Whitepaper

IT-governance en e-health

door Beer Franken[1]

Mei 2023

De waarde van normen

IT-governance en e-health

Whitepaper, door Beer Franken[1]

Managementsamenvatting

Organisaties worden steeds afhankelijker van IT en daarmee ook van het goed functioneren van IT. Maar IT goed laten functioneren is nog niet zo gemakkelijk. Een groot deel van de benutte kwaliteit van IT is afhankelijk van hoe goed de klant zijn vraag weet te formuleren. Want IT voert meestal simpelweg uit wat de klant vraagt. Als die klantvraag dus niet duidelijk of effectief is, dan zal de IT dat ook niet zijn. Bij kleinere organisaties is het goed formuleren van de klantvraag meestal geen probleem, maar wat als het een groot ziekenhuis betreft of een andere grote organisatie in de zorg die met e health aan de slag wil? Dit vraagstuk zien we terug in het negenvlaksmodel en de focus op demand en supply.

Een misvatting is, dat als er eenmaal een IT systeem staat, er geen investeringen meer nodig zijn. Maar organisaties krijgen te maken met verschillende kosten om hun IT systeem up-to-date te houden. Denk aan onderhoudskosten, licentiekosten, reparaties of aanpassingen. Al die dingen kosten geld en er komt geen extra IT functionaliteit voor terug (en om daarbij te helpen is er IT governance, zoals ISO 38500). Het bedrag dat overblijft kan worden besteed aan de nodige innovatie. Kosten voor beheer en innovatie – zoals rond e health – zijn dus sterk aan elkaar verbonden.

Een belangrijke opmerking tot slot, is dat IT, ondanks de associatie met computers, mensenwerk is. Het is belangrijk daar rekening mee te houden. Beleid op papier kan door de invloed van de menselijke factor in de praktijk vaak heel anders uitpakken.

Dit whitepaper gaat in op het hoe en het wat IT-governance in de zorg, een vereiste voor succesvol gebruik van e-health.

Aanleiding en inleiding

Eind 2021 publiceerde de Inspectie Gezondheidszorg en Jeugd (IGJ) het rapport «Professionele digitale zorg vraagt van ziekenhuizen steeds opnieuw evalueren en verbeteren».[2] Tijdens 22 inspectiebezoeken aan ziekenhuizen passeerden veel voorbeelden van e-health de revue. Onder andere werd gekeken naar EPD's, patiëntportalen, de inzet van tele-/thuismonitoring en oplossingen voor digitale gegevensuitwisseling met patiënten, professionals en andere zorgaanbieders. Maar ook digitale behandelprogramma's (zoals voor het beïnvloeden van leefstijl) kwamen aan bod. IGJ constateert dat ziekenhuizen digitale zorg steeds professioneler aanpakken. Wel signaleert de inspectie een aantal aandachtspunten.

Wat is het verschil tussen IT en ICT?
IT staat voor 'informatietechnologie' en ICT staat voor 'informatie- en communicatietechnologie'. Nederland is het enige land dat de afkorting ICT hanteert. In het buitenland wordt hetzelfde aangeduid met IT.

IT en ICT zijn dus elkaars synoniem.

Zo wordt ervoor gepleit om de IT-governance binnen zorginstellingen te verbeteren. Hierbij verwijst zij ondermeer naar de norm NEN-ISO 38500 (Information technology – Governance of IT for the organization), maar tegelijk constateert de IGJ in haar nieuwsbericht[3] naar aanleiding van het verschijnen van het rapport, dat er nog geen norm is voor IT-governance *in de zorg*. Ziekenhuizen moeten daarom vaak zelf bedenken hoe ze dit goed en veilig regelen. Het zou echter de kwaliteit en veiligheid van de digitale zorg ten goede als ziekenhuizen houvast hebben aan een norm.

Dit whitepaper is niet die norm. Het verkent daarentegen het domein van IT-governance met betrekking tot e-health. En waar mogelijk worden bestaande normen en raamwerken getoond die de IT-governance in relatie tot e-health kunnen ondersteunen.

Voordat dieper op de materie wordt ingegaan, is het praktisch om vast te stellen wat er met IT-governance en met e-health wordt bedoeld.

IT-governance

IT-governance is het geheel aan afspraken en processen in de organisatie om het huidig en toekomstig gebruik van de IT doeltreffend en doelmatige aan te sturen, met inbegrip van de rol van IT in strategische innovatie. Het 'kijkt' dus enerzijds naar de informatie-voorziening en anderzijds naar (de toekomst van) de organisatie.

e-health

Onder e-health wordt de inzet verstaan van IT om de gezondheid en gezondheidszorg te ondersteunen of te verbeteren. Hieronder worden niet alleen de moderne varianten, zoals patiëntportalen, tele-/thuismonitoring, Persoonlijke Gezondheid Omgevingen (PGO) en online behandelprogramma's, begrepen maar ook de bekendere zoals elektronische dossiersystemen en digitale gegevens-uitwisseling.

Plaatsbepaling

IT-governance met betrekking tot e-health richt zich dus op de informatievoorziening (nu en in de toekomst) ten dienste van het gebruik en ontwikkelingen van e-health door een zorgorganisatie zoals een ziekenhuis. E-health is niet weg te denken uit de zorgverlening en het belang neemt alleen maar toe. Elke zorgaanbieder is gebaat bij goede e-health en is daarom sterk afhankelijk van een goede governance van e-health. Daarom maakt IT-governance deel uit van de brede governance van de organisatie en is onder-meer afhankelijke van landelijke ontwikkelingen. Anders gezegd: het is geen technisch feestje (zie ook 'chefsache' op bladzijde 5).

primaire IT-governance

Grofweg omvat IT-governance twee samenhangende hoofdgebieden. Om te beginnen het dagelijkse beheer van IT-voorzieningen. IT is bijna nooit statisch en moet voortdu-rend worden onderhouden. Het lijkt het minst spannende onderdeel van IT-governance, maar het is zondermeer wel het meest kostbare. Zo'n 75 tot 85 % van de IT-kosten gaan gepaard met beheer. Denk bijvoorbeeld aan instandhouding van apparatuur, perso-neelskosten en licenties.

