Handleiding Risicomanagement

IBPDOC29

GEBRUIKERSGROEP IBP IN HET MBO

Kennisnet SURF saMBO-ICT

Verantwoording

Opdrachtgever

Kennisnet / saMBO-ICT

Dit document is geschreven voor IT managers, IT security officers, Information officers binnen de mbo sector. Dit document geeft een handleiding voor de inrichting en uitvoering van risicomanagement binnen de mbo Sector en handreiking voor de beoordeling van IT risico's. Het document is gemaakt in navolging op de 5 daagse mbo masterclasses.
In dit document wordt allereerst ingegaan op de inrichting van de Governance omtrent risicomanagement in het algemeen. Vervolgens wordt de uitvoering van de risico- en controlecyclus verder toegelicht. In het laatste hoofdstuk wordt een aanzet gegeven tot het beoordelen van de IT risico's binnen de mbo sector.

Auteurs

Maurits Toet (Cerrix BV)
Ludo Cuijpers (Leeuwenborgh)
Esther van der Hei (Nimeto Utrecht)
Mei 2015

Sommige rechten voorbehouden

Inhoudsopgave

1. Risico's in de mbo sector

1.1 Toelichting

De Taskforce heeft er voor gekozen om geen uitputtende risicoanalyses uit te voeren maar te werken vanuit het normenkader met als basis ISO 270001 en de checklist ISO 27002, de zogenaamde Code voor Informatiebeveiliging. ISO 27001 is wereldwijd tot stand gekomen door bij, vooral, multinationals te inventariseren welke risico's benoemd konden worden op het gebied van informatiebeveiliging en vervolgens zijn daar beheersmaatregelen bij benoemd zodat de risico's gemitigeerd kunnen worden. In feite zijn dan de risico's die samenhangen met informatiebeveiliging en een groot deel van de privacy risico's afgedekt in.
Dit betekent voor een mbo instelling dat de meest voorkomende risico's op het gebied van informatiebeveiliging en voor een groot deel op het gebied van privacy zijn afgedekt indien de beheersmaatregelen die voortvloeien uit ISO27002 in voldoende mate zijn toegepast.

1.2 Aanpak taskforce

De risico onderbouwing is door de Taskforce in 4 stappen opgepakt:

Stap 1: Er zijn 79 "normen" uit het ISO 27002 normenkader overgenomen die de informatiebeveiliging en een deel van de privacy risico's afdekken die binnen de mbo sector relevant zijn (IBPDOC2A: Normenkader Informatiebeveiliging mbo).

Stap 2: Deze normen zijn vertaald in 85 statements (een zestal normen zijn gesplitst in 2 statements) waar vervolgens bewijslast (evidence) aan is toegevoegd (IBPDOC3: Toetsingskader Informatiebeveiliging).

Stap 3: Tijdens de masterclasses IBP hebben alle cursisten 10 risico's benoemd binnen de groepen:

1. Beleid en personeel;
   1.1. Informatiebeveiliging;
   1.2. Privacy;
2. Toegang tot applicaties en data;
3. IT infrastructuur en externe verbindingen;
4. Examinering.

Dit leverde dus 400 risico's op met veel overlap. In totaal leidde dit tot 78 "unieke risico's".
Als volgt onderverdeeld:

1. Beleid en personeel: 29 risico's
2. Toegang tot applicaties en data: 28 risico's
3. IT infrastructuur en externe verbindingen: 27 risico's
4. Examinering: 4 risico's

(Zie bijlage 1: Overzicht risico's en maatregelen ISO27002/2013)

Stap 4: De risico's zijn vervolgens geplot (gekoppeld) aan de ISO 27002 normen.
(Zie bijlage 1: Overzicht risico's en maatregelen ISO27002/2013)
Deze normen kunnen, indien gewenst, weer "vertaald" worden naar het mbo normen en toetsingskader. Als service is bij 1.3 een "vertaaltabel" toegevoegd.

In bijlage 2 is een handleiding risicomanagement toegevoegd. Weliswaar moet een ibp-manager in staat zijn om een risico analyse op ibp gebied uit te voeren, maar het is niet zijn taak om alle mbo risico's in kaart te brengen.

1.3 Bevindingen

Er zijn in totaal door de deelnemers aan de masterclasses informatiebeveiliging ruim 400 risico's benoemd. Daaruit komen als belangrijkste risico's naar voren:

1. Toegangsbeveiliging;

2. Examinering (toets constructie ,toets afname en toets registratie);
3. Onrechtmatig gebruik van studentengegevens (m.n. zorgdossiers);
4. Onrechtmatig gebruik van medewerkersgegevens (m.n. gesprekscyclus dossier) en
5. Datalekken.

Deze risico's worden afdoende verkleind d.m.v. de toetsingskaders Informatiebeveiliging, examineren en privacy.

2. Praktische invulling

2.1 Beperkingen in de aanpak

Er is gekozen om het risicomanagement, binnen informatiebeveiliging en privacy, op een eenvoudige manier aan te pakken. In de bijlage zijn ruim 70 risico's beschreven die voor een groot deel van toepassing zijn voor iedere mbo instelling. Indien vanuit het CvB, het management en/of de accountant, de vraag wordt gesteld naar een "mbo specifieke" risicoanalyse dan kan er een keuze worden gemaakt uit de risico's zoals vermeld in de bijlage en eventueel aangevuld met "instelling specifieke" risico's.

2.2 Niet gebruikte normen uit ISO27002

De mbo sector maakt, in navolging van de ho sector, gebruik van 79 van de 114 normen uit het ISO27002 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	

Met ander woorden 35 normen worden niet gebruikt. In de bijlage zijn ze wel benoemd maar met geen verwijzing naar het mbo normenkader (gehanteerde tekst: **Geen mbo statement**). In 2017 is saMBO-ICT en Kennisnet voornemens om ook deze normen te gaan hanteren.

Bijlage 1 Overzicht risico's en maatregelen ISO27002/2013

Nr	Risicobeschrijving	Categorie	Mbo normenkader (ISO 27002-2013) verwijzing	Maatregelen
1	Het risico dat medewerkers en studenten onvoldoende bewust zijn van risico's met betrekking tot informatiebeveiliging door het niet beschikbaar zijn en/of onvoldoende communicatie van informatiebeveiligingsbeleid / procedures met als gevolg reputatieschade, operationele verstoringen, financiële schade.	**Beleid en personeel**	1.1 en 1.2 (ISO 5.1.1) Beleidsregels voor informatiebeveiliging. 1.3 (ISO 5.1.2) Beoordeling van het informatiebeveiligingsbeleid 1.6 en 3.1 (ISO 6.2.1) Beleid voor mobiele apparatuur 2.1 (ISO 7.1.2) Arbeidsvoorwaarden Geen mbo statement (ISO 7.2.1) Directieverantwoordelijkheden 2.2 (ISO 7.2.2) Bewustzijn, opleiding en training	1.1 en 1.2 (ISO 5.1.1) Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen. 1.3 (ISO 5.1.2) 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. 1.6 en 3.1 (ISO 6.2.1) Beleid en ondersteunende beveiligingsmaatregelen behoren te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren. 2.1 (ISO 7.1.2) De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden. Geen mbo statement (ISO 7.2.1) De directie behoort van alle medewerkers en contractanten te eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie. 2.2 (ISO 7.2.2) Alle studenten/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	Het risico dat IT medewerkers onvoldoende bekwaam zij door falende personeelsselectie en/of onvoldoende opleidingsmogelijkheden met als gevolg het niet kunnen schakelen bij veranderingen in IT omgeving van de instelling.	**Beleid en personeel**	1.4 (ISO 6.1.1) Rollen en verantwoordelijkheden bij informatiebeveiliging 2.7 (ISO 7.1.1) Screening 2.2 (ISO 7.2.2) Bewustzijn, opleiding en training.	1.4 (ISO 6.1.1) Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen. 2.7 (ISO 7.1.1) Verificatie van de achtergrond van alle kandidaten voor een dienstverband behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's te zijn. 2.2 (ISO 7.2.2) Alle studenten/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.
3	Het risico dat IT processen niet juist/volledig/tijdig worden uitgevoerd door onvoldoende afstemming van verantwoordelijkheden voor IT werkzaamheden tussen afdelingen/uitbestedingspartijen met als gevolg operationele verstoringen.	**Beleid en personeel**	1.4 (ISO 6.1.1) Rollen en verantwoordelijkheden bij informatiebeveiliging 1.21 (ISO 6.1.2) Scheiding van taken Geen mbo statement (ISO 6.1.3) Contact met overheidsinstanties Geen mbo statement (ISO 6.1.4) Contact met speciale belangengroepen 1.5 (ISO 6.1.5) Verantwoordelijkheden Informatiebeveiliging in projectbeheer	1.4 (ISO 6.1.1) Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen. 1.21 (ISO 6.1.2). Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen. Geen mbo statement (ISO 6.1.3) Organisaties behoren procedures te hebben die aangeven wanneer en door wie contact behoort te worden opgenomen met overheidsinstanties (bijv. politie, regelgevende organen, toezichthouders) en hoe geïdentificeerde informatiebeveiligingsincidenten tijdig behoren te worden gerapporteerd (bijv. indien het vermoeden bestaat dat mogelijk wetgeving is overtreden). Geen mbo statement (ISO 6.1.4) Er behoren passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en/of professionele organisaties te worden onderhouden. 1.5 (ISO 6.1.5) 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.
4	Het risico dat de instelling niet voldoet aan privacy wetgeving door onvoldoende controle hierop met als gevolg rechtzaken, claims, reputatieschade.	**Beleid en personeel**	1.1 en 1.2 (ISO 5.1.1) Beleidsregels voor informatiebeveiliging. 1.3 (ISO 5.1.2) Beoordeling van het informatiebeveiligingsbeleid Geen mbo statement (ISO 18.1.1) Vaststellen van toepasselijke wetgeving en contractuele eisen 1.19 (ISO 18.1.3) Beschermen van registraties 1.20 (ISO 18.1.4) Privacy en bescherming van persoonsgegevens	1.1 en 1.2 (ISO 5.1.1) Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen. 1.3 (ISO 5.1.2) 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. Geen mbo statement (ISO 18.1.1) Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen behoren voor elk informatiesysteem en de organisatie expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden. 1.19 (ISO 18.1.3) Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave. 1.20 (ISO 18.1.4) Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.

