Auditrapport

EN-ISO27001; 2013.
NEN 7510
Managementsysteem voor informatiebeveiliging

Share-board BV

10 augustus en 13 oktober

Kiwa Nederland B.V.
Kiwa NCP
Nevelgaarde 50
Postbus 510
3430 AM Nieuwegein

Tel. +31 88 998 3072
Fax +31 88 998 3059
Info.ncp@kiwa.nl
www.kiwa.nl
www.kiwafss.nl

Organisatie

Naam	:	Share-board BV
Contactpersoon	:	Dhr. Wim van Asperen
E-mail	:	Wim@share-board.nl
Relatienummer	:	
Vestigingsadres	:	Bosmanskamp 1B, 4191 MS Geldermalsen
Postadres	:	Idem
Telefoon	:	06 218 545 36

Aantal vestigingen	:	04	Medewerkers	:	3

Onderzoek

Soort onderzoek	:	initiële audit
Onderdeel	:	Implementatie
Datum onderzoek	:	10 augustus en 13 oktober
Datum rapport, versie	:	2017, versie 01

Auditteam

Auditor(en)	:	Berrie Steer;
Vakdeskundige(n)	:	

Certificatie-eisen

Reglement(en)	:	Kiwa-Reglement voor systeemcertificatie: 2014

SCOPE:

NEN 7510; 2011
Het ISMS van Share-board betreft de informatiebeveiliging en de privacybescherming van patiëntengegevens en/of bedrijfsgevoelige informatie alsmede de persoonsgegevens van de Gebruikers zelf, die door Gebruikers aan Share-board worden toevertrouwd om onderling makkelijk en vertrouwelijk te kunnen samenwerken.

ISO/IEC 27001; 2013
Het ISMS van Share-board betreft de informatiebeveiliging en de privacybescherming van bedrijfsgevoelige informatie en/of bijzondere persoonsgegevens alsmede de persoonsgegevens van de Gebruikers zelf, die door Gebruikers aan Share-board worden toevertrouwd om onderling makkelijk en vertrouwelijk te kunnen samenwerken.

Norm/regeling:	Toepassingsgebied(en):	Certificaatnr.
ISO/IEC 27001; 2013	34B – 38	
NEN 7510; 2011	38	

Samenvatting			**C/ NC**
Auditteam	:	De aard van het bedrijf geeft geen aanleiding om het auditteam te wijzigen	C
Normuitsluitingen	:	Normuitsluitingen zijn voldoende onderbouwd.	C
Auditplan	:	Het auditplan is ter afstemming per e-mail naar de klant verzonden en door de klant akkoord bevonden. Het auditplan in dit rapport is aangepast aan de daadwerkelijk uitgevoerde audit	C
Handboek, procedures	:	De systeemdocumentatie is vastgelegd in het handboek versie 2017. Indien van toepassing: handboek is aangepast naar de nieuwe norm.	C
Acties uit vorige audit	:	Corrigerende maatregelen n.a.v. de vorige audit zijn effectief doorgevoerd.	C
Multi Site Toetsing	:	Organisatie voldoet aan Multi Site voorwaarden De klant is er (in verband met het multi-site principe) op gewezen dat op een vestiging geconstateerde tekortkomingen consequenties hebben voor het gehele certificaat, incl. alle vestigingen. Bij de oplossing van geconstateerde tekortkomingen dienen alle relevante vestigingen in ogenschouw genomen te worden.	C
Certificatieovereenkomst	:	De huidige certificatieovereenkomst is actueel voor wat betreft de uitgangspunten. (data, logogebruik, reikwijdte/scope, aantal medewerkers, Fte totaal en per kritisch proces, vermelding vestigingen zijn gecontroleerd) De auditresultaten (van de afgelopen 3 jaar) geven (bij herevaluatie) geen aanleiding tot aanpassing van de uitgangspunten.	C
Uitvoering Fase 1 bij Herevaluatie	:	De resultaten uit de voorgaande audits, de beperkte wijzigingen in de organisatie, het managementsysteem en de van toepassing zijnde regelgeving geven geen aanleiding tot het (bij de herevaluatie) opnieuw uitvoeren van een Fase 1 onderzoek.	C
Beoordeling fase 1	:	Op grond van bovenstaande heeft er geen/een beperkt/ een compleet vooronderzoek (fase 1) bij het bedrijf plaatsgevonden (zie auditplanning). De resultaten zijn verwerkt in de auditmatrix. Na afloop van het vooronderzoek (fase1) zijn er aandachtsgebieden aan het bedrijf gerapporteerd waarbij is aangegeven dat deze gedurende fase 2 tot tekortkomingen kunnen leiden. Fase 1 is op de volgende facetten positief beoordeeld: - Bepaling audit doelstelling - Reikwijdte in relatie tot wet- en regelgeving - Reikwijdte in relatie tot kwalificatie auditteam - Verificatie bij personeel fase 2 audit - Prestaties ISMS - Het hebben van een directiebeoordeling en Interne audits conform de eisen uit het certificatie schema - Het beschreven hebben van de 6 verplichte procedures - Toewijzing middelen fase 2 - Verificatie gegevens klant in relatie tot calculatie gegevens - Toepassingsgebied in relatie tot norm	C
Effectiviteit systeem	:	Het systeem functioneert effectief (beleid, doelstellingen, review en acties).	C
Logo´s / pictogrammen	:	Het gebruik van logo's, pictogrammen, certificaat conform het reglement.	C
Klachten	:	De klachtenprocedure functioneert effectief.	C
Interne audits	:	De interne audits dragen effectief bij aan het systeem.	C

Adviseur	:	Het bedrijf wordt t.a.v. het beheer / onderhoud van hun zorgsysteem extern geadviseerd door: n.v.t.	NVT

Eventuele bijzonderheden:
Van toepassing zijnde wetten, normen, regelingen en voorschriften zijn in de regeling vervat en maken deel uit van de audit.

Bevindingen

C - Conform	:	Voldoet aan de normeis. Eventueel kunnen er verbeteraspecten ter informatie worden gerapporteerd. Deze aspecten verdienen nadere aandacht of kunnen in het systeem nog verder doorontwikkeld worden.
T - Tekortkoming	:	Na afloop van de audit is er geen tekortkoming geconstateerd. (en als zodanig geaccepteerd). Het managementsysteem voldoet op aspecten niet aan de certificatie-eis. Er is objectief bewijs van een situatie, waarbij op termijn moet worden getwijfeld of het zorgsysteem van de organisatie de beoogde output levert. Dit is belemmerend voor toekenning of behoud van het certificaat. De geplande corrigerende maatregelen moeten beoordeeld zijn alvorens het auditteam een certificatieadvies kan uitbrengen
KT - Kritische tekortkoming	:	Na afloop van de audit zijn 0 kritische tekortkomingen geconstateerd (en als zodanig geaccepteerd). Het managementsysteem voldoet niet aan de certificatie-eis. Er is objectief bewijs van een situatie, dat het zorgsysteem van de organisatie niet voldoet aan de norm en/of niet de beoogde output levert. Dit is belemmerend voor toekenning of behoud van het certificaat. Voor de afhandeling van de kritische tekortkoming is doorgaans een extra audit noodzakelijk alvorens het auditteam een certificatieadvies kan uitbrengen.