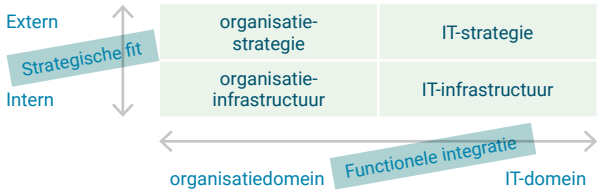
Het tweede gebied betreft innovatie. Het spreekt voor zich dat de koers voor innovatie moet worden bepaald op basis van de strategie van de organisatie. Maar ook bij het beheer is de strategie van de organisatie van belang, zoals bij beslissingen om het gebruik van bepaalde soft-ware te staken. Dit geeft aan dat IT-beheer en IT-innovatie enerzijds en de strategie van de organisatie anderzijds met elkaar samenhangen. Verder wordt de financiële ruimte voor innovatie bepaald door de kosten die worden gemaakt voor beheer, wat de onderlinge samenhang verder benadrukt.

Secundaire IT-governance

Naast het primaire domein van IT-governance (beheer en innovatie) richt IT-governance zich ook op samenhan-gende gebieden, zoals toezien op naleving (auditing), verantwoor-ding en informatiebeveiliging.

Viervlaksmodel

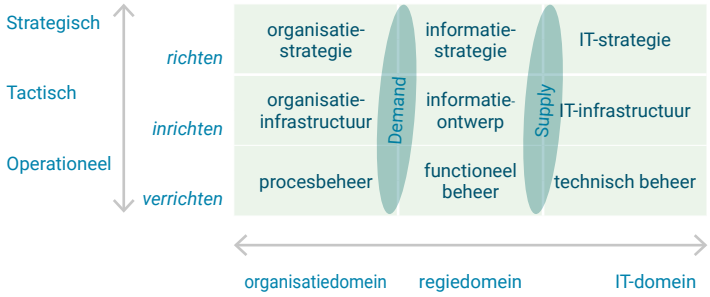
Om de samenhang tussen organisatie en IT, en tussen strategie en uitvoering grijpbaar te maken, ontstond in de jaren '90 het zogenaamde viervlaksmodel van Henderson en Venkatraman[4], waarbij de organisatie en IT in twee kolommen worden weergegeven en de externe respectie-velijk interne oriëntatie in twee rijen:



Een fundamentele aanname in dit model was dat organisatie en IT 'elkaar verstonden'. Dat bleek met de groeiende afhankelijkheid van IT én de toegenomen complexiteit van IT steeds minder het geval.

Negenvlaksmodel

Als reactie hierop, aangevuld met de observatie dat strategie een vertaling nodig heeft voordat het in een infrastructuur kan worden omgezet, leidde tot het negenvlaksmodel van Maes[5]:



Regie: demand en supply

Waar in het viervlaksmodel organisatie en IT elkaar niet verstonden, is er nu een sprake van regie. Hier komen enerzijds de behoefte van de organisatie (demand) naar voren en anderzijds de realisatie van de informatievoorziening als antwoord op de behoefte (supply). De organisatie moet vanuit haar strategie met betrekking tot e-health haar demand weten te articuleren. En IT moet in staat zijn om die demand te beantwoorden met de supply (een goed functionerende informatievoorziening). Natuurlijk rekening houdend met zaken als verantwoording, beschikbare budgetten, informatiebeveiliging, landelijkje ontwikkelingen enzovoorts.

Inrichting regie

De inrichting van het regiedomein wordt in belangrijke mate bepaald door ambities van en mogelijkheden binnen de organisatie. Zijn er bijvoorbeeld functionarissen als een CIO, CMIO, CNIO etc., dan ligt het voor de hand om hen een passende rol (met bijbehorende verantwoordelijkheden en bevoegdheden) toe te wijzen in de governance, aan de demand-zijde. Zijn zulke functionarissen niet beschikbaar, dan ligt een route met gremia voor de hand.

Demand: profiel

Aan de demand-zijde verwacht je mensen uit het primaire proces van de organisatie, die begrijpen wat wel en wat niet mogelijk is met IT. Voor de vereiste kennis zijn er enkele opleidingsmogelijkheden. Een lichten we eruit, omdat deze modulair is (je kiest zelf welke modules je wel en welke je niet volgt), online wordt aangeboden en kan leiden tot een academische master-titel. De tijdsindeling bepaal je zelf (het studietempo ligt wel vast) bij een studiebelasting van 10 tot 12 uur per week. Het gaat om de studie Master Health Informatics.[6]

Normen en raamwerken

Naast een regie-organisatie, gevuld met getrainde functionarissen, zijn er ook andere kaders nodig en gewenst. Te weten: best practices, zoals internationale normen en breed geaccepteerde raamwerken. Voor IT-governance zijn verschillende raamwerken en standaarden beschikbaar. (Voor IT-governance specifiek gericht op e-health echter niet.) Bekende raamwerken zijn COBIT, BiSL en ITIL; een bekende standaardenfamilie is ISO 3850X.

COBIT

COBIT[7] is een raamwerk voor IT-management en IT-governance (waarbij 'management' moet worden gelezen als 'beheren' en 'governance' meer gericht is op 'beheersen'). Het raamwerk is eigendom van ISACA (een Amerikaanse vakvereniging van IT-professionals). ISACA kent naast COBIT ook andere raamwerken, zoals voor audits en risico. De oorsprong ligt in compliance, security en risico's. Inmiddels beslaat COBIT het gehele IT-governance spectrum. Het is onderverdeeld in vijf domeinen en vervolgens 37 domeinen.

ITIL

ITIL[8] heeft een Britse achtergrond en beschrijft processen, procedures, taken en checklists die organisatie- noch technologie-specifiek zijn, maar kunnen worden toegepast bij het ontwikkelen van strategie en het handhaven van een competentieniveau. Het stelt in staat een baseline vast te stellen, plannen, implementeren en meten, en wordt gebruikt om naleving aan te tonen en verbetering te meten. Er is geen formele nalevingsbeoordeling voor ITIL-naleving in een organisatie: certificering in ITIL is alleen beschikbaar voor individuen. Sinds 2013 is ITIL eigendom van een joint venture met ondermeer de Britse overheid.

