Nederlandse Vereniging van Ziekenhuizen

de Nederlandse ggz

Zorgverzekeraars Nederland

NEDERLANDSE FEDERATIE VAN UNIVERSITAIR MEDISCHE CENTRA

Nederlandse Zorgautoriteit

HORIZONTAAL TOEZICHT ZORG

medisch specialistische zorg en geestelijke gezondheidszorg

Control Framework

(versie 4.0 definitief)

Oktober 2021

Control Framework

Bijlage 1 • Handvat Volwassenheid derde lijn

Bijlage 2 • Handvat IT General Controls en beheersmaatregelen met een IT-component

Bijlage 3 • Bestuurlijke afspraken deelwaarnemingen

Control Framework (1)

Inhoud

Control Framework versie 2022 (hierna 'CFW') heeft als doel om op een uniforme en efficiënte wijze verantwoording af te leggen in de keten. Dit document beschrijft de processtappen die zorgaanbieder en representerend verzekeraars jaarlijks doorlopen waarmee Horizontaal Toezicht in de praktijk wordt vormgegeven. Hierbij kunnen ze ondersteund worden door een assurance provider.

Er zijn zeven processtappen gedefinieerd:

0. Identificatie hoofd- en deelprocessen
1. Benoemen van beheersdoelstellingen
2. Identificeren van risico's
3. Uitvoeren risicoanalyse
4. Bepalen beheersmaatregelen
5. Beoordelen opzet en bestaan van de beheersmaatregelen
6. Verantwoorden over opzet, bestaan en werking.

Voorop staat dat de zorgaanbieder zelf een redelijke mate van zekerheid wil hebben dat beheersdoelstellingen zijn gerealiseerd. Hiervoor toetst de zorgaanbieder jaarlijks opzet, bestaan en werking van de beheersmaatregelen. Het CFW is hiervoor het middel. Ook kan het Control Framework als middel gebruikt worden om continue de zorgregistratie te verbeteren.
Verzekeraars steunen op het CFW maar zullen, ten behoeve van hun verantwoording verder in de keten, aanvullende controlewerkzaamheden moeten uitvoeren en eventueel aanvullende assurance van een assurance provider nodig hebben. Assurance is geen doel op zich, maar kan helpen het opgebouwde vertrouwen te funderen.

In dit document is per stap van het CFW beschreven welke rol zorgaanbieder, representerend verzekeraar, tweede verzekeraar en assurance provider hebben en welke werkzaamheden zij uitvoeren.

Wat is het Control Framework?

Het Control Framework is een gestructureerd beheersingskader dat in de praktijk de uitvoering van Horizontaal Toezicht faciliteert. Het maakt inzichtelijk of met de interne beheersing de onderkende beheersdoel-stellingen voor het rechtmatig registreren en declareren van zorg in toereikende mate worden behaald. Hiermee faciliteert het Control Framework de dialoog tussen een zorgaanbieder en de representerend verzekeraar.

Versiebeheer

Het streven is om vanaf 2022 jaarlijks in oktober een nieuwe versie van het CFW te publiceren dat geldig is voor het volgende jaar. D.w.z. in oktober 2022 wordt het CFW 2023 gepubliceerd. Inhoudelijke verdieping en verduidelijking op thema's in het CFW kunnen gedurende het jaar worden gecommuniceerd, maar zullen pas een formele plek krijgen in het CFW voor het volgende jaar.
Zorgaanbieder maakt gebruik van laatste versie van CFW, maar kan in overleg met verzekeraar hiervan afwijken.

Wijzigingen CFW versie 2022

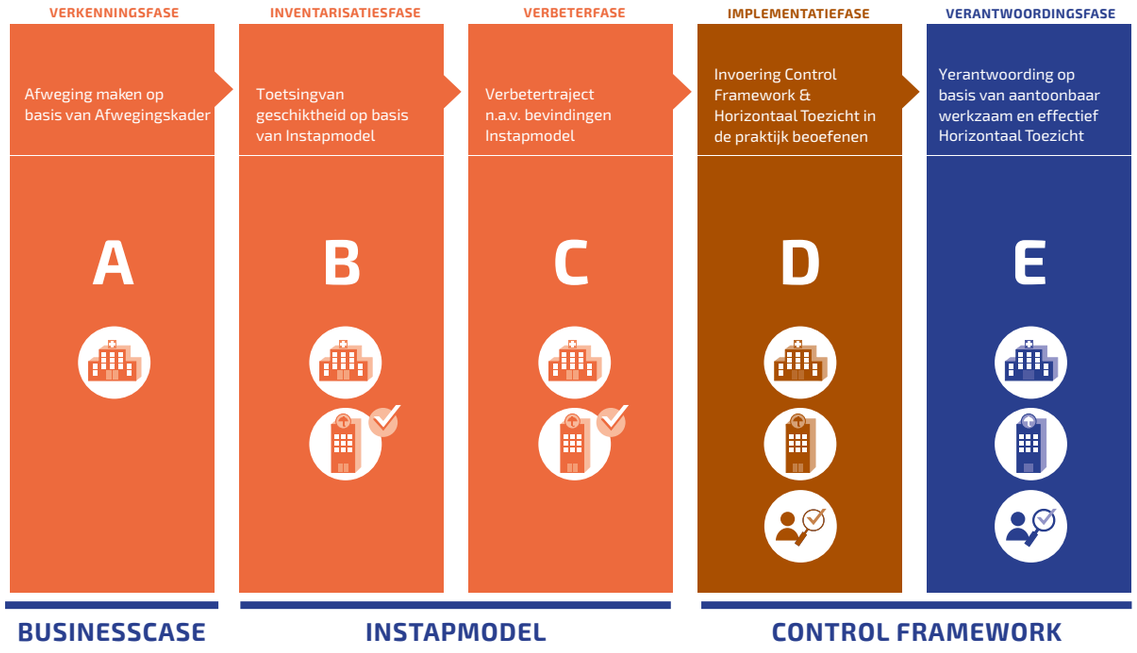
De belangrijkste wijziging in dit CFW t.o.v. de voorgaande versie is dat onderstaande documenten zijn geïntegreerd in dit CFW:

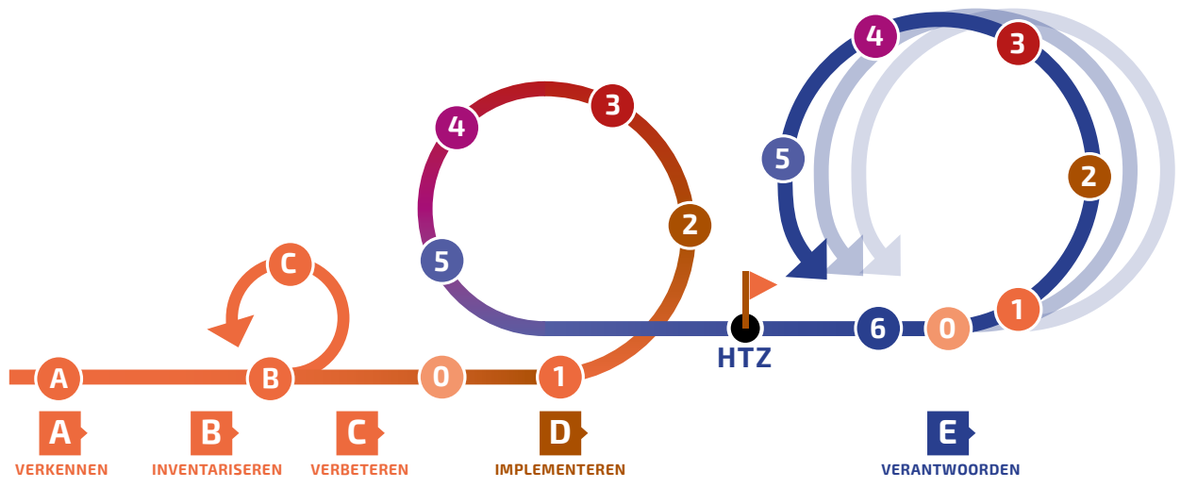
- Afspraken over efficiënte uitvoering van HT uit november 2019
- Handvat voor toepassing IT General Controls binnen HT
- Handvat Verantwoord Verminderen
- Handvat volwassenheid 3e lijn binnen HT
- Brief NZa – Positie deelwaarnemingen binnen HT
- Memo bestuurlijke commissie HT omgaan met deelwaarnemingen binnen HT

Control Framework (2)

Relatie met het implementatieplan

Het CFW wordt toegepast door zorgaanbieders die zich bevinden in de implementatiefase (fase D) of in de verantwoordingsfase (fase E). Ook in fase A t/m C kunnen voorbereidende stappen gezet worden om te komen tot een CFW.





In de implementatiefase doorloopt de zorgaanbieder de stappen 0 t/m 6 uit het CFW. De overgang naar processtap 6 is tegelijk ook de overgang naar fase E en dus de overgang naar een repeterende jaarcyclus van Horizontaal Toezicht.

In de HT-jaarcyclus voert de zorgaanbieder jaarlijks een verschillenanalyse uit t.o.v. het voorgaande jaar. Wijzigingen in risicodefinitie, risicoclassificatie en beheersmaatregelen voortkomend uit externe wijzigingen in wet- en regelgeving, dan wel interne wijzigingen in de beheersingsomgeving worden verwerkt in het CFW voor het aankomende jaar.

Control Framework (3)

Rol zorgaanbieder

De Zorgaanbieder draagt zorg voor het zelf 'in control' zijn en om 'continu te verbeteren'. Ook richt de zorgaanbieder zich op een efficiënte verantwoordingsketen, met zo min mogelijk administratieve lasten voor alle partijen. Hiertoe start de zorgaanbieder met de beheersdoelstellingen en hierna worden de risico's geïdentificeerd en geclassificeerd naar hoog/midden/laag. Daarbij wordt de inrichting van de three lines of defense beschreven waarbij de werkzaamheden van de eerste, tweede en derde lijn zijn opgenomen. De mate waarin de representerend verzekeraar op de werkzaamheden van de derde lijn kan steunen, is afhankelijk van de volwassenheid van de derde lijn. In bijlage 1 is het handvat "Volwassenheid derde lijn binnen HT" opgenomen, dat een relatie legt tussen de verschillende volwassenheidsniveaus van de derde lijn en de aanvullende controlewerkzaamheden van de representerend verzekeraar.

Rol representerend verzekeraar

De representerend zorgverzekeraar draagt bij aan het continu verbeteren en richt zich op een efficiënte verantwoordingsketen. Per stap van het CFW worden de werkzaamheden van de representerend verzekeraar beschreven. De aard van deze werkzaamheden is afhankelijk van de volwassenheid van de derde lijn van de zorgaanbieder.
Gedurende het proces past de representerend verzekeraar hoor en wederhoor toe bij de tweede verzekeraar voor de go/no go momenten binnen het CFW om zo eenduidige toepassing van het CFW te borgen.
Als voorbeeld is het beoordelen van de opzet van de beheersmaatregelen zo'n go/no go moment.

Rol tweede verzekeraar

De rol van de tweede verzekeraar is het vaststellen dat de representerend verzekeraar zijn werkzaamheden uitvoert in lijn met het landelijk representatie-raamwerk 1.0 en met voldoende kwaliteit.

De tweede verzekeraar is bij de implementatie van HT en in het eerste jaar bij fase E meer betrokken bij afstemming tussen zorgaanbieder en representerend verzekeraar. Vanaf het tweede jaar fase E stemmen representerend en tweede verzekeraar de gewenste momenten van betrokkenheid onderling af.

De tweede verzekeraar behoudt zijn verantwoordelijkheid toe te zien op de kwaliteit en werkwijze van de representerend verzekeraar. De tweede verzekeraar beoordeelt en accordeert daartoe het dossier van de representerend verzekeraar.
Eventuele bevindingen van de tweede verzekeraar aangaande de werkzaamheden van de representerende verzekeraar hebben daarbij echter alleen een prospectief effect. De bevindingen van de tweede verzekeraar worden aan de representerende verzekeraar meegegeven ten behoeve van het volgende HT-jaar. De representerende verzekeraar en de zorgaanbieder zijn gezamenlijk verantwoordelijk om in het volgende HT-jaar de bevindingen van de tweede verzekeraar op te pakken.

Dossiervoering verzekeraars

Het dossier van de representerend verzekeraar is inzichtelijk voor de tweede verzekeraar. Na afronding van een HT-jaar wordt het dossier vrijgegeven aan alle verzekeraars ter lering en verdere uniformering van de representatieaanpak.

Control Framework (3)

Rol assurance provider

De assurance provider kan in de implementatiefase van HT worden betrokken bij het geven van assurance over opzet en bestaan van IT General Controls, hierna ITGC's, middels een ISAE 3000 type 1 verklaring. In overleg met representerend verzekeraar, kan dit ook op andere manieren. De ITGC's worden in processtap 2 verder toegelicht.

De assurance provider geeft in de verantwoordingsfase van HT een ISAE 3000 type 2 verklaring af over bestaan en werking van de afgesproken beheersmaatregelen in het CFW. Om beter gebruik te maken van de expertise van verschillende partijen, wordt hierbij niet meer standaard uitgegaan van de beheersmaatregelen gekoppeld aan de hoge risico's. In het bilaterale overleg tussen de zorgaanbieder en de representerend verzekeraar worden deze beheersmaatregelen afgestemd, waarbij minimaal bestaan en werking van de ITGC's wordt meegenomen in de ISAE 3000 type 2 verklaring. Het is van belang om in gezamenlijk overleg te komen tot een goede scope van de werkzaamheden van de assurance provider, waarbij er geen verzwaring optreedt van de administratieve lasten voor zorgaanbieder, verzekeraar en assurance provider ten opzichte van de situatie CFW 3.0, versie juli 2019 (beheersing op hoge risico's).

De ISAE 3000 type 2 verklaring is verplicht voor de eerste 2 HT-verantwoordingsjaren. Daarna wordt de type 2 verklaring iedere 3 jaar uitgevoerd (ervan uitgaande dat in de eerste twee verantwoordingsjaren de beheersing in voldoende mate heeft gewerkt en er geen majeure wijzigingen in de interne beheersingsomgeving hebben voorgedaan). In het bilaterale HT-overleg tussen de zorgaanbieder en representerend verzekeraar kan in afwijking hiervan worden besloten dat een ISAE 3000 type 2 verklaring niet meer nodig is, omdat de derde lijn van de zorgaanbieder van voldoende volwassenheid is. Zie hiervoor ook bijlage 1 handvat "Volwassenheid derde lijn binnen HT".

0 **Identificeren hoofd- en deelprocessen**

1 **Benoemen van beheersdoelstellingen**

2 **Identificeren van risico's**

3 **Uitvoeren risicoanalyse**

4 **Bepalen beheersmaatregelen**

5 **Beoordelen opzet en bestaan van de beheersmaatregelen**

6 **Verantwoorden over opzet, bestaan en werking**

0 & 1 Identificatie van hoofd- en deelprocessen & benoemen van beheersdoelstellingen

De zorgaanbieder start met het identificeren van de hoofdprocessen voor het registreren en declareren van zorg die valt onder de Zvw. Een hoofdproces bestaat uit deelprocessen. Dit zijn verschillende stappen die bij een zorgaanbieder doorlopen moeten worden. De hoofd- en deelprocessen worden aangesloten met de omzetstromen van een zorgaanbieder. Processen zonder of met minimale financiële impact, hoeven na overleg met de representerend verzekeraar, niet in het CFW te worden opgenomen.

Zijn de hoofd- en deelprocessen geïdentificeerd, dan wordt per proces de beheersdoelstelling benoemd. In het kader van Horizontaal Toezicht zijn de beheersdoelstellingen primair gericht op juistheid van registratie en declaratie van de zorgaanbieder richting de zorgverzekeraar.

