Benchmark informatiebeveiliging in de mbo sector 2015

IBPDOC11b

GEBRUIKERSGROEP IBP IN HET MBO

Kennisnet SURF saMBO-ICT

Verantwoording

Productie

Kennisnet / saMBO-ICT
Benchmark is uitgevoerd met behulp van de tool Coable van het bedrijf Coblue Sybersecurity.
Het Hoger Onderwijs (SURF SCIPR) maakt ook gebruik van deze tool.

Auteurs

Leo Bakker (Kennisnet)
Ludo Cuijpers (saMBO-ICT, ROC Leeuwenborgh)
December 2015

Met dank aan

Aeres Groep	Martin Deiman
Albeda	Rienk de Vries
Arcus College	Joep Lemmens
Citaverde	Martijn van Hoorn
Deltion	Rene Dol
Graafschap College	Donny Toebos
Grafisch Lyceum Rotterdam	Don van der Linden
Hoornbeeck	Willem Flink
MBO Utrecht	Marjolein Rombouts
Nimeto	Esther van der Hei
Noorderpoort	Martijn Broekhuizen
Nordwin College	Rob Smit
Nova College	Rob Smit
Onderwijsgroep Tilburg	Brom Bogers
ROC TOP	Theo Kuilboer
ROC Twente	Kim Kuipers
ROC van Amsterdam	Co Klerkx
Summa College	Martien van Beekveld
Zadkine	Wim Arendse

Sommige rechten voorbehouden

Inhoudsopgave

1. Conclusies benchmark

1.1 Terugblik

Medio 2014 is de Taskforce Informatiebeveiliging en privacy van start gegaan met een duidelijke opdracht die verwoord is in het Verantwoordingsdocument[1]. De eerste paragraaf spreekt boekdelen:

> *… Het zal duidelijk zijn dat het thema Informatiebeveiliging en zeker ook privacy de laatste tijd met een sneltreinvaart in het onderwijs in de belangstelling is komen te staan. Dat heeft zo zijn redenen. Afgelopen jaren zijn in alle sectoren van het onderwijs incidenten rondom examinering in de publiciteit gekomen. In sommige gevallen ging dit ook om ernstige incidenten die breed in de media zijn uitgemeten. Dat levert voor het onderwijs veel schade op, waarbij imagoschade voorop staat. Het onderwijs wordt geacht op betrouwbare wijze diploma's uit te reiken en het kan niet zo zijn dat daar twijfels over bestaan omdat examens op straat liggen dan wel op het internet te koop zijn. Een ander voorbeeld is de vraag of het onderwijs met de toenemende registratie van gegevens van leerlingen de bescherming van de privacy nog kan waarborgen. Steeds vaker zijn hier ook externe partijen en leveranciers bij betrokken en zonder goede afspraken hierover kan de privacybescherming zomaar in het geding zijn. Zeker bij jonge kinderen wordt dit door de maatschappij onacceptabel gevonden.*
>
> ***Daar komt bij dat een vraag naar hoe het in de onderwijs sector gesteld is met de informatiebeveiliging en de bescherming van de privacy nauwelijks kan worden beantwoord. Dat beeld is op zijn minst zeer gebrekkig en onhelder te noemen. En om aan te geven of je iets op orde hebt moet je daarover ook eerste afspraken gemaakt hebben over wat dan op orde is. Die afspraken ontbreken vooralsnog.***
>
> *Daarom is het in het belang van zowel het onderwijs zelf als van het ministerie van Onderwijs, Cultuur en Wetenschap (OCW) dat er gemeenschappelijke afsprakenkaders komen, dat die met alle onderwijsinstellingen en ook met de relevante externe partijen worden gedeeld en geïmplementeerd. Pas dan kan er een beeld ontstaan van hoe scholen het doen op deze terreinen en kunnen er verbeteringstrajecten worden ingezet en doelen gesteld worden om een bepaalde graad van beveiliging en bescherming te creëren. In het hoger onderwijs is dit traject al eerder ingezet.*
>
> *Dit alles heeft er toe geleid dat OCW de vraag bij de mbo sector heeft neergelegd om een beeld van de stand van zaken in het mbo met betrekking tot informatiebeveiliging en privacy te schetsen en er voor te zorgen dat er naar een gewenste situatie kan worden toegewerkt. De sector heeft deze uitdaging opgepakt en wil met dit programma de stappen zetten om in het mbo op een volwassen wijze met deze problematiek om te gaan en een acceptabel niveau van beveiliging en bescherming te bieden aan al haar studenten en medewerkers….*

