GEMEENTEBARENDRECHT | Gemeente Albrandswaard | GEMEENTE RIDDERKERK

Aan de raden van de gemeenten Barendrecht, Albrandswaard en Ridderkerk
P/a griffie

Uw brief van:		Ons kenmerk:	1350128
Uw kenmerk:		Contact:	R. de Winter
Bijlage(n):		Doorkiesnummer:	
		E-malladres:	r.d.winter@bar-organisatie.nl
		Datum:	- 9 OKT 2018

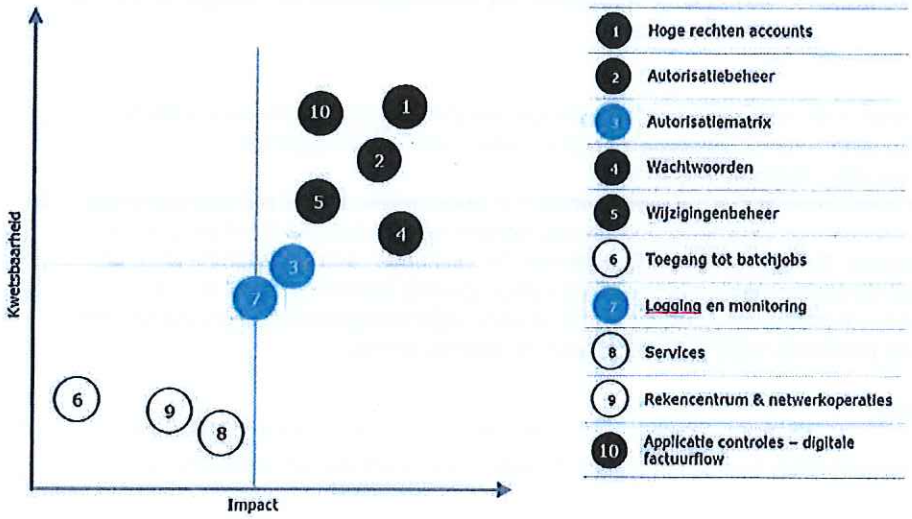
Betreft: Raadsinformatiebrief Voortgang acties IT Audit

Geachte raadsleden,

INLEIDING

Naar aanleiding van de bespreking van het accountantsverslag en de bevindingen van de accountant in de Managementletter 2017 is door enkele raadsleden gevraagd naar de bevindingen uit de IT-audit en de acties die hierop zijn ondernomen. In deze brief informeren wij u hierover.
In de Management Letter 2017 heeft Deloitte de bevindingen opgenomen van de IT-audit die in juli 2017 is uitgevoerd. De conclusie van de IT-audit was *dat de opzet en bestaan van de General IT Controls onvoldoende waarborg biedt voor de betrouwbaarheid van de geautomatiseerde informatievoorziening.*
In deze Raadsinformatiebrief wordt u geïnformeerd over de voortgang van de te nemen maatregelen.

AANPAK EN PLANNING
De IT-bevindingen van de accountant zijn als volgt samen te vatten:



In 2017 en 2018 is de organisatie aan de slag gegaan met de bevindingen.

De benodigde werkzaamheden zijn uitgevoerd door interne systeembeheerders, functioneel applicatiebeheerder (Key2Financiën) en met behulp van extern ingehuurde expertise.

ACTIES

1. **Hoge rechten accounts: Gebruik van hoge rechten aanpassen aan de gestelde eisen**

Betekenis van "hoge rechten accounts": het kunnen werken in de geautomatiseerde systemen van de BAR-organisatie met meer autorisatie dan nodig is voor de uit te voeren werkzaamheden.
Vastgesteld is dat regelmatig met te hoge rechten in de geautomatiseerde systemen wordt gewerkt, zonder dat een duidelijke traceerbaarheid naar een geautoriseerde medewerker te achterhalen is. In het informatiebeveiligingsbeleid zijn de richtlijnen omtrent het gebruik van accounts met hoge rechten vastgelegd.
Om de vastgestelde tekortkomingen te verhelpen, is een aantal maatregelen uitgevoerd. Deze maatregelen zorgen voor een duidelijke traceerbaarheid naar de medewerker.
Binnen de applicatie Key2Financien is het aantal medewerkers met hoge rechten teruggebracht naar twee. Dit betreft de applicatiebeheerders. Deze personen kunnen geen kritische handelingen uitvoeren in het financiële proces. Accounts staan altijd op naam van een medewerker.

2. **Autorisatiebeheer**

Voor het aanmaken en verwijderen van accounts bestaat de IDU-procedure (in dienst-uit dienst)
Binnen Key2Financiën bestond geen duidelijk vastlegging van het aanmaken van accounts. De procedure is inmiddels dusdanig aangepast dat bij aanmaken van nieuwe accounts in Key2Financiën een handtekening wordt gevraagd van de leidinggevende. Deze aanvraagformulieren worden opgeslagen.
Verwijderen accounts: Als medewerkers uit dienst gaan, komt er een melding uit Topdesk. Op basis hiervan wordt de einddatum van het account aangepast naar de datum uitdiensttreding.
Binnen Key2Financiën bestond één gastaccount. Dit om problemen te voorkomen in de uitvoering. Dit account wordt niet meer gebruikt.

3. **Autorisatiematrix**

In 2018 (vóór de interimcontrole die Deloitte gaat uitvoeren) zal een autorisatiematrix worden opgezet voor Key2Financiën.

