekken of aanpassen	P-E	2,7	7	15	25	8	1
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	P-E	2,0	10	35	11	0	0
2.5	13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	P	2,5	9	18	19	10	0
2.8	6.2.2	Telewerken (thuiswerken)	E	1,7	29	15	10	2	0
		Gemiddelde cluster 2		2,3					
3.5	11.1.3	Kantoren, ruimten en faciliteiten beveiligen	E	2,4	8	20	26	2	0
3.14	11.2.7	Veilig verwijderen of hergebruiken van apparatuur	P	2,7	7	13	27	8	1
3.21	8.3.3	Media fysiek overdragen	E	2,2	13	22	17	4	0
		Gemiddelde cluster 3		2,6					
4.5	12.3.1	Back-up van informatie	P	3,2	1	8	30	15	2
4.13	16.1.5	Respons op informatiebeveiligingsincidenten	E	3,1	3	5	33	14	1
4.14	17.1.2	Informatiebeveiligingscontinuïteit implementeren	P	2,0	16	25	12	3	0
4.15	17.2								
5.1	9.1								
5.2	9.1								
5.3	9.2								
5.4	9.2								
5.5	9.2								
5.6	9.2								
5.7	9.3								
5.8	9.4								
5.9	9.4								
5.10	10.1.2	Sleutelbeheer	P	2,2	15	18	21	2	0
5.12	12.4.2	Beschermen van informatie in logbestanden	P-E	2,0	20	19	14	3	0
5.16	13.2.3	Elektronische berichten	P	2,1	16	20	19	1	0
		Gemiddelde cluster 5		2,4					
6.1	9.2.5	Beoordeling van toegangsrechten van gebruikers	P-E	2,1	13	30	10	3	0
6.2	12.4.1	Gebeurtenissen registreren	P-E	2,0	16	26	12	2	0
6.3	12.4.3	Logbestanden van beheerders en operators	E	1,8	22	24	8	2	0
6.9	18.2.2	Naleving van beveiligingsbeleid en –normen	P	1,8	19	29	8	0	0
6.10	18.2.3	Beoordeling van technische naleving	P	2,3	12	24	14	5	1
		Gemiddelde cluster 6		2,1					

4. Continuïteit

4.5	12.3.1	Back-up van informatie	P	3,2	1	8	30	15	2
4.13	16.1.5	Respons op informatiebeveiligingsincidenten	E	3,1	3	5	33	14	1
4.14	17.1.2	Informatiebeveiligingscontinuïteit implementeren	P	2,0	16	25	12	3	0
4.15	17.2.1	Beschikbaarheid van informatie verwerkende faciliteiten	E	2,5	6	22	20	8	0
		Gemiddelde cluster 4		2,6					

NETWERK IBP IN HET MBO

Kennisnet SURF saMBO-ICT

5. Vertrouwelijkheid en integriteit

Informatiebeveiliging				2,5	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5
aantal deelnemers informatiebeveiliging: 56									
Nr.	ISO27002	Statement		Niveau 1 t/m 5					
1.1	5.1.1	Beleidsregels voor informatiebeveiliging	P	3,1	0	8	34	14	0
1.6	6.2.1	Beleid voor mobiele apparatuur	P	2,5	8	18	22	8	0
1.7	8.2.1	Classificatie van informatie	P	2,5	6	24	18	8	0
1.8	8.2.2	Informatie labelen	P	2,3	14	15	22	5	0
1.9	10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	P-E	2,3	10	23	18	5	0
1.15	15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	P-E	2,6	6	19	26	4	1
1.16	15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	E	3,1	0	5	41	10	0
1.17	16.1.1	Verantwoordelijkheden en procedures.	E	3,0	0	13	32	11	0
1.18	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	P-E	2,9	2	14	28	12	0
1.19	18.1.3	Beschermen van registraties	P-E	2,1	5	42	9	0	0
1.20	18.1.4	Privacy en bescherming van persoonsgegevens	P	3,1	0	7	37	12	0
		Gemiddelde cluster 1		2,6					
2.1	7.1.2	Arbeidsvoorwaarden	P	2,3	13	16	24	3	0
2.2	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	P	2,2	5	35	15	1	0
2.3	9.2.6	Toegangsrechten intrekken of aanpassen	P-E	2,7	7	15	25	8	1
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	P-E	2,0	10	35	11	0	0
2.5	13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	P	2,5	9	18	19	10	0
2.8	6.2.								
3.5	11.								
3.14	11.								
3.21	8.3.								
4.5	12.								
4.13	16.								
4.14	17.								
4.15	17.								
5.1	9.1.								
5.2	9.1.								
5.3	9.2.								
5.4	9.2.								
5.5	9.2.								
5.6	9.2.								
5.7	9.3.								
5.8	9.4.								
5.9	9.4.								
5.10	10.								
5.12	12.								
5.16	13.								
6.1	9.2.								
6.2	12.								
6.3	12.								
6.9	18.2.2	Naleving van beveiligingsbeleid en –normen	P	1,8	19	29	8	0	0
6.10	18.2.3	Beoordeling van technische naleving	P	2,3	12	24	14	5	1
		Gemiddelde cluster 6		2,1					

