Informatievoorziening binnen de P&C-cyclus (IT-auditor)

Positioneringsdocument B

Informatievoorziening moet een grotere plaats krijgen in Planning & Control-cyclus. De organisatie dwingt zich daarmee om ieder jaar te verbeteren en deze verbeteringen te waarborgen. De vergaande automatisering binnen de gemeente heeft ertoe geleid dat een groot gedeelte van de interne controle is geautomatiseerd en dat zogenaamde “controles buiten het systeem om” niet meer toereikend zijn. De gemeente wil haar zelf controlerend vermogen versterken en self compliant zijn (zowel op FA als IT gebied). Hierdoor is naast de huidige interne auditors op het gebied van financiën een interne auditor nodig gespecialiseerd in het auditen van de informatievoorziening.

Michelle van Geffen

10-11-2016

INFORMATIEVOORZIENING BINNEN DE P&C-CYCLUS (IT-AUDITOR)

Positioneringsdocument B

De informatievoorziening moet een grotere plaats krijgen in de Planning & Control-cyclus van Gemeente Haarlem. De organisatie dwingt zich daarmee om ieder jaar te verbeteren en deze verbeteringen te waarborgen. Zo adviseerde het Kwaliteits Instituut Nederlandse Gemeente (KING, 2013) "bestuurders (..) het aspect informatievoorziening een gewicht toe te kennen dat vergelijkbaar is met de verdeling van de beschikbare middelen"[1]. De noodzaak om met het verantwoordingsproces over informatieveiligheid aan te sluiten bij de gemeentelijke P&C-cyclus komt mede doordat er steeds meer samenhang bestaat tussen interne (financiële) beheersing en informatietechnologie. Gemeente Haarlem erkend deze samenhang en het belang van een betrouwbare informatie voorziening. Mede hierom heeft de gemeente in de Kadernota 2016 aangekondigd om vanaf 2017 'een interne auditor op het gebied van Informatiebeveiliging en Informatiebeheer aan te stellen'. Dit ook in lijn met de resolutie "Informatieveiligheid, randvoorwaarde voor de professionele gemeente", de daarop volgende Baseline Informatieveiligheid Gemeente (BIG) en de start van het project Eenduidige Normatiek Single Information Audit[2]. Om het verantwoordingsproces over de informatievoorziening bij gemeenten verder te professionaliseren, is er naast de huidige interne auditors op het gebied van financiën een interne auditor nodig gespecialiseerd in het auditen van de informatievoorziening. Het betrekken van de audit community bij de integratie van de informatievoorziening binnen de P&C-cyclus is een belangrijke stap, omdat zowel de toezichthouders als de gemeente zich realiseren dat vreemde ogen dwingen. Deze nota zet de keuze uiteen voor de positionering van deze auditor binnen het nieuwe "audit team".

Leeswijzer

- De nota start met een beschrijving van het project ENSIA; een project ingegeven door het rijk met als doel het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren.
- Waarna ingegaan wordt hoe en waarom Gemeente Haarlem deze professionalisering van de informatievoorziening wilt bereiken door aan te sluiten op de gemeentelijke Planning & Control-cyclus.
- Er wordt vervolgens in dit kader dieper ingegaan op de aan te stellen IT-auditor en de samenhang tussen de informatievoorziening en interne (financiële) beheersing.
- Tot slot wordt er kort ingegaan op de taken & vereisten van de aan te stellen IT-auditor.

[1] http://zorgendestad.digitalestedenagenda.nl/wp-content/uploads/sites/3/2014/01/eindadvies-visd-totaal-29-07-2013.pdf

[2] Het Rijk heeft verplichte IT audits in het kader van de BIG en aanverwante normenkaders aangekondigd, te beginnen in 2017.

