

Sommige auditonderwerpen zijn een grotere uitdaging dan andere. Wij hebben bij onze auditwerkzaamheden binnen ABN AMRO Group Audit ervaren hoe het is om agile-processen te auditen. En dat vinden we best lastig. In dit artikel delen we ervaringen en dilemma's.

# Audit en agile: een mooi duo?

Als je agile in het woordenboek opzoekt vind je vertalingen variërend van 'vlot' en 'alert' tot 'beweeglijk' en 'slagvaardig'. Het woord agile kreeg in 2001 meer betekenis doordat een aantal gelijkgestemden uit de IT-wereld het *Manifesto for agile software development* opstelde met als doel om de klassieke en de rigide waterval ontwikkelmethodieken (zoals Prince2) door een meer flexibele aanpak te vervangen.

Het Agile Manifesto is gebaseerd op vier waarden:

1. Mensen en hun onderlinge interactie boven processen en tools.
2. Werkende software boven allesomvattende documentatie.
3. samenwerking met de klant boven contract onderhandelingen.
4. Inspecteren op verandering boven het volgen van een plan.

## Hoe werkt agile binnen de organisatie?

Binnen ABN AMRO betekent de agile-werkwijze dat scrum-teams van maximaal negen collega's uit de business en IT dag in, dag uit intensief samenwerken. Elk team heeft zijn eigen doel (bijvoorbeeld het maken van een nieuwe app voor beleggen) en beschikt daarvoor over alle competenties (IT, product- en klantkennis, et cetera).

Scrum-teams werken in sprints (time boxes variërend van een tot vier weken) aan oplossingen voor klantwensen (user stories). Aan het eind van elke sprint volgt een sprint review. Het team en de product owner demonstreren dan hun resultaten, bijvoorbeeld nieuwe schermen voor de beleggingsapp, aan de stakeholders: klantpanels, verkoop-, product-, risk ma-

nagement en supportafdelingen of anderen. Met hun feedback bepaalt het team of de oplossingen goed genoeg zijn. Dit is een iteratief proces waarbij steeds feedback wordt gevraagd en een opgeleverde oplossing in opeenvolgende sprints telkens beter wordt. De product owners registreren ideeën en wensen tijdens dit proces in zogenaamde backlogs, een soort van werkvoorraad. Zie *figuur 1* voor het sprintproces.

## Wat maakt het auditen van een agile-proces anders?

'IT-ers leveren geen documentatie meer op. Accepteren doet de business in een demoesessie. Het management heft alle programboards op. Er zijn nu zelfsturende teams. In een week of drie gaat het van specificaties naar productie. En het hoofd Audit wil dat wij met standaard audittemplates werken en onze dossiervorming en afstemming net zoals altijd doen... Ja ja, en hoe gaan wij dit auditen?' Zo ongeveer klonk onze eerste kennismaking met agile. De invoering van agile zorgde voor een aantal dilemma's wat betreft onze auditwerkzaamheden, te weten:

## Aansturing met een flexibele scope

De ontwikkelteams werken in time boxes met een vaste capaciteit. De product owner houdt een backlog bij met mogelijke deliverables en bepaalt per sprint welke programmatuur door het ontwikkelteam gemaakt wordt. Deze aanpak maakt het vooraf bepalen van de scope van een audit veel ingewikkelder, omdat je pas bij het starten van de sprints weet wat opgeleverd gaat worden. Kortom, een belangrijke uitdaging is hoe je de scope van je audit op een juiste manier bepaalt.

### **Een volledige oplossing (met alles erop en eraan) is geen doel**

Initieel worden oplossingen bewust 'klein' gehouden (minimum viable products – MVP's) en daarna sprint na sprint steeds verder ontwikkeld. Een zorgvuldig afgestemd auditrapport over de eerste sprint heeft weinig toegevoegde waarde voor de opdrachtgever als het scrum-team ondertussen bij de vierde sprint is waarin tekortkomingen al zijn opgelost. Een uitdaging is hoe je auditbevindingen tijdig rapporteert, zodat deze bevindingen op het goede moment kunnen worden meegenomen in het ontwikkelproces.

