Onderwerp			Beheersmaatregel	Status beheersmaatregel 1)	Onderbouwing selectie/uitsluiting - generiek risico	Risico nummers, opmerkingen, eigenaar beheersmaatregel	Controlemaatregel
A.5 Informatie- beveiligingsbeleid	A.5.1.	Aansturing door de directie van de informatiebeveiliging	*Het verschaffen van directieaansturing van en -steun voor informatiebeveiliging in overeenstemming met bedrijfseisen en relevante wet- en regelgeving.*				
	A.5.1.1	Beleidsregels voor informatiebeveiliging	Ten behoeve van informatiebeveiliging moet een reeks beleidsregels worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	**3 = Aantoonbaar en geimplementeerd**	Beveiligingsinbreuken als gevolg van ontbreken van coördinatie vanuit de directie.	Risico 41 Bij een dispuut met een medewerker zal een rechter wegen of er regels gesteld waren. Het informatiebeveiligingsbeleid is in concept gereed, maar dient nog door de Directie te worden goedgekeurd. Voorgesteld wordt het beleid tijdens een volgende "top down / bottom up sessie" toe te lichten aan de medewerkers (notuleren). Naast beleid dienen er periodiek informatie-beveiligingsdoelstellingen te worden bepaald om proces van continue verbetering te kunnen plannen, bewaken en aantonen. **Eventuele IB doelstellingen 2017** - Behalen NEN7510 certificaat - Business Continuity Management (o.a. redundantie data center) - Concretisren afspraken met bedrijfskritische leveranciers (A) - IB aaantoonbaar meenemen in alle fasen software ontwikkeling - Vergroten Awareness / bewustwordeing (onderdeel 7510) - Aantoonbaar handelen overeenkomstig beleid / procedures (onderdeel 7510) - Implementeren SOM methodiek voor projectmatig werken. - Beschrijven (kritieke) bedrijfsprocessen	
	A.5.1.2	Beoordelen van het informatiebeveiligingsbeleid	Het beleid voor informatiebeveiliging moet met geplande tussenpozen of als zich significante veranderingen voordoen, worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	**3 = Aantoonbaar en geimplementeerd**	Medewerkers hebben onvoldoende aandacht voor het informatiebeveiligingsbeleid.	Risico 54 1x per 3 jaar (of indien nodig eerder) wordt het informatiebeveiligingsbeleid herbeoordeeld en opnieuw goedgekeurd (Informatiebeveiligingsbeleid). Door opname in Verbetercyclus als jaarplanitem wordt hierop toegezien.	
atiebeveiliging	A. 6.1	Interne organisatie	*Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen.*				

Onderwerp			Beheersmaatregel	Status beheersmaatregel 1)	Onderbouwing selectie/uitsluiting - generiek risico	Risico nummers, opmerkingen, eigenaar beheersmaatregel	Controlemaatregel
A.6. Organiseren van inform	A.6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging	Alle verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen.	**3 = Aantoonbaar en geimplementeerd**	Beveiligingsinbreuken als gevolg van het ontbreken of niet oppakken van verantwoordelijkheden door leidinggevenden.	Risico 41 en 43 Bij een dispuut met een medewerker zal een rechter wegen of er verantwoordelijkheden belegd waren. Rollen en Verantwoordelijkheden belegd middels: - Informatiebeveiligingsbeleid - Eigenaren beheersmaatregelen VVT - Proceseigenaren - Risicoeigenaren - Eigenaren bedrijfsmiddelen - Eigenaren documenten In alle procedures en werkinstructies zullen waar nodig verantwoordelijkheden in meer detail worden uitgewerkt. Door Wilco is een sjabloon gemaakt t.b.v. het uitwerken van procedures / ISMS documenten.	
	A.6.1.2	Scheiding van taken	Conflicterende taken en verantwoordelijkheidsgebieden moeten worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	**3 = Aantoonbaar en geimplementeerd**	Wegnemen van bedrijfsmiddelen. Misbruik van bevoegdheden.	Risico 43 Binnen de toepassingsgebeid van het ISMS (FysioOne) vloeien risico's hoofdzakelijk voort uit eventuele toegang tot gezondheidsinformatie door niet geautoriseerde personen. Intern op dit moment één type account. Alle interne medewerkers kunnen in het EPD van klanten. Op basis van risicobeoordeling is een verbetermaatregel opgenomen. Het aanmaken van FysioOne accounts is belegd bij de IT Directeur. Nog uitzoeken wie er eventueel nog meer bij kan en wie Wilco kan vervangen indien hij niet beschikbaar is. Nieuwe rollen en rechten module geef wel of geen toegang tot bepaalde menu items / schermen. Er is geen onderscheid te maken tussen creatie, lezen, muteren of verwijderen (CRUD)	
	A.6.1.3	Contact met overheidsinstanties	Er moeten passende contacten met relevante overheidsinstanties worden onderhouden.	**3 = Aantoonbaar en geimplementeerd**	Misbruik van bevoegdheden.	Procedure meldplicht datalekken beschrijft verantwoordelijkheden ten aanzien van contact met Autoriteit Persoonsgegevens. Nog te bepalen wie aangifte mag doen van een (vermoedelijk) strafbaar feit en wie contacten onderhoudt met Vecozo. (Vastleggen in ISMS Wiki of als bijlage bij beleid).	

Onderwerp			Beheersmaatregel	Status beheersmaatregel 1)	Onderbouwing selectie/uitsluiting - generiek risico	Risico nummers, opmerkingen, eigenaar beheersmaatregel	Controlemaatregel
	A.6.1.4	Contact met speciale belangengroepen	Er moeten passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en professionele organisaties worden onderhouden.	**3 = Aantoonbaar en geimplementeerd**	Toegang tot informatie door misbruik van kwetsbaarheden in applicaties.	IT Manager onderhoudt contacten met speciale belangengroepen (o.a. fora m.b.t. security, leveranciers m.b.t. kwetsbaarheden in hardware en software). Deze contacten zijn nu hoofdzakelijk reactief naar aanleiding van problemen.	
	A.6.1.5	Informatiebeveiliging in projectbeheer	Informatiebeveiliging moet aan de orde komen in projectbeheer, ongeacht het soort project.	**3 = Aantoonbaar en geimplementeerd**	Uitval van systemen door softwarefouten. Uitval van systemen door configuratiefouten. Fouten als gevolg van wijzigingen in andere systemen.	Risico 55 Op dit moment worden wijzigingen nog niet projectmatig aangepakt. Niels stelt een procedure / projectaanpak op. Een impactanalyse / risicobeoordeling ten aanzien van Informatiebeveiliging wordt onderdeel van de projectaanpak. SOM Academy zal als eerste (voorbeeld) project worden uitgewerkt. Migratie van klanten geregeld via standaard implementatieplan (customer journey)? Er dient een change proces te worden vastgesteld, waarin onderscheid wordt gemaakt tussen interne- en externe wijzigingen, grote- en kleine wijzigingen c. q. projecten. Aan te bevelen om bij implementaties onderscheid te gaan maken tussen ketens en individuele praktijken (hoe omgaan conversies)	
	A.6.2.	Mobiele apparatuur en telewerken	*Het waarborgen van de veiligheid van telewerken en het gebruik van mobiele apparatuur.*			\	
	A.6.2.1	Beleid voor mobiele apparatuur	Beleid en ondersteunende beveiligingsmaatregelen moeten worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	**3 = Aantoonbaar en geimplementeerd**	Verlies van mobiele apparatuur en opslagmedia	Risico 2 en 9 Gebruik van mobiele devices (BYOD) wordt toegestaan. Beleid en ondersteunende beheersmaatregelen zijn echter niet aanwezig. Diverse medewerkers gebruiken hun privé laptop / tablet om verbinding te maken met SOM netwerk. Dit geldt ook voor één van de ontwikkelaars die toegang heeft tot de FysioOne productie-omgeving. BYOD. Medewerkers ontvangen geen vergoeding voor gebruik van eigen apparatuur. Directie dient afweging te maken tussen voor- en nadelen (risico's), kosten en baten van het gebruik van eigen apparatuur.	
	A.6.2.2	Telewerken	Beleid en ondersteunende beveiligingsmaatregelen moeten worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties (thuiswerken) wordt bereikt, verwerkt of opgeslagen.	**3 = Aantoonbaar en geimplementeerd**	Toegang tot informatie doordat deze zich buiten de beschermde omgeving bevinden. Aanvallen via onbeveiligde systemen.	Risico 19 Doordat SpotOnMedics strategisch heeft gekozen voor cloudoplossingen is het makkelijk thuis te werken. Afspraken m.b.t. randvoorwaarden en acceptabel gebruik zijn niet aanwezig.	
Veilig personeel	A.7.1.	Voorafgaand aan het dienstverband	*Waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de functies waarvoor zij in aanmerking komen.*				

