Normenkader Informatiebeveiliging MBO

IBBDOC2

saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

Verantwoording

Bron:

SURFaudit toetsingskader
Stichting SURF
Februari 2015

Met dank aan:

Maturity Werkgroep SURFibo:

- Hans Alfons (Vrije Universiteit)
- Ludo Cuijpers (saMBO-ICT en Kennisnet)
- Bart van den Heuvel (Universiteit Maastricht)
- Alf Moens (SURF)
- Menno Nonhebel (KNAW)
- Anita Polderdijk-Rijntjes (Christelijke Hogeschool Windesheim)
- Rene Ritzen (Universiteit Utrecht)
- Ron Veldhoen (Universiteit Twente)

SURFibo

Het SURF Informatie Beveiligers Overleg is een community of practice binnen SURF samenwerkingsorganisatie met als doelen het actief stimuleren van en richting geven aan informatiebeveiliging binnen het hoger onderwijs en onderzoek (universiteiten, hogescholen, wetenschappelijk onderzoek en universitair medische centra). Dat wordt bereikt door het bevorderen van de samenwerking tussen informatiebeveiligers/kwartiermaker IB en het leveren van praktisch bruikbare adviezen.
Voor meer informatie zie www.surfibo.nl

Bewerkt door:

Kennisnet / saMBO-ICT

Auteurs

Hans Hoogduijn (ID College)
Victor Hunnik (Grafisch Lyceum Rotterdam)
Ludo Cuijpers (Leeuwenborgh)
Januari 2015

Sommige rechten voorbehouden

Inhoudsopgave

Verantwoording en toelichting

Toelichting

Dit document is een technische beschrijving van de gekozen statements en beheersmaatregelen uit het ISO27002 normenkader. Dit normenkader is de basis voor (o.a.) het toetsingskader informatiebeveiliging van de MBO sector. Het document (beschikbaar begin 2015) “MBO Toetsingskader Informatiebeveiligingsbeleid” (DOCIBB 2) bevat een uitvoerige toelichting op het normenkader en het gebruikte referentiekader.
Gekozen is voor de clusterindeling van het Hoger Onderwijs (HO: universiteiten en hogescholen) die ontwikkeld door SURFibo.

Aanpak in 6 fasen

Dit document) heeft een zestal fasen doorlopen:

1. SURFibo heeft in overleg met CIO platform en het CIO beraad een 88-tal statements (versie 2008) geselecteerd uit het ISO27002 normenkader.
2. De Taskforce Informatiebeveiliging heeft besloten het normenkader, ISO27002, en de selectie, gemaakt door SURFibo, over te nemen voor de MBO sector.
3. De werkgroep normenkader heeft het “SURF normen- en evidence kader” bewerkt voor de MBO sector (versie 0.1).
4. Versie 0.1 is voorgelegd aan de SURFibo ter controle en goedkeuring (versie 0.2).
5. Versie 0.2 is voorgelegd aan de Taskforce Informatiebeveiliging ter goedkeuring (versie 1.0).
6. Versie 1.0 is voorgelegd aan de het Ministerie van Onderwijs en Wetenschappen ter goedkeuring (versie 2.0).

Opbouw

Dit normenkader (versie 2013) bevat 82 statements verdeelt over de volgende clusters:

Cluster 1: Beleid en organisatie	20 statements
Cluster 2: Personeel, studenten en gasten	6 statements
Cluster 3: Ruimten en apparatuur	15 statements
Cluster 4: Continuïteit	14 statements
Cluster 5: Toegangsbeveiliging	17 statements
Cluster 6: Controle en logging	10 statements

Deze indeling wordt consequent gehanteerd in:

- De Quick Reference Guide MBO set ISO27002, een handzame samenvatting van het normenkader;
- Cluster ISO27002 MBO norm, een verantwoording van de gekozen statements met een toelichting op de afwijking van de HO sector;
- Clusters ISO 27002 MBO audit, de bewijsvoering om het volwassenheidsniveau van een MBO instelling aan te tonen.

De bijlagen zijn ook in Excel beschikbaar (site saMBO-ICT of Kennisnet).

Quick Reference Guide MBO set ISO27002

MBO audit - clusterindeling - ISO27002-2013

1: Beleid en Organisatie

Nr. cluster 1		ISO27002	Statement
1	1.1	5.1.1.1	**Beleidsregels voor informatiebeveiliging:** Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd en goedgekeurd door het bestuur.
1	1.2	5.1.1.2	**Beleidsregels voor informatiebeveiliging**: Het door het bestuur vastgestelde Informatiebeveiligingsbeleid wordt gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.
1	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.
1	1.4	6.1.1	**Beoordeling van het informatiebeveiligingsbeleid:** Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen
1	1.5	6.1.5	**Informatiebeveiliging in projectbeheer:** Informatiebeveiliging behoort aan de orde te komen in projectbeheer, ongeacht het soort project.
1	1.6	6.2.1.1	**Beleid voor mobiele apparatuur:** Er dient beleid te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.
1	1.7	8.2.1	**Classificatie van informatie:** Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.
1	1.8	8.2.2	**Informatie labelen:** Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.
1	1.9	10.1.1.1	**Beleid inzake het gebruik van crypto grafische beheersmaatregelen:** Ter bescherming van informatie behoort een beleid voor het gebruik van crypto grafische beheersmaatregelen te worden ontwikkeld.
1	1.10	10.1.1.2	**Beleid inzake het gebruik van crypto grafische beheersmaatregelen:** Ter bescherming van informatie zijn er tools of applicaties aanwezig waarmee het beleid voor het gebruik van crypto grafische beheersmaatregelen wordt geïmplementeerd.
1	1.11	11.2.5	**Verwijdering van bedrijfsmiddelen:** Apparatuur, informatie en software behoren niet van de locatie te worden meegenomen zonder voorafgaande goedkeuring.
1	1.12	13.2.1	**Beleid en procedures voor informatietransport:** Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.

MBO audit - clusterindeling - ISO27002-2013

1: Beleid en Organisatie

Nr. cluster 1		ISO27002	Statement
1	1.13	13.2.2	**Overeenkomsten over informatietransport:** Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.
1	1.14	14.1.1	**Analyse en specificatie van informatiebeveiligingseisen:** De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.
1	1.15	15.1.2	**Opnemen van beveiligingsaspecten in leveranciersovereenkomsten:** Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.
1	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.
1	1.17	16.1.1	**Verantwoordelijkheden en procedures:** Er zijn leidinggevende en -procedures vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.
1	1.18	16.1.2	**Rapportage van informatiebeveiligingsgebeurtenissen:** Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.
1	1.19	18.1.3	**Beschermen van registraties:** Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.
1	1.20	18.1.4	**Privacy en bescherming van persoonsgegevens:** Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.