Nr	Risicobeschrijving	Categorie	Mbo normenkader (ISO 27002-2013) verwijzing	Maatregelen
5	Het risico dat wijzigingen niet juist, volledig, tijdig worden ontwikkeld door ontbrekende processen met als gevolg foutieve wijzigingen en operationele verstoringen	**Beleid en personeel**	4,1 (ISO 12.1.2) Wijzigingsbeheer 4.2 (ISO 12.1.4) Scheiding van ontwikkel-, test- en productieomgevingen Geen mbo statement (ISO 14.2.1) Beleid voor beveiligd ontwikkelen Geen mbo statement (ISO 14.2.2) Procedures voor wijzigingsbeheer met betrekking tot systemen Geen mbo statement (ISO 14.2.3) Technische beoordeling van toepassingen na wijzigingen besturingsplatform Geen mbo statement (ISO 14.2.4) Beperkingen op wijzigingen aan softwarepakketten 4.10 (ISO 14.2.6) Beveiligde ontwikkelomgeving 6.4 (ISO 14.2.7) Uitbestede softwareontwikkeling 6.5 (ISO 14.2.8) Testen van systeembeveiliging 6.6 (ISO 14.2.9) Systeemacceptatietests	4,1 (ISO 12.1.2) Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst. 4.2 (ISO 12.1.4) Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen. Geen mbo statement (ISO 14.2.1). Voor het ontwikkelen van software en systemen behoren regels te worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie te worden toegepast. Geen mbo statement (ISO 14.2.2) Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer. Geen mbo statement (ISO 14.2.3) Als besturingsplatforms zijn veranderd, behoren bedrijf kritische toepassingen te worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie. Geen mbo statement (ISO 14.2.4) Wijzigingen aan softwarepakketten behoren te worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen behoren strikt te worden gecontroleerd. 4.10 (ISO 14.2.6) 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. 6.4 (ISO 14.2.7) Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de organisatie. 6.5 (ISO 14.2.8) Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest. 6.6 (ISO 14.2.9) Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.
6	Het risico dat changes / releases onvoldoende getest worden door onvoldoende inrichting van OTAP omgeving met als gevolg operationele verstoringen en financiële schade.	**Beleid en personeel**	4,1 (ISO 12.1.2) Wijzigingsbeheer 4.2 (ISO 12.1.4) Scheiding van ontwikkel-, test- en productieomgevingen	4,1 (ISO 12.1.2) Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst. 4.2 (ISO 12.1.4) Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.
7	Het risico dat inzicht op de samenhang van systemen/applicaties en op ontwerpbeslissingen ontbreekt door ontbrekende/onvoldoende IT beheerdocumentatie met als gevolg operationele verstoringen bij het doorvoeren van systeemwijzigingen.	**Beleid en personeel**	Geen mbo statement (ISO 12.1.1) Gedocumenteerde bedieningsprocedures 4,1 (ISO 12.1.2) Wijzigingsbeheer	Geen mbo statement (ISO 12.1.1) Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben. 4,1 (ISO 12.1.2) Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.
8	Het risico op onvolledige dienstverlening door leveranciers door een onvolledige/onjuiste SLA en/of onvoldoende monitoring met als gevolg operationele verstoringen.	**Beleid en personeel**	Geen mbo statement (ISO 15.1.1) Informatiebeveiligingsbeleid voor leveranciersrelaties 1.15 (ISO 15.1.2) Opnemen van beveiligingsaspecten in leveranciersovereenkomsten 1.16 (ISO 15.1.3) Toeleveringsketen van informatie- en communicatietechnologie. 6.7 (ISO 15.2.1) Monitoring en beoordeling van dienstverlening van leveranciers 4.11 (ISO 15.2.2) Beheer van veranderingen in dienstverlening van leveranciers	Geen mbo statement (ISO 15.1.1) Met de leverancier behoren de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, te worden overeengekomen en gedocumenteerd. 1.15 (ISO 15.1.2) 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. 1.16 (ISO 15.1.3) 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. 6.7 (ISO 15.2.1) Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen. 4.11 (ISO 15.2.2). 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.
9	Het risico dat adhoc oplossingen worden toegepast doordat IT-beleid niet helder is met als gevolg financiële schade en ontevredenheid doordat aangeschafte middelen niet passen binnen de coöperatieve afspraken.	**Beleid en personeel**	1.1 en 1.2 (ISO 5.1.1) Beleidsregels voor informatiebeveiliging. 1.3 (ISO 5.1.2) Beoordeling van het informatiebeveiligingsbeleid 1.6 en 3.1 (ISO 6.2.1) Beleid voor mobiele apparatuur	1.1 en 1.2 (ISO 5.1.1) Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen. 1.3 (ISO 5.1.2) 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. 1.6 en 3.1 (ISO 6.2.1) Beleid en ondersteunende beveiligingsmaatregelen behoren te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.

Nr	Risicobeschrijving	Categorie	Mbo normenkader (ISO 27002-2013) verwijzing	Maatregelen
10	Het risico dat IT incidenten niet juist, volledig en tijdig worden geregistreerd en afgehandeld door ontbreken van procedures en/of geen monitoring van opvolging met als gevolg operationele verstoringen.	**Beleid en personeel**	1.17 (ISO 16.1.1) Verantwoordelijkheden en procedures 1.18 (ISO 16.1.2) Rapportage van (informatiebeveiligings-) gebeurtenissen 2.6 (ISO 16.1.3) Rapportage van zwakke plekken in de informatiebeveiliging 4.12 (ISO 16.1.4) Beoordeling van en besluitvorming over (informatiebeveiligings-)gebeurtenissen 4.13 (ISO 16.1.5) Respons op informatiebeveiligingsincidenten Geen mbo statement (ISO 16.1.6) Lering uit informatiebeveiligingsincidenten	1.17 (ISO 16.1.1) Directieverantwoordelijkheden en -procedures behoren te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op (informatiebeveiligings-)incidenten te bewerkstelligen. 1.18 (ISO 16.1.2) Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd. 2.6 (ISO 16.1.3) 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. 4.12 (ISO 16.1.4) Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten. 4.13 (ISO 16.1.5) Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures. Geen mbo statement (ISO 16.1.6) Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen behoort te worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.
11	Het risico dat de geleverde IT diensten niet aansluiten bij de (beveiligings)behoefte en beleid van de Business door gebrek aan regie en alignement met als gevolg hoge kosten, inefficiëntie en onvoldoende uitvoering van het beleid	**Beleid en personeel**	6.9 (ISO 18.2.2) Naleving van beveiligingsbeleid en -normen 6.10 (ISO 18.2.3) Beoordeling van technische naleving	6.9 (ISO 18.2.2) De directie 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 (ISO 18.2.3) Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.
12	Het risico dat technische beveiligingsmaatregelen door de IT beheerorganisatie op het verkeerde niveau met verkeerde prioriteit worden behandeld door ontbreken van een adequate overlegstructuur op strategisch, tactisch en operationeel niveau, met als gevolg onvoorspelbare blootstelling aan technische beveiligingsrisico's.	**Beleid en personeel**	1.4 (ISO 6.1.1) Rollen en verantwoordelijkheden bij informatiebeveiliging	1.4 (ISO 6.1.1) Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.
13	Het risico dat verstoringen en beveiligingsincidenten worden veroorzaakt door de IT beheerorganisatie zelf doordat onvoldoende kwaliteitsnormen worden gehanteerd, taken bevoegdheden en verantwoordelijkheden en procedures onvoldoende zijn beschreven en/of geïmplementeerd met als gevolg een instabiel diensten en beveiligingsniveau.	**Beleid en personeel**	1.1 en 1.2 (ISO 5.1.1) Beleidsregels voor informatiebeveiliging. 1.3 (ISO 5.1.2) Beoordeling van het informatiebeveiligingsbeleid 1.4 (ISO 6.1.1) Rollen en verantwoordelijkheden bij informatiebeveiliging 1.6 en 3.1 (ISO 6.2.1) Beleid voor mobiele apparatuur	1.1 en 1.2 (ISO 5.1.1) Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen. 1.3 (ISO 5.1.2) 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. 1.4 (ISO 6.1.1) Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen. 1.6 en 3.1 (ISO 6.2.1) Beleid en ondersteunende beveiligingsmaatregelen behoren te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.
14	Het risico van organisatie-overhead door niet- of gebrekkig auditen van procedures met als gevolg (gevolgen) Verlies van kwaliteit en efficiëntie	**Beleid en personeel**	6.9 (ISO 18.2.2) Naleving van beveiligingsbeleid en -normen 6.10 (ISO 18.2.3) Beoordeling van technische naleving	6.9 (ISO 18.2.2) De directie 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 (ISO 18.2.3) Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.
15	Het risico dat dienstenniveaus niet voldoen aan de verwachting van de business door het ontbreken van een Service level manager met als gevolg een ontevreden organisatie.	**Beleid en personeel**	Nvt	1. Vastleggen taken en verantwoordelijkheden Service Manager 2. Vastleggen, communiceren en implementeren procedures omtrent inventariseren, vastleggen en vertalen van business behoeften naar IT oplossingen.
16	Het risico van onvolledige impact analyses t.b.v. wijzigingen in de infrastructuur door het ontbreken van een Configuration manager met als gevolg onvoorziene gevolgen van veranderingen in de infrastructuur.	**Beleid en personeel**	Geen mbo statement (ISO 8.1.1). Inventariseren van bedrijfsmiddelen	Geen mbo statement (ISO 8.1.1). Bedrijfsmiddelen die samenhangen met informatie en informatie verwerkende faciliteiten behoren te worden geïdentificeerd, en van deze bedrijfsmiddelen behoort een inventaris te worden opgesteld en onderhouden (dus ook de relaties met andere bedrijfsmiddelen). Aanvullend niet vallend onder ISO27002: 1. Impactanalyses worden uitgevoerd voorafgaand aan de infrastructuurwijziging. 2. Impact analyse rapport wordt besproken met en goedgekeurd door verantwoordelijke. 3. Plan van Aanpak wordt opgesteld en afgestemd met de verantwoordelijke. 4. Wijziging wordt gepland op tijdstip met minimale impact.