### **Multidisciplinaire scrum-teams vervangen programma- en projectgovernancestructuren**

Ontwikkelaars delen stuurinformatie en verantwoordingsrapportages dagelijks, bijvoorbeeld met een Jira board (elektronisch whiteboard). Er worden geen aparte managementrapportages meer gemaakt. De kortcyclische benadering en een multidisciplinaire zelforganiserende agile-aanpak maken dat teams meer dan in de oude situatie zelf verantwoordelijk zijn voor sturing en kwaliteit van risico- en interne controlemaatregelen. Er zijn minder harde overdrachtsmomenten, bijvoorbeeld tussen ontwikkelen, testen en accepteren van programmatuur en ook afzonderlijke quality-assurancefuncties ontbreken soms. Het dilemma is hoe je assurance geeft over het goed functioneren van de AO/IC rond het ontwikkelproces, en van de opgeleverde oplossingen en programmatuur.

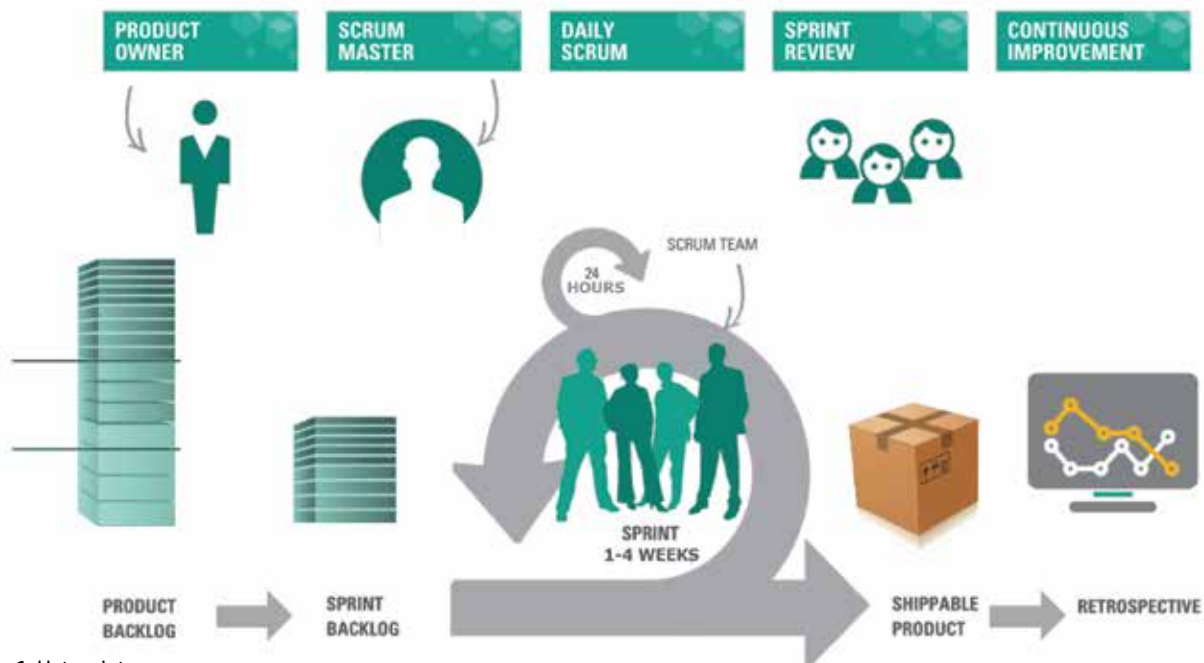
### **Meer accent op soft dan op hard controls**

Nieuwe functionaliteit wordt niet meer gedocumenteerd maar besproken in demosesies, daily huddles, team sync of MT meetings, en hangt aan de muur in de vorm van tientallen post-its of A4-posters. Het testen en het uitvoeren van kwaliteitscontroles vindt continu plaats door het scrum-team en niet aan het eind van een ontwikkeltraject. Een goede samenwerking en teamsamenstelling is dus vereist. We hebben binnen onze IAF een opleidingstraject Auditen van cultuur en gedrag gehad en passen dit meer en meer toe bij de audit van agile-processen.

