>>> CIIO Maatstaf Combi 2020

CIIO is door de Raad voor Accreditatie (RvA) erkend als certificeerder voor de professionele dienstverlening en informatiebeveiliging. Sinds 2006 toetst CIIO professionele dienstverleners aan de hand van de eigen CIIO Maatstaf. Dit is een door de Raad voor Accreditatie geaccepteerde praktische interpretatie van de ISO 9001 norm, helder en toegankelijk geformuleerd. In 2019 is de CIIO Maatstaf uitgebreid met de interpretatie van de ISO 27001 en NEN 7510 norm. Deze gecombineerde versie draagt de naam CIIO Maatstaf Combi 2020 en is nog niet door de RvA geaccepteerd.

De missie van CIIO is: door toetsing een wezenlijke bijdrage leveren aan de prestaties van haar klanten.

CIIO, de CIIO Maatstaf en de CIIO Maatstaf Combi

CIIO is een netwerkorganisatie van professionele en bevlogen beoordelaars. Kenmerkend is dat alle beoordelaars, naast het werk voor CIIO, ook werken in de kennisintensieve dienstverlening als adviseur, trainer, manager of onderzoeker. Deze praktijkervaring zet CIIO gericht in bij de organisaties die wij beoordelen. Klanten kunnen erop rekenen dat elk onderzoek met kennis van zaken en inlevingsvermogen wordt uitgevoerd.

De CIIO Maatstaf en de CIIO Maatstaf Combi geven professionele dienstverleners houvast en inspiratie voor het opzetten van een werkbaar en passend managementsysteem. CIIO stelt deze interpretaties zonder kosten op haar website beschikbaar.
De CIIO Maatstaven en de onderzoeken van CIIO worden door klanten ervaren als stimulans tot reflectie op hun vak, op hun bijdrage aan de processen in de organisatie en op het werken met en voor hun klanten.

De CIIO Maatstaf en de CIIO Maatstaf Combi worden toegepast in een aantal branches. In het kader van certificering worden deze branches ingedeeld in EA Codes. De CIIO Maatstaf is door de Raad voor Accreditatie geaccepteerd om professionele dienstverleners te toetsen die vallen onder de volgende EA Codes:

EAC	Organisaties
34	Architectenbureaus, ingenieursbureaus
35	Bureaus op het gebied van organisatieadvies, markt- en wetenschappelijk onderzoek opleiding en training, re-integratie en loopbaanadvies en interim- en projectmanagement
36	Overheidsdiensten, justitie en justitiële diensten
37	Onderwijs
38	Gezondheidszorg en welzijnszorg

Voor de CIIO Maatstaf Combi wordt acceptatie van de RvA gezocht in dezelfde branches.

Kenmerken professionele dienstverleners

Klanten van CIIO hebben veelal de volgende kenmerken:

- Zij kennen doorgaans geen productieproces maar verlenen diensten zoals advies, scholing, coaching, interim-management, onderzoek, overheidstaak of behandeling.
- Naast de directe klant of cliënt is er vaak sprake van een bredere groep belanghebbenden bij de dienstverlening met vaak verschillende belangen. Denk aan financiers, overheden, samenwerkingspartners, de directe omgeving van klanten/cliënten en burgers.

- De dienstverlening maakt regelmatig deel uit van een keten waarin ook allerlei andere organisaties een rol vervullen. Ketensamenwerking is dan aan de orde en essentieel om het gewenste kwaliteitsniveau te bereiken met het eigen kernproces.
- Er is weinig routinematig werk; dienstverlening is maatwerk. Er wordt gewerkt met een planmatige aanpak met fases als intake, klantafspraken, plan van aanpak, uitvoering, monitoring en waar nodig bijstelling en evaluatie. Dit alles in nauwe samenspraak en veelal in samenwerking met de klant.
- Een afwijking of incident is meestal niet via controle vooraf te voorkomen. Dit vergt een zorgvuldige risico-inschatting en een weloverwogen borging van werkprocessen.
- De professionals met hun competenties en ervaring (in dienst of als externe professional aan de organisatie verbonden) zijn sterk bepalend voor de kwaliteit die de klant ervaart. Zij vervullen in het algemeen zelf de werkzaamheden in contact met de klant en hebben daardoor met hun inzet en houding directe invloed op de klanttevredenheid.
- Kennismanagement en een professionele houding zijn sleutels voor succes.

Voor de klanten van CIIO voor de CIIO Maatstaf Combi komen daar de volgende kenmerken bij:
- Zij verwerken in een sterk IT gerichte omgeving veelal vertrouwelijke gegevens.
- Zij hechten een groot belang aan de beschikbaarheid, integriteit en/of vertrouwelijkheid van die gegevens .
- De dienstverlening maakt regelmatig deel uit van een keten waarin ook allerlei andere organisaties een rol vervullen. Ketensamenwerking is dan aan de orde en essentieel om het gewenste kwaliteitsniveau te bereiken met het eigen kernproces.

Professionele dienstverleners kiezen voor de CIIO Maatstaf of de CIIO Maatstaf Combi (en daarmee de ISO 9001, ISO 27001 en/of de NEN 7510 norm) om zich te laten certificeren:
- De Maatstaf geeft houvast bij de uitvoering van omgevingsanalyses, de inschatting van kansen en risico's en de opzet van het eigen managementsysteem.
- Het behalen van een CIIO Maatstaf certificaat (en daarmee een ISO 9001:2015 en na accreditatie door de RvA ook ISO 27001:2013 en/of NEN 7510:2017 certificaat) geeft vertrouwen aan klanten en andere belanghebbenden.
- Certificering geeft een voorsprong bij offreren en aanbesteden.

Uiteindelijke doelen zijn:
- Vergroten van klantgerichtheid.
- Verbeteren van prestaties.
- Innoveren van de dienstverlening.
- Beheersen van kwaliteitsrisico's.
- Beheersen van informatiebeveiligingsrisico's.
- Vergroten van efficiency.
- Beheersen van kosten.

Visie van CIIO op certificeren

CIIO hanteert de volgende uitgangspunten:
1. Het leveren van kwaliteit ziet CIIO niet los van de missie, visie en strategie van de organisatie. De ISO 9001 norm presenteert 'kwaliteit' als een aparte factor en spreekt van kwaliteitsbeleid, kwaliteitsdoelstellingen en kwaliteitsmanagementsysteem. Ook de ISO 27001 en NEN 7510 normen presenteren 'informatiebeveiliging' als een aparte factor en spreekt van informatiebeveiligingsbeleid, informatiebeveiligingsdoelstellingen en informatiebeveiligingmanagementsysteem.
   De CIIO Maatstaf en de CIIO Maatstaf Combi spreken van beleid, doelstellingen en managementsysteem, zonder het voorvoegsel 'kwaliteit' of 'informatiebeveiliging'.
2. De CIIO Maatstaf en de CIIO Maatstaf Combi zijn (net als de ISO 9001:2015) gebaseerd op de zeven principes van kwaliteitsmanagement: leiderschap, klantfocus, betrokkenheid van professionals, relatiemanagement, procesbenadering, risicomanagement en continu verbeteren. CIIO verwacht dat de leiding van een professionele organisatie deze principes uitdraagt.

3. Professionals zijn met hun competenties en ervaring cruciaal voor het leveren van kwaliteit. CIIO ziet professionals dan ook als onderdeel van het managementsysteem.
   Het managementsysteem omvat daarom niet alleen de 'harde' onderdelen (procedures, instructies, formats, criteria, software, specificaties, eisen) maar ook 'zachte' factoren (kennis, vaardigheden, gedrag, cultuur, normen en waarden, bewustzijn). Bij de toetsing van de werking van het managementsysteem kijkt CIIO dus niet alleen naar 'harde' bewijzen' (databases, netwerken, plannen, registraties, evaluaties en resultaten) maar ook naar 'softe' bewijzen (houding, inzet, motivatie, kennis delen, feedback geven).

Zo gaat de toetsing van CIIO

CIIO toetst organisaties aan de hand van de eisen in de CIIO Maatstaf. Beoordelaars voeren het onderzoek uit op een innovatieve, intelligente, integere en interactieve wijze. Dat gaat zo:

- Het onderzoek sluit aan bij de thematiek en karakteristiek van de organisatie. Vertrekpunt zijn de kenmerken, processen, systemen en afspraken van de organisatie. De CIIO Maatstaf is vervolgens het formele toetsingskader om hierover een oordeel te vormen.
- Het onderzoek wordt uitgevoerd door één of meer professionals die door hun kennis en ervaring in het werkveld van de betreffende dienstverlener direct tot de kern kunnen komen. Zij gaan met verstand van zaken in gesprek met medewerkers en partners.
- CIIO hanteert de volgende visie op 'het nieuwe beoordelen':

Van	>	**Naar**
Oordelen	>	Interveniëren
Procedure	>	Effect
Overlegstructuur	>	Multidisciplinaire samenwerking
Hoe het is	>	Hoe het ontwikkelt
Stellen	>	Vragen stellen
Momentopname	>	Continu leren
Dichttimmeren	>	Bandbreedte vaststellen
Structureren	>	Regelruimte
Terugkijken	>	Vooruitkijken
Corrigeren	>	Innoveren
Beoordelen	>	Waarderen
Proces	>	Resultaat
1ste orde vragen	>	2e orde vragen

- Het onderzoek levert een terugkoppeling en een rapportage op voor de organisatie, met concrete impulsen voor de verbetering van de kwaliteit van de dienstverlening. Naast de verbeterpunten komen ook de sterke kanten van de organisatie nadrukkelijk in beeld. Op deze wijze levert het onderzoek toegevoegde waarde aan de organisatie.
- Het resultaat van het onderzoek levert een erkend ISO 9001 certificaat op, als de organisatie aan alle eisen in de CIIO Maatstaf voldoet.
- Na accreditatie door de RvA levert het onderzoek een erkend ISO 27001 of NEN 7510 certificaat op, wanneer de organisatie aan de desbetreffende eisen in de CIIO Maatstaf Combi voldoet.

CIIO Maatstaf Combi en de ISO 9001, ISO 27001 en NEN 7510 normen

De CIIO Maatstaf Combi is een toegankelijke volledig dekkende interpretatie van de ISO 9001, ISO 27001 en NEN 7510 norm. De bijlagen bevatten gedetailleerde informatie over de overeenkomsten en verschillen tussen de eisen in de ISO norm en de formulering van die eisen in de CIIO Maatstaf. De bijlagen maken dan ook integraal deel uit van de CIIO Maatstaf Combi. De CIIO Maatstaf is gekoppeld aan de ISO 9001, ISO 27001 en NEN 7510 normen: wanneer een nieuwe uitgave van een van deze normen verschijnt, wordt ook de CIIO Maatstaf Combi aangepast aan de nieuwe norm.

Opbouw van de CIIO Maatstaf Combi

De CIIO Maatstaf Combi bestaat uit zes aandachtsgebieden:

Koers	Oriënteren op de omgeving, kansen en risico's vaststellen, leiderschap, aansturing, vernieuwing
Organisatie	Inrichting, verantwoordelijkheden en bevoegdheden, opzet en onderhoud van het managementsysteem, bedrijfszekerheid van de infrastructuur
Kernprocessen	Voor kwaliteitsmanagement: Afspreken, uitvoeren en afronden van dienstverlening Voor informatiebeveiliging: Selecteren van maatregelen, uitvoeren en beoordelen
Mensen	Werven, selecteren, ontwikkelen en evalueren van mensen
Partners	Samenwerken met partners, leveranciers en andere externen
Resultaten	Reflecteren op behaalde resultaten en vaststellen welke nieuwe maatregelen wenselijk zijn

Voor elk Maatstafonderdeel zijn eisen geformuleerd, ontleend aan ISO 9001:2015, ISO 27001:2013 en NEN 7510 en op maat gemaakt voor een kennisintensieve professionele dienstverlener. In de volgende hoofdstukken zijn de zes aandachtsgebieden van de maatstaf verder uitgewerkt in 18 maatstafonderdelen. Per maatstafonderdeel worden eisen geformuleerd. Per eis is als volgt aangegeven wanneer deze specifiek geldt voor de ISO 9001, ISO 27001 of NEN 7510 norm:

Markering voor de eis	**Betekenis markering**
>	Deze eis is op ISO 9001, ISO 27001 en NEN 7510 van toepassing
>K	Deze eis is specifiek voor ISO 9001 van toepassing (K staat voor kwaliteitsmanagement)
>IB	Deze eis is specifiek voor ISO 27001 en NEN 7510 van toepassing (IB staat voor informatiebeveiliging)
>IBZ	Deze eis is specifiek voor NEN 7510 van toepassing (Z staat voor zorg)

De aandachtsgebieden vormen samen een PDCA-cyclus:
Koers en Organisatie = PLAN,
Kernprocessen, Mensen en Partners = DO
Resultaten = CHECK en ACT

Het gaat hier om een cyclus van een half jaar tot meerdere jaren. Binnen de aandachtsgebieden bevinden zich korte PDCA-cycli, bijvoorbeeld het contracteren, uitvoeren en evalueren van een opdracht.