Vervolgafspraken
Het bedrijf presenteert corrigerende maatregelen aan Kiwa vóór n.v.t.
Kiwa beoordeelt de maatregelen n.a.v. kritische tekortkoming(en) tijdens een extra audit op n.v.t.
Kiwa beoordeelt de maatregelen n.a.v. tekortkoming tijdens de volgende audit op n.v.t.

Beoordeling corrigerende maatregelen

Beoordelingsresultaat N.a.v. Fase 1/ Fase 2 en/of Opvolgaudits	:	Overgang vooronderzoek (fase 1) naar implementatieonderzoek (fase 2): In overleg met de klant is na afloop van het vooronderzoek (fase 1) overgegaan naar het implementatieonderzoek (fase 2).

Eventuele toelichting:
…..

Certificatieadvies
Bij Fase 1: n.v.t.

Bij Fase 2 en /of opvolgingsbezoeken:
Het auditteam adviseert Kiwa tot uitgifte van het certificaat.
Zonder tegenbericht binnen 4 weken, is dit certificatieadvies ongewijzigd overgenomen als certificatiebeslissing.

Eventuele toelichting:

Leadauditor Kiwa	**Review en certificatiebeslissing Kiwa**
Naam : Berrie Steer Datum : november 2017 Handtekening: 	Akkoord met certificatieadvies: Naam : A.M. Nederlof Datum : 11-12-2017 Handtekening: 

Leeswijzer rapportage:

Dit rapport heeft de volgende bijlagen:
- Auditmatrix IEC 27001 en aanvulling NEN 7510
- Rapportbladen
- Auditplan
- Indien van Toepassing: Plan(-nen) van Aanpak

Indrukken en bevindingen

1.1. Algemene Indruk

Auditplan
Er zijn in de organisatie geen wijzigingen die invloed hebben op auditdoelstelling, auditprogramma, audittijdbesteding of toepassingsgebied. Dit is in het openingsgesprek geverifieerd.

Past performance
Het ISMS is goed van opzet en werkt voor de organisatie. Het systeem dient nog verder doorontwikkeld te werken. De meeste aandachtspunten uit Fase 1 zijn goed opgepakt. De PDCA cyclus dient nog verder rond gemaakt te worden. Met name de onderdelen van check en act van de cyclus kan beter.

Ontwikkelingen/sterke punten:
- Leercurve van de organisatie
- Bewustzijn en betrokkenheid van de medewerkers
- Medewerkers zijn zich bewust van het belang van een goed werkend ISMS.
- Klanten waarderen de voorstrekkersrol van Share-board IT Groep BV m.b.t. informatiebeveiliging.

MATRIX EN/ISO27001; 2013

Evaluation aspects	**Findings** *C=Conform, NC=Non Conformity, MC=Major Non Conformity*	**C/NC/MC**
4 Context of the organization		
4.1 Understanding the organization and its context Determine external and internal issues	Share-board IT Groep BV is actief binnen diverse werkvelden. Vandaar de vraag voor certificatie IEC 27001 / NEN 7510. Men heeft contact met alle partijen in het speelveld. Partijen in werkveld vragen ook om conformiteit op basis van NEN 7510 i.c.m. IEC 27001. Documenten aantoonbaar: KMS	C
4.2 Understanding needs & expectations of interested parties a. Parties b. Requirements	Tijdens de audit is gebleken dat de organisatie zich sterk bewust is van de aandachtpunten in het werkveld en van het ISMS. Als basis van de beoordeling is IEC 27001 en de bijlage gebruikt met aanvullende punten vanuit de NEN 7510. Documenten aantoonbaar: KMS	C
4.3 Determining the scope of the ISMS a. External & internal issues b. Requirements c. Interfaces & dependencies	overkoepelend ISMS, waarbij per deel activiteit aanvullende processen beschreven zijn die weer inhaken op het overkoepelden management systeem tbv ISO 27001 en NEN 7510 Documenten aantoonbaar: KMS	C
4.4 ISMS Establish, implement, maintain and continually improve	Door het team is vastgesteld dat de organisatie de PDCA cyclus begrijpt en gedeeltelijk toepast. Het ISMS dient nog verder doorontwikkeld te worden op effectmetingen van een aantal onderwerpen van het ISMS Op een aantal onderwerpen is men wel cyclus bezig met name met het uitvoeren van risicoprofielen en verbetermaatregelen. Documenten aantoonbaar: KMS	C

Evaluation aspects	Findings *C=Conform, NC=Non Conformity, MC=Major Non Conformity*	C/NC/MC
5 Leadership		
5.1 Leadership and commitment a. policy & objectives b. integration into process c. resources needed available d. communicating the importance e. achieves its intended outcome f. directing and supporting persons to contribute g. promoting continual improvement h. supporting other relevant management roles	De organisatie laat zien dat het wil heeft om te voldoen aan de normen van ISO27001 en NEN7510. Het leiderschap wat hierbij past wordt ook door de organisatie uitgedragen. Doelen zijn gesteld en worden ingevuld, de middelen die nodig zijn worden ter beschikking gesteld. Documenten aantoonbaar: KMS	C
5.2 Policy a. appropriate to the purpose of the organization b. information security objectives c. commitment to satisfy applicable requirements d. commitment to continual improvement e. available as documented information f. be communicated within the organization g. be available to interested parties, as appropriate	Het beleid is gericht op het invullen van de NEN 7510 en ISO27001. Hier wordt met de belanghebbend binnen en buiten de organisatie goed over gecommuniceerd. Men wil men zich hier ook graag in verbeteren en onderscheiden binnen de mogelijkheden die het markt sentiment om dit moment mogelijk maakt. Documenten aantoonbaar: KMS	C
5.3 Organizational roles, responsibilities and authorities Responsibilities and authorities for roles relevant to IS are assigned and communicated a. ensuring that the ISMS conforms to the requirements b. reporting performance to the Top Management	De functies zijn opgenomen in het ISMS en zijn bekend binnen de organisatie. Documenten aantoonbaar: KMS	C
6 Planning		
6.1.1 Actions to address risks and opportunities a. ensure intended outcome b. prevent, or reduce, undesired effects c. achieve continual improvement d. actions to address these risks and opportunities e. integrate & implement actions & evaluate effectiveness	Door het team is vastgesteld dat de organisatie de PDCA cyclus begrijpt en gedeeltelijk toepast. Het ISMS dient nog verder doorontwikkeld te worden op effectmetingen van een aantal onderwerpen van het ISMS Documenten aantoonbaar: JKMS	C
6.1.2 Information security risk assessment a. establishes & maintains risk acceptance criteria & criteria for performing ISRA b. ensures that repeated ISRA produce consistent, valid and comparable results c. identifies the ISR 1. loss confidentiality, integrity & availability for information 2. identify the risk owners d. analyses the information security risks 1. consequences 2. assess the realistic likelihood of the occurrence 3. determine the levels of risk e. evaluates ISR 1. compare 2. prioritize retain documented information about ISRA process.	Binnen het ISMS van de organisatie wordt gewerkt met een standaard model voor RA. Hierin is een soort vlinderdas methodiek opgenomen waarin naar het verlies, en Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) van informatie en communicatie wordt gekeken. Indien in de beoordeling blijkt dat het een kritische beveiligingsklasse betreft wordt er een aanvullende beoordeling alleen voor dit onderdeel gedaan. Hierin de persoon en de termijn genoemd met een bewaking op uitvoering. Er liggen criteria in het systeem om te komen tot weging van de beoordeelde punten, waarin de consequenties, de waarschijnlijkheid en het rest risico worden vastgesteld. Het prioriteren van de acties gebeurt in overleg binnen de directie. Binnen de high level structuur van het ISMS zijn alle risico beoordeling en de aanpak gelijk, daar waar de specifieke processen hebben zijn deze apart beoordeeld en gewogen. Documenten aantoonbaar: KMS	C
6.1.3 Information security risk treatment a. select appropriate ISRT options, taking account of the risk assessment results b. determine all controls that are necessary to implement the ISRT option(s) chosen	De BIV classificatie wordt minimaal 1 x per jaar geëvalueerd en op basis hiervan ook de weging. Er is een referentie tabel NEN7510 waarin de afleidingen voor de controls die in bijlage A van de IEC 27001 zijn benoemd. De controls geven invulling aan de verklaring van toepasselijkheid voor NEN 7510 en IEC	C