Nr	Risicobeschrijving	Categorie	Mbo normenkader (ISO 27002-2013) verwijzing	Maatregelen
17	Het risico dat er geen inzicht is in het aantal incidenten of het soort incidenten door onvoldoende registratie op de helpdesk met als gevolg dat de organisatie blijft hangen in ad hoc reageren op elk incident en uiteindelijk de ondersteuning van de klanten niet optimaal is.	**Beleid en personeel**	1.17 (ISO 16.1.1) Verantwoordelijkheden en procedures 1.18 (ISO 16.1.2) Rapportage van (informatiebeveiligings-) gebeurtenissen 2.6 (ISO 16.1.3) Rapportage van zwakke plekken in de informatiebeveiliging 4.12 (ISO 16.1.4) Beoordeling van en besluitvorming over (informatiebeveiligings-)gebeurtenissen 4.13 (ISO 16.1.5) Respons op informatiebeveiligingsincidenten Geen mbo statement (ISO 16.1.6) Lering uit informatiebeveiligingsincidenten	1.17 (ISO 16.1.1) Directieverantwoordelijkheden en -procedures behoren te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op (informatiebeveiligings-)incidenten te bewerkstelligen. 1.18 (ISO 16.1.2) Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd. 2.6 (ISO 16.1.3) 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. 4.12 (ISO 16.1.4) Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten. 4.13 (ISO 16.1.5) Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures. Geen mbo statement (ISO 16.1.6) Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen behoort te worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.
18	Het risico dat de ene medewerker niet op de hoogte is van het werk dat de andere medewerker heeft gedaan door het ontbreken van onderlinge werkafspraken met als gevolg slechte dienstverlening aan de klanten.	**Beleid en personeel**	Nvt	1. Werkoverleggen (ook met gerelateerde afdelingen) waarbij speciale aandacht is voor elkaar werkzaamheden.
19	Het risico van langdurige uitval van kernsystemen door het ontbreken van continuiteitsbeheer met als gevolg financiële en imago schade.	**Beleid en personeel**	Geen mbo statement (ISO 17.1.1) Informatiebeveiligingscontinuïteit plannen 4.14 (ISO 17.1.2) Informatiebeveiligingscontinuïteit implementeren Geen mbo statement (ISO 17.1.3) Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren 4.15 (ISO 17.2.1) Beschikbaarheid van informatie verwerkende faciliteiten	Geen mbo statement (ISO 17.1.1) De organisatie behoort haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, vast te stellen. 4.14 (ISO 17.1.2) 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. Geen mbo statement (ISO 17.1.3). De organisatie behoort de ten behoeve van informatiebeveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig te verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties. 4.15 (ISO 17.2.1) Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.
20	Het risico van het schenden van de privacy van studenten door het gebruik van een ander programma dan het voorgeschreven studentenregistratiesysteem met als gevolg een klacht tegen de school voor het schenden van de privacy van studenten.	**Beleid en personeel**	1.1 en 1.2 (ISO 5.1.1) Beleidsregels voor informatiebeveiliging. Geen mbo statement (ISO 8.1.3) Aanvaardbaar gebruik van bedrijfsmiddelen.	1.1 en 1.2 (ISO 5.1.1) Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen. Geen mbo statement (ISO 8.1.3). Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatie verwerkende faciliteiten behoren regels te worden geïdentificeerd, gedocumenteerd en geïmplementeerd.
21	Het risico van inconsistente/onvolledige data door onvoldoende geschoold personeel met als gevolg onvolledige informatievoorziening c.q. management informatie.	**Beleid en personeel**	nvt	1. Opzetten trainingsprogramma's gekoppeld aan het functieprofiel van de medewerker. 2. Invoeren rapportagestandaarden. 3. Kwaliteitscontrole (juistheid, volledigheid, tijdigheid) uitvoeren voorafgaand aan verzending van managementinformatie.
22	Het risico van lage procesvolwassenheid en onvoldoende kwaliteitsbewustzijn door ontbreken procesmanagement en onvoldoende kwaliteitscontrole met als gevolg dat belangrijke business doelstellingen niet worden behaald en de informatiebeveiliging te wensen overlaat.	**Beleid en personeel**	1.1 en 1.2 (ISO 5.1.1) Beleidsregels voor informatiebeveiliging. 1.3 (ISO 5.1.2) Beoordeling van het informatiebeveiligingsbeleid 6.9 (ISO 18.2.2) Naleving van beveiligingsbeleid en -normen 6.10 (ISO 18.2.3) Beoordeling van technische naleving	1.1 en 1.2 (ISO 5.1.1) Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen. 1.3 (ISO 5.1.2) 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. 6.9 (ISO 18.2.2) De directie 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 (ISO 18.2.3) Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.
23	Het risico dat ICT niet bijdraagt aan kwaliteit van het onderwijs doordat er geen geïmplementeerd beleid is, met als gevolg schade aan de kwaliteit van de opleidingen.	**Beleid en personeel**	nvt	1. Opstellen en periodiek beoordelen van IT-beleid, IT jaarplan, BIA (Business Impact Analyses) door directie en IT managers. 2. Jaarlijks opstellen en beoordelen van IT budget o.b.v. jaarplan.
24	Het risico van hoge IT kosten door ontbrekende visie op de ontwikkeling en toepassing van IT binnen de organisatie en/of ontbrekend IT beleidssplan en/of een begroting voor IT ontbreekt met als gevolg discontinuïteit van de instelling.	**Beleid en personeel**	nvt	1. Opstellen en periodiek beoordelen van IT-beleid, IT jaarplan, BIA (Business Impact Analyses) door directie en IT managers. 2. Jaarlijks opstellen en beoordelen van IT budget o.b.v. jaarplan.

Nr	Risicobeschrijving	Categorie	Mbo normenkader (ISO 27002-2013) verwijzing	Maatregelen
25	Het risico van desinformatie doorzelf opgestelde overzichten in plaats van standaardrapportages uit kernsystemen te gebruiken met als gevolg foutieve informatievoorziening.	**Beleid en personeel**	nvt	1. Inventariseren informatiebehoeften 2. Opzetten datawarehouse en reporting services.
26	Het risico dat systemen geen duidelijke eigenaar hebben door onvoldoende inrichting van IT governance met als gevolg hoge kosten, beheer issues.	**Beleid en personeel**	Geen mbo statement (ISO 8.1.1) Inventariseren van bedrijfsmiddelen Geen mbo statement (ISO 8.1.2) Eigendom van bedrijfsmiddelen	Geen mbo statement (ISO 8.1.1) Bedrijfsmiddelen die samenhangen met informatie en informatie verwerkende faciliteiten behoren te worden geïdentificeerd, en van deze bedrijfsmiddelen behoort een inventaris te worden opgesteld en onderhouden. Geen mbo statement (ISO 8.1.2) Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden, behoren een eigenaar te hebben.
27	Het risico van onvoldoende communicatie door HR over medewerkers die in een functie starten / van functie veranderen / hun functie beëindigen met als gevolg issues met autorisatiebeheer	**Beleid en personeel**	Geen mbo statement (ISO 7.3.1) Beëindiging of wijziging van verantwoordelijkheden van het dienstverband 5.3 (ISO 9.2.1) Registratie en afmelden van gebruikers 5.4 (ISO 9.2.2) Gebruikers toegang verlenen	Geen mbo statement (ISO 7.3.1) Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband behoren te worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer gebracht. 5.3 (ISO 9.2.1) Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken. 5.4 (ISO 9.2.2) 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.
28	Het risico dat persoonsgegevens onbeheerd op bureaus van medewerkers liggen door onvoldoende bewustzijn van medewerkers inzake informatiebeveiliging met als gevolg mogelijke diefstal van gegevens en/of reputatieschade.	**Beleid en personeel**	1.1 en 1.2 (ISO 5.1.1) Beleidsregels voor informatiebeveiliging. 1.3 (ISO 5.1.2) Beoordeling van het informatiebeveiligingsbeleid 1.6 en 3.1 (ISO 6.2.1) Beleid voor mobiele apparatuur 2.1 (ISO 7.1.2) Arbeidsvoorwaarden Geen mbo statement (ISO 7.2.1) Directieverantwoordelijkheden 2.2 (ISO 7.2.2) Bewustzijn, opleiding en training 2.4 (ISO 11.2.9) 'Clear desk'- en 'clear screen'-beleid	1.1 en 1.2 (ISO 5.1.1) Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen. 1.3 (ISO 5.1.2) 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. 1.6 en 3.1 (ISO 6.2.1) Beleid en ondersteunende beveiligingsmaatregelen behoren te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren. 2.1 (ISO 7.1.2) De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden. Geen mbo statement (ISO 7.2.1) De directie behoort van alle medewerkers en contractanten te eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie. 2.2 (ISO 7.2.2) Alle studenten/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. 2.4 (ISO 11.2.9) Er behoort een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatie verwerkende faciliteiten te worden ingesteld.
29	Het risico dat informatiebeveiliging van de instelling niet voldoet aan de gestelde standaard als gevolg van onvoldoende beoordeling door onafhankelijke auditors, directie met als gevolg mogelijke claims van toezichthouders	**Beleid en personeel**	Geen mbo statement (ISO 12.7.1) Beheersmaatregelen betreffende audits van informatiesystemen Geen mbo statement (ISO 18.2.1) Onafhankelijke beoordeling van informatiebeveiliging 6.9 (ISO 18.2.2) Naleving van beveiligingsbeleid en -normen 6.10 (ISO 18.2.3) Beoordeling van technische naleving	Geen mbo statement (ISO 12.7.1) Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, behoren zorgvuldig, te worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren. Geen mbo statement (ISO 18.2.1) De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheersdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen te worden beoordeeld. 6.9 (ISO 18.2.2) De directie 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 (ISO 18.2.3) Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.
30	Het risico op fraude bij invoer/mutaties van cijfers in het cijferregistratiesysteem door onvoldoende ingebouwde functiescheiding en/of controles met als gevolg reputatieschade en onjuiste beoordeling van studenten.	**Examinering**	1.14 (ISO 14.1.1) Analyse en specificatie van informatiebeveiligingseisen.	1.14 (ISO 14.1.1) De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen. .
31	Het risico dat digitale toetsen mislukken door onvoldoende stabiele beschikbare apparatuur op de schoollocatie met als gevolg operationele verstoringen en reputatieschade.	**Examinering**	4.15 (ISO 17.2.1) Beschikbaarheid van informatie verwerkende faciliteiten.	4.15 (ISO 17.2.1) Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.