ITIL wordt – althans in Europa – aanzienlijk breder toegepast dan COBIT.

BiSL

BiSL[9] richt zich met name op de demand zijde. Denk aan het continu aanpassen van bedrijfsapplicaties. Hiervoor wordt een raamwerk met 23 onderdelen gebruikt dat vooral het toepassen van best practices voor de informatievoorziening als doel heeft.

ISO 3850X

De ISO3850X-familie bestaat uit standaarden zoals ISO 38500 (IT voor de organisatie), ISO 38501 (implementatierichtlijnen), ISO 38502 (raamwerk en model), ISO 38504 (richtlijnen voor IT-governance standaarden), ISO 38505 (data) en ISO 38506 (IT-investeringen).

ISO 38500

ISO/IEC 38500 *Information technology — Governance of IT for the organization* (kortweg ISO 38500) biedt leidende principes voor de leiding van organisaties over het effectieve, efficiënte en acceptabele gebruik van IT binnen hun organisatie. Het biedt ook begeleiding aan degenen die leiding adviseren, informeren of bijstaan, zoals managers, degenen die de middelen binnen de organisatie bewaken, externe zakelijke adviseurs en technische specialisten, in- en externe dienstverleners (inclusief adviseurs) en in en externe accountants. De standaard:

- is van toepassing op het beheer van het huidige en toekomstige gebruik van IT door de organisatie, inclusief managementprocessen en beslissingen over het gebruik van IT;
- definieert de governance van IT als een onderdeel van de organisatorische (of corporate) governance; en
- is van toepassing op alle private en publieke organisaties, van elke omvang, ongeacht de mate van hun gebruik van IT.

ISO 38500 is een 'hoog over'-standaard van – in de kern – slechts 12 pagina's die een zestal principes modelmatig presenteert:

- verantwoording en verantwoordelijkheid,
- strategie,
- investeringen (acquisitie, aanschaf),
- prestaties (performance),
- conformiteit (naleving) en
- menselijk gedrag.

ISO 38500 vindt zijn oorsprong in ondermeer de OECD Principles of Corporate Governance uit 1999 (herzien in 2004). Zie voor een ziekenhuis-uitwerking bladzijde 6 en verder.

e-health specifiek

Zoals genoemd zijn de hiervoor genoemde IT-governance raamwerken en standaarden generiek van aard. Specifiek in de context van e-health heeft echter de IGJ aangegeven waar IT-governance met betrekking tot e-health zich ten minste zou moeten richten:[10]

- bestuurlijke aandacht voor e-health en de inzet van digitale middelen,
- visie, strategie en bijbehorende plannen en goede 'landing' hiervan in de organisatie,
- aansluiting tussen de werelden van zorg en IT respectievelijk tussen innovatie en de zorgpraktijk, waaronder de juiste expertise op de juiste plaats,
- bruikbare sturingsinformatie voor raden van bestuur om meer grip te krijgen op de complexe materie,
- vaststellen van de relevante taken, verantwoordelijkheden en bevoegdheden,
- inzichtelijke besluitvorming over e-health,
- betrokkenheid van de juiste belang¬hebbenden en deskundigheden op het juiste moment betrokken worden,
- evaluatie en (mogelijke) bijstelling van e-health beleid (plan-do-check-act) en
- beheersing van risico's, ook op het niveau van specifieke projecten.

hoe verder

Elke organisatie is anders, heeft een andere structuur, een andere geschiedenis, een andere context et cetera. Het vertrekpunt is daarom ook anders. Met dat in het achterhoofd liggen de volgende stappen voor de hand.

1. Maak de Raad van Bestuur eindverantwoordelijk voor de IT-governance ('chefsache', zie hierna) en wijs binnen de RvB een portefeuillehouder aan.
2. Zorg ervoor dat alle rollen binnen het negenvlaksmodel van Maes zijn belegd en zorg ervoor dat deze actoren voldoende kennis hebben om hun rol te kunnen vervullen.
3. Zorg ervoor dat al deze actoren elkaar structureel en proactief informeren en elkaar ondersteunen.
4. Zorg dat de organisatie haar demand voor e-health, nu en in de (nabije) toekomst, helder heeft en communiceer deze in een dialoog met de supply-organisatie. Denk hierbij aan externe invloeden zoals uit het Integraal Zorg Akkoord, en interne, uit de eigen strategie en operaties voortkomende vraagstukken voor governance.
5. Richt parallel hieraan de governance van de demand-organisatie in aan de hand van bekende en bewezen raamwerken als COBIT, BiSL of ITIL.
6. Ga over tot implementatie van ISO 38500 (een uitwerking voor een ziekenhuis is gegeven op bladzijde 6 e.v.) en vul aan waar de IGJ aangaf dat (ook) aandacht aan moest worden geschonken (zie hierboven).
7. Kom tot een jaarlijkse PDCA-cyclus met verantwoording over het afgelopen jaar die binnen de RvB wordt besproken en waarover zij een oordeel velt.

Bijlage

Ten aanzien van e-health, met name wat 'goed' is en hoe je het veilig aanpakt, bieden het Kenniscentrum digitale zorg van (nu nog) ZN (https://www.zn.nl/digitalezorg) en Z-CERT (https://www.z-cert.nl/) praktische informatie. Ook vanuit het NEN-programma Egiz, dat ingaat op ontwikkelingen rond de Wegiz (Wet elektronische gegevensuitwisseling in de zorg), is nuttige informatie beschikbaar (https://www.nen-egiz.nl/). Daarbij spelen diverse *inhoudelijke* standaarden voor gegevensverwerking een belangrijke rol.

Chefsache

Eind december 2022 werd de herziene richtlijn voor Network and Information Security (NIS-2) van kracht, die voor 18 oktober 2024 door de lidstaten moet zijn geïmplementeerd. NIS-2 legt onder andere aan 'essentiële entiteiten' een aantal verplichtingen op. Tot de essentiële entiteiten behoren ondermeer (rechts)personen of andere instanties die op het grondgebied van een lidstaat wettelijk gezondheidszorg verstrekken, dus onder andere ziekenhuizen.

