ORACLE EBS

Kun je de gegevens op het scherm wel vertrouwen?

8 september 2017

Accountant X gaat fluitend door het leven. Voor het uitvoeren van de laatste deelwaarneming logt hij nog één keer in op Oracle EBS om de goedkeuringshistorie te raadplagen. Hier maakt hij zich geen zorgen over, want de autorisatiematrix is strak ingevoerd. Op dat moment stapt de IT-auditor binnen met een verontrustende mededeling: 'Het is niet mogelijk de functiescheiding in het systeem te controleren. Wat je op het beeldscherm ziet kun je niet vertrouwen!'. Wat is er gebeurd?

In dit artikel maken we duidelijk dat de hierboven beschreven situatie maar al te reëel is als je te maken hebt met een groot ERP-pakket. Met enkele voorbeelden illustreren we dat dergelijke situaties zich in de praktijk kunnen voordoen en voor onaangename verrassingen kunnen zorgen. Bewustwording is de grootste stap richting een oplossing. Tevens beschrijven we hoe auditors én organisaties kunnen omgaan met situaties waarin niet zeker is of gepresenteerde data op het scherm overeenkomt met de werkelijkheid.

Achtergrond

ERP-systemen zijn niet meer weg te denken uit (grote) organisaties. Dergelijke systemen worden gebruikt voor de ondersteuning van (bijna) alle bedrijfsprocessen. Het zijn meestal grote en complexe pakketten met ingewikkelde structuren en duizenden functies, menu's en opties. Zo'n pakket kan op verschillende manieren worden geïmplementeerd. Dit, en eventueel maatwerkaanpassingen, zorgen ervoor dat de inrichting per organisatie flink kan verschillen. SAP en Oracle zijn momenteel de grootste aanbieders. Dit artikel richt zich op Oracle EBS.

De implementatie van een ERP-pakket is geen sinecure en vraagt veelal flinke investeringen, zowel in euro's als in uren. Ook na de implementatie kost de beveiliging van een ERP-pakket veel energie. Organisaties (maar ook auditors) leveren inspanningen om beheersing te realiseren en aan te tonen dat zij in control zijn op het gebied van de inrichting en toekenning van autorisaties. Ook de *application controls* in het ERP-pakket zelf zijn een aandachtsgebied van organisaties en auditors. Daarnaast wordt in toenemende mate onderzoek gedaan naar transacties. In dit artikel beschrijven wij een situatie die

zich kan voordoen in Oracle EBS waardoor alle hier genoemde inspanningen zo goed als ongedaan worden gemaakt.

De inrichting van de autorisatiematrix bepaalt welke handelingen gebruikers kunnen uitvoeren. Standaard maakt Oracle EBS het echter mogelijk dat gebruikers, al dan niet bewust, de ingestelde autorisatiematrix te niet doen. Hierdoor ontstaan 'olifantenpaadjes'. Dit zijn paden waardoor transacties in EBS een ander pad bewandelen dan vooraf beoogd en tijdens de inrichting gerealiseerd. In dit artikel nemen we het inkoopproces als voorbeeld, maar de bevindingen kunnen zich bij elk proces voordoen. Wij beschrijven de olifantenpaadjes die ontstaan door het delen van mandaat en hiaten in de mandaatinrichting in combinatie met een niet volledig betrouwbare logging. We geven ook aan hoe organisaties én accountants kunnen handelen.

Olifantenpaadjes Oracle door het delen van mandaat

Een medewerker kan handelingen in EBS uitvoeren door (in grote lijnen) een combinatie van toegekende rechten en instellingen en opties. Door dit goed in te regelen willen organisaties afdwingen dat een transactie via het voorgeschreven proces wordt afgehandeld door een daarvoor aangewezen medewerker. In EBS kan een gebruiker ervoor kiezen handelingen te laten uitvoeren door een andere (willekeurige) gebruiker. Dit kan door middel van de reguliere functionaliteiten overdraging en werklijsttoegang.