Nr	Risicobeschrijving	Categorie	Mbo normenkader (ISO 27002-2013) verwijzing	Maatregelen
32	Risico van ongeautoriseerde toegang tot KRD\cijfer-registratie door onrechtmatig verkregen autorisaties met als gevolg examenfraude	**Examinering**	5.1 (ISO 9.1.1) Beleid voor toegangsbeveiliging 5.2 (ISO 9.1.2) Toegang tot netwerken en netwerk-diensten. 5.3 (ISO 9.2.1) Registratie en afmelden van gebrui-kers 5.4 (ISO 9.2.2). Gebruikers toegang verlenen 5.5 (ISO 9.2.3) Beheer van speciale toegangsrech-ten 5.6 (ISO 9.2.4) Beheer van geheime authenticatie informatie van gebruikers 6.1 (ISO 9.2.5) Beoordeling van toegangsrechten van gebruikers 2.3 (ISO 9.2.6) Toegangsrechten intrekken of aan-passen	5.1 (ISO 9.1.1) Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen. 5.2 (ISO 9.1.2) Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. 5.3 (ISO 9.2.1) Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken. 5.4 (ISO 9.2.2). Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangs-rechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken. 5.5 (ISO 9.2.3) Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst. 5.6 (ISO 9.2.4) Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheers-proces. 6.1 (ISO 9.2.5) Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen. 2.3 (ISO 9.2.6) De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwer-kende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.
33	Risico dat mentoren toegang hebben tot gegevens van niet eigen studenten door onvoldoende schei-ding van netwerkrechten met als gevolg slechte tra-ceerbaarheid bij cijfer manipulatie.	**Examinering**	zie vorige	zie vorige
34	Het risico van Ddos aanvallen door studenten / ex medewerkers / derden van de instelling met als ge-volg operationele verstoringen.	**IT infrastruc-tuur en externe verbindingen**	5.13 (ISO 13.1.1) Beheersmaatregelen voor net-werken 5.14 (ISO 13.1.2) Beveiliging van netwerkdiensten 5.15 (ISO 13.1.3) Scheiding in netwerken	5.13 (ISO 13.1.1) Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te be-schermen. 5.14 (ISO 13.1.2) 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 (ISO 13.1.3) Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden geschei-den. Overige maatregelen buiten ISO 27002: 1. Redundantie van webserver en provider. Bij aanval op provider/webserver 1 kan webserver 1 en provider 1 worden afgesloten en het verkeer via webserver 2 en provider 2 met ander ip adres worden gereroute. (Uitzondering geldt voor DDOS aanval op DNS, er is dan geen) 2. Periodiek uitvoeren van vulnerability scans uitvoeren op de IT infrastructuur om in vroeg stadium zwakheden te ont-dekken.
35	Het risico dat IT systemen en IT infrastructuur niet voldoen aan het gewenste beveiligingsniveau door legacy en/of toenemende stroom van BYOD (smart phone, tablet, usb) met als gevolg reputatieschade, operationele verstoringen, financiële schade.	**IT infrastruc-tuur en externe verbindingen**	1.6 en 3.1 (ISO 6.2.1) Beleid voor mobiele appara-tuur 5.13 (ISO 13.1.1) Beheersmaatregelen voor net-werken 5.14 (ISO 13.1.2) Beveiliging van netwerkdiensten 5.15 (ISO 13.1.3) Scheiding in netwerken	1.6 en 3.1 (ISO 6.2.1) Beleid en ondersteunende beveiligingsmaatregelen behoren te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren. 5.13 (ISO 13.1.1) Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te be-schermen. 5.14 (ISO 13.1.2) 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 (ISO 13.1.3) Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden geschei-den.
36	Het risico van stelen/vernieling van apparatuur door onvoldoende fysieke toegangsbeveiliging met als ge-volg financiele schade.	**IT infrastruc-tuur en externe verbindingen**	Geen mbo statement (ISO 7.2.3) Disciplinaire pro-cedure 3.3 (ISO 11.1.1) Fysieke beveiligingszone 3.4 (ISO 11.1.2) Fysieke toegangsbeveiliging 3.5 (ISO 11.1.3) Kantoren, ruimte en faciliteiten beveiligen 3.7 (ISO 11.1.5) Werken in beveiligde gebieden 3.8 (ISO 11.1.6) Laad- en loslocatie 3.9 (ISO 11.2.1) Plaatsing en bescherming van ap-paratuur 3.13 (ISO 11.2.6) Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	Geen mbo statement (ISO 7.2.3) Er behoort een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging. 3.3 (ISO 11.1.1) Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten. 3.4 (ISO 11.1.2) Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zor-gen dat alleen bevoegd personeel toegang krijgt. 3.5 (ISO 11.1.3) Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast. 3.7 (ISO 11.1.5) Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast. 3.8 (ISO 11.1.6) Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kun-nen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van informatie verwerkende facilitei-ten om onbevoegde toegang te vermijden. 3.9 (ISO 11.2.1) 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.

				3.13 (ISO 11.2.6) 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.

Nr	Risicobeschrijving	Categorie	Mbo normenkader (ISO 27002-2013) verwijzing	Maatregelen
37	Het risico van een onbeheersbare IT omgeving door toenemend gebruik van SaaS diensten met als gevolg operationele verstoringen	**IT infrastructuur en externe verbindingen**	Geen mbo statement (ISO 15.1.1) Informatiebeveiligingsbeleid voor leveranciersrelaties 1.15 (ISO 15.1.2) Opnemen van beveiligingsaspecten in leveranciersovereenkomsten 1.16 (ISO 15.1.3) Toeleveringsketen van informatie- en communicatietechnologie. 6.7 (ISO 15.2.1) Monitoring en beoordeling van dienstverlening van leveranciers 4.11 (ISO 15.2.2) Beheer van veranderingen in dienstverlening van leveranciers	Geen mbo statement (ISO 15.1.1) Met de leverancier behoren de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, te worden overeengekomen en gedocumenteerd. 1.15 (ISO 15.1.2) 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. 1.16 (ISO 15.1.3) 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. 6.7 (ISO 15.2.1) Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen. 4.11 (ISO 15.2.2). 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.
38	Het risico van telefonische onbereikbaarheid (IP-telefonie) door falende technische infrastructuur met als gevolg operationele verstoringen.	**IT infrastructuur en externe verbindingen**	4.15 (ISO 17.2.1) Beschikbaarheid van informatie verwerkende faciliteiten.	4.15 (ISO 17.2.1) Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.
39	Het risico van uitval van de IT-Infrastructuur door een gebrek aan redundante uitvoer met als gevolg operationele verstoringen	**IT infrastructuur en externe verbindingen**	4.15 (ISO 17.2.1) Beschikbaarheid van informatie verwerkende faciliteiten.	4.15 (ISO 17.2.1) Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.
40	Het risico van dataverlies door ontbrekende/onjuiste backups met als gevolg operationele verstoringen	**IT infrastructuur en externe verbindingen**	4.5 en 4.6 (ISO 12.3.1) Back-up van informatie	4.5 en 4.6 (ISO 12.3.1) Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.
41	Het risico van verlies van personeelsgegevens door alleen papieren dossiers in simpele kast en geen digitale backup met als gevolg operationele verstoringen.	**IT infrastructuur en externe verbindingen**	4.5 en 4.6 (ISO 12.3.1) Back-up van informatie	4.5 en 4.6 (ISO 12.3.1) Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.
42	Het risico dat de communicatie tussen verschillende pakketten verstoord wordt door het aanpassen van een bronsysteem zonder overleg met als gevolg dat de integriteit van de gegevens in gevaar komt.	**IT infrastructuur en externe verbindingen**	4,1 (ISO 12.1.2) Wijzigingsbeheer 4.2 (ISO 12.1.4) Scheiding van ontwikkel-, test- en productieomgevingen Geen mbo statement (ISO 14.2.1) Beleid voor beveiligd ontwikkelen Geen mbo statement (ISO 14.2.2) Procedures voor wijzigingsbeheer met betrekking tot systemen Geen mbo statement (ISO 14.2.3) Technische beoordeling van toepassingen na wijzigingen besturingsplatform Geen mbo statement (ISO 14.2.4) Beperkingen op wijzigingen aan softwarepakketten 4.10 (ISO 14.2.6) Beveiligde ontwikkelomgeving 6.4 (ISO 14.2.7) Uitbestede softwareontwikkeling 6.5 (ISO 14.2.8) Testen van systeembeveiliging 6.6 (ISO 14.2.9) Systeemacceptatietests	4,1 (ISO 12.1.2) Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst. 4.2 (ISO 12.1.4) Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen. Geen mbo statement (ISO 14.2.1). Voor het ontwikkelen van software en systemen behoren regels te worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie te worden toegepast. Geen mbo statement (ISO 14.2.2) Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer. Geen mbo statement (ISO 14.2.3) Als besturingsplatforms zijn veranderd, behoren bedrijf kritische toepassingen te worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie. Geen mbo statement (ISO 14.2.4) Wijzigingen aan softwarepakketten behoren te worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen behoren strikt te worden gecontroleerd. 4.10 (ISO 14.2.6) 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. 6.4 (ISO 14.2.7) Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de organisatie. 6.5 (ISO 14.2.8) Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest. 6.6 (ISO 14.2.9) Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.
43	Het risico dat de restore van een backup niet slaagt doordat er geen periodieke restore wordt uitgevoerd als test met als gevolg gegevensverlies.	**IT infrastructuur en externe verbindingen**	4.5 en 4.6 (ISO 12.3.1) Back-up van informatie	4.5 en 4.6 (ISO 12.3.1) Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.
44	Het risico dat de instelling illegale software gebruikt door een niet-optimaal licentiebeleid met als gevolg boetes.	**IT infrastructuur en externe verbindingen**	4.9 (ISO 12.6.2). Beperkingen voor het installeren van software	4.9 (ISO 12.6.2) Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.