De opgelegde verplichtingen zijn ruwweg te verdelen over 'zorgplicht' en 'meldplicht': een plicht om je zaakjes op orde te hebben en een plicht om beveiligingsproblemen te melden (dus meer dan alleen datalekken).

Om NIS-2 tanden te geven, luidt artikel 32, zesde lid: "De lidstaten zorgen ervoor dat elke natuurlijke persoon die verantwoordelijk is voor … een essentiële entiteit …, de bevoegdheid heeft om ervoor te zorgen dat deze entiteit deze richtlijn nakomt. De lidstaten zorgen ervoor dat dergelijke natuurlijke personen aansprakelijk kunnen worden gesteld voor het niet nakomen van hun verplichtingen om te zorgen voor de naleving van deze richtlijn."

Met andere woorden: bestuurders worden hoofdelijk aansprakelijk voor goede informatiebeveiliging. Met IT-governance kun je daarvoor zorgdragen.

Uitwerking van ISO 38500 voor de RvB van een ziekenhuis

Omwille van de leesbaarheid is ISO 38500 op de volgende pagina's uitgewerkt voor een archetypisch ziekenhuis. In de laatste kolom is een voorbeeldinvulling vanuit het oogpunt van de RvB weergegeven.
De RvB dient volgens ISO 38500 de IT-governance uit te voeren via een drietal hoofdtaken:

Analyseer

Het analyseer van het huidige en het toekomstige gebruik van IT, zowel binnen de eigen instelling als zorgbreed.

Stuur

Het sturen van de voorbereiding en implementatie van strategieën en beleid om ervoor te zorgen dat het gebruik van IT voldoet aan de doelstellingen van het ziekenhuis.

Monitor

Het houden van toezicht op naleving van het beleid en de prestaties ten opzichte van de strategieën.

Deze hoofdtaken verbindt ISO 38500 aan een zestal principes:
- verantwoordelijkheid,
- strategie,
- investeringen,
- prestaties,
- conformiteit en
- menselijk gedrag.

Nota bene

Bevoegdheden voor specifieke aspecten van IT kunnen worden gedelegeerd aan managers binnen het ziekenhuis. Maar de verantwoordelijkheid voor het effectieve, efficiënte en acceptabele gebruik van IT door het ziekenhuis blijft bij de RvB en kan niet worden gedelegeerd.

ISO 38500 verwoordt voor de ziekenhuissituatie			*Voorbeeldinvulling voor de RvB van een ziekenhuis*
Principe	**1**	**Verantwoordelijkheid**	
doelstelling		Actoren binnen het ziekenhuis begrijpen en accepteren hun verantwoordelijkheden ten aanzien van zowel het aanbod van als de vraag naar IT (demand en supply). De verantwoordelijken voor acties hebben ook de bevoegdheid om die acties uit te voeren.	
analyseer	1.1	De RvB moet de opties analyseren voor het toewijzen van verantwoordelijkheden met betrekking tot het huidige en toekomstige gebruik van IT door de organisatie. Hierbij moet de RvB streven naar een effectief, efficiënt en acceptabel gebruik van IT ter ondersteuning van huidige en toekomstige zakelijke doelstellingen.	Ga na hoe demand en supply van de IT binnen het ziekenhuis is vormgegeven. Denk na over het zou moeten worden vormgegeven. Gebruik hiervoor het negenvlaksmodel van Maes (zie hiervoor) en beschrijf en beleg de verantwoordelijkheden voor elk van de negen vlakken. Beschrijf ook de interactie tussen aangrenzende vlakken. Organiseer actief de demand-zijde met mensen uit het primaire zorgproces. Denk na over rollen als CMIO (chief medical information officer), CNIO (chief nursing information officer) en CIO (chief information officer, nadrukkelijk iets anders dan de traditionele 'directeur IT').
	1.2	De RvB moet de kennis en kunde analyseren van de verantwoordelijken voor beslissingen te nemen met betrekking tot IT.	Bepaal dat de verantwoordelijken kunnen worden bijgestaan door IT-specialisten die het primaire proces van het ziekenhuis kennen. Ga daarnaast na of zij (met name de CMIO, CNIO en CIO) bijscholing nodig hebben om hun rol goed te kunnen vervullen. Overweeg hierbij de studie Master Health Informatics.[11]
stuur	1.3	De RvB moet aangeven dat er strategieën worden gevolgd in overeenstemming met de toegewezen IT-verantwoordelijkheden.	Stel een 'Informatiestatuut' op met daarin een beschrijving van de IT-governance (bijvoorbeeld een ingevuld negenvlaksmodel van Maes), de hierbij gebruikte rollen (CNIO, CMIO, CIO én directeur IT) en een samenvatting van de verantwoordelijkheden die bij die rollen horen. Maak het statuut bekend op intranet en maak bekend wie wat doet (namen en rugnummers).
	1.4	De RvB moet ervoor zorgen dat de verantwoordelijken de informatie ontvangen die zij nodig hebben om aan hun verantwoordelijkheden te voldoen en aansprakelijkheid te dragen.	Neem in het Informatiestatuut op wie waarover informeert en wie waarbij wordt betrokken bij besluitvorming. Bespreek met degenen die de betreffende rollen vervullen hun verantwoordelijkheden en maak duidelijk dat zij ook rekening moeten houden met enerzijds effectiviteit, efficiëntie en acceptatie en anderzijds met de huidige en de toekomstige situatie. Bevraag hen expliciet wat zij nodig zullen hebben om die verantwoordelijkheden te kunnen dragen (informatie, toegang tot de RvB, training, ondersteuning, tijd, geld, etc.). Maak hierover afspraken met hen.

