AUDIT
MAGAZINE

ARTIKELEN | 4 APRIL 2016

AUDITEN IN DE CLOUD

Auteur: Xander Bordeaux - Anouschka Carlier-Algoe - Suzanne Scheuller
Beeld: iStock - Adobe Stock
Leestijd: 7 min

Werken in de cloud is een trend die de afgelopen jaren sterk is toegenomen. Niet alleen privéapplicaties maar ook steeds meer bedrijfsapplicaties 'draaien' in de cloud. Hoe kan de auditor dit auditen? Een praktijkvoorbeeld bij ABN Amro.

De afgelopen jaren is veel gepubliceerd over de cloud en wordt steeds meer gebruikgemaakt van applicaties die in de cloud draaien. Denk aan e-mailtoepassingen waarbij een mailbox niet meer op de lokale IT-infrastructuur staat, maar in de publieke cloud. Niet alleen organisaties gebruiken steeds meer cloudapplicaties. Medewerkers doen dat zelf ook, denk aan community-cloudtoepassingen als Prezi en Trello.

Een andere trend is het migreren van bedrijfskritische applicaties naar een private cloud met als voordelen schaalbaarheid, selfservice en kostentransparantie. Zij hebben daarbij minder te maken met nadelen van een publieke cloud zoals het delen van de infrastructuur en beveiligingsaspecten.

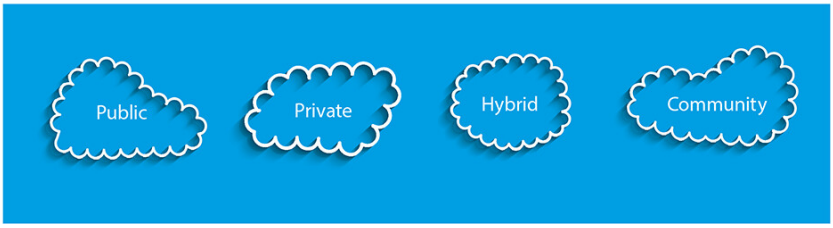
Cloudmodellen

NIST[1], het gezaghebbende Amerikaanse overheidsinstituut, onderscheidt vier cloudmodellen (zie *figuur 1*):

- Public cloud (applicaties en data in een publieke cloud-infra-structuur van een cloud provider gedeeld met anderen).
- Private cloud (applicaties en data in een private cloud-infrastructuur niet gedeeld met anderen).
- Hybride cloud (een combinatie van de hiervoor genoemde cloudtypen);

- Community cloud (applicaties en data worden door een selecte groep gebruikers gedeeld).

Op basis van het gekozen cloudmodel kan de internal auditor de meest geschikte auditscope kiezen en de bijbehorende controls bepalen. In de praktijk kiest de auditor vaak voor security en privacy controls vanwege de vertrouwdheid met het onderwerp, het beschikbaar zijn van normenkaders en expertise.



Figuur 1. De vier cloudmodellen

Scope van de cloud audit

ABN Amro heeft ervoor gekozen om een deel van de infrastructuur te migreren naar een private cloudomgeving. Dit betekent dat de locatie van de gegevens bekend is, namelijk in het eigen datacenter, en dat de cloudinfrastructuur niet wordt gedeeld met andere organisaties. Hiervoor is een private cloudproject gestart.

Als internal auditteam hebben we ervoor gekozen om de scope te richten op het cloudproject en het ontwerp van het businessmodel van de cloud. Dat betekent overigens niet dat beveiligingsaspecten van de cloudoplossing buiten de scope zijn gehouden, maar dat wij hiervoor steunen op de controls van de information securityafdelingen. De onderzoeksvraag is in hoeverre het private-cloudproject en de eerste ontwerpen van de private cloud voldoen aan de strategische doelstellingen van ABN Amro.

Soorten controls

Voor ons normenkader hebben wij gebruikgemaakt van twee soorten controls, namelijk project en solution design controls. De project controls – veelal gericht op integriteit en continuïteit – zijn reguliere project controls (gebaseerd op Prince2) zoals eigenaarschap, scope, doelstellingen, businesscase en risicomanagement. Aangezien het cloudproject onderdeel uitmaakt van een strategisch programma met verantwoordelijkheden bij andere projecten, hebben wij sommige controls buiten de scope van het project moeten testen.

Naast de project controls vormden de solution design controls, die meer zijn gericht op ‘effectiviteit’, het grootste deel van ons werkprogramma. Als je een ‘huis bouwt’ dan zijn niet alleen de project controls voor het bouwen in scope, maar ook de architectuurtekeningen met de ‘end state’ en mogelijk ook het bestemmingsplan, de plannen van de projectontwikkelaar en de werkzaamheden van onderaannemers. Een solution design control zou dan kunnen zijn of er voldoende kamers zijn ingetekend. Een meer securitygeoriënteerde solution design control zou de ligging van de nooduitgangen kunnen zijn.