Koers

***Oriëntatie** - De leiding houdt zicht op de factoren die essentieel zijn voor het realiseren van de ambities van de organisatie*

> Een omgevingsanalyse uitvoeren en daarbij de relevante interne en externe factoren vaststellen, monitoren en evalueren.
> De belanghebbenden vaststellen die relevant zijn voor de organisatie en bepalen wat hun eisen en wensen zijn. Vervolgens dit monitoren en evalueren.
> Vaststellen welke diensten verleend worden aan welke belanghebbenden en dit communiceren.
> De wet- en regelgeving vaststellen die relevant is voor de organisatie en bepalen hoe die bijgehouden en toegepast wordt in de organisatie.
> De kansen en risico's vaststellen die voortkomen uit bovenstaande analyses. Vervolgens bepalen wat de consequenties hiervan zijn voor de organisatie en haar ambities en diensten. Daarna de kansen benutten en de risico's afdekken.

***Leiderschap** - De leiding demonstreert eigenaarschap van de organisatie en zet de koers uit*

> Missie, visie en strategie formuleren en uitdragen, rekening houdend met belanghebbenden, waarden en cultuur van de organisatie.
> Missie, visie en strategie uitwerken in beleid, evalueerbare doelstellingen en concrete plannen van aanpak op de verschillende niveaus en onderdelen in de organisatie.
> Ervoor zorgen dat beleid en plannen consistent en relevant zijn, gebaseerd op het maatstafonderdeel Oriëntatie. Streven naar verbetering van klanttevredenheid.
> Ervoor zorgen dat mensen beleid en plannen begrijpen en afspraken maken over hun bijdrage aan de realisatie daarvan.
> Ervoor zorgen dat de competenties en middelen die nodig zijn voor de realisatie van beleid en plannen beschikbaar zijn.
> De realisatie van beleid en plannen monitoren op basis van relevante gegevens en waar nodig bijsturen.

***Vernieuwing** - De leiding zorgt voor beheerste ontwikkeling en invoering van nieuwe diensten in lijn met de ambities van de organisatie*

> Een proces vaststellen voor planvorming, ontwikkeling, toetsing, invoering en onderhoud van nieuwe dienstverlening.
> Voor elke vernieuwing een plan van aanpak vastleggen. Hierin staan: de eisen waaraan de dienst moet voldoen, benodigde infrastructuur, capaciteit en competenties, beoogde resultaten, te nemen stappen, te borgen risico's, tussen- en eindevaluaties, toetsen en keuringen, gewenste interne en externe communicatie, toedeling van verantwoordelijkheden en gedocumenteerde informatie.
> Zorgen dat de vernieuwing het plan van aanpak volgt. Het plan van aanpak zo nodig bijstellen en vastleggen op basis van tussenevaluaties, eisen, resultaten, stappen en verantwoordelijkheden.
> Een verantwoordelijke aanwijzen die de nieuwe dienst beoordeelt en goedkeurt voordat deze aan de klant wordt aangeboden.
> Vastleggen van de stappen in het proces, de eisen, de resultaten, de evaluaties en de bijstellingen.
>IB Borgen van security en privacy vanaf de planvorming tot en met de invoering van de vernieuwing.

Organisatie

Inrichting *- De inrichting van de organisatie ondersteunt de koers*

> De inrichting van de organisatie afstemmen op de resultaten van het maatstafonderdeel Koers.
> Voor elke rol en functie binnen (het managementsysteem van) de organisatie vaststellen wat taken, verantwoordelijkheden en bevoegdheden zijn en welke competenties hiervoor nodig zijn.
> Doelgericht intern en extern communiceren en overleggen. Vaststellen wie waartoe wanneer waarover en hoe met wie communiceert.
>K Beheerst doorvoeren van organisatieveranderingen; ervoor zorgen dat prestaties voor klanten op kwaliteitsniveau blijven.

Managementsysteem *- De leiding richt een effectief managementsysteem in dat in lijn ligt met de koers*

>K Uit het maatstafonderdeel Oriëntatie volgen scope en processen van het managementsysteem (waaronder inputs en outputs, samenhang, volgorde, werking en reikwijdte).
>IB Uit het maatstafonderdeel Oriëntatie volgen scope en inrichting van het managementsysteem voor informatiebeveiliging.
> Uit het maatstafonderdeel Oriëntatie volgt de wijze waarop de processen ingericht, geborgd, onderhouden en verbeterd worden.
> Gedocumenteerde informatie vastleggen voor zover dat nodig is voor het bereiken van effectieve resultaten en voor zover de Maatstaf dat verplicht stelt.
> Verantwoordelijkheid van de leiding tonen voor en betrokkenheid bij de opzet, inrichting, implementatie, verbetering en effectiviteit van het managementsysteem.
> Toegang verlenen aan medewerkers tot de gedocumenteerde informatie die zij nodig hebben om hun werk goed uit te voeren.
> Passende afspraken maken voor het opstellen, goedkeuren, bijhouden, evalueren, beveiligen, distribueren, archiveren, wijzigen, verbeteren en vernietigen van gedocumenteerde informatie.

Infrastructuur *- De organisatie zorgt voor de beschikbaarheid en inzet van de benodigde middelen voor het realiseren van de koers*

> De benodigde infrastructuur vaststellen, zoals gebouwen, werkruimten, voorzieningen, informatiesystemen, leermiddelen, modellen, (meet)instrumenten en vragenlijsten.
> De benodigde werkomgeving (zowel maatschappelijk, psychologisch als fysiek) vaststellen.
>K De benodigde infrastructuur en werkomgeving beschikbaar stellen en zorgen voor inzet op de beoogde wijze.
>K Passende maatregelen nemen en vastleggen om de veiligheid, bedrijfszekerheid, juistheid, betrouwbaarheid en (toekomstige) bruikbaarheid van de infrastructuur te borgen.

Kernprocessen Kwaliteitsmanagement

***Overeenkomst** - De organisatie sluit een passende overeenkomst met haar klant(en)*

>K Beheren van relaties met (mogelijke) klanten en daarbij niet meer beloven dan waargemaakt kan worden.
>K De expliciete en impliciete eisen en wensen van klanten vaststellen, evenals andere relevante eisen zoals wet- en regelgeving.
>K Risico's voor klant(en) en eigen organisatie inschatten en afdekken.
>K De benodigde infrastructuur, capaciteit en competenties bepalen en vaststellen of deze beschikbaar zijn.
>K Voordat een overeenkomst tot stand komt: op aantoonbare wijze beoordelen of aan alle eisen en wensen van de klant en de organisatie tegemoet kan worden gekomen en, indien nodig, daar gepast naar handelen.
>K Een gedocumenteerde overeenkomst sluiten met de klant(en) met daarin voor zover relevant de doelen, activiteiten, middelen, bijdragen en eigendommen van de klant, evaluatie en klachtafhandeling.

***Uitvoering** - De organisatie zorgt voor een beheerste uitvoering op basis van de overeengekomen afspraken*

>K De benodigde infrastructuur, capaciteit en competenties inzetten om aan de eisen en wensen van de klant en andere relevante (wettelijke) eisen te kunnen voldoen.
>K Een met de klant en/of een andere relevante belanghebbende afgestemde aanpak vastleggen en volgen.
>K De voortgang en de resultaten van de uitvoering monitoren en documenteren.
>K Zorgvuldig omgaan met gegevens en andere eigendommen van klanten, borgen van de vertrouwelijkheid en vastleggen van situaties waarin de borging tekortschiet.
>K Formele documenten laten beoordelen door een verantwoordelijke of deskundige, voordat deze informatie naar belanghebbenden buiten de organisatie gestuurd wordt.
>K Periodiek afstemmen met de klant en/of een andere relevante belanghebbende over de voortgang van de uitvoering.
>K Voorkomen van klachten, kritische signalen, (on)geplande afwijkingen en incidenten in de uitvoering. Als ze zich toch voordoen: de te nemen maatregelen met de klant en andere belanghebbenden afstemmen, de maatregelen realiseren, de effectiviteit beoordelen en vastleggen.

***Afronding** - De organisatie rondt de uitvoering beheerst af en leert hiervan*

>K De uitvoering aantoonbaar beëindigen wanneer aan de overeengekomen afspraken voldaan is, of wanneer met de klant of een andere relevante belanghebbenden overeenstemming bereikt is over beëindiging.
>K Nazorg verlenen wanneer dat wettelijk vereist of afgesproken is, of als het nodig is op basis van klantsignalen of –vragen.
>K Een relevante selectie van de uitvoeringsactiviteiten intern en extern evalueren en zo nodig direct passende maatregelen nemen.
>K Kennis en ervaring die tijdens de uitvoering zijn opgedaan intern delen en deze beschikbaar stellen voor toekomstig gebruik.

Kernprocessen Informatiebeveiliging

Maatregelenselectie *- De organisatie stelt beheersmaatregelen vast die de vertrouwelijkheid, integriteit en beschikbaarheid, en eventueel andere eisen voor informatie en bedrijfsmiddelen, beschermen*

>IB Bedrijfsmiddelen classificeren op basis van een classificatieschema.

>IB Voor het beschermen van informatie passende beheersmaatregelen selecteren die consistent zijn met de classificatie van de informatie.

>IBZ Binnen gezondheidssystemen die persoonlijke gezondheidsinformatie verwerken, zorgontvangers op unieke wijze identificeren en valideren dat de uit het systeem opgevraagde gezondheidsregistratie betrekking heeft op de cliënt die wordt behandeld.

Uitvoering *- De organisatie zorgt voor een beheerste uitvoering*

>IB Opstellen en uitvoeren van gedocumenteerde procedures voor bedieningsactiviteiten die samenhangen met informatieverwerkende en communicatiefaciliteiten.

>IB Borgen van vertrouwelijkheid, integriteit en beschikbaarheid tijdens de uitvoering van processen.

>IB Beheerst uitvoeren en documenteren van wijzigingen aan informatieverwerkende systemen.

Beoordeling *- De organisatie evalueert de beheersing van de informatiebeveiliging*

>IB Met geplande tussenpozen beoordelen en evalueren van de effectiviteit van de beheersmaatregelen die de vertrouwelijkheid, integriteit en beschikbaarheid, en eventueel andere eisen voor informatie en bedrijfsmiddelen, beschermen.

Mensen

Selectie *- De organisatie kan rekenen op mensen met competenties die nodig zijn voor het realiseren van de koers*

> De benodigde capaciteit en competenties vaststellen voor het realiseren van de koers.
> Mensen met de benodigde competenties werven en selecteren, met in achtneming van hun privacy.
> Beoordelen of de kandidaten aan de eisen voldoen door het toetsen van diploma's, registraties, kennis en ervaring.
> Een passende overeenkomst afsluiten met nieuwe medewerkers.
> Relevante informatie vastleggen over achtergrond, opleiding, ervaring en beroepsregistratie van elke medewerker.

Ontwikkeling *- De organisatie faciliteert een doeltreffende ontwikkeling van haar mensen*

> Nieuwe mensen en mensen met een nieuwe rol of functie doeltreffend inwerken, ook in de opzet en werking van het managementsysteem.
> Zorgen voor voldoende middelen voor de ontwikkeling van mensen, in lijn met de ambities van de organisatie.
> De benodigde kennis vaststellen om de koers te realiseren. Mensen toegang verlenen tot deze kennis.
>K Mensen bewust maken van het belang en hun bijdrage aan het managementsysteem, van het belang van het hanteren van de zeven principes van kwaliteitsmanagement en van de gevolgen van het niet-volgen daarvan.
>IB Mensen bewust maken van het belang en hun bijdrage aan het managementsysteem voor informatiebeveiliging en van de gevolgen van het niet-volgen daarvan.
> Bewijs van competentie vastleggen en bijhouden voor elke medewerker.
> Een relevante selectie van de ontwikkelactiviteiten evalueren en zo nodig direct maatregelen nemen.

Evaluatie *- De organisatie beoordeelt de bijdrage van de mensen aan het realiseren van de koers*

> Criteria vaststellen voor de prestaties van mensen en de wijze waarop beoordeeld wordt dat zij daaraan voldoen.
> Periodiek de prestatie van mensen evalueren op basis van de afgesproken criteria en de vastgestelde werkwijze en zo nodig maatregelen nemen.
> Met vertrekkende mensen een eindgesprek houden om hieruit te leren.

Partners

Samenwerking *- De organisatie werkt samen met partners om de koers te realiseren*

> De samenwerkingsverbanden vaststellen die de organisatie aangaat, inclusief de doelen die daarmee bereikt moeten worden, de risico's die een rol spelen en de beheersing hiervan.

>K De belanghebbende klanten informeren over de rol van keten- en samenwerkingspartners.

> Doel, reikwijdte, wederzijdse inbreng, vereiste competenties, overleg en wijze van evaluatie van de samenwerking overeenkomen en vastleggen.

> De prestaties van de partners periodiek evalueren op basis van de afspraken en zo nodig maatregelen nemen.

Derden *- De organisatie zet derden in om de koers te realiseren*

> De eisen (kennis, ervaring, competenties) vaststellen die gelden voor derden in een bepaalde rol of functie en de mensen selecteren die aan die eisen voldoen.

> Doel, reikwijdte, competenties, inzet, overleg en wijze van evaluatie met de in te zetten derden overeenkomen en vastleggen.