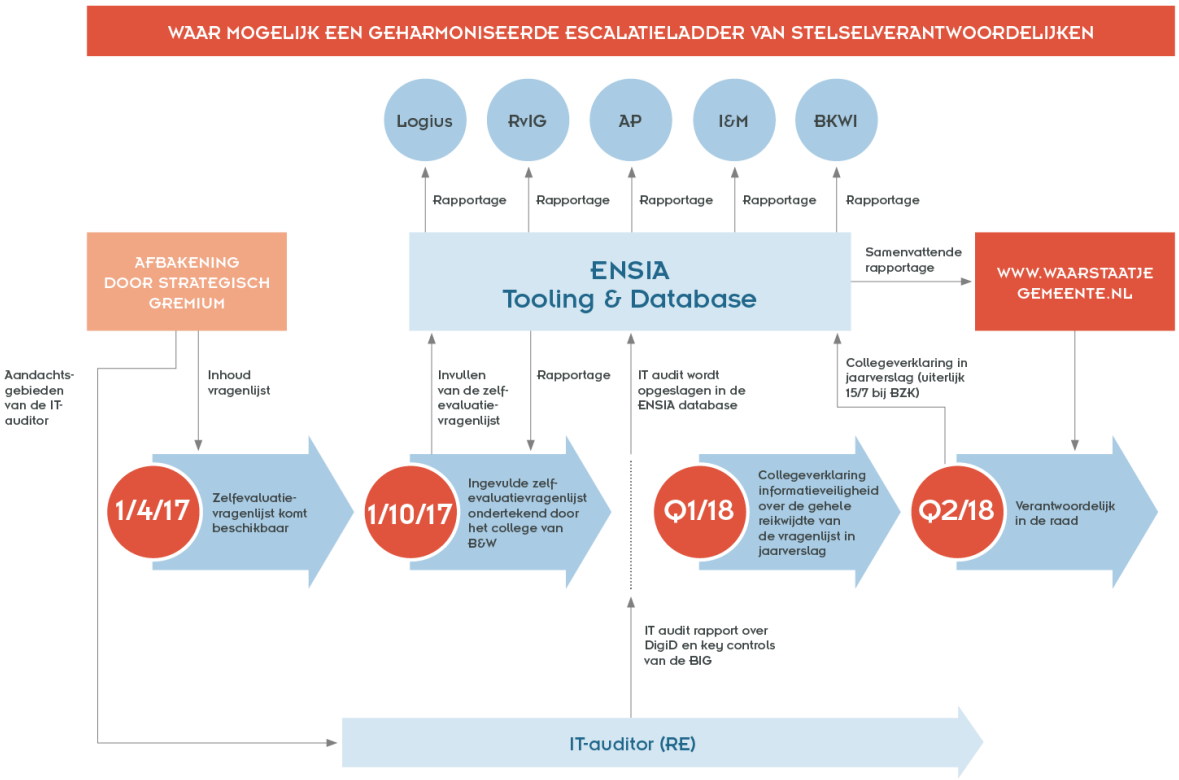
Project ENSIA

Met het aannemen van de resolutie “Informatieveiligheid, randvoorwaarde voor de professionele gemeente” deden de gemeenten gelijktijdig ook een oproep aan de Rijksoverheid om de verantwoordingslast over informatieveiligheid te verminderen. Dit laatste vormde de aanleiding voor de start van het project ENSIA.

Het Rijk stuurt aan op de invoering van een Eenduidige Normatiek Single Information Audit (ENSIA) per 2017. ENSIA heeft tot doel het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren door het toezicht te bundelen en aan te sluiten op de gemeentelijke Planning & Control-cyclus. Hierdoor heeft het gemeentebestuur meer overzicht over de stand van zaken van de informatieveiligheid en kan het hier ook beter op sturen.

Op dit moment loopt er een Pilot onder verschillende gemeentes die gestart zijn met de invoering van ENSIA. Vereniging van Nederlandse Gemeente (VNG) adviseert dat gemeente zelf de eerste voorbereidingsmaatregelen al kunnen treffen voor de komst van ENSIA door de verantwoording van het informatiebeveiligingsbeleid zowel horizontaal als verticaal goed in te richten.

Het verantwoordingsproces voorzien door de stuurgroep ENSIA is weergeven in figuur 1[3] (De pilots kunnen mogelijk nog aanleiding geven tot aanpassingen in het verantwoordingsstelsel).



FIGUUR 1: JAARLIJKS ENSIA VERANTWOORDINGSPROCES

[3] Bron: https://www.deitauditor.nl/informatiebeveiliging/doelmatiger-verantwoordingsproces-informatieveiligheid/

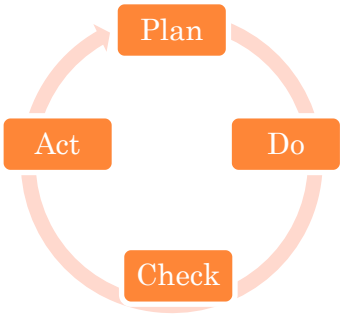
Toelichting op figuur 1: 'de verantwoording over de informatiebeveiliging komt in het jaarverslag tot uitdrukking in de Collegeverklaring Informatiebeveiliging, waarover een assurancerapport wordt uitgebracht door een IT-Auditor. Met deze verklaring geeft het College van B&W aan in hoeverre de gemeente voldoet aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording Informatiebeveiliging, de normen van de BIG en de normen van BRP, PUN, DigiD, SuwiNet, BAG en BGT. Ook worden de eventuele verbetermaatregelen vermeld die de gemeente gaat treffen. De ingevulde zelfevaluatievragenlijst vormt de basis voor het opstellen van de Collegeverklaring. Een IT-auditor controleert de zelfevaluatie en de collegeverklaring op een aantal in het strategisch gremium ENSIA afgesproken aandachtsgebieden. Op basis van een nader te bepalen normenstelsel[4] wordt over de zelfevaluatie en de daarop gebaseerde collegeverklaring een assurancerapport uitgebracht aan de hand van Richtlijn ISAE-3000'[5].