De auditor kiest vaak voor security en privacy controls vanwege de vertrouwdheid met het onderwerp

Ontwerp normenkader

In tegenstelling tot het bouwen van een huis bestaan voor het bouwen van een cloudomgeving geen standaard voorschriften of normenkaders die voorschrijven aan welke eisen een cloudomgeving in de ‘end state’ moet voldoen. Ons normenkader hebben we daarom zelf ontworpen op basis van twee bronnen: Gartner-onderzoeken en het

Readiness Assessment van VMware (een belangrijke cloud leverancier).[2,3] Ons normenkader bestond uit drie onderdelen:

1. IT business & consumer controls;
2. system controls;
3. operational controls.

1. ***IT business & consumer controls***
   Deze controls komen met name uit de Gartner-artikelen. Gartner waarschuwt dat 'with no clear strategy in place for private cloud, it will be just another IT technology being used'. Private cloud in de visie van Gartner is veel meer dan het neerzetten van een technische omgeving. Het is een nieuw paradigma dat belangrijke voordelen als efficiency en agility brengt. Een belangrijke control is de 'selfservice' mogelijkheid. Gebruikers van de cloud moeten in staat zijn om op basis van een service catalogus zelf infraservices te bestellen net zoals bij public cloudaanbieders als Amazon. De overige controls gaan over financial transparency en reporting. Onderdeel van het cloudparadigma is dat kosten op voorhand bekend zijn en dat gebruikers zijn geïnformeerd over hun verbruik zodat zij in staat zijn om, als het nodig is, bij te sturen.

2. ***De system controls***
   Bestaan uit controls voor de service catalogus en service level management. De service catalogus wordt getoetst op een aantal kenmerken zoals kwaliteitsaspecten en kosten van de aangeboden services. Deze kenmerken moeten al in de service catalogus bekend zijn. Daarnaast is ook het proces om services toe te voegen of te verwijderen beoordeeld. De catalogus moet up-to-date zijn. Het service level management verschilt in principe niet van andere IT-processen, maar heeft als belangrijkste verschil dat de service levels real time beschikbaar zijn voor stakeholders.

3. ***De operational controls***
   Dit zijn in principe de reguliere ITIL controls zoals change- en release management, incident- en problemmanagement, capacity en continuity management.[4] Bij deze controls is zoveel mogelijk gekeken naar cloudspecifieke aspecten. Een voorbeeld is capacity management. Een private cloud stelt gebruikers in staat eenvoudige infraservices bij te bestellen. Dit zijn virtuele machines. Maar de virtuele machines draaien op fysieke hardware. Mocht het aantal virtuele machines tegen de grenzen van de fysieke capaciteit aanlopen, dan moet de IT-organisatie ingrijpen. Het bestellen van fysieke capaciteit is echter niet zo snel en eenvoudig als het virtueel bijbestellen. Sterker nog, dit kan weken tot maanden in beslag nemen. Het zorgvuldig analyseren van de vraag en het doen van voorspellingen is dus een onderscheidend aspect voor de cloud binnen capacitymanagement.

Teamsamenstelling audit

Het is lastig om het ontwerp van een huis te beoordelen als je nooit een huis hebt gebouwd. Het is daarom handig een expert in je auditteam te hebben. Wij hebben ervoor gekozen om een solution architect toe te voegen met ervaring in het ontwerpen van een cloudoplossing in een vergelijkbare organisatie.

Dynamische auditaanpak

Het cloudproject loopt meerdere jaren. Door voortschrijdend inzicht en veranderende omstandigheden is het nodig de projectaanpak bij te stellen: 'het einddoel is eenduidig, maar de weg ernaartoe kan veranderen'. Dit betekent dat de auditor op de hoogte moet blijven van de dynamiek binnen het project. Daarom hebben wij als auditteam ervoor gekozen om het cloudproject vanaf de zijlijn te volgen met twee 'deep-divemomenten'. In de deep dive zijn wij ingegaan op voortgang en kwaliteit van het project. Deze deep-dive-momenten vielen samen met belangrijke levermomenten van het project.