Rol zorgaanbieder
- Identificeert hoofd- en deelprocessen
- Benoemt de beheersdoelstellingen o.b.v. wet- en regelgeving en inrichtingskeuze interne beheersing

Rol representerend verzekeraar
- Ondersteunt in identificatie hoofd- en deelprocessen
- Toetst geformuleerde beheersdoelstellingen

Stappenplan

Good practices van uitwerkingen in hoofd- en deelprocessen in de GGZ en MSZ zijn beschikbaar op www.horizontaatoezichtzorg.nl. Aanbevolen wordt ook om contact op te nemen met collega zorgaanbieders die hetzelfde EPD en/of daily auditing tool gebruiken en de transitie naar HT reeds hebben gemaakt.

2 Identificeren van risico's

Een risico is een onzekere gebeurtenis die ertoe kan leiden dat de beheersdoelstelling niet wordt gerealiseerd. Voor het identificeren van de risico's is van belang te redeneren vanuit de beheersdoelstellingen en de processen die hier aan ten grondslag liggen.
De zorgaanbieder identificeert per hoofd- en deelproces de risico's. Geadviseerd wordt om dit vanuit meerdere invalshoeken te bekijken (proces, techniek, wet- en regelgeving, wie zijn erbij betrokken etc.) en een vast format te hanteren met oog voor oorzaak en gevolg van het risico.

IT omgeving
Randvoorwaardelijk voor het borgen van de juiste en volledige dataverwerking zijn IT General Controls (hierna ITGC's). ITGC's zijn vrij vertaald algemene beheersmaatregelen (zoals beleidslijnen en procedures) rond de IT-omgeving, die ervoor moeten zorgen dat beheersmaatregelen met een IT-component continu betrouwbaar werken. ITGC's zijn geen doel op zich, maar zijn ondersteunend aan de beheersing op de procesrisico's en vormen hiermee een belangrijke randvoorwaarde om te verantwoorden middels Horizontaal Toezicht. Terugkerende vraag bij ITGC's voor HT is: Welke ITGC's zijn nodig om te waarborgen dat de data in de IT-systemen betrouwbaar is en blijft. De relevante IT risico's en scope staan benoemd in het Handvat voor toepassing IT General Controls binnen HT. - Bijlage 2

Rol zorgaanbieder
- Identificeren risico's voor opname in het CFW
- Onderbouwen van de aanpak en de uitvoering van de risico-identificatie (met het oog op een zo volledig mogelijke identificatie)

Rol representerend verzekeraar
- Beoordeelt volledigheid risico-identificatie

Rol tweede verzekeraar
- Beoordeelt representerend verzekeraar op zijn werkzaamheden ten aanzien van volledigheid risico-identificatie

Voor het identificeren van risico's is de procesgerichte aanpak noodzakelijk en kan de landelijke risicolijst als hulpmiddel ter controle van de volledigheid gebruikt worden. Ander gebruik van landelijke risicolijst wordt niet geadviseerd omdat deze niet geactualiseerd wordt en niet het juiste aggregatieniveau kent.

3 Uitvoeren risicoanalyse

Het classificeren van de geïdentificeerde risico's gebeurt aan de hand van de methodiek opgenomen in deze stap. Bij het classificeren van risico's wordt uitgegaan van bruto risico's, dat wil zeggen de risico's vóór het inrichten van beheersmaatregelen. Het classificeren van de risico's wordt tevens gedaan op basis van professionele inschatting, in samenspraak tussen de representerend verzekeraars en de zorgaanbieder.

De nauwkeurigheid van de risicoanalyse kan worden verhoogd door indicatoren[1] mee te nemen die het karakter hebben van een afslagcriterium op de uitkomst van de risicoclassificatie.

Door meer informatie te laten meewegen kan een betere inschatting gemaakt worden of risico's reëel zijn.

Rol zorgaanbieder
- Prioriteert en onderbouwt risicoclassificatie conform hierna beschreven model.
- Stemt risicoclassificatie af met representerend verzekeraar. In samenspraak kunnen risico's anders geclassificeerd worden.

Rol representerend verzekeraar
- Beoordeelt classificatie van de risico's (laag/midden/hoog)
- Stelt Topmemo op t.b.v. dossier verzekeraars. Hierin wordt vermeld: proces en conclusies op hoofdlijnen ten aanzien van volledigheid, risico-identificatie, en beoordeling risicoclassificatie

Rol tweede verzekeraar
- Beoordeelt representerend verzekeraar op zijn werkzaamheden ten aanzien van de beoordeling risicoclassificatie.

[1] Voorbeelden hiervan zijn:
- Uitkomsten/bevindingen voorgaande trajecten, zoals bijvoorbeeld zelfonderzoek;
- Procesmonitoringsinformatie over de mate waarin risico in het proces of de systemen wordt beheerst (bijvoorbeeld monitoringsinformatie over bevoegdheid zorgverlener);
- Generiek ingerichte beheersinstrumenten in de keten (bijvoorbeeld Vecozo);
- Opgebouwde kennis bij instelling of zorgverzekeraar over bepaalde risico's;
- Data-analyse of andere innovatieve instrumenten van zorgaanbieder of zorgverzekeraar die wijzen op het beheersen van het risico.

De risico-inschatting gebeurt op basis van de categorieën impact (kwantitatief en kwalitatief) en kans (kwantitatief en kwalitatief). In onderstaande schaalindeling zijn de mogelijke scores bij deze vier categorieën opgenomen.

Schaalindeling

Voor de categorieën “kans” en “impact” wordt een schaal van 1 t/m 4 gebruikt. De niveaus in de schaal hebben onderstaande betekenis:

Niveau	Betekenis
1	Niet waarschijnlijk/weinig
2	Mogelijk/af en toe
3	Waarschijnlijk/regelmatig
4	Zeer waarschijnlijk/vaak

Voor het bepalen van de score per risico kan gebruik worden gemaakt van het schema op de volgende pagina.

IT risico’s

De IT risico’s dienen niet te worden geprioriteerd en zijn daarom altijd in scope. Dit komt omdat de beheersing hierop (ITGC’s) randvoorwaardelijk is voor een betrouwbare werking van de application controls en IT-dependent controls.

Vervolgens wordt deze score afgezet tegen onderstaande tabel.

IMPACT (kwalitatief + kwantitatief) \ KANS (kwalitatief + kwantitatief)	2	3	4	5	6	7	8
8	10	11	12	13	14	15	16
7	9	10	11	12	13	14	15
6	8	9	10	11	12	13	14
5	7	8	9	10	11	12	13
4	6	7	8	9	10	11	12
3	5	6	7	8	9	10	11
2	4	5	6	7	8	9	10

Classificatie risico

Laag: 4 t/m 8 — Middel: 9 t/m 12 — Hoog: 13 t/m 16

Good practices van uitwerkingen van risicoclassificaties in de GGZ en MSZ zijn beschikbaar op www.horizontaatoezichtzorg.nl. Aanbevolen wordt ook om contact op te nemen met collega zorgaanbieders die hetzelfde EPD en/of daily auditing tool gebruiken en de transitie naar HT reeds hebben gemaakt.

	Categorie	Onderwerpen/hulpvragen	Niveau
IMPACT	**kwalitatief**	• Heeft het risico impact op de afleiding van een DBC-zorgproduct/ leidt het tot een fout in de factuurregel? • Hoe groot is de financiële fout?	**1 t/m 4**
	kwantitatief	• Zorgt dit proces voor een belangrijke bijdrage aan de omzet? [1] • Op welke percentage van de omzet heeft dit risico impact?	**1 t/m 4**
KANS*	**kwalitatief**	• Handmatig/geautomatiseerd proces. In hoeverre is het mogelijk om het risico met geautomatiseerde beheersmaatregelen (application controls) af te dekken, of moet er al snel worden overgegaan op handmatige beheermaatregelen/ IT afhankelijke handmatige beheersmaatregelen. • Soort software die de zorgaanbieder gebruikt/ volwassenheid systeem, ofwel de mogelijkheid om beheersmaatregelen adequaat in te kunnen richten.[2] Aantal verschillende toolings die worden gebruikt. • Vergt de registratie een inhoudelijke afweging van de registrerende zorgprofessional om vast te stellen of de declaratie rechtmatig is? (Bijv. wel of niet terecht parallelle trajecten) • Complexiteit van het proces/zorgactiviteit en de geldende wet- en regelgeving en/of eventuele wijzigingen hierin.	**1 t/m 4**
	kwantitatief	• Hoe vaak wordt de zorgactiviteit geregistreerd? • Hoe groot is de foutkans? (Hoe vaak leidt dit daadwerkelijk tot een registratiefout?)	**1 t/m 4**
			Totaal

*De volgende incidentele ontwikkelingen kunnen een kansverhogend effect hebben en leiden tot een hogere kans kwantitatief/kwalitatief:
- Wisselingen in kritieke functies van het personeel;
- Fusies/overnames/samenwerkingsverbanden;
- Grote wijzigingen in systeem/software.

[1] Voor bepaling van de bijdrage aan de omzet wordt gekeken naar de omzetstroom waarin het betreffende proces waardebepalend is. De bijdrage aan de omzet is gebaseerd op de risicogerichte massa vóór het inrichten van beheersmaatregelen.

[2] Het betreft het basis registratiesysteem van de zorgaanbieder. Wat is het volwassenheidsniveau van dit systeem en in hoeverre is het mogelijk om adequate beheermaatregelen in het systeem in te richten. Hiermee wordt niet bedoeld een eventuele daily auditing tool welke aan het einde van het proces wordt ingezet.

4 Bepalen beheersmaatregelen

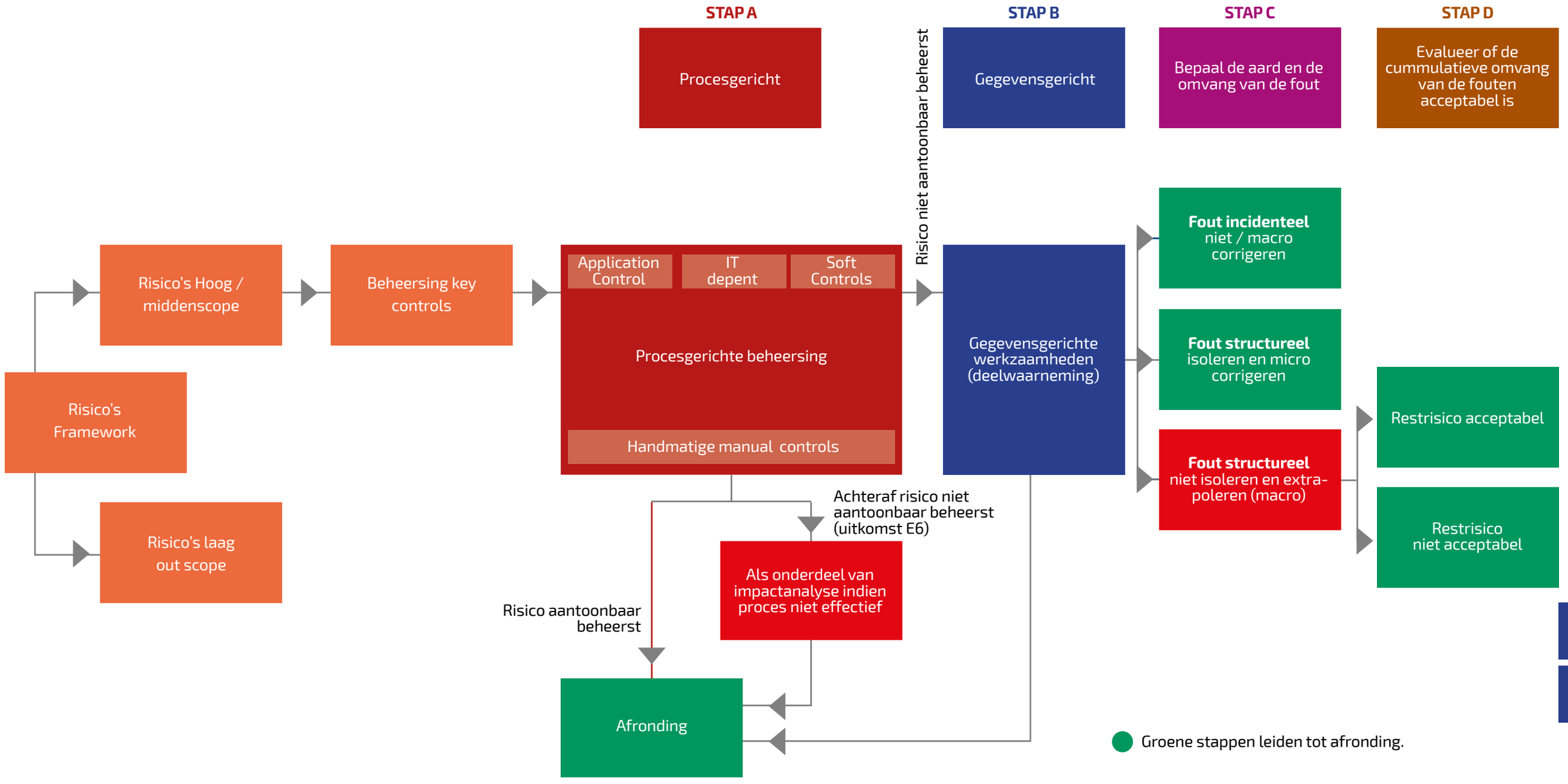
In deze stap bepaalt de zorgaanbieder de relevante beheersmaatregelen ter beheersing van de beheersdoelstellingen en de hiermee samenhangende geclassificeerde risico's. Met het Control Framework toont de zorgaanbieder aan hoe de realisatie van beheersdoelstellingen is geborgd. Dit vormt het uitgangspunt voor verantwoording vanuit een procesgerichte benadering. Het onderstaande figuur is een visuele weergave van de verantwoording op basis van een procesgerichte benadering (stap A).

De stappen B t/m D beschrijven de vervolgstappen zoals beschreven in hoofdstuk 4, 5 en 6, indien:

- sprake is van ontoereikende beheersmaatregelen
- dit qua aantonen werking efficiënter is dan procesgericht
- blijkt dat de werking niet effectief is (impactanalyse)

In deze gevallen zullen (aanvullend) gegevensgerichte werkzaamheden noodzakelijk zijn om te komen tot een uitspraak over de realisatie van beheersdoelstellingen en de mate waarin het restrisico tot een aanvaardbaar niveau is gereduceerd. In hoofdstuk 6 is de uitwerking van deze gegevensgerichte werkzaamheden nader toegelicht.

4 Bepalen beheersmaatregelen



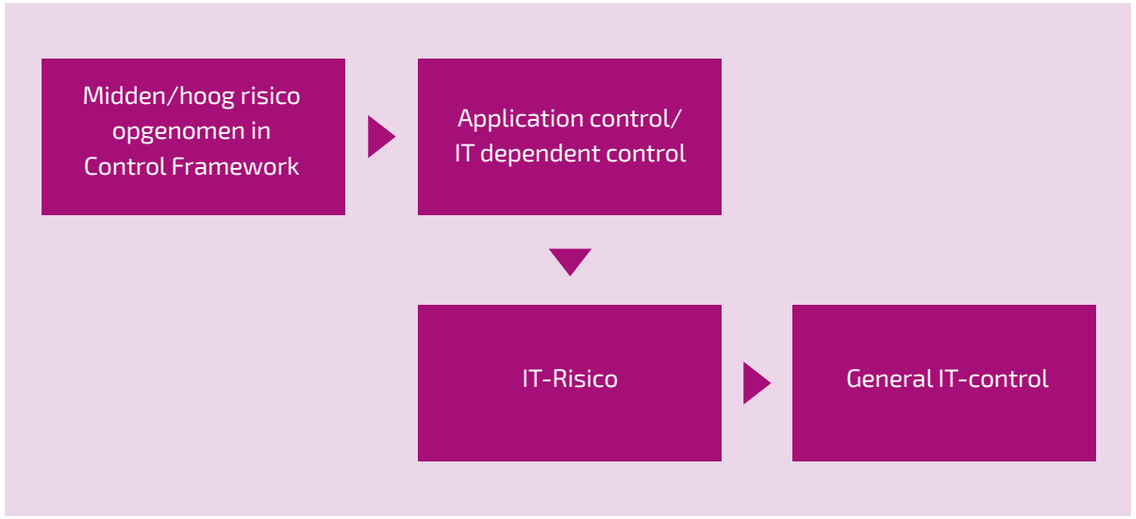
Procesgericht (stap A)
Het CFW gaat uit van een procesgerichte benadering van beheersmaatregelen vanuit het principe van het three lines-of-defence model. De keuze voor de aard en het type beheersmaatregel is aan de zorgaanbieder. De zorgaanbieder identificeert de beheersmaatregelen behorend bij de als hoog en midden geclassificeerde risico's. Bij de beschrijving van de beheersmaatregelen dient de zorgaanbieder aan te geven wie doet wat, wanneer, met welke frequentie en aan de hand waarvan. Beleid en procedures worden door een zorgaanbieder opgesteld, onderhouden en geïmplementeerd om zo de benodigde beheersmaatregelen te verankeren

Eén van de principes van Horizontaal Toezicht is dat risico's zoveel mogelijk beheerst worden 'aan de bron'. Dit betekent dat de beheersmaatregelen er zoveel mogelijk op gericht moeten zijn om de bronregistratie in één keer goed te laten plaatsvinden.