Evaluation aspects	Findings *C=Conform, NC=Non Conformity, MC=Major Non Conformity*	C/NC/MC
c. compare the controls determined in b with those in annex A and verify that no necessary controls have been omitted d. produce a Statement of Applicability that contains the necessary controls and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from annex A e. formulate an ISRT plan f. obtain risk owners' approval of the ISRT plan and acceptance of the residual information security risks	27001. De controls zijn te vinden in KMS Documenten aantoonbaar: KMS	
6.2 Information security objectives & planning to achieve them a. be consistent with the information security policy b. be measurable (if practicable) c. take into account applicable ISR, and results from risk assessment and risk treatment d. be communicated e. be updated as appropriate The organization shall retain documented information on the information security objectives. When planning how to achieve its information security objectives, the organization shall determine f. what will be done g. what resources will be required h. who will be responsible i. when it will be completed j. how the results will be evaluated	Er worden planningsactiviteiten ontwikkeld op basis van de gevonden maatregelen ter bestrijding van de gevonden risico's. deze opzet dekt de eisen van deze normparagraaf af. In de planning en evaluatie worden beoordeeld in hoeverre de bedreigingen en kwetsbaarheden in controls zijn. Documenten aantoonbaar: KMS	C
7 Support		
7.1 Resources Determine and provide the resources	De organisatie bepaald via de PDCA cyclus de behoefte aan middelen. Documenten aantoonbaar: KMS	C
7.2 Competence a. determine the necessary competence of person(s) doing work under its control that affects the IS performance; b. ensure that these persons are competent on the basis of appropriate education, training, or experience c. where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken d. retain appropriate documented information as evidence of competence	De competenties zijn bepaald en de medewerkers worden hierop getraind. Het gaat hierbij om een basis training beveiliging informatietechnologie voor al het personeel. Documenten aantoonbaar: KMS	C
7.3 Awareness a. the information security policy; b. their contribution to the effectiveness of the ISMS, including the benefits of improved information security performance c. the implications of not conforming with the ISMS requirements	Tijdens de interviews is vastgesteld dat het beleid bekend is en bijdraagt tot de beveiliging van de informatietechnologie en wat de voordelen van zijn naast het belang. Documenten aantoonbaar: KMS	C
7.4 Communication a. on what to communicate b. when to communicate c. with whom to communicate d. who shall communicate e. the processes by which communication shall be effected	De directie en security officer communiceren goed aangaande het belang van de beveiliging van de informatietechnologie. De organisatie heeft genoeg momenten om over het onderwerp beveiliging informatietechnologie te communiceren is vastgesteld tijdens de interviews. Er is een kwaliteitsoverleg om het ISMS verder te ontwikkelen en te beheren. Medewerkers ontvangen een mail als documenten zijn gewijzigd in het KMS Afspraken en acties worden vastgelegd en gecommuniceerd met de medewerkers.	C

Evaluation aspects	Findings *C=Conform, NC=Non Conformity, MC=Major Non Conformity*	C/NC/MC
	Documenten aantoonbaar: KMS	
7.5.1 Documented information a. documented information required by this Standard b. documented information determined by the organization as being necessary for the effectiveness of the ISMS	Er is een procedure die bekend is en wordt gehanteerd. Er is een referentie tabel NEN7510, alle onderdelen van de tabel NEN7510 dekken de onderdelen in IEC 27001 af. Documenten aantoonbaar: KMS	C
7.5.2 Creating and updating a. identification and description (e.g. a title, date, author, or reference number) b. format (e.g. language, software version, graphics) and media (e.g. paper, electronic) c. review & approval for suitability and adequacy	Er is een procedure die bekend is en wordt gehanteerd. Deze wordt ook voor software en data gebruikt. Documenten aantoonbaar: KMS	C
7.5.3 Control of documented information Shall be controlled to ensure: a. it is available and suitable for use, where and when it is needed b. it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity) c. distribution, access, retrieval & use d. storage & preservation, including the preservation of legibility e. control of changes (e.g. version control) f. retention and disposition	Er is een procedure die bekend is en wordt gehanteerd. Deze wordt ook voor software en data gebruikt. Hierin is tevens de toegang en de opslag meegenomen. Documenten aantoonbaar: KMS	C
8 Operation		
8.1 Operational planning and control - plan, implement & control - shall keep documented information - shall control planned changes & review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary - shall ensure that outsourced processes are determined & controlled	Share-board is nu bezig met het door ontwikkelen van het ISMS. Hierin is een duidelijk lijn te zien van plannen, artikelen en reviews. Documenten aantoonbaar: KMS	C
8.2 Information security risk assessment -shall perform ISRA at planned intervals or when significant changes are proposed or occur -shall retain documented information of the results of the ISRA	Binnen alle processen is geïdentificeerd wat het risico is op basis van het RA-model. Er wordt minimaal jaarlijks een nieuwe evaluatie gedaan en eerder indien nodig blijkt. Documenten aantoonbaar: KMS	
8.3 Information security risk treatment -shall implement the ISRT plan -shall retain documented information of results of the ISRT	Het ISRT plan t leidt tot verdere doorontwikkeling van het ISMS. Men gaat verder met de doorontwikkeling van dit ISMS. Documenten aantoonbaar: KMS	C
9.1 Monitoring, measurement, analysis and evaluation a. what needs to be monitored & measured, including information security processes & controls b. the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results c. when the monitoring and measuring shall be performed; d. who shall monitor and measure e. when the results from monitoring and measurement	Er zijn meerdere processen om beheersing te houden aangaande het ISMS. Deze zijn verder uitgewerkt in de bijlage A van dit rapport.	C

