

Raadsinformatiebrief

Van	Burgemeester en Wethouder/Burgemeester	Zaak nr.	583337
Aan	Gemeenteraad	RIB nr.	2019 - 62
Portefeuillehouder	K.J. Walters	Datum	21 oktober 2019
Informatie bij	Michiel van Oosterom	Tel. nr.	(035) 629 2945

Onderwerp

Rapportage 213a Onderzoek IT Audit

Kernboodschap

De ontwikkelingen op het gebied van informatisering en automatisering binnen de gemeenten bepalen tegenwoordig voor een groot deel het gezicht van de gemeente. Een goede beheersing van de informatisering en de automatisering wordt steeds belangrijker. Een goede betrouwbare IT-omgeving binnen Hilversum is randvoorwaardelijk voor het functioneren van de gemeente richting burgers, instellingen en bedrijven. Daarom is besloten tot het laten uitvoeren van een IT-audit in het kader van de jaarrekeningcontrole, met name gericht op de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking. Deze IT-audit is een nulmeting, gericht op de beoordeling van de kwaliteit van de algemene IT-beheersmaatregelen, en het verstrekken van assurance bij Eénduidige Normatiek Single Information Audit voor gemeenten (ENSIA).

In hoofdlijnen is de conclusie van het onderzoek dat voor wat betreft de IT General Controls (ITGC) er sprake is van een zorgvuldige aansturing en een gedegen inrichting door competente en betrokken teammanagers en medewerkers. In dit kader is de hoofdconclusie van het onderzoek dat de gemeente Hilversum in opzet en bestaan 'in control' is bij de beheersing van de ITGC, voor wat betreft de maatregelen die van materieel belang zijn in het kader van de jaarrekeningcontrole. In het kader van de jaarrekeningcontrole van de gemeente Hilversum heeft de VIC in samenwerking met extern bureau Noordbeek aspecten van de automatiseringsorganisatie onderzocht die zijn gericht op een betrouwbare gegevensverwerking.

Aanleiding

Kwalitatief goede IT general controls worden al jaren gezien als fundament om in de jaarrekening te kunnen steunen op geautomatiseerde informatiesystemen. Het inrichten en onderhouden van beheersingsmaatregelen rond informatietechnologie (IT controls) is de afgelopen jaren, ook als onderdeel van de financiële verslaglegging en de verantwoording die daarover moet worden afgelegd, belangrijker geworden. IT controls vormen een onderdeel van de algemene interne beheersingsmaatregelen die een organisatie kan treffen. Interne beheersing definiëren we hierbij als een stelsel van processen dat is ingericht door de leiding van een organisatie om een redelijke mate van zekerheid te krijgen over het realiseren van de effectiviteit en efficiency van de bedrijfsvoering, de betrouwbaarheid van de financiële verslaglegging en de naleving van relevante wet- en regelgeving.

In de management letter 2018 is als aanbeveling door de accountant aangegeven nader inzicht te krijgen in de kwaliteit van de IT omgeving. In het kader van de jaarrekeningcontrole 2018 van de gemeente

Hilversum heeft de interne audit functie in samenwerking met extern bureau Noordbeek de aspecten van de automatiseringsorganisatie onderzocht die zijn gericht op een betrouwbare financiële gegevensverwerking.

Uitkomsten IT Audit

In hoofdlijnen zien wij bij de IT General Controls (ITGC) een zorgvuldige aansturing en een gedegen inrichting door competente en betrokken teamleiders en medewerkers. In dit kader is de hoofdconclusie dat de gemeente Hilversum in opzet en bestaan 'in control' is bij de beheersing van de ITGC, voor wat betreft de maatregelen die van materieel belang zijn in het kader van de jaarrekeningcontrole.

Bij een meer diepgaande, deels technische analyse zijn er echter manco's geconstateerd in de instellingen van de netwerkbeveiliging, met name een incorrecte inrichting van het wachtwoordbeleid, soms ontbrekende wachtwoordexpiratie, onvoldoende lange wachtwoorden bij service- en systeemaccounts, het soms ontbreken van een afgedwongen wachtwoordsyntax, actieve accounts die te lang ongebruikt zijn etc. De meer gedetailleerde bevindingen zijn uitgeschreven als zeven bevindingen en zeven geprioriteerde adviezen.

In het uitgevoerde detailonderzoek zijn negen bevindingen gesignaleerd op de processen, die deels betrekking hebben op de betrouwbaarheid van de gegevensverwerking en deels op de efficiëntie van deze interne processen.

Reactie op rapportage

Ons college heeft met belangstelling kennis genomen van het rapport. De uitkomsten van het rapport komen overeen met onze perceptie omtrent de automatiseringsomgeving, die overall gekwalificeerd wordt als in control. Desalniettemin hechten wij waarde aan het verder verbeteren van de kwaliteit in de IT omgeving en nemen voor zover mogelijk de geïnventariseerde suggesties en/of aanbevelingen over.