Zorgaanbieders zorgen voor een mix van beheersmaatregelen om de risico's in voldoende mate op een efficiënte en effectieve wijze te beheersen. Binnen deze mix van beheersmaatregelen dient ook aandacht te worden geschonken aan de "soft controls" en de IT General Controls (ITGC's) die randvoorwaardelijk zijn voor het gebruik van geautomatiseerde beheersmaatregelen. De opzet van de beheersmaatregelen blijkt uit procesbeschrijvingen, werkinstructies en functionele ontwerpen van systemen. Een uitwerking van de soorten beheersmaatregelen is opgenomen in het kader op pagina 16.

Per risico in scope (hoog en midden) stelt de zorgaanbieder de key beheersmaatregelen vast. Een key beheersmaatregel is een beheersmaatregel die al dan niet tezamen met andere key beheersmaatregelen één of meerdere (oorzaken/gevolgen van) risico's volledig of grotendeels afdekken en hiermee het restrisico tot een aanvaardbaar niveau te reduceren. Bij voorkeur zijn key beheersmaatregelen geautomatiseerd en preventief van aard.

IT General Controls
De IT General Controls (ITGC's) op het gebied van Horizontaal toezicht zijn randvoorwaardelijk om te kunnen steunen op de beheersmaatregelen bij gebruik van application controls en IT-dependent controls. De samenhang tussen het gebruik van geautomatiseerde beheersmaatregelen en ITGC's is weergegeven in onderstaand figuur.



Beheersmaatregelen
Doel van beheersmaatregelen is om inzicht te krijgen in het registratie-/declaratieproces. Er bestaan vier soorten beheersmaatregelen, zie onderstaand:
• Application controls: beheersmaatregelen ingebouwd in het systeem (bijvoorbeeld: verplicht in te vullen velden voor BSN);
Application controls kunnen verdeeld worden in configureerbare- en niet configureerbare application controls.
- Configureerbare application controls zijn in de software geprogrammeerde controlemaatregelen die configureerbaar zijn door de gebruiker, waarbij verwerking op basis van die configuratie-instelling door de software plaatsvindt.
- Niet configureerbare application controls zijn door de software leverancier ingerichte application controls die niet aangepast kunnen worden door de gebruiker.

• IT-dependent controls: beheersmaatregelen waarbij gebruik wordt gemaakt van lijstwerk uit systemen (bijvoorbeeld controle aan de hand van signaleringslijsten);
• Handmatige beheersmaatregelen: beheersmaatregelen buiten de systemen om zijn ingericht (menselijk handelen). Zuiver handmatige beheersmaatregelen komen in de regel nagenoeg niet voor. Daarnaast is het van belang om handmatige beheersmaatregelen niet te verwarren met gegevensgerichte werkzaamheden zoals beschreven in hoofdstuk 6.
• Soft controls: beheersmaatregel die – meer dan hard controls – ingrijpt op c.q. appelleert aan het persoonlijk functioneren van medewerkers (overtuiging, persoonlijkheid). Soft controls zijn op te vatten als maatregelen die van invloed zijn op bijvoorbeeld de motivatie, loyaliteit, integriteit, inspiratie en normen en waarden van medewerkers.

De beheersmaatregelen van de zorgaanbieder kunnen een mix zijn van:
• hard controls en/of soft controls;
• preventieve en/of detectieve beheersmaatregelen;
• geautomatiseerde en/of handmatige beheersmaatregelen.

In hoeverre een beheersmaatregel effectief is om het risico procesgericht af te dekken verschilt per type beheersmaatregel. Hiervoor is ook de professionele inschatting nodig van de representerend verzekeraar en de zorgaanbieder. In het algemeen kan gesteld worden dat geautomatiseerde controls (application controls) meer zekerheid geven dan handmatige beheersmaatregelen.
Bij voorkeur zijn key beheersmaatregelen geautomatiseerd en preventief van aard.

Rol zorgaanbieder
• Beschrijft de beheersmaatregelen behorend bij de hoog en midden risico's
• Geeft per beheersmaatregel aan wie doet wat, wanneer, met welke frequentie en aan de hand waarvan.
• Geeft per beheersmaatregel aan of de beheersmaatregel key is.

Rol representerend verzekeraar
• Beoordeelt de navolgbaarheid van de beschrijving van de beheersmaatregelen.

5 Beoordelen opzet en bestaan van de beheersmaatregelen

Procesgericht (stap A)

Nadat de beheersmaatregelen zijn bepaald en beschreven, worden deze getoetst op toereikendheid. De beoordeling van opzet en bestaan van de beheersmaatregelen richt zich op de key beheersmaatregelen van de midden en hoge risico's. De mate van diepgang van de werkzaamheden is afhankelijk van de mix van beheersmaatregelen in relatie tot de beheersdoelstellingen die de zorgaanbieder wil bereiken.

Daar waar het bestaan niet kan worden aangetoond, is dit van invloed op de toereikendheid van de opzet en de inschatting van de mate waarin het restrisico is gemitigeerd. Indien geïdentificeerde key beheersmaatregelen (nog) niet bestaan, dan kan dit niet leiden tot een laag restrisico.

Gegevensgericht (stap B)

Indien de beheersmaatregelen het risico niet in voldoende mate afdekken, dan wordt beschreven hoe dit restrisico terug gebracht wordt tot een aanvaardbaar niveau door middel van gegevensgerichte werkzaamheden. Voorafgaand aan de overgang naar Horizontaal Toezicht of voorafgaand aan een nieuw verantwoordingsjaar moet duidelijk zijn hoe de hoge en midden risico's in het Control Framework tot een aanvaardbaar niveau worden verlaagd, ook indien hier gegevensgerichte werkzaamheden voor moeten worden beschreven. Voor de inrichting van gegevensgerichte werkzaamheden wordt verwezen naar processtap 6.

Vaststellen van het bestaan van een beheersmaatregel

Onderstaand is per type beheersmaatregel opgenomen hoe het bestaan hiervan wordt vastgesteld.

- **Application controls**
  De zorgaanbieder toont het bestaan van application controls aan middels testresultaten ('test-of-one'; positief en negatief) en stelt hiermee vast of de application control juist is ingericht en bestaat.
- **IT dependent controls**
  De zorgaanbieder doorloopt middels een lijncontrole het (deel)proces en stelt vast of de beheersmaatregelen in de praktijk bestaan. Hierbij wordt ook gekeken naar het geautomatiseerde deel van de beheersmaatregel (bv. naar de query).
- **Handmatige beheersmaatregelen**
  De zorgaanbieder doorloopt middels een lijncontrole het (deel)proces en stelt vast of de beheersmaatregelen in de praktijk bestaan.
- **Soft controls**
  De soft controls kennen een bijzondere positie binnen het Control Framework. Hoewel soft controls in belangrijke mate bijdragen aan het bereiken van de beheersdoelstellingen, is het bestaan en de werking van soft controls moeilijk objectief aantoonbaar. De soft controls worden wel beschreven in het Control Framework en meegewogen bij het bepalen van het restrisico, maar kunnen niet zelfstandig, als key beheersmaatregel het risico (gedeeltelijk) tot een aanvaardbaar niveau reduceren.

Resultaat processtap 1 t/m 5

De voorgaande processtappen leiden tot een ingevuld CFW met beheersdoelstellingen, risico's en beheersmaatregelen. De zorgaanbieder licht toe hoe het bruto risico wordt afgedicht en beschrijft in hoeverre het restrisico tot een aanvaardbaar niveau is gereduceerd. Van de beschreven beheersmaatregelen is het bestaan aangetoond.

Na het voor het eerst volledig doorlopen van stap 5 (inclusief beoordeling van bestaan van de beheersmaatregelen) is de zorgaanbieder over op Horizontaal Toezicht. Hierover ontvangt de zorgaanbieder een bevestigingsbrief van de representerend verzekeraar. Zorgaanbieder en representerend verzekeraar bepalen gezamenlijk vanaf welke periode de zorgaanbieder zich verantwoordt o.b.v. Horizontaal Toezicht.

EENMALIG TIJDENS IMPLEMENTATIEFASE

Rol zorgaanbieder
- Beoordeling bestaan beheersmaatregelen: Het aantonen van het bestaan van de beheersmaatregelen op de midden, hoge en IT risico's in het CFW. Bij eventuele bevindingen ten aanzien van het bestaan van de beheersmaatregelen op de midden en hoge risico's wordt de impact hiervan bepaald en wordt dit besproken met de representerend verzekeraar. Indien nodig en mogelijk worden aanvullende werkzaamheden uitgevoerd.

Rol representerend verzekeraar
- De representerende verzekeraar beoordeelt inhoudelijk het bestaan de beheersmaatregelen.
- In het Topmemo worden de conclusies op hoofdlijnen vermeld.

Rol tweede verzekeraar
- Beoordeling van de oordeelsvorming van de representerend verzekeraar ten aanzien van bestaan van de beheersmaatregelen. Hiervoor wordt het oordeel van de representerend verzekeraar bij een aantal hoge en midden risico's beoordeeld op navolgbaarheid. Afstemming met representerend verzekeraar over eventuele bevindingen en aanvullende beheersmaatregelen.
  Doel: go/no go van tweede verzekeraar.
- Vastlegging go/no go in dossier.

IEDER VERANTWOORDINGSJAAR

Rol zorgaanbieder
- De beheersmaatregelen toetsen op toereikendheid.
- Toelichten hoe met de beheersmaatregelen de midden en hoog geclassificeerde risico's het (bruto) risico is afgedekt en beschrijven in hoeverre het restrisico beheerst is.
- Indien de beheersmaatregelen in opzet het risico niet in voldoende mate afdekken, dan wordt beschreven hoe dit restrisico terug gebracht wordt tot een aanvaardbaar niveau door middel van gegevensgerichte werkzaamheden, zie hiervoor tevens hoofdstuk 6.

Rol representerend verzekeraar
- Inhoudelijke beoordeling of beheersmaatregelen voor midden en hoge risico's in opzet voldoende zijn om risico af te dichten.
- Beoordelen van restrisico en vaststellen of dit beheerst is, danwel op een andere wijze tot een aanvaardbaar niveau wordt gereduceerd.
- In het Topmemo worden de conclusies op hoofdlijnen vermeld.

Rol tweede verzekeraar
- Beoordeling van oordeelsvorming van de representerend verzekeraar ten aanzien van de opzet en de toereikendheid van de beheersmaatregelen. Hiervoor wordt het oordeel van de representerend verzekeraar bij een aantal hoge en midden risico's beoordeeld op navolgbaarheid.

6 Verantwoorden over opzet, bestaan en werking

Zorgaanbieders en verzekeraars hebben een gezamenlijke ketenverantwoordelijkheid voor de verantwoording van de zorgkosten. Dat betekent dat alle partijen (ook de toezichthouder NZa) moeten kunnen steunen op de werkzaamheden die in de gehele keten worden uitgevoerd.

Hiervoor wordt in een verantwoordingsjaar binnen Horizontaal Toezicht het bestaan en werking van de beheersing vastgesteld. Daarnaast worden (waar nodig of gewenst) gegevensgerichte werkzaamheden uitgevoerd. Om de werkzaamheden vast te leggen, wordt een controleplan opgesteld.

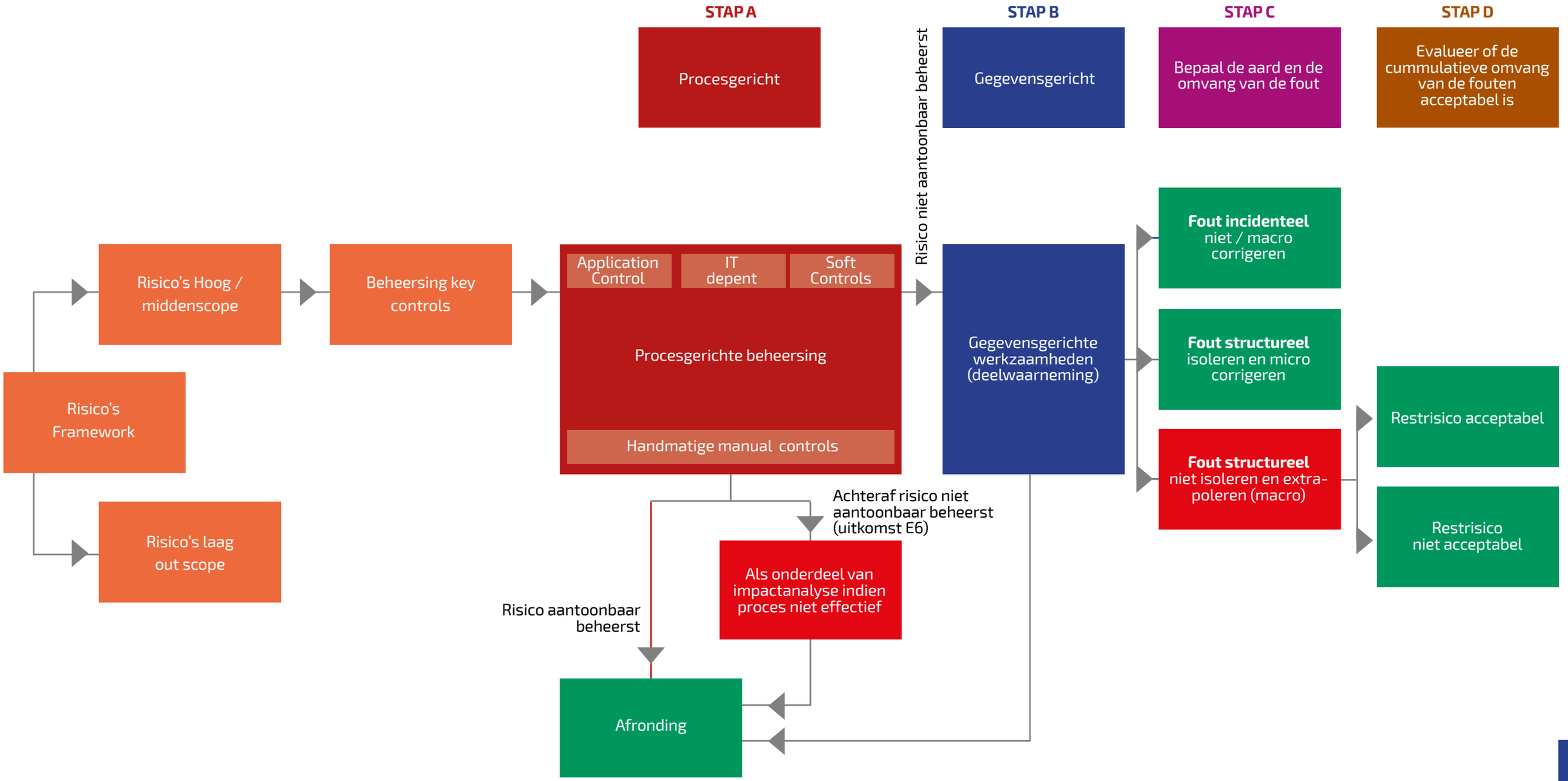
Opstellen Controleplan

De zorgaanbieder stelt een controleplan op met daarin opgenomen:

1 hoe de opzet & bestaan van beheersmaatregelen is vastgesteld (zie processtap 5)
2 hoe de werking van beheersmaatregelen gedurende het jaar getoetst wordt.
3 hoe de gegevensgerichte werkzaamheden worden uitgevoerd en hoe hierbij omgegaan wordt met verschillende soorten gevonden fouten

Dit controleplan wordt afgestemd met de representerend verzekeraar.