MBO audit - clusterindeling - ISO27002-2013

2: Personeel, studenten en gasten

Nr. cluster 2		ISO27002	Statement
2	2.1	7.1.2	**Arbeidsvoorwaarden:** De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden.
2	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.
2	2.3	9.2.6	**Toegangsrechten intrekken of aanpassen:** De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.
2	2.4	11.2.9	**'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.
2	2.5	13.2.4	**Vertrouwelijkheids- of geheimhoudingsovereenkomst:** Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.
2	2.6	16.1.3	**Rapportage van zwakke plekken in de informatiebeveiliging:** Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.

MBO audit - clusterindeling - ISO27002-2013

3: Ruimten en apparatuur

Nr. cluster 3		ISO27002	Statement
3	3.1	6.2.1.2	**Beleid voor mobiele apparatuur:** Er dienen beveiligingsmaatregelen te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beperken.
3	3.2	8.3.2	**Verwijderen van media:** Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.
3	3.3	11.1.1	**Fysieke beveiligingszone:** Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten.
3	3.4	11.1.2	**Fysieke toegangsbeveiliging:** Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.
3	3.5	11.1.3	**Kantoren, ruimten en faciliteiten beveiligen:** Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.
3	3.6	11.1.4	**Beschermen tegen bedreigingen van buitenaf:** Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.
3	3.7	11.1.5	**Werken in beveiligde gebieden:** Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast.
3	3.8	11.1.6	**Laad- en loslocatie:** Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van informatie verwerkende faciliteiten om onbevoegde toegang te vermijden.
3	3.9	11.2.1	**Plaatsing en bescherming van apparatuur:** Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.
3	3.10	11.2.2	**Nutsvoorzieningen:** Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.
3	3.11	11.2.3	**Beveiliging van bekabeling:** Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen interceptie, verstoring of schade.
3	3.12	11.2.4	**Onderhoud van apparatuur:** Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.

MBO audit - clusterindeling - ISO27002-2013

3: Ruimten en apparatuur

Nr. cluster 3		ISO27002	Statement
3	3.13	11.2.6	**Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein:** Bedrijfsmiddelen die zich buiten het terrein bevinden, behoren te worden beveiligd, waarbij rekening behoort te worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.
3	3.14	11.2.7	**Veilig verwijderen of hergebruiken van apparatuur:** Alle onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.
3	3.15	12.4.4	**Kloksynchronisatie:** De klokken van alle relevante informatie verwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.

MBO audit - clusterindeling - ISO27002-2013

4: Continuïteit

Nr. cluster 4		ISO27002	Statement	#
4	1	12.1.2	**Wijzigingsbeheer:** Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.	42
4	2	12.1.4	**Scheiding van ontwikkel-, test- en productieomgevingen** Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toe-gang tot of veranderingen aan de productieomgeving te verlagen.	
4	3	12.2.1.1	**Beheersmaatregelen tegen malware:** Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd.	44
4	4	12.2.1.2	**Beheersmaatregelen tegen malware:** Er zijn geschikte procedures ingevoerd om het bewustzijn van de gebruikers te vergroten ten aanzien van het gevaar van virussen en dergelijke.	45
4	5	12.3.1.1	**Back-up van informatie:** Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt.	46
4	6	12.3.1.2	**Back-up van informatie:** Gemaakte back ups worden regelmatig getest conform het back-up beleid.	47
4	7	12.5.1	**Software installeren op operationele systemen:** Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd.	52
4	8	12.6.1	**Beheer van technische kwetsbaarheden:** Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken.	48
4	9	12.6.2	**Beperkingen voor het installeren van software:** Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.	49
4	10	14.2.6	**Beveiligde ontwikkelomgeving:** Organisaties behoren beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.	53
4	11	15.2.2	**Beheer van veranderingen in dienstverlening van leveranciers:** Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, behoren te worden, beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.	43

.	MBO audit - clusterindeling - ISO27002-2013		
4: Continuïteit			
Nr. cluster 4		**ISO27002**	**Statement**
4	**12**	**16.1.4**	**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.
4	**13**	**16.1.5**	**Respons op informatiebeveiligingsincidenten:** Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.
4	**14**	**17.1.2**	**Informatiebeveiligingscontinuïteit implementeren:** De organisatie behoort processen, procedures en beheersmaatregelen vast te stellen, te documenteren, te implementeren en te handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.
4	**15**	**17.2.1**	**Beschikbaarheid van informatie verwerkende faciliteiten:** Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.

MBO audit - clusterindeling - ISO27002-2013

5: Toegangsbeveiliging en integriteit

Nr. cluster 5		ISO27002	Statement
5	1	9.1.1	**Beleid voor toegangsbeveiliging:** Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.
5	2	9.1.2	**Toegang tot netwerken en netwerkdiensten:** Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.
5	3	9.2.1	**Registratie en afmelden van gebruikers:** Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.
5	4	9.2.2	**Gebruikers toegang verlenen:** Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.
5	5	9.2.3	**Beheren van speciale toegangsrechten:** Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.
5	6	9.2.4	**Beheer van geheime authenticatie-informatie van gebruikers:** Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces.
5	7	9.3.1	**Geheime authenticatie-informatie gebruiken:** Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatieinformatie houden aan de praktijk van de organisatie.
5	8	9.4.1	**Beperking toegang tot informatie:** Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.
5	9	9.4.2	**Beveiligde inlogprocedures:** Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.
5	10	10.1.2.1	**Sleutelbeheer:** Met betrekking tot het gebruik, de bescherming en de levensduur van crypto grafische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld.
5	11	10.1.2.2	**Sleutelbeheer:** Er wordt gebruik gemaakt van tools om crypto grafische sleutels tijdens hun gehele levenscyclus adequaat te beheren.
5	12	12.4.2	**Beschermen van informatie in logbestanden:** Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.

MBO audit - clusterindeling - ISO27002-2013

5: Toegangsbeveiliging en integriteit

Nr. cluster 5		ISO27002	Statement
5	13	13.1.1	**Beheersmaatregelen voor netwerken:** Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.
5	14	13.1.2	**Beveiliging van netwerkdiensten:** Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.
5	15	13.1.3	**Scheiding in netwerken:** Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden.
5	16	13.2.3	**Elektronische berichten**: Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd
5	17	14.1.3	**Transacties van toepassingen beschermen:** Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.