Onderwerp			Beheersmaatregel	Status beheersmaatregel 1)	Onderbouwing selectie/uitsluiting - generiek risico	Risico nummers, opmerkingen, eigenaar beheersmaatregel	Controlemaatregel
	7.1.1	Screening	Verificatie van de achtergrond van alle kandidaten voor een dienstverband moet worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en moet in verhouding staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.	**3 = Aantoonbaar en geimplementeerd**	Medewerkers hebben voldoende aandacht voor het informatiebeveiliging sbeleid. Misbruik van bevoegdheden	Risico 32 In gevallen waarbij gewerkt wordt voor overheden is screening verplicht O.a. support- en IT medewerkers van SOM hebben toegang tot gevoelige persoonsgegevens / gezondheidsinformatie van duizenden patiënten / cliënten. In enkele gevallen is er een verklaring omtrent gedrag (VOG) aangevraagd (IT Manager), maar dit is geen onderdeel van een structurele procedure. Door nieuwe rollen/rechten module kan toegang tot vertrouwelijke / gevoelige persoonsgegevens beter worden geregeld, maar risico's blijven bij bepaalde functies aanwezig.	
	7.1.2	Arbeidsvoorwaarden	De contractuele overeenkomst met medewerkers en contractanten moet hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie vermelden.	**3 = Aantoonbaar en geimplementeerd**	Medewerkers hebben voldoende aandacht voor het informatiebeveiliging sbeleid. Misbruik van bevoegdheden	Risico 32 In burgerlijk wetboek is een arbeidscontract verplicht gesteld	
	A.7.2	Tijdens het dienstverband	*Ervoor zorgen dat medewerkers en contractanten zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen.*				
	A.7.2.1	Directieverantwoordelijkheden	De directie moet van alle medewerkers en contractanten eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.	**3 = Aantoonbaar en geimplementeerd**	Beveiligingsinbreuken als gevolg van het ontbreken of niet oppakken van verantwoordelijkheden door leidinggevenden	Risico 32 Verantwoordelijkheden van de bestuurder(s) worden genoemd in BW	
	A.7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	Alle medewerkers van de organisatie en, voor zover relevant, contractanten moeten een passende bewustzijnsopleiding en -training krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	**3 = Aantoonbaar en geimplementeerd**	Medewerkers hebben onvoldoende aandacht voor het informatiebeveiliging sbeleid	Risico 10, 12, 17, 19, 20, 28, en 32 Bij een dispuut met een medewerker zal een rechter wegen of beleid toegelicht is	

Onderwerp			Beheersmaatregel	Status beheersmaatregel 1)	Onderbouwing selectie/uitsluiting - generiek risico	Risico nummers, opmerkingen, eigenaar beheersmaatregel	Controlemaatregel
	A.7.2.3	Disciplinaire procedure	Er moet een formele en gecommuniceerde disciplinaire procedure zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.	**3 = Aantoonbaar en geimplementeerd**	Beleid wordt niet gevolgd door ontbreken van sanctie	Risico 23 In burgerlijk wetboek wordt toegelicht hoe een dossier bij bijvoorbeeld ontslag opgezet moet worden	
	A.7.3	Beëindiging en wijziging van dienstverband	*Het beschermen van de belangen van de organisatie als onderdeel van de wijzigings- of beëindigingsprocedure van het dienstverband.*				
	7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband moeten worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer worden gebracht.	**3 = Aantoonbaar en geimplementeerd**	Onterecht hebben van rechten.	Risico 13, 18, 23 en 39	
A.8 Beheer van bedrijfsmiddelen	A.8.1.	Verantwoordelijkheid voor bedrijfsmiddelen	*Bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren.*				
	A.8.1.1	Inventariseren van bedrijfsmiddelen	Bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten moeten worden geïdentificeerd, en van deze bedrijfsmiddelen moet een inventaris worden opgesteld en onderhouden.	**3 = Aantoonbaar en geimplementeerd**	Wegnemen van bedrijfsmiddelen.	Bedrijfsmiddelen zijn nog niet geinventariseerd. Binnen scope is belangrijk deel van de middelen IT gerelateerd. Daarnaast echter ook algemen beveiligingsmiddelen en fysieke documenten.	
	A.8.1.2	Eigendom van bedrijfsmiddelen	Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden moeten een eigenaar hebben.	**3 = Aantoonbaar en geimplementeerd**	Wegnemen van bedrijfsmiddelen.		
	A.8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen	Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten moeten regels worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	**3 = Aantoonbaar en geimplementeerd**	Systemen worden niet gebruikt waarvoor ze bedoeld zijn	Risico 2, 9 en 19 Bij een dispuut met een medewerker zal een rechter wegen of er regels gesteld waren Niels aangesteld als kennishouder. voor Google drive. Instructiedocment beschikbaar.	

Onderwerp			Beheersmaatregel	Status beheersmaatregel 1)	Onderbouwing selectie/uitsluiting - generiek risico	Risico nummers, opmerkingen, eigenaar beheersmaatregel	Controlemaatregel
	A.8.1.4	Teruggeven van bedrijfsmiddelen	Alle medewerkers en externe gebruikers moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst teruggeven.	**3 = Aantoonbaar en geimplementeerd**	Wegnemen van bedrijfsmiddelen, Onterecht hebben van rechten	Risico 13 en 18, Beeindigingsprocedure.	
	A.8.2.	Informatieclassificatie	*Bewerkstelligen dat informatie een passend beschermingsniveau krijgt dat in overeenstemming is met het belang ervan voor de organisatie.*				
	A.8.2.1	Classificatie van informatie	Informatie moet worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	**3 = Aantoonbaar en geimplementeerd**	Toegang tot informatie door onduidelijkheid over bevoegdheid en vertrouwelijkheid van informatie.	Risico 3, 15, 40 en 42. Organisties die gezondheidsinformatie verwerken behoren dergelijke gegevens op uniforme wijze als vertrouwelijk te classificeren.	
	A.8.2.2	Informatie labelen	Om informatie te labelen moet een passende reeks procedures worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	**3 = Aantoonbaar en geimplementeerd**	Toegang tot informatie door onduidelijkheid over bevoegdheid en vertrouwelijkheid van informatie.Onveilig versturen van gevoelige informatie.	Risico 42	
	A.8.2.3	Behandelen van bedrijfsmiddelen	Procedures voor het behandelen van bedrijfsmiddelen moeten worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	**3 = Aantoonbaar en geimplementeerd**	Toegang tot informatie door onduidelijkheid over bevoegdheid en vertrouwelijkheid van informatie.	Risico 2, 9, 16, 19 en 20	
	A.8.3	Behandelen van media	*Onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie die op media is opgeslagen voorkomen.*				
	A.8.3.1	Beheer van verwijderbare media	Voor het beheren van verwijderbare media moeten procedures worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.	**3 = Aantoonbaar en geimplementeerd**	Toegang tot informatie op systemen of systeemonderdelen bij reparatie of verwijdering.	Risico 56 Beleid is dat er geen (gezondheids)informatie op laptops / desktops / mobiele devices aanwezig zou moeten zijn. Productie-data en testdata (demo praktijk) opgeslagen in gecertificeerd datacenter.	

Onderwerp			Beheersmaatregel	Status beheersmaatregel 1)	Onderbouwing selectie/uitsluiting - generiek risico	Risico nummers, opmerkingen, eigenaar beheersmaatregel	Controlemaatregel
	A.8.3.2	Verwijderen van media	Media moeten op een veilige en beveiligde manier worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures	**3 = Aantoonbaar en geimplementeerd**	Toegang tot informatie op systemen of systeemonderdelen bij reparatie of verwijdering.	Risico 20 Indien privacy gevoelige informatie; bewaartermijnen respecteren conform eis in WBP. https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/bewaren-van-persoonsgegevens Afrspraken over het veilig verwijderen van media (disks, vertrouwelijke documenten) ontbreken. Wellicht taak voor partij die werkplekbeheer	
	A.8.3.3	Media fysiek overdragen	Media die informatie bevatten, moeten worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.	**3 = Aantoonbaar en geimplementeerd**	Onveilig versturen van gevoelige informatie.Versturen van gevoelige informatie naar onjuiste persoon.	Risico 16 Vertrouwelijke informatie o.a. ID's van klanten worden nu onveilig verstuurd via o.a. E-mail. Praktijkhouder stuurt informatie per e-mail naar wilco t.b.v. migratie / conversie. Niet bekend of klanten data meegeven aan medewerkers. Sinds 1 januari 2017 werken alle nieuwe klanten op nieuwe manier. Conversiebestanden worden geupoad in portal Fysio-toekomst.nl. Deze omgeving komt op dit moment pas beschikbaar voor klanten na ondertekening van het contract en het verstrekken van het ID.	
A.9 Toegangsbeveiliging	A.9.1	Bedrijfseisen voor toegangsbeveiliging	*Toegang tot informatie en informatieverwerkende faciliteiten beperken.*				
	A.9.1.1	Beleid voor toegangsbeveiliging	Een beleid voor toegangsbeveiliging moet worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	**3 = Aantoonbaar en geimplementeerd**	Toegang tot informatie door onduidelijkheid over bevoegdheid en vertrouwelijkheid van informatie	Risico 21 en 34 Nu hebben alle interne medewerkers de Kwaliteitsmanagers rol (en kunnen alles zien). Uitgangspunt is dat praktijken toestemming gaan geven (eenmalig of voor lagere tijd) aan SpotOnMedics voor het vervullen van bepaalde rollen en het beschikken over bijbehorende toegangsrechten. Praktijk kan per rol opgeven of clientgegevens geanonimiseerd dienen te worden. Deze toestemmingsfunctie zal gebouwd worden en de gegeven toestemming zal worden gelogd. Teammanagers bepalen per rol / functie welke rechten nodig zijn. De rechten per rol worden "eenmalig" door IT ingericht. Teammanager stuurt e-mail naar IT, welke medewerker welke rol moet krijgen. Bespreken met Frans of in Bewerkersovereenkomst nog zal worden opgenomen dat voor het uitvoeren van bepaalde werkzaamheden er SOM medewerkers zijn met bepaalde rollen en bijbehorende rechten (declaratiecontract).	
	A.9.1.2	Toegang tot netwerken en netwerkdiensten	Gebruikers moeten alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	**3 = Aantoonbaar en geimplementeerd**	Toegang tot informatie door onduidelijkheid over bevoegdheid en vertrouwelijkheid van informatie	Risico 21 en 34 Gebruikers van FysioOne hebben toegang tot productie omgeving. IT heeft toegang tot servers en databases van productie-omgeving en daarnaast over test en acceptatie omgevingen, die eveneens in het datacenter worden gehost. Gasten WiFi gescheiden van SOM omgeving.	

