IT General Controls en beheersmaatregelen met een IT-component

Handvat voor toepassing IT General Controls
binnen Horizontaal Toezicht

(versie 1.0 definitief) september 2019

HORIZONTAALTOEZICHTZORG

Nederlandse Vereniging van Ziekenhuizen
GGZNEDERLAND
Zorgverzekeraars Nederland
NFU NEDERLANDSE FEDERATIE VAN UNIVERSITAIR MEDISCHE CENTRA
Nederlandse Zorgautoriteit

IT General Controls en beheersmaatregelen met een IT-component

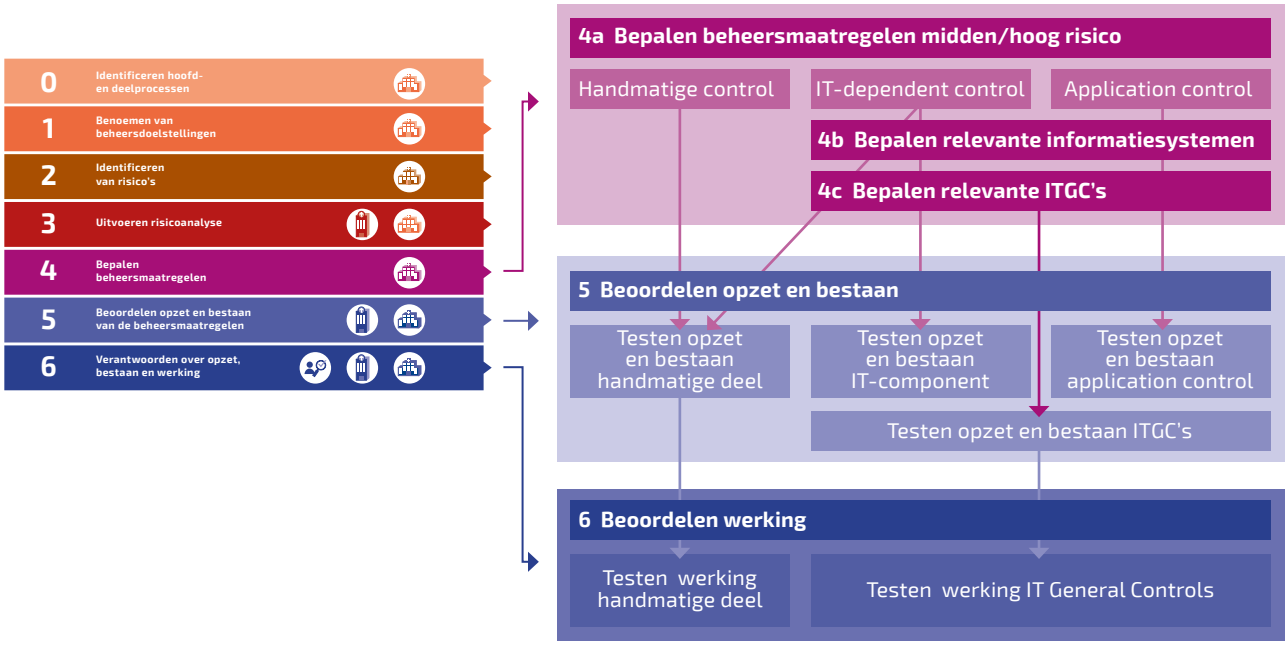
Alle zorginstellingen maken gebruik van IT-systemen voor hun EPD, zorgregistratie en –facturatie. Dit betekent dat we in de praktijk altijd steunen op in deze systemen aanwezige beheersmaatregelen. Belangrijke beheersmaatregelen in de processen zijn (ingebouwde) functiescheiding, werklijsten en invoercontroles.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



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.

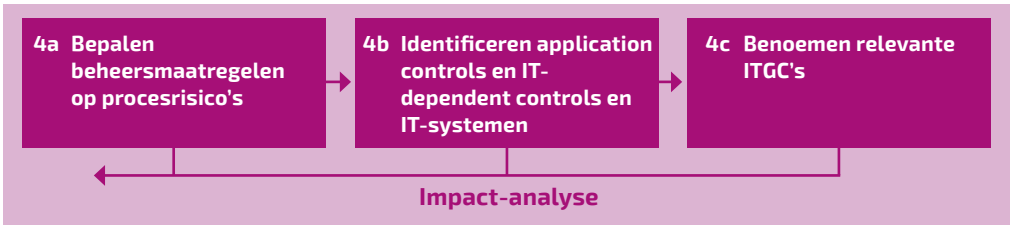
Lesson learned:
Of het datawarehouse in scope is voor ITGC is afhankelijk van het gebruik van het DWH in het kader van Horizontaal Toezicht en in hoeverre de betrouwbaarheid van de data wordt beheerst. Een voorbeeld van beheersing is dat de data in het DWH periodiek integraal wordt aangesloten met het 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);
  - 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 systeemwijzgingen) 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.