De zorgaanbieder stelt conform de afspraken uit het controleplan het bestaan van de beheersmaatregelen vast en toetst de werking op basis van de hierna stappen A t/m D uit de proces flow, zie volgende pagina.



Groene stappen leiden tot afronding.

Periodieke verantwoording

Periodiek en bij voorkeur per kwartaal rapporteert de zorgaanbieder aan de verzekeraar over de voortgang van het controleplan, de eventuele bevindingen die hieruit voortkomen en hoe bevindingen worden opgevolgd. Zorgaanbieder en verzekeraar bespreken deze rapportage samen door. Bestaan en werking van de key-beheersmaatregelen zijn minimaal onderdeel van deze HT verantwoording.

Periodiciteit in aantonen beheersmaatregelen

Indien de werking van beheersmaatregelen twee jaar op een rij is vastgesteld en de controle-omgeving stabiel is, stemt de zorgaanbieder met de representerende zorgverzekeraar of het jaarlijks aantonen van de werking van een beheersmaatregel kan worden gewijzigd naar eens in de twee of drie jaar. Dit geldt voor zowel de midden als de hoge risico's. Wel moet dan gemonitord worden of er geen veranderingen, signalen of andere invloeden zijn die de aannames verstoren. Als dat zich voordoet kan er aanleiding bestaan dat er alsnog tussentijds getoetst moet worden (afhankelijk van aard en impact van de verandering). Partijen worden opgeroepen om de mogelijkheid van het aanbrengen van periodiciteit ook daadwerkelijk te benutten.

Procesgericht (stap A)

Bij stap A kan gebruik gemaakt worden van de richtlijnen in het kader op de volgende pagina.

Nieuwe risico's en vaststelling CFW

Wanneer de zorgaanbieder gedurende het jaar een nieuw risico constateert dat geen onderdeel uitmaakt van het vastgestelde CFW maakt de zorgaanbieder in eerste instantie een inschatting van het risico. Wanneer het risico wordt ingeschat als midden of hoog, zal de zorg-aanbieder een impactanalyse maken. Afhankelijk van de omvang van de impact overlegt de zorgaanbieder aan de zorgverzekeraar de vervolg werkzaamheden. Voor het volgende jaar zal het risico worden opgenomen in het CFW en worden voorzien van passende beheersmaatregelen die het risico in voldoende mate mitigeren.

Als de zorgaanbieder de werking van de beheersmaatregelen op de (door de zorgaanbieder en zorgverzekeraar gezamenlijk) vooraf geïdentificeerde risico's aantoont, conform de gedefinieerde beheersmaatregelen in het Control Framework, dan is de beheersing ten aanzien van de rechtmatigheid voor dat jaar toereikend. Aandachtspunten m.b.t. de toereikendheid van beheersmaatregelen bij het vastgestelde Control Framework moeten voor het volgende jaar worden betrokken en hebben geen consequenties voor de beheersing van het lopende jaar.

Richtlijnen aantonen werking beheersmaatregelen (stap A)

Werking application controls
De werking van application controls wordt eenmaal per verantwoordingsjaar aangetoond ('test-of-one'; positief en negatief), onder de voorwaarde dat de ITGC's gedurende het gehele jaar aantoonbaar hebben gewerkt en de control(s) inhoudelijk niet zijn gewijzigd. Indien de ITGC's niet (aantoonbaar) gedurende het gehele jaar hebben gewerkt, dient de werking van de application controls op een andere wijze te worden aangetoond. Dit kan via een data-analyse en/of door middel van het gebruik van de frequentietabel hieronder.

Werking IT dependent controls
De werking van IT dependent controls kan worden aangetoond via een data-analyse en/of door middel van het gebruik van de frequentietabel hieronder. Hierbij wordt ook gekeken naar het geautomatiseerde deel van de beheersmaatregel (bv. naar de query).

Werking handmatige beheersmaatregelen
De werking van handmatige beheersmaatregelen kan worden aangetoond via een data-analyse en/of door middel van het gebruik van de frequentietabel hieronder

Werking ITGC's
De werking van ITGC's kan worden aangetoond door middel van data-analyse en/of door middel van de frequentietabel hieronder. Daarnaast wordt verwezen naar het handvat ITGC's (bijlage 2), voor verdere uitleg.

Frequentie maatregel	Omvang deelwaarneming op jaarbasis
(Meer dan) Dagelijks	25
Wekelijks	5
Maandelijks	2
Kwartaalbasis	2
Jaarlijks	1

Deze aantallen zijn evenredig verdeeld over het jaar.

Impactanalyse beheersmaatregelen en ITGC's

Indien (enige) onregelmatigheden geconstateerd zijn in de werking van de beheersmaatregelen dan moet de impact hiervan op het restrisico worden beoordeeld door de zorgaanbieder. De zorgaanbieder voert een impact-analyse uit. In deze analyse bepaalt de zorgaanbieder op basis van de impact of en welke vervolgwerkzaamheden worden uitgevoerd. De zorgaanbieder stemt de impactanalyse af met de zorgverzekeraar.

Voor de ITGC's kan de impact van een bevinding ten aanzien de effectiviteit worden bepaald door het pad uit het schema uit Stap 4 (onder ITGC's) in omgekeerde volgorde te doorlopen. Wanneer blijkt dat een ITGC niet optimaal functioneert, beoordeelt de zorgaanbieder of dit effect heeft op de beheersing van het IT-risico. In dat geval moet gekeken worden of met compenserende maatregelen de betrouwbaarheid van de beheersmaatregelen die afhankelijk zijn van dit IT risico alsnog kan worden vastgesteld. Als dit niet mogelijk is dan wordt het betreffende IT-risico niet voldoende beheerst. Dit betekent dat niet gesteund kan worden op de geformuleerde application control of IT-dependent control voor het risico. De zorgaanbieder bepaalt de impact van het niet kunnen steunen op de betreffende beheersmaatregelen en treedt in overleg met de zorgverzekeraar over deze impact en wanneer van toepassing welke compenserende maatregelen getroffen kunnen worden.

Op restrisico's die (nog steeds) als laag worden ingeschat, hoeven geen aanvullende gegevensgerichte werkzaamheden worden uitgevoerd. Op restrisico's die als 'niet als laag' worden ingeschat, zijn compenserende gegevensgerichte werkzaamheden gewenst.

De term 'restrisico' moet niet verward worden met de term 'laag bruto risico' die voortkomt uit de risicoanalyse. Voor de lage bruto risico's uit de risicoanalyse geldt dat, gegeven een bepaald minimaal volwassenheids-niveau, dit in voldoende mate wordt ondervangen in de bedrijfsvoering van de zorgaanbieders. De elementen hiervoor zijn opgenomen in het instapmodel.

Gegevensgericht (stap B)

De zorgaanbieder heeft gekozen voor gegevensgerichte werkzaamheden in de volgende gevallen:
1 bij ontoereikende beheersmaatregelen
2 als dit qua aantonen werking efficiënter is dan procesgericht
3 als blijkt dat werking niet effectief is (impactanalyse).

Indien er risico's zijn die niet of niet volledig beheerst worden, beoordeelt de zorgaanbieder middels gegevensgerichte werkzaamheden of de juiste keuzes zijn gemaakt in de registratie.

Gegevensgerichte werkzaamheden kunnen er toe leiden dat er fouten worden gesignaleerd, waar vervolgens naar de aard van de fout en de omvang die deze fout/onrechtmatigheid bepaald zou moeten worden. Om de juiste impact aan een fout/onrechtmatigheid te kunnen geven is het in beginsel alleen mogelijk om deze gegevensgerichte werkzaamheden uit te voeren op gefactureerde massa. Bij het uitvoeren van gegevensgerichte werkzaamheden gebeurt dit op basis van de aantallen opgenomen in kader

op de volgende pagina.

Gegevensgerichte werkzaamheden

Bij gegevensgerichte werkzaamheden is er de mogelijkheid om te kiezen voor integrale controle/data analyse of deelwaarneming.
Voor het bepalen van de omvang van de deelwaarneming, ten behoeve van de tweedelijns werkzaamheden, moet onderscheid gemaakt worden tussen deelwaaneming op hoge risico's of deelwaarneming op midden risico's.

- Hoge risico's: Voor hoge risico's is het uitgangspunt dat een deelwaarneming op 10% van het aantal items van de risicogerichte massa wordt uitgevoerd, met een minimum van 25 items en een maximum van 250 items per jaar.
- Midden risico's: Voor midden risico's wordt volstaan met een deelwaarneming op 10% van het aantal items van de risicogerichte massa met een minimum van 25 items en een maximum van 100 items per jaar.

Risico's die al deels wordt gemitigeerd door beheersmaatregelen kunnen zorgaanbieder en zorgverzekeraar onderling besluiten om het aantal te beoordelen regels te verlagen.

Andere manier om beheersing gegevensgericht aan te tonen

Op dit moment wordt binnen HT (logischerwijs) vooral de focus gelegd op beheersmaatregelen waarvan ook de werking kan worden aangetoond. Er is ruimte om te kijken naar beheersmaatregelen die meer preventief van aard zijn of meer gericht op de soft controls. Bijvoorbeeld instructies aan zorgprofessionals, opleidingen, aandacht vanuit management, etc.

Dit kan bijvoorbeeld via data-analyses, monitoringsinformatie of benchmarks of via bijvoorbeeld gesproken KPI's. Het bepalen van de norm voor een dergelijke monitor gebeurt in onderlinge afstemming tussen zorgaanbieder en zorgverzekeraar.

Gegevensgerichte werkzaamheden uit het verleden

Indien het risico wordt gemitigeerd door andere beheersmaatregelen en-/of resultaten uit het verleden, dan kunnen deze worden meegenomen in de afweging van de gegevensgerichte werkzaamheden. Zorgaanbieder en zorgverzekeraar kunnen dan onderling besluiten om het aantal regels van de deelwaarneming hierop te verlagen.

Bepaal de aard van de fout en de omvang (stap C)

Het gaat binnen HT primair om het 'in control zijn' en het 'continue verbeteren'. Geconstateerde tekortkomingen en/of fouten leiden dus primair tot het inrichten van een adequate verbetercyclus. Binnen HT is het sanctioneren van het verleden geen doel op zich. De primaire doelstelling is het aantonen van de aanwezige beheersing. Het is wel zo, dat áls er fouten worden aangetroffen, het logisch is – en in lijn met het Controleprotocol Zvw en het memo bestuurlijke commissie HT omgaan met deelwaarnemingen binnen HT (zie bijlage 3) – om geconstateerde fouten binnen het HT-proces te corrigeren voor het lopende verantwoordingsjaar.

Binnen Horizontaal Toezicht wordt een onderscheid gemaakt in 3 soorten fouten bij gegevensgerichte werkzaamheden uitgevoerd op de gefactureerde massa van het controle jaar. Deze worden hieronder nader toegelicht:

1 De geconstateerde fout is op basis van de impactanalyse incidenteel. Uit de impactanalyse moet blijken dat de fout incidenteel van aard is. De gevonden (incidentele) fout wordt gecorrigeerd. Daarmee is de bevinding in voldoende mate opgevolgd en hoeft de gecorrigeerde fout niet opgenomen te worden in de foutentabel (financiële bijlage van HT).
2 De geconstateerde fout is op basis van de impact-analyse structureel. De zorgaanbieder heeft de mogelijkheid om de structurele fout te isoleren, bijvoorbeeld via een bestandsanalyse, en corrigeert de geïsoleerde fout. Daarmee is de bevinding in voldoende mate opgevolgd en hoeft de gecorrigeerde fout niet opgenomen te worden in de foutentabel.
3 De geconstateerde fout is op basis van de impactanalyse structureel, maar de zorgaanbieder kan deze door de aard van de fout niet isoleren. Deze fout

kan niet geïsoleerd worden en moet worden geëxtrapoleerd om de totale onrechtmatigheid in de massa te bepalen.

Evalueer of de cumulatieve omvang van de fouten acceptabel is (stap D)

De geëxtrapoleerde fouten zijn weliswaar onrechtmatig maar hoeven niet in alle gevallen als zodanig te worden verwerkt/afgerekend en tevens niet als 'onrechtmatig' in de foutentabel te worden opgenomen.

Deze ruimte kan mogelijk volgens de NZa worden geboden indien de totale beheersing bij de zorgaanbieder overwegend adequaat is ingericht en werkt en daarnaast een voldoende verbetercyclus is ingericht (zie ook het memo bestuurlijke commissie HT omgaan met deelwaarnemingen binnen HT zoals ook opgenomen in bijlage 3). Het is echter niet toegestaan om dit te relateren aan de materialiteit die de accountants van zorgverzekeraar hanteren voor de (financiële) verantwoordingen. Afspraken hierover worden aan de lokale tafel gemaakt.

Samenvattend de uitgangspunten acceptabel restrisico

1 Acceptabel restrisico is voorwaardelijk en gekoppeld aan de totale beheersing en verbetermaatregelen
2 Doel is bewegingsruimte zonder afbreuk te doen aan stimulans om constant te verbeteren.
3 Heeft geen invloed op de risico analyse die wordt uitgevoerd door zorgaanbieders.
4 Heeft geen invloed op de omvang van werkzaamheden die de zorgaanbieder uitgevoerd heeft.

Assurance

De doelstelling van assurance is om het onderlinge vertrouwen te versterken en een bepaalde mate van zekerheid te geven voor de andere stakeholders (zoals NZa, verzekeraars en accountants van verzekeraars)

Een assurance rapport geeft een redelijke mate van zekerheid over opzet, bestaan en werking van de ITGC's en de afgesproken beheersmaatregelen in het CFW, met betrekking tot hoge en midden risico's;

- Op een afgesproken tijdstip (ISAE 3000 type 1), of;
- Over een afgesproken werkingsperiode (ISAE 3000 type 2).

In dit document wordt gesproken over een type 1 en type 2 rapportage.

Met een type 1 rapportage wordt een rapportage ten aanzien van 'bestaan' bedoeld en met een type 2 rapportage wordt een rapportage ten aanzien van 'bestaan en werking' bedoeld.

Type 1

De assurance provider kan in de implementatiefase van HT worden betrokken bij het geven van assurance over opzet en bestaan van ITGC's, middels een ISAE 3000 type 1 verklaring. In overleg met representerend verzekeraar, kan dit ook op andere manieren, dan middels een type 1 verklaring.

Type 2

De assurance provider geeft in de verantwoordingsfase van HT een ISAE 3000 type 2 verklaring af over bestaan en werking van de afgesproken ITGC's en beheersmaatregelen in het CFW. Om beter gebruik te maken van de expertise van verschillende partijen, wordt hierbij niet meer standaard uitgegaan van de beheersmaatregelen gekoppeld aan de hoge risico's. In het bilaterale overleg tussen de zorgaanbieder en de representerend zorgverzekeraar worden deze beheersmaatregelen afgestemd, waarbij minimaal bestaan en werking van de ITGC's wordt meegenomen in de ISAE 3000 type 2 verklaring. Het is van belang om in gezamenlijk overleg te komen tot een goede scope van de werkzaamheden van de assurance provider.

Assurance in de keten

- De zorgaanbieder en verzekeraar schatten samen de risico's in op hoog, midden of laag (processtap 3) en kijken gezamenlijk naar de opzet van de beheersmaatregelen (processtap 5). In deze fases is er geen accountantscontrole.