Als sector hebben we het afgelopen jaar hard gewerkt om Informatiebeveiliging en privacy in onze sector op de strategische agenda te zetten. Op tactisch niveau hebben we een groot aantal documenten opgeleverd (zie bijlage 1) en is er volop geschoold in de masterclasses informatiebeveiliging en privacy (ibp) waar een vijftigtal mbo instellingen aan hebben deelgenomen. Op operationeel niveau is deze kennis binnen de mbo instellingen vertaald in een actief IBP beleid. Weliswaar staan we als sector aan het begin van een lange weg maar toch hebben we het gevoel dat we een vliegende start hebben gemaakt. We willen nu graag weten waar de mbo sector staat. Daarvoor hebben we een benchmark uitgevoerd om de bepalen op welk volwassenheidsniveau, de nulmeting, we ons nu bevinden.

1.2 Representativiteit

Aan de eerste IBP benchmark hebben 19 mbo instellingen deel genomen waaronder 3 AOC's, 14 ROC's en 2 vakscholen. De regionale spreiding was afdoende. Zowel grote (ROC Amsterdam) als kleine (Nimeto) mbo instellingen hebben deelgenomen. Het is dan ook statistisch verdedigbaar dat deze deelwaarneming een getrouw beeld schetst van de 51 mbo instellingen die actief betrokken zijn bij het informatie en privacy beleid in onze sector. Van 14 instellingen is niet duidelijk of zij stappen genomen hebben op dit gebied.

[1] Zie IBPDOC1: Verantwoordingsdocument Informatiebeveiliging en privacy (ibp) in het mbo.

1.3 Bevindingen

De benchmark is uitgevoerd op basis van het vastgestelde toetsingskader ibp[2]. De toets is dan ook uitgevoerd op de 6 clusters die afgeleid zijn van het ISO 27001/2 normenkader. De opzet van de benchmark is gelijk aan die van het Hoger Onderwijs.

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

Cluster 1: Beleid en organisatie	**1.7**
Cluster 2: Personeel, studenten en gasten	**1.7**
Cluster 3: Ruimtes en apparatuur	**2.1**
Cluster 4: Continuïteit	**2.0**
Cluster 5: Vertrouwelijkheid en integriteit	**2.0**
Cluster 6: Controle en Logging	**1.6**

De gemiddelde score van de mbo sector is: **1,9**
Ter vergelijking de score van het Hoger Onderwijs in 2013 was 2,2.
In hoofdstuk 2 worden de resultaten verder toegelicht.

1.4 Aanbevelingen

Volwassenheidsniveau 1 (ad hoc) betekent dat de mbo instelling het ibp probleem onderkent maar nog geen actie heeft ondernomen. Niveau 2 houdt in dat er goedgekeurd beleid is dat echter nog niet bij de hele mbo instelling bekend is, laat staan gedragen wordt. Alleen een kleine groep (managers, functioneel en technisch beheerders, etc.) weet van de hoed en de rand. Stel dat we niveau 2 als baseline (gewenst niveau in 2016/2017) hanteren dan leiden de resultaten tot de volgende aanbevelingen binnen onze sector:

Aanbeveling 1:	Onderzoek waarom 14 mbo instellingen niet deelnemen aan de initiatieven (conferenties, masterclasses, benchmark, etc.) van de Taskforce ibp in het mbo. Wellicht dat de MBO-Raad hier een inspirerende rol in kan spelen.
Aanbeveling 2:	Cluster 2 (Personeel, studenten en gasten) scoort onder de maat. Awareness sessies en trainingen van personeel kunnen leiden tot een betere acceptatie van het ibp beleid binnen de mbo sector. Het is zinvol om best practices en tools vanuit Kennisnet aan te bieden.
Aanbeveling 3:	Cluster 6 is onder de maat. Ondersteuning vanuit Kennisnet en SURF is gewenst.