Evaluation aspects	Findings *C=Conform, NC=Non Conformity, MC=Major Non Conformity*	C/NC/MC
shall be analysed and evaluated f. who shall analyse and evaluate these results	Documenten aantoonbaar:KMS	
9.2 Internal audit a1. own requirements a2. requirements of this Standard b. effectively implemented and maintained c. PEIM an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits; d. define the audit criteria and scope for each audit; e. select auditors and conduct audits that ensure objectivity and the impartiality of the audit process; f. ensure that the results of the audits are reported to relevant management; and g. retain documented information as evidence of the audit programme(s) and the audit results 9.3 Management review a. the status of actions from previous management reviews b. changes in external and internal issues that are relevant to the ISMS c. feedback on the information security performance, including trends in 1) nonconformities and corrective actions 2) monitoring and measurement results 3) audit results 4) fulfilment of information security objectives d. feedback from interested parties; e. results of RA & status of RTP f. opportunities for continual improvement.	Interne audit wordt uitgevoerd binnen alle organisatie-onderdelen. Alle verbeteracties zijn gelabeld (actie, verantwoordelijk, realisatiedatum, status en opmerking) en inzichtelijk in het KMS. De directiebeoordeling van de afgelopen jaar ingezien en doorgenomen. In de directiebeoordeling zijn effectmetingen nog onderbelicht. Documenten aantoonbaar: KMS	C
10 Improvement		
10.1 Nonconformity and corrective action a. react to the nonconformity, b. evaluate the need for action to eliminate the causes of nonconformity c. implement any action needed d. review the effectiveness of any corrective action taken e. make changes to the ISMS Corrective actions shall be appropriate to the effects of the nonconformities encountered. The organization shall retain documented information as evidence of f. the nature of the nonconformities and any subsequent actions taken, and g. the results of any corrective action.	Gebaseerd op de interne evaluaties door de organisatie zelf en de externe evaluatie door Kiwa zelf is vastgesteld dat de organisatie een werkend procedure heeft aangaande het verbeteren van het niveau en het herstellen van afwijkingen. Dit is vastgesteld tijdens de interviews en aantoonbaar dat er mutaties in het verbeterregister zijn gemuteerd. Deze mutaties komen voort uit o.a. uit de interne audits, risicoanalyses en externe audit. De status van preventieve en corrigerende maatregelen wordt met codes aangegeven in het verbetermanagement. **Sterke punt:** De geïnterviewde medewerkers waren bekend met het melden van incidenten (wat, hoe en waarom is het belangrijk om te melden) en de wet- regelgeving m.b.t. datalekken.	C
10.2 Continual improvement shall continually improve the suitability, adequacy and effectiveness of the ISMS	Tijdens de audit is vastgesteld dat men de wil heeft om continue te verbeteren en dit ook laat zien op basis van gestelde plannen en acties.	C

Annex A, table A1 EN-ISO27001 (normative)

Evaluation aspects & Findings	Control objectives & controls *C=Conform, NC=Non Conformity, MC=Major Non Conformity, NA=Not Applicable*	C/NC/MC/ NA
5 Information security policies		
5.1 Management direction for information security	Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.	-
5.1.1 Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties; In het beleid van het ISMS opgenomen; WPB is opgenomen in het beleid naast wet criminaliteit Meldplicht datalekken is dieper in het ISMS opgenomen. NEN7510 staat in de doelstellingen / uitgangspunten. NEN7512 en 7513 is niet direct van toepassing gezien de scope van de organisatie. Het wordt echter wel meegenomen als dienstverlening naar de klanten toe.	C
5.1.2 Review of the policies for information security	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness; Het beleid en informatiebeleidsplan worden ieder jaar geëvalueerd. Indien nodig wordt beleid en procedures tussentijds aangepast,	C
6 Organization of information security		
6.1 Internal organization	Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization	-
6.1.1 Information security roles and responsibilities	All information security responsibilities shall be defined and allocated; . Documenten aantoonbaar: Rollen en functies zijn beschreven	C
6.1.2 Segregation of duties	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets; Documenten aantoonbaar: In de verantwoordelijk heden matrix is dit opgenomen. Er is een tabel die dit regelt	C
6.1.3 Contact with authorities	Appropriate contacts with relevant authorities shall be maintained ; lid van diverse brancheorganisaties en commissies, men houd zich zelf via kennis deling op de hoogte VNG, VWS als informatieverstrekker. Autoriteit Persoonsgegevens is informatief.	C
6.1.4 Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained; Documenten aantoonbaar: KMS	C
6.1.5 Information security in project management	Information security shall be addressed in project management, regardless of the type of the project; Heeft een doorlopende ontwikkeling, in alle projecten staat IB hoog op de agenda.	C
6.2 Mobile devices and teleworking	Objective: To ensure the security of teleworking and use of mobile devices.	-
6.2.1 Mobile device policy	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices; Definitie "mobile devices" is alles wat mobiel data kan bevatten en in het ISMS gespecificeerd. Dit is ook in de arbeidsovereenkomst opgenomen, indien extern ingelogd wordt om data te verwerken.	C

Evaluation aspects & Findings	Control objectives & controls *C=Conform, NC=Non Conformity, MC=Major Non Conformity, NA=Not Applicable*	C/NC/MC/ NA
6.2.2 Teleworking	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites; Documenten aantoonbaar: KMS.	C
7 Human resource security		
7.1 Prior to employment	Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.	-
7.1.1 Screening	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks; Opgenomen in het ISMS is dat een VOG wordt aangevraagd. Er is een specifieke categorie die hierin van toepassing is	C
7.1.2 Terms and conditions of employment	The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security; Er zijn overeenkomsten waarin de spelregels ten aanzien van vertrouwelijkheid en beveiliging. De template is opgeslagen in het KMS	C
7.2 During employment	Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.	-
7.2.1 Management responsibilities	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization; Dit is opgenomen in de functieomschrijvingen en matrix bevoegdheden en toegang.	C
7.2.2 Information security awareness, education and training	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function; (ISMS)heeft de volgende rubrieken, introductie ISMS, crisisteam, verdiepende scholing ISO27001/NEN7510 en continuiteitsbeheer Ieder jaar ontvangt een medewerker een vragenlijst ISMS. De uitkomsten van de vragenlijsten wordt weergegeven in de directiebeoordeling.	C
7.2.3 Disciplinary process	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach; In het ISMS is dit opgenomen	C
7.3 Termination and change of employment	Objective: To protect the organization's interests as part of the process of changing or terminating employment	-
7.3.1 Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced; Bij de beëindiging van de arbeidsovereenkomst wordt een "checklist einde dienstverband" gebruikt,	C
8 Asset management		
8.1 Responsibility for assets	Objective: To identify organizational assets and define appropriate protection responsibilities.	-
8.1.1 Inventory of assets	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained; Er is een BIV lijst. In deze lijst is aangegeven wat het risico is (BIV). BIV classificatie is voor het laatst geactualiseerd 2017.	C