MBO audit - clusterindeling - ISO27002-2013

6: Controle en logging

Nr. cluster 6		ISO27002	Statement
6	1	9.2.5	**Beoordeling van toegangsrechten van gebruikers:** Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.
6	2	12.4.1	**Gebeurtenissen registreren:** Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.
6	3	12.4.3	**Logbestanden van beheerders en operators:** Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.
6	4	14.2.7	**Uitbestede softwareontwikkeling:** Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de organisatie.
6	5	14.2.8	**Testen van systeembeveiliging:** Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest.
6	6	14.2.9	**Systeemacceptatietests:** Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.
6	7	15.2.1	**Monitoring en beoordeling van dienstverlening van leveranciers:** Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen.
6	8	16.1.7	**Verzamelen van bewijsmateriaal:** De organisatie behoort procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.
6	9	18.2.2	**Naleving van beveiligingsbeleid en –normen:** Het management behoort regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.
6	10	18.2.3	**Beoordeling van technische naleving:** Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.

Bijlage 1: Clusters ISO27002 MBO norm

Clus-ters		ISO 27002 2013	onderwerp	ISO maatregel	Ge-splitst	HO tekst	HO uitleg	Uitleg MBO	verantwoor-ding wijziging
1	**Beleid en Organisatie - MBO norm**								
1	5	5.1.1	Beleidsregels voor informatiebe-veiliging	Ten behoeve van informatiebe-veiliging behoort een reeks be-leidsregels te worden gedefini-eerd, goedgekeurd door de direc-tie, gepubliceerd en gecommuni-ceerd aan medewerkers en rele-vante externe partijen.	1/2	Ten behoeve van informatiebe-veiliging behoort een reeks be-leidsregels te worden gedefini-eerd en goedgekeurd door het bestuur.	Er is beleid voor informatiebevei-liging door het College van Be-stuur vastgesteld, gepubliceerd en beoordeeld op basis van in-zicht in risico's, kritische be-drijfsprocessen en toewijzing van verantwoordelijkheden.	Een document met informa-tiebeveiligingsbeleid moet door de directie worden goedgekeurd en gepubli-ceerd en kenbaar worden gemaakt aan alle werkne-mers en relevante externe partijen (Er is beleid voor informatie-beveiliging door het College van Bestuur vastgesteld, gepubliceerd en beoordeeld op basis van inzicht in risico's, kritische bedrijfsprocessen en toewij-zing van verantwoordelijk-heden.)	
1	5		Beleidsregels voor informatiebe-veiliging		2/2	Het door het bestuur vastgestel-de informatiebeveiligingsbeleid wordt gepubliceerd en gecom-municeerd aan medewerkers en relevante externe partijen.	Een document met informatiebe-veiligingsbeleid moet door de directie worden goedgekeurd en gepubliceerd en kenbaar worden gemaakt aan alle werknemers en relevante externe partijen		
1	5	5.1.2	Beoordeling van het informatie-beveiligingsbeleid	Het beleid voor informatiebevei-liging behoort met geplande tus-senpozen of als zich significante veranderingen voordoen, te wor-den beoordeeld om te waarbor-gen dat het voortdurend pas-send, adequaat en doeltreffend is.	1/1	Het beleid voor informatiebevei-liging behoort met geplande tus-senpozen of als zich significante veranderingen voordoen, te wor-den beoordeeld om te waarbor-gen dat het voortdurend pas-send, adequaat en doeltreffend is.	Het informatiebeveiligingsbeleid moet met geplande tussenpozen, of zodra zich belangrijke wijzi-gingen voordoen, worden beoor-deeld om te bewerkstelligen dat het geschikt, toereikend en doel-treffend blijft. (Het in-formatiebeveiligingsbeleid wordt met geplande tussenpozen of na een belangrijke verandering in de organisatie, technische infra-structuur of een ingrijpend bevei-ligingsincident, beoordeeld om te bewerkstelligen dat het geschikt, toereikend en doeltreffend blijft.)		Tekst is net iets specifieker dan de HO uitleg die een kopie is van de ISO maatregel.

1	6	6.1.1	Beoordeling van het informatiebeveiligingsbeleid	Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen	1/1	Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	Alle verantwoordelijkheden voor informatiebeveiliging behoren duidelijk te zijn gedefinieerd. Toewijzing vindt plaats in overeenstemming met het beleid. Verantwoordelijkheden worden waar nodig aangevuld met meer gedetailleerde richtlijnen. Lokale verantwoordelijkheden, bijv. t.a.v. continuïteitsplanning, behoren duidelijk te worden gedefinieerd. Bevoegdheden zijn duidelijk gedefinieerd en gedocumenteerd.		
1	6	6.1.5	Informatiebeveiliging in projectbeheer	Informatiebeveiliging behoort aan de orde te komen in projectbeheer, ongeacht het soort project.	1/1	Informatiebeveiliging behoort aan de orde te komen in projectbeheer, ongeacht het soort project.	Informatiebeveiliging behoort te worden geïntegreerd in de projectbeheermethode(n) van de organisatie om ervoor te zorgen dat informatiebeveiligingsrisico's 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, IT, 'facility management' en andere ondersteunende processen.		
1	6	6.2.1	Beleid voor mobiele apparatuur	Beleid en ondersteunende beveiligingsmaatregelen behoren te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	1/2	Er dient beleid te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.		Er moet in het informatiebeveiligingsbeleid apart worden aangeven welk beleid er wordt gehanteerd en welke maatregelen er zijn genomen om de risico's voor het gebruik van mobiele apparatuur te beheren.	Nieuw, dus was er geen uitleg.
1	8	8.2.1	Classificatie van informatie	Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	1/1	Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	Informatie behoort te worden geclassificeerd met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie (Classificatie en bijbehorende beheersmaatregelen houden rekening met de behoefte aan het delen van informatie of het beperken ervan en de invloed van deze behoefte op de organisatie. Richtlijnen voor classificatie zijn in overeenstemming met vastgesteld toegangsbeleid.)		

1	8	8.2.2	Informatie labelen	Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	1/1	Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en ge•mplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Er behoren geschikte, samenhangende procedures te worden ontwikkeld en geïmplementeerd voor de labeling en verwerking van informatie overeenkomstig het classificatiesysteem dat de organisatie heeft geïmplementeerd. (Procedures voor labelen van informatiebedrijfsmiddelen omvat zowel fysieke als elektronische hulpmiddelen. Het gaat om uitvoer van geclassificeerde gegevens, bestanden en bestandsoverdracht. Het is een hoofdeis voor overeenkomsten waar het delen van informatie wordt vastgelegd. Waar labelen niet mogelijk is kunnen andere manieren van classificatie van informatie worden toegepast, bijvoorbeeld via procedures of metadata.)		
1	10	10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	1/2	Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld.	Er is beleid ontwikkeld en geïmplementeerd voor het gebruik van cryptografische beheersmaatregelen voor de bescherming van informatie. (Besluiten over het passend zijn van een cryptografische oplossing is onderdeel van het proces risicobeoordeling en de keuze van beheersmaatregelen: wanneer is welk type maatregel passend, voor welk doel en welk bedrijfsproces.)		
1	10		Beleid inzake het gebruik van cryptografische beheersmaatregelen		2/2	Ter bescherming van informatie zijn er tools of applicaties aanwezig waarmee het beleid voor het gebruik van crypto grafische beheersmaatregelen wordt geimplementeerd.	Er is beleid ontwikkeld en geïmplementeerd voor het gebruik van cryptografische beheersmaatregelen voor de bescherming van informatie.		