5.1	9.1.1	Beleid voor toegangsbeveiliging	P	2,4	9	17	27	2	1
5.2	9.1.2	Toegang tot netwerken en netwerkdiensten	P-E	2,5	9	16	27	4	0
5.3	9.2.1	Registratie en afmelden van gebruikers	P-E	2,6	9	17	20	9	1
5.4	9.2.2	Gebruikers toegang verlenen	P	2,6	9	13	24	9	1
5.5	9.2.3	Beheren van speciale toegangsrechten	P	2,4	11	17	20	8	0
5.6	9.2.4	Beheer van geheime authenticatie-informatie van gebruikers	P	2,6	8	17	22	9	0
5.7	9.3.1	Geheime authenticatie-informatie gebruiken	P	2,5	8	15	28	5	0
5.8	9.4.1	Beperking toegang tot informatie	P	2,4	9	20	25	2	0
5.9	9.4.2	Beveiligde inlogprocedures	P-E	2,5	7	21	23	4	1
5.10	10.1.2	Sleutelbeheer	P	2,2	15	18	21	2	0
5.12	12.4.2	Beschermen van informatie in logbestanden	P-E	2,0	20	19	14	3	0
5.16	13.2.3	Elektronische berichten	P	2,1	16	20	19	1	0
		Gemiddelde cluster 5		2,4					

NETWERK IBP IN HET MBO

Kennisnet SURF saMBO-ICT

6. Controle en logging

Informatiebeveiliging				2,5	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5
aantal deelnemers informatiebeveiliging: 56									
Nr.	ISO27002	Statement		Niveau 1 t/m 5					
1.1	5.1.1	Beleidsregels voor informatiebeveiliging	P	3,1	0	8	34	14	0
1.6	6.2.1	Beleid voor mobiele apparatuur	P	2,5	8	18	22	8	0
1.7	8.2.1	Classificatie van informatie	P	2,5	6	24	18	8	0
1.8	8.2.2	Informatie labelen	P	2,3	14	15	22	5	0
1.9	10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	P-E	2,3	10	23	18	5	0
1.15	15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	P-E	2,6	6	19	26	4	1
1.16	15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	E	3,1	0	5	41	10	0
1.17	16.1.1	Verantwoordelijkheden en procedures.	E	3,0	0	13	32	11	0
1.18	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	P-E	2,9	2	14	28	12	0
1.19	18.1.3	Beschermen van registraties	P-E	2,1	5	42	9	0	0
1.20	18.1.4	Privacy en bescherming van persoonsgegevens	P	3,1	0	7	37	12	0
		Gemiddelde cluster 1		2,6					
2.1	7.1.2	Arbeidsvoorwaarden	P	2,3	13	16	24	3	0
2.2	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	P	2,2	5	35	15	1	0
2.3	9.2.6	Toegangsrechten intrekken of aanpassen	P-E	2,7	7	15	25	8	1
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	P-E	2,0	10	35	11	0	0
2.5	13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	P	2,5	9	18	19	10	0
2.8	6.2.2	Telewerken (thuiswerken)	E	1,7	29	15	10	2	0
		Gemiddelde cluster 2		2,3					
3.5	11.1.3	Kantoren, ruimten en faciliteiten beveiligen	E	2,4	8	20	26	2	0
3.14	11.2.7	Veilig verwijderen of hergebruiken van apparatuur	P	2,7	7	13	27	8	1
3.21	8.3.3	Media fysiek overdragen	E	2,2	13	22	17	4	0
		Gemiddelde cluster 3		2,6					
4.5	12.3.1	Back-up van informatie	P	3,2	1	8	30	15	2
4.13	16.1.5	Respons op informatiebeveiligingsincidenten	E	3,1	3	5	33	14	1
4.14	17.1.2	Informatiebeveiligingscontinuïteit implementeren	P	2,0	16	25	12	3	0
4.15	17.2.1	Beschikbaarheid van informatie verwerkende faciliteiten	E	2,5	6	22	20	8	0
		Gemiddelde cluster 4		2,6					
5.1	9.1.1	Beleid voor toegangsbeveiliging	P	2,4	9	17	27	2	1
5.2	9.1.2	Toegang tot netwerken en netwerkdiensten	P-E	2,5	9	16	27	4	0
5.3	9.2.1	Registratie en afmelden van gebruikers	P-E	2,6	9	17	20	9	1
5.4	9.2.2	Gebruikers toegang verlenen	P	2,6	9	13	24	9	1
5.5	9.2.3								
5.6	9.2.4								
5.7	9.3.1								
5.8	9.4.1								
5.9	9.4.2								
5.10	10.1.2								
5.12	12.4.2								
5.16	13.2.3								
6.1	9.2.5								
6.2	12.4.1								
6.3	12.4.3								
6.9	18.2.2								
6.10	18.2.3	Beoordeling van technische naleving	P	2,3	12	24	14	5	1
		Gemiddelde cluster 6		2,1					