Evaluation aspects & Findings	Control objectives & controls *C=Conform, NC=Non Conformity, MC=Major Non Conformity, NA=Not Applicable*	C/NC/MC/ NA
8.1.2 Ownership of assets	Assets maintained in the inventory shall be owned; De eigenaren en beheerders zijn beschreven in deze lijst.	C
8.1.3 Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented;	C
8.1.4 Return of assets	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement; Documenten aantoonbaar: checklist einde dienstverband	C
8.2 Information classification	Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization	-
8.2.1 Classification of information	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification; Documenten aantoonbaar: BVI Er zijn 4 niveaus volgens indeling NEN7510. Er is een procedure die omschrijft hoe toegang en beveiliging is georganiseerd.	C
8.2.2 Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization; Documenten aantoonbaar: De labeling is ingestoken op basis van de classificatie.	C
8.2.3 Handling of assets	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization; BIV lijst geeft inzage in de middelen; BIV classificatie bedrijfsmiddelen.	C
8.3 Media handling	Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.	-
8.3.1 Management of removable media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization; Zie 8.2.3.	C
8.3.2 Disposal of media	Media shall be disposed of securely when no longer required, using formal procedures; Procedure gezien en akkoord	C
8.3.3 Physical media transfer	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation; Alle data staat op de server, data dragers in de serverruimte komen niet buiten de server ruimte.	C
9 Access control		
9.1 Business requirements of access control	Objective: To limit access to information and information processing facilities	**T**
9.1.1 Access control policy	An access control policy shall be established, documented and reviewed based on business and information security requirements; Er is een procedure dat omschrijft hoe toegang en beveiliging is georganiseerd.	C
9.1.2 Access to networks and network services	Users shall only be provided with access to the network and network services that they have been specifically authorized to use;	C

Evaluation aspects & Findings	Control objectives & controls *C=Conform, NC=Non Conformity, MC=Major Non Conformity, NA=Not Applicable*	C/NC/MC/ NA
	Er zijn overzichten van de infrastructuur hoe deze is opgebouwd en beveiligd, er is hierbij naar NEN7512 gekeken en heeft een eigen classificatie qua beveiligingen gekozen. Er is een DMZ getekend in het netwerk. De gevoelige klantdata staat in het data center. (gecertificeerd)	
9.2 User access management	Objective: To ensure authorized user access and to prevent unauthorized access to systems and services	-
9.2.1 User registration and de-registration	A formal user registration and de-registration process shall be implemented to enable assignment of access rights; Het gaat hierbij over de rechten lijst.	C
9.2.2 User access provisioning	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services; Het lopende system met certificaten (licentie codes) maakt het mogelijk om rechten te installeren en te de installeren.	C
9.2.3 Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled; Documenten aantoonbaar: De directie en de admistrator hebben meer bevoegdheden dan gemiddeld. Dit is opgenomen in de risico analyse. Ontwikkelaar kan met eigen PC via een VPN in het systeem, Algemene voorwaarden gezien	C
9.2.4 Management of secret authentication information of users	The allocation of secret authentication information shall be controlled through a formal management process; Dossier staat in de kast met acces control.	C
9.2.5 Review of user access rights	Asset owners shall review users' access rights at regular intervals; Documenten aantoonbaar: KMS	C
9.2.6 Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change; Zie 9.2.2 en 8.1.	C
9.3 User responsibilities	Objective: To make users accountable for safeguarding their authentication information	-
9.3.1 Use of secret authentication information	Users shall be required to follow the organization's practices in the use of secret authentication information; User list.	C
9.4 System and application access control	Objective: To prevent unauthorized access to systems and applications	-
9.4.1 Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy; User list	C
9.4.2 Secure log-on procedures	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure; Er zijn 4 niveaus volgens indeling NEN7510. Er is een procedure die omschrijft hoe toegang en beveiliging is georganiseerd.	C
9.4.3 Password management system	Password management systems shall be interactive and shall ensure quality passwords;	C

Evaluation aspects & Findings	Control objectives & controls *C=Conform, NC=Non Conformity, MC=Major Non Conformity, NA=Not Applicable*	C/NC/MC/ NA
	Wachtwoordprocedure KMS Er is een beschrijving gekoppeld aan de interne hosting in een apart dossier.	
9.4.4 Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled; *Zie 9.9.2*	C
9.4.5 Access control to program source code	Access to program source code shall be restricted; Er zijn source codes voor de eigen ontwikkelde software. De ontwikkelaars en de directie hebben toegang.	C
10 Cryptography		
10.1 Cryptographic controls	Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information	-
10.1.1 Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented; Wordt jaarlijks vervangen door de leverde partijen.	C
10.1.2 Key management	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle; Wordt jaarlijks vervangen door de leverde partijen.	C
11 Physical and environmental security		
11.1 Secure areas	Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities	-
11.1.1 Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities; Acces control is georganiseerd.	C
11.1.2 Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access; Acces control is georganiseerd.	C
11.1.3 Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and applied; Acces control is georganiseerd.	C
11.1.4 Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied; Directie vindt dit niet aannemelijk (dat de locatie hier niet mee te maken krijgt).	NA
11.1.5 Working in secure areas	Procedures for working in secure areas shall be designed and applied; Acces control is georganiseerd	C
11.1.6 Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access; Deze zijn niet aanwezig.	NA
11.2 Equipment	Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations	-
11.2.1 Equipment siting and protection	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. Zie 11.1.2 en 11.1.4.	NA

Evaluation aspects & Findings	Control objectives & controls *C=Conform, NC=Non Conformity, MC=Major Non Conformity, NA=Not Applicable*	C/NC/MC/ NA
11.2.2 Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities; UPS draait; 5 + 10 minuten is de eis voor gecontroleerd afschakelen, er is nu autonomie voor 1 uur.	C
11.2.3 Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage; Alle kabels in het pand liggen in kabelgoten.	C
11.2.4 Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity; UPS wordt zelf gemonitord er is geen extern onderhoud. Er zijn geen kritische componenten die verder onderhoud vragen.	C
11.2.5 Removal of assets	Equipment, information or software shall not be taken off-site without prior authorization; Is geregeld.	C
11.2.6 Security of equipment and assets off-premises	Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises; Is geregeld in de contracten personeel en het document toegang en beveiliging.	C
11.2.7 Secure disposal or reuse of equipment	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use; Zie eerdere.	C
11.2.8 Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection; Overeenkomst personeel	C
11.2.9 Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted; Documenten aantoonbaar: Clear screen en disk is beschreven	C
12 Operations security		
12.1 Operational procedures and responsibilities	Objective: To ensure correct and secure operations of information processing facilities; Documenten aantoonbaar: KMS	-
12.1.1 Documented operating procedures	Operating procedures shall be documented and made available to all users who need them; Documenten aantoonbaar: KMS Alle procedures zijn toegankelijk	C
12.1.2 Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled; Organisatie werkt via "ITIL" tijdens alle interviews komt dit goed naar voren, medewerkers zijn inhoudelijk goed op de hoogte.	C
12.1.3 Capacity management	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance;	C