Volgens ENSIA is de aan te stellen IT-auditor een Register EDP-Auditor - een titel die kan worden behaald aan de door de NOREA erkende opleidingen is Executive Master of IT-auditing (EMITA). Het betrekken van de audit community bij de integratie van de informatievoorziening binnen de P&C-cyclus is een belangrijke stap, omdat zowel de toezichthouders als de gemeente zich realiseren dat vreemde ogen dwingen.

Integratie Informatie Voorziening in P&C-Cyclus

Cirkel van Deming

Het opnemen van de beheersing van de informatievoorziening in de P&C cyclus is een voor de hand liggende manier om de gehele organisatie te laten meewerken aan het op uniforme en geborgde wijze verbeteren van de informatievoorziening. Hiermee wordt een kwaliteitscirkel van Deming op gang gebracht waarbij de informatievoorziening over de volle breedte van de organisatie voortdurend verbetert, ondersteund door alle binnen de P&C cyclus beschikbare sturingsmiddelen. Door de verbetering te waarborgen komt de organisatie ook op dit onderdeel aantoonbaar 'in control'. Hiermee zijn de BIG-normen niet het doel op zich zelf, maar komt de implementatie van BIG de bedrijfsvoering doelen ten goede.



Ook de Handreiking **Kwaliteitssysteem Informatiebeheer Decentrale Overheden** (KIDO)[6] beroept zich op de Cirkel van Deming om de kwaliteit van het informatiebeheer te managen (zie positioneringspaper A). KIDO richt zich op het ontwikkelen van een kwaliteitssysteem voor informatiebeheer, zoals bedoeld in artikel 16 van de Archiefregeling. Volgens de Projectgroep KIDO/TwynstraGudde; 'Het verdient aanbeveling

[4] Vooralsnog is het voorstel van de ENSIA stuurgroep om het eerste jaar de zogenoemde **key-controls van de ISO-standaard 27002 plus aanvullende aspecten die voor DigiD en BIR** van belang zijn als uitgangspunt voor de aandachtsgebieden van de IT-audit te nemen.
[5] Ibid. 2 Let op: ISAE-3000 heeft niet enkel betrekking op financiële processen.
[6] https://vng.nl/files/vng/20160113-handreiking-kido.pdf ook de BIR maakt een zelfde referentie.

om het verbeterplan mee te nemen in de jaarlijkse beleids- en plancyclus van de organisatie met bijbehorende governance. Hetzelfde geldt voor de blijvende verbeteringen, die input zijn voor het nieuwe beleid in de komende (plan)periode. Voor de inrichting van kwaliteitsmanagement (het continue verbeteren) binnen de organisatie, verwijzen we naar de hiervoor aanwezige normen en richtlijnen, zoals ISO 9001 en INK'.

Three Lines of Defence

De verantwoordelijkheid voor het voldoen aan vrijwel alle normen op het gebied van informatievoorziening ligt in de lijn, bij de afdelingshoofden. Dit ligt vast in de van toepassing verklaarde normenkaders. Door informatievoorziening op te nemen in de P&C cyclus wordt aangesloten bij het in Haarlem voor de financiële beheersing gekozen Three Lines of Defence (3LoD) model. In dit model is het lijnmanagement verantwoordelijk voor de eigen processen. De tweede lijn ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering. In 2015 is het auditteam binnen de Gemeente Haarlem meer onafhankelijk gepositioneerd binnen de organisatie door deze medewerkers direct onder de concerncontroller binnen de afdeling Concernstaf te positioneren. Door de IT-auditor ook te positioneren binnen het audit-team is de onafhankelijke positie van de auditor geborgd.