- De toereikendheid van de opzet van de beheersmaatregelen in het CFW wordt in onderling overleg tussen de representerend verzekeraar en de zorgaanbieder vastgesteld.

- De verplichting voor een type 1 verklaring vervalt. Het is de verantwoordelijkheid van de zorgaanbieder om opzet en bestaan van de ITGC's aan te tonen. Dit mag via een type 1 verklaring, maar dit kan ook op andere manieren. De representerende zorgverzekeraar en de zorgaanbieder maken hierover samen afspraken.

- De representerend verzekeraar beoordeelt bestaan en werking van de beheersmaatregelen op de midden en hoge risico's.

- De type 2 verklaring wordt voor de eerste 2 HT-verantwoordingsjaren verplicht. Daarna wordt de type 2 verklaring iedere 3 jaar uitgevoerd (ervan uitgaande dat in de eerste twee verantwoordingsjaren de beheersing in voldoende mate heeft gewerkt). In het bilaterale HT-overleg tussen de representerende zorgverzekeraar en de zorgaanbieder kan in afwijking hiervan worden besloten dat deze type 2 verklaring van de externe accountant niet meer nodig is, omdat de derde lijn van de zorgaanbieder van voldoende kwaliteit is.

- Er is een handvat beschikbaar om de volwassenheid van de derde lijn te kunnen vaststellen. Dit handvat kan door zorgaanbieders en zorgverzekeraars in onderling overleg gebruikt worden om te bepalen in welke mate de derde lijn ingezet kan worden en wat dit betekent voor de controlewerkzaamheden.

- De ontwikkeling en de inzet van de assurance provider binnen horizontaal toezicht zal aandacht behouden van alle betrokken partijen. Dit om te blijven werken aan de optimale mix tussen zekerheid, kosten, werkzaamheden en ketenoptimalisatie.

Rol zorgaanbieder

- Stelt jaarlijks controleplan op met daarin opgenomen hoe bestaan en werking gedurende het jaar wordt getoetst.
- Stemt controleplan af met representerend verzekeraar
- Toont bestaan en werking van de beheersmaatregelen op de midden, hoge en IT risico's in het CFW aan en voert gegevensgerichte werkzaamheden uit conform controleplan/CFW HT.
- Rapporteert periodiek, bij voorkeur per kwartaal, over voortgang en evt. controlebevindingen aan representerend verzekeraar.

Rol Representerend verzekeraar

- Beoordeelt controleplan en vult, waar nodig, aan.
- Beoordeelt bestaan & werking van nieuwe en/of aangepaste beheersmaatregelen t.o.v. vorig HT jaar.
- Beoordeelt werking bestaande beheersmaatregelen
- Beoordeelt de (kwartaal)rapportage van de zorgaanbieder ten aanzien van bestaan en werking van de beheersmaatregelen op de midden en hoge risico's en bespreekt dit met de zorgaanbieder.
- In het Topmemo worden de conclusies op hoofdlijnen vermeld.

Rol tweede verzekeraar

- Beoordeelt oordeelsvorming van de representerend verzekeraar ten aanzien van de opzet, bestaan en werking van de beheersmaatregelen. Hiervoor wordt het oordeel van de representerend verzekeraar bij een aantal hoge en midden risico's beoordeeld op navolgbaarheid.

Jaarplanning

Het Horizontaal Toezicht CFW is een beheersingskader dat verankerd wordt in de planning & control cyclus van de zorgaanbieder en de verzekeraar. Jaarlijks keren de meeste activiteiten uit de stappen 0 t/m 6 terug. De benodigde capaciteit die gevraagd wordt zal voor een aantal activiteiten wel sterk afnemen naarmate zorgaanbieder en verzekeraar verder Horizontaal Toezicht ingroeien. Wanneer processen van het ene
op het andere jaar niet veranderen hoeft de opzet niet steeds opnieuw te worden beoordeeld. Ook de risico-classificatie zal steeds gemakkelijker worden.

Voor een voorbeeld van een jaarplanning zie “good practices”

Bijlagen

Bijlage 1 • Handvat volwassenheid derde lijn binnen HT
Bijlage 2 • Handvat IT General Controls en beheersmaatregelen met een IT-component
Bijlage 3 • Bestuurlijke afspraken deelwaarnemingen

Bijlage 1

Handvat volwassenheid derde lijn

Juli 2020

Inleiding

De meeste zorginstellingen die bezig zijn met HT beschikken over derdelijns auditfunctie. In het instapmodel HT (onderdeel 6 Intern Toezicht) wordt immers al getoetst in hoeverre een zorginstelling beschikt over een onafhankelijke derde lijn. De mate van volwassenheid van deze derdelijns functie bij zorginstellingen verschilt. In hoeverre binnen Horizontaal Toezicht gebruik gemaakt kan worden van de werkzaamheden van deze derde lijn van een zorgaanbieder hangt af van de mate van volwassenheid. Hoe meer volwassen de derde lijn van de zorginstelling is, hoe meer het werk van de zorgverzekeraar verschuift van eigen onderzoek naar een beoordeling van de rapportage.

Dit handvat is opgesteld om de volwassenheid van de derde lijn te kunnen vaststellen. Er zijn verschillende mogelijkheden waarbij gebruik gemaakt kan worden van de controlewerkzaamheden in de derde lijn:

1. Een tweede lijn van de zorgaanbieder die derdelijns werkzaamheden in het kader van HT uitvoert en in voldoende mate voldoet aan de minimale eisen (zie ad 1 en bijlagen A en B). Dit wordt aangeduid als een tweede lijn 'plus'. Een voorbeeld hiervan is een (business) controller of interne controleafdeling in een zorginstelling die in het kader van HT deelwaarnemingen uitvoert om de werking van de beheersmaatregelen aan te tonen. Onder deze categorie valt ook een derde lijn die niet aan de minimale eisen voldoet;
2. De derde lijn van de zorgaanbieder voldoet aan de minimale eisen (zie ad 2. en bijlagen A en B)[1];
3. De derde lijn voldoet volledig aan de normen COS 610 van de NBA voor het kunnen steunen op de derde lijn door de externe accountant;
4. De derde lijn beschikt over het certificaat kwaliteitstoetsing IIA/NBA.

Hoe volwassener de derde lijn van een zorginstelling is, hoe meer de representerende zorgverzekeraar gebruik kan maken van de werkzaamheden van de derde lijn. Dit betekent ook dat de zwaarte van het beoordelen van de HT-werkzaamheden van de derde lijn afneemt. In de onderstaande tabel is aangegeven voor de bovenstaande mogelijkheden welk scenario van toepassing kan zijn voor het beoordelen van de HT-werkzaamheden van de derde lijn door de representerende zorgverzekeraar:

Scenario	Inspectie	Review	Reperformance
1	v	v	v
2	v	v	
3	v		
4	v		

Toelichting:

Inspectie:	De representerende zorgverzekeraar bekijkt kritisch of de opzet en rapportage van de uitgevoerde werkzaamheden in orde is.
Review:	De representerende zorgverzekeraar beoordeelt de opzet, uitvoering en rapportage van de uitgevoerde werkzaamheden.
Reperformance:	De representerende zorgverzekeraar voert een bepaalde hoeveelheid uitgevoerde testen nogmaals uit en/of doet aanvullend eigen testen (indien noodzakelijk).

Indien blijkt dat de derde lijn niet (geheel) voldoet aan de minimale eisen van de IIA/NBA (scenario 1 en 2), dan zal de zorgverzekeraar een review doen op

1 Of een derde lijn onder 1 of 2 valt hangt af van de kwalitatieve beoordeling op basis van minimale eisen. De scheidslijn tussen 1 en 2 is niet zwart- wit en wordt in overleg tussen representerende zorgverzekeraar en zorginstelling bepaald.

de werkzaamheden van de tweede en derde lijn en eventueel aanvullend eigen onderzoek (inspectie en/of reperformance) om de restrisico's af te kunnen dekken.

Indien de derde lijn voldoet aan de COS 610, of een beschikt over een certificering van IIA/NBA (scenario 3 en 4), dan hoeft de zorgverzekeraar alleen een inspectie uit te voeren op de werkzaamheden van de derde lijn.

De omvang en diepgang van de werkzaamheden van de representerende zorgverzekeraar is afhankelijk van het oordeel over de kwaliteit en professionaliteit van de derde lijn. De zorgaanbieder en representerende zorgverzekeraar maken hierover onderling afspraken (maatwerk).

Ad 1. De tweede lijn voldoet in voldoende mate aan de minimale eisen (tweede lijn 'plus')
De tweedelijns audit (controle)-afdeling van een zorginstelling voldoet aan de minimaal te stellen eisen, als aan twee belangrijke voorwaarden wordt voldaan, te weten:
- Onafhankelijkheid[2] en objectiviteit;
- Vakbekwaamheid en beroepsmatige zorgvuldigheid.

Onder deze categorie valt ook een derde lijn die niet aan de minimale eisen voldoet genoemd onder Ad. 2.

Ad 2. De derde lijn van de zorginstelling voldoet aan de minimale eisen (maar niet aan de formele eisen van IIA-NBA).
De derde lijns-afdeling van een zorginstelling voldoet aan de minimaal te stellen eisen, als aan twee belangrijke voorwaarden wordt voldaan, te weten:
- Onafhankelijkheid en objectiviteit;
- Vakbekwaamheid en beroepsmatige zorgvuldigheid.

Toelichting ad 1. en 2.:
De zorginstelling stelt door middel van zelfreflectie vast in hoeverre aan de minimale eisen wordt voldaan. De uitkomsten hiervan worden met de zorgverzekeraars gedeeld.
Afhankelijk van de uitkomsten van de zelfreflectie kan de zorgverzekeraar bepalen in hoeverre op de werkzaamheden van de tweede e/o derde lijn kan worden gesteund en in welke mate/omvang reviewwerkzaamheden noodzakelijk zijn. Aanvullend kunnen de zorgverzekeraars eigen onderzoek doen om de restrisico's af te dekken (incl. reperformance). De uitwerking van deze afstemming met de zorgverzekeraar en het uitvoeren van de zelfreflectie is aangegeven in de bijlagen A en B.

Ad 3. De derde lijn voldoet volledig aan de normen COS 610 van de NBA
Als de accountant van de zorginstelling al beoordeeld heeft dat gesteund kan worden op de werkzaamheden van de derde lijn, omdat deze voldoet aan de COS 610 (paragraaf 15) van de NBA, of de zorginstelling kan aantonen dat zij voldoet aan de COS 610, is dit voldoende voor de beoordeling of de zorgverzekeraar gebruik kan maken van de werkzaamheden van de derde lijn.

Ad 4. De derde lijn beschikt over het certificaat kwaliteitstoetsing IIA/NBA
Indien de zorgaanbieder beschikt over het certificaat kwaliteitstoetsing, dan is het overleggen van het certificaat voldoende om te beoordelen of gebruik gemaakt kan worden van de werkzaamheden van de derde lijn.

2 Of een derde lijn onder 1 of 2 valt hangt af van de kwalitatieve beoordeling op basis van minimale eisen. De scheidslijn tussen 1 en 2 is niet zwart- wit en wordt in overleg tussen representerende zorgverzekeraar en zorginstelling bepaald.

Bijlage A: Kwaliteitskenmerken Interne Auditafdeling

De derde lijns-afdeling van een zorginstelling voldoet aan de minimaal te stellen eisen, als aan twee belangrijke voorwaarden wordt voldaan, te weten:

- Onafhankelijkheid en objectiviteit;
- Vakbekwaamheid en beroepsmatige zorgvuldigheid.

Dit is nader uitgewerkt in de IIA-standaarden.

1100 – Onafhankelijkheid en objectiviteit

1110 Organisatorische onafhankelijkheid
1120 Individuele objectiviteit

1200 – Vakbekwaamheid en beroepsmatige zorgvuldigheid

1210 Vakbekwaamheid
1220 Beroepsmatige zorgvuldigheid
` 1230 Voortdurende vaktechnische ontwikkeling.

De zorgaanbieder stelt jaarlijks vast in hoeverre aan bovenstaande eisen wordt voldaan (zelfreflectie). Dit kan op basis van de normen zoals aangegeven in bijlage B.
De zorgaanbieder kan per onderdeel een score aangeven:

- Onvoldoende
- Matig (niet aantoonbaar)
- Voldoende
- Goed

Deze bevindingen worden met de zorgverzekeraars gedeeld. De zorgverzekeraars kunnen mede op basis van deze zelfreflectie de volwassenheid van de derde lijns functie inschatten c.q. bepalen.
Het eindoordeel van de zorgverzekeraar is gebaseerd op:

- Beoordelen reflectie -documentatie
- Gesprekken/interview met de IA-afdeling
- Ervaring van de zorgverzekeraar met de producten van de IA-afdeling

Bijlage B

Norm	Toelichting	Uitleg	Noodzakelijkheid
1100 Onafhankelijkheid en objectiviteit	De internal auditfunctie moet onafhankelijk zijn en de internal auditors moeten objectief zijn bij het uitvoeren van hun werk	Onafhankelijkheid = vrij van bedreiging om onpartijdig de werkzaamheden te kunnen doen. Objectiviteit = onbevooroordeelde instelling	(te scoren onderdelen) Onbeperkte toegang tot het senior management en bestuur IA's maken hun oordeel niet ondergeschikt aan anderen
1110 Organisatorische onafhankelijkheid	• Rapporteren aan het juiste niveau • Jaarlijkse bevestigingen van de onafhankelijkheid door hoofd IA aan het bestuur	Hoofd IA rapporteert functioneel aan het bestuur 1111. Hoofd IA communiceert en werkt samen met het bestuur Risico: IA krijgt additionele rollen en verantwoordelijkheden	Acties vanuit het bestuur: • Goedkeuring IA-charter • Goedkeuring IA-plan • Toekennen budget • Ontvangen informatie over de uitvoering van de auditwerkzaamheden • Benoemen en ontslaan hoofd IA • Goedkeuren beloning hoofd IA • Informatie opvragen over het bestaan van ongewenste beperkingen ten aanzien van de reikwijdte en de middelen.
1120 Individuele objectiviteit	IA moeten een onpartijdige en onbevooroordeelde houding hebben (en belangenverstrengeling vermijden)	Risico: strijdig beroepsmatig of persoonlijk belang	• Geen (aantoonbare) mogelijke belangenverstrengeling

Norm		Toelichting	Uitleg	Noodzakelijkheid
	1130 **Aantasting van onafhankelijkheid of objectiviteit**		Risico's: • Persoonlijke belangen verstrengeling • Beperkingen in de reikwijdte • Beperking in toegang tot documenten • Beperking in personeel en middelen	Voorwaarden: • Niet uitvoeren van onderzoeken waar de IA in voorgaande jaren zelf verantwoordelijke voor was; • Geen audit over onderdelen waar de internal audit verantwoordelijk voor is • PS: Audit volgend op adviesdiensten is toegestaan
1200 **Vakbekwaamheid en beroepsmatige zorgvuldigheid**		De opdrachten moeten met vakbekwaamheid en beroepsmatig zorgvuldigheid worden uitgevoerd.		
	1210 **Vakbekwaamheid**	• Kennis • Vaardigheden • Overige competenties	Aandacht voor: • Lopende activiteiten • Trends • Ontwikkelingen	Aan te tonen door: • Vakinhoudelijke certificaten en kwalificaties

