

DE QUICK WINS VAN EEN RISK BASED AUDIT

Risk based auditing kan het beslag dat een audit op een organisatie legt verminderen. Met behoud van kwaliteit kost de audit medewerkers en auditors minder tijd en levert daardoor een besparing op in geld. Dit artikel bespreekt de ervaringen van de auteurs met het toepassen van risk based auditing bij de overheidorganisatie Logius waar beheersing van klantrisico's centraal staat.

door: Klaske van Walderveen en Johan van den Bosch

Logius is de dienst digitale overheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De dienst beheert overheidsbrede ict-oplossingen en gemeenschappelijke standaarden die de communicatie tussen overheden, burgers en bedrijven moeten vereenvoudigen. Met oog voor de samenhang in de infrastructuur van de e-overheid. Logius levert producten op het gebied van toegang, gegevensuitwisseling, standaardisatie en informatiebeveiliging. Logius wil haar klanten van de producten DigiD voor Burgers, Digipoort (voorheen de Overheidstransactiepoort) en PKloverheid laten weten dat het gebruik van deze producten veilig is. Zij doet dit door het meeleveren van een Third Party Mededeling (TPM) bij haar jaarlijkse verantwoording. Door middel van de TPM-verklaring krijgt de klant van een product een bevestiging dat risico's die hij zelf niet onder controle heeft, door Logius worden beheerst. De TPM-audit is eind 2007 voor het eerst uitgevoerd. Dit gebeurde volgens de traditionele manier van auditing. Deze manier gebruikt een uitgebreid normenkader en heeft een heel brede scope ongeacht de hoogte van het risico; doel is het bieden

van maximale zekerheid. Om die reden worden uitgebreide checklists doorgenomen zonder het belang en het risico in te schatten. Een dergelijke werkwijze legt een hoog capaciteitsbeslag op medewerkers van Logius, bij (outsourcing)leveranciers en bij de auditors. Toen Logius een nieuwe TPM-cyclus wilde doorlopen, werd gekozen voor een risk based aanpak (figuur 1). Men verwachtte dat de traditionele aanpak nog meer capaciteit aan menskracht zou vergen dan bij de eerste keer, mede omdat het productenpakket sindsdien fors is uitgebreid.

Hoe is risk based auditing toegepast?

In de traditionele audit zijn vrijwel alle beheerprocessen en techniekdelen aan een onderzoek onderworpen. Ongeacht de mate van belangrijkheid van het product. Bij de risk based audit zijn alleen die procesonderdelen en technologie beoordeeld die een directe relatie hebben met de risico's van klanten. Hiermee wordt geaccepteerd dat er geen zekerheid bestaat over de niet onderzochte beheerprocesdelen of technologie. Door op twee manieren te kijken naar een product wordt bepaald welke beheerprocessen en technologie onderzocht moeten worden in de TPM:

- Wat is het belang van het product voor klanten en gebruikers;
- Wat is het belang van specifieke onderdelen van het product (infrastructuur, applicatie, helpdesk, et cetera) voor het functioneren van het product als geheel.

Uit het belang worden vervolgens de risico's afgeleid die het uitvallen of compromitteren van het product heeft voor de klanten. In essentie betekent risk based auditing voor Logius dat in de TPM-audit vooral die onderdelen geaudit worden die een directe relatie hebben met de

risico's van klanten en die risico's die gebruikers juist willen voorkomen.

Bepalen van risico's en keuze van de normen

Per itil-beheerproces zijn de risico's geanalyseerd en vastgelegd in het risicoprofiel van het product. Dit is in feite de argumentatie van Logius om bepaalde delen van beheerprocessen en technologie wel of niet te laten onderzoeken. Het risicoprofiel van het product is de basis van de risk based audit. De risico's zijn geanalyseerd per risicocategorie. Het gaat daarbij om de volgende risicocategorieën:

- beschikbaarheid (bijvoorbeeld uitval of een tekort aan capaciteit);
- vertrouwelijkheid (bijvoorbeeld privacyschending of misbruik);
- integriteit (risico's voor de juistheid van de gegevens bij de verwerking en de opslag, bijvoorbeeld moedwillige verandering).