Onderwerp			Beheersmaatregel	Status beheersmaatregel 1)	Onderbouwing selectie/uitsluiting - generiek risico	Risico nummers, opmerkingen, eigenaar beheersmaatregel	Controlemaatregel
	A.9.2	Beheer van toegangsrechten van gebruikers	*Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen.*				
	A.9.2.1	Registratie en uitschrijving van gebruikers	Een **formele** registratie- en uitschrijvingsprocedure moet worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	**3 = Aantoonbaar en geimplementeerd**	Misbruik van andermans identiteit. Onterecht hebben van rechten.	Risico 23 en 39 Bij een dispuut met een medewerker zal een rechter wegen of aantoonbaar is wie wat gedaan heeft. Toegang tot FysioOne is geregeld via domain controler / active directory. In kantoor SpotOnMedics geen domain controler beschikbaar. Sommige medewerkers hebben admin rechten op eigen PC. Bij nieuwe PC is IT administrator en heeft de mederker een gebruikersaccount. Als een nieuwe medewerker volgens de authorisatiematrix toegang mag hebben tot FysioOne, dan pakt de IT manager deze actie op, op basis van de e-mail van HR / Frans.	
	A.9.2.2	Gebruikers toegang verlenen	Een **formele** gebruikerstoegangsverleningsprocedure moet worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	**3 = Aantoonbaar en geimplementeerd**	Inbreuk op vertrouwelijkheid van informatie door het toelaten van externen in het pand of op het netwerk. Onterecht hebben van rechten	Risico 21, 28 en 34 Gebruikerswachtwoorden in database FysioOne zijn MD5 versleuteld. Regels voor sterke wachtwoorden zijn in FysioOne instelbaar. Default is een sterk wachtwoord; praktijkhouder kan kiezen voor éénvoudigere wachtwoorden. Default is dat ieder e 90 dagen wachtwoord dient te worden gewijzigd. Volledige wachtwoordhistorie wordt bewaard, waardoor hergebruik oude wachtwoorden niet mogelijk is.	
	A.9.2.3	Beheren van speciale toegangsrechten	Het toewijzen en gebruik van bevoorrechte toegangsrechten moeten worden beperkt en gecontroleerd.	**3 = Aantoonbaar en geimplementeerd**	Misbruik van bevoegdheden. Het niet hard kunnen maken van welke persoon over welk account beschikt.	Een Datacenter Administrator (Bekend in IT team) Iedere it medewerker heeft persoonlijk account met admin rechten. Via zelfde account / rechten kan vpn toegang worden verkregen tot datacenter. Alle IT medewerkers hebben toegang tot Datacenter portal (VMWare, zie screenshot). Alle medewerkers hebben Kwaliteitsmedewerker Profiel in FysioOne. Enkele medewerkers hebben super user account.	

Onderwerp			Beheersmaatregel	Status beheersmaatregel 1)	Onderbouwing selectie/uitsluiting - generiek risico	Risico nummers, opmerkingen, eigenaar beheersmaatregel	Controlemaatregel
	A.9.2.4	Beheer van geheime authenticatie-informatie van gebruikers	Het toewijzen van geheime authenticatie-informatie moet worden beheerst via een formeel beheersproces.	**3 = Aantoonbaar en geimplementeerd**	Misbruik van andermans identiteit.	FysioOne: accountnaam wordt per e-mail verstuurd en op papier verstrekt. Medewerker vraagt wachtwoord op via wachtwoord vergeten functie.Voor pc's, gebruiker direct wachtwoord laten wijzigen (IT maakt het gebruikersaccount op de PC). Google for domains. Derde partij? beheert Google cloud omgeving voor SpotOnMedics. Slack communicatiemiddel?	
	A.9.2.5	Beoordeling van toegangsrechten van gebruikers	Eigenaren van bedrijfsmiddelen moeten toegangsrechten van gebruikers regelmatig beoordelen.	**3 = Aantoonbaar en geimplementeerd**	Het niet hard kunnen maken van welke persoon over welk account beschikt. Onterecht hebben van rechten.	Risico 39 Jaarplan item in verbetercyclus FysioOne.Alle teamleiders + diirectie beoordelen jaarlijks of rollen en rechten nog up to date zijn.	
	A.9.2.6	Toegangsrechten intrekken of aanpassen	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten moeten bij beëindiging van hun dienstverband, contract of overeenkomst worden verwijderd, en bij wijzigingen moeten ze worden aangepast.	**3 = Aantoonbaar en geimplementeerd**	Onterecht hebben van rechten	Risico 13, 18, 23 en 39 Directie mailt lijnmanagers dat medewerker uit dienst is. Lijnmanagers bepalen welke acties ze moeten doen om rechten in te trekken of accounts te disabelen. Teamleiders stuurt mail naar it als medewerker andere rol krijgt of account dient te worden gedisabled (twee mogelijkheden: je mag niet inloggen account geblokkerd, account verwijderd. Defeted flag, zodat acties e.d. wel aan persoon gekoppeld blijven.	
	A.9.3	Verantwoordelijkheden van gebruikers	*Gebruikers verantwoordelijk maken voor het beschermen van hun authenticatie-informatie.*				
	A.9.3.1	Geheime authenticatie-informatie gebruiken	Van gebruikers moet worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.	**3 = Aantoonbaar en geimplementeerd**	Toegang tot informatie door slecht wachtwoordgebruik.	Risico 35	
	A.9.4	Toegangsbeveiliging van systeem en toepassing					
	A.9.4.1	Beperking toegang tot informatie	Toegang tot informatie en systeemfuncties van applicaties moet worden beperkt in overeenstemming met het beleid voor toegangscontrole.	**3 = Aantoonbaar en geimplementeerd**	Onterecht hebben van rechten	Risico 21, 28 en 34 Bij een dispuut met een medewerker zal een rechter wegen of de medewerker toegang had	
	A.9.4.2	Beveiligde inlogprocedures	Indien het beleid voor toegangsbeveiliging dit vereist, moet toegang tot systemen en toepassingen worden beheerst door een beveiligde inlogprocedure.	**3 = Aantoonbaar en geimplementeerd**	Toegang tot informatie door slecht wachtwoordgebruik	Beleid: ieder systeem / applicatie heeft minimaal gebruikersnaam, wachtwoord. FysioOne 2 factor authenticatie waarschijnlijk in Q2 beschikbaar. Nog standpunt in te nemen t.a.v. interne medewerkers. Wanneer 2 factor nodig (ook in geval van telewerken / mobiel gebruik). Er is een mobiele agenda voor FysioOne (mobiele website). Praktijkhouder mag bepalen of hij 2factor wil toepassen.	