> Voorzien in een doeltreffende introductie, ook in de relevante onderdelen van het managementsysteem.

> De prestaties van derden periodiek evalueren op basis van de afspraken en zo nodig maatregelen nemen.

Leveranciers *- De organisatie neemt diensten en producten af die bijdragen aan het realiseren van de koers*

> De eisen vaststellen waaraan leveranciers en hun producten en diensten moeten voldoen en de criteria die gelden voor (her-)selectie.

> Waar relevant overeenkomen en vastleggen van de te leveren diensten en producten en de wijze van controleren, vrijgeven en evalueren.

> Bij levering controleren of de diensten of producten aan de eisen voldoen en zo nodig direct maatregelen nemen.

> De prestaties van leveranciers periodiek evalueren op basis van de afspraken en zo nodig direct maatregelen nemen.

Resultaten

Toetsing *- De organisatie meet en verzamelt informatie over haar resultaten*

> Gegevens en evaluatie- en meetmethoden vaststellen en verzamelen die nodig zijn om de doeltreffendheid van het managementsysteem en de organisatie als geheel te kunnen beoordelen.
> Feedback van klanten, opdrachtgevers, medewerkers, partners en andere relevante belanghebbenden vaststellen en verzamelen.
> Deze gegevens en feedback vastleggen, beoordelen en zo nodig direct maatregelen nemen.
> Een interne audit met geplande tussenpozen aantoonbaar plannen, uitvoeren, rapporteren en opvolgen. Met als doel: beoordelen of het managementsysteem voldoet aan de eigen eisen en aan die van de Maatstaf.

Reflectie *- De leiding reflecteert op de resultaten van de organisatie*

>K Reflecteren op metingen, evaluaties en feedback uit de maatstafonderdelen Oriëntatie en Toetsing.
>IB Reflecteren op feedback van belanghebbenden, informatiebeveiligingsprestaties, wijzigingen in interne en externe onderwerpen, resultaten van risicobeoordeling, de status van het risicobehandelplan, de status en effectiviteit van eerder genomen maatregelen en kansen voor continue verbetering.
>K De resultaten van die reflectie gebruiken voor het evalueren van de dienstverlening, de klanttevredenheid, het managementsysteem, organisatieveranderingen, kansen en risico's, partners en de status en effectiviteit van eerder genomen maatregelen.
>IB De resultaten van die reflectie gebruiken om de continue geschiktheid en doeltreffendheid van het managementsysteem voor informatiebeveiliging te beoordelen.
> Met geplande tussenpozen en ten minste jaarlijks bovenstaande resultaten van reflectie in samenhang analyseren in een directiebeoordeling.
> Vastleggen van het resultaat van de directiebeoordeling. Het gaat om beslissingen en maatregelen ten aanzien van eventuele verbeteringen, het managementsysteem, behoefte aan middelen en de Koers.

Maatregelen *- De leiding neemt passende maatregelen zonder onnodig uitstel om de resultaten en het managementsysteem te verbeteren*

> Uitvoeren van beslissingen en maatregelen die voortkomen uit het maatstafonderdeel Reflectie, om afwijkingen te corrigeren en om de oorzaak van de afwijkingen weg te nemen.
> Verbeterkansen benutten die naar voren komen naar aanleiding van de maatstafonderdelen Oriëntatie, Toetsing en Reflectie.
> Vastleggen van de afwijkingen, de maatregelen en de resultaten van die maatregelen.

Bijlage: Begrippen

In de tekst van de Maatstaf worden begrippen gebruikt die in deze context een specifieke betekenis hebben. Deze worden hieronder wordt toegelicht.

Term	Omschrijving
Afwijkingen	(On)geplande gebeurtenissen in de uitvoering. Zoals: het niet kunnen leveren van afgesproken diensten, het optreden van menselijke fouten, incidenten of calamiteiten, wijzigingen van eisen, optreden van schade aan eigendommen van de klant, onvrede bij de klant door onvoldoende te voldoen aan de afgesproken eisen en wensen van de klant. Hier kan de organisatie op één of meer van de volgende manieren mee omgaan: • Risicoanalyse en passend herstel uitvoeren. • Onderbreken of stopzetten van de levering van de dienst. • De klant op de hoogte stellen en tot een overeenkomst komen over te nemen maatregelen (eventueel akkoord van de klant verkrijgen voor afwijkende levering). • Indien wettelijk verplicht: melden bij een toezichthoudende instantie. Eventuele maatregelen om herhaling te voorkomen zijn nodig. Daarnaast dient de organisatie bovenstaande zaken (inclusief de besluitvorming) te documenteren.
Analyseren	Informatie uit verschillende bronnen met elkaar in verband brengen en interpreteren.
Beleid	Het uitgangspunt voor doelstellingen en plannen, rekening houdend met missie en visie van de organisatie. Onder beleid wordt ook kwaliteitsbeleid verstaan. Voor beleid geldt: • Het ligt in lijn met het doel en de context van de organisatie. • Het vormt een raamwerk voor het stellen en herzien van kwaliteitsdoelstellingen. • Het bevat de toezegging om te voldoen aan alle van toepassing zijnde eisen, inclusief het voldoen aan de Maatstaf. • Het bevat de toezegging om het managementsysteem voortdurend te verbeteren.
Beoordelen	Zie Evalueren.
Communicatie faciliteiten	Alle middelen waarmee informatie gecommuniceerd kan worden. Zoals telefoon, mail, netwerken etc.
Directiebeoordeling	Onderwerpen die bij een directiebeoordeling aan de orde komen: • Follow-up vorige directiebeoordelingen. • Interne en externe onderwerpen die relevant zijn voor het managementsysteem, inclusief de strategiekoers van de organisatie. • Effectiviteit van het omgaan met risico's en kansen. • Geschiktheid, toereikendheid, doeltreffendheid van het managementsysteem, inclusief verdere verbetermogelijkheden. Trends en indicatoren die hierbij gebruikt worden: • Klachten, afwijkingen en maatregelen. • Evaluaties en meetresultaten. • Resultaten van audits. • Klanttevredenheid. • Samenwerkingspartners. • Ondersteuning voor het managementsysteem, waaronder toereikendheid van middelen. • Procesprestaties. • Voldoen van de dienstverlening aan de eisen en wensen van de klant.

Doelstelling	Voor doelstellingen geldt: • Ze zijn consistent met het beleid. • Ze zijn meetbaar of evalueerbaar. • Ze hebben betrekking op relevante eisen. • Ze zijn relevant voor het nakomen van afspraken en het verbeteren van de klanttevredenheid. • Ze worden bewaakt. • Ze worden gecommuniceerd. • Ze worden, passend bij de situatie, herzien wanneer nodig.
Evalueren	Het verzamelen, bespreken, interpreteren en presenteren van informatie om de waarde van een resultaat of proces te bepalen.
Gedocumenteerde informatie vastleggen	Het zodanig omgaan met gedocumenteerde informatie (op papier/digitaal) met als resultaat: • Elk document is identificeerbaar. • Het format en het medium zijn passend. • Elk document is beoordeeld en goedgekeurd voor vrijgave (op geschiktheid en toereikendheid). • Elk document is beschikbaar waar en wanneer nodig en geschikt voor het gebruik. • De eventuele vertrouwelijkheid is gewaarborgd. • Documentatie wordt beschermd tegen onbedoelde wijzigingen, verlies of oneigenlijk gebruik. • Er zijn afspraken voor toegang, verspreiding en gebruik. • De opslag is zodanig dat de leesbaarheid behouden blijft. • Wijzigingen vinden beheerst plaats. • Er zijn afspraken voor de bewaartermijn en vernietiging. Indien nodig voor de planning en uitvoering van het managementsysteem geldt dit ook voor informatie van externe oorsprong.
Herstel	Ervoor zorgen dat de effecten van een afwijking teniet gedaan worden, zodat alsnog aan de eisen en wensen van de klant voldaan kan worden. Indien de effecten niet teniet gedaan kunnen worden, wordt adequate compensatie afgesproken en doorgevoerd.
Infrastructuur	Voorbeelden van infrastructuur (incl. werkomgeving): • Gebouwen. • Werkruimten. • Voorzieningen. • Informatiesystemen en programmatuur. • Leermiddelen. • Modellen. • Instrumenten, meetinstrumenten, apparatuur. • Vragenlijsten. Het gaat hierbij om middelen voor de dienstverlening als om middelen voor het inrichten, implementeren, onderhouden en het continu verbeteren van het managementsysteem. Hierbij dient de organisatie na te denken over de volgende punten: • Mogelijkheden en beperkingen van interne middelen. • Wat er verkregen moet worden van externe aanbieders. • Hoe middelen onderhouden moeten worden om blijvend beschikbaar te zijn voor hun doel. • Bescherming tegen oneigenlijk gebruik of gegevensverlies.

IT Infrastructuur	Verbijzondering van "infrastructuur" m.b.t. informatiesystemen. Onder de IT Infrastructuur wordt alle hardware en software gerekend, waaronder applicaties.
Interne audit	Interne toetsing om te beoordelen of het managementsysteem effectief is en aan de eisen van de Maatstaf voldoet. Het interne auditprogramma wordt afgestemd op: • Doelstellingen. • Het belang van de te onderzoeken processen. • Feedback van klanten. • Veranderingen van invloed op de organisatie. • Resultaten van vorige audits. Het meerjarenprogramma interne audit bevat de volgende onderdelen: • Frequentie, methode(n), verantwoordelijkheden. • Wijze van plannen en rapporteren. • Voor elke audit: scope/reikwijdte en criteria. • Voor elke audit: objectieve en onpartijdige auditor(s). De organisatie zorgt voor rapportage aan het verantwoordelijke management die moet besluiten over opvolging. Het management voert eventuele maatregelen door en beoordeelt deze op effectiviteit. ISO 19011 bevat richtlijnen voor interne audits.
Kennis	Alle kennis en ervaring die nodig is om de organisatiedoelen te bereiken. Kennisbronnen zijn zowel intern (basiskennis van medewerkers, leren van evaluaties, overdracht van kennis 'on the job') als extern (normen, congressen, enquêtes, methoden, technieken).
Klant	Degene met wie de organisatie impliciete en expliciete afspraken maakt voor de levering van een dienst. De klant kan tegelijk opdrachtgever en ontvanger van de dienst zijn alsmede betaler van de dienst. Dit kunnen echter ook verschillende partijen of personen zijn.
Klant centraal	De leiding stelt de klant centraal: • Aan klantenwensen en –eisen en geldende wet- en regelgeving wordt voldaan. • De risico's en kansen die invloed hebben op de dienstverlening en de klanttevredenheid zijn vastgesteld en passende maatregelen worden genomen. • De nadruk ligt op het verstrekken van een consistente dienstverlening. • De nadruk ligt op het verhogen van de klanttevredenheid.
Klanttevredenheid	Het gaat om de perceptie van klanten in hoeverre aan hun eisen en wensen voldaan is. De organisatie verzamelt informatie daarover. Voorbeelden: enquêtes, marktaandeelanalyses, complimenten, claims en evaluatiegesprekken.
Leiding	Topmanagement van de organisatie waarop het managementsysteem betrekking heeft.
Maatregelen	Acties om herhaling van een bepaalde afwijking of klacht te voorkomen: • Beoordelen van de afwijking of klacht. • Vaststellen van de oorzaak van de afwijking of klacht. • Vaststellen of de afwijking of klacht vaker voorgekomen is of voor zou kunnen komen. • Maatregelen nemen (die mede de geschiktheid, toereikendheid en doeltreffendheid van het managementsysteem verbeteren). • Evalueren van de effectiviteit van de maatregelen. • Aanpassen van het managementsysteem (inclusief eerder gesignaleerde risico's en kansen), waar nodig.

Managementsysteem	Het managementsysteem regelt het goed verloop van de processen van de organisatie: • Noodzakelijke inputs en verwachte outputs. • Volgorde en interactie. • Hoe zij effectief verlopen, inclusief de criteria, methoden, metingen en evaluaties die daarvoor nodig zijn. • Noodzakelijke ondersteuning en middelen. • Verantwoordelijkheden en bevoegdheden die met het proces samenhangen. • Risico's en kansen die met het proces samenhangen inclusief de maatregelen hoe daarmee om te gaan. • Wijze van bewaking, meting, evaluatie en waar nodig verandering, zodat elk proces het beoogde resultaat heeft. • Geïdentificeerde verbetermogelijkheden.
Mensen	Alle medewerkers die een bijdrage leveren aan het bereiken van de doelen van de organisatie en die binnen het managementsysteem vallen. Dit zijn in principe mensen met een tijdelijke of vaste arbeidsovereenkomst. Wanneer het om ingehuurde zzp'ers, onderaannemers, freelancers, gedetacheerden, stagiaires of vrijwilligers gaat, spreken we van 'derden'. Dit valt dan onder de rubriek Partners.
Meten	Vaststellen hoe de organisatie scoort op een bepaalde prestatie-indicator, bij voorbeeld de effectiviteit van een bepaalde aanpak of behandeling, verloop of verzuim van medewerkers, de mate waarin de organisatie tevreden is over de bijdrage van samenwerkingspartners.
Missie	Formulering van het bestaansrecht en de identiteit van een organisatie.
Monitoren	Het waarnemen en verzamelen van informatie over iets, gedurende langere tijd teneinde te evalueren.
Omgeving	Relevante omgevingsfactoren: • Fysieke factoren. • Sociale factoren. • Psychologische factoren. • Milieufactoren. • Economische factoren. • Juridische factoren, zoals wet- en regelgeving.
Organisatie-verandering	Organisatieveranderingen (inclusief wijzigingen in het managementsysteem) dienen op geplande wijze te worden uitgevoerd. De organisatie neemt adequate besluiten over de volgende zaken: • Doel van de veranderingen, mogelijke gevolgen en bepaling van de effectiviteit van de verandering. • Eenheid en samenhang van (het managementsysteem van) de organisatie. • Beschikbaarheid van mensen en middelen. • Eventuele wijzigingen in verantwoordelijkheden en bevoegdheden.
Plan (van aanpak)	Wanneer gepland wordt hoe doelstellingen gerealiseerd gaan worden, stelt de organisatie vast: • Wat wordt gedaan? • Welke inzet is nodig? • Wie is verantwoordelijk? • Wanneer moet het af zijn? • Hoe wordt het resultaat geëvalueerd?
Plan voor vernieuwing	Plan dat voorziet in meetbare doelen, gespecificeerde eisen, planning, begroting van de inzet, vastgelegde tussentijdse en eindbeoordelingen inclusief beslismomenten en per fase heldere verantwoordelijkheden en bevoegdheden.
Reflecteren	Nadenken over een bepaald gegeven (handeling, gedachte, prestatie) om er iets uit te leren voor verbetering in de toekomst.