6.1	9.2.5	Beoordeling van toegangsrechten van gebruikers	P-E	2,1	13	30	10	3	0
6.2	12.4.1	Gebeurtenissen registreren	P-E	2,0	16	26	12	2	0
6.3	12.4.3	Logbestanden van beheerders en operators	E	1,8	22	24	8	2	0
6.9	18.2.2	Naleving van beveiligingsbeleid en –normen	P	1,8	19	29	8	0	0
6.10	18.2.3	Beoordeling van technische naleving	P	2,3	12	24	14	5	1
		Gemiddelde cluster 6		2,1					

NETWERK IBP IN HET MBO

Kennisnet SURF saMBO-ICT

Privacy

2,5

aantal deelnemers privacy: 56

Nr.	Statement	Niveau 1 t/m 5	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5
P.1	Privacy-beleid	3,2	0	7	34	14	1
P.2	Functionaris gegevensbescherming	3,4	1	1	29	23	2
P.3	Rechtmatige verwerking van persoonsgegevens	2,6	2	26	21	7	0
P.4	Register van verwerkingsactiviteiten (dataregister)	2,6	2	28	19	7	0
P.5	Bewaartermijnen	2,0	8	39	8	1	0
P.6	Verwerking t.b.v. onderzoek	2,0	21	18	15	2	0
P.7	Verwerking van bijzondere persoonsgegevens	2,3	13	19	18	6	0
P.8	Geautomatiseerde besluitvorming	2,3	14	17	20	5	0
P.9	Informatiebeveiliging	2,4	11	22	15	8	0
P.10	Verwerkersovereenkomsten	2,8	0	19	31	6	0
P.11	Transparant over privacy	2,8	1	15	37	3	0
P.12	Informeren over verwerkingen	2,7	1	22	27	6	0
P.13	Procedures rechten van de betrokkenen	2,6	6	18	26	6	0
P.14	Geheimhouding	2,5	4	26	18	8	0
P.15	Bewustzijn, opleiding en training ten aanzien van privacy	2,3	4	34	16	2	0
P.16	Bewijs van vernietiging persoonsgegevens	2,6	6	19	22	9	0
P.17	Dataclassificatie	2,5	7	19	24	6	0
P.18	Datalekken en beveiligingsincidenten	3,2	0	6	36	11	3
P.19	Vervallen, zie P.7, P.9 en P.17						
P.20	Privacy by design en privacy by default	2,2	12	24	19	1	0
P.21	Data Protection Impact Assessment (DPIA)	2,1	12	28	16	0	0
P.22	Controle naleving beleid	2,3	7	28	19	2	0
P.23	Vervallen, zie P.2, P.11, P.12, P.18 en IB1.18						
P.24	Vervallen, zie IB6.2						