1	11	11.2.5	Verwijdering van bedrijfsmiddelen	Apparatuur, informatie en software behoren niet van de locatie te worden meegenomen zonder voorafgaande goedkeuring.	1/1	Apparatuur, informatie en software behoren niet van de locatie te worden meegenomen zonder voorafgaande goedkeuring.	Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen. Er is duidelijk vastgesteld wie vanuit welke rol toestemming hebben om apparatuur mee te nemen of buiten de locatie te gebruiken. Er zijn tijdslimieten en bij inlevering wordt gecontroleerd op de naleving daarvan. Waar nodig wordt geregistreerd wat de locatie verlaat en wanneer het weer wordt teruggebracht.		
1	13	13.2.1	Beleid en procedures voor informatietransport	Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.	1/1	Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.	Er behoren formeel beleid, formele procedures en formele beheersmaatregelen te zijn vastgesteld om de uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen. (De uitwisseling tussen organisaties is gebaseerd op formeel uitwisselingsbeleid, in lijn met uitwisselingsovereenkomsten en in overeenstemming met relevante wetgeving. Eer zijn procedures en normen vastgesteld ter bescherming van informatie die wordt uitgewisseld.)		
1	13	13.2.2	Overeenkomsten over informatietransport	Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	1/1	Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	Er behoren overeenkomsten te worden vastgesteld voor de uitwisseling van informatie en programmatuur tussen de organisatie en externe partijen.	Er behoren overeenkomsten te worden vastgesteld voor de veilige uitwisseling van informatie en programmatuur tussen de organisatie en externe partijen.	De HO tekst was te veel afgestemd op de ISO norm. Later doorgevoeren.

1	14	14.1.1	Analyse en specificatie van informatiebeveiligingseisen	De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	1/1	De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	In bedrijfseisen voor nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen behoren ook eisen voor beveiligingsmaatregelen te worden opgenomen. (Beveiligingseisen en maatregelen zijn een afspiegeling van de waarde van de informatie voor de organisatie, en de mogelijke schade als gevolg van falen of ontbreken van beveiliging.)	Beveiligingseisen en maatregelen zijn een afspiegeling van de waarde van de informatie voor de organisatie, en de mogelijke schade als gevolg van falen of ontbreken van beveiliging.	De HO tekst was te veel afgestemd op de ISO norm.Later doorvoeren.
1	15	15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.	1/1	Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leve-rancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.	In overeenkomsten met derden waarbij toegang tot, het verwerken van, communicatie van of beheer van informatie of IT-voorzieningen van de organisatie, of toevoeging van producten of diensten aan IT voorzieningen waarbij sprake is van toegang, behoren alle relevante beveiligingseisen te zijn opgenomen. (Waarborgen dat geen misverstanden bestaan tussen organisatie en derde partij, de organisatie vergewist zich ervan dat de wederzijdse aansprakelijkheid voldoende is afgedekt.)	Waarborgen dat geen misverstanden bestaan tussen organisatie en derde partij m.b.t. onder andere informatiebeveiliging, de organisatie vergewist zich ervan dat de wederzijdse aansprakelijkheid voldoende is afgedekt.	Eerste deel tekst HO is oude norm. Deze info kan weggelaten worden. Later doorvoeren.
1	15	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.	1/1	Overeenkomsten met leveranciers behoren eisen te bevatten die betrekking hebben op de informatiebeveili-gingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.	Met leveranciers die toegang hebben tot bedrijfsmiddelen van de organisatie (applicaties, systemen en/of gegevens) dienen in overeenkomsten eisen gesteld te worden aan toeleveranciers en/of samenwerkingspartners van deze leverancier. De toeleveringsketen van informatie- en communicatietechnologie omvat eveneens dienstverlening op het gebied van 'cloud computing'.		
1	16	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	1/1	Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd. (Er is een procedure voor het rapporteren van beveiligingsgebeurtenissen vastgesteld, in combinatie met een reactie- en escalatieprocedure voor incidenten, waarin de handelingen worden vastgelegd die moeten worden genomen na het ontvangen van een rapport van een beveiligingsincident.)	Er is een procedure voor het rapporteren van beveiligingsgebeurtenissen vastgesteld, in combinatie met een reactie- en escalatieprocedure voor incidenten, waarin de handelingen worden vastgelegd die moeten worden genomen na het ontvangen van een rapport van een beveiligingsincident.	Eerste deel tekst HO is oude norm. Deze info kan weggelaten worden.

1	16	16.1.1	Verantwoordelijkheden en procedures	Directieverantwoordelijkheden en -procedures behoren te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.	1/1	Er zijn leidinggevende en -procedures vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.	Er behoren leidinggevende verantwoordelijkheden en procedures te worden vastgesteld om een snelle, doeltreffende en ordelijke reactie op informatiebeveiligingsincidenten te bewerkstelligen. (Er zijn dwingende verantwoordelijkheden en procedures vastgesteld om een snelle, doeltreffende en ordelijke reactie op informatiebeveiligingsincidenten te bewerkstelligen.)	Er zijn dwingende verantwoordelijkheden en procedures vastgesteld om een snelle, doeltreffende en ordelijke reactie op informatiebeveiligingsincidenten te bewerkstelligen.	Eerste deel tekst HO is oude norm. Deze info kan weggelaten worden.
1	18	18.1.3	Beschermen van registraties	Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	1/1	Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	Om registraties te beschermen worden richtlijnen verstrekt voor het bewaren, opslaan, behandelen en verwij-deren van registraties en informatie, wordt een bewaarschema opgesteld en wordt een inventarisoverzicht van bronnen van belangrijke informatie bijgehouden.		
1	18	18.1.4	Privacy en bescherming van persoonsgegevens	Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	1/1	Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	De bescherming van gegevens en privacy wordt bewerkstelligd overeenkomstig relevante wetgeving, voorschriften en (indien van toepassing) contractuele bepalingen.	Zie pluscluster 8 voor verdere uitwerking.	