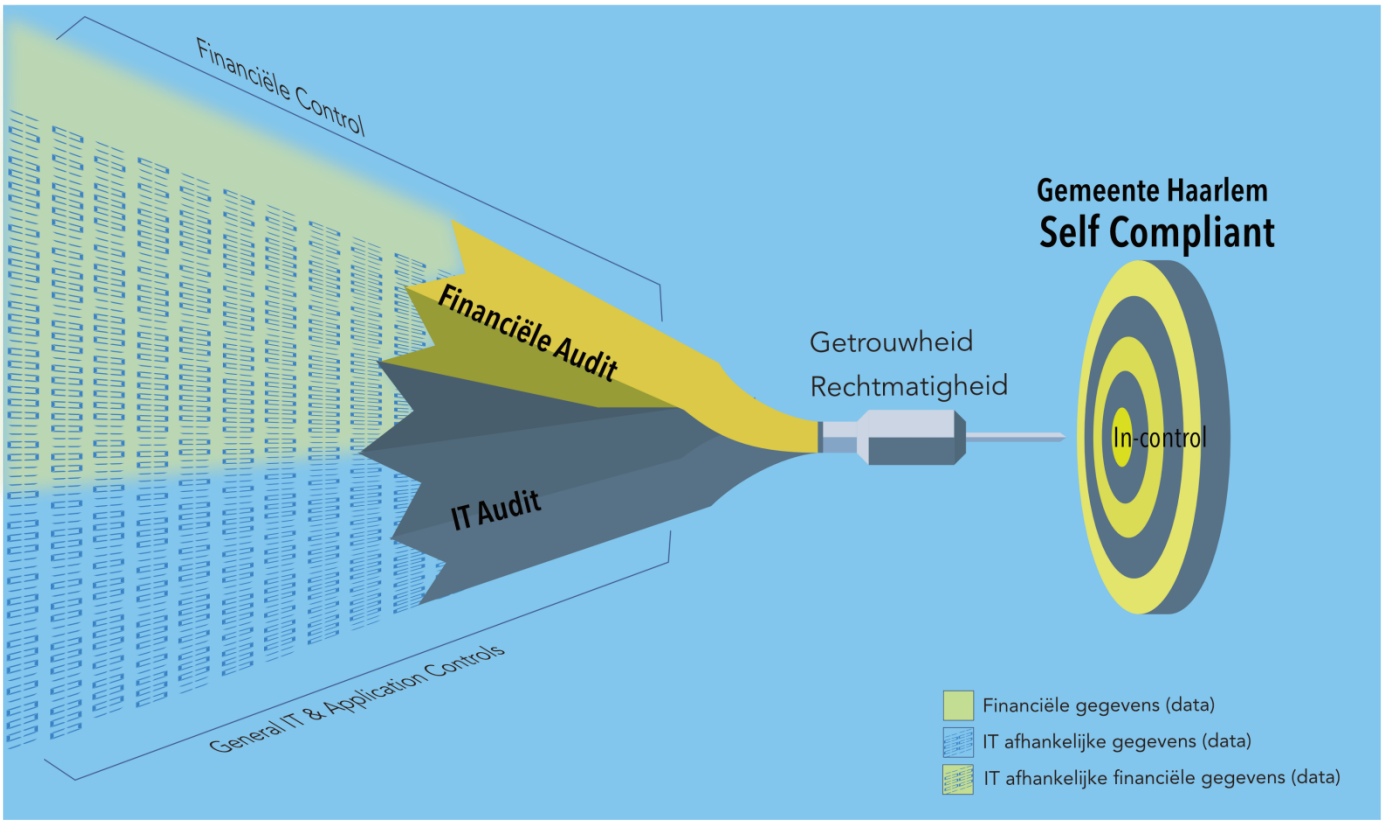
IT-auditor en/of FA-auditor

De noodzaak om met het verantwoordingsproces over informatieveiligheid aan te sluiten bij de Haarlemse gemeentelijke P&C-cyclus komt mede doordat er steeds meer samenhang bestaat tussen interne (financiële) beheersing en informatietechnologie. Dit door de vergaande automatisering binnen de gemeente en doordat de interne toets op het 'self compliant' zijn van de organisatie niet enkel betrekking heeft op financiële processen, maar ook op de gehele informatievoorziening. In andere woorden, de financiële beheersing kan niet meer heen om IT en IT kan niet meer heen om compliance eisen (zie o.a. BIG en ENSIA).

IT en FA, samen self-compliant

In het programma 'Haarlem presteert beter' is benoemd dat de gemeente haar zelf controlerend vermogen wil versterken en self compliant wil zijn. De afgelopen jaren heeft de accountant (PWC) vertrouwen uitgesproken in de kwaliteit van het Financial Auditteam dat verantwoordelijk is voor de interne toets op het 'self compliant' zijn van de organisatie (zie PWC controle 2014, 2015). Oftewel, voor de oordeelsvorming kan de accountant terugvallen op het Financial Auditteam[7]. Ook op het gebied van IT zou dit een wenselijke ontwikkeling zijn. Beide (FA en IT) dragen op die manier bij aan de getrouwheid en rechtmatigheid van de P&C-producten (zie figuur 1). Een opbouw van eigen controlewerkzaamheden door Haarlem betekent gelijktijdig op termijn een afbouw van werkzaamheden van PWC.

[7] In de concept rapportage van PwC (2016) wordt er gesteld dat: Door verscherpte aandacht van de AFM het Audit Team volgens PwC niet als een interne accountantsdienst beschouwt kan worden. Dit doet geen afbreuk aan de kwaliteit en onafhankelijkheid van het team, die beide als goed worden beschouwd (op basis van het toetsingskader NV COS 610).



Figuur 1: Self compliance met Audit team

Investeren in een IT-audit aan de voorkant, oftewel geïntegreerd bij het werkproces, zorgt voor eigen inzicht in de mogelijke risico's als gevolg van de geautomatiseerde gegevensverwerking. Noodzakelijke aanpassingen / uit te voeren werkzaamheden kunnen hierdoor reeds in een vroegtijdig stadium worden opgepakt zonder dat voor dit aspect op de bevindingen van de externe accountant gewacht moet worden. Dit draagt bij aan een verbeterde risicobeheersing en bespaard tijd bij de externe accountantscontrole.

