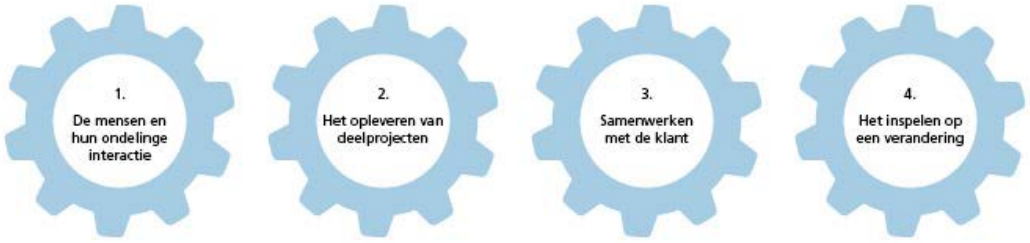
Deel 2: De agile-succesfactoren toegepast

Interne (IT-)auditor levert meer waarde met een 'Audit Manifesto'

4 december 2020

Edwin Galama

Dit is deel 2 van mijn tweedelige artikel over de richting waarin onze beroepsgroep zou moeten bewegen om te blijven aansluiten op de trend van de agile-transformatie. Deel 1 ging over het agile-gedachtengoed, het 'Manifesto for agile software development' uit 2001 (hierna: Agile Manifesto [AGIL01]), de belangrijkste veranderingen (*shifts*) bij een agile-transformatie en de vier agile-succesfactoren. In dit tweede deel pas ik de vier agile-succesfactoren toe op de werkwijze van een IT-auditor. Het resultaat is een concreet Audit Manifesto voor de IT-auditor. Net als het *Agile* Manifesto heeft dit *Audit* Manifesto vier kernwaarden en twaalf principes; deze stellen IT-auditors in staat hun opdrachtgevers meer zichtbare toegevoegde waarde te leveren. In figuur 1 zijn de vier agile-succesfactoren uit deel 1 opnieuw weergegeven.



Figuur 1: De vier agile-succesfactoren van agile

De huidige werkwijze van de IT-auditor is veelal proces- en plan-gedreven en gebaseerd op traditionele normenkaders. Met de (paradigma)shift in het achterhoofd zullen ook IT-auditors hun werkwijze moeten transformeren van een proces-gedreven naar een meer verander-gedreven aanpak. Dit kan door de agile-succesfactoren toe te passen. Voordat ik de agile-succesfactoren concreet toepas op het auditproces, volgen hierna enkele randvoorwaarden en uitgangspunten.

Alleen met een agile-mindset kan een auditteam de agile-succesfactoren goed toepassen. Hiervoor is een goed begrip van het agile-gedachtengoed en de onderliggende shifts noodzakelijk. De ervaring die de IT-auditor opdoet met het toepassen van deze agile-succesfactoren is essentieel om zelf een beoordeling te kunnen doen op bijvoorbeeld een agile IT-voortbrengingsproces. Het begrip en de ervaring van de agile manier van werken is daarom van groot belang voor de IT-auditor om te blijven aansluiten op de agile-transformatie die gaande is.

Door de agile-succesfactoren toe te passen, kan de IT-auditor meer toegevoegde waarde leveren. De toegevoegde waarde van de IT-auditor is het meest concreet zichtbaar in de gerapporteerde verbeterpunten gericht op de interne beheersing en staat centraal in dit artikel. Hoe eerder in het auditproces het inzicht in deze verbeterpunten wordt verstrekt, hoe meer toegevoegde waarde de opdrachtgever zal ervaren. Hiernaast leveren IT-auditors ook waarde door met hun opdrachtgevers in gesprek te gaan over de noodzaak van adequate interne beheersing, en deze te laten aansluiten bij de agile-benadering. Het intensiveren van de interactie met de opdrachtgevers is geborgd in de toepassing van de agile-succesfactoren.

Zoals in Deel 1 toegelicht, heb ik ervoor gekozen zoveel mogelijk de spelregels van Scrum te gebruiken voor het toepassen van de agile-succesfactoren. Deze agile-werkwijze en haar spelregels zijn erop gericht het meest waardevolle op te leveren binnen de beperkingen van tijd en budget. De spelregels en definities voor de manier van werken volgens Scrum staan in de zogenoemde Scrum-gids, die door Ken Schwaber en Jeff Sutherland in 2016 is opgesteld. [SCRU17] Met het omarmen van de Scrum-spelregels wordt ook al ingespeeld op een aantal belangrijke shifts uit deel 1.