2	**Personeel, studenten en gasten - MBO norm**							
2	7	7.1.2	Arbeidsvoorwaarden	De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden.	1/1	De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden.	Als onderdeel van hun contractuele verplichting behoren werknemers, ingehuurd personeel en externe gebruikers de algemene voorwaarden te aanvaarden en te ondertekenen van hun arbeidscontract, waarin hun verantwoordelijkheden en die van de organisatie ten aanzien van informatiebeveiliging behoren te zijn vastge-legd. (Er mag een gedragscode worden gebruikt om de verantwoordelijkheden van gebruikers te dekken ten aanzien van vertrouwelijkheid, gegevensbescherming, ethiek, passend gebruik van voorzieningen enz. Inge-huurde of gedetacheerde gebruikers zijn verbonden met een externe organisatie, die op haar beurt weer verplicht kan zijn om contracten af te sluiten namens de ingehuurde persoon.)		
2	7	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.	1/1	Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewust-zijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	Alle werknemers van de organisatie en, voor zover van toepassing, ingehuurd personeel en externe gebruikers, behoren geschikte training en regelmatige bijscholing te krijgen met betrekking tot beleid en procedures van de organisatie, voor zover relevant voor hun functie. (Bewustmakingstraining, bijv. een introductieprogramma waarin de verwachtingen van de organisatie worden behandeld voordat toegang wordt verleend tot informatie of diensten. Voortgezette en/of periodieke bewustwordingsprogramma's voor relevante groepen gebruikers.)		
2	9	9.2.6	Toegangsrechten intrekken of aanpassen	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.	1/1	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.	De toegangsrechten van alle werknemers, ingehuurd personeel en externe gebruikers tot informatie en IT-voorzieningen worden geblokkeerd bij beëindiging van het dienstverband, het contract of de overeenkomst, of ze worden na wijziging aangepast. (Bij beëindiging of wijziging van een rol of functie worden de toegangsrechten beoordeeld, en indien nodig ingetrokken of gewijzigd. Het gaat om fysieke en logische toegangsmiddelen (sleutels, accounts, medewerkerskaart, abonnementen).)).		

2	11	11.2.9	'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.	1/1	Er behoort een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatie verwerkende faciliteiten te worden ingesteld.	Er behoort een "clear desk"-beleid voor papier en verwijderbare opslagmedia en een "clear screen"-beleid voor IT-voorzieningen te worden ingesteld.		
2	13	13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.	1/1	Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betref-fende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.	Eisen voor vertrouwelijkheid of geheimhoudingsovereenkomst die een weerslag vormen van de behoefte van de organisatie aan bescherming van informatie behoren te worden vastgesteld en regelmatig te worden beoordeeld. (Vertrouwelijkheidseisen (o.a. een geheimhoudingsovereenkomst) vormen een weerslag van de behoefte van de organisatie aan bescherming van informatie binnen juridisch afdwingbare voorwaarden. Denk bij die eisen aan o.a.: welke informatie, looptijd, eigendom van informatie, toegelaten gebruik, wat te doen bij inbreuk e.d.).		
2	16	16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging	Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.	1/1	Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organi-satie behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.	Van alle werknemers, ingehuurd personeel en externe gebruikers van informatiesystemen en -diensten behoort te worden geeist dat zij alle waargenomen of verdachte zwakke plekken in systemen of diensten registreren en rapporteren (Gebruikers worden geïnformeerd dat zelf testen op zwakke plekken uitgelegd kan worden als potentieel misbruik. Het zou ook schade kunnen veroorzaken en leiden tot wettelijke aansprake-lijkheid.)		

3	**Ruimten en Apparatuur - MBO norm**								
3	6	6.2.1	Beleid voor mobiele apparatuur	Beleid en ondersteunende beveiligingsmaatregelen behoren te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	2/2	Er dienen beveiligingsmaatregelen te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beperken.		Er dienen beveiligingsmaatregelen te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beperken.	Nieuw, dus was er geen uitleg. Later doorvoeren.
3	8	8.3.2	Verwijderen van Media			Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, over-eenkomstig formele procedures.	Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, over-eenkomstig formele procedures. (9.2.6 gaat over opslag voorzieningen in een apparaat bv. harde schijf. 10.7.2 is gericht op mobiele/verwijderbare media, zoals USB sticks, geheugenkaarten, externe harddisks, disks, cards, tapes.)		
3	11	11.1.1	Fysieke beveiligingszone	Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten.	1/1	Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten.	Er behoren toegangsbeveiligingen (barrières zoals muren, toegangspoorten met kaartsloten of een bemande receptie) te worden aangebracht om ruimten te beschermen waar zich informatie en IT-voorzieningen bevinden. (Denk daarbij aan serverruimte, backup-ruimte, (MER) OTAP-straat en patchruimtes (SER). Denk ook aan kasten met persoonsdossiers, afgedrukte tentamenvragen enz.)		
3	11	11.1.2	Fysieke toegangsbeveiliging	Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	1/1	Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	Beveiligde zones behoren te worden beschermd door geschikte toegangsbeveiliging, om te bewerkstelligen dat alleen bevoegd personeel wordt toegelaten. (Het gaat hier eigenlijk om een classificatie van fysieke ruimte. Er wordt een indeling in zones voorgesteld, van openbaar (publiek toegankelijk), voor studenten, voor afdelin-gen/medewerkers (kantoorruimte), voor medewerkers tbv werkzaamheden met speciale bevoegdheden (ruimte met kluis, infrastructuur, gevaarlijke stoffen).)		

3	11	11.1.3	Kantoren, ruimten en faciliteiten beveiligen	Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.	1/1	Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.	Er behoort fysieke beveiliging van kantoren, ruimten en faciliteiten te worden ontworpen en toegepast.		
3	11	11.1.4	Beschermen tegen bedreigingen van buitenaf	Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.	1/1	Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.	Er behoort fysieke bescherming tegen schade door brand, overstroming, aardschokken, explosies, oproer en andere vormen van natuurlijke of menselijke calamiteiten te worden ontworpen en toegepast.		Zie toetsingskader vanwege andere uitleg???
3	11	11.1.5	Werken in beveiligde gebieden	Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast.	1/1	Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast.	Er behoren een fysieke bescherming en richtlijnen voor werken in beveiligde ruimten te worden ontworpen en toegepast.		