Norm		Toelichting	Uitleg	Noodzakelijkheid
	1220 Beroepsmatige zorgvuldigheid	Werkzaamheden uitvoeren met de zorg en vakmanschap die van een verstandige en bekwame IA verwacht worden		De IA houdt bij zijn werkzaamheden rekening met: **Professionele zorgvuldigheid** • De omvang van de werkzaamheden die nodig zijn voor het realiseren van de doelstelling • De relatieve complexiteit, materialiteit of heb belang van de audit onderwerkpen • De toepasselijkheid en doeltreffendheid van de processen van Governance • De waarschijnlijkheid van belangde fouten of niet naleving van wet- en regelgeving • De kosten van verhoogde zekerheid tegenover de mogelijke baten. **Beroepsmatige zorgvuldigheid** • Overwegen gebruik te maken van geautomatiseerde audithulpmiddelen • Bedacht zijn op belangrijke risico's • Beroepsmatig rekening houden met: - behoeften en verwachting van de opdrachtgevers -Betrekkelijke complexiteit en de omvang van de werkzaamheden
	1230 Voortdurende vaktechnische ontwikkeling	IA's moeten hun kennis, vaardigheden en overige competenties verbeteren via voortdurende vaktechnische ontwikkeling.		Aantoonbare voortdurende vaktechnische ontwikkeling • 1300 Programma voor kwaliteitsbewaking en –verbetering. PS: in het kader van HT niet nodig nader uit te werken

Bijlage 2

Handvat IT General Controls en beheersmaatregelen met een IT-component

September 2019

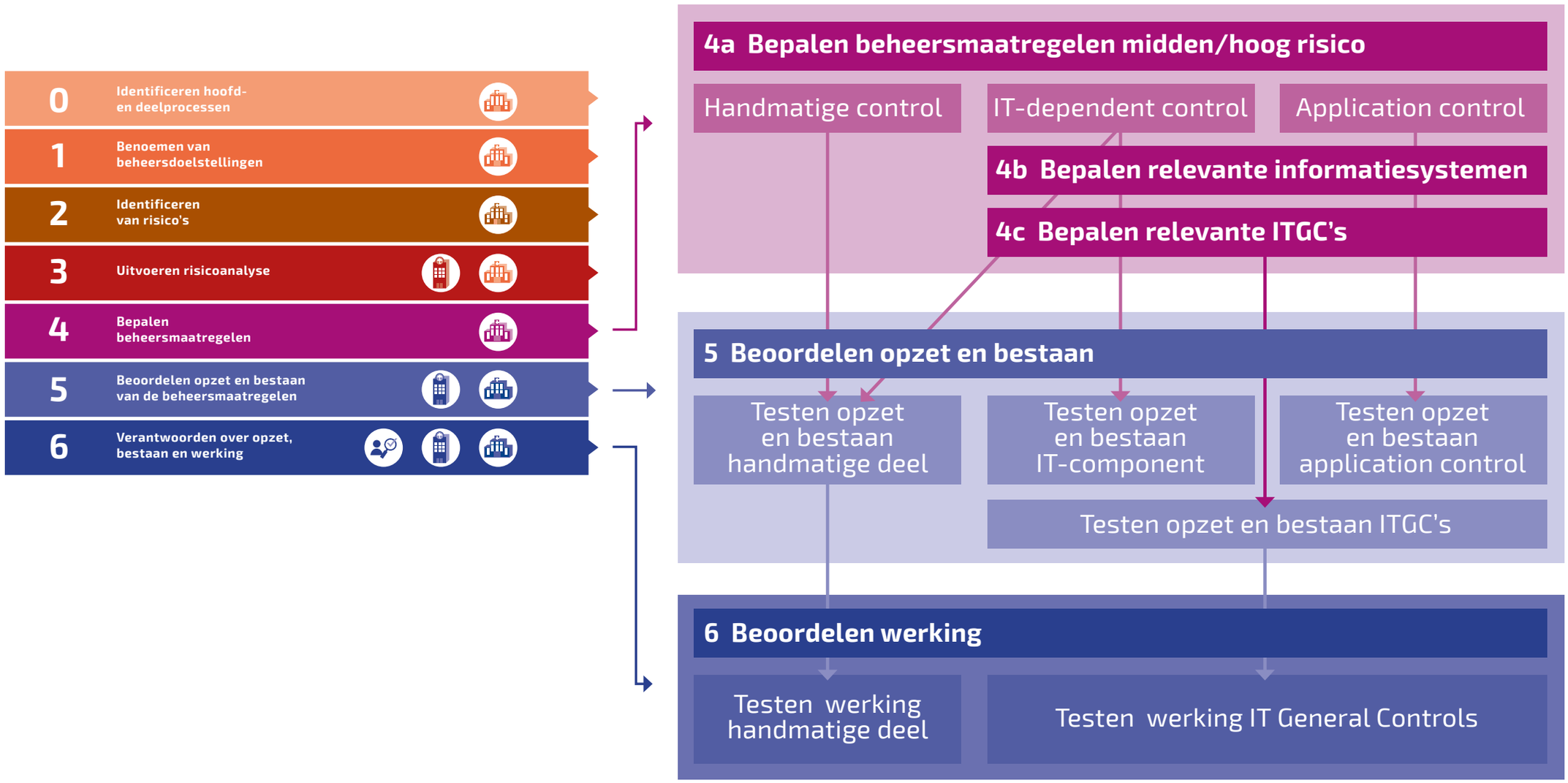
IT General Controls en beheersmaatregelen met een IT-component

Alle zorginstellingen maken gebruik van IT-systemen voor hun EPD, zorgregistratie en –facturatie. Dit betekent dat we in de praktijk altijd steunen op in deze systemen aanwezige beheersmaatregelen. Belangrijke beheersmaatregelen in de processen zijn (ingebouwde) functiescheiding, werklijsten en invoercontroles. Dit zijn de IT-dependent controls en application controls. Oftewel beheersmaatregelen met een IT-component.

Voorbeeld van een beheersmaatregel met een IT-component:
Werklijst: de IT component is het feit dat het ZIS automatisch dagelijks een lijst genereert met (mogelijk) foutieve registraties. De IT-component bestaat uit de definitie van wat er op de werklijst terecht moet komen en hoe vaak deze beschikbaar wordt gesteld.

Voordat we kunnen vaststellen of een beheersmaatregel met een IT-component werkt moet ook de basis voor deze beheersmaatregel goed zijn. Dit zijn de IT General Controls. IT General Controls (ITGC's) zijn vrij vertaald algemene beheersmaatregelen (zoals beleidslijnen en procedures) rond de IT-omgeving, die ervoor moeten zorgen dat beheersmaatregelen met een IT-component continu betrouwbaar werken. Triggers voor de ITGC's liggen niet in het proces dat binnen HT wordt gecontroleerd, waardoor deze beheersmaatregelen apart moeten worden toegevoegd aan het CFW.

Voorbeelden van ITGC's zijn:
1) Wanneer een wijziging wordt doorgevoerd in het systeem (bijvoorbeeld nieuwe wijze van berekening van een dagbesteding/dagverpleging) alleen deze methodiek van de software wordt gewijzigd en dat niet per ongeluk ook andere onderdelen worden aangepast met als gevolg dat verblijfsdagen niet meer worden geregistreerd (change management).
2) Alleen bevoegde medewerkers hebben toegang tot de IT-systemen. Bij het in- en uit dienst treden of wijzigen van functie moeten ook de rechten van deze medewerker worden aangepast om te voorkomen dat deze (nog steeds) consulten registreert (logische toegangsbeveiliging).


0 Identificeren hoofd- en deelprocessen
1 Benoemen van beheersdoelstellingen
2 Identificeren van risico's
3 Uitvoeren risicoanalyse
4 Bepalen beheersmaatregelen
5 Beoordelen opzet en bestaan van de beheersmaatregelen
6 Verantwoorden over opzet, bestaan en werking
4a Bepalen beheersmaatregelen midden/hoog risico
Handmatige control
IT-dependent control
Application control
4b Bepalen relevante informatiesystemen
4c Bepalen relevante ITGC's
5 Beoordelen opzet en bestaan
Testen opzet en bestaan handmatige deel
Testen opzet en bestaan IT-component
Testen opzet en bestaan application control
Testen opzet en bestaan ITGC's
6 Beoordelen werking
Testen werking handmatige deel
Testen werking IT General Controls

Anders dan bij de beheersing op de procesrisico's, zijn de ITGC's geen doel op zich, maar zijn zij ondersteunend aan de beheersing op de procesrisico's en vormen hiermee een belangrijke randvoorwaarde om te verantwoorden middels Horizontaal Toezicht. Terugkerende vraag bij ITGC's voor HT is: Welke ITGC's zijn nodig om te waarborgen dat de data in de IT-systemen betrouwbaar is en blijft. Indien voor de beheersing gesteund wordt op beheersmaatregelen met een IT-component dienen de relevante ITGC's te worden opgenomen in het Control Framework. De ITGC's processen die van belang zijn in het kader van HT zijn wijzigingsbeheer, logische toegangsbeveiliging en continuïteit.

Relevante IT-systemen in het kader van ITGC

In **stap 4** van het Control Framework (Bepalen beheersmaatregelen) bepaalt de zorgaanbieder welke maatregelen hij/zij treft om de geïdentificeerde risico's in het proces te beheersen.

Figuur 1: processtappen control framework

Er bestaan vier soorten beheersmaatregelen, zie onderstaand:

1. Handmatige controles: beheersmaatregelen die buiten de systemen om zijn ingericht;
2. IT-dependent controls: beheersmaatregelen waarbij gebruik wordt gemaakt van lijstwerk uit systemen (bijvoorbeeld controle aan de hand van signaleringslijsten);
3. Application controls: beheersmaatregelen ingebouwd in het systeem (bijvoorbeeld: verplicht in te vullen velden voor BSN);
4. Soft controls: beheersmaatregel die – meer dan hard controls – ingrijpt op c.q. appelleert aan het persoonlijk functioneren van medewerkers (overtuiging, persoonlijkheid). Soft controls zijn op te vatten als maatregelen die van invloed zijn op bijvoorbeeld de motivatie, loyaliteit, integriteit, inspiratie en normen en waarden van medewerkers.

Stap 4b: bepaal van elke beheersmaatregel in welke categorie (1 t/m 4) deze valt. Geef voor categorie 2 en 3 aan in welk informatiesysteem (bijvoorbeeld het EPD) de control is ingebouwd. De uitkomst hiervan is de scope qua informatiesystemen, waarvoor de ITGC's relevant zijn. Door op deze manier inzichtelijk te maken welke informatiesystemen en ITGC's (stap 4c) relevant zijn wordt tevens richting gegeven aan het bepalen van de impact op het risico in het geval van afwijkingen. Hierbij gaat het uiteindelijk om de vraag wat de impact is op het risico.

Systemen in scope voor HT

- EPD / ECD
- Eventueel aanvullende pakketten waarin initiële registratie van zorgactiviteiten met midden/hoog risico plaatsvindt, danwel die relevant zijn voor de rechtmatigheid van de zorguitgaven. Houdt hierbij rekening dat ook de betrouwbaarheid van de koppelingen (hoe weten we dat de gegevens volledig en correct overgaan van het ene systeem naar het andere) tussen de systemen.

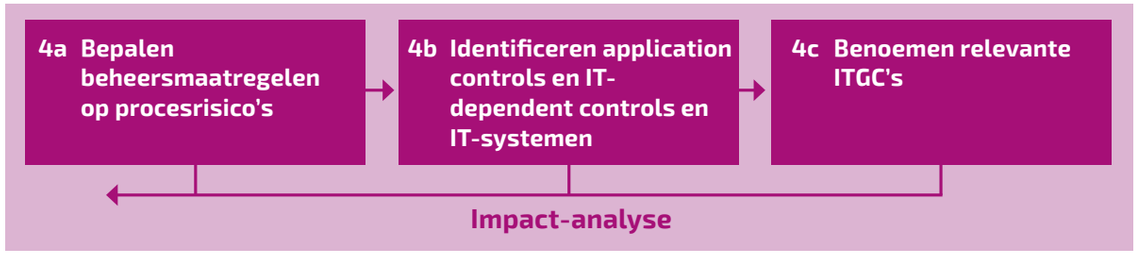
Lesson learned:
Of het datawarehouse in scope is voor ITGC is afhankelijk van het gebruik van het DWH in het kader van Horizontaal Toezicht en in hoeverre de betrouwbaarheid van de data wordt beheerst. Een voorbeeld van beheersing is dat de data in het DWH periodiek integraal wordt aangesloten met het EPD/ECD. Als hier voldoende op kan worden gesteund is het testen van de ITGC niet van toepassing. Het is dus per zorgaanbieder verschillend hoe hier mee om moet worden gegaan.

Stap 4c: bepaal welke ITGC's relevant zijn. Het uitgangspunt hierbij is dat de ITGC nodig zijn om te kunnen steunen op de beheersmaatregelen uit categorie 2 en 3 (zie stap 4a). De volgende ITGC's zullen altijd van toepassing zijn (opzet, bestaan en werking):

- Logische toegangsbeveiliging
- Wijzigingsbeheer

De ITGC continuïteit is in het kader van HT relevant, maar hoeft niet altijd op werking te worden getoetst. Dit wordt verderop nader toegelicht.

Impact-analyse



Het kan zijn dat er bevindingen zijn op de werking van de ITGC's. De zorgaanbieder gaat dan na in hoeverre gesteund kan worden op de application controls en IT-dependent controls. Niet alle bevindingen op ITGC's hebben een directe relatie met de beheersing op de procesrisico's en daarom is het belangrijk om de impact goed te bepalen. Voor de bevindingen die een effect hebben op de werking van de application controls en IT-dependent controls, dient de zorgaanbieder te bepalen of en in welke mate de beheersing wordt geraakt per procesrisico en welk effect dit heeft op het restrisico. Indien het restrisico te hoog blijft, dient de zorgaanbieder aanvullende werkzaamheden te doen om te komen tot een acceptabel restrisico.

Handreiking scope bepaling ITGC processen

Zoals in het control framework HT verwoord zijn IT general controls randvoorwaardelijk voor een betrouwbare werking van de application controls. Indien voor de beheersing gesteund wordt op application controls en/of IT dependent controls dienen de relevante IT General Controls (ITGC's) te worden opgenomen in het Control Framework. Hieronder volgt een handreiking ten aanzien van de scope van deze processen.

ITGC processen voor HT

De voor HT minimaal noodzakelijke General IT Controls bestaan uit 2 ITGC processen:

1. Toegangsbeveiliging
2. Wijzigingsbeheer

Toegangsbeveiliging

De toegangsbeveiliging bestaat uit fysieke toegangscontrole en logische toegangs-controle. Fysieke toegangsbeveiliging heeft tot doel dat er controle is op wie fysiek bijvoorbeeld bij de servers kan waarop persoonsgegevens zijn opgeslagen. Ten aanzien van logische toegangscontrole is van belang dat alleen een medewerker rechten heeft om bijvoorbeeld medische gegevens te verwerken (bijv. DBC's aanmaken) indien hij daarvoor rechten via een aanvraagproces heeft gekregen. Belangrijk hierbij zijn identificatie (wie wil toegang), authenticatie (is degene

wie hij zegt te zijn) en autorisatie (welke handelingen mag deze persoon verrichten). Logische toegangscontrole is dus een maatregel om te beheren wie toegang heeft tot gegevens en wat hij ermee mag doen.
De uitwerking van het beleid op toegangsrechten zal normaal gesproken bestaan uit:

- Procedure verkrijgen toegangsrechten. In deze procedure wordt geregeld hoe toegang verkregen kan worden tot de systemen cq gegevens (bijvoorbeeld via indiensttredingsprocedures) en op welke wijze het doorvoeren en beheersen van mutaties (zoals uitdiensttreding) in deze rechten is geregeld.
  In deze procedure zal minimaal uitgewerkt moeten zijn:
  - hoe toegang verkregen wordt bij indiensttreding (wie vraagt aan, wie geeft akkoord, wie voert door, periodieke check);
  - hoe mutaties in toegangsrechten worden beheerst (wie vraagt aan, wie geeft akkoord, wie voert door, periodieke check);
  - hoe toegang ingetrokken wordt bij uitdiensttreding en functiewijziging (wie is verantwoordelijk voor het doorvoeren van wijzigingen?); en
  - hoe periodieke review op (ruime) toegangsrechten is vorm gegeven (superusers/applicatiebeheerders).
- Autorisatiematrix. Hierin staan rechten beschreven en welke medewerkers welke rechten hebben en waarom.
  In deze procedure zal minimaal uitgewerkt moeten zijn hoe gezorgd wordt dat de autorisatie matrix actueel is en blijft (periodieke check, wie voert mutaties door).
- Authenticatiebeleid. Om authenticatie te borgen worden, in lijn met het wachtwoordbeleid, wachtwoorden toegekend. Daarnaast kan het voorkomen dat de instelling andere middelen voor authenticatie gebruikt (bedrijfstoegangspas, biometrische gegevens, etc.) In het wachtwoordbeleid worden de minimale eisen die gesteld worden aan wachtwoorden (lengte, complexiteit), alsmede de frequentie van wijzigen geregeld. Tevens wordt in het wachtwoordbeleid indien van toepassing single sign on en/of wachtwoordbeleid op netwerkniveau uitgewerkt. In deze procedure zal minimaal uitgewerkt moeten zijn de gestelde restricties ten aanzien van lengte, complexiteit, periodiek wijzigen en het bewaren van de wachtwoordhistorie en op welk niveau het wachtwoordbeleid is geregeld (applicatie niveau, netwerkniveau).