De IT-auditor moet vanuit een agile-mindset kunnen werken en tegelijkertijd de beroepsregels in het oog houden. Belangrijke beroepsvoorwaarden liggen op het terrein van objectiviteit, onderbouwing uitkomsten, documentatie, inschakelen deskundigen en geheimhouding. De IT-auditor kan naar de opdrachtgevers veel transparanter zijn dan gebruikelijk over de na te leven beroepsregels. We kunnen actiever de beroepsregels uitleggen aan onze opdrachtgevers. Hierdoor ontwikkelen onze opdrachtgevers meer kennis en begrip over onze rol, wat de samenwerking bevordert.

In de volgende paragrafen pas ik de vier agile-succesfactoren toe op het auditproces en de werkwijze van de IT-auditor voor een intern agile-auditteam.

Succesfactor 1. De mensen en hun onderlinge interactie

Deze succesfactor is vooral gericht op het interne auditteam zelf, maar komt ook terug bij de derde succesfactor: samenwerken met de klant. De IT-auditor werkt zoveel mogelijk multidisciplinair samen met collega's uit andere auditdisciplines zoals financial audit, operational audit en met andere specifieke deskundigen zoals de data-analist, non-functional specialisten, toolspecialisten en dergelijke. Met de introductie van *Scrum-gebeurtenissen* zoals *stand-ups*, *sprints* en *retrospectives* zal meer onderlinge interactie en feedback ontstaan.

Bij de onderlinge interactie tussen teamleden en de overige deskundigen moet transparantie en kennisdeling het uitgangspunt zijn, gericht op het gezamenlijke doel. Indien de IT-auditor samenwerkt met specifieke deskundigen is het van belang dat de auditor de beroepsregels voor het inschakelen van deskundigen blijft naleven. Dit betekent dat de werkzaamheden van de deskundige, zoals gebruikelijk, goed onderbouwd moeten worden gedocumenteerd in relatie tot de zelfstandig gerapporteerde uitkomsten en verbeterpunten van de IT-auditor. Vanuit onze beroepsregels rondom geheimhouding voelt het streven naar transparantie én kennisdeling wellicht tegenstrijding. We kunnen echter in overleg met de opdrachtgever veel meer informatie delen dan we denken.

Het auditteam inspecteert voortdurend of teamverbeteringen mogelijk zijn wat betreft het functioneren van de teamleden, de onderlinge relaties en de beschikbaarheid van kennis en tools. Hiervoor wordt na afloop van elke periode (*timebox*) een retrospective georganiseerd.

In overleg met de opdrachtgevers en relevante kennishebbers worden de te onderzoeken auditonderwerpen via een organisatiebrede risicoanalyse op de auditbacklog geplaatst. Alleen auditonderwerpen die voldoen aan de *definition of ready* (DOR) kunnen op de auditbacklog worden opgenomen. Met de DOR wordt geborgd dat de auditonderwerpen op de auditbacklog voldoen aan eisen zoals omvang, mate van detaillering, kennisniveau en verwachte doorlooptijd. Dit als voorwaarde om binnen de vastgestelde timebox te blijven. De auditonderwerpen worden voortdurend geprioriteerd op de auditbacklog, waarbij een vaktechnisch aandachtpunt is dat de IT-auditor bij herprioritering de risicoafwegingen goed documenteert.

Het auditteam werkt als een zelfsturend team en kan zo zelfstandig en sneller beslissingen nemen over de uit te voeren auditonderwerpen, waarbij alle belangen en behoeften van de stakeholders zorgvuldig worden afgewogen. De opdrachtgever (bestuur, toezichthouder, auditcommissie) vertrouwt dat het auditteam het gewenste gedrag en eigenaarschap laat zien en faciliteert het auditteam op het gebied van kennis en competenties om adequate besluiten te nemen. Dit vertrouwen sluit aan bij de *bottom-up* gedachte van Scrum en draagt bij aan de volgens onze *code of ethics* vereiste objectieve positie van het auditteam.