IT en Gemeente Haarlem

Uit de benchmark M&I rapportage blijkt dat Haarlem het iets beter doet dan andere gemeenten op het gebied van de "volwassenheid van de informatievoorziening". Gemeente Haarlem zet zich al een aantal jaar in op het verbeteren van de digitale dienstverlening. T.a.v. technische en operationele ICT kant zijn er de afgelopen jaren vele verbeteringen aangebracht in aanleg en beheer van de werkplekken, servers, netwerk kortom de infrastructuur, beheer van ICT contracten, centralisatie van het ICT budget, beheer van applicaties etc. en technische informatiebeveiliging. Ook is er een Stuurgroep Informatievoorziening actief, die overzicht houdt en de voortgang bewaakt van digitaliseringsprojecten. Het Informatiebeveiligings-beleidsplan is vastgesteld en de rol van Informatie

Niveau 0: Niet bestaand proces

Niveau 1: Ad hoc

Niveau 2: Gedefinieerd
Het proces is gestandaardiseerd, gedocumenteerd en wordt uitgedragen. Het proces is nog steeds reactief en het is aan de uitvoerende persoon om het proces te volgen.

Niveau 3: Meetbaar
Processen worden consistent uitgevoerd. De prestaties zijn meetbaar en worden ook gerapporteerd. Uitzonderingen op de 'standaard' worden geëvalueerd.

Niveau 4: Continu verbeteren
Het proces wordt continu verbeterd en er wordt gebruik gemaakt van best-practices.

M&I (2016): Schaal IV Volwassenheid

Security Officer is belegd. Bovendien, gezien de breedte en de urgentie van het onderwerp beschouwt de directie Informatievoorziening en Digitalisering als een topprioriteit. Deze prioriteit heeft vorm gekregen door een directe sturende rol van de directie te beleggen in de rol/functie van Chief Information Officer. Het opnemen van de CIO-rol in een directiefunctie heeft ook als voordeel dat de doelen van (bestuur en) de organisatie, die vertaling behoeven in aspecten van de Informatievoorziening, via een korte lijn worden ingebracht in het team CIO en vandaar kunnen worden opgepakt.

Toch is er genoeg ruimte voor verbetering. Volgens de Benchmark presteert de Gemeente Haarlem rond niveau twee *Gedefinieerd* (zie kader: Schaal IV Volwassenheid). De volgende stap is het evalueren en leren van gemaakte fouten, en hier ligt een rol voor de IT-auditor. Door de verbeteringen te waarborgen binnen de P&C-cyclus komt de organisatie ook op dit onderdeel aantoonbaar 'in control'.

Daarmee wordt ook de beweging gemaakt van reactief naar proactief (en richting self-compliance): Het is geen extra werk maar een verschuiving van werk, omdat het aantal incidenten afneemt. Een goed voorbeeld is een eerdere casus bij gemeente Haarlem op het gebied van patchmanagement. Patches zijn doorgaans kleine programma's die aanpassingen maken om fouten op te lossen of verbeteringen aan te brengen in bestaande programmatuur en/of hardware. Leveranciers van software en hardware geven regelmatig informatie over gevonden zwakheden in hun systemen, met daarbij een aanwijzing hoe deze zwakheid te bestrijden (versie-updates). In plaats van de oorzaak te onderzoeken bij specifieke incidenten waarbij de systemen niet up-to-date zijn, werd in dit geval gecheckt of de gemeente compliant was aan de normen, wat resulteerde in de identificatie van meer dan 200 gevallen. In plaats van voortdurend dweilen verschuift de actie naar het dichtdraaien van de kraan.

Naast de benodigde beweging van de informatie voorziening richting self-compliance, kan gelijktijdig financiële beheersing niet meer heen om IT.

Accountant moet kunnen steunen op lijstwerk IT

Zelfs de meest traditionele accountant zal ondervinden dat hij/zij niet meer om de computer heen kan controleren. De vergaande automatisering binnen de gemeente heeft ertoe geleid dat een groot gedeelte van de interne controle is geautomatiseerd en dat zogenaamde "controles buiten het systeem om" niet meer toereikend zijn (zie positioneringsdocument A). Oftewel de financial audit en IT zijn onlosmakelijk met elkaar verbonden.