Onderwerp			Beheersmaatregel	Status beheersmaatregel 1)	Onderbouwing selectie/uitsluiting - generiek risico	Risico nummers, opmerkingen, eigenaar beheersmaatregel	Controlemaatregel
	A.9.4.3	Systeem voor wachtwoordbeheer	Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden waarborgen.	**3 = Aantoonbaar en geimplementeerd**	Toegang tot informatie door slecht wachtwoordgebruik	Uitgebreide module beschikbaar. Zie screen shots. Vaste policy, wachtwoord lengte, min 8 max 16 positie, alphanumeriek, hoofdletter, kleine letter, cijfer, vooraf bepaalde bijzondere tekens minimaal 1. Frequentie vast 90 dagen. Wachtwoordbeleid t.a.v. admin accounts servers nog bepalen en daarna implementeren.	
	A.9.4.4	Speciale systeemhulpmiddelen gebruiken	Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen moet worden beperkt en nauwkeurig worden gecontroleerd.	**3 = Aantoonbaar en geimplementeerd**	Onterecht hebben van rechten.	Alle systeemhulpmiddelen voor alle IT'ers beschikken. Beleid bepalen (Wilco)	
	A.9.4.5	Toegangsbeveiliging op programmabroncode	Toegang tot de programmabroncode moet worden beperkt.	**3 = Aantoonbaar en geimplementeerd**	Onterecht hebben van rechten. Onvoldoende aandacht voor beveiliging bij softwareontwikkeling	Team foundation server. Alle IT'ers toegang tot productie code. Ontwikkelomgeving op eigen laptop.	
A.10 Cryptografie	A.10.1	Cryptografische beheersmaatregelen	*Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.*				
	A.10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels moet tijdens hun gehele levenscyclus een beleid worden ontwikkeld en geïmplementeerd.	**3 = Aantoonbaar en geimplementeerd**	Inbreuk op vertrouwelijkheid door wetgeving ten aanzien van gebruik van cryptografie	Risico 27 Aantal mensen met laptop "moeten" informatie bij hebben. Op deel van de laptops is Bitlocker ingeschakeld. Er is geen beleid beschikbaar. FysioOne broncode wordt beheerd met Team Foundation Server. Beleid is dat alle informatie in de cloud wordt opgeslagen in niet op locale drive. Alle backups en kopieën blijven in het datacenter. Sommige medewerkers versturen bestanden die met wachtwoorden zijn beveiligd(wachtwoorden mondeling communiceren). Gebruikerswachtwoorden in database zijn MD5 versleuteld. Toegang tot datacenter is nu met persoonlijke certificaten. Hypergrid beheeromgeving is nu toegankelijk met gebruikersnaam en wachtwoord; zou 2 factor moeten zijn.	
	A.10.1.2	Sleutelbeheer		**3 = Aantoonbaar en geimplementeerd**	Inbreuk op vertrouwelijkheid door wetgeving ten aanzien van gebruik van cryptografie.		

Onderwerp			Beheersmaatregel	Status beheersmaatregel 1)	Onderbouwing selectie/uitsluiting - generiek risico	Risico nummers, opmerkingen, eigenaar beheersmaatregel	Controlemaatregel
A.11 Fysieke beveiliging en beveiliging van de omgeving	A.11.1	Beveiligde gebieden	*Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatieverwerkende faciliteiten van de organisatie voorkomen.*				
	A.11.1.1	Fysieke beveiligingszone	Beveiligingszones moeten worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten.	**3 = Aantoonbaar en geimplementeerd**	Ongeautoriseerde fysieke toegang	Risico 1, 50 en 52 Of een gebouwkantoor afdoende beveiligd was zal door bijvoorbeeld een verzekeraar gewogen worden	
	A.11.1.2	Fysieke toegangsbeveiliging	Beveiligde gebieden moeten worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	**3 = Aantoonbaar en geimplementeerd**	Inbreuk op vertrouwelijkheid van informatie door het toelaten van externen in het pand of op het netwerk. Brand	Risico 1, 13 en 37 Deur naar centrale hal (personeelsingang) is gedurende de dag open. Printer(s) toegankelijk voor alle medewerkers. Niet alle kasten met vertrouwelijke informatie zijn afsluitbaar of afgesloten. Vertrouwelijke klantinformatie (patiëntgegevens) opgeslagen in datacenter. Beleid is dat geen vertrouwelijke informatie aanwezig is op lokale PC's	
	A.11.1.3	Kantoren, ruimten en faciliteiten beveiligen	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en toegepast.	**3 = Aantoonbaar en geimplementeerd**	Wegnemen van bedrijfsmiddelen. Ongeautoriseerde fysieke toegang.	Risico 1, 37, 50 en 52	
	A.11.1.4	Beschermen tegen bedreigingen van buitenaf	Tegen natuurrampen, kwaadwillige aanvallen of ongelukken moet fysieke bescherming worden ontworpen en toegepast.	**3 = Aantoonbaar en geimplementeerd**	Overstroming en wateroverlastBrand, Explosie, Rampen		
	A.11.1.5	Werken in beveiligde gebieden	Voor het werken in beveiligde gebieden moeten procedures worden ontwikkeld en toegepast.	**3 = Aantoonbaar en geimplementeerd**	SpotOnMedics heeft geen beveiligde gebieden.	Volgens ARBO zijn regels voor (veilig) werken in beschermde ruimten verplicht	
	A.11.1.6	Laad- en loslocatie	Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, moeten worden beheerst, en zo mogelijk worden afgeschermd van informatieverwerkende faciliteiten om onbevoegde toegang te vermijden.	**0 = Buiten scope**	SpotOnMedics heeft geen laad en loslocatie		
	A.11.2	Apparatuur	*Verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie voorkomen.*				

Onderwerp			Beheersmaatregel	Status beheersmaatregel 1)	Onderbouwing selectie/uitsluiting - generiek risico	Risico nummers, opmerkingen, eigenaar beheersmaatregel	Controlemaatregel
	A.11.2.1	Plaatsing en bescherming van apparatuur	Apparatuur moet zo worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.	**3 = Aantoonbaar en geimplementeerd**	Toegang tot informatie door middel van afluisterapparatuur. Ongeautoriseerde fysieke toegang	Risico 15 Productie omgeving in gecertificeerd datacenter. Apparatuur in kantoor betreft standaard werkplekken.	
	A.11.2.2	Nutsvoorzieningen	Apparatuur moet worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	**3 = Aantoonbaar en geimplementeerd**	Uitval van facilitaire middelen (gas, water, electra, airco).	Productie omgeving in gecertificeerd datacenter. Apparatuur in kantoor betreft standaard werkplekken. Kantoorwerkzaamheden kunnen op iedere locatie worden uitgevoerd, omdat met Cloudoplossingen wordt gewerkt.	
	A.11.2.3	Beveiliging van bekabeling	Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen interceptie, verstoring of schade.	**3 = Aantoonbaar en geimplementeerd**	Toegang tot informatie door misbruiken van zwakheden in netwerkbeveiliging.	Productie omgeving in gecertificeerd datacenter. Apparatuur in kantoor betreft standaard werkplekken. Kantoorwerkzaamheden kunnen op iedere locatie worden uitgevoerd, omdat met Cloudoplossingen wordt gewerkt.	
	A.11.2.4	Onderhoud van apparatuur	Apparatuur moet correct worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	**3 = Aantoonbaar en geimplementeerd**	Uitval van systemen door hardwarefouten.	Apparatuur in datacenter is geen eigendom van SOM. Server- en opslagcapaciteit wordt als dienst afgenomen.	
	A.11.2.5	Verwijdering van bedrijfsmiddelen	Apparatuur, informatie en software mogen niet van de locatie worden meegenomen zonder voorafgaande goedkeuring.	**3 = Aantoonbaar en geimplementeerd**	Wegnemen van bedrijfsmiddelen Toegang tot informatie doordat deze zich buiten de beschermde omgeving bevinden.	Risico 57	
	A.11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	Bedrijfsmiddelen die zich buiten het terrein bevinden, moeten worden beveiligd, waarbij rekening moet worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.	**3 = Aantoonbaar en geimplementeerd**	Toegang tot informatie doordat deze zich buiten de beschermde omgeving bevinden.	Risico 9 en 57	
	A.11.2.7	Veilig verwijderen of hergebruiken van apparatuur	Alle onderdelen van de apparatuur die opslagmedia bevatten, moeten worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of veilig zijn overschreven.	**3 = Aantoonbaar en geimplementeerd**	Toegang tot informatie op systemen of systeemonderdelen bij reparatie of verwijdering	Risico 14 Door beleid alle date in cloud op te slaan. Risico beperkt van locale data op apparatuur.	

Onderwerp			Beheersmaatregel	Status beheersmaatregel 1)	Onderbouwing selectie/uitsluiting - generiek risico	Risico nummers, opmerkingen, eigenaar beheersmaatregel	Controlemaatregel
	A.11.2.8	Onbeheerde gebruikersapparatuur	Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.	**3 = Aantoonbaar en geimplementeerd**	Toegang tot informatie door onbeheerd achterlaten van werkplekken	Risico 1, 14 en 37	
	A.11.2.9	'Clear desk'- en 'clear screen'-beleid	Er moet een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten worden ingesteld.	**3 = Aantoonbaar en geimplementeerd**	Misbruik van andermans identiteit Toegang tot informatie door onbeheerd achterlaten van werkplekken.	Risico 14, 15 en 20 Op sommige PC's is automatische vergrendeling ingesteld. Hier is nog geen beleid voor beschikbaar.	
A.12 Beveiliging bedrijfsvoering	A.12.1	Beveiliging bedrijfsvoering	*Correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen.*				
	A.12.1.1	Gedocumenteerde bedieningsprocedures	Bedieningsprocedures moeten worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben.	**3 = Aantoonbaar en geimplementeerd**	Niet beschikbaar zijn van informatie of diensten vanuit derden.Kwijtraken van belangrijke kennis bij vertrek of niet beschikbaar zijn van medewerker	Risico 4, 12, 17, 32 en 38 Bij een dispuut met een medewerker zal een rechter wegen of werkwijzen duidelijk waren Al diverse (concept) procedures en werkinstructies aanwezig. O.a. het OTAP proces, backup proces en template voor bestellen nieuwe server.	
	A.12.1.2	Wijzigingsbeheer	Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging moeten worden beheerst.	**3 = Aantoonbaar en geimplementeerd**	Fouten als gevolg van wijzigingen in andere systemen.	Risico 4 Er is een wensenlijst (1100 wensen). Klanten zijn niet tevreden over het aantal wensen dat dat geimplementeerd wordt. Besloten is wensenlijst in Academy toe te voegen. Klanten krijgen 3 votes, waarmee zij kunnen beïnvloeden welke wijzigingen worden meegenomen in voglende release. Academy wordt aparte website (o.a. e-learning; waarschijnlijk ook voor interne medewerkers). Releaseboard gaat stemmen welke wensen / aanpassingen in release worden meegenomen. Releaseboard onderhoudt "Releasplanningsspreadsheet". IT Manager maakt met team een schatting van benodigde ontwikkeltijd voor geselecteerde items. Na bepalen definitieve inhoudt wordt ontwikkeling in detail gepland door IT manager. Productmanager en IT Manager bespreken periodiek inhoud / voortgang release (releaseplanning gesprek). Dit overleg heeft nog geen formele status. In dit overleg zou risicobeoordeling t.a.v. wijzigingen kunnen worden geborgd. Productmanager / Nicole geeft akkoord op requirements en na ontwikkeling toetsen of conform requirements ontwikkeld is.	