Verantwoordelijkheid van de leiding voor het managementsysteem	De leiding laat haar verantwoordelijkheid voor en betrokkenheid bij het managementsysteem op de volgende manieren zien: • De leiding is aanspreekbaar op de effectiviteit van het managementsysteem. • De leiding zorgt ervoor dat kwaliteitsbeleid en -doelstellingen zijn vastgesteld en in lijn liggen met de strategische richting en context van de organisatie. • De leiding zorgt ervoor dat het kwaliteitsbeleid gecommuniceerd wordt, bekend is en begrepen wordt in de organisatie. • De leiding zorgt ervoor dat het managementsysteem geïntegreerd is in de bedrijfsprocessen. • De leiding vergroot het bewustzijn van de procesaanpak. • De leiding stelt de nodige ondersteuning voor het managementsysteem beschikbaar. • De leiding benadrukt het belang van effectief kwaliteitsmanagement en het volgen van het managementsysteem. • De leiding zorgt ervoor dat het managementsysteem de beoogde resultaten oplevert en dat zij daarover gerapporteerd krijgt. • De leiding zet mensen in en leidt ze en ondersteunt ze om bij te dragen aan de effectiviteit van het managementsysteem. • De leiding streeft continue verbetering na. • De leiding ondersteunt alle relevante managementrollen.
Verbetermogelijkheden	Wanneer verbetermogelijkheden aan de orde zijn, wordt hierop gedoeld: • Het verbeteren van processen, zodat afwijkingen worden voorkomen. • Het verbeteren van dienstverlening, zodat aan (toekomstige) eisen wordt voldaan. • Het verbeteren van de resultaten van het managementsysteem. De realisatie van verbetering gebeurt bijvoorbeeld door te reageren op afwijkingen, stapsgewijs zoals in continue verbetering, via innovatie of door reorganisatie.
Vernieuwing	Vernieuwing is aan de orde wanneer dienstverlening gevraagd wordt of op voorhand door de organisatie ontwikkeld wordt waarvoor nog geen afgesproken klantspecificaties beschikbaar zijn. Voor het proces van vernieuwing voor een kennisintensieve dienstverlener kan gekozen worden voor de specifieke aandachtspunten uit Koers - Vernieuwing (aan de orde bij geheel nieuwe vormen van dienstverlening) of uit Kernproces - Uitvoering (aan de orde bij maatwerk volgens een vast stramien). Vernieuwing in de CIIO Maatstaf is wat de ISO 9001 norm 'Ontwerp en Ontwikkeling' noemt. De ISO 9001 norm noemt een aantal fasen in het ontwerpproces die goed traceerbaar zijn bij het ontwerp van tastbare producten. Ze zijn echter niet altijd een-op-een over te zetten naar de ontwikkeling van een dienst, zoals een bepaalde methode van adviseren of opleiden. De ISO 9001 norm maakt onderscheid tussen: 1) Planning van ontwerp en ontwikkeling (het bepalen van de ontwikkelingsstappen met bijbehorende verantwoordelijkheden, benodigdheden, interactie en het bepalen van de wijze waarop elke ontwikkelingsstap wordt beoordeeld, geverifieerd en geldig verklaard). 2) Inputs voor ontwerp en ontwikkeling (aan welke functionele en prestatie eisen en wet- en regelgeving, normen en gedragscodes voldaan moet worden, welke informatie van vergelijkbare activiteiten gebruikt kan worden). De input moet beoordeeld worden voordat hij wordt gebruikt en de eisen mogen niet strijdig zijn met elkaar. 3) Beheersmaatregelen voor ontwerp en ontwikkeling (definiëren van te behalen resultaten, beoordelingen uitvoeren om te evalueren of de resultaten kunnen voldoen aan de inputeisen, feitelijk verifiëren of de resultaten voldoen aan de inputeisen, valideren of de resultaten voldoen

	aan de gewenste toepassing/beoogde gebruik, eventueel te nemen maatregelen om aangetroffen problemen op te lossen). 4) Output van ontwerp en ontwikkeling (de output moet voldoen aan de inputeisen, moet toereikend zijn voor aansluitende processen van dienstverlening, moet criteria voor monitoring, meten en acceptatie bevatten en kenmerken specificeren die essentieel zijn voor een juist en veilig gebruik voor het beoogde doel). 5) Beheersing van wijzigingen in ontwerp en ontwikkeling (wijzigingen moeten worden geïdentificeerd, beoordeeld, vastgesteld en beheerst en eventuele maatregelen moeten worden genomen om nadelige effecten op het voldoen aan de eisen te voorkomen). Gedocumenteerde informatie is op al deze aspecten vereist.
Verwerken	Alle handelingen die een organisatie kan uitvoeren met informatie, van verzamelen tot en met vernietigen.
Visie	Het toekomstig en ambitieus beeld van wat een organisatie wil zijn.
Waarden en cultuur	De gemeenschappelijke normen binnen de organisatie, geschreven en ongeschreven, die richting geven aan houding en gedrag van de leden van de organisatie. Dit kan vastgelegd zijn in een gedragscode.

Bijlage 9001: Gedocumenteerde informatie

Volgens de ISO 9001 norm is het verplicht om 'gedocumenteerde informatie' beschikbaar te hebben en deze een passende (of wettelijk vastgelegde) periode te bewaren. Hiervoor wordt in de Maatstaf-eisen de term 'vastleggen' gebruikt. Het gaat zowel om beschrijvingen van hoe iets tot stand zou moeten komen, als om bewijs dat een bepaald proces gevolgd is of dat een bepaald resultaat gehaald is. Samenvattend volgt hieronder een overzicht van aspecten waarvoor dit geldt, met een verwijzing naar het Maatstaf-onderdeel en de ISO 9001:2015-clausule.

Maatstafonderdeel	Onderwerp en relevante ISO 9001:2015 clausule	Gedocumenteerde informatie over
Koers - Leiderschap	5.2 Beleid	Beleid, beschikbaar voor alle relevante stakeholders.
Koers - Leiderschap	6.2.1 Doelstellingen	Doelstellingen, beschikbaar voor relevante functies, niveaus en processen.
Koers - Vernieuwing	8.3.2 Planning van vernieuwing	Beheersing (zoals eisen, stappen, middelen en toetsingen) van het vernieuwingsproces.
Koers - Vernieuwing	8.3.3 Inputs voor vernieuwing	Inputs in het vernieuwingsproces.
Koers - Vernieuwing	8.3.4 Bewijs dat voldaan is aan ontwerpeisen	Checks/goedkeuring (door de organisatie zelf dan wel de klant) dat voldaan is aan de eisen.
Koers - Vernieuwing	8.3.5 Outputs van vernieuwing	Outputs (resultaten) van het vernieuwingsproces.
Koers – Vernieuwing	8.3.6 Wijzigingen in vernieuwing	Bijstellingen van het plan op basis van tussentijdse evaluaties, toetsing en/of tests; deze aanpassingen vinden beheerst plaats en worden vastgelegd.
Organisatie – Managementsysteem	4.4.2/8.1.e/8.5.1 Informatie over processen	Documentatie voor zover nodig om ervoor te zorgen dat processen uitgevoerd worden zoals gepland en waarmee de organisatie kan aantonen dat zij uitgevoerd zijn als gepland.
Organisatie – Managementsysteem	4.3 Toepassingsgebied van het managementsysteem	Toepassingsgebied, begrenzing en reikwijdte van het managementsysteem (ook wel scope).
Organisatie - Managementsysteem	7.5.1 Managementsysteem documentatie	Dat wat moet volgens de Maatstaf en wat nodig is volgens de organisatie.
Organisatie - Infrastructuur	7.1.3 Infrastructuur 7.1.4 Omgeving voor uitvoering van processen 7.1.5 Middelen voor monitoring en meting	Passend bewijs van geschiktheid voor het doel van monitoring- en meetmiddelen.
Kernprocessen - Overeenkomst	8.2.3.2 Beoordeling van eisen en wensen van de klant	Beoordeling of de organisatie kan voldoen aan de eisen en wensen van de klant, inclusief wet- en regelgeving, nieuwe eisen aan diensten en de zaken die de organisatie zelf belangrijk vindt.
Kernprocessen - Uitvoering	8.5.1 Beheersing van de uitvoering 8.5.2 Identificatie en naspeurbaarheid	Dienstverlening, uit te voeren activiteiten, te behalen en behaalde resultaten.
Kernprocessen - Uitvoering	8.5.3 Eigendom van klanten of partners	Wat zich heeft voorgedaan wanneer er iets is gebeurd met eigendommen van klanten of partners.

Maatstafonderdeel	Onderwerp en relevante ISO 9001:2015 clausule	Gedocumenteerde informatie over
Kernprocessen - Uitvoering	8.5.6 Beoordeling van wijzigingen in de uitvoering	Beoordelen van onvoorziene wijzigingen in de dienstverlening, vastleggen van de uitkomst van deze beoordeling, actie ondernemen om ervoor te zorgen dat het eindresultaat aan de eisen blijft voldoen.
Kernprocessen - Uitvoering	8.7.2 Afwijkingen en klachten	Afwijkingen en klachten, de maatregelen die genomen zijn (inclusief de verantwoordelijken en/of de acceptatie van de afwijking door de klant) en de resultaten die met de maatregelen geboekt zijn.
Kernprocessen – Afronding	8.6 Vrijgave van producten en diensten	Beëindigen van de dienstverlening, op basis van wat er afgesproken is en wie toestemming heeft gegeven voor beëindiging.
Mensen - Selectie	7.2d Competenties	Achtergrond, opleiding, ontwikkeling, ervaring en beroepsregistratie van elke medewerker.
Mensen - Ontwikkeling	7.2d Competenties	Passend bewijs van competenties van mensen.
Partners	8.4.1 Beheersing van extern geleverde processen, producten en diensten	Resultaten van evaluaties en (her)beoordeling van de prestatie van partners en de maatregelen die daaruit volgen.
Resultaten – Toetsing	9.1.1 Evaluaties en metingen	Resultaten van evaluaties en metingen en op grond hiervan genomen maatregelen.
Resultaten - Toetsing	9.2.2 Intern auditprogramma	Implementatie van het auditprogramma en de resultaten ervan (zie ISO 19011 voor richtlijnen).
Resultaten - Reflectie	9.3.3 Directiebeoordeling	Resultaten van de directiebeoordeling.
Resultaten – Maatregelen	10.2.2 Maatregelen	Afwijkingen, genomen maatregelen en resultaten van die afwijkingen.