NETWERK IBP IN HET MBO

Kennisnet SURF saMBO-ICT

Gemeenschappelijk normenkader PRIVACY

2,4

aantal deelnemers informatiebeveiliging: **56**

Nr.	ISO27002	Statement		Niveau 1 t/m 5	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5
1.1	5.1.1	Beleidsregels voor informatiebeveiliging	P	3,1	0	8	34	14	0
1.6	6.2.1	Beleid voor mobiele apparatuur	P	2,5	8	18	22	8	0
1.7	8.2.1	Classificatie van informatie	P	2,5	6	24	18	8	0
1.8	8.2.2	Informatie labelen	P	2,3	13	15	22	5	0
1.9	10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	P-E	2,3	10	23	18	5	0
1.15	15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	P-E	2,6	6	19	26	4	1
1.18	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	P-E	2,9	2	14	28	12	0
1.19	18.1.3	Beschermen van registraties	P-E	2,1	5	42	9	0	0
1.20	18.1.4	Privacy en bescherming van persoonsgegevens	P	3,1	0	7	37	12	0
2.1	7.1.2	Arbeidsvoorwaarden	P	2,3	13	16	24	3	0
2.2	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	P	2,2	5	35	15	1	0
2.3	9.2.6	Toegangsrechten intrekken of aanpassen	P-E	2,7	7	15	25	8	1
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	P-E	2,0	10	35	11	0	0
2.5	13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	P	2,5	9	18	19	10	0
3.14	11.2.7	Veilig verwijderen of hergebruiken van apparatuur	P	2,7	7	13	27	8	1
4.5	12.3.1	Back-up van informatie	P	3,2	1	8	30	15	2
4.14	17.1.2	Informatiebeveiligingscontinuïteit implementeren	P	2,0	16	25	12	3	0
5.1	9.1.1	Beleid voor toegangsbeveiliging	P	2,4	9	17	27	2	1
5.2	9.1.2	Toegang tot netwerken en netwerkdiensten	P-E	2,5	9	16	27	4	0
5.3	9.2.1	Registratie en afmelden van gebruikers	P-E	2,6	9	17	20	9	1
5.4	9.2.2	Gebruikers toegang verlenen	P	2,6	9	13	24	9	1
5.5	9.2.3	Beheren van speciale toegangsrechten	P	2,4	11	17	20	8	0
5.6	9.2.4	Beheer van geheime authenticatie-informatie van gebruikers	P	2,6	8	17	22	9	0
5.7	9.3.1	Geheime authenticatie-informatie gebruiken	P	2,5	8	15	28	5	0
5.8	9.4.1	Beperking toegang tot informatie	P	2,4	9	20	25	2	0
5.9	9.4.2	Beveiligde inlogprocedures	P-E	2,5	7	21	23	4	1
5.10	10.1.2	Sleutelbeheer	P	2,2	15	18	21	2	0
5.12	12.4.2	Beschermen van informatie in logbestanden	P-E	2,0	20	19	14	3	0
5.16	13.2.3	Elektronische berichten	P	2,1	16	20	19	1	0
6.1	9.2.5	Beoordeling van toegangsrechten van gebruikers	P-E	2,1	13	30	10	3	0
6.2	12.4.1	Gebeurtenissen registreren	P-E	2,0	16	26	12	2	0
6.9	18.2.2	Naleving van beveiligingsbeleid en –normen	P	1,8	19	29	8	0	0
6.10	18.2.3	Beoordeling van technische naleving	P	2,3	12	24	14	5	1