Overdraging

Overdraging houdt in dat de door het proces voorgeschreven goedkeurder de goedkeuringsbeslissing laat nemen door een andere medewerker. Deze overdraging kan eenmalig zijn of voor een bepaalde periode (bijvoorbeeld vakantie). Bij overdraging laat EBS op het beeldscherm (=de view van de database) de naam zien van de medewerker die een transactie (na overdraging) feitelijk heeft goedgekeurd.

Werklijsttoegang

Een andere mogelijkheid is dat de door het proces voorgeschreven goedkeurder een andere medewerker toegang geeft tot zijn werkvoorraad met goedkeuringsbeslissingen. Hiervoor verschaft hij werklijsttoegang aan deze medewerker. Wanneer een aanvraag ter goedkeuring in het postvak van de voorgeschreven goedkeurder verschijnt, kan de aanvraag zowel worden afgehandeld door de voorgeschreven goedkeurder zelf als ook door de medewerker aan wie werklijsttoegang is verschaft. Bij werklijsttoegang laat EBS op het scherm altijd de naam van de volgens het voorgeschreven proces beoogde goedkeurder zien, óók wanneer de transactie niet door de beoogde goedkeurder zelf, maar door overdraging of via werklijsttoegang is goedgekeurd door een andere medewerker. Dit verschilt dus van overdraging, waarbij altijd de feitelijke goedkeurder wordt getoond.

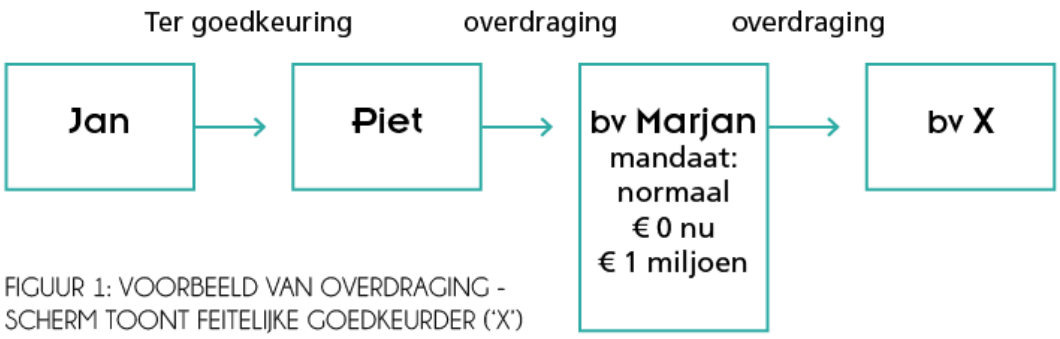
In de kaders 1, 2 en 3 lichten we deze functionaliteiten apart en gecombineerd toegepast toe aan de hand van de goedkeuring van een bestelaanvraag.

Gewenste situatie

Jan maakt een bestelaanvraag aan voor tien pc's. Via de workflow komt deze aanvraag ter goedkeuring terecht in de werklijst (te vergelijken met een postvak) van Piet. Piet is mandaathouder en heeft bij de inrichting van EBS goedkeuringsrechten toegewezen gekregen. Piet pakt de aanvraag op en keurt hem goed.