3	11	11.1.6	Laad- en loslocatie	Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van informatie verwerkende faciliteiten om onbevoegde toegang te vermijden.	1/1	Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van informatie verwerkende faciliteiten om onbevoegde toegang te vermijden.	De toegangspunten zoals gebieden voor laden en lossen en andere punten waar onbevoegden het terrein kunnen betreden, worden beheerst en indien mogelijk afgeschermd van IT-voorzieningen, om onbevoegde toegang te voorkomen. (Onderwijsinstellingen zijn per definitie publiek toegankelijk. Beveiliging van laad/lospunten zijn vooral gericht op het voorkomen van diefstal van geleverde of af te voeren goederen.)		
3	11	11.2.1	Plaatsing en bescherming van apparatuur	Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.	1/1	Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.	Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van schade en storing van buitenaf en de gelegenheid voor onbevoegde toegang wordt verminderd.		
3	11	11.2.2	Nutsvoorzieningen	Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	1/1	Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	Apparatuur behoort te worden beschermd tegen stroomuitval en andere storingen door onderbreking van nutsvoorzieningen.		

3	11	11.2.3	Beveiliging van bekabeling	Voedings- en telecommunicatie-kabels voor het versturen van gegevens of die informatiedien-sten ondersteunen, behoren te worden beschermd tegen inter-ceptie, verstoring of schade.	1/1	Voedings- en telecommuni-catiekabels voor het ver-sturen van gegevens of die informatiediensten onder-steunen, behoren te worden beschermd tegen interceptie, verstoring of schade.	Voedings- en telecommunicatie-kabels die voor dataverkeer of ondersteunende informatiedien-sten worden gebruikt, behoren tegen interceptie of beschadiging te worden beschermd.		
3	11	11.2.4	Onderhoud van apparatuur	Apparatuur behoort correct te worden onderhouden om de con-tinue beschikbaarheid en integri-teit ervan te waarborgen.	1/1	Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waar-borgen.	Apparatuur behoort op correcte wijze te worden onderhouden, om te waarborgen dat deze voortdurend beschikbaar is en in goede staat verkeert.		
3	11	11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het ter-rein	Bedrijfsmiddelen die zich buiten het terrein bevinden, behoren te worden beveiligd, waarbij reke-ning behoort te worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.	1/1	Bedrijfsmiddelen die zich buiten het terrein bevinden, behoren te worden beveiligd, waarbij rekening behoort te worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.	Apparatuur buiten de terreinen behoort te worden beveiligd waarbij rekening wordt gehouden met de diverse risico's van wer-ken buiten het terrein van de organisatie. (Denk hier aan be-veiligde/beheerde werkplekken en notebooks. Mobiele devices en BYOD wordt in toegangsbeleid meegenomen.)		
3	11	11.2.7	Veilig verwijderen of hergebrui-ken van apparatuur	Alle onderdelen van de appara-tuur die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan ver-wijdering of hergebruik zijn ver-wijderd of betrouwbaar veilig zijn overschreven.	1/1	Alle onderdelen van de ap-paratuur die opslagmedia bevatten, behoren te worden geverifieerd om te waarbor-gen dat gevoelige gegevens en in licentie gegeven soft-ware voorafgaand aan ver-wijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.	Alle apparatuur die opslagmedia bevat, behoort te worden gecon-troleerd om te bewerkstelligen dat alle gevoelige gegevens en in licentie gebruikte programmatuur zijn verwijderd of veilig zijn over-schreven voordat de apparatuur wordt verwijderd. (Dit betreft informatie op zowel servers, werkplekken, beheerde/geleende notebooks, tablets, smartphones en ook eigen devices die worden hergebruikt of voor hergebruik worden afgevoerd. Maatregelen 10.7.2 is met name gericht op mobiele opslagmedia	Dit betreft informatie op zowel servers, werkplekken, beheerde/geleende note-books, tablets, smartphones en ook eigen devices die worden hergebruikt of voor hergebruik worden afge-voerd. Maatregelen met name ge-richt op mobiele opslagme-dia (cards, disks, harddisks, usb-sticks etc.).	Verwijzing naar oude maatregelen. Later doorvoeren.

							(cards, disks, harddisks, usb-sticks etc.).)		
3	12	12.4.4	Kloksynchronisatie	De klokken van alle relevante informatie verwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.	1/1	De klokken van alle relevante informatie verwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.	De klokken van alle relevante informatiesystemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met een overeengekomen nauwkeurige tijdsbron.		

4	**Continuïteit - MBO norm**								
4	12	12.1.2	Wijzigingsbeheer	Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.	1/2	Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.	Wijzigingen in IT-voorzieningen en informatiesystemen behoren te worden beheerst.		
4		12.1.4	Scheidiing van ontwikkel-, test-en productieomgevingen			Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	Het scheidingsniveau tussen productie-, test- en ontwikkelomgevingen dat nodig is om operationele problemen te voorkomen behoort te worden geïdentificeerd en geïmplementeerd.		
4	12	12.2.1	Beheersmaatregelen tegen malware	Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.	1/2	Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd.	Er worden maatregelen getroffen voor detectie, preventie en herstel om te beschermen tegen virussen en er zijn geschikte procedures ingevoerd om het bewustzijn van de gebruikers te vergroten.		

4	12		Beheersmaatregelen tegen malware		2/2	Er zijn geschikte procedures ingevoerd om het bewustzijn van de gebruikers te vergroten ten aanzien van het gevaar van virussen en dergelijke.	Er worden maatregelen getroffen voor detectie, preventie en herstel om te beschermen tegen virussen en er zijn geschikte procedures ingevoerd om het bewustzijn van de gebruikers te vergroten.		
4	12	12.3.1	Back-up van informatie	Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	1/2	Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt.	Er worden back-up kopieën van informatie en programmatuur gemaakt en regelmatig getest overeenkomstig het vastgestelde back-upbeleid.		
4	12		Back-up van informatie		2/2	Gemaakte back ups worden regelmatig getest conform het back-up beleid.	Er worden back-up kopieën van informatie en programmatuur gemaakt en regelmatig getest overeenkomstig het vastgestelde back-upbeleid.		