De 51 mbo instellingen moeten in staat zijn om de overige clusters op niveau 2 te brengen. Cluster 1 scoort onder de maat maar kan snel op een hoger niveau komen als de instellingen de ibp beleidsstukken binnen de instellingen geïmplementeerd hebben.

1.5 Hoe nu verder?

De mbo sector is voornemens om in 2016 een peer review uit te voeren. Wellicht dat in 2017 peer audits mogelijk worden uitgevoerd. Een en ander moet er toe leiden dat we in de toekomst binnen onze sector middels zelf regulatie kunnen aantonen dat ibp in control is. In hoofdstuk 3 wordt een en ander uitvoerig beschreven.

[2] IBPDOC3: Toetsingskader informatiebeveiliging cluster 1 t/m 6

2. Resultaten ibp benchmark

2.1 Toelichting op de tabellen

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

Nr.	ISO27002	Statement	niveau 1	niveau 2	niveau 3	niveau 4	niveau 5	Gem
1.1	5.1.1.1	**Beleidsregels voor informatiebeveiliging** (beleid gedefinieerd en goedgekeurd door CvB)	7	8	3	1		1,9

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

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

		Clusterindeling Hoger Onderwijs						
Hoofdstukken ISO-27002	ISO-27002	**1**: Beleid	**2**: personeel	**3**: Ruimten	**4**: Continuïteit	**5**: Toegang	**6**: Controle	Niet gebruikt
5. Informatiebeveiligingsbeleid	**2**	2						
6. Organiseren van informatiebeveiliging	**7**	4		0				3
7. Veilig personeel	**6**		3					3
8. Beheer van bedrijfsmiddelen	**10**	2		1				7
9. Toegangsbeveiliging	**14**		1			9	1	3
10. Cryptografie	**2**	1				1		
11. Fysieke beveiliging en beveiliging van de omgeving	**15**	1	1	12				1
12. Beveiliging bedrijfsvoering	**14**			1	7	1	2	3
13. Communicatiebeveiliging	**7**	2	1			4		
14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen	**13**	1			1	1	3	7
15. Leveranciersrelaties	**5**	2			1		1	1
16. Beheer van informatiebeveiligingsincidenten	**7**	2	1		2		1	1
17. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	**4**				2			2
18. Naleving	**8**	2					2	4
	114	**19**	**7**	**14**	**13**	**16**	**10**	**35**
Clustertotaal inclusief splitsing (85)		21	7	15	15	17	10	

Nr.	ISO27002	Statement	niveau 1	niveau 2	niveau 3	niveau 4	niveau 5	Gem
1.1	5.1.1.1	**Beleidsregels voor informatiebeveiliging** (beleid gedefinieerd en goedgekeurd door CvB)	7	8	3	1		1,9

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

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

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

Bij ieder volwassenheidsniveau is de score weergegeven van de deelnemende mbo instellingen aan de benchmark.
“Niveau 2” is rood omkaderd als een mogelijke baseline voor de sector.
De modale klasse (klasse met de hoogste frequentie dichtheid) is weergegeven in geel. Indien 2 klassen dezelfde dichtheid hebben is de hoogste klasse geel gearceerd.
Het gemiddelde cijfer is het rekenkundige gemiddelde van de individuele waarnemingen.

2.2 Wat gaat goed en wat gaat minder goed?

Best scorende statements.