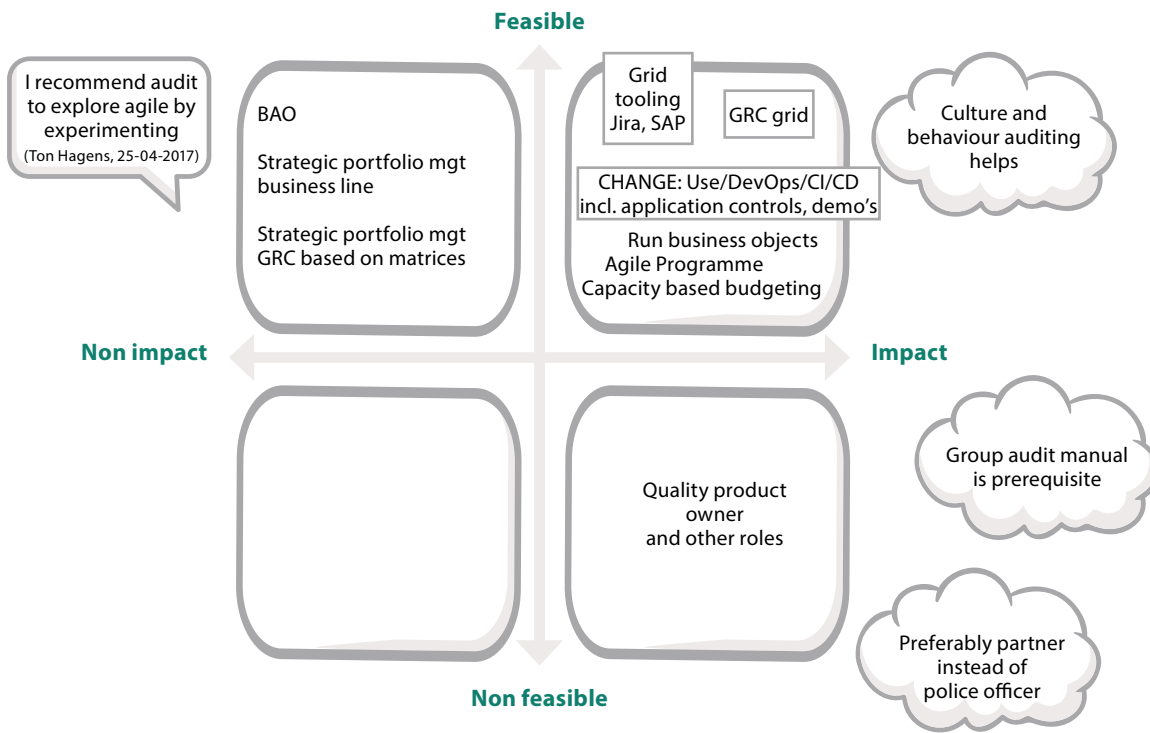
### **Hoe gaan wij als auditors met de veranderingen om?**

Agile verandert de manier waarop software ontwikkeld wordt. Dit heeft direct impact op onze manier van auditen. Hoe ga je hier als internal auditafdeling mee om? Vijf nuttige tips.

1. **Stimuleer enthousiasme** – Niet iedereen binnen de IAF is vooraf positief over agile. Laat een aantal internal auditors die geïnteresseerd zijn in agile een inventarisatie maken van de mogelijke auditonderwerpen. Rubriceer deze onderwerpen op impact en uitvoerbaarheid (zie *figuur 2* voor een voorbeeld). Voer daarna een aantal audits uit, op een agile-maniër, dus in sprints en deel de resultaten. Ofwel, learning by doing.
2. **Geef aandacht aan soft controls** – Agile vereist meer aandacht voor cultuur en gedragsaspecten omdat goede samenwerking essentieel is. Observatie geeft een goed beeld van de cultuur en gedragsaspecten (soft controls) bijvoorbeeld door demosesies te observeren. Ook is het mogelijk om mensen te interviewen over de kwaliteit van de samenwerking.
3. **Nodig gastsprekers uit** – Regelmatig delen de product owners, de ontwikkelaars en de scrum masters hun kennis en ervaring van agile met internal auditors. Internal auditors die minder affiniteit met agile hebben, kunnen zo in het agile-gedachtegoed worden meegenomen. Verder kunnen ze in dialogen met collega's uit het bedrijf wettelijk aan de praktische implicaties van deze nieuwe manier van werken.
4. **Zorg voor aangepaste (agile-)controleprogramma's** – In auditteams bediscussiëren van 'oude' auditprogramma's en deze transformeren naar een agile-omgeving is een leuke uitdaging. Je ziet dat de traditionele manier van auditen zoals dat ooit is opgeschreven niet past bij de agile-aanpak. Zo krijgen internal auditors beter inzicht in het effect van agile. Er is ook een agile e-learning opgenomen in het auditopleidingscurriculum.
5. **Experimenteer met audits in sprints** – Audits kun je opknippen in sprints van twee weken, om zo per sprint assurance aan de opdrachtgever te geven over een deel van de key controls. Dit kan door middel van een rapport maar ook in een gallery walk. Hierbij neem je de auditee mee in de audit met observaties en quotes van auditees op posters 'aan de muur'. De dynamiek van gallery walks kan leiden tot meer open discussies en betere oplossingen dan de traditionele slotbesprekingen van rapporten. Door een snellere en meer