Examinering

2,5

aantal deelnemers examinering: 50

Nr.	Statement	Niveau 1 t/m 5	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5
E.1	Beleidsplan beveiliging examinering	2,0	20	15	11	4	0
E.2	Gedragscodes en richtlijnen afname examens	2,5	5	22	16	7	0
E.3	Trainingen en vaardigheden m.b.t. richtlijnen	2,8	3	15	22	10	0
E.4	Continuïteitsplan	2,1	19	13	13	5	0
E.5	Archiveren en vernietigen examenmateriaal	2,6	4	19	21	6	0
E.6	Richtlijn inkoop, construeren en vaststellen examens in een beveiligde omgeving	2,5	7	16	24	3	0
E.7	Richtlijnen bij constatering van onregelmatigheden die tot fraude kunnen leiden bij examens	2,9	3	10	24	13	0
E.8	Voorkomen van examenfraude	2,6	10	8	24	8	0
E.9	Procedure voorbereiden en afnemen examens	2,4	11	14	17	8	0
E.10	Extra ondersteuning bij (digitale) examens	3,1	1	7	28	14	0
E.11	Beveiligde examenruimtes	2,2	15	15	16	4	0
E.12	Het beheren en documenteren van ict-faciliteiten voor examinering	2,0	17	20	9	4	0
E.13	Hanteren van digitaal examenmateriaal	2,1	14	22	10	4	0
E.14	Toewijzen examens aan studenten	2,6	6	18	17	7	2
E.15	Kopieerbeveiliging examenvragen i.v.m. mogelijk hergebruik	2,2	20	11	12	5	2
E.16	Voorbereiden op vaststellen diplomabesluit door de examencommissie	3,4	1	4	23	19	3
E.17	Borgen dat diploma en overige waardedocumenten rechtmatig, veilig en correct worden aangemaakt en afgedrukt	3,2	4	5	22	16	3
E.18	Eindevaluatie examenproces en de integriteit van de resultaten	2,6	9	16	13	12	0

NETWERK IBP IN HET MBO
Kennisnet SURF saMBO-ICT

Gemeenschappelijk normenkader EXAMINERING

2,4

aantal deelnemers informatiebeveiliging: **56**

Nr.	ISO27002	Statement		Niveau 1 t/m 5	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5
1.9	10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	P-E	2,3	10	23	18	5	0
1.15	15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	P-E	2,6	6	19	26	4	1
1.16	15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	E	3,1	0	5	41	10	0
1.17	16.1.1	Verantwoordelijkheden en procedures.	E	3,0	0	13	32	11	0
1.18	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	P-E	2,9	2	14	28	12	0
1.19	18.1.3	Beschermen van registraties	P-E	2,1	5	42	9	0	0
2.3	9.2.6	Toegangsrechten intrekken of aanpassen	P-E	2,7	7	15	25	8	1
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	P-E	2,0	10	35	11	0	0
2.8	6.2.2	Telewerken (thuiswerken)	E	1,7	29	15	10	2	0
3.5	11.1.3	Kantoren, ruimten en faciliteiten beveiligen	E	2,4	8	20	26	2	0
3.21	8.3.3	Media fysiek overdragen	E	2,2	13	22	17	4	0
4.13	16.1.5	Respons op informatiebeveiligingsincidenten	E	3,1	3	5	33	14	1
4.15	17.2.1	Beschikbaarheid van informatie verwerkende faciliteiten	E	2,5	6	22	20	8	0
5.2	9.1.2	Toegang tot netwerken en netwerkdiensten	P-E	2,5	9	16	27	4	0
5.3	9.2.1	Registratie en afmelden van gebruikers	P-E	2,6	9	17	20	9	1
5.9	9.4.2	Beveiligde inlogprocedures	P-E	2,5	7	21	23	4	1
5.12	12.4.2	Beschermen van informatie in logbestanden	P-E	2,0	20	19	14	3	0
6.1	9.2.5	Beoordeling van toegangsrechten van gebruikers	P-E	2,1	13	30	10	3	0
6.2	12.4.1	Gebeurtenissen registreren	P-E	2,0	16	26	12	2	0
6.3	12.4.3	Logbestanden van beheerders en operators	E	1,8	22	24	8	2	0

