

Audits temidden van misverstanden

In zijn artikel 'Audits zijn bron van misverstanden' (Automatisering Gids 11 april 2003) geeft R. Stouthart een visie op het optreden van auditors in project reviews, en signaleert hij wat een projectmanager zou moeten doen om de conclusies in zijn voordeel te draaien. Enige correctie en nuancering is geboden, om spraakverwarring te voorkomen.

Om met de deur in huis te vallen: audits zijn inderdaad een bron van misverstanden. Maar audits zijn ook, nog veel meer, slachtoffer van misverstanden.

Misverstand nummer een is dat audits alleen maar lastig zijn. Het gaat er bij audits, en bij reviews, en bij assessments, om dat de opdrachtgever een frisse blik krijgt op de stand van een project of een doorlichting van een beheerafdeling, met als einddoel betere beheersing van de processen in de organisatie. Beheersingsmaatregelen – in hedendaagse managementspeak 'controls' geheten – zijn immers wat de interne klanten, 'de business' en/of de project-opdrachtgevers, nodig hebben om 'in control' te zijn. Oftewel: de bestuurder wil stuur en pedalen plus een dashboard, anders belandt de hele organisatie in de vangrails. En kreukelzones, gordels en een setje airbags zijn toch ook wel aardig. Daar kijkt de auditor dus naar, als APK-keuring. Want zonder audits zouden onder druk van allerlei externe en interne factoren van tijd, geld, motivatie en bereidheid tot samenwerken, die beheersingsmaatregelen vaak al snel onder een aanvaardbaar niveau zakken.

Dat geldt des te meer in tijden van outsourcing, waar het voor de interne klanten steeds minder mogelijk is om eventjes bij de IT-manager te buurten om wat zaken informeel recht te zetten. Er zal meer formeel moeten worden vertrouwd op het toezicht dat auditors houden op het service management en de service delivery die buiten de deur gebeuren. En dan gaan we er voor het gemak maar vanuit dat het toezicht door auditors, in de uitbestedingscontracten goed is geregeld.

Redelijk volgens het boekje

Misverstand nummer twee is dat de auditor een strenge oom is die geen grijstinten kent. De auditor zoekt helemaal niet naar 'complete processen' (*whatever that may be*), maar is zich zeer bewust van de beperkingen die het gevecht van alledag in organisaties betekent voor de beheersingsmaatregelen. Dat is juist waarvoor de beheersingsmaatregelen bestaan – in een ideale wereld gaat immers alles vanzelf en zonder bijsturing goed, nietwaar?

Een IT-auditor spreekt, zeker als het om projecten gaat, overigens liever van een 'review'; bij een doorlichting die een audit mag heten, zal de hele projectorganisatie zo precies tegen een norm worden aangehouden dat geen project er goed vanaf kan komen. Als een auditor met een normverzameling komt, zal dat dan ook eerder een minimum- dan een maximumset zijn van wat er aan activiteiten en deliverables door het project zouden moeten worden opgeleverd. De normen worden ook in principe niet door de auditor vastgesteld, maar door de opdrachtgever, waarbij de auditor hoogstens bij gebrek daaraan een eigen verzameling zal aandragen.

Van zo'n projectaudit-tot-in-alle-detail wordt een auditor ook niet warm omdat hij (zij) heus wel dat gevecht van alledag ziet. En het exact naleven door een project van alle denkbare procedurebureaucratie is vaak niet nuttig voor het algemeen (organisatie)belang. En jawel, dat is de drijfveer van de auditor. Daardoor zal een auditor, ook bij een projectreview, niet alleen kijken naar de opzet en het bestaan maar ook naar de werking van procedures en maatregelen, én naar de werking van de deliverables. Nog steeds zijn er ook bedrijven en afdelingen die keurig netjes 'volgens ISO 9000' vierkante wielen produceren maar – misverstand nummer drie – auditors kijken wel degelijk ook naar de uiteindelijke uitkomsten, dus of de procedures en maatregelen wel hebben bereikt waarvoor ze waren ingesteld; vierkante wielen voldoen niet. Als een auditor daar niet op let, dan is dát nou iets om hem (haar) op aan te spreken.

Daarbij aansluitend zou er sprake zijn van een spanningsveld tussen auditor en manager over *evidence*. Evidence (bewijsstukken die beweringen van de gecontroleerde onderbouwen) verzamelen doen ook de grootste dorknopers onder de auditors helemaal niet voor de lol. Ook hier geldt dat de waarde die auditors, en anderen, aan evidence hechten, voortkomt uit de benodigde controleerbaarheid van het auditwerk. Die controleerbaarheid is nodig om duidelijke redenen: Een

ander moet kunnen zien dat de auditor zijn werk naar behoren heeft gedaan, zodat duidelijk is dat de bevindingen van de auditor niet voortkomen uit een onderbuikgevoel of vooroordelen – een auditor heeft ook een paar menselijke trekjes en die moeten worden tegengegaan. Kortom, de auditor doet wat hij doet niet alleen voor zijn eigen plezier.