**Figuur 1.** Het sprintproces



**Figuur 2.** Inventarisatie, impact en uitvoerbaarheid mogelijke auditonderwerpen

gevisualiseerde terugkoppeling aan de opdrachtgever en andere stakeholders worden bevindingen en risico's meteen duidelijk na iedere sprint en niet pas aan het eind van de audit. Zowel internal auditors als auditees blijken enthousiast over deze aanpak, en de klanttevredenheid verhoogt de acceptatie en toegevoegde waarde van audits.

#### Welke invloed heeft agile op de organisatie van de IAF?

De invoering van agile heeft ook impact op de organisatie van onze IAF:

- Bij ABN AMRO zijn IT-auditors (RE's), data-analisten en andere specialisten organisatorisch bij elkaar ondergebracht in auditteams om met een multidisciplinaire blik naar nieuwe ontwikkelingen te kijken. Zo spiegelen we ons met de multidisciplinaire agile-ontwikkelteams. Auditprofessionals uit de verschillende teams met een specifieke expertise zoals IT of betalingsverkeer, komen regelmatig bij elkaar om best practices uit te wisselen en auditstandaards te waarborgen.

#### Wat vinden wij van het auditen van agile?

De invoering van agile is een uitdaging voor internal auditors. Standaarden, normen en aanpak voor het auditen van agile-processen zijn niet vastomlijnd. Dit voelt soms ongemakkelijk, maar leidt ook tot mooie nieuwe, originele en uitdagende vragen als:

- Zijn foto's van posters en schermen die je bij een demosessie maakt evidence? Voeg je deze toe in je auditdossier?
- Als je staand bij een demo je mening geeft over nieuwe functionaliteit, leg je dit dan alsnog vast, stem je af en verstuur je je memo wanneer de sprint is afgerond?
- Hoe ziet een agile-auditrapport eruit en hoe zorg je voor een time-to-market die past bij het tempo van sprints?
- De product owner plaatst mijn auditissue op een backlog, zonder duidelijke deadline. Is dit acceptabel?

## De dynamiek van gallery walks kan leiden tot meer open discussies en betere oplossingen

- Een auditteam dat agile werkt heeft voordeel bij het hantieren van aangepaste auditrollen, bijvoorbeeld een auditmanager die als een product owner prioriteiten stelt voor de audit sprints of iemand die binnen het team de coachende rol van scrum master vervult.
- Voor de visualisatie van de bevindingen is de aanwezigheid van creatieve vaardigheden een absolute must.
- Auditteams opereren in een wereld met credo's als 'mensen en hun interactie boven processen en tools' en 'inspelen op verandering boven het volgen van een plan', waar werkprogramma's en templates voor systeem- en productontwikkeling met focus op hard controls minder goed bruikbaar blijken te zijn. Nieuwe werkprogramma's en templates met meer aandacht voor cultuur en gedrag blijken beter bruikbaar.

Nieuwe en opkomende vragen die ons aan het denken zetten. Kennis van het internal auditvak, de businessprocessen, bedrijfsdoelstellingen en bijbehorende risico's vragen zo om een frisse blik en een vernieuwende aanpak. Hoe kun je agile het best aanpakken en toegevoegde waarde blijven leveren? Dit alles is een mooie uitdaging voor de liefhebbers van het auditvak. Daarom, audit en agile, een mooi duo! <<

Hans Koster, Hugo van Bers en Herbert Pellegrom werken bij Group Audit ABN AMRO. Dit artikel is op persoonlijke titel geschreven.