NETWERK IBP IN HET MBO

Kennisnet SURF saMBO-ICT

Nieuwe statements Informatiebeveiliging

2,3

aantal deelnemers informatiebeveiliging: **56**

Nr.	ISO27002	Statement		Niveau 1 t/m 5	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5
1.22	6.1.3	Contact met overheidsinstanties		2,7	5	16	26	9	0
1.23	6.1.4	Contact met speciale belangengroepen		2,8	5	9	32	10	0
1.24	8.2.3	Behandelen van bedrijfsmiddelen		2,3	10	23	17	6	0
1.25	18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen		2,2	14	24	13	5	0
1.26	18.1.2	Intellectuele eigendomsrechten		2,3	16	12	21	7	0
1.27	18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen		2,1	17	19	17	3	0
2.8	6.2.2	Telewerken (thuiswerken)	E	1,7	29	15	10	2	0
2.9	7.1.3	Disciplinaire procedure		2,3	11	25	13	7	0
2.10	7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband		2,3	16	16	17	7	0
3.16	8.1.1	Inventariseren van bedrijfsmiddelen		2,9	5	13	23	15	0
3.17	8.1.2	Eigendom van bedrijfsmiddelen		3,0	3	8	31	14	0
3.18	8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen		2,8	3	15	28	10	0
3.19	8.1.4	Teruggeven van bedrijfsmiddelen		2,6	4	18	29	5	0
3.20	8.3.1	Beheer van verwijderbare media		2,2	12	20	23	1	0
3.21	8.3.3	Media fysiek overdragen	E	2,2	13	22	17	4	0
4.16	12.1.1	Gedocumenteerde bedieningsprocedures		2,4	11	18	19	8	0
4.17	12.1.3	Capaciteitsbeheer		2,5	8	20	21	7	0
4.18	17.1.1	Informatiebeveiligingscontinuïteit plannen		2,2	15	16	23	2	0
4.19	17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren		1,9	21	19	14	2	0
5.18	9.4.3	Systeem voor wachtwoordbeheer		2,7	7	12	26	11	0
5.19	9.4.4	Speciale systeemhulpmiddelen gebruiken		2,3	15	18	16	7	0
5.20	9.4.5	Toegangsbeveiliging op programmabroncode		2,4	13	15	21	7	0
5.22	14.2.1	Beleid voor beveiligd ontwikkelen		2,3	16	12	23	5	0
5.23	14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen		2,3	17	11	23	5	0
5.24	14.2.3	Technische beoordeling van toepassingen na wijzigingen bedieningsplatform		2,2	15	18	18	5	0
5.25	14.2.4	Beperkingen op wijzigingen aan softwarepakketten		2,4	13	15	21	7	0
5.27	14.3.1	Bescherming van testgegevens		1,7	24	23	9	0	0
6.11	7.2.1	Directieverantwoordelijkheden		1,5	34	14	8	0	0
6.12	12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen		2,0	24	14	11	7	0
6.13	16.1.6	Lering uit informatiebeveiligingsincidenten		2,6	10	10	30	6	0
6.14	18.2.1	Onafhankelijke beoordeling van informatiebeveiliging		2,2	18	17	15	6	0

Ranking Informatiebeveiliging: 1-15

Ranking: 1-15

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**

NETWERK IBP IN HET MBO
Kennisnet SURF saMBO-ICT

Ranking Informatiebeveiliging: 16-30

Ranking: 16-30

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 Informatiebeveiliging: 31-45

Ranking: 31-45

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 Informatiebeveiliging: 46-56