4	12	12.5.1	Software installeren op operationele systemen	Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd.	1/2	Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïm-plementeerd.	De integriteit van operationele systemen dient gewaarborgd te blijven. Alleen dan kan informatieverwerking betrouwbaar plaatsvinden.		
4	12	12.6.1	Beheer van technische kwetsbaarheden	Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken.	1/2	Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken.	Er behoort tijdig informatie te worden verkregen over technische kwetsbaarheden van de gebruikte informatiesystemen. De mate waarin de organisatie blootstaat aan dergelijke kwetsbaarheden behoort te worden geëvalueerd en er behoren geschikte maatregelen te worden genomen voor behandeling van daarmee samenhangende risico's.		
4	12	12.6.2	Beperkingen voor het installeren van software	Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.	1/2	Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.	De organisatie behoort een strikt beleid te definiëren en ten uitvoer te brengen met betrekking tot de soorten software die gebruikers mogen installeren.		
4	14	14.2.6	Beveiligde ontwikkelomgeving	Organisaties behoren beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.	1/2	Organisaties behoren beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.	Een beveiligde ontwikkelomgeving omvat personen, processen en technologie die in verband staan met systeemontwikkeling en integratie.		
4	15	15.2.2	Beheer van veranderingen in dienstverlening van leveranciers	Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, behoren te worden, beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico’s.	1/2	Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, behoren te worden, beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico’s.	Wijzigingen in de dienstverlening door derden, waaronder het bijhouden en verbeteren van bestaande beleidslijnen, procedures en maatregelen voor informatiebeveiliging, worden beheerd, waarbij rekening wordt gehouden met de onmisbaarheid van de betrokken bedrijfssystemen en -processen en met heroverweging van risico's.		

4	16	16.1.4	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.	1/1	Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiliging incidenten.	Het contactpunt beoordeelt gebeurtenissen volgens het classificatieschema en prioriteert deze indien het incidenten zijn. Classificatie en prioritering worden in detail in een verslag vastgelegd. Een responseteam (indien in de organisatie aanwezig) ontvangt deze rapportage en bevestigt of herbeoordeelt het besluit.		
4	16	16.1.5	Respons op informatiebeveiligingsincidenten	Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.	1/1	Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumen-teerde procedures.	Op informatiebeveiligingsincidenten behoort te worden gereageerd door een aangewezen contactpunt en andere relevante personen van de organisatie of externe partijen.		
4	17	17.1.2	Informatiebeveiligingscontinuïteit implementeren	De organisatie behoort processen, procedures en beheersmaatregelen vast te stellen, te documenteren, te implementeren en te handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.	1/2	De organisatie behoort processen, procedures en beheersmaatregelen vast te stellen, te documenteren, te implementeren en te handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.	Ook tijdens ongunstige situaties, zoals tijdens crises en rampen, dient de kwaliteit van de informatiebeveiliging overeenkomstig de gestelde eisen te blijven functioneren. Daartoe worden maatregelen (in de vorm van pro-cessen, procedures en beheersmaatregelen, mogelijk in calamiteits- of continuïteitsplan) getroffen om de kwaliteit van de beveiliging tijdens ongunstige situaties op het vastgestelde niveau te handhaven.		

5	**Toegangsbeveiliging en integriteit - MBO norm**								
5	9	9.1.1	Beleid voor toegangsbeveiliging	Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	1/1	Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	Er behoort toegangsbeleid te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfseisen en beveiligingseisen voor toegang.		
5	9	9.1.2	Toegang tot netwerken en netwerkdiensten	Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	1/1	Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	Een beleid voor het gebruik van netwerken en netwerkdiensten behoort te worden geformuleerd.		
5	9	9.2.1	Registratie en afmelden van gebruikers	Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	1/1	Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	Er behoren formele procedures voor het registreren en afmelden van gebruikers te zijn vastgesteld om het verlenen en intrekken van toegangsrechten tot alle informatiesystemen en –diensten mogelijk te maken.		

5	9	9.2.2	Gebruikers toegang verlenen	Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	1/1	Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	Een procedure voor het verlenen (toekennen, intrekken) van autorisaties aan gebruikers voor alle systemen en diensten is beschreven. Deze procedure is vastgesteld en aantoonbaar in gebruik.		
5	9	9.2.3	Beheren van speciale toegangsrechten	Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.	1/1	Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.	De toewijzing en het gebruik van speciale bevoegdheden behoren te worden beperkt en beheerst.		
5	9	9.2.4	Beheer van geheime authenticatie-informatie van gebruikers	Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces.	1/1	Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces.	De toewijzing van wachtwoorden behoort met een formeel beheerproces te worden beheerst.		
5	9	9.3.1	Geheime authenticatie-informatie gebruiken	Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatie informatie houden aan de praktijk van de organisatie.	1/1	Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatieinformatie houden aan de praktijk van de organisatie.	Gebruikers dienen op juiste wijze gebruik van te maken van de aan hen toegekende wachtwoorden, pincodes, tokens of certificaten. Dit wordt bereikt door gebruikers te informeren over de wijze waarop zij met deze geheime authenticatieinformatie dienen om te gaan.		

5	9	9.4.1	Beperking toegang tot informatie	Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.	1/1	Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.	Toegang tot informatie en functies van toepassingssystemen door gebruikers en ondersteunend personeel behoort te worden beperkt overeenkomstig het vastgestelde toegangsbeleid.		
5	9	9.4.2	Beveiligde inlogprocedures	Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.	1/1	Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.	Toegang tot besturingssystemen behoort te worden beheerst met een beveiligde inlogprocedure.		
5	10	10.1.2	Sleutelbeheer	Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld en geïmplementeerd.	1/2	Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld.	Er is sleutelbeheer vastgesteld ter ondersteuning van het gebruik van cryptografische technieken binnen de organisatie.		
5	10				2/2	Er wordt gebruik gemaakt van tools om cryptografische sleutels tijdens hun gehele levenscyclus adequaat te beheren.	Er is sleutelbeheer vastgesteld ter ondersteuning van het gebruik van crypto grafische technieken binnen de organisatie.		
5	12	12.4.2	Beschermen van informatie in logbestanden	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	1/1	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen inbreuk en onbevoegde toegang.		

5	13	13.1.1	Beheersmaatregelen voor netwerken	Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	1/1	Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Er behoren beheersmaatregelen te worden geïmplementeerd om de veiligheid van informatie in netwerken te waarborgen en aangesloten diensten tegen onbevoegde toegang te beschermen.		
5	13	13.1.2	Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	1/1	Beveiligingsmechanismen, dienstverleningsniveaus en beheer eisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	Tot netwerkdiensten behoren het leveren van aansluitingen, particuliere netwerkdiensten, netwerken met toegevoegde waarde en beheerde netwerkbeveiligingsoplossingen zoals firewalls en inbraakdetectiesystemen.		
5	13	13.1.3	Scheiding in netwerken	Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden.	1/1	Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden.	Groepen informatiediensten, gebruikers en informatiesystemen behoren op netwerken te worden gescheiden.		