Bijlage 9001: ISO 9001:2015 versus Maatstaf Combi 2020

ISO 9001:2015	CIIO Maatstaf Combi 2020
4 Context van de organisatie	
4.1 Inzicht in de organisatie en haar context	Koers - Oriëntatie
4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden	Koers - Oriëntatie
4.3 Het toepassingsgebied van het kwaliteitsmanagementsysteem vaststellen	Organisatie - Managementsysteem
4.4 Kwaliteitsmanagementsysteem en de processen ervan	Organisatie - Managementsysteem
4.4.1 Kwaliteitsmanagementsysteem	Organisatie - Managementsysteem
4.4.2 Gedocumenteerde informatie	Organisatie - Managementsysteem
5 Leiderschap	
5.1 Leiderschap en betrokkenheid	Koers - Leiderschap Organisatie - Managementsysteem
5.1.1 Leiderschap en betrokkenheid algemeen	Koers – Leiderschap Organisatie – Managementsysteem Mensen - Ontwikkeling
5.1.2 Klantgerichtheid	Koers - Oriëntatie
5.2 Beleid	Koers - Leiderschap
5.2.1 Het kwaliteitsbeleid vaststellen	Koers - Leiderschap
5.2.2 Het kwaliteitsbeleid kenbaar maken	Koers - Leiderschap
5.3 Rollen, verantwoordelijkheden en bevoegdheden	Koers - Leiderschap Organisatie - Inrichting
6 Planning	
6.1.1 Plannen van het kwaliteitssysteem	Koers – Oriëntatie Organisatie – Managementsysteem
6.1.2 Plannen van het kwaliteitssysteem	Koers - Oriëntatie
6.2.1 Kwaliteitsdoelstellingen	Koers - Leiderschap
6.2.2 Bij het plannen vast te stellen	Koers - Leiderschap
6.3 Planning van wijzigingen	Organisatie - Inrichting
7 Ondersteuning	
7.1 Middelen	Koers - Leiderschap
7.1.1 Algemeen	Koers – Leiderschap Organisatie – Infrastructuur Partners
7.1.2 Personeel	Mensen - Selectie
7.1.3 Infrastructuur	Organisatie - Infrastructuur
7.1.4 Omgeving voor de uitvoering van processen	Organisatie - Infrastructuur
7.1.5 Middelen voor monitoring en meten	
7.1.5.1 Algemeen	Organisatie - Infrastructuur
7.1.5.2 Naspeurbaarheid	Organisatie – Infrastructuur
7.1.6 Kennis binnen de organisatie	Kernprocessen – Afronding Mensen – Ontwikkeling
7.2 Competenties	Mensen – Ontwikkeling Mensen - Evaluatie
7.3 Bewustzijn	Koers – Leiderschap Mensen – Ontwikkeling
7.4 Communicatie	Organisatie – Inrichting
7.5 Gedocumenteerde informatie	Organisatie – Managementsysteem
7.5.1 Gedocumenteerde informatie algemeen	Organisatie – Managementsysteem
7.5.2 Creëren en actualiseren	Organisatie – Managementsysteem
7.5.3 Beheersing van gedocumenteerde informatie	

ISO 9001:2015	CIIO Maatstaf Combi 2020
7.5.3.1 Beschikbaarheid en beveiliging van gedocumenteerde informatie	Organisatie – Managementsysteem
7.5.3.2 Activiteiten voor de beheersing van gedocumenteerde informatie	Organisatie – Managementsysteem
8 Uitvoering	
8.1 Operationele planning en beheersing	Kernprocessen – Uitvoering Koers – Oriëntatie Koers – Leiderschap Organisatie – Managementsysteem Organisatie - Infrastructuur
8.2 Eisen voor producten en diensten	Kernprocessen - Uitvoering
8.2.1 Communicatie met de klant	Kernprocessen - Overeenkomst
8.2.2 Het vaststellen van de eisen voor producten en diensten	Kernprocessen - Overeenkomst
8.2.3 Beoordeling van de eisen voor producten en diensten	Kernprocessen - Overeenkomst
8.2.3.1 Vermogen om te voldoen aan de eisen	Kernprocessen - Overeenkomst
8.2.3.2 Gedocumenteerde informatie	Kernprocessen – Overeenkomst
8.2.4 Wijzigingen in de eisen voor producten en diensten	Kernprocessen – Overeenkomst
8.3 Ontwerp en ontwikkeling van producten en diensten	Koers – Vernieuwing
8.3.1 Algemeen	Koers – Vernieuwing
8.3.2 Planning van ontwerp en ontwikkeling	Koers – Vernieuwing
8.3.3 Inputs voor ontwerp en ontwikkeling	Koers – Vernieuwing
8.3.4 Beheersmaatregelen voor ontwerp en ontwikkeling	Koers – Vernieuwing
8.3.5 Ontwerp en ontwikkelingsoutputs	Koers – Vernieuwing
8.3.6 Wijzigingen met betrekking tot ontwerp en ontwikkeling	Koers – Vernieuwing
8.4 Beheersing van extern geleverde processen, producten en diensten	Partners – Samenwerking Partners – Derden Partners – Leveranciers
8.4.1 Algemeen	Partners – Samenwerking Partners – Derden Partners – Leveranciers
8.4.2 Soort en mate van beheersing	Partners – Samenwerking Partners – Derden Partners – Leveranciers
8.4.3 Informatie voor externe aanbieders	Partners – Samenwerking Partners – Derden Partners – Leveranciers
8.5 Productie en het leveren van diensten	Kernprocessen – Uitvoering
8.5.1 Beheersing van productie en het leveren van diensten	Kernprocessen – Uitvoering Kernprocessen – Afronding
8.5.2 Identificatie en naspeurbaarheid	Kernprocessen – Uitvoering
8.5.3 Eigendom van klanten / externe aanbieders	Kernprocessen – Uitvoering
8.5.4 In stand houden	Kernprocessen – Uitvoering
8.5.5 Nazorgactiviteiten	Kernprocessen – Afronding
8.6 Vrijgave van producten en diensten	Kernprocessen – Uitvoering
8.7 Beheersing van afwijkende outputs	Kernprocessen – Uitvoering
8.7.1 Outputs die niet voldoen	Kernprocessen – Uitvoering
8.7.2 Afwijkingen	Kernprocessen – Uitvoering
9 Evaluatie van de prestaties	
9.1 Monitoren, meten, analyseren en evalueren	Kernprocessen – Uitvoering

ISO 9001:2015	CIIO Maatstaf Combi 2020
	Kernprocessen – Afronding Mensen – Ontwikkeling Mensen – Evaluatie Partners – Samenwerking Partners – Derden Partners – Leveranciers Resultaten – Toetsing
9.1.1 Algemeen	Resultaten – Toetsing
9.1.2 Klanttevredenheid	Resultaten – Toetsing
9.1.3 Analyse en evaluatie	Resultaten – Reflectie
9.2 Interne audit	Resultaten - Toetsing
9.2.1 Interne audits plannen en houden	Resultaten – Toetsing
9.2.1 Interne audits uitvoeren	Resultaten – Toetsing
9.3 Directiebeoordeling	Resultaten - Reflectie
9.3.1 Algemeen	Resultaten - Reflectie
9.3.2 Inputs voor directiebeoordeling	Resultaten - Reflectie
9.3.3 Outputs van directiebeoordeling	Resultaten - Maatregelen
10 Verbetering	
10.1 Algemeen	Resultaten - Maatregelen
10.2 Afwijkingen en corrigerende maatregelen	Resultaten - Maatregelen
10.2.1 Werkwijze in geval van afwijkingen	Resultaten - Maatregelen
10.2.2 Documentatie van bewijsvoering m.b.t. afwijkingen	Resultaten - Maatregelen
10.3 Continue verbetering	Resultaten - Maatregelen

Bijlage 9001: Maatstaf Combi 2020 versus ISO 9001:2015

CIIO Maatstaf Combi 2020	ISO 9001:2015
Koers - Oriëntatie	
Omgevingsanalyse	4.1 Inzicht in de organisatie en haar context
Belanghebbendenanalyse	4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden
Dienstenaanbod	4.3.c Vaststellen van de producten en diensten van de organisatie
Wet- en regelgeving	4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden 5.1.2 Klantgerichtheid
Kansen- en risicoanalyse	6.1 Acties om kansen en risico's op te pakken
Koers - Leiderschap	
Visie, missie, strategie formuleren/communiceren	5.1 Leiderschap en betrokkenheid
Beleid, doelstellingen en plannen	5.2 Beleid 6.2 Kwaliteitsdoelstellingen en de planning om ze te bereiken
Criteria beleid en plannen	5.2.1 Het kwaliteitsbeleid vaststellen 6.2.1 Kwaliteitsdoelstellingen
Draagvlak voor en afspraken over beleid en plannen	5.1 Leiderschap en betrokkenheid 7.3 Bewustzijn
Benodigde competenties en middelen	5.1 Leiderschap en betrokkenheid 5.3 Rollen, verantwoordelijkheden en bevoegdheden 7.1 Middelen
Aansturen en bijsturen	5.1.1 Leiderschap en betrokkenheid algemeen
Koers - Vernieuwing	
Het proces van vernieuwing	8.3 Ontwerp en ontwikkeling van producten en diensten
Plan van aanpak	8.3.4 Beheersmaatregelen voor ontwerp en ontwikkeling
Uitvoeren plan van aanpak	8.3.4/6 Beheersmaatregelen voor ontwerp en ontwikkeling
Vrijgave na toets	8.3.4 Beheersmaatregelen voor ontwerp en ontwikkeling
Aantoonbare processtappen	8.3.5 Ontwerp en ontwikkelingsoutputs
Organisatie - Inrichting	
Inrichting afgestemd op koers	5.3 Rollen, verantwoordelijkheden en bevoegdheden
Rollen en competenties duidelijk	5.3 Rollen, verantwoordelijkheden en bevoegdheden
Overleg en communicatie	7.4 Communicatie
Organisatieveranderingen beheerst	6.3 Planning van wijzigingen
Organisatie - Managementsysteem	
Processen en scope vaststellen	4.3 Het toepassingsgebied van het kwaliteitsmanagementsysteem vaststellen 4.4 Kwaliteitsmanagementsysteem en de processen ervan
Borging laten aansluiten op Oriëntatie	4.4 Kwaliteitsmanagementsysteem en de processen ervan
Noodzakelijke gedocumenteerde informatie	4.4.2 Gedocumenteerde informatie 7.5.1 Gedocumenteerde informatie algemeen
Verantwoordelijkheid van de leiding	5.1 Leiderschap en betrokkenheid

CIIO Maatstaf Combi 2020	ISO 9001:2015
Informatie is beschikbaar	7.5.3 Beheersing van gedocumenteerde informatie
Onderhoud gedocumenteerde informatie	7.5.2 Creëren en actualiseren
Organisatie - Infrastructuur	
Infrastructuur vaststellen	7.1.3 Infrastructuur 7.1.5 Middelen voor monitoring en meten
Werkomgeving vaststellen	7.1.4 Omgeving voor de uitvoering van processen
Gebruik van de infrastructuur en werkomgeving zoals beoogd	7.1.3 Infrastructuur 7.1.4 Omgeving voor de uitvoering van processen 7.1.5 Middelen voor monitoring en meten
Bedrijfszekerheid infrastructuur	7.1.3 Infrastructuur 7.1.4 Omgeving voor de uitvoering van processen 7.1.5 Middelen voor monitoring en meten
Kernprocessen - Overeenkomst	
Communicatie met (mogelijke) klanten	8.2.1 Communicatie met de klant
Klanteisen inventariseren	8.2.2 Het vaststellen van de eisen voor producten en diensten
Risico's inschatten	8.2.2 Het vaststellen van de eisen voor producten en diensten
Benodigde competenties/capaciteit bepalen	8.2.2 Het vaststellen van de eisen voor producten en diensten
Contractreview/4 ogen principe/Aanbod/Check	8.2.3 Beoordeling van de eisen voor producten en diensten
Gedocumenteerde overeenkomst	8.2.4 Wijzigingen in de eisen voor producten en diensten
Kernprocessen - Uitvoering	
Resultaatverantwoordelijke en team	8.1 Operationele planning en beheersing
Plan van aanpak	8.1 Operationele planning en beheersing 8.5.1 Beheersing van productie en het leveren van diensten
Gedocumenteerde verantwoording	8.5.1 Beheersing van productie en het leveren van diensten 8.5.2 Identificatie en naspeurbaarheid
Vertrouwelijkheid	8.5.3 Eigendom van klanten of externe aanbieders
Vier ogen principe	8.6 Vrijgave van producten en diensten
Voortgang en bijsturing inclusief klantcontact	8.5.1 Beheersing van productie en het leveren van diensten 9.1 Monitoren, meten, analyseren en evalueren
Afwijkingen, inclusief klachten en klantsignalen	8.7 Beheersing van afwijkende outputs
Kernprocessen - Afronding	
Overeenkomst beëindigen	8.5.1 Beheersing van productie en het leveren van diensten
Nazorg	8.5.5 Nazorgactiviteiten
Evaluatie intern en extern	9.1 Monitoren, meten, analyseren en evalueren
Ontsluiten van opdrachtervaringen	7.1.6 Kennis binnen de organisatie
Mensen - Selectie	
Competentie/capaciteit behoefte vaststellen	7.1.2 Personeel
Zorgvuldig werven en selecteren	7.1.2 Personeel
Kandidaten verifiëren	7.1.2 Personeel
Overeenkomst met mensen	7.1.2 Personeel
P-dossier	7.1.2 Personeel
Mensen - Ontwikkeling	
Doeltreffende introductie	7.2 Competenties
Ontwikkelingsbeleid en -afspraken	7.2 Competenties