Nr	Risicobeschrijving	Categorie	Mbo normenkader (ISO 27002-2013) verwijzing	Maatregelen
45	Het risico van te grote responstijden bij incidenten door nalatig incidentmanagement met als gevolg ontevredenheid bij eindgebruikers en wantrouwen.	**IT infrastructuur en externe verbindingen**	1.17 (ISO 16.1.1) Verantwoordelijkheden en procedures 1.18 (ISO 16.1.2) Rapportage van (informatiebeveiligings-) gebeurtenissen 2.6 (ISO 16.1.3) Rapportage van zwakke plekken in de informatiebeveiliging 4.12 (ISO 16.1.4) Beoordeling van en besluitvorming over (informatiebeveiligings-)gebeurtenissen 4.13 (ISO 16.1.5) Respons op informatiebeveiligingsincidenten Geen mbo statement (ISO 16.1.6) Lering uit informatiebeveiligingsincidenten	1.17 (ISO 16.1.1) Directieverantwoordelijkheden en -procedures behoren te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op (informatiebeveiligings-)incidenten te bewerkstelligen. 1.18 (ISO 16.1.2) Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd. 2.6 (ISO 16.1.3) 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. 4.12 (ISO 16.1.4) Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten. 4.13 (ISO 16.1.5) Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures. Geen mbo statement (ISO 16.1.6) Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen behoort te worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.
46	Het risico van niet-relevante ICT-inkoop door niet afstemmen van vraag en aanbod met als gevolg financieel verlies .	**IT infrastructuur en externe verbindingen**	nvt	1. Vaststellen functionele en technische requirements. 2. Opstellen business case inclusief leveranciersanalyse. 3. Goedkeuring door manager ICT en verantwoordelijk directielid voor aankoop op basis van businesscase.
47	Het risico van onderbezetting servicedesk door toename omvang aantal applicaties met als gevolg teruglopend niveau van dienstverlening en ontevreden gebruikers.	**IT infrastructuur en externe verbindingen**	nvt	1. Personeelsplanning. 2. Perdiodieke herbeoordeling applicatielandschap.
48	Het risico van versnippering van IT-beheer door applicatie georiënteerd beheer of lokaal georiënteerd beheer met als gevolg een overall IT-beheer met weinig samenhang en inefficiënt IT-beheer.	**Beleid en personeel**	nvt	1. Beschrijven specifieke taken en verantwoordelijkheden. 2. Periodieke herbeoordeling IT beheer en aanpassingen doorvoeren waar nodig.
49	Het risico van bedrijfsschade door onvoldoende kennisborging bij de IT-beheerprocessen met als gevolg dat identieke (IT)verstoringen van bedrijfsprocessen zich steeds blijven herhalen tegen oplopende kosten.	**IT infrastructuur en externe verbindingen**	nvt	1. Opzetten trainingsprogramma's gekoppeld aan het functieprofiel van de medewerkers. 2. Documenteren best-practice werkinstructies. 3. Kwaliteitscontrole (juistheid, volledigheid, tijdigheid) uitvoeren voorafgaand aan communicatie van best-practice
50	Het risico van backup-uitval door gebrek aan monitoring met als gevolg moeizame tot onmogelijke recovery.	**IT infrastructuur en externe verbindingen**	4.5 en 4.6 (ISO 12.3.1) Back-up van informatie	4.5 en 4.6 (ISO 12.3.1) Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.
51	Het risico van oververhitting van het datacenter door falende koeling en gebrekkig monitoren met als gevolg uitval van het datacenter.	**IT infrastructuur en externe verbindingen**	3.10 (ISO 11.2.2) Nutsvoorzieningen 3.12 (ISO 11.2.4) Onderhoud van apparatuur	3.10 (ISO 11.2.2) Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen. 3.12 (ISO 11.2.4) Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.
52	Het risico dat uitgeleende apparatuur niet ingeleverd wordt door onvoldoende monitoring met als gevolg dat de apparatuur zoek raakt, dus kapitaal vernietigd wordt.	**IT infrastructuur en externe verbindingen**	Geen mbo statement (ISO 8.1.1) Inventariseren van bedrijfsmiddelen Geen mbo statement (ISO 8.1.2) Eigendom van bedrijfsmiddelen Geen mbo statement (ISO 8.1.4) Teruggeven van bedrijfsmiddelen	Geen mbo statement (ISO 8.1.1). Bedrijfsmiddelen die samenhangen met informatie en informatie verwerkende faciliteiten behoren te worden geïdentificeerd, en van deze bedrijfsmiddelen behoort een inventaris te worden opgesteld en onderhouden. Geen mbo statement (ISO 8.1.2) Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden, behoren een eigenaar te hebben. Geen mbo statement (ISO 8.1.4) Alle medewerkers en externe gebruikers behoren alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst terug te geven.
53	Het risico dat een leverancier/producent failliet gaat door het ontbreken van escrow afspraken met als gevolg onderbreken continuïteit van de organisatie.	**IT infrastructuur en externe verbindingen**	6.7 (ISO 15.2.1) Monitoring en beoordeling dienstverlening van leveranciers	6.7 (ISO 15.2.1) Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen.
54	Risico van uitval van de SAN door leeftijd SAN en opgezegd onderhoudscontract Dell met als gevolg continuïteit verlies en dataverlies.	**IT infrastructuur en externe verbindingen**	3.12 (ISO 11.2.4) Onderhoud van apparatuur	3.12 (ISO 11.2.4) Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.
55	Het risico op instabiliteit van de ICT-infrastructuur door het niet op tijd vervangen van verouderde ser-vers met als gevolg dat systemen niet beschikbaar zijn.	**IT infrastructuur en externe verbindingen**	3.12 (ISO 11.2.4) Onderhoud van apparatuur	3.12 (ISO 11.2.4) Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.
56	Het risico dat er te veel applicaties aan de kernsystemen gekoppeld zijn door onvoldoende ontwikkelmogelijkheden binnen de kernsystemen met als gevolg beheer issues	**IT infrastructuur en externe verbindingen**	nvt	1.Functionele eisen specificeren in selectietraject. 2.Eisen met betrekking tot interfacing opnemen in selectie traject. 3. Servicecontracten afsluiten voor maatwerk ontwikkelingen