Onderwerp			Beheersmaatregel	Status beheersmaatregel 1)	Onderbouwing selectie/uitsluiting - generiek risico	Risico nummers, opmerkingen, eigenaar beheersmaatregel	Controlemaatregel
	A.12.1.3	Capaciteitsbeheer	Het gebruik van middelen moet worden gemonitord en afgestemd, en er moeten verwachtingen worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.	**3 = Aantoonbaar en geimplementeerd**	Overbelasten van netwerkdiensten.	Overzicht van databases / servers aanwezig op computer van ontwikkelaar Tom. Dit wordt een beeldscherm aan de muur van IT. Taken en verantwoordelijkheden niet aantoonbaar belegd. Door IT is Spmonitor programma ontwikkeld, waarmee diverse kengetallen / lopende activiteiten zichtbaar worden gemaakt (status batchprocessen, openstaande support tickets, aantal connecties). Spmonitor monitor schermen worden in vorm van slide show vertoond op een scherm bij IT aan de muur.	
	A.12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	**3 = Aantoonbaar en geimplementeerd**	Uitval van systemen door softwarefouten. Uitval van systemen door configuratiefouten.	Risico 55 Er wordt sinds kort gewerkt met een OTAP straat; voorheen OP. IT Manger werkt aan OTAP document dat nog wordt besproken met het team. Alle ontwikkelaars hebben toegang tot alle klant-omgevingen en klantdata; van deze toegang wordt geen log bijgehouden. In principe werken ontwikkelaars met een eigen demo praktijk (toegang tot database is niet willekeurig, maar wordt bewust gekozen). Er zijn meerdere database servers aanwezig. Op server 1 staat de master, die gebruikers doorleidt naar de juiste database server. Test-, Acceptatie- en Productie omgevingen draaien in zelfde datacenter op eigen virtuele servers.	
	A.12.2	Bescherming tegen malware	*Waarborgen dat informatie en informatieverwerkende faciliteiten beschermd zijn tegen malware.*				
	A.12.2.1	Beheersmaatregelen tegen malware	Ter bescherming tegen malware moeten beheersmaatregelen voor detectie, preventie en herstel worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.	**3 = Aantoonbaar en geimplementeerd**	Systemen raken besmet met malware.	Risico 27 en 28 Alleen websevers hebben verbinding met internet (geen anti virus nodig). Alleen toegang met valide gebruikersnaam en wachtwoord. Upload bestanden beperkt aantal formaten. Bestanden worden niet geopend op server. Ontwikkelaars kunnen alleen via VPN op server met eigen account. Domainserver in datacenter aanwezig, zodat servers met elkaar kunnen communiceren. Toepassing van de server bepaalt wat voor server het is (web, file, database, application server, conversion server, main server voor code waarvan het gedistribueerd wordt.). Ontwikkelaars hebben niet allemaal een laptop van de zaak. Kans aanwezig dat besmetting vanaf prive PC op server terecht komt.	
	A.12.3	Back-up	*Beschermen tegen het verlies van gegevens.*				

Onderwerp			Beheersmaatregel	Status beheersmaatregel 1)	Onderbouwing selectie/uitsluiting - generiek risico	Risico nummers, opmerkingen, eigenaar beheersmaatregel	Controlemaatregel
	A.12.3.1	Back-up van informatie	Regelmatig moeten back-upkopieën van informatie, software en systeemafbeeldingen worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	**3 = Aantoonbaar en geimplementeerd**	Informatieverlies door verlopen van houdbaarheid van opslagwijze. Wegnemen van bedrijfsmiddelen. Systemen raken besmet met malware.	Risico 3 en 24 Virtuele machines worden gebackuped. Backups blijven in datacenter in backup opslaglocatie. Backups 1e maand, 1e kwartaal en 1e jaar worden bewaar en alle backups van laatse 14 dagen. Onlangs dataverlies doordat een dagbackup niet bleek te functioneren. Tekening en beschrijving van backup proces in concept beschikbaar.	
	A.12.4	Verslaglegging en monitoren	*Gebeurtenissen vastleggen en bewijs verzamelen.*				
	A.12.4.1	Gebeurtenissen registreren	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, moeten worden gemaakt, bewaard en regelmatig worden beoordeeld.	**3 = Aantoonbaar en geimplementeerd**	Tijdens een rechtszaak is het bedrijf niet in staat om de benodigde bewijzen te kunnen leveren.	Risico 17, 27 en 28 Bij diverse functies in FysioOne historie aanwezig. Nog geen logging wie welke gezondheisinformatie heeft geraadpleegd of gewijzigd. Met nieuwe rollen/rechtenmodule kan toegang tot functies/schermen beter worden geregeld. Toegang tot een scherm betekent vooralsnog dat ook kan worden gemuteerd of dat gegevens kunnen worden verwijderd. Een deel van informatie in EPD kan worden geanonimiseerd omdat dit automatisch wordt samengesteld; dit geldt niet voo informatie die door therapeut in "het verhaal" wordt opgenomen.	
	A.12.4.2	Beschermen van informatie in logbestanden	Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang.	**2 = Deels geregeld**	Het niet hard kunnen maken van welke persoon over welk account beschikt.	Logbestanden zijn nu nog niet gescheiden van logs in productie- omgeving. IT medewerkers hebben toegang tot alles en kunnen indien ze dit willen eigen sporen uitwissen.	
	A.12.4.3	Logbestanden van beheerders en operators	Activiteiten van systeembeheerders en -operators moeten worden vastgelegd en de logbestanden moeten worden beschermd en regelmatig worden beoordeeld.	**2 = Deels geregeld**	Het niet hard kunnen maken van welke persoon over welk account beschikt. Misbruik van bevoegdheden.	Logbestanden zijn nu nog niet gescheiden van logs in productie- omgeving. IT medewerkers hebben toegang tot alles en kunnen indien ze dit willen eigen sporen uitwissen. SLA ondertekenen? Klant toestemming laten geven. (via FysioOne of door een ticket in te sturen?)	
	A.12.4.4	Kloksynchronisatie	De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein moeten worden gesynchroniseerd met één referentietijdbron.	**3 = Aantoonbaar en geimplementeerd**	Tijdens een rechtszaak is het bedrijf niet in staat om de benodigde bewijzen te kunnen leveren.	Bij een dispuut zal een rechter wegen of bewijs jundisch bruikbaar is. Er wordt gebruikgemaakt van de mechanismen in de Microsoft besturngssystemen. Eventueel kunnen tijden worden meegestuurd door programma's.	
	A.12.5	Beheersing van operationele software	*De integriteit van operationele systemen waarborgen.*				