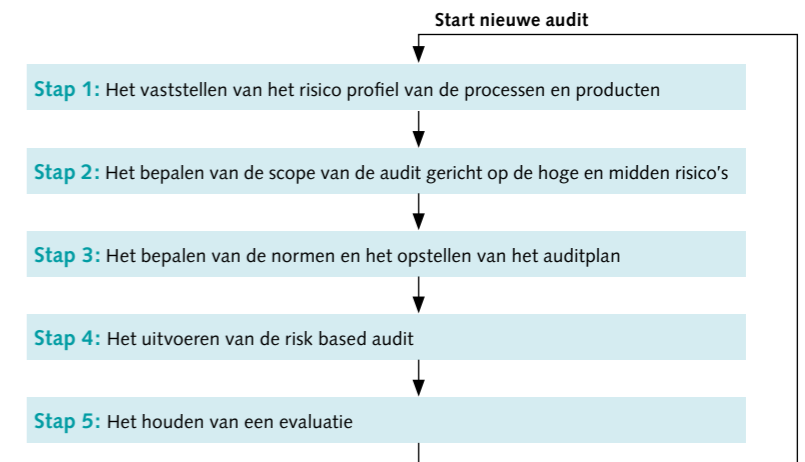
Het vaststellen van een risicoprofiel van het product is een verantwoordelijkheid van Logius. Essentieel is dat de proceseigenaar of producteigenaar betrokken is bij het vaststellen van een risicoprofiel. Alleen de eigenaar kan een juiste afweging maken. Ideaal - maar niet altijd mogelijk - is als de klanten van het product worden betrokken bij de opstelling en vaststelling van het bedoelde risicoprofiel. Het gaat immers om het beheersen van de risico's voor hun beheerprocessen. Zoals eerder aangegeven zijn de risico's gedefinieerd op basis van de gevolgen die het uitvallen of compromitteren van het product heeft voor de klanten. Bijvoorbeeld voor het product DigiD voor Burgers is een risico dat iemand misbruik maakt van een DigiD. De TPM-audit richt zich dus op het controleren of risico's zijn afgedekt. De risico's worden afgedekt door de manier waarop Logius in voldoende mate de beheerprocessen heeft ingericht, door het nemen van de juiste maatregelen en door de inhoud van de opdracht die aan (outsourcing) leveranciers is verstrekt om het product in te richten en te onderhouden.

Beschikbaarheid DigiD voor Burgers

Een voorbeeld van een hoog risicoproces voor een klant is het uitvallen van DigiD voor Burgers met consequenties voor de beschikbaarheid van het bedrijfsproces van de klant. Dit is een risico dat als 'hoog' beoordeeld is. In dit geval van de risicogebaseerde audit is er vooral gekeken of:

- de mate van redundantie in de infrastructuur (onder meer dubbel uitvoeren, uitwijk) voldoende is (technologie en architectuur);
- het crisis- en calamiteitenmanagement (proces incidentmanagement) goed werkt;
- wijzigingen in de infrastructuur op een gecontroleerde manier worden aangebracht (proces wijzigingenbeheer) waardoor de kans klein is dat er storingen ontstaan;
- er voldoende op wordt gelet of de capaciteit van het product in relatie tot de groei van het gebruik overeenkomt (proces behoeftemanagement).

Het gebruikte normenkader bij de audit wordt met de risk based manier van auditeren kleiner. De tijd die de auditors aan een onderzoek besteden, neemt af en de tijd



Figuur. 1: Stappenplan risk based audit

die de leverancier er in moet steken om met de auditors te spreken, wordt dus ook beperkt. Daarnaast hoeft door de leverancier minder bewijsmateriaal te worden verzameld dan wanneer alle normen worden onderzocht, terwijl de gewenste zekerheid over de kwaliteit van de dienstverlening hetzelfde is.

Het auditplan

De keuze van de normen die worden getoetst, is aan Logius. Aangezien de auditors die het TPM onderzoek uitvoeren, de beroepsplicht hebben om in te staan voor de kwaliteit van hun beoordeling, is er overeenstemming nodig met auditors over de 'juiste' normen die in het TPM-onderzoek gehanteerd gaan worden. De auditors verwerken de normen daarna in het auditplan voor het TPM-onderzoek.

De auditors hanteren de volgende criteria om de keuze van Logius te beoordelen:

- de kwaliteit van het risicoprofiel van het product;
- de kwaliteit van de afstemming van het risicoprofiel met de klanten en eigenaar van het product;
- professionele beoordeling van de betrokken auditors.

Conclusie

De auteurs hebben geconstateerd dat bij leveranciers waar een concentratie van risico's aanwezig is, de tijdsbesteding hetzelfde is als bij de traditionele manier van auditing. Maar bij leveranciers waar weinig risico's aanwezig zijn, is de tijdswinst groot, zowel bij de leveranciers, de auditors als bij de begeleiders van Logius. Dit kan oplopen tot wel vijftig procent minder uren. Deze tijdswinst levert weer een besparing op van kosten. De auteurs hebben de volgende leerervaringen bij het toepassen met risk based auditing bij Logius:

- Grote tijdswinst bij leveranciers met weinig risico's;
- Effectievere manier van auditeren;
- Risico's worden beter beheerst;
- Minder beslag op de tijd van de medewerkers van Logius. ■



Over de auteurs:
Drs Klaske van Walderveen RRM en drs Johan van den Bosch MCM zijn respectievelijk adviseur en senior adviseur bij Verdonck Klooster & Associates (VKA).