Risico bij overdraging

De bestelaanvraag is in het postvak van Piet binnengekomen. Piet kan gebruikmaken van de functionaliteit van overdraging en hiermee de goedkeuring overdragen aan iedere andere gebruiker in EBS. De gebruiker aan wie de goedkeuring is overgedragen erft voor deze beslissing de rechten van Piet en kan hierdoor de aanvraag afhandelen. EBS stelt hier standaard geen beperkingen aan. Piet kan de beslissing overdragen, bijvoorbeeld aan Marjan. Dit kan Piet incidenteel doen voor één aanvraag, maar ook voor langere tijd bijvoorbeeld bij afwezigheid door vakantie. Op het beeldscherm toont EBS de overdraging en de naam van de medewerker die de bestelaanvraag daadwerkelijk heeft goedgekeurd. In dit voorbeeld is dit dus Marjan. Marjan kan op haar beurt de beslissing weer doormandateren aan elke andere medewerker. Hoewel EBS de naam toont van de daadwerkelijke goedkeurder – dus Marjan of aan wie zij de goedkeuring heeft doorgemandateerd – loopt de organisatie wel het risico dat ze geen controle meer heeft op wie wat goedkeurt en met welk mandaat. Immers, de medewerkers kunnen de beoogde mandaatregeling met iedere doormandatering doorbreken zonder dat dit vooraf bekend is. Er hangt dus veel af van het gedrag van de medewerkers. Het is hierbij de vraag in hoeverre medewerkers zich bewust zijn van de consequenties van overdraging én in welke mate dit bewustzijn het handelen beïnvloedt.

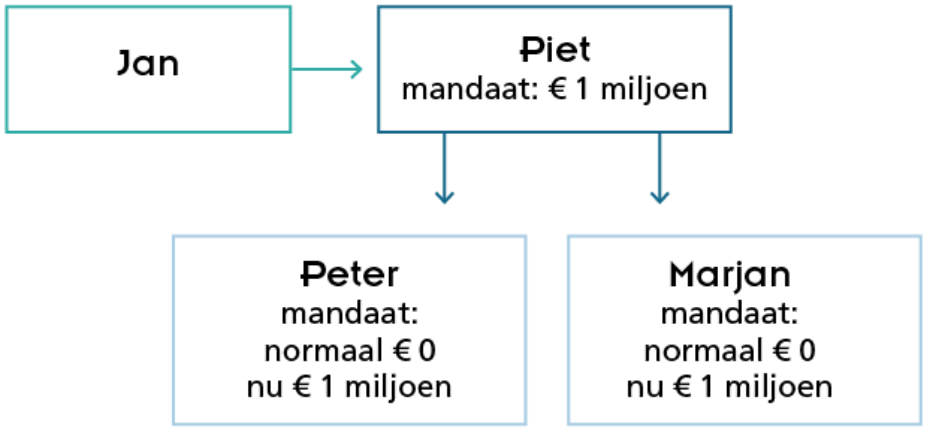


FIGUUR 1: VOORBEELD VAN OVERDRAGING - SCHERM TOONT FEITELIJKE GOEDKEURDER ('X')

Door organisatie beoogde goedkeurder bestelaanvraag 1: Piet
Goedkeurder volgens scherm bestelaanvraag 1: Marjan
Werkelijke goedkeurder bestelaanvraag 1: Marjan

Risico bij werklijsttoegang

Bij werklijsttoegang stelt Piet zijn werklijst open voor bijvoorbeeld Marjan en Peter, die hierdoor aanvragen in het postvak van Piet kunnen openen en afhandelen. Dit kan handig zijn als Piet niet in de gelegenheid is om de aanvragen zelf af te handelen. Op het scherm staat als goedkeurder de naam van Piet. Dat de goedkeuring door bijvoorbeeld Marjan heeft plaatsgevonden wordt in EBS standaard gelogd. Maar omdat het loggen van deze gegevens ten koste kan gaan van de performance, adviseert Oracle op haar supportsite om de logging van data die inmiddels verouderd is, periodiek te vernietigen (bron: http://support.oracle.com[1]). Hierdoor is achteraf niet meer inzichtelijk of medewerkers gebruik hebben gemaakt van werklijsttoegang. Ofwel, er kan niet met zekerheid worden vastgesteld of degene die daadwerkelijk heeft goedgekeurd ook de door de organisatie beoogde goedkeurder is.