Succesfactor 2. Het opleveren van deelprojecten (verbeterpunten)

De audit-tegenhanger van de deelprojecten bij Scrum zijn de gerapporteerde verbeterpunten voor de interne beheersing. De IT-auditor kan regelmatiger, eerder en adoptiever (gericht op adoptie door de opdrachtgever) inzicht in die verbeterpunten geven. We moeten daarbij korter, meer *to the point* en meer visueel rapporteren. De theoretische vaktechnische aspecten moeten in de eindrapportage tot een minimum worden beperkt. Het begrip 'adoptie' staat in de agile-benadering voor begrip en acceptatie van de

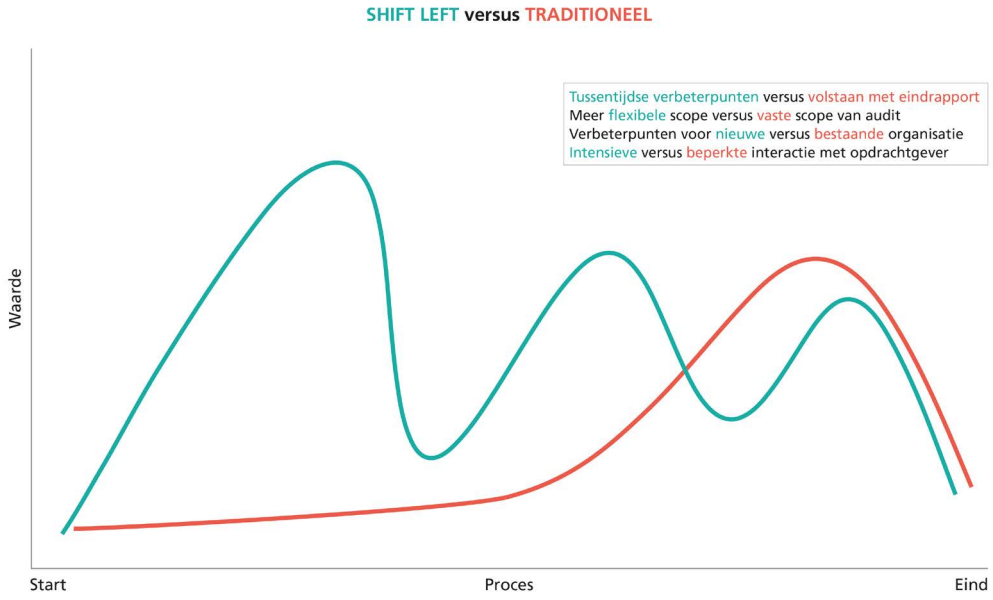
verbeterpunten bij de opdrachtgever en de wil om het verbeterpunt te willen opvolgen.

Met de DOR borgt de IT-auditor dat de auditonderwerpen voldoende concreet, gedetailleerd en niet te omvangrijk zijn. Hierdoor kunnen auditteam en opdrachtgever goed overzien wat het object van onderzoek is en kunnen de verbeterpunten verstrekt worden met de regelmaat van de timebox, of eerder al tijdens de audit.

De adoptie van de verbeterpunten wordt vergroot door de verbeterpunten samen met de opdrachtgever en de personen die de opvolging moeten gaan realiseren tot stand te laten komen.

De shift-left houdt in dat dat wij al gedurende onze audits de verbeterpunten kenbaar maken en goed bespreken, in plaats van pas bij afronding. Hierdoor is het mogelijk om verbeterpunten eerder onder de aandacht te brengen. Daarnaast is de IT-auditor met een faciliterende interactie met opdrachtgevers in staat bij het inrichten van processen dan wel bij de ontwikkeling van systemen, waarde te leveren door verbeterpunten aan te dragen.

Deze shift-left raakt de kern van het toepassen van de agile-succesfactoren voor de IT-auditor. Voor de duidelijkheid: met 'faciliteren' bedoel ik niet dat IT-auditors hun opdrachtgever moeten gaan helpen met het daadwerkelijk inrichten van de processen en systemen. Ik doel op de mindset van de IT-auditor om samen met de opdrachtgevers en andere tweedelijns-kennishebbers de interne beheersing te verbeteren. De IT-auditor moet immers objectief blijven om de processen en systemen te kunnen blijven beoordelen.