Nr	Risicobeschrijving	Categorie	Mbo normenkader (ISO 27002-2013) verwijzing	Maatregelen
57	Het risico dat de serverruimte niet brandveilig is door ontbrekende brandbeveiligingsmaatregelen met als gevolg operationele verstoringen	**IT infrastructuur en externe verbindingen**	3.6 (ISO 11.1.4) Bedreigingen van buitenaf. 3.9 (ISO 11.2.1) Plaatsing en bescherming van apparatuur	3.6 (ISO 11.1.4) Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast. 3.9 (ISO 11.2.1) 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.
58	Het risico dat de internetverbinding aan zijn maximale capaciteit zit door onvoldoende inzicht in verbruik en/of onvoldoende infrastructuur met als gevolg operationele verstoringen.	**IT infrastructuur en externe verbindingen**	Geen mbo statement (ISO 12.1.3) Capaciteitsbeheer	Geen mbo statement (ISO 12.1.3) Het gebruik van middelen behoort te worden gemonitord en afgestemd, en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.
59	Het risico van Cybercrime (Phising, SPAM, hacking) door onvoldoende ingerichte beveiligingsmaatregelen met als gevolg operationele verstoringen, financiele schade en reputatieschade.	**IT infrastructuur en externe verbindingen**	4.3 en 4.4 (ISO 12.2.1) Beheersmaatregelen tegen malware 5.13 (ISO 13.1.1) Beheersmaatregelen voor netwerken 5.14 (ISO 13.1.2) Beveiliging van netwerkdiensten 5.15 (ISO 13.1.3) Scheiding in netwerken 1.12 (ISO 13.2.1) Beleid en procedures voor informatietransport 5.16 (ISO 13.2.3) Elektronische berichten	4.3 en 4.4 (ISO 12.2.1) Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers. 5.13 (ISO 13.1.1) Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen. 5.14 (ISO 13.1.2) 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 (ISO 13.1.3) Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden. 1.12 (ISO 13.2.1) Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn. 5.16 (ISO 13.2.3) Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd.
60	Het risico dat onbevoegden toegang hebben tot ruimtes door versnipperde en onvoldoende procedurele afspraken met betrekking tot fysieke toegangsbeleid en beveiliging met als gevolg dat informatie en/of andere eigendommen gestolen worden.	**IT infrastructuur en externe verbindingen**	Geen mbo statement (ISO 7.2.3) Disciplinaire procedure 5.1 (ISO 9.1.1) Beleid voor toegangsbeveiliging 3.3 (ISO 11.1.1) Fysieke beveiligingszone 3.4 (ISO 11.1.2) Fysieke toegangsbeveiliging 3.5 (ISO 11.1.3) Kantoren, ruimte en faciliteiten beveiligen 3.7 (ISO 11.1.5) Werken in beveiligde gebieden 3.8 (ISO 11.1.6) Laad- en loslocatie 3.9 (ISO 11.2.1) Plaatsing en bescherming van apparatuur 3.13 (ISO 11.2.6) Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	Geen mbo statement (ISO 7.2.3) Er behoort een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging. 5.1 (ISO 9.1.1) Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen. 3.3 (ISO 11.1.1) Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten. 3.4 (ISO 11.1.2) Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt. 3.5 (ISO 11.1.3) Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast. 3.7 (ISO 11.1.5) Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast. 3.8 (ISO 11.1.6) 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. 3.9 (ISO 11.2.1) 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. 3.13 (ISO 11.2.6) 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.
61	Het risico dat bedrijfsgegevens gelekt worden door grotere vraag naar business intelligence en reporting met als gevolg reputatieschade.	**Toegang tot applicaties en data**	1.1 en 1.2 (ISO 5.1.1) Beleidsregels voor informatiebeveiliging. 1.7 (ISO 8.2.1) Classificatie van informatie 1.8 (ISO 8.2.2) Informatie labelen Geen mbo statement (ISO 8.2.3) Behandelen van bedrijfsmiddelen	1.1 en 1.2 (ISO 5.1.1) Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen. 1.7 (ISO 8.2.1) Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging. 1.8 (ISO 8.2.2) 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. Geen mbo statement (ISO 8.2.3) Procedures voor het behandelen van bedrijfsmiddelen behoren te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.
62	Het risico dat wachtwoorden van medewerkers en studenten bekend zijn bij onbevoegden door onvoldoende risicobewustzijn van medewerkers / studenten met als gevolg van fraude.	**Toegang tot applicaties en data**	1.1 en 1.2 (ISO 5.1.1) Beleidsregels voor informatiebeveiliging. 1.3 (ISO 5.1.2) Beoordeling van het informatiebeveiligingsbeleid 1.6 en 3.1 (ISO 6.2.1) Beleid voor mobiele apparatuur 2.1 (ISO 7.1.2) Arbeidsvoorwaarden Geen mbo statement (ISO 7.2.1) Directieverantwoordelijkheden 2.2 (ISO 7.2.2) Bewustzijn, opleiding en training	1.1 en 1.2 (ISO 5.1.1) Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen. 1.3 (ISO 5.1.2) 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. 1.6 en 3.1 (ISO 6.2.1) Beleid en ondersteunende beveiligingsmaatregelen behoren te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren. 2.1 (ISO 7.1.2) De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden. Geen mbo statement (ISO 7.2.1) De directie behoort van alle medewerkers en contractanten te eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie. 2.2 (ISO 7.2.2) Alle studenten/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.

Nr	Risicobeschrijving	Categorie	Mbo normenkader (ISO 27002-2013) verwijzing	Maatregelen
63	Het risico dat data bij SaaS leveranciers beschikbaar is voor onbevoegden door onvoldoende beveiliging bij de SaaS leveranciers met als gevolg reputatieschade voor de instelling	**Toegang tot applicaties en data**	Geen mbo statement (ISO 15.1.1) Informatiebeveiligingsbeleid voor leveranciersrelaties 1.15 (ISO 15.1.2) Opnemen van beveiligingsaspecten in leveranciersovereenkomsten 1.16 (ISO 15.1.3) Toeleveringsketen van informatie- en communicatietechnologie. 6.7 (ISO 15.2.1) Monitoring en beoordeling van dienstverlening van leveranciers 4.11 (ISO 15.2.2) Beheer van veranderingen in dienstverlening van leveranciers	Geen mbo statement (ISO 15.1.1) Met de leverancier behoren de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, te worden overeengekomen en gedocumenteerd. 1.15 (ISO 15.1.2) 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. 1.16 (ISO 15.1.3) 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. 6.7 (ISO 15.2.1) Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen. 4.11 (ISO 15.2.2). 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.
64	Het risico op fraude of onrechtmatige invoer in het kernregistratiesysteem door onvoldoende scheiding van rechten over groepen van personen met als gevolg reputatieschade.	**Toegang tot applicaties en data**	5.1 (ISO 9.1.1) Beleid voor toegangsbeveiliging. 5.3 (ISO 9.2.1) Registratie en afmelden van gebruikers. 5.4 (ISO 9.2.2) Gebruikers toegang verlenen	5.1 (ISO 9.1.1) Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen. 5.3 (ISO 9.2.1) Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken. 5.4 (ISO 9.2.2) 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.
65	Het risico dat de AD niet op orde is doordat gegevens uit Topdesk niet matchen met AD met als gevolg dat verkeerde applicaties aan verkeerde personen / werkstations gekoppeld worden.	**Toegang tot applicaties en data**	5.1 (ISO 9.1.1) Beleid voor toegangsbeveiliging. 5.3 (ISO 9.2.1) Registratie en afmelden van gebruikers. 6.1 (ISO 9.2.5) Beoordeling van toegangsrechten van gebruikers.	5.1 (ISO 9.1.1) Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen. 5.3 (ISO 9.2.1) Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken. 6.1 (ISO 9.2.5) Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.
66	Het risico dat ongeautoriseerde personen toegang krijgen tot het Data Center door het ontbreken van een periodieke controle op de autorisaties met als gevolg dat servers door ongeautoriseerde personen benaderd kunnen worden.	**Toegang tot applicaties en data**	5.4 (ISO 9.2.2) Gebruikers toegang verlenen 6.1 (ISO 9.2.5) Beoordeling van toegangsrechten van gebruikers.	5.4 (ISO 9.2.2) 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. 6.1 (ISO 9.2.5) Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.
67	Het risico dat hackers makkelijk toegang krijgen tot het netwerk doordat minimale wachtwoordvereisten niet worden afgedwongen met als gevolg dat gevoelige informatie ontvreemd wordt.	**Toegang tot applicaties en data**	5.1 (ISO 9.1.1) Beleid voor toegangsbeveiliging. 5.7 (ISO 9.3.1) Geheime authenticatie-informatie gebruiken. 5.14 (ISO 13.1.2) Beveiliging van netwerken.	5.1 (ISO 9.1.1) Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen. 5.7 (ISO 9.3.1) Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatie informatie houden aan de praktijk van de organisatie. 5.14 (ISO 13.1.2) 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.
68	Het risico dat er spookmedewerkers worden aangemaakt door het ontbreken van functiescheiding binnen Profit met als gevolg onterechte salarisuitbetaling.	**Toegang tot applicaties en data**	5.1 (ISO 9.1.1) Beleid voor toegangsbeveiliging 6.1 (ISO 9.2.5) Beoordeling van toegangsrechten van gebruikers	5.1 (ISO 9.1.1) Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen. 6.1 (ISO 9.2.5) Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen. Los van ISO27002: 1. Maandelijkse controle op salarisoverzicht (preventief) 2. Functiescheiding in betalingsapplicaties (preventief) 3. Maandelijkse controle op uitbetaalde salarissen (reactief)
69	Het risico dat er ongeoorloofde mutaties plaats vinden doordat logging niet structureel gecontroleerd wordt met als gevolg een kans op fraude.	**Toegang tot applicaties en data**	6.2 (ISO 12.4.1) Gebeurtenissen registreren 5.12 (ISO 12.4.2) Beschermen van informatie in logbestanden 6.3 (ISO 12.4.3) Logbestanden van beheerders en operators 3.15 (ISO 12.4.4) Kloksynchrronisatie	6.2 (ISO 12.4.1) Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld. 5.12 (ISO 12.4.2) Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang. 6.3 (ISO 12.4.3) Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld. 3.15 (ISO 12.4.4) De klokken van alle relevante informatie verwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.