Zo constateerde de Autoriteit Financiële Markten (AFM) binnen het jaarlijkse onderzoek naar de zogenaamde Big 4-accountantsorganisaties[8] dat de "externe accountants geen of onvoldoende werkzaamheden [uitvoerden] om de general IT controls[9] en application

[8] AFM - Uitkomsten onderzoek kwaliteit wettelijke controles Big 4-accountantsorganisaties

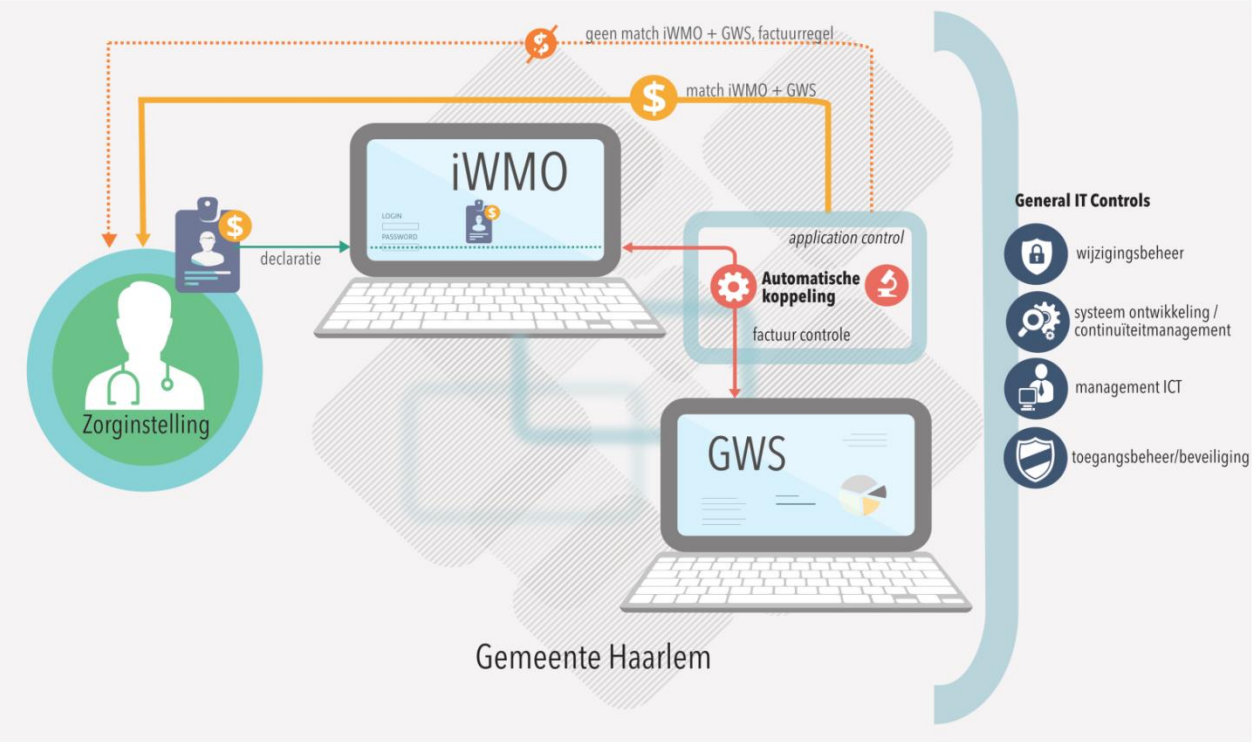
[9] General IT controls; zijn interne beheersingsmaatregelen met betrekking tot de geautomatiseerde gegevensverwerking en dienen de betrouwbare werking van deze geautomatiseerde gegevensverwerking te waarborgen.

controls[10] te beoordelen terwijl de accountant wel volledig steunt op de informatie en lijstwerk[11]" (zie AFM en Positioneringsdocument A). Oftewel, het risico van het niet integreren van IT in de controle aanpak/werkzaamheden is dat er gesteund wordt op data (geautomatiseerde gegevens) terwijl er onvoldoende IT werkzaamheden zijn uitgevoerd om vast te stellen of de betrouwbaarheid van deze data (output van de applicaties/systemen) voldoende is gewaarborgd (zie figuur 2 voor voorbeeld van het belang van de werking van IT controls).

Geheel in lijn met de hierboven beschreven constatering, zijn de aanbevelingen van PriceWaterCooper[12] voor Gemeente Haarlem. De accountant rapporteerde de volgende verbetermaatregelen:

a) op orde brengen van (het proces rond) de gebruikersautorisaties, het verhogen van het beveiligingsbewustzijn
b) binnen de organisatie, concrete zaken als het integreren van de testprocedure in het wijzigingsbeheer en het opstellen van een continuïteits- of herstelplan, met name voor kritieke systemen.
c) een verschuiving naar zogenaamde 'application controls' nodig is om de benodigde inspanning om in control te zijn en blijven te doen afnemen (zie voor een voorbeeld figuur 2 & positioneringsdocument A).

Ook is binnen de Gemeente Haarlem het ordenen/archiveren van de (digitale) informatiestromen nog niet op het door de Archiefinspectie vereiste niveau; vanuit de inspectie wordt dan ook jaarlijks op verbetering van het informatiebeheer aangedrongen.