CIIO Maatstaf Combi 2020	ISO 9001:2015
Kennismanagement	7.1.6 Kennis binnen de organisatie
Bewijs van competenties	7.2 Competenties
Bewustzijn bewerkstelligen	7.3 Bewustzijn
Evaluatie ontwikkelactiviteiten	9.1 Monitoren, meten, analyseren en evalueren
Mensen - Evaluatie	
Prestatie-eisen vaststellen	7.2 Competenties
Evaluatie medewerkers	9.1 Monitoren, meten, analyseren en evalueren
Exitgesprekken/Eindgesprekken	9.1 Monitoren, meten, analyseren en evalueren
Partners - Samenwerking	
Samenwerkingsverbanden	8.4 Beheersing van extern geleverde processen, producten en diensten
Klanten informeren over partners	8.4 Beheersing van extern geleverde processen, producten en diensten
Gedocumenteerde afspraken	8.4.2 Soort en mate van beheersing
Evaluatie samenwerking	8.4.3 Informatie voor externe aanbieders 9.1 Monitoren, meten, analyseren en evalueren
Partners - Derden	
Selecteren van/eisen aan in te zetten derden	8.4 Beheersing van extern geleverde processen, producten en diensten
Gedocumenteerde afspraken	8.4.2 Soort en mate van beheersing
Inwerken van derden	8.4.2 Soort en mate van beheersing
Evaluatie derden	8.4.3 Informatie voor externe aanbieders 9.1 Monitoren, meten, analyseren en evalueren
Partners - Leveranciers	
Selecteren van/eisen aan leveranciers	8.4 Beheersing van extern geleverde processen, producten en diensten
Gedocumenteerde afspraken	8.4.2 Soort en mate van beheersing
Controle producten en diensten	8.4.2 Soort en mate van beheersing
Evaluatie leveranciers	8.4.3 Informatie voor externe aanbieders 9.1 Monitoren, meten, analyseren en evalueren
Resultaten - Toetsing	
(Geaggregeerde) resultaten van evaluaties vaststellen en verzamelen	9.1 Monitoren, meten, analyseren en evalueren
Feedback van belanghebbenden verzamelen	4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden
Vastleggen, rapporteren, maatregelen nemen	9.1 Monitoren, meten, analyseren en evalueren
Interne audit plannen en uitvoeren	9.2 Interne audit
Resultaten - Reflectie	
Reflectie op toetsing	9.1.3 Analyse en evaluatie
Resultaten van reflectie voor evaluatie	9.1.3 Analyse en evaluatie
Directiebeoordeling	9.3 Directiebeoordeling
Resultaat van de directiebeoordeling	9.3.3 Outputs van directiebeoordeling
Resultaten - Maatregelen	
Maatregelen vanuit Reflectie	9.3.3 Outputs van directiebeoordeling
Verbeterkansen benutten	10 Verbetering
Vastleggen maatregelen	10.2.2 Maatregelen

Bijlage ISO 27001/ NEN 7510: Gedocumenteerde informatie

Volgens de ISO 27001 norm is het verplicht om 'gedocumenteerde informatie' beschikbaar te hebben en deze een passende (of wettelijk vastgelegde) periode te bewaren. Hiervoor wordt in de Maatstaf-eisen de term 'vastleggen' gebruikt. Het gaat zowel om beschrijvingen van hoe iets tot stand zou moeten komen, als om bewijs dat een bepaald proces gevolgd is of dat een bepaald resultaat gehaald is. Samenvattend volgt hieronder een overzicht van aspecten waarvoor dit geldt, met een verwijzing naar het Maatstaf-onderdeel en de ISO 27001:2013-clausule.

CIIO Maatstaf Combi 2020	Onderwerp en relevante ISO 27001:2013 clausule	Gedocumenteerde informatie over
Koers - Oriëntatie	4 De organisatie heeft externe en interne onderwerpen vastgesteld die relevant zijn voor haar doelstelling en die haar vermogen beïnvloeden om het (de) beoogde resulta(a)t(en) van haar managementsysteem voor informatiebeveiliging te behalen.	Context- en stakeholderanalyse
Organisatie - Managementsysteem	4.3 Het toepassingsgebied (van het managementsysteem voor informatiebeveiliging) is als gedocumenteerde informatie beschikbaar.	Toepassingsgebied/ scope informatiebeveiligingssysteem
Koers - Leiderschap	5.2 De directie heeft een informatiebeveiligingsbeleid vastgesteld.	Beleid, beschikbaar voor alle relevante stakeholders.
Koers - Oriëntatie	6.1.2 De organisatie heeft een risicobeoordelingsprocedure voor informatiebeveiliging definiëren	Risicobeoordelingsproces
Koers - Oriëntatie	6.1.3 De organisatie moet een behandelprocedure voor informatiebeveiligingsrisico's definiëren	Procedure voor het behandelen van risico's.
Koers - Oriëntatie	6.1.3 De organisatie heeft een verklaring van toepasselijkheid die de benodigde beheersmaatregelen bevat (zie 6.1.3 b) en c)): een rechtvaardiging voor het opnemen ervan, de informatie of ze zijn geïmplementeerd of niet, en de rechtvaardiging om beheersmaatregelen van bijlage A uit te sluiten;	Verklaring van toepasselijkheid
Koers - Leiderschap	6.2 De organisatie bewaart gedocumenteerde informatie over de informatiebeveiligingsdoel-stellingen.	Informatiebeveiligingsdoelstellingen
Mensen - Ontwikkeling	7.2 De organisatie moet geschikte gedocumenteerde informatie als bewijsmateriaal van competentie bewaren	Bewijs van competenties

CIIO Maatstaf Combi 2020	Onderwerp en relevante ISO 27001:2013 clausule	Gedocumenteerde informatie over
Organisatie - Managementsysteem	7.5.1 Informatie die de organisatie zelf vaststelt als noodzakelijk	Verschillend per organisatie
Koers – Oriëntatie	8.1 De organisatie houdt gedocumenteerde informatie bij in de omvang die nodig is om het vertrouwen te hebben dat de processen volgens planning zijn uitgevoerd.	Planning en voortgang op de uitvoering van het risicobehandelplan en het evalueren van de (rest)risico's
Koers – Oriëntatie	8.2 De organisatie bewaart gedocumenteerde informatie van de resultaten van de risicobeoordelingen van informatiebeveiliging.	Zie 8.1
Koers – Oriëntatie	8.3 De organisatie bewaart gedocumenteerde informatie bewaren van de resultaten van het behandelen van informatiebeveiligingsrisico's.	Zie 8.1
Resultaten - Toetsing	9.1 De organisatie bewaart geschikte gedocumenteerde informatie als bewijsmateriaal van de resultaten van het monitoren en meten.	Opstellen van IB prestatie-indicatoren en het meten en evalueren hiervan vastleggen.
Resultaten - Toetsing	9.2 (een) auditprogramma('s) plannen, vaststellen, implementeren en onderhouden, met inbegrip van de frequentie, methoden, verantwoordelijkheden, planningseisen en rapportage.	Opstellen van een (intern?) auditprogramma
Resultaten - Reflectie	9.3 De organisatie bewaart gedocumenteerde informatie als bewijsmateriaal van de resultaten van de directiebeoordeling.	Registratie van de directiebeoordeling
Annex A		
Koers - Oriëntatie	A.5.1.1 Ten behoeve van informatiebeveiliging is een reeks beleidsregels gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	Zie 5.2
Koers - Oriëntatie	A.6.2.1 Beleid en ondersteunende beveiligingsmaatregelen is vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	Zie ook 5.2; Het IB beleid bevat beveiligingsmaatregelen omtrent het gebruik van mobiele apparatuur.
Koers - Oriëntatie	A.6.2.2 Beleid en ondersteunende beveiligingsmaatregelen zijn	Zie ook 5.2; Het IB beleid bevat beveiligingsmaatregelen omtrent telewerken

CIIO Maatstaf Combi 2020	Onderwerp en relevante ISO 27001:2013 clausule	Gedocumenteerde informatie over
	geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt bereikt, verwerkt of opgeslagen.	
Kernprocessen IB - Maatregelenselectie	8.2.1 Classificatie van informatie	Hoewel in deze maatregel volgens de norm geen documentatie verplichting is, wordt in A.8.2.2 gerefereerd aan een opgesteld dataclassificatieschema
Kernprocessen IB - Maatregelenselectie	8.2.2 Om informatie te labelen is een passende reeks procedures ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Labelingsprocedures zijn opgesteld
Kernprocessen IB - Maatregelenselectie Kernprocessen IB - Uitvoering	A.8.2.3 Procedures voor het behandelen van bedrijfsmiddelen zijn ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Procedures voor het behandelen van bedrijfsmiddelen zijn ontwikkeld
Kernprocessen IB - Maatregelenselectie Kernprocessen IB - Uitvoering	A.8.3.1 Voor het beheren van verwijderbare media zijn procedures geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.	Procedures voor het beheren van verwijderbare media
Kernprocessen IB - Maatregelenselectie Kernprocessen IB - Uitvoering	A.8.3.2 Media worden op een veilige en beveiligde manier verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.	Procedures voor het veilig verwijderen van media
Koers - Oriëntatie	A.9.1.1 Een beleid voor toegangsbeveiliging is vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	Zie ook 5.2: Het IB beleid bevat regels omtrent (logische) toegangsbeveiliging.
Kernprocessen IB - Maatregelenselectie Kernprocessen IB - Uitvoering	A.9.2.1 Een formele registratie- en uitschrijvingsprocedure is geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	Een formele registratie- en uitschrijvingsprocedure
Kernprocessen IB - Maatregelenselectie	A.9.2.2 Een formele gebruikerstoegangsverlenings-procedure is geïmplementeerd om toegangsrechten voor alle	Een formele gebruikerstoegangsverlenings-procedure

CIIO Maatstaf Combi 2020	Onderwerp en relevante ISO 27001:2013 clausule	Gedocumenteerde informatie over
Kernprocessen IB - Uitvoering	typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	
Kernprocessen IB – Maatregelenselectie Kernprocessen IB - Uitvoering	A.9.2.4 Het toewijzen van geheime authenticatie-informatie wordt beheerst via een formeel beheersproces.	Een formeel beheersproces voor het toewijzen van geheime authenticatie-informatie
Koers - Oriëntatie	A.10.1.1 Ter bescherming van informatie is er beleid voor het gebruik van cryptografische beheersmaatregelen Ontwikkeld.	Zie ook 5.2: Het IB beleid bevat regels omtrent het gebruik van cryptografische beheersmaatregelen.
Koers - Oriëntatie	A.10.1.2 Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels is tijdens hun gehele levenscyclus een beleid ontwikkeld.	Zie ook 5.2: Het IB beleid bevat regels omtrent het gebruik, de bescherming en de levensduur van cryptografische sleutels.
Kernprocessen IB – Maatregelenselectie Kernprocessen IB - Uitvoering	A.11.1.5 Voor het werken in beveiligde gebieden worden procedures ontwikkeld en toegepast.	Procedures voor het werken in beveiligde gebieden.
Koers - Oriëntatie	A.11.2.9 Er moet een ‘clear desk’-beleid voor papieren documenten en verwijderbare opslagmedia en een ‘clear screen’-beleid voor informatieverwerkende faciliteiten worden ingesteld.	Zie ook 5.2: Het IB beleid moet regels omtrent clear desk en clear screen bevatten
Kernprocessen IB – Maatregelenselectie Kernprocessen IB - Uitvoering	A.12.1.1 Bedieningsprocedures moeten worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben.	Zie 7.5.1
Koers – Vernieuwing	A.12.1.2 Wijzigingsbeheer	Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging, vinden beheerst plaats en zijn vastgelegd.
Koers - Oriëntatie	A.12.3.1 Regelmatig moeten back-upkopieën van informatie, software en systeemafbeeldingen worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	Zie ook 5.2: Het IB beleid bevat regels omtrent back-up van informatie.

CIIO Maatstaf Combi 2020	Onderwerp en relevante ISO 27001:2013 clausule	Gedocumenteerde informatie over
Kernprocessen IB – Maatregelenselectie Kernprocessen IB - Uitvoering	A.12.5.1 Om het op operationele systemen installeren van software te beheersen moeten procedures worden geïmplementeerd.	Procedures voor het installeren van software op operationele systemen
Koers - Oriëntatie	A.13.2.1 Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, moeten formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht zijn.	Zie ook 5.2: Het IB beleid bevat regels omtrent informatietransport
Kernprocessen IB – Maatregelenselectie Kernprocessen IB - Uitvoering	A.14.2.1 Voor het ontwikkelen van software en systemen moeten regels worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie worden toegepast.	Regels voor het ontwikkelen van software
Koers – Vernieuwing Kernprocessen IB – Maatregelenselectie Kernprocessen IB – Uitvoering	A.14.2.2 Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling moeten worden beheerst door het gebruik van formele controleprocedures voor wijzigingsbeheer.	Controleprocedures voor wijzigingsbeheer
Partners - Leveranciers	A.15.1.1 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.	Vastgelegde afspraken omtrent informatiebeveiligingseisen (bijv. een contract)
Kernprocessen Kwaliteit - Uitvoering	A.16.1.1 Directieverantwoordelijk-heden en -procedures moeten worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincident en te bewerkstelligen.	Informatiebeveiligingsincidenten proces
Kernprocessen IB – Maatregelenselectie Kernprocessen IB – Uitvoering	A.16.1.7 De organisatie moet procedures definiëren en toepassen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	Procedures definiëren en toepassen voor het identificeren, verzamelen, verkrijgen de naleving van intellectuele-eigendomsrechten publiceren dat het wettig gebruik van software en informatieproducten definieert)

CIIO Maatstaf Combi 2020	Onderwerp en relevante ISO 27001:2013 clausule	Gedocumenteerde informatie over
Kernprocessen IB - Maatregelenselectie Kernprocessen IB - Uitvoering	A.17.1.2 De organisatie moet processen, procedures en beheersmaatregelen vaststellen en documenteren om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.	Beheersmaatregelen om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.
Koers - Oriëntatie	A.18.1.2 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.	Zie ook 5.2: Het IB beleid omvat publicatie van regels over de naleving van intellectuele-eigendomsrechten en bevat het wettig gebruik van software en informatieproducten.