Nr	Risicobeschrijving	Categorie	Mbo normenkader (ISO 27002-2013) verwijzing	Maatregelen
70	Het risico dat speciale rechten van systeembeheerders ongepast worden gebruikt, doordat een formele autorisatieprocedure, toegespitst op functies, rollen en taken in overeenstemming met het toegangsbeveiligingsbeleid ontbreekt, met als gevolg dat onbevoegd toegang wordt verkregen tot vertrouwelijke informatie.	**Toegang tot applicaties en data**	5.1 (ISO 9.1.1) Beleid voor toegangsbeveiliging 5.5 (ISO 9.2.3) Beheer van speciale toegangsrechten	5.1 (ISO 9.1.1) Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen. 5.5 (ISO 9.2.3) Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.
71	Het risico van virusaanvallen door achterstallige updates van virusdefinities met als gevolg uitval van het datacenter en dataverlies.	**Toegang tot applicaties en data**	4.3 en 4.4 (ISO 12.2.1) Beheersmaatregelen tegen malware 4.7 (ISO 12.5.1) Software installeren op operationele systemen 4.8 (ISO 12.6.1) Beheer van technische kwetsbaarheden Geen mbo statement (ISO 14.2.2) Procedures voor wijzigingsbeheer met betrekking tot systemen	4.3 en 4.4 (ISO 12.2.1) Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers. 4.7 (ISO 12.5.1) Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd. 4.8 (ISO 12.6.1) 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. Geen mbo statement (ISO 14.2.2) Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.
72	Uitval van applicaties door het ontbreken van lifecyclemanagement met als gevolg schade voor het primair proces.	**Toegang tot applicaties en data**	Geen mbo statement (ISO 14.2.2) Procedures voor wijzigingsbeheer met betrekking tot systemen	Geen mbo statement (ISO 14.2.2) Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.
73	Het risico van onterecht bestaande gebruikersaccounts door niet afmeldingen medewerkers als ze uit dienst gaan met als gevolg dat de active directory vervuild is en er geen overzicht is van actieve gebruikers.	**Toegang tot applicaties en data**	Geen mbo statement (ISO 7.3.1) Beëindiging of wijziging van verantwoordelijkheden van het dienstverband. 5.1 (ISO 9.1.1) Beleid voor toegangsbeveiliging 5.3 (ISO 9.2.1) Registratie en afmelden van gebruikers	Geen mbo statement (ISO 7.3.1) Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband behoren te worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer gebracht. 5.1 (ISO 9.1.1) Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen. 5.3 (ISO 9.2.1) Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.
74	Het risico van geinfecteerde data door virussen met als gevolg data inconsistentie of totaal dataverlies	**Toegang tot applicaties en data**	Geen mbo statement (ISO 12.1.1) Beheersmaatregelen tegen malware	4.3 en 4.4 (ISO 12.2.1) Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.
75	Het risico van onvoldoende redundantie van gegevens door ontbreken van versiebeheer met als gevolg onduidelijkheid in statussen van documenten, verschillende versies, inefficiënt databeslag.	**Toegang tot applicaties en data**	1.7 (ISO 8.2.1) Classificatie van informatie 1.8 (ISO 8.2.2) Informatie labelen	1.7 (ISO 8.2.1) Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging. 1.8 (ISO 8.2.2) 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.

Nr	Risicobeschrijving	Categorie	Mbo normenkader (ISO 27002-2013) verwijzing	Maatregelen
76	Het risico van ongewenste authenticatie door ontbreken van authenticatierollen met als gevolg ongewenste toegang tot vertrouwelijke gegevens en het kunnen muteren/verwijderen van deze gegevens.	**Toegang tot applicaties en data**	5.1 (ISO 9.1.1) Beleid voor toegangsbeveiliging 5.2 (ISO 9.1.2) Toegang tot netwerken en netwerkdiensten. 5.3 (ISO 9.2.1) Registratie en afmelden van gebruikers 5.4 (ISO 9.2.2). Gebruikers toegang verlenen 5.5 (ISO 9.2.3) Beheer van speciale toegangsrechten 5.6 (ISO 9.2.4) Beheer van geheime authenticatie informatie van gebruikers 6.1 (ISO 9.2.5) Beoordeling van toegangsrechten van gebruikers 2.3 (ISO 9.2.6) Toegangsrechten intrekken of aanpassen. 5.7 (ISO 9.3.1) Geheime authenticatie informatie gebruiken 5.8 (ISO 9.4.1) Beperking toegang tot informatie 5.9 (ISO 9.4.2) Beveiligde inlogprocedures Geen mbo statement (ISO 9.4.3) Systeem voor wachtwoordbeheer Geen mbo statement (ISO 9.4.4) Speciale systeemhulpmiddelen gebruiken Geen mbo statement (ISO 9.4.5) Toegangsbeveiliging op programmabroncode	5.1 (ISO 9.1.1) Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen. 5.2 (ISO 9.1.2) Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. 5.3 (ISO 9.2.1) Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken. 5.4 (ISO 9.2.2). 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 (ISO 9.2.3) Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst. 5.6 (ISO 9.2.4) Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces. 6.1 (ISO 9.2.5) Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen. 2.3 (ISO 9.2.6) 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. 5.7 (ISO 9.3.1) Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatie informatie houden aan de praktijk van de organisatie. 5.8 (ISO 9.4.1) Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging. 5.9 (ISO 9.4.2) Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure. Geen mbo statement (ISO 9.4.3) Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen. Geen mbo statement (ISO 9.4.4) Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen behoort te worden beperkt en nauwkeurig te worden gecontroleerd. Geen mbo statement (ISO 9.4.5) Toegang tot de programmabroncode behoort te worden beperkt.
77	Het risico van verlies van vertrouwelijke data door onduidelijkheid over wie de eigenaar van de applicatie met als gevolg imagoschade voor de school.	**Toegang tot applicaties en data**	Geen mbo statement (ISO 8.1.2) Eigendom van bedrijfsmiddelen	Geen mbo statement (ISO 8.1.2) Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden, behoren een eigenaar te hebben.
78	Het risico van fraude / ongeautoriseerde toegang tot data en systemen door ontbrekend wachtwoordenbeleid en procedures met als gevolg reputatie en financiële schade.	**Toegang tot applicaties en data**	5.1 (ISO 9.1.1) Beleid voor toegangsbeveiliging 5.2 (ISO 9.1.2) Toegang tot netwerken en netwerkdiensten. 5.3 (ISO 9.2.1) Registratie en afmelden van gebruikers 5.4 (ISO 9.2.2). Gebruikers toegang verlenen 5.5 (ISO 9.2.3) Beheer van speciale toegangsrechten 5.6 (ISO 9.2.4) Beheer van geheime authenticatie informatie van gebruikers 6.1 (ISO 9.2.5) Beoordeling van toegangsrechten van gebruikers 2.3 (ISO 9.2.6) Toegangsrechten intrekken of aanpassen. 5.7 (ISO 9.3.1) Geheime authenticatie informatie gebruiken 5.8 (ISO 9.4.1) Beperking toegang tot informatie 5.9 (ISO 9.4.2) Beveiligde inlogprocedures Geen mbo statement (ISO 9.4.3) Systeem voor wachtwoordbeheer Geen mbo statement (ISO 9.4.4) Speciale systeemhulpmiddelen gebruiken Geen mbo statement (ISO 9.4.5) Toegangsbeveiliging op programmabroncode	5.1 (ISO 9.1.1) Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen. 5.2 (ISO 9.1.2) Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. 5.3 (ISO 9.2.1) Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken. 5.4 (ISO 9.2.2). 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 (ISO 9.2.3) Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst. 5.6 (ISO 9.2.4) Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces. 6.1 (ISO 9.2.5) Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen. 2.3 (ISO 9.2.6) 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. 5.7 (ISO 9.3.1) Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatie informatie houden aan de praktijk van de organisatie. 5.8 (ISO 9.4.1) Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging. 5.9 (ISO 9.4.2) Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure. Geen mbo statement (ISO 9.4.3) Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen. Geen mbo statement (ISO 9.4.4) Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen behoort te worden beperkt en nauwkeurig te worden gecontroleerd. Geen mbo statement (ISO 9.4.5) Toegang tot de programmabroncode behoort te worden beperkt.

Bijlage 2 Vertaaltabel ISO 27002 naar mbo normenkader

5	Informatiebeveiligingsbeleid	
5.1	Aansturing door de directie van de informatiebeveiliging	
ISO nummer en naamgeving van statements		MBO nr.
5.1.1	Beleidsregels voor informatiebeveiliging (1 van 2)	1.1
	Beleidsregels voor informatiebeveiliging (2 van 2)	1.2
5.1.2	Beoordeling van het informatiebeveiligingsbeleid	1.3

6	Organiseren van informatiebeveiliging	
6.1	Interne organisatie	
ISO nummer en naamgeving van statements		MBO nr.
6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging	1.4
6.1.2	Scheiding van taken	1.21
6.1.3	Contact met overheidsinstanties	niet[1]
6.1.4	Contact met speciale belangengroepen	niet
6.1.5	Informatiebeveiliging in projectbeheer	1.5
6.2	Mobiele apparatuur en telewerken	
ISO nummer en naamgeving van statements		MBO nr.
6.2.1	Beleid voor mobiele apparatuur (1 van 2)	1.6
	Beleid voor mobiele apparatuur (2 van 2)	3.1
6.2.2	Telewerken	niet

7	Veilig personeel	
7.1	Voorafgaand aan het dienstverband	
ISO nummer en naamgeving van statements		MBO nr.
7.1.1	Screening	2.7
7.1.2	Arbeidsvoorwaarden	2.1
7.2	Tijdens het dienstverband	
ISO nummer en naamgeving van statements		MBO nr.
7.2.1	Directieverantwoordelijkheden	niet
7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	2.2
7.2.3	Disciplinaire procedure	niet
7.3	Beëindiging en wijziging van dienstverband	
ISO nummer en naamgeving van statements		MBO nr.
7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	niet

[1] Deze norm uit ISO27002 wordt niet gebruikt in het mbo normenkader en het daarvan afgeleide mbo toetsingskader.