Nr.	ISO27002	Statement	niveau 1	niveau 2	niveau 3	niveau 4	niveau 5	Gem
4.5	12.3.1.1	**Back-up van informatie**	1	7	9	2		2,6
3.9	11.2.1	**Plaatsing en bescherming van apparatuur**		11	7	1		2,5
3.10	11.2.2	**Nutsvoorzieningen**	3	5	9	2		2,5
4.7	12.5.1	**Software installeren op operationele systemen**	2	7	9	1		2,5
4.9	12.6.2	**Beperkingen voor het installeren van software**.	1	9	8	1		2,5
5.13	13.1.1	**Beheersmaatregelen voor netwerken**	2	7	9	1		2,5
4.3	12.2.1.1	**Beheersmaatregelen tegen malware** (beheersmaatregelen)		11	8			2,4
5.3	9.2.1	**Registratie en afmelden van gebruikers**	1	11	6	1		2,4

Opvallend is dat de top 8 van de goed scorende statements allemaal in de cluster 3, 4 en 5 zitten. Technisch lijkt het dus in orde te zijn.

Slechts scorende statements.

Nr.	ISO27002	Statement	niveau 1	niveau 2	niveau 3	niveau 4	niveau 5	Gem
1.7	8.2.1	**Classificatie van informatie**	13	6				1,3
1.8	8.2.2	**Informatie labelen**	13	6				1,3
1.10	10.1.1.2	**Beleid inzake het gebruik van cryptografische beheersmaatregelen** (beleid geïmplementeerd)	13	6				1,3
5.10	10.1.2.1	**Sleutelbeheer**	13	6				1,3
5.11	10.1.2.2	**Sleutelbeheer**	14	5				1,3
6.5	14.2.8	**Testen van systeembeveiliging**	13	6				1,3
2.2	7.2.2	**Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging**	13	5	1			1,4
2.5	13.2.4	**Vertrouwelijkheids- of geheimhoudingsovereenkomst**	12	7				1,4
2.6	16.1.3	**Rapportage van zwakke plekken in de informatiebeveiliging**	11	8				1,4
4.14	17.1.2	**Informatiebeveiligingscontinuïteit implementeren**	12	7				1,4
6.8	16.1.7	**Verzamelen van bewijsmateriaal**	14	4		1		1,4

Cluster 3 kent geen statement dat zeer slecht scoort. Cluster 1 en 2, beleid en personeel, zijn oververtegenwoordigd.

2.3 Beleid en organisatie

Nr.	ISO27002	Statement	niveau 1	niveau 2	niveau 3	niveau 4	niveau 5	Gem
1.1	5.1.1.1	**Beleidsregels voor informatiebeveiliging** (beleid gedefinieerd en goedgekeurd door CvB)	7	8	3	1		1,9
1.2	5.1.1.2	**Beleidsregels voor informatiebeveiliging** (gecommuniceerd met medewerkers en externen)	10	8	1			1,5
1.3	5.1.2	**Beoordeling van het Informatiebeveiligingsbeleid**	10	6	2	1		1,7
1.4	6.1.1	**Taken en verantwoordelijkheden informatiebeveiliging**	3	12	4			2,1
1.5	6.1.5	**Informatiebeveiliging in projectbeheer**	13	3	3			1,5
1.6	6.2.1.1	**Beleid voor mobiele apparatuur** (beleid vastgesteld)	6	11	2			1,8
1.7	8.2.1	**Classificatie van informatie**	13	6				1,3
1.8	8.2.2	**Informatie labelen**	13	6				1,3
1.9	10.1.1.1	**Beleid inzake het gebruik van cryptografische beheersmaatregelen** (beleid vastgesteld)	12	5	2			1,5
1.10	10.1.1.2	**Beleid inzake het gebruik van cryptografische beheersmaatregelen** (beleid geïmplementeerd)	13	6				1,3
1.11	11.2.5	**Verwijdering van bedrijfsmiddelen**	9	7	3			1,7