Evaluation aspects & Findings	Control objectives & controls *C=Conform, NC=Non Conformity, MC=Major Non Conformity, NA=Not Applicable*	C/NC/MC/ NA
	Documenten aantoonbaar: KMS	
12.1.4 Separation of development, testing and operational environments	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment;	C
12.2 Protection from malware	Objective: To ensure that information and information processing facilities are protected against malware	-
12.2.1 Controls against malware	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness; Documenten aantoonbaar: op alle systemen draaien programma's om dit te voorkomen. Updates draaien real-time.	C
12.3 Backup	Objective: To protect against loss of data.	-
12.3.1 Information backup	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy; Documenten aantoonbaar: Risicoprofiel 2017 Leveranciersbeoordeling 2017 Worden gedraaid in het data center i.v.m. de externe hosting, heeft een back-up. Op basis van een tweede partij audit bij het data center is de SLA aangepast. 4 uurs eis is nog niet duidelijk gecommuniceerd. Dit wordt ook voor het eigen data center ook gedaan.	C
12.4 Logging and monitoring	Objective: To record events and generate evidence	-
12.4.1 Event logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed; Is opgenomen.	C
12.4.2 Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access; Is opgenomen.	C
12.4.3 Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed Bevoegdheden structuur.	C
12.4.4 Clock synchronisation	The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source; Is georganiseerd via de diverse software, waarin dit standaard is opgenomen.	C
12.5 Control of operational software	Objective: To ensure the integrity of operational systems	-
12.5.1 Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems;	C
12.6 Technical vulnerability management	Objective: To prevent exploitation of technical vulnerabilities	-
12.6.1 Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk; Dit is meegenomen in de risico analyse. Hierin zijn kwetsbaarheden in de evaluatie opgenomen. *Er zijn nog geen testen gepland conform bijlage D2 van IEC27005 conform de huidige inzichten.*	C

Evaluation aspects & Findings	Control objectives & controls *C=Conform, NC=Non Conformity, MC=Major Non Conformity, NA=Not Applicable*	C/NC/MC/ NA
	Er is verder wel sprake van een complete review van software en hardware o.b.v. de laatste inzichten, *pen-testen* kunnen dan een onderdeel van dit management gaan uitmaken.	
12.6.2 Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented; Er is overzicht van de lopende software. Men is aan het bepalen welke software op welke hardware mag staan binnen de fysieke beveiligde omgeving en de hardware die daar buiten kan functioneren en de hardware die valt onder categorie “bring your own device”. Hierbij wordt ook naar tablets en smart-phones gekeken.	C
12.7 Information systems audit considerations	Objective: To minimise the impact of audit activities on operational systems.	-
12.7.1 Information systems audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes; Er is een software tool die alle logfiles verzameld, deze tool ontvangt alle loggings op basis waarvan de nodige verificaties gedaan kunnen worden.	C
13 Communications security		
13.1 Network security management	Objective: To ensure the protection of information in networks and its supporting information processing facilities	-
13.1.1 Network controls	Networks shall be managed and controlled to protect information in systems and applications; SIEM; tools en maatregelen	C
13.1.2 Security of network services	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced; De netwerk aansluitingen gaan via het datacenter.	C
13.1.3 Segregation in networks	Groups of information services, users and information systems shall be segregated on networks; Productie is gescheiden van ontwikkeling.	C
13.2 Information transfer	Objective: To maintain the security of information transferred within an organization and with any external entity	-
13.2.1 Information transfer policies and procedures	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities; De netwerk aansluitingen gaan via het data center.	C
13.2.2 Agreements on information transfer	Agreements shall address the secure transfer of business information between the organization and external parties; Er zijn uitwisselingsovereenkomsten waar voorafgaand een sreening op personen en partijen plaatsvindt voordat de uitwisseling plaatsvindt.	C
13.2.3 Electronic messaging	Information involved in electronic messaging shall be appropriately protected; NAD is geregeld.	C
13.2.4 Confidentiality or nondisclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information shall be identified, regularly reviewed and documented; NAD is geregeld.	C
14 System acquisition, development and maintenance		
14.1 Security requirements of information systems	Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks	-
14.1.1 Information security	The information security related requirements shall be included in the requirements	C

Evaluation aspects & Findings	Control objectives & controls *C=Conform, NC=Non Conformity, MC=Major Non Conformity, NA=Not Applicable*	C/NC/MC/ NA
requirements analysis and specification	for new information systems or enhancements to existing information systems; Er is een beschrijving van de de software. Dit is opgenomen binnen het proces ontwikkeling software. Er wordt binnen het proces OTAP toegepast. (Ontwikkeling – Testsen – Acceptatie – Productie) Er is een stappenplan waarin de uitgangspunten software is opgenomen hoe de authenticatie is verzorgd in tabel 3 van het document omschrijft het niveau aan beveiliging. De standaard lagen methodiek is toegepast	
14.1.2 Securing application services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification; *Idem*	C
14.1.3 Protecting application services transactions	Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay; *Idem*	C
14.2 Security in development and support processes	Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems	-
14.2.1 Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organization; Proces beschrijving. Gezien en changes doorlopen	C
14.2.2 System change control procedures	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures; Updates worden gelijk behandeld als initiële ontwikkelingen waarbij ook OTAP wordt toegepast.	C
14.2.3 Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security; Idem	C
14.2.4 Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled; Er is een drie lagen model, waarbij de klant nooit op de belangrijkste laag kan komen.	C
14.2.5 Secure system engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts; SOA en OTAP	C
14.2.6 Secure development environment	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle; De software wordt alleen op het kantoor ontwikkeld.	C
14.2.7 Outsourced development	The organization shall supervise and monitor the activity of outsourced system development; NVT	NA
14.2.8 System security testing	Testing of security functionality shall be carried out during development	-
14.2.9 System acceptance testing	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions; OTAP ontwikkeling Ontwikkel server worden alle wijzigingen in verwerkt. Ontwikkeling en release van software	C

Evaluation aspects & Findings	Control objectives & controls *C=Conform, NC=Non Conformity, MC=Major Non Conformity, NA=Not Applicable*	C/NC/MC/ NA
	Semi gecreëerde (O)TAP omgeving vanuit de ontwikkelsoftware is te connecteren naar alle databases, produktiedata staat alleen in produktie omgeving. Autorisaties worden op verschillende plekken uitgezet 3 fase structuur - Transport - Transport met dummy - Transport met volledige autorisatie Aandachtspunt: vanuit ontwikkel kan je inloggen naar alle omgevingen, het zou mooi zijn als hier een afscheiding komt dat je alleen naar ontwikkel of test omgevingen kunt inloggen.	
14.3 Test data	Objective: To ensure the protection of data used for testing	-
14.3.1 Protection of test data	Test data shall be selected carefully, protected and controlled; OTAP	C
15 Supplier relationships		
15.1 Information security in supplier relationships	Objective: To ensure protection of the organization's assets that is accessible by suppliers	-
15.1.1Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented; Documenten aantoonbaar: Data center; contract gezien	C
15.1.2 Addressing security within supplier agreements	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information;	C
15.1.3 Information and communication Technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain;	C
15.2 Supplier service delivery management	Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements	-
15.2.1 Monitoring and review of supplier services	Organizations shall regularly monitor, review and audit supplier service delivery; Leveranciersbeoordeling heeft plaatsgevonden in 2017. OP basis hiervan zijn verbeteringen toegepast.	C
15.2.2 Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks;	C
16 Information security incident management		
16.1 Management of information security incidents and improvements	Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses	-
16.1.1 Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents; Is geregeld in het ISMS	C
16.1.2 Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible;	C
16.1.3 Reporting information security weaknesses	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services;	C
16.1.4 Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents;	C
16.1.5 Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures;	C