Figuur 2: Voorbeeld Application - IT controls in het sociaal domein

[10] Application controls; zijn interne beheersingsmaatregelen binnen de applicatie. (Zie Positioneringsdocument A, voor uitleg en relevantie)
[11] Lijstwerk; de voor de accountantscontrole relevante output uit de applicaties.
[12] Interim Management Letter 2015, paragraaf 2.9

Kansen voor de toekomst: Data-analyse inzetten voor controle

De betrouwbaarheid van de data is van belang voor data-analyse en controle. Enerzijds moet de data voldoende betrouwbaar zijn om uit de analyses voldoende zekerheid te verkrijgen. Anderzijds kan data-analyse juist worden gebruikt om uitspraken te kunnen doen over de betrouwbaarheid van de data. Oftewel, slimme en efficiënte controle en het verdiepen van de controlewerkzaamheden.

Data-analyse toepassen als integraal onderdeel van de jaarrekeningcontrole zou in theorie voor een efficiënter en effectiever controleproces kunnen zorgen (mogelijk kan de IT-auditor hier een rol inspelen). Door de toenemende complexiteit en het aantal interne beheersings-maatregelen neemt ook het aantal controlewerkzaamheden toe. Data-analyse binnen de jaarrekening-controle biedt de mogelijkheid om uit grote verzamelingen van gegevens met behulp van tools bruikbare informatie te halen.

Ook vanuit het Haarlemse Financiële Audit team wordt aangegeven dat in de praktijk van vandaag nog veel gegevensgericht werk verricht wordt en de wens bestaat om meer systeemgericht te gaan opereren. Oftewel controle meer richten op het toetsen van het proces zelf: is de opzet (inrichting) van een proces goed en wordt daadwerkelijk gewerkt zoals het proces is opgezet. Zo stelt PwC (2016, concept) dat de aanpak verschilt per proces waardoor er niet gesteld kan worden dat er sprake is van een systematische aanpak. Daarnaast biedt de inzet van data-analyse voor het Financiële Audit team kansen om in de toekomst ook het gegevensgericht werk efficiënter uit te voeren (zie kader).

Audit team (A-team)

De IT auditor en accountant zullen dezelfde "taal" moeten spreken om de bevindingen van de IT auditor te kunnen vertalen naar bijvoorbeeld de jaarrekening controle[13] en kennisuitwisseling mogelijk te maken. Als de IT Auditor zich op een te grote afstand van de FA afdeling/controle team begeeft, loopt de organisatie het risico dat er te weinig gericht word op "audit risks" en te veel op "business risks"[14]. De bevindingen die de IT-auditor doet, moeten vertaald kunnen worden naar control.

Ook is het een vereiste dat de IT- auditor inzicht heeft in de achterliggende processen en de inhoudelijke (financiële) betekenis van de gegevens kent die hij analyseert. De ideale IT-auditor is hiermee niet alleen een Register EDP-Auditor (RE), maar ook iemand met bijvoorbeeld een vooropleiding als Register Accountant (RA). Het grote voordeel hiervan is dat de accountants en IT-auditor elkaar beter zullen begrijpen. Bundeling van kennis binnen een multidisciplinair audit team biedt veel mogelijkheden om tot een efficiëntere audit te komen.

Taak IT-auditor binnen A-team

De verwachting is dat de auditor de eerste periode voornamelijk bezig is met het vormgeven van de P&C cyclus op informatievoorziening gebied en daarna de periodieke interne audits voor zijn of haar rekening neemt (qua timing en ritme in lijn met de P&C producten). Als de general IT controls adequaat werken de gewenste application controls

[13] Voorbeeld: https://www.compact.nl/articles/accountant-en-it-auditor-samenwerking-in-de-praktijk/

[14] Audit risks omvat factoren die een afwijking, fout of nalatigheid kunnen veroorzaken in de jaarrekening. Business risks hebben betrekking op het bedrijf/gemeente zelf, met inbegrip van de stakeholders

ingebouwd zijn, zal dit een uiteindelijke lastenvermindering/verschuiving van werk kunnen betekenen voor de (financiële tak van het) audit team.

Gezien dat de normenkaders gesteld in ENSIA & BIG niet enkel betrekking hebben op financiële processen en er binnen de gemeente een groot onontgonnen terrein is op het gebied van application control, is er een afweging te maken ten overstaande van het takenpakket van de aan te stellen IT auditor. Ofwel de focus ligt op *verdieping*[15] van de (financiële) controlewerkzaamheden of wel op de *verbreding* van de controlewerkzaamheden .