8	Beheer van bedrijfsmiddelen	
8.1	Verantwoordelijkheid voor bedrijfsmiddelen	
ISO nummer en naamgeving van statements		MBO nr.
8.1.1	Inventariseren van bedrijfsmiddelen	niet
8.1.2	Eigendom van bedrijfsmiddelen	niet
8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen	niet
8.1.4	Teruggeven van bedrijfsmiddelen	niet
8.2	Informatieclassificatie	
ISO nummer en naamgeving van statements		MBO nr.
8.2.1	Classificatie van informatie	1.7
8.2.2	Informatie labelen	1.8
8.2.3	Behandelen van bedrijfsmiddelen	niet
8.3	Behandelen van media	
ISO nummer en naamgeving van statements		MBO nr.
8.3.1	Beheer van verwijderbare media	niet
8.3.2	Verwijderen van media	3.2
8.3.3	Media fysiek overdragen	niet

9	Toegangsbeveiliging	
9.1	Bedrijfseisen voor toegangsbeveiliging	
ISO nummer en naamgeving van statements		MBO nr.
9.1.1	Beleid voor toegangsbeveiliging	5.1
9.1.2	Toegang tot netwerken en netwerkdiensten	5.2
9.2	Beheer van toegangsrechten van gebruikers	
ISO nummer en naamgeving van statements		MBO nr.
9.2.1	Registratie en afmelden van gebruikers	5.3
9.2.2	Gebruikers toegang verlenen	5.4
9.2.3	Beheren van speciale toegangsrechten	5.5
9.2.4	Beheer van geheime authenticatie-informatie van gebruikers	5.6
9.2.5	Beoordeling van toegangsrechten van gebruikers	6.1
9.2.6	Toegangsrechten intrekken of aanpassen	2.3
9.3	Verantwoordelijkheden van gebruikers	
ISO nummer en naamgeving van statements		MBO nr.
9.3.1	Geheime authenticatie-informatie gebruiken	5.7
9.4	Toegangsbeveiliging van systeem en toepassing	
ISO nummer en naamgeving van statements		MBO nr.
9.4.1	Beperking toegang tot informatie	5.8
9.4.2	Beveiligde inlogprocedures	5.9
9.4.3	Systeem voor wachtwoordbeheer	niet
9.4.4	Speciale systeemhulpmiddelen gebruiken	niet
9.4.5	Toegangsbeveiliging op programmabroncode	niet

10	Cryptografie	
10.1	Cryptografische beheersmaatregelen	
ISO nummer en naamgeving van statements		MBO nr.
10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen (1 van 2)	1.9
	Beleid inzake het gebruik van cryptografische beheersmaatregelen (2 van 2)	1.10
10.1.2	Sleutelbeheer (1 van 2)	5.10
	Sleutelbeheer (2 van 2)	5.11

11	Fysieke beveiliging en beveiliging van de omgeving	
11.1	Beveiligde gebieden	
ISO nummer en naamgeving van statements		MBO nr.
11.1.1	Fysieke beveiligingszone	3.3
11.1.2	Fysieke toegangsbeveiliging	3.4
11.1.3	Kantoren, ruimten en faciliteiten beveiligen	3.5
11.1.4	Beschermen tegen bedreigingen van buitenaf	3.6
11.1.5	Werken in beveiligde gebieden	3.7
11.1.6	Laad- en loslocatie	3.8
11.2	Apparatuur	
ISO nummer en naamgeving van statements		MBO nr.
11.2.1	Plaatsing en bescherming van apparatuur	3.9
11.2.2	Nutsvoorzieningen	3.10
11.2.3	Beveiliging van bekabeling	3.11
11.2.4	Onderhoud van apparatuur	3.12
11.2.5	Verwijdering van bedrijfsmiddelen	1.11
11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	3.13
11.2.7	Veilig verwijderen of hergebruiken van apparatuur	3.14
11.2.8	Onbeheerde gebruikersapparatuur	niet
11.2.9	Clear desk'- en 'clear screen'-beleid	2.4

12	Beveiliging bedrijfsvoering	
12.1	Bedieningsprocedures en verantwoordelijkheden	
ISO nummer en naamgeving van statements		MBO nr.
12.1.1	Gedocumenteerde bedieningsprocedures	niet
12.1.2	Wijzigingsbeheer	4.1
12.1.3	Capaciteitsbeheer	niet
12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen	4.2
12.2	Bescherming tegen malware	
ISO nummer en naamgeving van statements		MBO nr.
12.2.1	Beheersmaatregelen tegen malware (1 van 2)	4.3
	Beheersmaatregelen tegen malware (2 van 2)	4.4
12.3	Back-up	
ISO nummer en naamgeving van statements		MBO nr.
12.3.1	Back-up van informatie (1 van 2)	4.5
	Back-up van informatie (2 van 2)	4.6
12.4	Verslaglegging en monitoren	
ISO nummer en naamgeving van statements		MBO nr.
12.4.1	Gebeurtenissen registreren	6.2
12.4.2	Beschermen van informatie in logbestanden	5.12
12.4.3	Logbestanden van beheerders en operators	6.3
12.4.4	Kloksynchronisatie	3.15
12.5	Beheersing van operationele software	
ISO nummer en naamgeving van statements		MBO nr.
12.5.1	Software installeren op operationele systemen	4.7
12.6	Beheer van technische kwetsbaarheden	
ISO nummer en naamgeving van statements		MBO nr.
12.6.1	Beheer van technische kwetsbaarheden	4.8
12.6.2	Beperkingen voor het installeren van software	4.9
12.7	Overwegingen betreffende audits van informatiesystemen	
ISO nummer en naamgeving van statements		MBO nr.
12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen	niet

13	Communicatiebeveiliging	
13.1	Beheer van netwerkbeveiliging	
ISO nummer en naamgeving van statements		MBO nr.
13.1.1	Beheersmaatregelen voor netwerken	5.13
13.1.2	Beveiliging van netwerkdiensten	5.14
13.1.3	Scheiding in netwerken	5.15
13.2	Informatietransport	
ISO nummer en naamgeving van statements		MBO nr.
13.2.1	Beleid en procedures voor informatietransport	1.12
13.2.2	Overeenkomsten over informatietransport	1.13
13.2.3	Elektronische berichten	5.16
13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	2.5

14	Acquisitie, ontwikkeling en onderhoud van informatiesystemen	
14.1	Beveiligingseisen voor informatiesystemen	
ISO nummer en naamgeving van statements		MBO nr.
14.1.1	Analyse en specificatie van informatiebeveiligingseisen	1.14
14.1.2	Toepassingen op openbare netwerken beveiligen	niet
14.1.3	Transacties van toepassingen beschermen	5.17
14.2	Beveiliging in ontwikkelings- en ondersteunende processen	
ISO nummer en naamgeving van statements		MBO nr.
14.2.1	Beleid voor beveiligd ontwikkelen	niet
14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen	niet
14.2.3	Technische beoordeling van toepassingen na wijzigingen besturingsplatform	niet
14.2.4	Beperkingen op wijzigingen aan softwarepakketten	niet
14.2.5	Principes voor engineering van beveiligde systemen	niet
14.2.6	Beveiligde ontwikkelomgeving	4.10
14.2.7	Uitbestede softwareontwikkeling	6.4
14.2.8	Testen van systeembeveiliging	6.5
14.2.9	Systeemacceptatietest	6.6
14.3	Testgegevens	
ISO nummer en naamgeving van statements		MBO nr.
14.3.1	Bescherming van testgegevens	niet

15	Leveranciersrelaties	
15.1	Informatiebeveiliging in leveranciersrelaties	
ISO nummer en naamgeving van statements		MBO nr.
15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties	niet
15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	1.15
15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	1.16
15.2	Beheer van dienstverlening van leveranciers	
ISO nummer en naamgeving van statements		MBO nr.
15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	6.7
15.2.2	Beheer van veranderingen in dienstverlening van leveranciers	4.11

16	Beheer van informatiebeveiligingsincidenten	
16.1	Beheer van informatiebeveiligingsincidenten en -verbeteringen	
ISO nummer en naamgeving van statements		MBO nr.
16.1.1	Verantwoordelijkheden en procedures	1.17
16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	1.18
16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging	2.6
16.1.4	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	4.12
16.1.5	Respons op informatiebeveiligingsincidenten	4.13
16.1.6	Lering uit informatiebeveiligingsincidenten	niet
16.1.7	Verzamelen van bewijsmateriaal	6.8

17	Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	
17.1	Informatiebeveiligingscontinuïteit	
ISO nummer en naamgeving van statements		MBO nr.
17.1.1	Informatiebeveiligingscontinuïteit plannen	niet
17.1.2	Informatiebeveiligingscontinuïteit implementeren	4.14
17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	niet
17.2	Redundante componenten	
ISO nummer en naamgeving van statements		MBO nr.
17.2.1	Beschikbaarheid van informatie verwerkende faciliteiten	4.15

18	Naleving	
18.1	Naleving van wettelijke en contractuele eisen	
ISO nummer en naamgeving van statements		MBO nr.
18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen	niet
18.1.2	Intellectuele-eigendomsrechten	niet
18.1.3	Beschermen van registraties	1.19
18.1.4	Privacy en bescherming van persoonsgegevens	1.20
18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	niet
18.2	Informatiebeveiligingsbeoordelingen	
ISO nummer en naamgeving van statements		MBO nr.
18.2.1	Onafhankelijke beoordeling van informatiebeveiliging	niet
18.2.2	Naleving van beveiligingsbeleid en -normen	6.9
18.2.3	Beoordeling van technische naleving	6.10

Bijlage 3: Framework informatiebeveiliging en privacy in het mbo