1.12	13.2.1	Beleid en procedures voor informatietransport	7	12				1,6
1.13	13.2.2	Overeenkomsten over informatietransport	4	13	2			1,9
1.14	14.1.1	Analyse en specificatie van informatiebeveiligingseisen	4	13	2			1,9
1.15	15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	11	6	2			1,5
1.16	15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	7	11	1			1,7
1.17	16.1.1	Verantwoordelijkheden en procedures	6	11	1	1		1,8
1.18	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	6	10	2	1		1,9
1.19	18.1.3	Beschermen van registraties	9	8	2			1,6
1.20	18.1.4	Privacy en bescherming van persoonsgegevens	4	13	2			1,9
1.21	6.1.2	Scheiding van taken	5	11	3			1,9

In dit cluster valt veel winst te behalen. Een goedgekeurd ibp beleidsplan heeft invloed op de statements: 1.1, 1.2, 1.3, 1.4, 1.7, 1.8 en 1.20. Dit cluster is voor een gemiddelde instelling te behalen in een aantal maanden.

2.4 Personeel, studenten en gasten

Nr.	ISO27002	Statement	niveau 1	niveau 2	niveau 3	niveau 4	niveau 5	Gem
2.1	7.1.2	Arbeidsvoorwaarden	6	9	4			1,9
2.2	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	13	5	1			1,4
2.3	9.2.6	Toegangsrechten intrekken of aanpassen	3	11	5			2,1
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	12	5	2			1,5
2.5	13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	12	7				1,4
2.6	16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging	11	8				1,4
2.7	7.1.1	Screening	4	10	4	1		2,1

Dit is een moeilijk te realiseren cluster voor veel mbo instellingen. Met name de statements 2.2. en 2.4 vragen veel tijd en energie van alle medewerkers en studenten.

2.5 Ruimtes en apparatuur

Nr.	ISO27002	Statement	niveau 1	niveau 2	niveau 3	niveau 4	niveau 5	Gem
3.1	6.2.1.2	Beleid voor mobiele apparatuur	4	8	7			2,2
3.2	8.3.2	Verwijderen van media	4	12	2	1		2,0
3.3	11.1.1	Fysieke beveiligingszone.	3	10	6			2,2
3.4	11.1.2	Fysieke toegangsbeveiliging	4	13	2			1,9

3.5	11.1.3	Kantoren, ruimten en faciliteiten beveiligen	2	13	4			2,1
3.6	11.1.4	Beschermen tegen bedreigingen van buitenaf	1	11	7			2,3
3.7	11.1.5	Werken in beveiligde gebieden.	8	9	2			1,7
3.8	11.1.6	Laad- en loslocatie.	7	9	2		1	1,9
3.9	11.2.1	Plaatsing en bescherming van apparatuur		11	7	1		2,5
3.10	11.2.2	Nutsvoorzieningen	3	5	9	2		2,5
3.11	11.2.3	Beveiliging van bekabeling	4	8	6	1		2,2
3.12	11.2.4	Onderhoud van apparatuur.		14	4	1		2,3
3.13	11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	5	12	2			1,8
3.14	11.2.7	Veilig verwijderen of hergebruiken van apparatuur.	3	12	4			2,1
3.15	12.4.4	Kloksynchronisatie.	4	10	5			2,1

Het best scorende statement van de mbo sector geeft weinig aanleiding voor kritische beschouwingen. Feit blijft dat een aantal instellingen niveau niet realiseren. Nader onderzoek is dan ook gewenst om de oorzaak te kunnen achterhalen.