Onderwerp			Beheersmaatregel	Status beheersmaatregel 1)	Onderbouwing selectie/uitsluiting - generiek risico	Risico nummers, opmerkingen, eigenaar beheersmaatregel	Controlemaatregel
	A.12.5.1	Software installeren op operationele systemen	Om het op operationele systemen installeren van software te beheersen moeten procedures worden geïmplementeerd.	**2 = Deels geregeld**	Fouten als gevolg van wijzigingen in andere systemen	Nu kan iedere IT medewerker / ontwikkelaar software in productie nemen. We willen naar automatische deployment (meenemen in development proces). Er is nu geen dedicated test server. Het zijn gescheiden virtuele servers op zelfde infrastructuur.	
	A.12.6	Beheer van technische kwetsbaarheden	*Benutting van technische kwetsbaarheden voorkomen.*				
	A.12.6.1	Beheer van technische kwetsbaarheden	Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt moet tijdig worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en passende maatregelen moeten worden genomen om het risico dat ermee samenhangt aan te pakken.	**3 = Aantoonbaar en geimplementeerd**	Systemen raken besmet met malware. Toegang tot informatie door misbruik van kwetsbaarheden in applicaties Toegang tot informatie door misbruiken van zwakheden in netwerkbeveiliging.	Risico 27 Het doorvoeren van Windows Update in het VDC is een taak van IT & development. Wekelijks worden eventuele updates doorgevoerd op advies van Microsoft. Doorgevoerde updates worden geregistreerd in het "Windows Update Log"	
	A.12.6.2	Beperkingen voor het installeren van software	Voor het door gebruikers installeren van software moeten regels worden vastgesteld en geïmplementeerd.	**3 = Aantoonbaar en geimplementeerd**	Systemen raken besmet met malware. Informatieverlies door verlopen van houdbaarheid van opslagwijze.	Risico 27 Verantwoordelijkheden m.b.t. beheer computerapparatuur / lokale netwerk onduidelijk. Beperking m.b.t. installeren van software opnemen in beleid m.b.t. aanvaardbaar gebruik (Personeels-handboek)	
	A.12.7	Overwegingen betreffende audits van informatiesystemen	*De impact van auditactiviteiten op uitvoeringssystemen zo gering mogelijk maken.,*				
	A.12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen	Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, moeten zorgvuldig worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.	**3 = Aantoonbaar en geimplementeerd**	Toegang tot informatie door onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.	Risico 27 Niet bekend of pen tests zijn uitgevoerd en wat bevindingen zijn. We hebben de guard / vulnerability scanner van McAfee. Als er iets mis is geeft de Guard een melding naar Wilco. Als reactie van SOM op kwetsbaarheid uitblijft, dan wordt telefonisch contact opgenomen met Wilco.	
tiebeveiliging	A.13.1	Beheer van netwerkbeveiliging	*De bescherming van informatie in netwerken en de ondersteunende informatieverwerkende faciliteiten waarborgen.*				

Onderwerp			Beheersmaatregel	Status beheersmaatregel 1)	Onderbouwing selectie/uitsluiting - generiek risico	Risico nummers, opmerkingen, eigenaar beheersmaatregel	Controlemaatregel
A.13 Communica	A.13.1.1	Beheersmaatregelen voor netwerken	Netwerken moeten worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	**3 = Aantoonbaar en geimplementeerd**	Toegang tot informatie door misbruiken van zwakheden in netwerkbeveiliging. Aanvallen via onbeveiligde systemen	Risico 27 Netwerk InternedServices te besturen via HyperGnd portal. Welke machine welke netwerkkaart, interne en externe ip adressen, domain controller. Deel door SOM beheerd en deel door IS. (input TOM, configuratie Datacenter (oa. dmz, firewalls, ...) *** vertrouwelijk ***	
	A.13.1.2	Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten moeten worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	**3 = Aantoonbaar en geimplementeerd**	Toegang tot informatie door misbruiken van zwakheden in netwerkbeveiliging. Aanvallen via onbeveiligde systemen	VPN voor communicatie van locale pc naar server (RDP, username / password), na vpn login nog server login. SSL voor communicatie tussen browser en website/api. Via RDP ook ftp communicatie. Ophalen data via FTP bij externe t.b.v. conversies (bron: Wilco)	
	A.13.1.3	Scheiding in netwerken	Groepen van informatiediensten, -gebruikers en -systemen moeten in netwerken worden gescheiden.	**3 = Aantoonbaar en geimplementeerd**	Systemen raken besmet met malware.Toegang tot informatie door misbruiken van zwakheden in netwerkbeveiliging.	Risico 34 Gescheiden gasten wifi, eigen wifi (2 accounts). Kleine server + switch (onderscheid voip + internet). (kast is nog niet beveiligd, geen eigenaar). toevoegen aan inventarisatie bedrijfsmiddelen. Taken server (finance?)?	
	A.13.2	Informatietransport	*Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe entiteit.*				
	A.13.2.1	Beleid en procedures voor informatietransport	Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, moeten formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht zijn.	**3 = Aantoonbaar en geimplementeerd**	Toegang tot informatie door onduidelijkheid over bevoegdheid en vertrouwelijkheid van informatie. Onveilig versturen van gevoelige informatie.	Risico 8 en 31 Bij een dispuut zal een rechter wegen of er regels gesteld waren Communicatie tussen SOM en externe partijen via SSL. Geen bewerkersovereenkomsten. Overeenkomsten tussen klanten SOM en derden. Social Media berichtgeving wordt gevolgd door Marketing met behulp van Hootsuite tool.	
	A.13.2.2	Overeenkomsten over informatietransport	Overeenkomsten moeten betrekking hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	**2 = Deels geregeld**	Onveilig versturen van gevoelige informatie.	Risico 8 Bij een dispuut zal een rechter wegen of er regels gesteld waren Overeenkomsten met derden ivm koppeling / datauitwisseling (input Directie)	
	A.13.2.3	Elektronische berichten	Informatie die is opgenomen in elektronische berichten moet passend beschermd zijn.	**3 = Aantoonbaar en geimplementeerd**	Versturen van gevoelige informatie naar onjuiste persoon	Risico 31, 38 en 40 Classificatie / Aanvaardbaar gebruik Mailverkeer (Marc)	

Onderwerp			Beheersmaatregel	Status beheersmaatregel 1)	Onderbouwing selectie/uitsluiting - generiek risico	Risico nummers, opmerkingen, eigenaar beheersmaatregel	Controlemaatregel
	A.13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen moeten worden vastgesteld, regelmatig worden beoordeeld en gedocumenteerd.	**3 = Aantoonbaar en geimplementeerd**	Tegen het bedrijf worden juridische stappen genomen vanwege het niet veilig omgaan met vertrouwelijke informatie.Misbruik van bevoegdheden	Risico 31, 38 Bij een dispuut zal een rechter wegen of er regels gesteld waren.	
A.14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen	A.14.1	Beveiligingseisen voor informatiesystemen	*Waarborgen dat informatiebeveiliging integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus. Hiertoe behoren ook de eisen voor informatiesystemen die diensten verlenen via openbare netwerken.*				
	A.14.1.1	Analyse en specificatie van informatiebeveiligingseisen	De eisen die verband houden met informatiebeveiliging moeten worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	**3 = Aantoonbaar en geimplementeerd**	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	Risico 8 Door Productmanager FysioOne (Nicole) wordt releaseplanning bijgehouden. Informatie-beveiligingseisen zullen aan dit spreadsheet worden toegevoegd. Requirements zullen in meer detail uitgewerkt moeten gaan worden; hierbij kan dan ook de impact (risicobeoordeling) ten aanzien van beschikbaarheid, integriteit en veiligheid (B.I.V.) worden meegenomen.	
	A.14.1.2	Toepassingsdiensten op openbare netwerken beveiligen	Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, moet worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.	**3 = Aantoonbaar en geimplementeerd**	Inbreuk op vertrouwelijkheid door wetgeving ten aanzien van informatie in de cloud	Verbinding tussen webclient & FysioOne server is versleuteld via SSL. Er wordt gebruik gemaakt van een Extended Validation certificaat. Certificaten worden geleverd door Networkin4all, die SpotOnMedics ook per e-mail op de hoogte houdt van vervaldata. Communicatie tussen FysioOne en externe partijen zoals Vecozo verloopt eveneens via SSL. Vecozo geeft certificaat aan praktijken, die dit op hun beurt aan SOM verstrekken, zodat het op de SOM server geinstalleerd kan worden. Zonder certificaat kunnen berichten niet worden verzonden. Aandachtspunt Informatics koppeling slaat batch bestand op lokale PC van gebruiker op.	

Onderwerp			Beheersmaatregel	Status beheersmaatregel 1)	Onderbouwing selectie/uitsluiting - generiek risico	Risico nummers, opmerkingen, eigenaar beheersmaatregel	Controlemaatregel
	A.14.1.3	Transacties van toepassingsdiensten beschermen	Informatie die deel uitmaakt van transacties van toepassingsdiensten moet worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.	**3 = Aantoonbaar en geimplementeerd**	Tegen het bedrijf worden juridische stappen genomen vanwege het niet veilig omgaan met vertrouwelijke informatie.	Gebruik SSL bij alle communicatie Zie 14.1.2	
	A.14.2	Beveiliging in ontwikkelings- en ondersteunende processen	*Bewerkstelligen dat informatiebeveiliging wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevenscyclus van informatiesystemen.*				
	A.14.2.1	Beleid voor beveiligd ontwikkelen	Voor het ontwikkelen van software en systemen moeten regels worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie worden toegepast.	**3 = Aantoonbaar en geimplementeerd**	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	Risico 11 Ervaren ontwikkelaars betrokken bij ontwikkeling van FysioOne. Dagelijks wordt TrustGuard Vulnerability scan uitgevoerd.	
	A.14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen	Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling moeten worden beheerst door het gebruik van formele controleprocedures voor wijzigingsbeheer.	**3 = Aantoonbaar en geimplementeerd**	Fouten als gevolg van wijzigingen in andere systemen.	Risico 8 en 11	
	A.14.2.3	Technische beoordeling van toepassingen na wijzigingen bedieningsplatform	Als bedieningsplatforms zijn veranderd, moeten bedrijfskritische toepassingen worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie.	**3 = Aantoonbaar en geimplementeerd**	Toegang tot informatie door misbruik van kwetsbaarheden in applicaties. Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	Risico 11 SOM is verantwoordelijk voor het patchen van de besturingssystemen.	
	A.14.2.4	Beperkingen op wijzigingen aan softwarepakketten	Wijzigingen aan softwarepakketten moeten worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen moeten strikt worden gecontroleerd.	**3 = Aantoonbaar en geimplementeerd**	Toegang tot informatie door misbruik van kwetsbaarheden in applicaties.Fouten als gevolg van wijzigingen in andere systemen.	Risico 11	