Verwachtingen

De middelen bij uitstek om onaangename verrassingen en frustraties rond reviewuitkomsten te voorkomen, zijn dan ook het (project)werk goed doen en open kaart te spelen. Voorbereiding door alvast bij voorbaat geschut in stelling te brengen, is daarin belangrijk, niet om dat tegen de auditor te richten maar tegen de problemen waar de auditor net als ieder ander tegenaan zou kunnen lopen.

Terzijde: De auditor ziet heus wel dat auditprobleempunten net de dag voordat de auditor langskomt, zijn opgeruimd. Maar dat is niet eens zo erg, als de probleempunten maar worden opgelost... en geborgd is dat niet de volgende dag de controls weer de kast ingaan. Het heeft ook geen zin om de boodschapper aan te vallen. Dat maakt alleen maar duidelijk dat de projectmanager geen verweer heeft tegen de inhoudelijkheid van de bevindingen. Zachte, wollige formuleringen kunnen helpen, maar de goede lezer haalt de boodschap tussen de regels er toch wel uit.

Het gaat dus niet om de eigen wensen voor de uitkomsten openlijk of door verleidingstrucs te dicteren, maar om het afstemmen van de verwachtingen van de plaats van de review in het grotere geheel van project governance of bedrijfsbrede beheersing. De auditor moet daarom de verwachtingen van de projectmanager scherpstellen. En ook moeten de projectmanager én de auditor naar andere partijen duidelijk maken dat de review niet bedoeld kan zijn om een cijfer voor vlijt, ijver en netheid te geven of juist het hoofd van de projectmanager op het hakblok te leggen. De auditor kan zelf heus wel zien dat de projectmanager roeit met de riemen die hij heeft, en dat het vullen van gaten alleen gaat als ook de auditor, vaak op een hoger organisatieniveau, de lacunes duidt en de tekorten in resources eens te meer onder de aandacht brengt.

Afstandelijkheid en onafhankelijkheid van de auditor zijn dan ook nodig om op die hogere niveaus erkenning te krijgen van de auditresultaten. De eigenlijke opdrachtgever is anders snel genoeg duidelijk dat de auditor zich voor het karretje van de projectmanager heeft laten spannen. Overigens zal er inderdaad in rapporten ruimte moeten zijn voor managementreacties. Beter dat die bij de bevindingen staan – ook al is het ‘agree to disagree’ – dan dat achteraf allerlei ‘ja-maar’s de ronde doen.

Te laat?

Als er een punt is dat tot problemen kan leiden, dan is het wel dat een projectreview nogal eens pas wordt uitgevoerd als het project is vastgelopen – of op z’n vroegst als de stuurgroep zenuwachtig is geworden door geruchten of gebrek aan goede informatie van de projectmanager. Het invoeren van een auditor (van buiten) is dan een negatief signaal op zich. Zelfs in zo’n geval is een review tóch op z’n plaats. Soms blijkt er niet eens bijzonder veel mis te zijn, en is het meer het algemene gevoel van onzekerheid over de toekomst dat opspeelde. De frisse blik kan ook helpen aan te wijzen wat er anders moet om het project alsnog met enig, of veel, succes af te ronden. En een review kan een extra zet zijn om anderen dan alleen de kerngroep van het projectteam, in actie te zetten om met het project mee te denken. Communicatiestoornissen (denk aan verwachtingsmanagement) ontstaan juist als er een te sterke wij-zij-cultuur ontstaat tussen projectteam en de ‘stakeholders’, waarvan gebruikers en gebruikersmanagement nogal eens in een andere denkwereld leven dan de ontwikkelaars. De auditor kan dan, maar dan moet hij wel z’n best doen, een brug slaan tussen die partijen.

Toch is het vaak veel handiger om een auditor al eerder bij projecten te betrekken. De auditor kan – om de onafhankelijkheid te bewaren – geen vervanging zijn van de quality-assurancefunctie die namens de projectmanager de kwaliteit van deliverables in de gaten houdt. Maar hij kan wel al gaandeweg de ontwikkelingen van een project, aanwijzen wat er buiten de band van de normen gaat lopen, waar procedures nog niet voldoende zijn, wat er aan informatiebeveiliging anders moet, etc. Dan komen er niet pas aan het eind van een project allerlei vervelende konijnen uit de hoge hoed en tijdens het project bijsturen is meestal veel minder duur dan achteraf de noodzakelijke verbeteringen doorvoeren. De gebreken moeten toch wel worden opgelost – de auditor signaleert ze niet voor niets.

Audits zijn dus niet (noodzakelijkerwijs) hinderlijk, noch overbodig of nutteloos, maar horen er gewoon bij. Al met al is er niks mis mee om een auditor over de vloer te hebben. Als boodschap voor R. Stouthart ten slotte: Roeland, kom bij ons werken dan leg ik het nog wel een keer uit.

Jurgen van der Vlugt

Ir.dr.s. J. van der Vlugt RE CISA (JurgenHimself@vdlugt.com) is IT audit manager bij Group Audit van ABN AMRO Bank. Dit artikel is geschreven op persoonlijke titel.