Veldwerk

Tijdens onze audit hebben wij specifiek gekeken naar de bijdrage aan de strategisch ambities en naar de afhankelijkheden met andere projecten. Een goed voorbeeld is de business-case: het cloudproject vereist een grote investering en heeft op korte termijn een negatieve bijdrage. Echter, als onderdeel van het programma zal het cloudproject op termijn wel voordelen (benefits) laten zien. Zo is parallel een project uitgevoerd om een deel van het applicatielandschap te migreren naar de private cloud. Dit maakt het mogelijk om verouderde infrastructuuronderdelen op te ruimen en te standaardiseren. Een gestandaardiseerd landschap is goedkoper, kent minder incidenten en kan sneller inspelen op veranderingen.

De solution design controls zijn getoetst op de drie controlonderdelen zoals beschreven in het normenkader. Voor sommige controls kwam de audit te vroeg, bijvoorbeeld bij IT business & consumer control. Gartner adviseert om te starten met een private control en om binnen enkele jaren over te stappen naar een hybride variant waarbij de IT-afdeling zowel private als public-clouddiensten aanbiedt. Deze hybride vorm stond bij ABN Amro nog niet in de planning. Deze controls hebben wij in principe laten staan in het normenkader om wellicht in de toekomst wel te testen. De meeste controls, zoals de operational control over capacitymanagement, bleken goed te testen omdat de ontwerpen in detail waren uitgewerkt.

Projectmanagement is geneigd issues en risico's lager in te schatten en komt

vaak met argumenten waarom een issue buiten de scope van het project valt of niet relevant is

Rapportage

Na het veldwerk en de deep-divemomenten hebben wij auditrapporten uitgebracht. Het is meestal lastig om als auditor issues te rapporteren tijdens een project. Projectmanagement is geneigd issues en risico's lager in te schatten en komt vaak met argumenten waarom een issue buiten de scope van het project valt of niet relevant is. Echter, als issues te maken hebben met toekomstige oplossingen dan is het nog complexer om te rapporteren. Het operationele risico bestaat immers nog niet. Als we het huis weer als metafoor gebruiken: het ontbreken van nooduitgangen in de ontwerpen betekent nog niet een verhoogd risico op brandgevaar. We hebben daarom in overleg met de auditee gekozen voor een rapport met overwegingen en observaties (dus niet issues), zodat de projectmanager tijdens het project kan bijsturen. Deze rapportagevorm leverde meer toegevoegde waarde dan een traditioneel auditrapport. Let op: de observaties en overwegingen worden natuurlijk wel door audit gemonitord om te kijken naar de follow-up.

Conclusies

Samengevat is dit een zeer interessant en leerzame audit geweest waarover we onze ervaringen graag delen. Interessant omdat het thema actueel is en de geschiedenis hierover vandaag wordt geschreven. Veel good practices zijn nog niet beschikbaar. Leerzaam omdat we ons gericht hebben op de project controls in brede zin als onderdeel van een strategisch programma en de afhankelijkheden met andere IT-projecten. Dit vergde flexibiliteit in onze auditaanpak en rapportagevorm. Maar ook leerzaam omdat we samen met een expert veel aandacht hebben besteed aan het auditen van solution design controls van de cloudoplossing. Op deze manier hebben we als team kennis over de private cloud opgedaan, een goede relatie met onze auditee opgebouwd en waarde kunnen toevoegen voor de organisatie.

Noten

1. National Institute of Standards and Technology (www.nist.gov).
2. Gartner: *The ten fundamentals of building a Private Cloud*, 19 May 2011, *When building a Private Cloud, Start Small, Think Big*, 25 november 2013 and *Six reasons Private Clouds fail, and how to Succeed*, 25 oktober 2014.
3. CloudWarriors Private Cloud Readiness Assessment, based on *VMware Operational Readiness for Cloud Computing Service Delivery Reference Guide*, 12, maart 2013.
4. Information Technology Infrastructure Library, wordt gebruikt als een referentiekader voor het inrichten van de beheerprocessen binnen een IT-organisatie.

Over

Anouschka Carlier-Algoe is consultant bij het Center of Expertise Service Orientation bij ABN Amro. Hiervoor werkte zij jarenlang als IT-auditor en adviseur in de publieke en private sector.

Xander Bordeaux is senior auditor bij ABN Amro. Hij heeft jarenlange ervaring als technisch IT-auditor op het gebied van informatiebeveiliging en cybersecurity binnen de publieke en de private sector.

Suzanne Scheuller is auditor bij ABN Amro. Als IT-auditor heeft zij brede ervaring opgedaan binnen het cloudproject. Hiervoor heeft zij succesvol het management traineeship van de bank afgerond.

De auteurs waren gedurende de audit allen internal auditor bij ABN Amro Group Audit.

Tags: Auditmethodiek

Bron url: https://auditmagazine.nl/artikelen/auditen-in-de-cloud/