Voor HT wordt van een instelling verwacht dat bovenstaand beleid op toegangsrechten aantoonbaar is ingericht en functioneert. Fysieke toegangscontrole is gezien de beperkte impact op rechtmatig declareren geen onderdeel van de minimale eisen voor HT.

Wijzigingsbeheer
Het doel van wijzigingsbeheer is om gecontroleerd (zonder verstoringen) wijzigingen in systemen door te voeren waardoor de informatie in de systemen, alsmede bestaande functionaliteiten, betrouwbaar blijven en niet aangetast worden. De beheersingsdoelstellingen die hiermee samenhangen zijn:

- Wijzigingsaanvragen moeten zijn geautoriseerd op basis van geïdentificeerde risico's (uitgevoerde impact analyse);
- Wijzigingen worden juist, volledig en tijdig doorgevoerd;
- Bescherming tegen verstoringen door onjuiste wijzingen en door ontwikkel- en testactiviteiten.

De uitwerking van wijzigingsbeheer zal normaal gesproken bestaan uit een wijzigingsprocedure waarin bovenstaande beheersdoelstellingen zijn uitgewerkt. In deze procedure zal minimaal uitgewerkt moeten zijn hoe (en door wie) wijzigingen worden gemeld, hoe (en door wie) wijzigingen worden getest (inclusief procedure voor het documenteren van test werkzaamheden), hoe (en door wie) wijzigingen worden geaccordeerd en hoe (en door wie) wijzigingen worden gemonitord. Het aanwezig zijn van een separate test- en productieomgeving is hierbij een essentiële randvoorwaarde.

Voor HT wordt van een instelling verwacht dat bovenstaand beleid op wijzigingenbeheer aantoonbaar is ingericht en functioneert.

Overige ITGC processen
De overige ITGC processen zijn alleen van toepassing indien er zicht bijzondere situaties hebben voorgedaan of als er specifieke risico's in het CFW zijn opgenomen waar deze processen een belangrijke rol in spelen. Een voorbeeld van een bijzondere situatie is het terugzetten van een omvangrijke back up. Omdat dit een situatie is die zich mogelijk voor kan doen, wordt hieronder continuiteit in het kader van calamiteiten en beveiliging/integriteit van data nader toegelicht.
Continuïteit, met specifieke aandacht voor calamiteitenbeheer in relatie tot beveiliging/integriteit van data

Hoewel continuiteits management een breed IT beheer proces kan zijn, wordt voor HT primair het onderdeel calamiteitenbeheer relevant geacht. Immers, bij HT gaat het om rechtmatig declareren. De belangrijkste beheersdoelstelling voor HT is dat data niet onterecht wordt gewijzigd. Dit risico treedt alleen op wanneer er een back up wordt teruggeplaatst, waarmee (continue) beschikbaarheid van data (waar continuïteit primair op is gericht) minder relevant is. Daarnaast wordt gezien de aard van de primaire processen van zorginstellingen en de afhankelijkheid van IT daarbij continuïteitsmanagement geacht op orde te zijn (met als gevolg een laag risico op terug moeten zetten van back up).
Voor HT wordt van een instelling ten aanzien van calamiteitenbeheer minimaal verwacht dat in kaart gebracht wordt hoeveel calamiteiten zich in een jaar hebben voorgedaan en vastgesteld wordt in hoeverre die calamiteiten hebben geleid tot problemen van beveiliging/integriteit van data.

ITGC processen bij externe leveranciers

Bovenstaande uitwerking veronderstelt dat applicaties en beheer processen in eigen beheer zijn. Als sprake is van uitbestede applicaties en/of beheer processen, kan aan de beheersdoelstellingen worden voldaan door middel van een iSAE 3402 rapport van de externe service provider. In de bijlage 'Beoordeling ISAE3402' zijn de voorwaarden hiervoor uitgewerkt.

Lesson learned:
Hoewel de in deze notitie beschreven procedures en beleid een technisch karakter hebben en ziekenhuizen mogelijk geneigd zijn dit te beleggen bij de I(C)T afdeling, benadrukken wij het belang van de verantwoordelijkheden van de lijnorganisatie (bijvoorbeeld voor het bepalen van de inhoud van autorisatie matrices en het testen van voorgestelde systeemwijzigingen) en HR (bijvoorbeeld voor het inrichten van adequate in- en uitdienstprocedures) en dat deze organisatieonderdelen dus ook worden betrokken bij de ITGC's.

Lesson learned:
Veel instellingen zullen in het kader van privacy/AVG aandacht besteden aan data beveiliging; sluit hierbij zoveel mogelijk aan voor het onderdeel toegangsbeveiliging van de ITGC's.

Minimale set risico's en aandachtspunten voor beheersing

Dit overzicht bevat een lijst van de minimale risico's en aandachtspunten voor de beheersing waar aandacht aan moet worden besteed in het kader van Horizontaal Toezicht. De beschrijvingen moeten nog specifiek worden gemaakt voor de situatie van de zorgaanbieder. De kolom aandachtspunten beheersing bevat de voor HT belangrijkste elementen van beheersing die in de ITGC processen toegangsbeveiliging of wijzigingsbeheer worden geborgd.

No.	Beheersdoelstelling	Soort	Risico en oorzaken	Aandachtspunten beheersing
1	Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat de toegang tot programma's en data beheerst is ter voorkoming van ongeautoriseerd gebruik van de applicatie.	Toegangsbeveiliging	Ongeautoriseerde toegang tot applicaties (en daarmee mutatie in zorgactiviteiten, DBC-gegevens, etc.) is mogelijk doordat de wachtwoorden niet voorzien zijn van voldoende restricties ten aanzien van lengte, complexiteit, periodiek wijzigen en het bewaren van de wachtwoordhistorie.	De wachtwoorden (of andere authenticatie-middelen) voldoen aan de genoemde restricties en wachtwoordhistorie wordt bewaard.
2a	Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat de toegang tot programma's en data beheerst is ter voorkoming van ongeautoriseerd gebruik van de applicatie.	Toegangsbeveiliging	Ongeautoriseerde toegang tot applicaties (en daarmee mutatie in zorgactiviteiten, DBC-gegevens, etc.) is mogelijk doordat identititeitskenmerken zoals username en wachtwoord worden verstrekt aan de verkeerde personen.	Er dienen procedures voor het aanvragen/toekennen van autorisaties te zijn opgesteld en geïmplementeerd.
2b	Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat de toegang tot programma's en data beheerst is ter voorkoming van ongeautoriseerd gebruik van de applicatie.	Toegangsbeveiliging	Ongeautoriseerde toegang tot applicaties (en daarmee mutatie in zorgactiviteiten, DBC-gegevens, etc.) is mogelijk doordat identititeitskenmerken zoals username en wachtwoord worden verstrekt aan de verkeerde personen.	Er dienen procedures voor het muteren van autorisaties te zijn opgesteld en geïmplementeerd.
2c	Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat de toegang tot programma's en data beheerst is ter voorkoming van ongeautoriseerd gebruik van de applicatie.	Toegangsbeveiliging	Ongeautoriseerde toegang tot applicaties (en daarmee mutatie in zorgactiviteiten, DBC-gegevens, etc.) is mogelijk doordat identititeitskenmerken zoals username en wachtwoord worden verstrekt aan de verkeerde personen.	Er dienen procedures voor het intrekken van autorisaties te zijn opgesteld en geïmplementeerd.

No.	Beheersdoelstelling	Soort	Risico en oorzaken	Aandachtspunten beheersing
3	Beheersdoelstelling Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat de toegang tot programma's en data beheerst is ter voorkoming van ongeautoriseerd gebruik van de applicatie.	Toegangsbeveiliging	Acties van gebruikers en beheerders zijn niet te herleiden tot unieke natuurlijke personen, waardoor de oorzaak van onjuiste of onrechtmatige mutaties niet goed onderzocht kan worden.	- Voor het uitgeven en toezicht houden op beheerrechten dient een procedure te zijn opgesteld en geïmplementeerd. - Het gebruik van groepsaccounts is beperkt en conform de geldende procedure. - Logging is ingericht op kritische punten in de applicatie (bijvoorbeeld de mogelijkheid om beheersmaatregelen aan/uit te zetten of configuraties van beheersmaatregelen aan te passen).
4	Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat de toegang tot programma's en data beheerst is ter voorkoming van ongeautoriseerd gebruik van de applicatie.	Toegangsbeveiliging	Ongeautoriseerde toegang tot applicaties (en daarmee mutatie in zorgactiviteiten, DBC-gegevens, etc.) is mogelijk doordat toegangsrechten en autorisaties worden verstrekt aan de verkeerde personen.	- Er dienen procedures voor het aanvragen, toekennen, muteren en intrekken van autorisaties te zijn opgesteld en geïmplementeerd. - Periodiek (minimaal jaarlijks) dient een risico gerichte evaluatie op toegekende rechten plaats te vinden, waarbij minimaal de hoge toegangsrechten (rechten met de mogelijkheid om beheersmaatregelen aan/uit te zetten of configuraties van beheersmaatregelen aan te passen) worden geevalueerd. - De organisatie heeft een autorisatiematrix (soll situatie). Hierin staat beschreven welke medewerkers welke rechten hebben. Hierbij is het logisch dat voorafgaand aan het opstellen van de autorisatiematrix toetsing plaatsvindt (zoals bij functiescheiding). Aangezien dit een relatief nieuw onderwerp is, is toetsing mogelijk (nog) niet gedocumenteerd bij de zorgaanbieder en is mondelinge toelichting noodzakelijk. In de procedure rondom de autorisatiematrix wordt weergegeven hoe wordt geborgd dat de matrix actueel blijft en wie wijzingen kan doorvoeren.

No.	Beheersdoelstelling	Soort	Risico en oorzaken	Aandachtspunten beheersing
5	Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat de toegang tot programma's en data beheerst is ter voorkoming van ongeautoriseerd gebruik van de applicatie.	Toegangsbeveiliging	Ongeautoriseerde toegang tot applicaties (en daarmee mutatie in zorgactiviteiten, DBC-gegevens, etc.) is mogelijk doordat toegangsrechten en autorisaties niet (tijdig) worden aangepast bij veranderingen in de werkzaamheden van de medewerkers aan wie ze zijn toegekend.	- Er dienen procedures voor het aanvragen, toekennen, muteren en intrekken van autorisaties te zijn opgesteld en geïmplementeerd. - Er dienen werkzaamheden uitgevoerd te worden om vast te stellen dat rechten tijdig worden ingetrokken. - Periodiek (minimaal jaarlijks) dient een risico gerichte evaluatie op toegekende rechten plaats te vinden, waarbij minimaal de hoge toegangsrechten (= rechten die mogelijkheid geven om beheersmaatregelen aan/uit te zetten of toleranties aan te passen) worden geevalueerd. - Het aantal gebruikers met hoge rechten is beperkt tot personen die deze rechten uit hoofde van hun functie nodig hebben voor hun dagelijkse werkzaamheden.
6	Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat wijzigingen op een beheerste wijze worden doorgevoerd.	Wijzigingsbeheer	Wijzigingsaanvragen worden ongeautoriseerd en/of zonder impactanalyse doorgevoerd, waardoor verstoringen kunnen optreden.	- Alleen geautoriseerde wijzigingsverzoeken worden doorgevoerd. - Alleen wijzigingsverzoeken waar een impactanalyse is uitgevoerd worden doorgevoerd - Er is beleid t.a.v. spoedfixes beschreven
7	Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat wijzigingen op een beheerste wijze worden doorgevoerd.	Wijzigingsbeheer	Wijzingen worden niet juist en/of niet tijdig en/of niet volldig doorgevoerd, waardoor verstoringen kunnen optreden.	- Er is beleid beschreven t.a.v. het aanvragen, goedkeuren, testen en accepteren van wijzigingen. Hierin zijn o.a. beschreven de stappen van het wijzigingsbeheerproces: 1 Aanvraag 2 Autorisatie inzetten wijziging 3 Testing/goedkeuren testresultaten 4 Autorisatie in productie name 5 In productie name Tevens dient de werking van dit beleid (de procedures) aangetoond te worden.

No.	Beheersdoelstelling	Soort	Risico en oorzaken	Aandachtspunten beheersing
8	Beheersingsmaatregelen bieden een redelijke mate van zekerheid dat wijzigingen op een beheerste wijze worden doorgevoerd.	Wijzigingsbeheer	Organisatie is onvoldoende beschermd tegen verstoringen door onjuiste wijzigingen beschermd en/of ontwikkel- en testactiviteiten.	- Alleen geautoriseerde wijzigingsverzoeken worden doorgevoerd. - Alleen wijzigingsverzoeken waar een impactanalyse is uitgevoerd worden doorgevoerd - Er is beleid t.a.v. spoedfixes beschreven - Er is beleid beschreven t.a.v. het aanvragen, goedkeuren, testen en accepteren van wijzigingen. Hierin zijn o.a. beschreven de stappen van het wijzigingsbeheerproces: 1 Aanvraag 2 Autorisatie inzetten wijziging 3 Testing/goedkeuren testresultaten 4 Autorisatie in productie name 5 In productie name Tevens dient de werking van dit beleid (de procedures) aangetoond te worden.

Bijlage 3

Bestuurlijke afspraken deelwaarnemingen

Juni 2021

Inleiding

Met Horizontaal Toezicht dragen zorgaanbieders en zorgverzekeraars samen zorg voor een juiste besteding van de zorguitgaven. Vertrouwen is het fundament. En dat vertrouwen groeit door een gelijkwaardige samenwerking, wederzijdse transparantie en heldere communicatie. HT gaat niet over het sanctioneren van het verleden, maar over verbeteren richting de toekomst.

Binnen HT werken we samen om risico's op een procesgerichte manier te beheersen. Dit doen we zo dicht mogelijk op het zorgproces (dus voor in de keten) en goed ingebed in de IT-systemen. In één keer juist registreren en declareren staan centraal. HT is erop gericht om als zorgaanbieder zelf 'in control' te zijn en om 'continu te verbeteren'. Ook richt HT zich op een efficiënte verantwoordingsketen, met zo min mogelijk administratieve lasten voor alle partijen.

Zijn er binnen HT geconstateerde fouten en/of bevindingen, dan houdt de zorgaanbieder het proces kritisch tegen het licht en gaan we in gezamenlijkheid op zoek naar verbetermogelijkheden. Horizontaal Toezicht staat voor gezamenlijke analyse en focus op verbeteringen naar de toekomst. Tevens is binnen HT afgesproken dat de gevonden fouten en/of bevindingen geen impact meer zullen hebben op afgeronde (oude) jaren. Tot slot is afgesproken dat in het lopende HT-jaar gevonden fouten en/of bevindingen wél worden gecorrigeerd al dan niet financieel) én dat waar nodig naar aanleiding van die fouten en/of bevindingen het Control Framework van het aankomende HT-jaar wordt aangepast om fouten in toekomst te voorkomen.