Figuur 2: Shift-left

Samenvattend: de shift-left stelt de IT-auditor in staat de opdrachtgever eerder, regelmatiger en meer adoptief verbeterpunten aan te leveren. Hoe eerder inzicht in verbeterpunten voor de interne beheersing wordt verstrekt, hoe meer toegevoegde waarde de opdrachtgever krijgt en ervaart.

Succesfactor 3. Samenwerken met de klant

Met het omarmen van Scrum in het auditproces zal de IT-auditor, regelmatiger dan bij reguliere audits het geval is, contact met de klanten (opdrachtgevers) hebben over relevante auditonderwerpen voor de auditbacklog. Door meer transparantie in de gehanteerde normstellingen ontstaan meer gezamenlijk gedragen doelstellingen. Dit bevordert de samenwerking en kennisdeling.

Bij niet-agile methoden worden prioriteiten vaak door het interne auditteam alleen bepaald. In een agile-aanpak evalueert de IT-auditor samen met de opdrachtgever gedurende de uitvoering van de audits de auditonderwerpen op de backlog en vraagt regelmatig om feedback, gericht op maximalisatie van de toegevoegde waarde. De opdrachtgever krijgt hierdoor ook beter zicht op waar de IT-auditor zich op wil richten. IT-auditors blijven bij deze intensievere samenwerking alert op hun objectiviteit bij het bepalen van de te beoordelen interne beheersing.

De timing van de audits sluit zoveel mogelijk aan op de cadans (planning & control cyclus) van de opdrachtgever en de organisatie.

Bij de uitvoering van de audits let de IT-auditor erop dat het proces van de opdrachtgever zo min mogelijk wordt verstoord. De IT-auditor zal meer gebruik moeten maken van observatietechnieken en eventueel naderhand verdiepingsinterviews. Als de IT-auditor bijvoorbeeld binnen een agile IT-voorbrengingsproces de toepassing en kwaliteit van de retrospective wil beoordelen, zal hij deze bijwonen zonder veel vragen te stellen en naderhand verdiepingsvragen/interviews houden. Hierdoor is de IT-auditor ook in staat om de meer mens en cultuur gerichte aspecten te beoordelen. Tevens zijn er minder uitgebreide notulen/vastleggingen beschikbaar van de retrospectives omdat het agile-werken streeft naar minimale documentatie. De interviewtechniek moet vooral gericht zijn op het resultaat van de te ontwikkelen applicatie. Dit kan de IT-auditor doen door bijvoorbeeld te vragen naar de omvang en oorzaken van *rework* (extra werk dat nodig is om achteraf tekortkomingen te herstellen). Zo komen relevante verbeterpunten voor de interne beheersing meer in de taal van de opdrachtgever naar boven.

Gedurende de uitvoering van de audits evalueert de IT-auditor met de opdrachtgever de auditonderwerpen op de backlog en vraagt regelmatig om feedback, gericht op maximalisatie van de toegevoegde waarde. De IT-auditor stelt zich kwetsbaarder op en agendeert bij de eindbespreking standaard een slot-evaluatiemoment.

De IT-auditor levert met de regelmatige inzichten in verbeterpunten toegevoegde waarde. Het streven naar transparantie en kennisdeling over bijvoorbeeld gehanteerde normenkaders, manier van werken en naleven van beroepsregels draagt bovendien bij aan de samenwerking.

De focus moet vooral gericht zijn op het gezamenlijke belang de interne beheersing te verbeteren. IT-auditors kunnen een meer faciliterende houding en instelling naar hun opdrachtgevers aannemen. Met een faciliterende houding van de IT-auditor zal de opdrachtgever ook gemakkelijker een hulpvraag op tafel leggen. Voor de duidelijkheid: de IT-audit stelt zich faciliterend op, maar blijft objectief. Zoals ook al aangegeven bij de eerste succesfactor, blijft het interne auditteam apart als zelfstandig team bestaan. Hiermee is het interne auditteam uitgezonderd van het streven naar een volledig met de business geïntegreerd ontwikkelteam voor een agile IT-voortbrengingsproces.