4. **Wachtwoorden;**

Het bestaande wachtwoordbeleid binnen Active Directory wordt als 'te vrij/te makkelijk' bevonden. Dit centrale beleid, dat standaard geldt voor alle Active Directory accounts, is aangepast alsmede ook inhoudelijk doorgevoerd voor alle gebruikersaccounts.
De complexiteit van de wachtwoorden binnen Key2Financiën zijn gebonden aan de mogelijkheden die de leverancier geeft. Deze sluiten niet geheel aan met de door Deloitte aanbevolen tabel. Het is niet mogelijk om met "speciale tekens" te werken. Met behulp van een script van de leverancier is geregeld dat alle accounts voldoen aan de standaardeisen zowel voor wat betreft de complexiteit als de geldigheid van het wachtwoord.

5. **Wijzigingenbeheer:**

MS Windows; Patch Management. Het bestaande patch managementbeleid (installeren van software updates) wordt altijd en volledig automatisch uitgevoerd. Het update beleid en de controle op de beheertaken is aangescherpt en vindt maandelijks plaats.
De bestaande procedure voor wijzigingenbeheer Key2Financiën is goedgekeurd door het management van domein Financiën. Het overzicht van de doorgevoerde wijzigingen wordt standaard ontvangen per release of patch van de leverancier. Er is geen scheiding tussen de productie en de testomgeving, wij achten dit ook niet nodig omdat de testomgeving en de productieomgeving identiek dienen te zijn. Wijzigingen voor de testomgeving worden, na goedgekeurde testen, altijd doorgevoerd in productie. Het beheer van de wijzigingen in de productie wijkt dus niet af van de testomgeving.

6. **Toegang tot batchjobs:**

Voor zover bekend hebben wij geen batch jobs. Deze vaak nachtelijke processen waarbij er zonder gebruikers interactie gegevensverwerking kan plaatsvinden is geen onderdeel van dit werkproces.

7. **Logging en monitoring**

De ontbrekende logging op essentiële onderdelen van Active Directory zijn geïnventariseerd. Er zijn maatregelen genomen om deze daar waar mogelijk in te schakelen. Ook zijn maatregelen genomen om de gewenste logging-levels te controleren en te realiseren.

8. Services

Een van de punten uit de audit is dat op belangrijke servers taken actief zijn die wellicht niet direct noodzakelijk zijn voor het functioneren van de desbetreffende server. Het uitzetten van deze taken vermindert de kans op mogelijk misbruik en toegang die deze taken bieden. In het derde kwartaal van 2018 wordt een programma in gebruik genomen dat er voor kan zorgen dat overbodige services worden uitgeschakeld.

9. Rekencentrum en netwerk operaties

De beveiligingsmaatregelen voor het hebben van toegang tot de serverruimtes zijn aangescherpt en worden maandelijks gecontroleerd.

10. Applicatie controles – digitale factuurflow

De audit stelt volgende maatregelen voor ten aanzien van de digitale factuurflow:

- In het derde kwartaal 2018 wordt een pilot uitgevoerd om te kijken of het (qua systeemmogelijkheden en tijdbesteding) uitvoerbaar is om de gevraagde audit trail (het digitale controlespoor) uit te voeren op crediteuren stamgegevens en toegevoegde / verwijderde / gewijzigde autorisaties.
- Factuurroutering-Key2Financiën: Facturen die gescand worden, worden centraal opgeslagen op het netwerk. Het opslaan van deze scans op dat stukje van het netwerk is alleen mogelijk via deze ene factuurscanner. Alle medewerkers van de crediteurenafdeling hebben leesrechten om de facturen in te kunnen zien. Zij kunnen dus geen scans toevoegen, wijzigen of verwijderen.
- Autorisaties met betrekking tot accorderen: er wordt voorgesteld een procuratiematrix op te stellen met goedkeuringslimieten per budgethouder en andere goedkeurende medewerkers. In de mandaatregeling is een en ander reeds vastgelegd. Procuratie is ons inziens van belang bij de opdrachtverstrekking, niet bij de facturenkant. Bij het geven van een opdracht aan een leverancier gaan we een verplichting aan. Dat is het moment waarop autorisatie nodig is. Facturen zijn altijd achteraf. De opdracht is al gegeven en uitgevoerd. Achteraf goedkeuring geven voor iets wat al gedaan is vinden wij niet zinvol.
- Eindcontrole betaalbaarstelling: het advies is om eindcontroleurs geen factuurdetails te laten aanpassen. Tijdens de audit bleek dat dit alleen mogelijk was voor Stichting Gebouwenbeheer Barendrecht (SGB) en Ontwikkelingsmaatschappij Midden-IJsselmonde (OMMIJ). Deze twee bedrijven zijn per 1 januari 2018 vervallen. De verbetersuggestie is daarmee niet meer van toepassing.
- Hetzelfde geldt voor de functiescheiding ten aanzien van registreren, coderen, goedkeuren, eindcontrole van facturen: tijdens de audit bleek dat dit vanwege de kleine omvang van de organisaties, niet volledig in te regelen was voor SGB en OMMIJ.

Samenvattend kunnen we stellen dat de genoemde punten uit de audit inmiddels grotendeels zijn opgelost. Voor een aantal punten lopen er nog acties in het derde/vierde kwartaal van 2018.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,

Het dagelijks bestuur van de BAR-organisatie,

Hans Cats
secretaris

drs. Hans-Christoph Wagner
voorzitter DB