Onderwerp			Beheersmaatregel	Status beheersmaatregel 1)	Onderbouwing selectie/uitsluiting - generiek risico	Risico nummers, opmerkingen, eigenaar beheersmaatregel	Controlemaatregel
	A.14.2.5	Principes voor engineering van beveiligde systemen	Principes voor de engineering van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.	**3 = Aantoonbaar en geimplementeerd**	Uitval van systemen door softwarefouten. Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.		
	A.14.2.6	Beveiligde ontwikkelomgeving	Organisaties moeten beveiligde ontwikkelomgevingen vaststellen en passend beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.	**3 = Aantoonbaar en geimplementeerd**	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	Risico 11	
	A.14.2.7	Uitbestede softwareontwikkeling	Uitbestede systeemontwikkeling moet onder supervisie staan van en worden gemonitord door de organisatie.	**3 = Aantoonbaar en geimplementeerd**	SpotOnMedics besteed vanaf eind 2020/2021 softwareontwikkeing uit.	Niet van toepassing (in toekomst wellicht freelancers)	
	A.14.2.8	Testen van systeembeveiliging	Tijdens ontwikkelactiviteiten moet de beveiligingsfunctionaliteit worden getest.	**3 = Aantoonbaar en geimplementeerd**	Uitval van systemen door softwarefouten. Uitval van systemen door configuratiefouten.	Risico 11 - Ontwikkelaar test eigen werk - Als getest dan naar testomgeving - Iemand buiten team test opgeleverde stuk - Als er tekortkomingen zijn, dan terug naar ontwikkelaar - Nu mondelinge communicatie tussen ontwikkeling en testen - Als test akkoord dan naar acceptatie - Acceptatietest door .... en eventueel met klant - In het verleden op live getest; nu is er een testomgeving - Nu uitgangspunt: wat ontwikkeld / aangepast is wordt getest - toekomst: het systeem of belangrijke delen ervan worden (opnieuw) getest - Testcases worden nog niet gemaakt. - Evaluatie van release nog niet geformaliseerd -> inplannen retrospective.	
	A.14.2.9	Systeemacceptatietests	Voor nieuwe informatiesystemen, upgrades en nieuwe versies moeten programma's voor het uitvoeren van acceptatietests en gerelateerde criteria worden vastgesteld.	**3 = Aantoonbaar en geimplementeerd**	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling. Uitval van systemen door softwarefouten. Uitval van systemen door configuratiefouten	Risico 11 Zie 14.2.8	
	A.14.3	Testgegevens	*Bescherming waarborgen van gegevens die voor het testen zijn gebruikt.*			\	

Onderwerp			Beheersmaatregel	Status beheersmaatregel 1)	Onderbouwing selectie/uitsluiting - generiek risico	Risico nummers, opmerkingen, eigenaar beheersmaatregel	Controlemaatregel
	A.14.3.1	Bescherming van testgegevens	Testgegevens moeten zorgvuldig worden gekozen, beschermd en gecontroleerd.	**3 = Aantoonbaar en geimplementeerd**	Tegen het bedrijf worden juridische stappen genomen vanwege het niet veilig omgaan met vertrouwelijke informatie.	Risico 5 en 25 Voor bijvoorbeeld privacy gevoelige informatie, een control die al snel volgens de WBP noodzakelijk is Opnemen in SO beleid (demo gegevens niet uitgebreid genoeg)	
A.15 Leveranciersrelaties	A.15.1	Informatiebeveiliging in leveranciersrelaties	*De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers.*				
	A.15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties	Met de leverancier moeten de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, worden overeengekomen en gedocumenteerd.	**3 = Aantoonbaar en geimplementeerd**	Inbreuk op vertrouwelijkheid van informatie door het toelaten van externen in het pand of op het netwerk Toegang tot informatie door onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.	Risico 22, 25, en 33 Bij een dispuut zal een rechter wegen of er regels gesteld waren	
	A.15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	Alle relevante informatiebeveiligingseisen moeten 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.	**3 = Aantoonbaar en geimplementeerd**	Inbreuk op vertrouwelijkheid van informatie door het toelaten van externen in het pand of op het netwerk Toegang tot informatie door onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.	Bij een dispuut zal een rechter wegen of er regels gesteld waren	
	A.15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	Overeenkomsten met leveranciers moeten eisen 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.	**3 = Aantoonbaar en geimplementeerd**	Inbreuk op vertrouwelijkheid door wetgeving ten aanzien van informatie in de cloud.Toegang tot informatie door onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.		

Onderwerp			Beheersmaatregel	Status beheersmaatregel 1)	Onderbouwing selectie/uitsluiting - generiek risico	Risico nummers, opmerkingen, eigenaar beheersmaatregel	Controlemaatregel
	A.15.2	Beheer van dienstverlening van leveranciers	*Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven.*				
	A.15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	Organisaties moeten regelmatig de dienstverlening van leveranciers monitoren, beoordelen en auditen.	**3 = Aantoonbaar en geimplementeerd**	Toegang tot informatie door misbruik van kwetsbaarheden in applicaties.Toegang tot informatie door misbruiken van zwakheden in netwerkbeveiliging.	Risico 25 en 36	
	A.15.2.2	Beheer van veranderingen in dienstverlening van leveranciers	Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, moeten worden beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.	**3 = Aantoonbaar en geimplementeerd**	Niet beschikbaar zijn van informatie of diensten vanuit derden.Inbreuk op vertrouwelijkheid van informatie door het toelaten van externen in het pand of op het netwerk.	Risico 36	
ebeveiligingsincidenten	A.16.1	Beheer van informatiebeveiligingsincidenten en -verbeteringen	*Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.*				

Onderwerp			Beheersmaatregel	Status beheersmaatregel 1)	Onderbouwing selectie/uitsluiting - generiek risico	Risico nummers, opmerkingen, eigenaar beheersmaatregel	Controlemaatregel
A.16 Beheer van informati	A.16.1.1	Verantwoordelijkheden en procedures	Directieverantwoordelijkheden en -procedures moeten worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.	**3 = Aantoonbaar en geimplementeerd**	Beveiligingsinbreuken als gevolg van het ontbreken of niet oppakken van verantwoordelijkheden door leidinggevenden.	Risico 42, 43 en 61 Support proces beschreven in Customer Journey. Incidenten / support vragen komen via verschillende kanalen binnen (support, accountmanager, financieel). Indien een incident / vraag niet bij support binnenkomt, dan klant vragen of melding via support al heeft plaatsgevonden. Zo niet, klant verzoeken dit alsnog te doen of melding namens klant vastleggen in FysioOne. Support hangt categorie aan de melding en zet deze door naar verantwoordelijke persoon / afdeling. Besloten om vastlegging Informatiebeveiligingsgebeurtenis- en incidenten in FysioOne te doen. Detaillering m.b.v. sjabloon Informatiebeveiligingsincident in Google Drive. Later besluiten of uitbreiding / vervanging van supportsysteem nodig is.	
	A.16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	Informatiebeveiligingsgebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd.	**3 = Aantoonbaar en geimplementeerd**	De gevolgen van incidenten worden onnodig groot, doordat deze niet tijdig gezien / opgepakt worden.	Risico 42 en 61 Service levels vastgelegd in SLA document Google Drive (review). Rapportagemogelijkheden FysioOne m.b.t. geregistreerde en afgehandelde tickets eventueel per medewerker zijn beperkt. - Niet zichtbaar dat klant al eerder gebeld heeft. Formulier Infromatiebeveiligingsincident beschikbaar voor gedetailleerde beschrijving en analyse van IB incidenten. IB incidenten die niet door klanten worden gemeld, dienen bij de leidinggevende te worden gemeld, die het formulier Informatiebeveiligingsincident invult en naar de Security Officer stuurt. De security officer werkt het overzicht Informatibeveiligingsincidenten bij en slaat het formulier op in de Google drive (ISMS)	