ISO 38500 verwoordt voor de ziekenhuissituatie			*Voorbeeldinvulling voor de RvB van een ziekenhuis*
monitor	1.5	De RvB moet erop toezien dat passende mechanismen voor IT-beheer worden ingesteld.	Laat de directeur IT uitleggen of ITIL, BiSL, COBIT of een ander passend mechanisme voor IT-beheer wordt gebruikt. Indien dat niet het geval is, moet toepassing van zo'n mechanisme worden opgelegd.
	1.6	De RvB moet erop toezien dat de verantwoordelijken hun verantwoordelijkheden erkennen en begrijpen.	Houd jaarlijks gesprekken met de verantwoordelijken en bevraag hen op hun verantwoordelijkheden, zodanig dat kan worden vastgesteld of deze worden begrepen en erkend. Vraag daarbij ook naar het overall functioneren van de IT-governance en de onderlinge verdeling van verantwoordelijkheden daarbinnen.
	1.7	De RvB moet toezicht houden op de prestaties van degenen die verantwoordelijk zijn voor het beheer van IT.	Laat de directeur IT uitleggen in welke mate het mechanisme (zoals bedoeld in 1.5: ITIL, COBIT, BiSL of …) wordt gebruikt. Kom tot jaarlijkse afspraken waarbij wordt vastgelegd dat het gebruikte mechanisme steeds verder (meer gebieden) en beter (hogere volwassenheid) wordt gebruikt. Laat periodiek (bijvoorbeeld vijfjaarlijks) door een externe, onafhankelijke en deskundige partij de toepassing van het gebruikte mechanisme bij het IT-beheer beoordelen en aanbevelingen doen voor verbetering. Overweeg een a priori beoordeling bij wijze van nul-meting. Bevraag anderen (bijvoorbeeld ook aan de mensen die zitting hebben in stuurgroepen of voorstellen indienen bij de RvB) naar hun ervaringen met IT-beheer.
Principe	**2**	**Strategie**	
doelstelling		De strategie van het ziekenhuis houdt rekening met de huidige en toekomstige mogelijkheden van IT; de plannen voor het gebruik van IT voldoen aan de huidige en voortdurende behoeften van de bedrijfsstrategie van het ziekenhuis.	
analyseer	2.1	De RvB moet ontwikkelingen in IT en bedrijfsprocessen analyseren om ervoor te zorgen dat IT de toekomstige behoeften van het ziekenhuis ondersteunt.	Voer jaarlijks een management review uit naar de (1) geschiktheid, (2) toereikendheid en (3) doeltreffendheid van de IT governance (zowel de structuur als de werking), niet alleen met betrekking tot de huidige informatiebehoeften van het ziekenhuis, maar (vooral) ook de toekomstige behoeften én elektronische uitwisseling in ketens en standaardisatie van gegevens.

	ISO 38500 verwoordt voor de ziekenhuissituatie		*Voorbeeldinvulling voor de RvB van een ziekenhuis*
	2.2	Bij het overwegen van plannen en beleid moet de RvB het gebruik van IT en IT-activiteiten analyseren om ervoor te zorgen dat ze aansluiten bij de doelstellingen van het ziekenhuis en voldoen aan de belangrijkste gerechtvaardigde verlangens van belanghebbenden. De RvB moet hierbij zo veel als mogelijk gebruik maken van good practices.	Schrijf voor dat IT-investeringsvoorstellen altijd aandacht moeten besteden aan enerzijds de aansluiting bij doelstellingen van het ziekenhuis en anderzijds de belangrijkste gerechtvaardigde verlangens van belanghebbenden. Laat in die voorstellen ook aangeven bij welke good practices wel en – belangrijker – bij welke niet wordt aangesloten.
	2.3	De RvB moet ervoor zorgen dat het gebruik van IT onderworpen is aan passend risicobeheer.	NEN 7510 gaat indringend in op de beheersing van risico's omtrent beschikbaarheid, integriteit en vertrouwelijkheid van de gebruikte informatie(voorziening). Zorg ervoor dat NEN 7510 in z'n geheel is geïmplementeerd, inclusief het managementsysteem (en niet alleen de beheersmaatregelen uit deel 2). Bewerkstellig dat het ziekenhuis binnen afzienbare tijd een onder accreditatie verleend certificaat voor NEN 7510 behaald en behoudt. NEN 7512 gaat meer specifiek (en ook indringend) in op risico's die samenhangen met gegevensuitwisseling met derde partijen. Zorg dat NEN 7512 voor *alle* vormen van gegevensuitwisseling van toepassing is verklaard en geheel wordt nageleefd.
stuur	2.4	De RvB moet de voorbereiding en het gebruik van strategieën en beleid sturen, zodat het ziekenhuis profiteert van ontwikkelingen in IT.	Stel samen met de actoren in de strategische en tactische echelons van de IT-governance (zie het negenvlaksmodel van Maes) een IT-strategie toekomstvisie op en werk dit jaarlijks bij.
	2.5	De RvB moet het indienen van voorstellen voor innovatief gebruik van IT aanmoedigen, mits deze het ziekenhuis in staat stelt te reageren op nieuwe kansen of uitdagingen, nieuwe zaken te op te pakken of processen te verbeteren.	Wijs in het IT-budget ruimte aan die uitsluitend kan worden aangewend voor zorggerichte innovatie (in tegenstelling tot IT-technische innovatie). Besluit over besteding van dat budget, nadat de strategische echelon van de IT-governance is gehoord.
monitor	2.6	De RvB moet toezicht houden op de voortgang van goedgekeurde IT-voorstellen om ervoor te zorgen dat de doelstellingen binnen de vereiste tijdsbestekken worden bereikt met behulp van toegewezen middelen.	Laat de goedgekeurde IT-voorstellen elke kwartaal volgens een vast stramien rapporteren.
	2.7	De RvB moet toezicht houden op het gebruik van IT om ervoor te zorgen dat de beoogde voordelen worden bereikt.	Laat de goedgekeurde en inmiddels gerealiseerde en geïmplementeerde IT-voorstellen gedurende de eerste vijf jaar, jaarlijks volgens een vast stramien rapporteren.