Positie van deelwaarnemingen binnen HT

Zoals verwoord is binnen HT een procesgerichte manier van beheersen de aanpak voor het 'in control' zijn. Gegevensgerichte beheersing, zoals deelwaarnemingen, is in feite niet de beoogde HT-manier van beheersen. Soms spreken een zorgaanbieder en een representerende zorgverzekeraar echter toch vooraf af (in het Control Framework van de zorgaanbieder) dat een deelwaarneming wordt ingezet als vervangende of aanvullende beheersmaatregel. Er zijn twee mogelijke redenen hiervoor[1]:

- vooraf is vastgesteld dat het risico niet op een procesgerichte manier beheerst kan worden (en er daarmee geen sprake is van een acceptabel restrisico[2]), óf;
- vooraf is vastgesteld dat een procesgerichte manier van beheersen onevenredig veel werk (administratieve last) of extra kosten met zich meebrengt, waardoor een deelwaarneming de meeste efficiënte beheersmaatregel is.

Wanneer een deelwaarneming wordt ingezet, kan het gebeuren dat er een bevinding is in de deelwaarneming. Dan komt de logische vervolgvraag: hoe ga je in deze situatie de 'fout' voor het lopende HT-jaar corrigeren. Een 'fout' in een deelwaarneming kan immers een grotere fout in de massa illustreren.

Over de positie van deelwaarnemingen en hoe je omgaat met fouten in deelwaarnemingen heeft de NZa een brief gestuurd (d.d. 1 februari 2021, bijlage A). Daarin wordt uitgelegd hoe je in deze situatie kunt handelen. Bij een gevonden fout in een deelwaarneming maak je een impactanalyse (en eventueel verbeterplan). Onderdeel van de impactanalyse is de classificatie van de aangetroffen fout. Er zijn drie mogelijkheden:

1. De fout is incidenteel. De gevonden incidentele fout wordt gecorrigeerd en de bevinding is voldoende opgevolgd.
2. De fout is structureel, maar kan geïsoleerd worden. De geïsoleerde fouten worden gecorrigeerd.
3. De fout is structureel, maar kan niet geïsoleerd worden. Bij classificatie 3 geldt dat feitelijke fouten niet gevonden gaan worden en om die reden wordt dan, conform de brief van de NZa, de impact berekend door extrapolatie. De

1 Een deelwaarneming kan ook worden ingezet om te laten zien dat er sprake was van procesgerichte beheersing. Daar richt deze notitie zich niet op.
2 Voor de definitie van restrisico verwijzen wij naar het Control Framework 4.0.

grote vraag is dan of dat berekende bedrag in de impactanalyse ook afgerekend moet worden. De NZa geeft aan dat het beantwoorden van die vraag maatwerk vraagt en dat daarbij het totaalbeeld van de beheersing van de zorgaanbieder in ogenschouw moet worden genomen.

De bestuurlijke commissie benadrukt dat bij het interpreteren van de uitkomst van een deelwaarneming allereerst de focus moet liggen op verbetering van het proces om fouten in de toekomst te voorkomen. Laat met een verbeterplan zien hoe de kans op fouten in de toekomst aanzienlijk wordt verkleind en laat dit plan en de snelheid waarmee de verbeteringen worden opgepakt ook meewegen in de afspraken die je onderling maakt als zorgverzekeraar en zorgaanbieder over het lopende HT-jaar.

Als een representerende zorgverzekeraar en zorgaanbieder samen besluiten om niet financieel af te rekenen, wordt dit wederzijds bestempeld als een acceptabel restrisico. Bij een acceptabel restrisico hoeven de zorgverzekeraars volgens het Controleprotocol Zvw deze fout ook niet op te nemen in de foutentabel.

Besluit

De 4 branchepartijen, vertegenwoordigd in de bestuurlijke commissie HT, hebben aangegeven de inhoud van de NZa-brief te onderschrijven en deze inhoud ook op te zullen nemen in het Control Framework 4.0.

De bestuurlijke commissie heeft verder besloten dat afronding van de HT-verantwoording lokaal moet plaatsvinden (maatwerk). Er komen géén landelijke/generieke afspraken over bijvoorbeeld percentages of bandbreedtes wanneer wel of niet moet worden afgerekend.

Overwegingen

Wel geeft de bestuurlijke commissie HT de volgende overwegingen mee voor de lokale HT-tafel.

Leidende principes

De leidende principes van HT moeten ook op de lokale HT-tafel het startpunt zijn van het gesprek. Het is belangrijk om elkaar de ruimte te geven, samen deze principes te reflecteren op de lokale situatie en om goed naar elkaar te luisteren. Alleen dan kan het wederzijds vertrouwen groeien.

Constructieve dialoog over corrigeren

Corrigeren hoort ook bij HT. In ieder geval voor zover dit gaat over het lopende HT-jaar. Oude jaren vallen per definitie buiten schot, maar fouten in een lopend HT-jaar moet je corrigeren. Samen moeten we ervoor zorgen dat corrigeren niet persé iets ergs is, maar juist hoort bij de hygiëne van het 'in control' zijn. Wel of niet afrekenen van een berekende impact als gevolg van bevindingen in een deelwaarneming wordt aan de lokale HT-tafel via een constructieve dialoog bepaald.

Totaalbeeld van de organisatie

Zoals de NZa ook beschreef moet ook het totaalbeeld van de beheersing binnen een zorgaanbieder meegewogen worden. Hoe is het gesteld met de totale beheersing van de zorgaanbieder? Is dit een incident, of zijn er iteratieve bevindingen over de jaren heen? Hoe gaat een aanbieder om met bevindingen? Wat is de kwaliteit van totale beheersing? Is er sprake van monitoring? Hoe werkt de PDCA-cyclus? Etc.

Balans tussen maatwerk en uniform handelen

Het is belangrijk het tweezijdige karakter van HT-afspraken te benadrukken. Afspraken maak je samen en ook de consequenties van die afspraken draag je samen. Wanneer je dat vergeet kan maatwerk gaan voelen als een ongelijke behandeling. Zeker wanneer blijkt dat een andere aanbieder of een andere zorgverzekeraar een andere inhoudelijke afspraak heeft gemaakt. En aangezien het gras bij de buren altijd groener lijkt wanneer je je daarop focust, benadrukken wij vooral het belang van een goede focus op de eigen situatie en de onderlinge relatie en afspraken (lokaal maatwerk).

Bijlage A: Brief NZa over positie deelwaarnemingen in HT

Nederlandse Zorgautoriteit

De Nederlandse Federatie van Universitair Medische Centra
GGZ Nederland
Nederlandse Vereniging van ziekenhuizen
Zorgverzekeraars Nederland

In kopie aan APZ en Coziek

Newtonlaan 1-41
3584 BX Utrecht

Postbus 3017
3502 GA Utrecht

T 030 296 81 11
F 030 296 82 96
E info@nza.nl
I www.nza.nl

Behandeld door	Telefoonnummer	E-mailadres	Kenmerk
dhr. E. Langeveld	030 29 68 930	info@nza.nl	388848/823489

Onderwerp
Positie deelwaarnemingen binnen horizontaal toezicht (HT)

Datum
1 februari 2021

Geachte heer/mevrouw,

Binnen HT werken zorgaanbieders en zorgverzekeraars op basis van gefundeerd vertrouwen samen aan de rechtmatigheid van de zorguitgaven. Op 4 november 2019 hebben wij een brief gestuurd met onze standpunten over de beheersing van het Control Framework (CFW) binnen HT.

De deelnemende partijen hebben recent aangegeven behoefte te hebben aan een nadere duiding van de positie van deelwaarnemingen binnen de beheersing van het CFW. En vooral hoe om te gaan met geconstateerde fouten in deelwaarnemingen, mede in relatie tot het Controleprotocol Zvw van de NZa.

Visie NZa over beheersing binnen HT
Beheersing binnen HT vindt bij voorkeur plaats door processen en procedures aan de voorkant goed in te richten. Dit vindt zo vroeg mogelijk in de registratie- en declaratieketen plaats en is ingebed in de zorgprocessen, inclusief beheersing van relevante IT-systemen[1]. Hiermee staat het in één keer juist en tijdig registreren en declareren van rechtmatig geleverde zorg binnen HT centraal. Het gaat binnen HT primair om het 'in control zijn' en het 'continue verbeteren'. Geconstateerde tekortkoningen en/of fouten leiden dus primair tot het inrichten van een adequate verbetercyclus. Binnen HT is het sanctioneren van het verleden geen doel op zich, de primaire doelstelling is het aantonen van de aanwezige beheersing.

Positie deelwaarnemingen binnen HT
Het gebeurt in de praktijk frequent dat met de inzet van alleen een proces- en systeemgerichte aanpak de beheersing van één of meerdere risico's niet toereikend is en/of niet toereikend aangetoond kan worden. Dit leidt dan tot een niet aanvaardbaar restrisico, dat met behulp van zogenaamde gegevensgerichte werkzaamheden, bijvoorbeeld een

[1] Om te kunnen steunen op de werking van in de systemen opgenomen geprogrammeerde controles (application controls) zijn ook de general it controls (GITC's) van belang.

deelwaarneming[2], afgedekt wordt of gemitigeerd wordt tot een wel aanvaardbaar restrisico.

Omgang met fouten in deelwaarnemingen
Het is, zoals eerder gezegd, geen zelfstandig doel om fouten op te sporen. Het is wel zo, dat áls er fouten worden aangetroffen, het logisch is – en in lijn met het Controleprotocol Zvw – om geconstateerde fouten binnen het HT-proces te corrigeren voor het lopende verantwoordingsjaar[3].

In het Controleprotocol Zvw is in paragraaf 2.6 onder andere opgenomen dat:

- *Gevonden fouten over het desbetreffende verantwoordingsjaar moeten worden gecorrigeerd.*
- *Indien de werking van de bepaalde beheersingsmaatregelen op de Midden en Hoge risico's in onvoldoende mate kan worden aangetoond, maakt de zorginstelling een impact-analyse. In deze analyse bepaalt de zorgaanbieder op basis van de impact of en welke vervolgwerkzaamheden worden uitgevoerd.*
- *Als er sprake is van acceptabele restrisico's (geen of laag restrisico) neemt de zorgverzekeraar geen fout of onzekerheid op zijn foutentabel.*

Mochten er fouten ontdekt worden in een deelwaarneming, dan dient de impact van die fout in kaart te worden gebracht. De zorgaanbieder bepaalt op basis van de aard en omvang van de aangetroffen fout de opzet en inhoud van de impact-analyse. Als onderdeel van de impactanalyse dient ook een classificatie van de aangetroffen fout plaats te vinden.

Wij zien drie mogelijkheden:

- De geconstateerde fout is op basis van de impactanalyse incidenteel. Uit de impactanalyse moet blijken dat de fout incidenteel van aard is. De gevonden (incidentele) fout wordt gecorrigeerd. Daarmee is de bevinding in voldoende mate opgevolgd en hoeft de gecorrigeerde fout niet opgenomen te worden in de foutentabel.

- De geconstateerde fout is op basis van de impact-analyse structureel. De zorgaanbieder heeft de mogelijkheid om de structurele fout te isoleren, bijvoorbeeld via een bestandsanalyse, en corrigeert de geïsoleerde fout. Daarmee is de bevinding in voldoende mate opgevolgd en hoeft de gecorrigeerde fout niet opgenomen te worden in de foutentabel.

- De geconstateerde fout is op basis van de impactanalyse structureel, maar de zorgaanbieder kan deze door de aard van

[2] Er zijn (soms) andere mogelijkheden, zoals het uitvoeren van een bestandsanalyse. Het afwegen van de effectiviteit en efficiency van een maatregel is primair aan de instelling, die dit afstemt met de representerende zorgverzekeraar. Daarnaast zijn in het handvat "Verantwoord verminderen" diverse alternatieve beheersingsvormen genoemd, waardoor het niet altijd noodzakelijk is om te kiezen voor een deelwaarneming. We gaan hier verder niet op in, omdat dit een casusspecifieke afweging vergt en dus maatwerk is.
[3] Deelnemende partijen zijn binnen HT overeengekomen dat er geen correcties worden doorgevoerd op afgeronde verantwoordingsjaren. Niet werkende beheersmaatregelen kunnen ten hoogste effect hebben op het lopende (nog niet afgeronde) HT verantwoordingsjaar. De NZa is hiermee akkoord, gezien de doelstellingen van HT en de focus op beheersing.

de fout niet isoleren. Deze laatste situatie roept in de praktijk de meeste vragen op. Is er ruimte voor een maatwerkafspraak tussen de zorgaanbieder en representerende zorgverzekeraar of geldt hierbij de harde eis dat de geëxtrapoleerde fout altijd moet worden gecorrigeerd?

Wat wij hierbij van belang vinden is dat het totaalbeeld[4] van de beheersing door de zorgaanbieder in ogenschouw wordt genomen. Is er bijvoorbeeld sprake van een overwegend beheerst proces met een adequate verbetercyclus? Wat is de aard en (geschatte) omvang van de geconstateerde fout, mede in relatie tot het geconstateerde risico/proces en wat is een eventueel acceptabel restrisico? Welke signalen en/of overige informatie hebben de zorgaanbieder en/of zorgverzekeraar uit bijvoorbeeld data-analyse? En wat geeft die informatie aan? Wat is het toekomst- en verbeterperspectief van de specifieke processen? Is er recente(re) informatie beschikbaar, bijvoorbeeld vanuit 'continious monitoring'? En wat zegt dit over de wijze van beheersing?

Dit soort vragen kunnen een rol spelen in het bepalen of de berekende omvang van de fout afgerekend moet worden door de zorgaanbieder en of deze opgenomen wordt in de foutentabel[5] door de zorgaanbieder en zorgverzekeraar. Dit betreft maatwerk. De doelstelling van deze brief is erop gericht om bewegingsruimte te geven voor dit maatwerk, passend bij de doelstellingen van HT (o.a. gefundeerd vertrouwen, procesgericht, toekomstgerichte verbeteringen). Wij zijn ons ervan bewust dat zonder ruimte voor maatwerk, HT kan vervallen tot een lineair kader, waarbinnen mechanische keuzes het onderling vertrouwen eerder kunnen schaden dan versterken.

Als besloten wordt de geëxtrapoleerde fout vanwege de gezamenlijke afweging op basis van bovengenoemde factoren niet af te rekenen, wordt dit wederzijds bestempeld als een geaccepteerd risico. Bij een geaccepteerd risico hoeft volgens het Controleprotocol Zvw geen opname in de foutentabel plaats te vinden. De zorgaanbieder en de zorgverzekeraar leggen hun gezamenlijke afwegingen en besluit op transparante wijze vast.

Wij hopen hiermee voldoende ruimte te bieden om lokaal tot passende afspraken te komen.

[4] De vragen die vervolgens in deze alinea zijn opgenomen, zijn bedoeld als voorbeeld en denkrichting. Het is geen limitatieve opsomming en het zijn ook geen vragen die persé allemaal op 'groen' zouden moeten staan. Dit is maatwerk en is ter beoordeling van het lokale overleg.
[5] Hierbij geldt dat de in de deelwaarneming geconstateerde detailfouten altijd worden gecorrigeerd.

Tot slot
Wij hopen u toereikend te hebben geïnformeerd. Voor vragen kunt u terecht bij dhr. E. Langeveld RA, zijn gegevens staan in het briefhoofd.

Met vriendelijke groet,
Nederlandse Zorgautoriteit,

mw. mr. drs. K. Raaijmakers
directeur Toezicht en Handhaving

Nederlandse Vereniging van Ziekenhuizen

de Nederlandse ggz

Zorgverzekeraars Nederland

NEDERLANDSE FEDERATIE VAN UNIVERSITAIR MEDISCHE CENTRA

Nederlandse Zorgautoriteit

HORIZONTAALTOEZICHTZORG

www.horizontaaltoezichtzorg.nl

info@horizontaaltoezichtzorg.nl