Conclusie

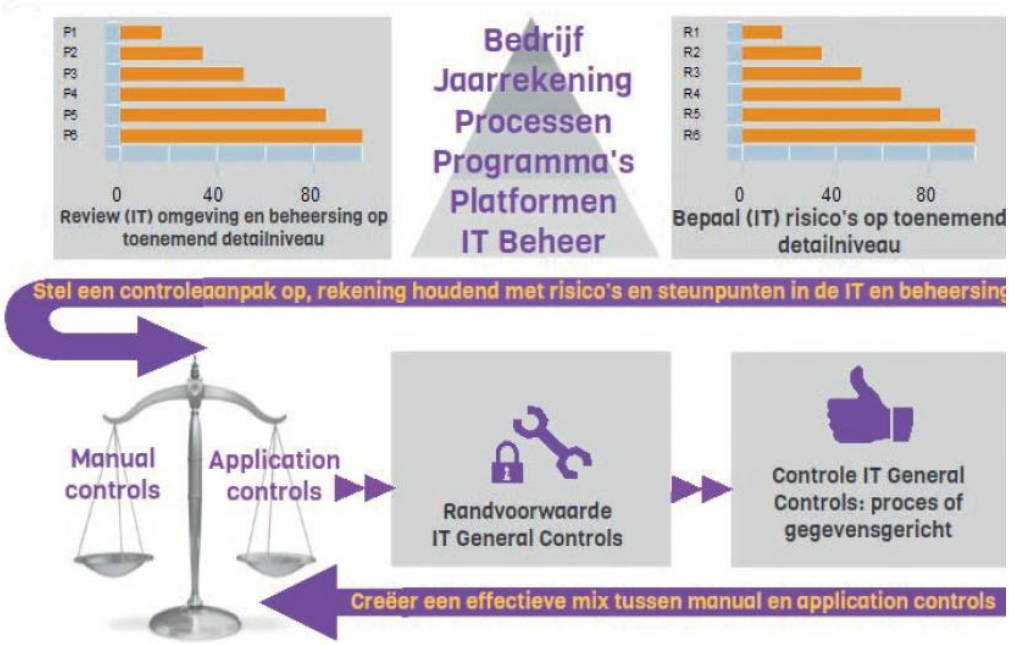
De informatievoorziening van Gemeente Haarlem moet een grotere plaats krijgen in Planning & Control-cyclus. De organisatie dwingt zich daarmee om ieder jaar te verbeteren en deze verbeteringen te waarborgen. Gezien de vergaande samenhang tussen interne (financiële) beheersing en informatietechnologie, is er noodzaak om het verantwoordingsproces over de informatievoorziening bij de gemeente verder te professionaliseren. Hierdoor is er naast de huidige interne auditors op het gebied van financiën is een interne auditor nodig gespecialiseerd in het auditen van de informatievoorziening. Investeren in een IT-audit aan de voorkant, oftewel geïntegreerd bij het werkproces, zorgt voor eigen inzicht in de mogelijke risico's als gevolg van de geautomatiseerde gegevensverwerking. Noodzakelijke aanpassingen / uit te voeren werkzaamheden kunnen hierdoor reeds in een vroegtijdig stadium worden opgepakt zonder dat voor dit aspect op de bevindingen van de externe accountant gewacht moet worden. Dit draagt bij aan een verbeterde risicobeheersing en bespaard tijd bij de externe accountantscontrole. Door de IT-auditor ook te positioneren binnen het audit-team onder de concerncontroller is de onafhankelijke positie van de auditor geborgd. Hiermee zal de gemeente haar zelf controlerend vermogen versterken en self-compliant zijn/blijven (zowel op FA als IT gebied).

[15] Waarbij de vraag is in hoeverre verdieping mogelijk is zonder voorafgaande verbreding (general IT controls & application controls) ten behoeve van de betrouwbaarheid van het lijstwerk waar de accountant op steunt. Zie: bijlage en eerdere paragraaf; Accountant moet kunnen steunen op lijstwerk IT.

Bijlage: Integrated Audit Approach

Schellevis, W. & van Dijk, V. (2014) Jaarrekening controle in het mkb: IT audit geïntegreerd in de controle-aanpak

De "integrated audit approach[16]" is een aanpak ontwikkeld door de NBA en NOREA, om IT in de controle aanpak te integreren. Gebaseerd op een risicoanalyse komt de controleaanpak tot stand:



Vervolgens bij de uitvoering van een geïntegreerde IT audit, wordt er de aanbeveling gedaan te starten met testen van de general IT controls. Zodat bij eventuele ontoereikende controls direct de controleaanpak kan worden herzien (algemene IT randvoorwaarden). Vervolgens worden de geselecteerde application controls getest - mede ingegeven door de normenkaders gesteld in ENSIA & BIG. Aanvullend op deze controle werkzaamheden worden overige (gegevensgerichte) controle werkzaamheden uitgevoerd die noodzakelijk zijn voor het verkrijgen van voldoende zekerheid (bijv. data-analyse).

[16] Schellevis, W. & van Dijk, V. (2014) Jaarrekening controle in het mkb: IT audit geïntegreerd in de controle-aanpak. https://www.nba.nl/Vaktechniek/Vaktechnische-themas/ICTXBRL/IT-Audit/