ISO 38500 verwoordt voor de ziekenhuissituatie			*Voorbeeldinvulling voor de RvB van een ziekenhuis*
Principe	**3**	**Investeringen**	
doelstelling		IT-investeringen worden om geldige redenen gedaan, op basis van een passende en voortdurende analyse, met duidelijke en transparante besluitvorming. Er is een juiste balans tussen baten, kansen, kosten en risico's, zowel op korte als op lange termijn.	
analyseer	3.1	Om goedgekeurde voorstellen te kunnen realiseren, moet de RvB opties analyseren voor IT supply, waarbij de enerzijds risico's en anderzijds de prijs/kwaliteit-verhouding van voorgestelde investeringen worden afgewogen.	Schrijf voor dat in IT-investeringsvoorstellen altijd meerdere opties worden gepresenteerd en bij elk daarvan aandacht wordt besteed aan zowel de risico's als de prijs/kwaliteitverhouding.
stuur	3.2	De RvB moet ervoor zorgen dat IT-activa (systemen en infrastructuur) op een gepaste manier worden aangeschaft (koop, huur, lease etc.), inclusief het opstellen van geschikte documentatie, en ze ervoor zorgen dat de vereiste competenties/capaciteiten worden geboden.	Laat de directeur IT – in samenspraak met de directeur Financiën – IT-acquisitie-beleids¬regels opstellen, met onder andere aandacht voor documentatie en (toekomstige) competenties en capaciteiten. Stel deze IT-acquisitie¬beleidsregels vast.
	3.3	De RvB moet ervoor zorgen dat regelingen voor uitgifte van IT-voorzie¬ningen (zowel intern als extern) de behoeften van het ziekenhuis ondersteunen.	Draag ervoor zorg dat het uitgiftebeleid de behoeften van het ziekenhuis als uitgangspunt gebruiken.
	3.4	De RvB moet ervoor zorgen dat het ziekenhuis en haar leveranciers een gedeeld begrip verkrijgen van de intentie van het ziekenhuis bij elke IT aanschaf.	Zie erop toe dat het IT-acquisitiebeleid (zie 3.2) aangeeft staan dat elk verzoek voor offerte (RfI, RfP etc.) vergezeld gaat van het doel dat het ziekenhuis met de aanschaf wenst te bereiken.
monitor	3.5	De RvB moet IT-investeringen monitoren om vast te stellen dat ze de vereiste capaciteiten/competenties bieden.	Verlang dat in elk verzoek voor een IT-gerelateerde offerte de vereiste capaciteiten en competenties worden vermeld en wordt aangegeven dat dit 'harde' voorwaarden zijn ('knock-out' criteria). Bij de beoordeling van deze offertes moet altijd worden gecontroleerd of aan de vereiste capaciteiten en competenties tegemoet wordt gekomen; offertes die dat niet doen, dienen te worden afgewezen.
	3.6	De RvB moet controleren in hoeverre het ziekenhuis en haar leveranciers het gedeelde begrip behouden van de intentie van het ziekenhuis bij het doen van een IT aanschaf.	Eis dat bij de beoordeling van IT-gerelateerde offertes (zie 3.5) moet worden beoordeeld of het doel dat het ziekenhuis met de aanschaf wenst te bereiken (zie 3.4) met de voorgestelde offerte kan worden bereikt en onder welke voorwaarden. Een alternatief is dat de aanbieder van de offerte dit verlangde doel expliciet in de offerte heeft herhaald.

ISO 38500 verwoordt voor de ziekenhuissituatie			*Voorbeeldinvulling voor de RvB van een ziekenhuis*
Principe	**4**	**Prestaties**	
doelstelling		IT is 'fit for purpose' bij het ondersteunen van het ziekenhuis, het leveren van de diensten, serviceniveaus en kwaliteit die nodig zijn om te voldoen aan de huidige en toekomstige vereisten.	
analyseer	4.1	De RvB moet ingediende plannen beoordelen om vast te stellen dat IT de bedrijfsprocessen met de vereiste bekwaamheid en capaciteit zal ondersteunen. Deze voorstellen moeten betrekking hebben op de voortzetting van de normale werking van het ziekenhuis en de behandeling van risico's die samenhangen met het gebruik van IT.	Draag ervoor zorg dat elk IT-gerelateerd voorstel onderbouwd aangeeft dat de voortzetting van de normale werking van het ziekenhuis niet met het voorstel wordt bedreigd. Evenzo moet elk IT-gerelateerd voorstel vergezeld gaan van een ondubbelzinnige verklaring van de directeur IT, dat 'zijn' supply-organisatie de geschetste bedrijfsprocessen met de vereiste bekwaamheid en capaciteit kan en zal ondersteunen, met specifieke aandacht voor (zie 4.3) de bescherming van IT-activa, inclusief het intellectuele eigendom en 'organisational memory'. En elk IT-gerelateerd voorstel moet vergezeld gaan van een duidelijke verklaring van de CISO (chief information security officer) dat de normale werking van de risicobehandeling die samenhangen met het IT-gebruik binnen het voorstel niet wordt bedreigd, met specifieke aandacht voor (zie 4.3) de integriteit van informatie.
	4.2	De RvB moet de risico's analyseren die voortvloeien uit IT-activiteiten en samenhangen met de continuïteit van de bedrijfsvoering.	Betrek in het beoordelingsproces voor IT-gerelateerd voorstellen de (zie 4.1) verklaring van de indiener.
	4.3	De RvB moet de risico's analyseren met betrekking tot de integriteit van informatie en de bescherming van IT-activa, inclusief het samenhangende intellectuele eigendom en 'organisational memory'[12].	Betrek in het beoordelingsproces voor IT-gerelateerd voorstellen de (zie 4.1) verklaringen van de directeur IT en van de CISO.
	4.4	De RvB moet opties zodanig analyseren dat wordt gezorgd voor effectieve en tijdige beslissingen over het gebruik van IT ter ondersteuning van doelstellingen van het ziekenhuis.	Beoordeel IT-gerelateerd voorstellen gestroomlijnd en volgens een vast stramien (zie ook 4.2 en 4.3).
	4.5	De RvB moet regelmatig de effectiviteit en prestaties van de IT-governance van de organisatie analyseren.	Voer jaarlijks een management review uit naar de (1) geschiktheid, (2) toereikendheid en (3) doeltreffendheid van de IT governance (zowel de structuur als de werking), niet alleen met betrekking tot de huidige informatiebehoeften van het ziekenhuis, maar (vooral) ook de toekomstige behoeften (zie ook 2.1).