5	13	13.2.3	Electronische berichten			Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd	Informatie die een rol speelt bij elektronische berichtuitwisseling op geschikte wijze beschermd.		
5	14	14.1.3	Transacties van toepassing-beschermen			Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.	De omvang van de aangenomen beheersmaatregelen behoort in overeenstemming te zijn met het niveau van het risico dat samenhangt met elke transactievorm van toepassingen. Transacties moeten mogelijk voldoen aan de eisen van wet- en regelgeving van het rechtsgebied waarin de transactie is gegenereerd, verwerkt, uitgevoerd of opgeslagen.		

6	**Controle en Logging - MBO norm**							
6	9	9.2.5	Beoordeling van toegangsrechten van gebruikers	Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.	1/1	Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.	De directie behoort de toegangsrechten van gebruikers regelmatig te beoordelen in een formeel proces. (Het gaat om periodieke toetsing van toegekende toegangsrechten om de toegang tot gegevens en diensten te kunnen beheersen; niet alleen uitgeven maar ook intrekken, gelet op verhuizingen, speciale bevoegdheden (kortere periodes en inhoudelijk), speciale bevoegdheden.		
6	12	12.4.1	Gebeurtenissen registreren	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	1/1	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen behoren te worden vast-gelegd in audit-logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole. (Audit logbestanden van o.m. de volgende gegevens: gebruikers-ID's, data, tijdstippen en details van in- en uitloggen, identiteit device/locatie, geslaagde/geweigerde pogingen om toegang te krijgen, gebruik van speciale bevoegdheden en dergelijke. Waar mogelijk behoren systeembeheerders geen toestemming te hebben om logbestanden van hun eigen activiteiten te wissen of deactiveren.)		

6	12	12.4.3	Logbestanden van beheerders en operators	Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.	1/1	Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.	Activiteiten van systeemadministrators en systeemoperators behoren in logbestanden te worden vastgelegd. (In logbestanden wordt onder meer vastgelegd: tijdstip succes/storing gebeurtenis, welke beheerder of operator, welke processen.)		
6	14	14.2.7	Uitbestede softwareontwikkeling	Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de organisatie.	1/1	Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de organisatie.	Uitbestede ontwikkeling van programmatuur behoort onder supervisie te staan van en te worden gecontroleerd door de organisatie. (Aandachtspunten: licentieovereenkomsten, intellectueel eigendom (broncode), certificatie, kwaliteits- en continuïteitsborging, recht op audit, contractuele eisen voor de kwaliteit en beveiligingsfunctionaliteit van de broncode, testen.)		

6	14	14.2.8	Testen van systeembeveiliging	Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest.	1/1	Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest.	Tijdens de ontwikkelprocessen zijn voor nieuwe en geactualiseerde systemen uitvoerige tests en verificatie nodig, met inbegrip van het opstellen van een gedetailleerd schema van activiteiten en tests van inputs en verwachte outputs onder diverse omstandigheden. De omvang van het testen behoort in verhouding te staan tot de belangrijkheid en de aard van het systeem.		
6	14	14.2.9	Systeemacceptatietests	Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.	1/1	Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.	Er zijn aanvaardingscriteria vastgesteld voor nieuwe informatiesystemen, upgrades en nieuwe versies en er wordt een geschikte acceptatietest van het systeem of de systemen uitgevoerd alvorens deze worden overgezet naar de productieomgeving.		
6	15	15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen.	1/1	Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen.	De diensten, rapporten en registraties die door de derde partij worden geleverd, worden regelmatig gecontroleerd en beoordeeld en er worden regelmatig audits uitgevoerd. (Controle en beoordeling van dienstverlening door derden behoort te waarborgen dat de voorwaarden van de overeenkomsten voor de informatiebeveiliging worden nageleefd, dat incidenten en problemen goed worden afgehandeld. Er is een proces voor het beheer van de dienstverlening (prestatieniveaus, DVO's, audittrails, change- en problemmanagement))		

6	16	16.1.7	Verzamelen van bewijsmateriaal	De organisatie behoort procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	1/1	De organisatie behoort procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	Waar een vervolgprocedure tegen een persoon of organisatie na een informatiebeveiligingsincident juridische maatregelen omvat (civiel of strafrechtelijk), behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd. (Implementatierichtlijnen uit 27002 norm: Houdt rekening met: de toelaatbaarheid van het bewijs in een rechtszaak, de kwaliteit en volledigheid van het bewijsmateriaal, waarborgen dat informatiesystemen in overeenstemming zijn met gepubliceerde normen of praktijkcodes voor het genereren van toelaatbaar bewijsmateriaal, de kwaliteit en volledigheid van de beheersmaatregelen die zijn genomen om het verkregen bewijsmateriaal correct en consequent te beschermen.)	Houdt rekening met: de toelaatbaarheid van het bewijs in een rechtszaak, de kwaliteit en volledigheid van het bewijsmateriaal, waarborgen dat informatiesystemen in overeenstemming zijn met gepubliceerde normen of praktijkcodes voor het genereren van toelaatbaar bewijsmateriaal, de kwaliteit en volledigheid van de beheersmaatregelen die zijn genomen om het verkregen bewijsmateriaal correct en consequent te beschermen.	Vermelding van ISO norm onnodig. Eventueel later aanpassen.
6	18	18.2.2.	Naleving van beveiligingsbeleid en -normen	Het management behoort regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	1/1	Het management behoort regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	Managers behoren te bewerkstelligen dat alle beveiligingsprocedures die binnen hun verantwoordelijkheid vallen correct worden uitgevoerd om naleving te bereiken van beveiligingsbeleid en -normen. (Implementatierichtlijnen uit 27002 norm: Managers behoren regelmatig te beoordelen of de informatieverwerking binnen hun verantwoordelijkheidsgebied voldoet aan het geldende beveiligingsbeleid, normen en andere beveiligingseisen.)	Managers behoren regelmatig te beoordelen of de informatieverwerking binnen hun verantwoordelijkheidsgebied voldoet aan het geldende beveiligingsbeleid, normen en andere beveiligingseisen.	Vermelding van ISO norm onnodig. Eventueel later aanpassen.
6	18	18.2.3	Beoordeling van technische naleving	Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	1/1	Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	Informatiesystemen behoren regelmatig te worden gecontroleerd op naleving van implementatie van beveiligingsnormen. (implementatierichtlijnen uit 27002 norm: Controle automatisch of handmatig; ervaren sys-teemtechnicus; technische rapportage; Eventueel penetratieproeven of kwetsbaarheidsbeoordelingen (gepland, gedocumenteerd en herhaalbaar).	Controle automatisch of handmatig; ervaren systeemtechnicus; technische rapportage; Eventueel penetratieproeven of kwetsbaarheidsbeoordelingen (gepland, gedocumenteerd en herhaalbaar).	Vermelding van ISO norm onnodig. Eventueel later aanpassen