Door de intensievere samenwerking tussen de IT-auditor en opdrachtgever ontstaat bij de opdrachtgever meer inzicht in normen, risico's en interne beheersing.

Succesfactor 4. Het inspelen op een verandering

Inspelen op veranderingen zit verankerd in de vorige drie agile-succesfactoren. In dit verband is een belangrijke shift voor de IT-auditor om de auditbacklog met auditonderwerpen en scope van de audits flexibeler te maken, al naar gelang de omstandigheden. Wel moeten wijzigingen in de backlog en scope van het onderzoek goed onderbouwd gedocumenteerd worden.

De IT-auditor moet zich bij de nieuwe manier van werken bewust zijn van de in deel 1 behandelde shifts:

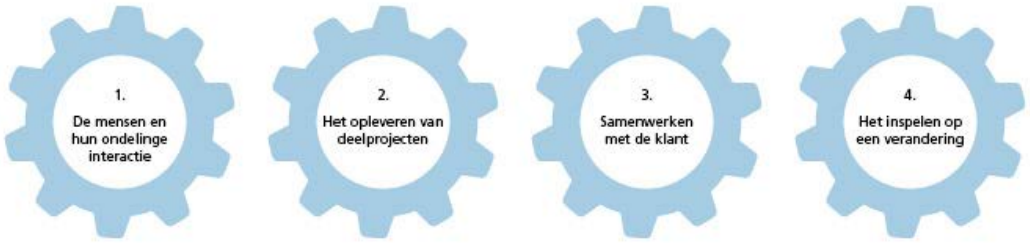
- Van plan naar verandergedreven (paradigma-shift)
- Naar voren in het proces (shift-left)
- Van proces naar resultaat gericht
- Van top-down naar bottum-up.

De bewustwording in deze shifts stelt IT-auditors in staat om proactief in te spelen op de veranderende interne beheersing van hun onderzoekobjecten.
Het stelsel van de interne beheersing voor bijvoorbeeld het (agile) IT-voorbrengingsproces transformeert van procesgericht naar meer cultuur- en techniekgericht. Inherent aan een cultuurverandering kan dit transformatieproces soms wel enkele jaren duren. Hierdoor is vaak sprake van verschillende volwassenheidsniveaus en dus van hybride situaties die traditionele beheersing en agile-beheersing combineren.

Transformatie van de interne beheersing vraagt om een geschikt normenkader, vast te stellen door de IT-auditor en de opdrachtgever samen. Het normenkader is beperkt tot het minimaal noodzakelijke, dat wil zeggen enkel gericht op samen onderkende risico's of ontwikkelgebieden. Het wordt aangepast als de omstandigheden hierom vragen. In mijn scriptie heb ik op basis van de verkregen inzichten een richtinggevend beheerskader opgenomen voor het IT-voortbrengingsproces. [GALA20]

AFSLUITING

De vier agile-succesfactoren van de softwareontwikkelaar zijn door de IT-auditor zinvol toe te passen. De vier moeten wel als één geheel worden toegepast, omdat ze elkaar aanvullen en invloed op elkaar hebben – vandaar de visualisering als tandwielen.



Figuur 3: Nogmaals de vier agile succesfactoren

Belangrijk is dat de IT-auditor in een eigen zelfsturend auditteam blijft werken en geen onderdeel is van het geïntegreerd multidisciplinaire ontwikkelteam binnen het agile IT-voortbrengingsproces. Hiermee borgen wij onze objectieve positie binnen de organisatie.

In dit artikel is meermaals aangegeven dat veranderen een samenspel is tussen IT-auditor en opdrachtgever; we moeten elkaar dus opzoeken. Zo maakt de IT-auditor een shift-left en zouden onze opdrachtgevers van hun kant eerder aan ons moeten denken. Door de nieuwe manier van werken van de IT-ontwikkelteams past de IT-auditor het auditproces en de normenkaders aan. Met het omarmen van de Scrum-spelregels ontstaat meer interactie tussen de teamleden, kennishebbers en opdrachtgevers. Daarnaast kunnen eerder, concreter en meer adoptief verbeterpunten voor de interne beheersing opgeleverd worden.
Met het bewust zijn van de shifts kan de IT-auditor samen met de opdrachtgevers tot een geschikter normenkader komen. Dit is nodig gezien de transformatie van procesgerichte naar cultuur- en techniekgerichte interne beheersing. Belangrijk voor de IT-auditor is om de reguliere beroepsregels te blijven respecteren en ze aan de opdrachtgever uit te leggen. Hierdoor kan de scope vaker wijzigen en kan meer informatie worden gedeeld, terwijl we de beroepsregels blijven naleven.