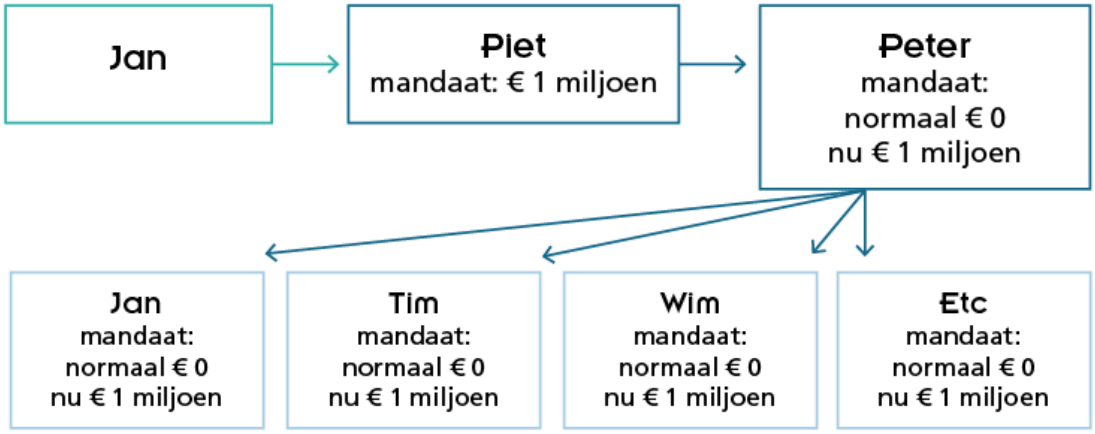


FIGUUR 2: VOORBEELD VAN WERKLIJSTTOEGANG

Door organisatie beoogde goedkeurder bestelaanvraag 2: Piet
Goedkeurder volgens scherm bestelaanvraag 2: Piet
Werkelijke goedkeurder bestelaanvraag 2: Marjan

Risico bij gecombineerde overdraging en werklijsttoegang

Overdraging kan ook in combinatie met werklijsttoegang voorkomen. Hierbij worden de risico's uit de voorbeelden in figuur 1 en figuur 2 gecombineerd. Wanneer de organisatie geen zicht heeft op de medewerkers die werklijsttoegang hebben verschaft en waar combinaties met overdraging zich voordoen, neemt het inzicht en de beheersing in de



FIGUUR 3: VOORBEELD VAN GECOMBINEERDE OVERDRAGING EN WERKLIJSTTOEGANG

Door organisatie beoogde goedkeurder bestelaanvraag 3: Piet
Goedkeurder volgens scherm bestelaanvraag 3: Peter
Werkelijke goedkeurder bestelaanvraag 3: Jan/Tim/Wim/et cetera

afhandeling van de bestelaanvraag nog verder af. Piet krijgt de bestelaanvraag in het voorbeeld in figuur 3 van Jan ter goedkeuring in zijn postvak. Piet draagt de goedkeuring over aan Peter. Peter heeft werklijsttoegang verschaft aan tien medewerkers. Eén van deze tien medewerkers handelt de bestelaanvraag af.

Medewerkers aan wie goedkeuring is overgedragen en die bovendien werklijsttoegang hebben, hebben later in het proces de mogelijkheid ook nog handelingen uit te voeren zoals het geven van de prestatieverklaring. Door onzekerheid over de feitelijke goedkeurder is het dan niet meer mogelijk om vast te stellen of er functiescheiding heeft plaatsgevonden tussen de goedkeuring van de bestelaanvraag en het geven van de prestatieverklaring. Zeker niet als voor het geven van de prestatieverklaring ook weer geldt dat dit kan door toegekende rechten via overdraging mandaat óf via werklijsttoegang.[2] Hierdoor ontstaat een ondoorzichtige situatie. Zo kan Piet de goedkeuring van de bestelaanvraag overdragen aan Peter, die werklijsttoegang heeft verschaft aan Klaas. Later in het proces handelt een daartoe geautoriseerde medewerker (bijvoorbeeld Irene) de prestatieverklaring af. Irene heeft echter werklijsttoegang verschaft aan zes medewerkers, waaronder Klaas. Hiermee ontstaat het risico dat één persoon, in dit voorbeeld Klaas, alle goedkeuringshandelingen in het inkoopproces zelf uitvoert. Van een goede werking waarbij onwenselijkheden preventief via application controles worden voorkomen, is dan zeker geen sprake. In het meest gunstige geval is er goede logging waarmee de werkelijke procesgang achteraf in kaart kan worden gebracht. Dit zal helaas niet altijd het geval zijn.