2.6 Continuïteit

Nr.	ISO27002	Statement	niveau 1	niveau 2	niveau 3	niveau 4	niveau 5	Gem
4.1	12.1.2	Wijzigingsbeheer	4	9	5	1		2,2
4.2	12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen	5	11	3			1,9
4.3	12.2.1.1	**Beheersmaatregelen tegen malware** (beheersmaatregelen)		11	8			2,4
4.4	12.2.1.2	**Beheersmaatregelen tegen malware** (bewustzijn)	7	8	4			1,8
4.5	12.3.1.1	Back-up van informatie	1	7	9	2		2,6
4.6	12.3.1.2	Back-up van informatie	5	10	3	1		2,0
4.7	12.5.1	Software installeren op operationele systemen	2	7	9	1		2,5
4.8	12.6.1	Beheer van technische kwetsbaarheden	6	11	2			1,8
4.9	12.6.2	Beperkingen voor het installeren van software.	1	9	8	1		2,5
4.10	14.2.6	Beveiligde ontwikkelomgeving	7	10	2			1,7
4.11	15.2.2	Beheer van veranderingen in dienstverlening van leveranciers	6	12	1			1,7
4.12	16.1.4	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen.	9	9	1			1,6
4.13	16.1.5	Respons op informatiebeveiligingsincidenten	8	9	1	1		1,7
4.14	17.1.2	Informatiebeveiligingscontinuïteit implementeren	12	7				1,4
4.15	17.2.1	Beschikbaarheid van informatie verwerkende faciliteiten	7	9	2	1		1,8

Cluster 4 scoort goed. Opvallend is statement 4,14 dat uit de toon valt. Nota bene een belangrijk statement in het ibp veld (informatiebeveiligingscontinuïteit implementeren).

2.7 Vertrouwelijkheid en integriteit

Nr.	ISO27002	Statement	niveau 1	niveau 2	niveau 3	niveau 4	niveau 5	Gem
5.1	9.1.1	Beleid voor toegangsbeveiliging	2	13	3	1		2,2
5.2	9.1.2	Toegang tot netwerken en netwerkdiensten.	2	10	7			2,3
5.3	9.2.1	Registratie en afmelden van gebruikers	1	11	6	1		2,4
5.4	9.2.2	Gebruikers toegang verlenen	3	14	2			1,9
5.5	9.2.3	Beheren van speciale toegangsrechten	1	17	1			2,0
5.6	9.2.4	Beheer van geheime authenticatie-informatie van gebruikers	4	6	7			2,2
5.7	9.3.1	Geheime authenticatie-informatie gebruiken	6	8	4	1		2,0
5.8	9.4.1	Beperking toegang tot informatie	3	10	6			2,2
5.9	9.4.2	Beveiligde inlogprocedures	1	11	7			2,3
5.10	10.1.2.1	Sleutelbeheer	13	6				1,3
5.11	10.1.2.2	Sleutelbeheer	14	5				1,3
5.12	12.4.2	Beschermen van informatie in logbestanden	12	4	2	1		1,6
5.13	13.1.1	Beheersmaatregelen voor netwerken	2	7	9	1		2,5
5.14	13.1.2	Beveiliging van netwerkdiensten	7	9	3			1,8
5.15	13.1.3	Scheiding in netwerken.	4	8	7			2,2
5.16	13.2.3	Elektronische berichten	6	10	3			1,8
5.17	14.1.3	Transacties van toepassingen beschermen	10	7	2			1,6

Dit cluster scoort gemiddeld. Opvallend is dat de (digitaal) sleutelbeheer onder de maat scoort.

2.8 Controle en Logging

Nr.	ISO27002	Statement	niveau 1	niveau 2	niveau 3	niveau 4	niveau 5	Gem
6.1	9.2.5	Beoordeling van toegangsrechten van gebruikers.	7	10	2			1,7
6.2	12.4.1	Gebeurtenissen registreren	8	10	1			1,6
6.3	12.4.3	Logbestanden van beheerders en operators	9	9	1			1,6
6.4	14.2.7	Uitbestede softwareontwikkeling	7	12				1,6
6.5	14.2.8	Testen van systeembeveiliging	13	6				1,3
6.6	14.2.9	Systeemacceptatietests	6	9	2	2		2,0

6.7	15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	12	5	2			1,5
6.8	16.1.7	Verzamelen van bewijsmateriaal	14	4		1		1,4
6.9	18.2.2	Naleving van beveiligingsbeleid en –normen	10	9				1,5
6.10	18.2.3	Beoordeling van technische naleving	11	7	1			1,5

Dit cluster scoort ver onder de maat. Registratie van informatie zal sector breed aangepakt moeten worden.

Bijlage 1: Framework informatiebeveiliging en privacy in het mbo