De vier agile-succesfactoren stellen de IT-auditor in staat om de opdrachtgever beter zichtbare toegevoegde waarde te leveren, gericht op het verbeteren van de interne beheersing. De opdrachtgever begrijpt onze rol beter en we werken meer vanuit een gezamenlijk doel.

Het toepassen van de agile-succesfactoren is samen te vatten in een Audit Manifesto met vier kernwaarden en twaalf principes, zie het tekstkader 'Audit Manifesto'.

Audit Manifesto

Kernwaarden

In de formulering van de kernwaarden geeft het woord 'boven' aan dat wat aan de rechterkant staat weliswaar belangrijk blijft, maar dat wat links staat wezenlijk is in de agile benadering.

- Transparante interactie gericht op kennisdeling boven geheimhouding
- Regelmatig adoptieve verbeterpunten boven vaktechnische eindrapportages.
- Faciliterende houding boven objectiveren
- Culturele en technische beheersing boven procesbeheersing

Principes

1. Ervaar en begrijp de agile manier van werken en haar shifts.
2. Verrijk het auditproces met een agile (Scrum-spelregels) manier van werken.
3. Streef naar transparantie en kennisoverdracht voor een gezamenlijk doel.
4. Respecteer onze beroepsregels en leg ze uit aan de opdrachtgever.
5. Streef naar een zelfsturend (objectief) agile auditteam.
6. Neem als auditteam een faciliterende houding aan naar de opdrachtgevers
7. Werk multidisciplinair met (externe) kennishebbers en (agile) auditors.
8. Leg uit, evalueer, wijzig waar nodig en streef naar eenvoudige en enkel relevante normenkaders.
9. Pas de werkwijze aan door observatie en interviews gericht op de resultaten.
10. Voer de werkzaamheden uit in de cadans van de organisatie.
11. Pas de auditonderwerpen en scoping aan als de omstandigheden dit rechtvaardigen.
12. Verstrek eerder, regelmatiger en meer adoptief verbeterpunten voor de interne beheersing.

Literatuur

[AGIL01] agilemanifesto.org, *Manifesto for agile Software Development*, 2001, http://agilemanifesto.org, geraadpleegd op 2 september 2020.

[SCRU17] Scrum Guides, *De ScrumGids – De definitieve gids voor Scrum: De regels van het spel*, https://www.scrumguides.org/docs/scrumguide/v2017/2017-Scrum-Guide-Dutch.pdf, 2017, geraadpleegd op 2 september 2020.

[GALA20] Edwin Galama, afstudeerscriptie: *Agile IT voortbrengingsproces, inzichten en handvaten voor de IT auditor*, 10 januari 2020. Op aanvraag via mail verkrijgbaar bij de auteur: edwin.galama@gmail.com.

E.N. (Edwin) Galama RA | Senior interne auditor bij *het CJIB*

Edwin Galama werkte van 1996 tot en met 2010 bij EY, waarvan vier jaar op de Nederlandse Antillen. Als externe registeraccountant was hij in de functie van auditmanager verantwoordelijk voor jaarrekeningcontroles en diverse bijzondere onderzoeken, waarvan veel in de publieke sector. In 2010 maakte hij de overstap naar de interne auditafdeling van het Centraal Justitioneel Incasso Bureau (CJIB). Het CJIB is het grootste software house van Friesland met veel financiële stromen, waar Edwin met nog vier collega's de interne auditfunctie verzorgt. Sinds de onlangs afgeronde eenjarige opleiding voor IT-auditor aan de Universiteit van Amsterdam, verschuiven de werkzaamheden steeds meer van het beoordelen van financiële stromen naar de (onderliggende) ICT-processen en -omgevingen. Hiernaast levert hij een bijdrage binnen de NOREA-kennisgroep Software Development.