Wat moet de organisatie doen?

We hebben laten zien dat we niet zonder meer kunnen vertrouwen dat de namen die EBS op het scherm toont die van de daadwerkelijke goedkeurders zijn. Wat nu? In deze paragraaf bespreken we wat de organisatie moet doen en in de volgende paragraaf beschrijven we wat de IT-auditor te doen staat.

Beleid en spelregels

Allereerst zou de organisatie zich ervan bewust moeten zijn dat het automatiseren van een workflow nieuwe risico's met zich meebrengt. De organisatie moet zeker weten dat de view van de database die op het scherm te zien is, juist weergeeft wie de feitelijke goedkeuring heeft gegeven. De organisatie moet bij het opstellen van het autorisatiebeleid rekening houden met de mogelijkheden die het systeem biedt.[3] Als bepaalde onderdelen van dat beleid niet via het systeem zijn af te dwingen, moet de organisatie aanvullend spelregels opstellen waar de gebruikers van het systeem zich aan te houden hebben. In het geval van overdraging en/of werklijsttoegang moet de organisatie bepalen waar en wanneer het gebruik van werklijsttoegang en/of werklijsttoegang toegestaan is én waar en wanneer niet. Bijvoorbeeld door overdraging alleen toe te staan aan hiërarchisch gelijke of hogere gemandateerden. Het is noodzakelijk dat de organisatie het beleid en de spelregels actief aan de gebruikers overbrengt. Daarbij kan het zeker geen kwaad om rondom vakantieperiodes hier extra aandacht voor te vragen. Dit helpt de mandaatstructuur van de organisatie in stand te houden en kan zo problemen voorkomen.

Monitoren en handhaven

Vervolgens moet de organisatie monitoren of beleid en spelregels in de praktijk ook in acht worden genomen. Deze monitoring vormt de basis om handhavende maatregelen te treffen. Uiteraard heeft de organisatie gegevens nodig om te kunnen monitoren. Hierbij kun je denken aan de gegevens over de ingestelde werklijsttoegang en het gebruik ervan. De huidige ingestelde werklijsttoegang is door middel van een query relatief eenvoudig te achterhalen. Om ervoor te zorgen dat de in het verleden ingestelde maar inmiddels verwijderde werklijsttoegang inzichtelijk blijft, is het noodzakelijk dat de desbetreffende tabel wordt gelogd en wordt bewaard op een veilige plaats. Dit, zodat deze informatie integer blijft. Het achterhalen van het werkelijke gebruik, dus het feitelijk goedkeuren van bijvoorbeeld een bestelaanvraag, via werklijsttoegang kost iets meer inspanning. Zoals eerder vermeld, adviseert Oracle op haar supportsite om vanwege performance-redenen logging periodiek te vernietigen. Het is echter een relatief kleine ingreep om de logging van het gebruik van werklijsttoegang veilig te stellen en te analyseren.

Wat kan de auditor doen?