Onderwerp			Beheersmaatregel	Status beheersmaatregel 1)	Onderbouwing selectie/uitsluiting - generiek risico	Risico nummers, opmerkingen, eigenaar beheersmaatregel	Controlemaatregel
	A.16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging	Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie moet worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.	**3 = Aantoonbaar en geimplementeerd**	De gevolgen van incidenten worden onnodig groot, doordat deze niet tijdig gezien / opgepakt worden.	Risico 42 en 61 Besloten om	
	A.16.1.4	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	Informatiebeveiligingsgebeurtenissen moeten worden beoordeeld en er moet worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.	**3 = Aantoonbaar en geimplementeerd**	Incidenten kunnen niet (snel genoeg) opgelost worden omdat de nodige informatie en actieplannen ontbreken.	Risico 61 Deels geregeld in procedure datalekken	
	A.16.1.5	Respons op informatiebeveiligingsincidenten	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	**3 = Aantoonbaar en geimplementeerd**	Incidenten kunnen niet (snel genoeg) opgelost worden omdat de nodige informatie en actieplannen ontbreken.	Risico 61	
	A.16.1.6	Lering uit informatiebeveiligingsincidenten	Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen moet worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.	**3 = Aantoonbaar en geimplementeerd**	Herhaling van incidenten	Risico 61 Lering van incidenten vindt wel plaats, maar niet op een gestructureerde / aantoonbare manier.	
	A.16.1.7	Verzamelen van bewijsmateriaal	De organisatie moet procedures definiëren en toepassen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	**3 = Aantoonbaar en geimplementeerd**	Tijdens een rechtszaak is het bedrijf niet in staat om de benodigde bewijzen te kunnen leveren.Het niet hard kunnen maken van welke persoon over welk account beschikt.	Risico 61 Bij een dispuut zal een rechter wegen of bewijs juridisch bruikbaar is	
uiteitsbeheer	A.17.1	Informatiebeveiligingscontinuïteit	*Informatiebeveiligingscontinuïteit moet worden ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie.*				

Onderwerp			Beheersmaatregel	Status beheersmaatregel 1)	Onderbouwing selectie/uitsluiting - generiek risico	Risico nummers, opmerkingen, eigenaar beheersmaatregel	Controlemaatregel
A.17 Informatiebeveiligingsaspecten van bedrijfscontin	A.17.1.1	Informatiebeveiligingscontinuïteit plannen	De organisatie moet haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, vaststellen.	**3 = Aantoonbaar en geimplementeerd**	Beveiligingsinbreuken als gevolg van ontbreken van coördinatie vanuit de directie. Incidenten kunnen niet (snel genoeg) opgelost worden omdat de nodige informatie en actieplannen ontbreken.Brand, Overstroming, Explosie, Rampen	Risico 22, 24 en 33 Indien een organisatie contracten afsluit met garanties over B, I en V dan wellicht relevant	
	A.17.1.2	Informatiebeveiligingscontinuïteit implementeren	De organisatie moet processen, procedures en beheersmaatregelen vaststellen, documenteren, implementeren en handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.	**3 = Aantoonbaar en geimplementeerd**	ncidenten kunnen niet (snel genoeg) opgelost worden omdat de nodige informatie en actieplannen ontbreken.Brand, Overstroming, Explosie, Rampen	Risico 22, 24 en 33	
	A.17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	De organisatie moet de ten behoeve van informatiebeveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.	**3 = Aantoonbaar en geimplementeerd**	Brand, Overstroming, Explosie, Rampen	Risico 22, 24 en 33 Testen wordt opgenomen in disaster recovery plan. Security Officer zal periodiek een aantal aspecten van het plan testen.	
	A.17.2	Redundante componenten	*Beschikbaarheid van informatieverwerkende faciliteiten bewerkstelligen.*			It gaat het arrchitectuurdocument uitbreiden met een onderdeel redundantie en / of dit actualiseren op basis van recente ervaringen.	
	A.17.2.1	Beschikbaarheid van informatieverwerkende faciliteiten	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	**3 = Aantoonbaar en geimplementeerd**	Overbelasten van netwerkdienstenNiet beschikbaar zijn van informatie of diensten vanuit derden	Risico 22, 24 25 en 33 Indien een organisatie contracten afsluit met garanties over beschikbaarheid dan wellicht relevant. 99,9% beschikbaarheid in SLA. Virtualisatie en redundantie toegepast in productie-omgeving. Er is geen uitwijklocatie beschikbaar.	
A.18 Naleving	A.18.1	Naleving van wettelijke en contractuele eisen	*Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingseisen.*				

Onderwerp			Beheersmaatregel	Status beheersmaatregel 1)	Onderbouwing selectie/uitsluiting - generiek risico	Risico nummers, opmerkingen, eigenaar beheersmaatregel	Controlemaatregel
	A.18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen	Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen moeten voor elk informatiesysteem en de organisatie expliciet worden vastgesteld, gedocumenteerd en actueel gehouden.	**3 = Aantoonbaar en geimplementeerd**	Tegen het bedrijf worden juridische stappen genomen vanwege het niet veilig omgaan met vertrouwelijke informatie.Inbreuk op vertrouwelijkheid door wetgeving ten aanzien van het bezoeken van dat land	Risico 36, 44 en 45 Iedere ondernemer wordt geacht de wet te respecteren	
	A.18.1.2	Intellectuele eigendomsrechten	Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectuele- eigendomsrechten en het gebruik van eigendomssoftwareproducten te waarborgen moeten passende procedures worden geïmplementeerd.	**3 = Aantoonbaar en geimplementeerd**	Tegen het bedrijf worden juridisch stappen genomen vanwege schenden van auteursrechten / IPR.	Licenties toevoegen aan overzicht van bedrijfsmiddelen. Overzicht IT middelen beschikbaar van verhuizing. Dient nog bijgewerkt te worden. Keuze opnemen in lijst bedrijfsmiddelen? (serienummers e.d., aanschafdatum, leverancier). Beperkt aantal compenenten in hoofdkantoor. Broncode op alle productie servers, 1 centrale server met alle code in datacenter (test, acceptatie, live). Backup van centrale server gebruikt in geval van calamiteiten. TFS is onderhande werk (ook oudere versies).	
	A.18.1.3	Beschermen van registraties	Registraties moeten in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	**3 = Aantoonbaar en geimplementeerd**	Tegen het bedrijf worden juridische stappen genomen vanwege het niet veilig omgaan met vertrouwelijke informatie.	Risico 3, 7, 38 en 44 Archiefwet voor overheden, wet op de rijksbelastingen voor overige bedrijven Broncode wijziging wordt gelogd in TFS. Toegang tot database direct wordt niet gelogd. (Wilco bespreekt met team hoe dit te organiseren). IT'ers doen niets meer dan support. Besluit: we moeten meer gaan loggen (nu reactief op basis van opmerkingen / klachten van klanten). Opnemen in toegangsbeleid (rollen en rechten + logging). Voorbeeld: BSN en Bankrekeningnummer is voor weinig functies benodigd. Releasekalender opnemen: bepaalde rubrieken achter knop. Drukken op knop is bewuste actie en kan eventueel worden gelogd.	

Onderwerp			Beheersmaatregel	Status beheersmaatregel 1)	Onderbouwing selectie/uitsluiting - generiek risico	Risico nummers, opmerkingen, eigenaar beheersmaatregel	Controlemaatregel
	A.18.1.4	Privacy en bescherming van persoonsgegevens	Privacy en bescherming van persoonsgegevens moeten, voor zover van toepassing, worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	**3 = Aantoonbaar en geimplementeerd**	Tegen het bedrijf worden juridische stappen genomen vanwege het niet veilig omgaan met vertrouwelijke informatie.Inbreuk op vertrouwelijkheid door wetgeving ten aanzien van informatie in de cloud.	Risico 21, 25, 38 en 44 Wet Bescherming Persoonsgegevens	
	A.18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	Cryptografische beheersmaatregelen moeten worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.	**3 = Aantoonbaar en geimplementeerd**		In sommige jurisdicties is niet alle invoer/uitvoer van cryptografie toegestaan	
	A.18.2	Informatiebeveiligingsbeoordelinge n	*Verzekeren dat informatiebeveiliging wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van de organisatie.*				
	A.18.2.1	Onafhankelijke beoordeling van informatiebeveiliging	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), moeten onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen worden beoordeeld.	**3 = Aantoonbaar en geimplementeerd**	Systemen worden niet gebruikt waarvoor ze bedoeld zijn. Beveiligingsinbreuke n als gevolg van het ontbreken of niet oppakken van verantwoordelijkhede n door leidinggevenden.	Risico 45 Dagelijkse test dooor McAffee.	
	A.18.2.2	Naleving van beveiligingsbeleid en -normen	Het management moet regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	**3 = Aantoonbaar en geimplementeerd**	Systemen worden niet gebruikt waarvoor ze bedoeld zijn. Beveiligingsinbreuke n als gevolg van het ontbreken of niet oppakken van verantwoordelijkhede n door leidinggevenden.	Risico 45 Iedere ondernemer wordt geacht de wet te respecteren	

SpotOnMedics VVT v4.0 d.d. 12-05-2021

Onderwerp			Beheersmaatregel	Status beheersmaatregel 1)	Onderbouwing selectie/uitsluiting - generiek risico	Risico nummers, opmerkingen, eigenaar beheersmaatregel	Controlemaatregel
	A.18.2.3	Beoordeling van technische naleving	Informatiesystemen moeten regelmatig worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	**3 = Aantoonbaar en geimplementeerd**	Systemen raken besmet met malware. Toegang tot informatie door misbruik van kwetsbaarheden in applicaties.	Risico 27 Relevant voor veiligheid zoals vastgelegd in NEN1010 Ook rol voor datacenter. SOM probeert met McAfee in te breken op software. Inbreken op server / netwerk / poorten ook met McAfee. Nog in gesprek met Datacenter over taakverdeling / verantwoordelijkheden. Voorbeelden: ddos, patchen servers, poorten firewalls (opdracht vanuit som m.b.t. poorten), bandbreedte / quality of service. Zie contract met KPN + adendum (Marien)	