Ranking: 46-56

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 scorende statements

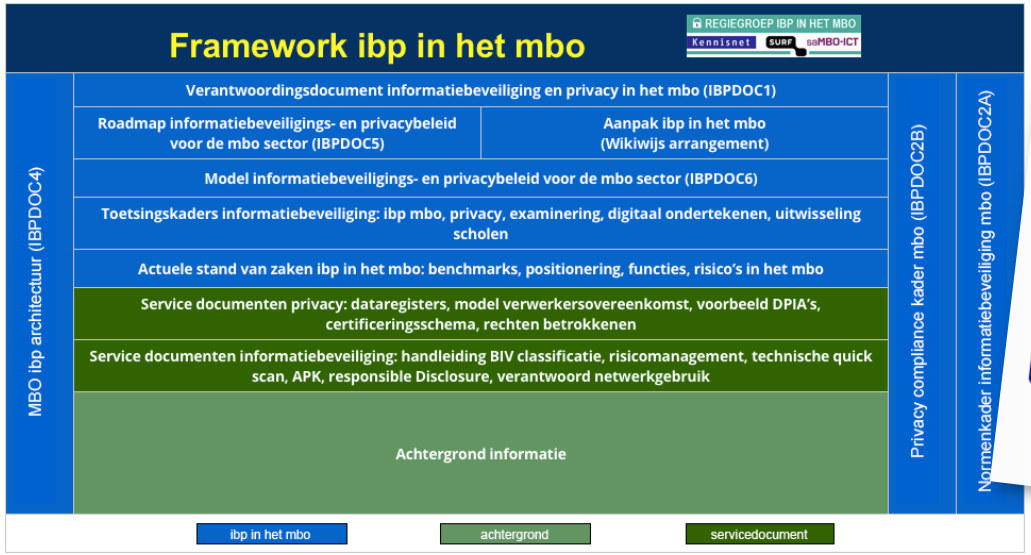
4.5	12.3.1	Back-up van informatie	3,2
3.15	12.4.4	Kloksynchronisatie	3,1
1.1	5.1.1	Beleidsregels voor informatiebeveiliging	3,1
1.13	13.2.2	Overeenkomsten over informatietransport	3,1
1.16	15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	3,1
1.20	18.1.4	Privacy en bescherming van persoonsgegevens	3,1
4.3	12.2.1	Beheersmaatregelen tegen malware	3,1
4.13	16.1.5	Respons op informatiebeveiligingsincidenten	3,1
3.10	11.2.2	Nutsvoorzieningen	3,1
5.15	13.1.3	Scheiding in netwerken	3,0
3.17	8.1.2	Eigendom van bedrijfsmiddelen	3,0
1.17	16.1.1	Verantwoordelijkheden en procedures.	3,0
4.12	16.1.4	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	2,9
1.18	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	2,9
4.7	12.5.1	Software installeren op operationele systemen	2,9

De laagst scorende statements

1.19	18.1.3	Beschermen van registraties	2,1
6.1	9.2.5	Beoordeling van toegangsrechten van gebruikers	2,1
1.5	6.1.5	Informatiebeveiliging in projectbeheer	2,0
4.14	17.1.2	Informatiebeveiligingscontinuïteit implementeren	2,0
6.7	15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	2,0
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	2,0
6.12	12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen	2,0
5.12	12.4.2	Beschermen van informatie in logbestanden	2,0
6.2	12.4.1	Gebeurtenissen registreren	2,0
4.19	17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	1,9
6.3	12.4.3	Logbestanden van beheerders en operators	1,8
6.9	18.2.2	Naleving van beveiligingsbeleid en –normen	1,8
2.8	6.2.2	Telewerken (thuiswerken)	1,7
5.27	14.3.1	Bescherming van testgegevens	1,7
6.11	7.2.1	Directieverantwoordelijkheden	1,5

Rapportage Benchmark IBP/E 2019

- Zie Framework IBP in het mbo www.sambo-ict.nl/framework-ibp
- IBPDOC11e



NETWERK IBP IN HET MBO
Kennisnet SURF saMBO-ICT

Aanbevelingen: Benchmark naar 3.0

- Ondersteuning vanuit saMBO-ICT en Kennisnet
  - aandacht voor de zwakke clusters / statements
  - handreikingen, modeldocumenten
  - onderhoud Framework
  - uitwisselingsplatform voor instellingen?
- Ondersteuning voor de onvoldoende scorende instellingen
  - is er behoefte aan extra ondersteuning?
  - tegen welke achtergrond kwamen deze scores tot stand?
  - hoe kunnen wij (als sector) helpen?

➢ **Werkgroep 3: Benchmark naar 3.0 (Co)**

Aanbevelingen: toetsingskader IB

- Beschrijving van de bewijslast
  - bedoeld om richting te geven, soms te letterlijk geïnterpreteerd
  - meer duiding en instructie nodig
  - onderzoek andere vormen van instructie (just-in-time)
  - tekstuele aanpassingen
- Review (nieuwe) statements
- Mogelijkheid optionele statements, afhankelijk situatie

➢ **Werkgroep 4: doorontwikkeling toetsingskaders (Fung Yee)**

Aanbevelingen: Peer review

- Onderlinge afwijkingen in benchmarkscores
  - interpretatieverschillen toetsingskader / bewijslast
  - mate van aandacht, grondigheid
  - bias invuller

- Vast onderdeel benchmark, maar dan wel:
  - beperken tot de kern
  - efficiënter georganiseerd

➢ **Werkgroep 5: peer review (Richard**)