Bijlage 27001: ISO 27001:2013/ NEN 7510 versus CIIO Maatstaf Combi 2020

ISO 27001:2013	CIIO Maatstaf Combi 2020
4 Context van de organisatie	
4.1 Inzicht verkrijgen in de organisatie en haar context	Koers - Oriëntatie
4.2 Inzicht verkrijgen in de behoeften en verwachtingen van belanghebbenden	Koers - Oriëntatie
4.3 Het toepassingsgebied van het managementsysteem voor informatiebeveiliging vaststellen	Organisatie - Managementsysteem
4.4 Managementsysteem voor informatiebeveiliging	Organisatie - Managementsysteem
5 Leiderschap	
5.1 Leiderschap en betrokkenheid	Koers - Leiderschap Organisatie - Managementsysteem
5.2 Beleid	Koers - Leiderschap
5.3 Rollen, verantwoordelijkheden en bevoegdheden	Koers - Leiderschap Organisatie - Inrichting
6 Planning	
6.1 Maatregelen om risico's te beperken en kansen te benutten	Organisatie - Managementsysteem
6.1.1 Algemeen	Koers - Oriëntatie Organisatie - Managementsysteem
6.1.2 Risicobeoordeling van informatiebeveiliging	Koers - Oriëntatie
6.1.3 Behandeling van informatiebeveiligingsrisico's	Koers - Leiderschap Koers - Infrastructuur
6.2 Informatiebeveiligingsdoelstellingen en de planning om ze te bereiken	Koers - Leiderschap Koers - Infrastructuur
7 Ondersteuning	
7.1 Middelen	Koers - Leiderschap Koers - Infrastructuur
7.2 Competenties	Mensen - Ontwikkeling

ISO 27001:2013	CIIO Maatstaf Combi 2020
	Mensen - Evaluatie
7.3 Bewustzijn	Koers - Leiderschap Mensen - Ontwikkeling
7.4 Communicatie	Organisatie - Inrichting
7.5 Gedocumenteerde informatie	Organisatie - Managementsysteem
7.5.1 Algemeen	Organisatie - Managementsysteem
7.5.2 Creëren en actualiseren	Organisatie - Managementsysteem
7.5.3 Beheersing van gedocumenteerde informatie	Organisatie - Managementsysteem Kernprocessen IB - Uitvoering
8 Uitvoering	
8.1 Operationele planning en beheersing	Kernprocessen - Uitvoering Koers - Oriëntatie Koers - Leiderschap Organisatie - Managementsysteem Organisatie - Infrastructuur
8.2 Risicobeoordeling van informatiebeveiliging	Kernprocessen - Uitvoering
8.3 Informatiebeveiligingsrisico's behandelen	Koers - Vernieuwing
9 Evaluatie van de prestaties	
9.1 Monitoren, meten, analyseren en evalueren	Kernprocessen - Uitvoering Kernprocessen - Afronding Mensen - Ontwikkeling Mensen - Evaluatie Partners - Samenwerking Partners - Derden Partners - Leveranciers Resultaten - Toetsing
9.2 Interne audit	Resultaten - Toetsing
9.3 Directiebeoordeling	Resultaten - Reflectie
10 Verbetering	
10.1 Afwijkingen en corrigerende maatregelen	Resultaten - Maatregelen
10.2 Continue verbetering	Resultaten - Maatregelen
Annex A	
A.5 Informatiebeveiligingsbeleid	
A.5.1.1 Beleidsregels voor informatiebeveiliging	Koers - Leiderschap
A.5.1.2 Beoordelen van het informatiebeveiligingsbeleid	Resultaten - Toetsing Resultaten - Reflectie
A.6 Organiseren van informatiebeveiliging	
A.6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging	Koers - Leiderschap Organisatie - Inrichting
A.6.1.2 Scheiding van taken	Organisatie - Inrichting
A.6.1.3 Contact met overheidsinstanties	Koers - Oriëntatie Organisatie - Inrichting
A.6.1.4 Contact met speciale belangengroepen	Organisatie - Inrichting
A.6.1.5 Informatiebeveiliging in projectbeheer	Koers - Vernieuwing
A.6.2.1 Beleid voor mobiele apparatuur	Koers - Leiderschap
A.6.2.2 Telewerken	Koers - Leiderschap
A.7 Veilig personeel	
A.7.1.1 Screening	Mensen - Selectie
A.7.1.2 Arbeidsvoorwaarden	Mensen - Selectie
A.7.2.1 Directieverantwoordelijkheden	Organisatie - Inrichting Mensen - Ontwikkeling
A.7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	Mensen - Ontwikkeling
A.7.2.3 Disciplinaire procedure	Mensen - Selectie

ISO 27001:2013	CIIO Maatstaf Combi 2020
A.7.3.1 Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	Mensen - Selectie
A.8 Beheer van bedrijfsmiddelen	
A.8.1.1 Inventariseren van bedrijfsmiddelen	Organisatie - Infrastructuur
A.8.1.2 Eigendom van bedrijfsmiddelen	Organisatie - Infrastructuur
A.8.1.3 Aanvaardbaar gebruik van bedrijfsmiddelen	Organisatie – Infrastructuur Mensen - Ontwikkeling
A.8.1.4 Teruggeven van bedrijfsmiddelen	Mensen - Ontwikkeling
A.8.2.1 Classificatie van informatie	Kernprocessen IB - Maatregelenselectie
A.8.2.2 Informatie labelen	Kernprocessen IB - Maatregelenselectie
A.8.2.3 Behandelen van bedrijfsmiddelen	Kernprocessen IB - Maatregelenselectie
A.8.3.1 Beheer van verwijderbare media	Kernprocessen IB - Uitvoering
A.8.3.2 Verwijderen van media	Kernprocessen IB - Uitvoering
A.8.3.3 Media fysiek overdragen	Kernprocessen IB - Uitvoering
A.9 Toegangsbeveiliging	
A.9.1.1 Beleid voor toegangsbeveiliging	Koers - Leiderschap
A.9.1.2 Toegang tot netwerken en netwerkdiensten	Koers - Leiderschap
A.9.2.1 Registratie en uitschrijving van gebruikers	Kernprocessen IB - Uitvoering
A.9.2.2 Gebruikers toegang verlenen	Kernprocessen IB - Uitvoering
A.9.2.3 Beheren van speciale toegangsrechten	Kernprocessen IB - Uitvoering
A.9.2.4 Beheer van geheime authenticatie informatie van gebruikers	Kernprocessen IB - Uitvoering
A.9.2.5 Beoordeling van toegangsrechten van gebruikers	Kernprocessen IB - Uitvoering Resultaten - Toetsing
A.9.2.6 Toegangsrechten intrekken of aanpassen	Kernprocessen IB - Uitvoering
A.9.3.1 Geheime authenticatie-informatie gebruiken	Mensen - Ontwikkeling
A.9.4.1 Beperking toegang tot informatie	Kernprocessen IB - Uitvoering
A.9.4.2 Beveiligde inlogprocedures	Kernprocessen IB - Uitvoering
A.9.4.3 Systeem voor wachtwoordbeheer	Kernprocessen IB - Uitvoering
A.9.4.4 Speciale systeemhulpmiddelen gebruiken	Kernprocessen IB - Uitvoering
A.9.4.5 Toegangsbeveiliging op programmabroncode	Kernprocessen IB - Uitvoering
A.10 Cryptografie	
A.10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen	Kernprocessen IB - Uitvoering
A.10.1.2 Sleutelbeheer	Kernprocessen IB - Uitvoering
A.11 Fysieke beveiliging en beveiliging van de omgeving	
A.11.1.1 Fysieke beveiligingszone	Kernprocessen IB - Uitvoering Kernprocessen IB - Maatregelenselectie
A.11.1.2 Fysieke toegangsbeveiliging	Kernprocessen IB - Uitvoering
A.11.1.3 Kantoren, ruimten en faciliteiten beveiligen	Kernprocessen IB - Uitvoering
A.11.1.4 Beschermen tegen bedreigingen van buitenaf	Kernprocessen IB - Uitvoering
A.11.1.5 Werken in beveiligde gebieden	Kernprocessen IB - Uitvoering
A.11.1.6 Laad- en loslocatie	Kernprocessen IB - Uitvoering
A.11.2.1 Plaatsing en bescherming van apparatuur	Kernprocessen IB - Uitvoering
A.11.2.2 Nutsvoorzieningen	Kernprocessen IB - Uitvoering
A.11.2.3 Beveiliging van bekabeling	Kernprocessen IB - Uitvoering
A.11.2.4 Onderhoud van apparatuur	Kernprocessen IB - Uitvoering

ISO 27001:2013	CIIO Maatstaf Combi 2020
A.11.2.5 Verwijdering van bedrijfsmiddelen	Kernprocessen IB - Uitvoering
A.11.2.6 Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	Kernprocessen IB - Uitvoering
A.11.2.7 Veilig verwijderen of hergebruiken van apparatuur	Kernprocessen IB - Uitvoering
A.11.2.8 Onbeheerde gebruikersapparatuur	Kernprocessen IB - Uitvoering
A.11.2.9 'Clear desk'- en 'clear screen'-beleid	Koers - Leiderschap
A.12 Beveiliging bedrijfsvoering	
A.12.1.1 Gedocumenteerde bedieningsprocedures	Organisatie – Managementsysteem Kernprocessen IB - Maatregelenselectie
A.12.1.2 Wijzigingsbeheer	Kernprocessen IB - Uitvoering
A.12.1.3 Capaciteitsbeheer	Kernprocessen IB - Uitvoering
A.12.1.4 Scheiding van ontwikkel-, test- en productieomgevingen	Organisatie - Infrastructuur
A.12.4.2 Beschermen van informatie in logbestanden	Kernprocessen IB - Uitvoering
A.12.4.3 Logbestanden van beheerders en operators	Kernprocessen IB - Uitvoering
A.12.4.3 Kloksynchronisatie	Kernprocessen IB - Uitvoering
A.12.5.1 Software installeren op operationele systemen	Kernprocessen IB - Uitvoering
A.12.6.1 Beheer van technische kwetsbaarheden	Kernprocessen IB – Uitvoering Kernprocessen IB - Beoordeling
A.12.6.2 Beperkingen voor het installeren van software	Koers - Leiderschap
A.12.7.1 Beheersmaatregelen betreffende audits van informatiesystemen	Kernprocessen IB - Beoordeling
A.13 Communicatiebeveiliging	
A.13.1.1 Beheersmaatregelen voor netwerken	Kernprocessen IB - Uitvoering
A.13.1.2 Beveiliging van netwerkdiensten	Kernprocessen IB - Uitvoering
A.13.1.3 Scheiding in netwerken	Kernprocessen IB - Uitvoering
A.13.2.1 Beleid en procedures voor informatietransport	Koers - Leiderschap
A.13.2.2 Overeenkomsten over informatietransport	Partners – Samenwerken Partners - Leveranciers
A.13.2.3 Elektronische berichten	Kernprocessen IB - Uitvoering
A.13.2.4 Vertrouwelijkheids- of geheimhoudingsovereenkomst	Partners – Samenwerken Partners - Leveranciers
A.14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen	
A.14.1.1 Analyse en specificatie van informatiebeveiligingseisen	Koers – Vernieuwing Kernprocessen IB - Maatregelenselectie
A.14.1.1.1 Zorgontvangers op unieke wijze identificeren	Kernprocessen IB – Maatregelenselectie
A.14.1.1.2 Validatie van outputgegevens	Kernprocessen IB – Maatregelenselectie
A.14.1.2 Toepassingsdiensten op openbare netwerken beveiligen	Partners – Samenwerken Partners - Leveranciers
A.14.1.3 Transacties van toepassingsdiensten beschermen	Kernprocessen IB - Uitvoering
A.14.1.3.1 Openbaar beschikbare gezondheidsinformatie	Kernprocessen IB - Uitvoering
A.14.2.1 Beleid voor beveiligd ontwikkelen	Koers - Leiderschap
A.14.2.2 Procedures voor wijzigingsbeheer met betrekking tot systemen	Koers – vernieuwing