De auditor moet de organisatie bevragen of zij 'in control is over eigen informatie'. De auditor moet hierbij onderzoeken of er wellicht ongewenste handelingen en/of kritische doorbreking van functiescheiding heeft plaatsgevonden in het inkoopproces. Hiervoor is vooraf een soll-positie vastgesteld. Dit kan bijvoorbeeld in de vorm van een scenarioschets waarin de verschillende (on)gewenste combinaties van goedkeuringen, doormandatering en werklijsttoegang zijn beschreven. Hierbij is het van belang om ook de impact en de gevolgen van het voordoen van de scenario's op te nemen voor de controle. Dit ook in situaties waarin zaken achteraf niet meer kunnen worden vastgesteld door bijvoorbeeld het ontbreken van goede logging. Afhankelijk van de volwassenheid van de logging van de EBS-applicatie kan de auditor gebruikmaken van bovengenoemde door de organisatie getroffen beheersmaatregelen. Uiteraard moet de auditor vaststellen dat de organisatie heeft geborgd dat eventuele logging betrouwbaar/integer is. Is dit niet mogelijk, dan kan er wellicht niet gesteund worden op de logging en kan er niet (voldoende) zekerheid worden verkregen uit de analyses op basis van de logging.

Indien er logging van het gebruik van werklijsttoegang beschikbaar is, dan kan door middel van tooling worden vastgesteld of doorbreking van gewenste (soll-positie) functiescheiding heeft plaatsgevonden. Hierbij kan tooling zoals *process mining* gebruikt worden.

Als logging niet beschikbaar is, kan doorbreking van de functiescheiding alleen worden vastgesteld voor wat betreft het gebruik van overdragen van mandaat. De vraag of werklijsttoegang gezorgd heeft voor ongewenste doorbreking van functiescheiding blijft dan echter onbeantwoord. Om te bepalen of dit risico reëel is kan de auditor beoordelen welke medewerkers werklijsttoegang hebben verschaft en aan wie. Hij kan dan op basis van een goedgekeurde autorisatiematrix bepalen of hiertussen ongewenste combinaties zitten. Indien dat het geval is, kan vervolgens worden bepaald of de medewerkers die werklijsttoegang hebben gekregen andere kritische handelingen hebben verricht in het inkoopproces, zoals het aanmaken van een inkooporder of het geven van een prestatieverklaring. Op deze manier kan het effect van de ingestelde werklijsttoegang op de functiescheiding beter worden vastgesteld.

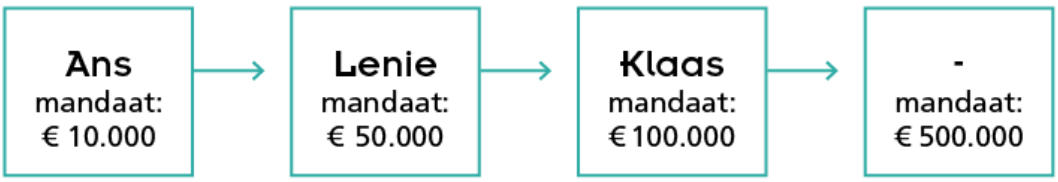
Afhankelijk van de mate van volwassenheid van de tweede of eerste *line of defence* van de organisatie voeren deze *lines* zelf de bovengenoemde controles uit. In dat geval beperkt de auditor zich tot een review van deze werkzaamheden. In het geval dat de organisatie nog niet zo ver is, liggen er meer werkzaamheden op het bordje van de auditor en zijn er kansen voor hem om de organisatie te helpen bij deze groei.

Olifantenpaadjes Oracle door hiaten in mandaatstructuur

Naast de problemen rond werklijsttoegang en overdraging is er nóg een risico dat voortvloeit uit de inrichting van EBS, te weten: goedkeuren boven mandaat, al dan niet zonder dat men zich hier bewust van is.

Een aanvraag kan (afhankelijk van de inrichting) in EBS ter goedkeuring een weg afleggen langs meerdere goedkeurders, met bijvoorbeeld een steeds oplopend mandaatbedrag. In dat geval gaat de goedkeuringsbeslissing langs meerdere gemandateerden totdat een medewerker met voldoende mandaat een beslissing heeft genomen. Dit kan in volgorde van het mandaat zijn. Een bestelaanvraag à € 100.000,- gaat eerst naar de laagst gemandateerde (Ans), daarna naar de daaropvolgende (Lenie), net zo lang tot die bestelaanvraag is goedgekeurd door de medewerker met een mandaat van € 100.000,- (Klaas). Omdat Klaas over afdoende mandaat beschikt, is met zijn goedkeuring het goedkeuringsproces afgerond.