		ISO 38500 verwoordt voor de ziekenhuissituatie	*Voorbeeldinvulling voor de RvB van een ziekenhuis*
stuur	4.6	De RvB moet ervoor zorgen dat er voldoende middelen worden toegewezen zodat IT voldoet aan de behoeften van de organisatie, volgens de overeengekomen prioriteiten en budgettaire beperkingen.	Stel het IT-budget vast op basis van reële behoeften en niet aan de hand van historische ontwikkelingen. Maak onderscheid naar beheer en innovatie (in de verhouding van – qua orde-grootte – 80/20 tot 95/5). Probeer gaandeweg het aandeel voor innovatie te vergroten richting de 20%.[13]
	4.7	De RvB moet verantwoordelijken instrueren dat IT de organisatie ondersteunt met correcte en actuele gegevens die beschermd zijn tegen verlies of misbruik.	Stel een capabele en proactieve CISO (chief information security officer) in een met de FG (functionaris gegevensbescherming) vergelijkbare onafhankelijke rol en positie. Steun de CISO – net als de FG – door dik en dun tegen weerstanden binnen het ziekenhuis. Maak informatieveilig gedrag een speerpunt voor de organisatie.[14]
monitor	4.8	De RvB moet monitoren in hoeverre IT de business ondersteunt, en controleren in hoeverre toegewezen middelen en budgetten worden geprioriteerd in overeenstemming met de doelstellingen van het ziekenhuis.	Laat periodiek (bijvoorbeeld eens in de vijf jaar) een extern onderzoek uitvoeren naar de business/IT-alignment, inclusief de financiële component.
	4.9	De RvB moet monitoren in hoeverre het beleid, zoals voor gegevensnauwkeurigheid en efficiënt gebruik van IT, correct wordt gevolgd.	Laat een audit programma inrichten en uitvoeren dat jaarlijks de stand van zaken in kaart brengt in welke mate het met IT samenhangende beleid wordt gevolgd.
Principe	**5**	**Conformiteit**	
doelstelling		Het gebruik van IT voldoet aan alle dwingende wet- en regelgeving. Beleid en praktijken zijn duidelijk gedefinieerd, geïmplementeerd en gehandhaafd.	
analyseer	5.1	De RvB moet regelmatig analyseren in hoeverre IT voldoet aan verplichtingen (wet- en regelgeving, contracten), intern beleid, normen en professionele richtlijnen.	Beleg de rol van compliance officer op een onafhankelijke positie binnen het ziekenhuis. Laat de compliance officer jaarlijks rapporteren over de naleving van wet- en regelgeving, contractuele afspraken, het interne beleid, normen en professionele richtlijnen, voor zover deze betrekking hebben op de informatievoorziening. Bespreek de rapportage in de RvB, spreek verantwoordelijken aan bij kleinere tekortkomingen en treed op (grijp in) bij ernstige tekortkomingen.
	5.2	De RvB moet regelmatig de conformiteit van het ziekenhuis met haar raamwerk voor het beheer van IT analyseren.	Laat periodiek (bijvoorbeeld vijfjaarlijks) door een externe, onafhankelijke en deskundige partij de toepassing van het gebruikte mechanisme bij het IT-beheer beoordelen en aanbevelingen doen voor verbetering (zie ook 1.7).

ISO 38500 verwoordt voor de ziekenhuissituatie			*Voorbeeldinvulling voor de RvB van een ziekenhuis*
stuur	5.3	De RvB moet de verantwoordelijken opdracht geven om standaardmechanismen in te richten die ervoor zorgen dat het gebruik van IT voldoet aan relevante verplichtingen, interne beleidslijnen, normen en richtlijnen.	Laat de directeuren IT, JZ en HR een voorstel ontwikkelen voor een acceptable use policy (AUP) of acceptabel gebruiksbeleid.[15]
	5.4	De RvB moet beleid opstellen en handhaven waardoor het ziekenhuis in staat is te voldoen aan interne verplichtingen bij het gebruik van IT.	Stel het AUP (zie 5.3) vast en verklaar deze van toepassing op alle gebruikers van IT (in eigen dienst of anderszins).
	5.5	De RvB moet aangeven dat IT-personeel de relevante richtlijnen voor professioneel gedrag en professionele ontwikkeling volgt.	Ga in overleg met de directeur HR na in hoeverre een en ander al door wet- en regelgeving is 'afgedekt'. Zie ook 5.3.
	5.6	De RvB moet ervoor zorgen dat alle handelingen met betrekking tot IT ethisch verantwoord zijn.	Zorg ervoor dat in het informatiebeveiligingsmanagementforum (IBMF; zie 6.1.1 van NEN 7510-2) ruim aandacht is voor ethische. Ga na of dit ook in andere gremia kan worden toegepast.
monitor	5.7	De RvB moet naleving en conformiteit van IT monitoren door middel van passende rapportage- en auditpraktijken, en ervoor zorgen dat beoordelingen tijdig, volledig en geschikt zijn voor de evaluatie van de mate van tevredenheid van de organisatie.	Zie 1.7/5.2: vraag de directeur IT om een reflectie op deze audits. Zie 1.7: laat de directeur rapporteren over de naleving van de jaarlijkse afspraken omtrent het steeds verder (meer gebieden) en beter (hogere volwassenheid) toepassen van het gebruikte mechanisme voor IT-beheer (COBIT, BiSL, ITIL, …). Laat de gebruikerstevredenheid jaarlijks peilen onder een representatief deel van de gebruikers.
	5.8	De RvB moet toezicht houden op IT-activiteiten, inclusief het verwijderen van bedrijfsmiddelen en gegevens, om ervoor te zorgen dat wordt voldaan aan verplichtingen op het gebied van milieu, privacy, strategisch kennisbeheer, behoud van het 'organisational memory'[16] en andere relevante verplichtingen.	Zie erop toe dat maatregel 8.3.2 (Verwijderen van media) en 11.2.7 (Veilig verwijderen of hergebruiken van apparatuur) van NEN 7510-2, rekening houden met het ziekenhuismilieubeleid, het ziekenhuisprivacybeleid en met andere relevante (in- of externe) verplichtingen, waaronder strategisch kennisbeheer, behoud van het 'organisational memory'.