ISO 27001:2013	CIIO Maatstaf Combi 2020
A.14.2.3 Technische beoordeling van toepassingen na wijzigingen bedieningsplatform	Koers - vernieuwing
A.14.2.4 Beperkingen op wijzigingen aan softwarepakketten	Kernprocessen IB - Uitvoering
A.14.2.5 Principes voor engineering van beveiligde systemen	Koers - Leiderschap
A.14.2.6 Beveiligde ontwikkelomgeving	Organisatie - Infrastructuur
A.14.2.7 Uitbestede softwareontwikkeling	Partners - Samenwerken Partners - Leveranciers
A.14.2.8 Testen van systeembeveiliging	Koers - vernieuwing
A.14.2.9 Systeemacceptatietests	Koers - vernieuwing
A.14.3.1 Bescherming van testgegevens	Koers - vernieuwing
A.15 Leveranciersrelaties	
A.15.1.1 Informatiebeveiligingsbeleid voor leveranciersrelaties	Koers - Leiderschap Partners - Samenwerken Partners - Leveranciers
A.15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	Partners - Samenwerken Partners - Leveranciers
A.15.1.3 Toeleveringsketen van informatie- en communicatietechnologie	Partners - Samenwerken Partners - Leveranciers
A.15.2.1 Monitoring en beoordeling van dienstverlening van leveranciers	Partners - Samenwerken Partners - Leveranciers Kernprocessen IB - Beoordeling
A.15.2.2 Beheer van veranderingen in dienstverlening van leveranciers	Partners - Samenwerken Partners - Leveranciers
A.16 Beheer van informatiebeveiligingsincidenten	
A.16.1.1 Verantwoordelijkheden en procedures	Koers - Leiderschap Kernprocessen kwaliteit - Uitvoering
A.16.1.2 Rapportage van informatiebeveiligingsgebeurtenissen	Kernprocessen kwaliteit - Uitvoering
A.16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging	Kernprocessen IB - Uitvoering Kernprocessen IB - Beoordeling
A.16.1.4 Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	Kernprocessen kwaliteit - Uitvoering
A.16.1.5 Respons op informatiebeveiligingsincidenten	Kernprocessen kwaliteit - Uitvoering
A.16.1.6 Lering uit informatiebeveiligingsincidenten	Kernprocessen kwaliteit - Uitvoering Resultaten - Reflectie
A.16.1.7 Verzamelen van bewijsmateriaal	Kernprocessen kwaliteit - Uitvoering
A.17 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	
A.17.1.1 Informatiebeveiligingscontinuïteit plannen	Kernprocessen IB - Maatregelenselectie
A.17.1.2 Informatiebeveiligingscontinuïteit implementeren	Koers - vernieuwing Kernprocessen IB - Uitvoering
A.17.1.3 Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	Kernprocessen IB - Beoordeling
A.17.2.1 Beschikbaarheid van informatieverwerkende faciliteiten	Kernprocessen IB - Maatregelenselectie Kernprocessen IB - Uitvoering
A.18 Naleving	
A.18.1.1 Vaststellen van toepasselijke wetgeving en contractuele eisen	Koers - Oriëntatie
A.18.1.2 Intellectuele eigendomsrechten	Koers - Oriëntatie
A.18.1.3 Beschermen van registraties	Koers - Oriëntatie

ISO 27001:2013	CIIO Maatstaf Combi 2020
A.18.1.4 Privacy en bescherming van persoonsgegevens	Koers – Oriëntatie Koers – vernieuwing Kernprocessen IB – Maatregelenselectie Kernprocessen IB – Uitvoering
A.18.1.5 Voorschriften voor het gebruik van cryptografische beheersmaatregelen	Koers – Oriëntatie
A.18.2.1 Onafhankelijke beoordeling van informatiebeveiliging	Kernprocessen IB – Beoordeling Resultaten - Toetsing
A.18.2.2 Naleving van beveiligingsbeleid en -normen	Resultaten - Reflectie
A.18.2.3 Beoordeling van technische naleving	Kernprocessen IB – Beoordeling Resultaten - Toetsing
NEN 7510 specifieke eisen	
A.14.1.1.1 Zorgontvangers op unieke wijze identificeren	Kernprocessen IB - Maatregelenselectie
A.14.1.1.2 Validatie van outputgegevens	Kernprocessen IB - Maatregelenselectie
A.14.1.3.1 Openbaar beschikbare gezondheidsinformatie	Organisatie – Inrichting Kernprocessen IB - Maatregelenselectie

Bijlage 27001: CIIO Maatstaf Combi 2020 versus ISO 27001:2013/NEN 7510:2017

CIIO Maatstaf Combi 2020	ISO 27001:2013/NEN 7510:2017
Koers - Oriëntatie	
Omgevingsanalyse	4.1 Inzicht in de organisatie en haar context
Belanghebbendenanalyse	4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden
Dienstenaanbod	4.3.c Vaststellen van de producten en diensten van de organisatie
Wet- en regelgeving	4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden A.18.1.1 Vaststellen van toepasselijke wetgeving en contractuele eisen
Kansen- en risicoanalyse	8.2 Risicobeoordeling van informatievoorziening 8.3 Informatiebeveiligingsrisico's behandelen
Koers - Leiderschap	
Visie, missie, strategie formuleren/communiceren	5.1 Leiderschap en betrokkenheid
Beleid, doelstellingen en plannen	5.2 Beleid 6.2 Informatiebeveiligingsdoelstellingen en de planning om ze te bereiken Zie ook *Bijlage 27001/ 7510: Gedocumenteerde informatie (verplichte elementen)*
Criteria beleid en plannen	5.2.1 Het informatiebeveiligingsbeleid vaststellen 6.2.1 Kwaliteitsdoelstellingen
Draagvlak voor en afspraken over beleid en plannen	5.1 Leiderschap en betrokkenheid 7.3 Bewustzijn
Benodigde competenties en middelen	5.1 Leiderschap en betrokkenheid 5.3 Rollen, verantwoordelijkheden en bevoegdheden 7.1 Middelen
Aansturen en bijsturen	5.1 Leiderschap en betrokkenheid
Koers - Vernieuwing	
Het proces van vernieuwing	A.6.1.5 Informatiebeveiliging in projectbeheer A.14.1 Beveiligingseisen voor informatiesystemen A.14.2 Beveiliging in ontwikkelings- en ondersteunende projecten
Plan van aanpak	A.6.1.5 Informatiebeveiliging in projectbeheer A.14.1.1 Analyse en specificatie van informatiebeveiligingseisen A.14.2.2 Procedures voor wijzigingsbeheer met betrekking tot systemen
Uitvoeren plan van aanpak	A.12.1.2 Wijzigingsbeheer
Vrijgave na toets	A.14.2.8 Testen van systeembeveiliging A.14.2.9 Systeemacceptatietests
Aantoonbare processtappen	A.6.1.5 Informatiebeveiliging in projectbeheer A.14.1 Beveiligingseisen voor informatiesystemen A.14.2 Beveiliging in ontwikkelings- en ondersteunende projecten
Security en privacy by design	A.6.1.5 Informatiebeveiliging in projectbeheer
Organisatie - Inrichting	

CIIO Maatstaf Combi 2020	ISO 27001:2013/NEN 7510:2017
Inrichting afgestemd op koers	5.3 Rollen, verantwoordelijkheden en bevoegdheden
Rollen en competenties duidelijk	5.3 Rollen, verantwoordelijkheden en bevoegdheden
Overleg en communicatie	7.4 Communicatie
Organisatie - Managementsysteem	
Processen en scope vaststellen	4.3 Het toepassingsgebied van het kwaliteitsmanagementsysteem vaststellen 4.4 Kwaliteitsmanagementsysteem en de processen ervan
Borging laten aansluiten op Oriëntatie	4.4 Managementsysteem voor informatiebeveiliging
Noodzakelijke gedocumenteerde informatie	7.5.1 Gedocumenteerde informatie A.12.1.1 Gedocumenteerde informatie Nb: Zie ook *Bijlage 27001/ 7510: Gedocumenteerde informatie (verplichte elementen)*
Verantwoordelijkheid van de leiding	5.1 Leiderschap en betrokkenheid A.5.1 Aansturing door de directie van de informatiebeveiliging
Informatie is beschikbaar	7.5.3.a …informatie beschikbaar is en geschikt is voor gebruik, waar en wanneer het nodig is;
Onderhoud gedocumenteerde informatie	7.5.2 Creëren en actualiseren
Organisatie - Infrastructuur	
Infrastructuur vaststellen	7.1 Middelen A.8.1.1 Inventariseren van bedrijfsmiddelen
Werkomgeving vaststellen	7.1 Middelen A.8.1.1 Inventariseren van bedrijfsmiddelen
Kernprocessen kwaliteit - Overeenkomst	
Communicatie met (mogelijke) klanten	8.2.1 Communicatie met de klant
Klanteisen inventariseren	8.2.2 Het vaststellen van de eisen voor producten en diensten
Risico's inschatten	8.2.2 Het vaststellen van de eisen voor producten en diensten
Benodigde competenties/capaciteit bepalen	8.2.2 Het vaststellen van de eisen voor producten en diensten
Contractreview/4 ogen principe/Aanbod/Check	8.2.3 Beoordeling van de eisen voor producten en diensten
Gedocumenteerde overeenkomst	8.2.4 Wijzigingen in de eisen voor producten en diensten
Kernprocessen Informatiebeveiliging - maatregelenselectie	
Classificatie van bedrijfsmiddelen	A.8.2.1
Beschermen van informatie	A.8.2.3 A.14.1.1 Analyse en specificatie van beveiligingseisen
Identificeren zorgontvangers	A.14.1.1.1 A.14.1.1.2
Kernprocessen Informatiebeveiliging - Uitvoering	
Documenteren bedieningsprocedures	A.12.1.1
Borgen vertrouwelijkheid, integriteit en beschikbaarheid van informatie geborgd	8.3 Informatiebeveiligingsrisico's behandelen Afhankelijk van de risico's; selectie van de maatregelen op basis van de risicoanalyse in

CIIO Maatstaf Combi 2020	ISO 27001:2013/NEN 7510:2017
	samenhang met de dataclassificatie. De Annex A wordt gebruikt om te verifiëren dat er geen belangrijke beheersmaatregelen zijn weggelaten
Wijzigingen	A.12.1.2
Kernprocessen Informatiebeveiliging - Beoordeling	
Beoordelen en evalueren effect beheersmaatregelen	9.1 A.18.2 Informatiebeveiligingsbeoordelingen
Mensen - Selectie	
Competentie/capaciteit behoefte vaststellen	7.2.a Competentie
Zorgvuldig werven en selecteren	7.2.c Competenties
Kandidaten verifiëren	A.7.1.1 Screening
Overeenkomst met mensen	A.7.1.2 Arbeidsvoorwaarden
P-dossier	7.2.d Competenties
Mensen - Ontwikkeling	
Doeltreffende introductie	7.3 Bewustzijn A.7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging
Ontwikkelingsbeleid en -afspraken	7.2d Competenties
Kennismanagement	7.4 Communicatie 7.5.3 Beheer van gedocumenteerde informatie
Bewijs van competenties	7.2.d Competenties
Bewustzijn bewerkstelligen	A.7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging
Evaluatie ontwikkelactiviteiten	7.2.c Competenties
Mensen - Evaluatie	
Prestatie-eisen vaststellen	7.2.a Competenties
Evaluatie medewerkers	7.2.c Competenties
Exitgesprekken/Eindgesprekken	9.1 Monitoren, meten, analyseren en evalueren A.7.3.1 Beëindiging of wijziging van verantwoordelijkheden van het dienstverband
Partners - Samenwerking	
Samenwerkingsverbanden	4.2 Inzicht verkrijgen in de behoeften en verwachtingen van belanghebbenden 7. Ondersteuning
Gedocumenteerde afspraken	7.4 Communicatie
Evaluatie samenwerking	9.1 Monitoren, meten, analyseren en evalueren
Partners - Derden	
Selecteren van/eisen aan in te zetten derden	7.2 Competentie
Gedocumenteerde afspraken	A.7.1.2 Arbeidsvoorwaarden
Inwerken van derden	A.7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging
Evaluatie derden	9.1 Monitoren, meten, analyseren en evalueren
Partners - Leveranciers	
Selecteren van/eisen aan leveranciers	A.15.2 Beheer van dienstverlening van leveranciers A.15.1.3 Toeleveringsketen van informatie- en communicatietechnologie
Gedocumenteerde afspraken	A.15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten
Controle producten en diensten	A.14.2.7 Uitbestede softwareontwikkeling A.14.2.9 Systeemacceptaties
Evaluatie leveranciers	9.1 Monitoren, meten, analyseren en evalueren

CIIO Maatstaf Combi 2020	ISO 27001:2013/NEN 7510:2017
	A.15.2.1 Monitoring en beoordeling van dienstverlening van leveranciers
Resultaten - Toetsing	
(Geaggregeerde) resultaten van evaluaties vaststellen en verzamelen	9.1 Monitoren, meten, analyseren en evalueren A.18.2 Informatiebeveiligingsbeoordelingen
Feedback van belanghebbenden verzamelen	4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden
Vastleggen, rapporteren, maatregelen nemen	9.1 Monitoren, meten, analyseren en evalueren
Interne audit plannen en uitvoeren	9.2 Interne audit A.18.2 Informatiebeveiligingsbeoordelingen
Resultaten - Reflectie	
Reflectie op toetsing	9.1 Monitoren, meten, analyseren en evalueren
Resultaten van reflectie voor evaluatie	9.1 Monitoren, meten, analyseren en evalueren
Directiebeoordeling	9.3 Directiebeoordeling A.18.2.2 Naleving van beveiligingsbeleid en -normen
Resultaat van de directiebeoordeling	9.3 Directiebeoordeling
Resultaten - Maatregelen	
Maatregelen vanuit Reflectie	9.3 Directiebeoordeling
Verbeterkansen benutten	10 Verbetering
Vastleggen maatregelen	10 Verbetering