Bij een bestelaanvraag van € 500.000,- worden wederom goedkeurders om hun akkoord gevraagd. In principe is na het akkoord van de medewerker met een mandaat van € 100.000,- (Klaas) ook nog het akkoord nodig van een medewerker met een mandaat van minimaal € 500.000,-. In dit voorbeeld is de positie van de goedkeurder met het mandaat van € 500.000,- tijdelijk niet ingevuld. Hierdoor kán de bestelaanvraag niet worden goedgekeurd door een medewerker met voldoende mandaat. Door het ontbreken van een medewerker met voldoende mandaat neemt EBS genoegen met de goedkeuring van de goedkeuring door de medewerker (Klaas) met het mandaat van € 100.000,-. Klaas heeft dus, mogelijk zonder dat hij het zelf weet, boven het mandaat goedgekeurd.



FIGUUR 4: VOORBEELD VAN GOEDKEURING BOVEN MANDAAT DOOR HIAAT IN DE MANDAATSTRUCTUUR

Door organisatie beoogde goedkeurder: - (niet gedefnieerd, positie is immers tijdelijk niet ingevuld)
Goedkeurder volgens scherm: Klaas
Werkelijke goedkeurder: Klaas

Wat kan de organisatie doen?

De organisatie moet zich allereerst bewust zijn van de werkwijze van EBS. Daarnaast zou zij idealiter ervoor moeten zorgen dat het proces zó wordt ingericht dat er altijd iemand aftekent met voldoende mandaat.

Wat kan de auditor doen?

De auditor kan op basis van de logging nagaan of iemand boven mandaat heeft afgetekend. Voor die posten die van kritisch belang zijn, kan de auditor de organisatie vragen deze alsnog door een juist gemandateerde te laten beoordelen.

Samenvatting

Het doeltreffend inrichten van complexe systemen zoals een ERP-pakket is een lastig karwei. Door mogelijkheden die Oracle EBS biedt en door het gedrag van mensen kunnen olifantenpaadjes ontstaan. Het gebruik van overdragingen en werklijsttoegang is een belangrijke oorzaak van deze olifantenpaadjes, maar er zijn ook nog andere oorzaken waardoor processen niet de gewenste flow doorlopen. We hebben deze niet allemaal in dit artikel kunnen behandelen. Organisaties in de eerste plaats, maar ook auditors, moeten zich hier bewust van zijn. Technieken zoals process mining[4] kunnen organisaties helpen achteraf inzicht te krijgen in eventuele ongewenste paden binnen de workflow. Hiermee kunnen organisaties bewuster worden van de problematiek, waardoor ze beter in staat zijn de preventieve maatregelen goed in te richten.

Tot slot: En hoe is het met accountant ‘X’afgelopen?

Accountant X heeft direct actie ondernomen nadat hij van de IT-auditor hoorde dat hij de informatie op zijn beeldscherm niet kon vertrouwen én dat de logging van werklijsttoegang niet bewaard werd. Hij heeft de IT-auditor gevraagd te onderzoeken wat er wel aan logging was en welke analyses wel uitgevoerd konden worden.

Terwijl de IT-auditor dit onderzocht, heeft de accountant genoemde verschillende scenario’s uitgewerkt waarmee impact en gevolgen van overdraging en werklijsttoegang worden geduid. Met deze scenario’s worden vragen beantwoord zoals: Wat als iemand zijn werklijst heeft opengesteld of overgedragen aan een lager/hoger gemandateerde? En wat als een van die mogelijke goedkeurders ook een goedkeuring heeft gegeven aan een andere kritische beslissing in het proces? Per scenario is aangegeven wat de gevolgen voor de jaarrekeningcontrole zijn. Hierbij kan het ene scenario bijvoorbeeld een beheerissue opleveren en het andere een financiële fout.