Evaluation aspects & Findings	Control objectives & controls *C=Conform, NC=Non Conformity, MC=Major Non Conformity, NA=Not Applicable*	C/NC/MC/ NA
16.1.6 Learning from information security incidents	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents; Er zitten in hety KMS indicatoren om zaken te rubriceren, hiervan kunnen statistieken gedraaid worden voor analyses. Er wordt voldoende geleerd van incidenten en verbetermaatregelen uitgevoerd.	C
16.1.7 Collection of evidence	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence; Auditlogs of anders klachten die gemeld zijn.	C
17 Information security aspects of business continuity management		
17.1 Information security continuity	Objective: Information security continuity shall be embedded in the organization's business continuity management systems	-
17.1.1 Planning information security continuity	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster; Procedures en werkwijze zijn gezien,.	C
17.1.2 Implementing information security continuity	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation; Idem.	C
17.1.3 Verify, review and evaluate information security continuity	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations;	C
17.2 Redundancies	Objective: To ensure availability of information processing facilities	-
17.2.1 Availability of information Processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements; Infra structuur maakt dit mogelijk	C
18 Compliance		
18.1 Compliance with legal and contractual requirements	Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements	-
18.1.1 Identification of applicable legislation and contractual requirements	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization; Wetgeving is opgenomen in het ISMS en akkoord. Er is referentie tabel NEN 7510.	C
18.1.2 Intellectual property rights	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products; Er wordt met eigen software gewerkt. Het beleid aangaande software van derden is dat deze minimaal wordt ingezet en legaal moet zijn. Escrow nog niets concreet er zijn al wel gedachte hierover en hebben al gesprekken plaatsgevonden. Verder op basis van klanteisen	C
18.1.3 Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements;	C
18.1.4 Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable;	C
18.1.5 Regulation of cryptographic	Cryptographic controls shall be used in compliance with all relevant agreements,	C

Evaluation aspects & Findings	Control objectives & controls *C=Conform, NC=Non Conformity, MC=Major Non Conformity, NA=Not Applicable*	C/NC/MC/ NA
Controls	legislation and regulations; Is gebaseerd op de netwerk structuren.	
18.2 Information security reviews	Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures	-
18.2.1 Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur; Kiwa komt jaarlijks auditen. Er is verder een ontwikkeling om de software en de infra structuur te beoordelen.	C
18.2.2 Compliance with security policies and standards	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements;	C
18.2.3 Technical compliance review	Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards; Er is verder een ontwikkeling om de software en de infra structuur te beoordelen.	C

Procesbeoordeling	NEN 7510	Overzicht gecontroleerde documentatie
Beveiligde ruimten Fysieke beveiliging van de omgeving	9.1	Zie IEC27001; bijlage A9
Uitwisseling van informatie	10.8	
Beleid en procedures voor informatie-uitwisseling Bepaal voor de uitwisseling van zorginformatie de minimaal vereiste maatregelen volgens de aanwijzingen van NEN7512 *VPN / PKI*	10.8.1	Zie IEC27001; bijlage A13
Elektronische berichtenuitwisseling Volg de aanwijzingen in NEN7512	10.8.4	Zie IEC7001; bijlage A13. Er is een BIV classificatie gemaakt voor bedrijfsmiddelen. Vanuit data classificatie zijn er 4 niveaus. Voor 4B is er een golden key.
Vertrouwensbasis voor gegevensuitwisseling Vertrouwen Vertrouwensdomein Vertrouwde instantie; *CIBG / UZI - pas* Vertrouwende partij Te vertrouwen partij Zekerheid; *4 levels: L, M, H en ZH; ISO/IEC 29115; identificatie & authenticatie*	-4	NEN7512
Risicobeheersing van de gegevensuitwisseling	-5.1	NEN7512
Classificeren van de gegevensuitwisseling; *4 levels Beschikbaarheid; Integriteit; Vertrouwelijkheid*	-5.2	Zie annex A
Bepalen van de bedreigingen; *relevante bedreigingen meegenomen* Bepalen van de kwetsbaarheden; *'robuustheid' en 'veerkracht' (resilience)*	-5.3	Zie annex A
Risicobeoordeling ; *figuur 2*	-5.4	Zie annex A
Behandelen van de risico's *het vermijden van risico's* *het treffen van geschikte beheersmaatregelen* *het overdragen van risico's* *het bewust en objectief aanvaarden van risico's*	-5.5	Zie annex A
Beheersmaatregelen	-6	NEN7512

Beheersmaatregelen omtrent de te maken afspraken Beleid en procedures voor gegevensuitwisseling Uitwisselingsovereenkomsten Beheer van de dienstverlening door derde partij; *SLA / Programma van eisen Goedbeheerd ZorgNetwerk (GZN-eisen)* Bedieningsprocedures	-6.2	Zie annex A
Beheersmaatregelen omtrent de uitvoering van de afspraken	-6.3	NEN7512
Toekenning en beheer van identificatoren (KvK)	-6.3.1	Zie annex A
Registratie van entiteiten (keuze vlgs. tabel 5)	-6.3.2	Zie annex A
Authenticatie (keuze vlgs. tabel 6)	-6.3.3	Zie annex A
Elektronische berichtenuitwisseling Geen BSN; Exclusiviteitsniveau en aftapbaarheid van het kanaal tussen zender en ontvanger (uitersten zijn het publieke internet en een exclusief, niet-toegankelijk en afgeschermd fysiek medium); Toegepast encryptie-algoritme	-6.3.4	NVT,
Ondertekening Burgerlijk Wetboek Telecommunicatiewet – PKI – SSCD	-6.3.5	Zie annex A
Logging NEN7513	-6.3.6	Zie annex A
Beheersmaatregelen omtrent beheer en naleving Beheer van informatiebeveiligingsincidenten Capaciteitsbeheer Back-up en herstel Continuïteitsbeheer Naleving	-6.4	NEN7512
Overzicht van beheersmaatregelen en zekerheidsniveaus Tabel 7	-6.5	NEN7512
Controle	10.10	
Aanmaken audit-logbestanden Zie NEN7513	10.10.1	Zie IEC27001; bijlage A12.7

Te loggen gebeurtenissen - NEN7513 Operationele gebeurtenissen Gebeurtenissen die de toegangsregeling betreffen Gebeurtenissen die het loggen en de logging beïnvloeden	-6	NEN7513
Gegevensvelden in de logging - NEN7513 Identificatie van de gebeurtenis Identificatie van de gebruiker Identificatie van een betrokken object Identificatie van het toegangspunt Identificatie van de bron van de loggegevens	-7	NEN7513
Zekerheidseisen – NEN7513 Verantwoordelijkheid – WGBO Integriteit en onweerlegbaarheid van de logging Beschikbaarheid en toegankelijkheid van de logging Toegang tot de logging – WGBO/WBP Bewaartermijnen (15 jaar) Voorwaarden voor interoperabiliteit	-8	NEN7513
Toegangsbeveiliging voor besturingssystemen	11.5	
Beveiligde inlogprocedures Zie NEN7512	11.5.1	Zie annex A
Gebruikersidentificatie en -authenticatie Zie NEN7512	11.5.2	
Toegangsbeheersing voor toepassingen en informatie Beheersen van toegang tot informatie Isoleren van gevoelige systemen	11.6	Zie annex A
Beveiliging van systeembestanden Procedures voor Beheersing van operationele programmatuur	12.4	Zie annex A