ISO 38500 verwoordt voor de ziekenhuissituatie			*Voorbeeldinvulling voor de RvB van een ziekenhuis*
Principe	**6**	**Menselijk gedrag**	
doelstelling		IT-beleid, praktijken en beslissingen tonen respect voor menselijk gedrag, inclusief de huidige en evoluerende behoeften van alle deelnemers binnen een bedrijfsproces.	
analyseer	6.1	De RvB moet IT-activiteiten analyseren om ervoor te zorgen dat menselijk gedrag wordt geïdentificeerd en op passende wijze wordt overwogen.	Laat op basis van auditrapporten, gebruikerstevredenheidsrapportages (zie 5.7), bekende kwetsbaarheden (zie 12.6.1 van NEN 7510-2), gerapporteerde zwakheden (zie 16.1.3 van NEN 7510-2) gemelde incidenten (VIM) en dergelijke een analyse uitvoeren op onvoorzien/onwenselijk menselijk gedrag, met aanbevelingen voor verbetering. Maak daarbij gebruik van de op informatieveilig gedrag gerichte hulpmiddelen[17]. Neem een besluit over de gedane aanbevelingen en zie toe op uitvoering daarvan.
stuur	6.2	De RvB moet ervoor zorgen dat IT-activiteiten in overeenstemming zijn met geïdentificeerd menselijk gedrag.	Besteed ruime aandacht aan UX (user experience)[18] in de selectie/aankoop dan wel ontwikkeling van systemen.
	6.3	De RvB moet ervoor zorgen dat risico's, kansen, problemen en zorgen door iedereen op elk moment kunnen worden aangegeven en gemeld. Deze risico's moeten worden beheerd in overeenstemming met gepubliceerde beleidslijnen en procedures en worden geëscaleerd naar de relevante besluitvormers.	Ontwikkel beleid voor het (veilig) melden van IT-gerelateerde risico's, kansen, problemen en zorgen en betrek de analyse van de meldingen in de aansturing van IT-ontwikkelingen. Maak (en houd) het beleid bekend onder medewerkers. Zorg dat 'natuurlijke meldpunten' – zoals een servicedesk en een vertrouwenspersoon – weten waarnaar dergelijke meldingen moeten worden doorgestuurd.
monitor	6.4	De RvB moet IT-activiteiten monitoren om ervoor te zorgen dat geïdentificeerd menselijk gedrag relevant blijft en dat er voldoende aandacht aan wordt besteed.	Laat de analyse van 6.1 periodiek uitvoeren (inclusief aanbevelingen) en betrek daar ook de inspanningen op het gebied van UX (zie 6.2) bij. Neem een besluit over de gedane aanbevelingen en zie toe op uitvoering daarvan.
	6.5	De RvB moet (de toepassing van) interne procedures monitoren om ervoor te zorgen dat ze consistent zijn met het juiste gebruik van IT.	Laat bij de (periodieke) herziening van interne procedures inventariseren of het gebruik in de praktijk consistent is het juist IT-gebruik en verwerk de bevindingen in nieuwe versies van de procedures.

Footnotes

1 Beer Franken is zelfstandig adviseur en coach op de gebieden gegevensbescherming en informatiebeveiliging Hij heeft een bachelor Hogere Informatica van de Haagse Hogeschool en een master Information Management van TIAS/Univer¬siteit Tilburg.. Hij is lid van de norm-commissies 303006 (Informatievoorziening in de zorg) en 381027 (Informatiebeveiliging, cyber security en privacy). Franken was/is inhou-delijk betrokken bij de totstandkoming/herziening van de normen NEN 7510 (Informatiebeveiliging in de zorg), NEN 7512 (Vertrouwens¬basis voor gegevensuitwisseling), NEN 7513 (Logging - Vastleggen van acties op elektronische patiëntdossiers), NEN 7524 (Pseudonimisatie-dienstverlening), NTA 7516 (Eisen voor veilige e-mail en chatapplicaties) en normontwerp NEN 7521 (Decentrale toestemmingsverlening). Hij is bereikbaar via beer.franken@piasau.nl en 06 5534 7977

2 https://www.igj.nl/publicaties/rapporten/2021/12/21/professionele-digitale-zorg-vraagt-van-ziekenhuizen-steeds-opnieuw-evalueren-en-verbeteren

3 https://www.igj.nl/actueel/nieuws/2021/12/21/inspectie-vraagt-ziekenhuizen-informatiebeveiliging-te-verbeteren

4 Henderson JC, Venkatraman H. Strategic alignment: Leveraging information technology for transforming organizations. IBM systems journal. 1999;38(2.3):472-84.

5 Maes R, Rijsenbrij D, Truijens O, Goedvolk H. Redefining business-IT alignment through a unified framework. Universiteit Van Amsterdam/Cap Gemini White Paper. 2000 May.

6 https://www.amc.nl/web/leren/master-health-informatics-1.htm

7 De afkorting staat voor “control objectives for information and related technologies”.

8 De afkorting staat voor “information technology infrastructure library”.

9 De afkorting staat voor Business Information Services Library.

10 Zie het Toetsingskader ‘Inzet van e-health door zorgaanbieders’ van de IGJ: https://www.igj.nl/binaries/igj/documenten/toetsingskaders/2019/10/18/toetsingskader-inzet-van-e-health-door-zorgaanbieders/Toetsingskader_IGJ_Inzet+e-health+door+zorgaan¬bie¬-ders.pdf.

11 https://www.amc.nl/web/leren/master-health-informatics-1.htm

12 De verzamelde gegevens, informatie en kennis die in de loop van het bestaan van een organisatie is ontstaan.

13 Een (veel) hoger aandeel dan 20% heeft geen zin, want alle innovatie moet uiteindelijk ook weer worden beheerd.

14 https://www.informatieveiliggedragzorg.nl/

15 De AUP behandelt de belangrijkste punten over wat gebruikers wel en niet mogen doen met de IT-systemen en verwijst gebruikers naar het uitgebreidere beveiligingsbeleid. Het geeft ook aan welke sancties kunnen worden toegepast als een gebruiker de AUP overtreedt.

16 Zie voetnoot 11.

17 https://www.informatieveiliggedragzorg.nl/downloads/

18 Hoe een gebruiker omgaat met en een product, systeem of dienst ervaart, en omvat iemands percepties van nut, gebruiksgemak en efficiëntie.

Bezoekadres
Vlinderweg 6
2623 AX Delft

Postadres
Postbus 5059
2600 GB Delft

De waarde
van normen