Hierna heeft de IT-auditor overzichten opgeleverd van medewerkers die gebruik hadden gemaakt van overdraging. Daarnaast heeft hij overzichten opgeleverd waaruit bleek welke medewerkers werklijsttoegang hadden verschaft én aan wie zij dit gedaan hadden. Met deze informatie kon worden vastgesteld of genoemde scenario's zich hadden voorgedaan en zijn de gevolgen voor de jaarrekeningcontrole bepaald. Bovendien is de accountant het gesprek aangegaan met de desbetreffende organisatie, wat bij de organisatie het bewustzijn van de beperkingen van het digitale systeem flink heeft getriggerd. Dit voorbeeld illustreert wat een IT-auditor concreet kan bijdragen, zowel aan de jaarrekeningcontrole als, in een adviesrol, aan de IT-beheersing van organisaties.

Noten

1 **Quick Reference: How To Purge Obsolete Workflow Runtime Data For Applications (Doc ID 264191.1):** 'Purging Oracle Workflow tables of obsolete workflow runtime information for completed workflow processes is a required regular maintenance task'.
ADetailed Approach To Purging Oracle Workflow Runtime Data (Doc ID 144806.1): 'One of the essential administrative tasks concerning Oracle Workflow is to purge of runtime data that is no longer required without affecting active Workflow processes'.
Purge Permanent (PERM) Workflow Item Type Runtime Data? (Doc ID 1520305.1): '(…) Workflow purge is REQUIRED to have good performance including permanent items (PERM) (…) Oracle Workflow and Oracle XML Gateway access several tables that can grow quite large with obsolete workflow information that is stored for all completed workflow processes, as well as obsolete information for XML transactions. The size of these tables and indexes can adversely affect performance. These tables should be purged on a regular basis (…)'.

2 Bijvoorbeeld doordat de prestatieverklaring via een workflow gaat of doordat via de workflow de noodzaak aan een prestatieverklaring kan worden overruled.

3 Je kunt EBS bijvoorbeeld zo inrichten dat het voor gebruikers onmogelijk is om de werklijst te delen of beslissingen over te dragen. Dit neemt echter de (legitieme behoefte) bij medewerkers niet weg. Mogelijk gaan medewerkers dan deze behoefte invullen door bijvoorbeeld gebruikersnamen en wachtwoorden uit te wisselen.

4 **Process Mining als gereedschap voor (it-)auditors,** *naar een softwarematige analyse van bedrijfsprocessen voor auditing*
Lessons Learned bij toepassing van process mining

J. van Bruchem RE RO en R.P. de Goede RE

Jaap is werkzaam als auditor bij de Auditdienst Rijk. Hij begon zijn carrière in 2006 bij de toenmalige Auditdienst van Economische Zaken. In respectievelijk 2009 en 2015 rondde hij de opleiding tot operational auditor en die van IT-auditor af. Beide aan de Erasmus Universiteit. Als RO RE is Jaap werkzaam in alle auditdisciplines maar hij houdt zich op dit moment vooral bezig met het inzetten van process mining in de Financial audit bij verschillende ministeries. Jaap schreef dit artikel op persoonlijke titel. Ronald is sinds 2008 werkzaam als auditor bij de Auditdienst Rijk en haar voorgangers. In 2012 rondde hij de opleiding tot IT-auditor af en in 2015 de opleiding tot operational auditor. Beide aan de Erasmus Universiteit. Vanuit deze achtergrond voert hij verschillende soorten audits uit, maar hij richt zich vooral op de toepassing van process mining en andere tooling ten behoeve van Financial Audit bij verschillende ministeries. Ronald schreef dit artikel op persoonlijke titel.