3. Auditprogramma/plan

Naam	:	Share-board IT Groep B
Contactpersoon	:	DhWim van Asperen
E-mail	:	Wim@Share-board.nl
Relatienummer	:	
Vestigingsadres	:	Bosmanskamp 1B, 4191 MS Geldermalsen
Postadres	:	Idem
Telefoon	:	06 218 545 36

Aantal vestigingen : 01 Medewerkers : 3

Onderzoek

Soort onderzoek	:	initiële audit
Onderdeel	:	Implementatie
Datum onderzoek	:	10 augustus en 13 oktober 2017
Datum rapport, versie	:	November 2017, versie 01

Auditteam
Lead Audito Berrie Steer
Auditor (-en)
Materiedeskundige
Reglement(en)

Norm(en)	Toepassingsgebied(en)	Scope/ NACE	Certificaatnr. en afloopdatum
Norm ISO27001: 2013 en NEN 7510:2011	34B - 38 38		

SCOPE:

NEN7510:2011
Het ISMS van Share-board betreft de informatiebeveiliging en de privacybescherming van patiëntengegevens en/of bedrijfsgevoelige informatie alsmede de persoonsgegevens van de Gebruikers zelf, die door Gebruikers aan Share-board worden toevertrouwd om onderling makkelijk en vertrouwelijk te kunnen samenwerken.

ISO27001:2013
Het ISMS van Share-board betreft de informatiebeveiliging en de privacybescherming van bedrijfsgevoelige informatie en/of bijzondere persoonsgegevens alsmede de persoonsgegevens van de Gebruikers zelf, die door Gebruikers aan Share-board worden toevertrouwd om onderling makkelijk en vertrouwelijk te kunnen samenwerken.

Auditplanning

Bij de uitvoering van de audit zal het onderstaande schema worden aangehouden. Indien de omstandigheden hiertoe aanleiding geven, kan in onderling overleg van deze planning worden afgeweken.

De contactpersoon draagt er zorg voor dat de betrokken personen op het aangegeven tijdstip beschikbaar zijn voor het interview. Wij verzoeken u een andere auditee te vragen, daar waar mogelijk, dan degene die al eerder zijn geïnterviewd.

De audit verloopt het prettigst als men niet door externe factoren gestoord wordt.

Interne auditoren zijn welkom, mits zij een passieve houding tijdens het interview aannemen.

Het kan zijn dat de auditees worden gevraagd naar aantoonbaarheid van documenten en/of procedures. Het verdient daarom de voorkeur dat deze tijdens het interview snel te traceren zijn.

Graag, *indien relevant en/of aanwezig*, ter inzage klaarleggen de volgende documenten:

- ISMS-procedures/werkinstructies
- Aangewezen verantwoordelijken m.b.t. ISMS
- Risico-inventarisatie – en analyses
- Beleid voor ISMS (incl. toepassingsgebied)
- Informatiebeveiligingsplan
- Continuïteitsplan(nen)
- Directiebeoordeling ISMS
- Verslagen en Planning van interne ISMS-audits
- Incidentmeldingen met doorlopen PDCA cyclus
- Contracten/overeenkomsten (met derde partijen)
- Documenten t.b.v. onderhoud apparatuur (indien van toepassing)
- Personeelsdossiers
- Indien van toepassing Plannen van Aanpak voorafgaande audits voorzien van actuele status acties

Auditplan voor auditor : **Berrie Steer**			
Datum : 10 augustus 2017			
Locatie : Geldermalsen			
Tijd	Activiteit	Processen en normeisen	Naam en functie Auditees
2)			
09.00 - 9.30	Openingsgesprek		Management en Belangstellenden
09.30- 10.00	doornemen gevraagde bovenstaande documenten Berrie Steer	n.v.t.	n.v.t.
10.00 - 11.30	Interview 1 Berrie Steer	Organisatie & informatiebeleid - Beheersing risico-inventarisatie – en analyses - Beleid voor ISMS (incl. toepassingsgebied) - Informatiebeveiligingsplan - Continuiteitsplan(nen) - Directiebeoordeling ISMS - Interne en externe communicatie - Ketenpartners	Directie
11.30 - 12.30	Interview 2	Audits Interne audits - ISMS-procedures/werkinstructies - Beheer documenten - Meldingen	Directie
12.30 - 13.15	Lunch		
13.15- 14.30	Interview 3	HR security - HR processen - Controle personeelsdossiers	Directie
14.30- 15.15	Interview 4	Backoffice - Informatie aan klanten - Verwerken klantgegevens - Privacy wetgeving - Beheer klantgegevens	Directie
15.15 - 16.00	Interview 5	Business development - Privacy wetgeving - klantgegevens - ISMS-procedures	Directie Business developer
16.00- 17.00	Interview 6	Front office - Informatie aan klanten - Verwerken klantgegevens - Privacy wetgeving - Beheer klantgegevens	Directie
17.30 – 18.00	Eindgesprek 1e auditdag		Aanwezigen: **Directie**

Auditplan voor auditor : **Berrie Steer**			
Datum : 13 oktober 2017			
Locatie : Geldermalsen			
Tijd	Activiteit	Processen en normeisen	Naam en functie Auditees
2)			
09.00 - 9.30	Openingsgesprek		Directie Business developer
09.30- 10.00	doornemen gevraagde bovenstaande documenten Berrie Steer	n.v.t.	n.v.t.
10.00 - 11.30	Interview 1 Berrie Steer	Organisatie & informatiebeleid - Beheersing risico-inventarisatie – en analyses - Beleid voor ISMS (incl. toepassingsgebied) - Informatiebeveiligingsplan - Continuiteitsplan(nen) - Directiebeoordeling ISMS - Interne en externe communicatie - Ketenpartners	Directie Business developer
11.30 - 12.30	Interview 2	Audits Interne audits - ISMS-procedures/werkinstructies - Beheer documenten - Meldingen	Directie Business developer
12.30 - 13.15	Lunch		
13.15- 14.30	Interview 3	HR security - HR processen - Controle personeelsdossiers	Directie Business developer
14.30- 15.15	Interview 4	Backoffice - Informatie aan klanten - Verwerken klantgegevens - Privacy wetgeving - Beheer klantgegevens	Directie Business developer
15.15 - 16.00	Interview 5	Business development - Privacy wetgeving - klantgegevens - ISMS-procedures	Directie Business developer
16.00- 17.00	Interview 6	Front office - Informatie aan klanten - Verwerken klantgegevens - Privacy wetgeving - Beheer klantgegevens	Directie Business developer
17.30 – 18.00	Eindgesprek 2de auditdag		Aanwezigen: Directie Business developer