Vervolgtraject

Het uitgevoerde onderzoek en de uitkomsten zijn besproken met de interne organisatie. Na toezending van dit rapport aan de raad wordt dit geagendeerd in de Audit- en Rekeningcommissie ter bespreking van de uitkomsten en de voorgestelde suggesties en/of aanbevelingen.

Burgemeester en wethouders van Hilversum,
de gemeentesecretaris,

de burgemeester,

D. Emmer

P.I. Broertjes

Bijlage(n):

1. intern rapport Noordbeek IT-audit Hilversum 2018
2. Samenvatting en status bevindingen IT-Audit (bijlage A)

Deze raadsinformatiebrief is digitaal beschikbaar op [internet](#) onder "Vergaderstukken", B&W-vergadering van 15 oktober 2019.

Bijlage A : Samenvatting en status van bevindingen IT Audit

1. Strategie en beleid;
Er is al twee jaar geen informatiemanager werkzaam bij de gemeente Hilversum. Mede hierdoor moet het nieuwe informatiebeleid nog worden opgesteld. Er is geconstateerd dat de IT-strategie en het IT-beleid kunnen worden toegelicht, maar niet zijn vastgelegd. *Inmiddels is er een strategische informatiemanager aan de slag gegaan en wordt gewerkt aan kaderstellend IT beleid welke in najaar naar de raad zal gaan.*
2. IT-organisatie en Control
De IT-organisatie is adequaat ingericht. Een kanttekening wordt geplaatst bij de borging van de continuïteit van het functioneel applicatiebeheer van Key2Financiën. Geconstateerd wordt dat het ontbreken van een tweede functionele applicatiebeheerder een risico is voor de gemeente, aangezien er dan geen adequate vervanging beschikbaar is bij eventuele afwezigheid of een vertrek. *Het College heeft in de kadernota en begroting 2020 extra gelden hiervoor vrijgemaakt om dit applicatiebeheer op peil te brengen.*
3. Risicobeheersing:
VOG Voor alle medewerkers van de gemeente Hilversum dient bij indiensttreding een geheimhoudingsverklaring en een Verklaring Omtrent Gedrag (VOG) te worden gevraagd. Geconstateerd wordt echter dat in de 'ENSIA Rapportage zelfevaluatie' bij vraag 8.1.2.b 'Worden de gegevens die de medewerker opgeeft voorafgaand aan het dienstverband geverifieerd?' als antwoord staat 'Nee'. Hierbij staat als opmerking 'VOG is niet altijd aanwezig voor aanvang van de werkzaamheden. *In het werving en selectie procedure en aanstellingsbrieven is deze plicht nader benoemd en wordt door het lijnmanagement gestuurd hierop. Ook wordt bij de uitgifte van gebouw Keys inlog codes aan nieuwe gebruikers als extra waarborg een kopie paspoort en kopie VOG ter inzage gevraagd.*
4. Risico's in de expiratie-instellingen van administrator-accounts
Bij de analyse van de Active Directory (AD) blijkt dat voor zes administrator-accounts de wachtwoordexpiratie niet actief is, waardoor sommige wachtwoorden al een of twee jaar niet zijn gewijzigd. *De gemeente Hilversum heeft deze melding geverifieerd en vastgesteld dat de instelling van drie van deze zes administrator-accounts onjuist is. Dit is direct opgepakt en gecorrigeerd.*
5. Risicovolle service- en systeemaccounts in de AD
Bij 1.102 accounts is de wachtwoordexpiratie niet geactiveerd in de Active Directory (AD). Van deze 1.102 accounts hebben er 625 de status 'Enabled' en kunnen worden gebruikt. Geconstateerd wordt dat de service- en systeemaccounts toegang geven tot veel interne functionaliteit van de infrastructuur en applicaties, en dat zwak wachtwoordbeheer voor deze accounts leidt tot onacceptabele risico's voor de gemeente Hilversum. *Na vaststelling van het nieuwe wachtwoorden beleid (zie punt 9) wordt dit z.s.m. opgepakt.*
6. Risico's door het ontbreken van een afgedwongen wachtwoordsyntax
Bij 206 accounts is geen wachtwoordsyntax vereist *Met het vernieuwde en snellere wifi netwerk in september 2019 is dit opgelost en voorkomen we nieuwe vervuiling.*
7. Risico's van actieve accounts die langdurig niet of nooit zijn gebruikt
Er zijn 787 accounts met de status 'Enabled' die langer dan één jaar niet hebben ingelogd. Dat zijn serviceaccounts, medewerkers die langdurig afwezig zijn en niet-afgemelde vertrokken medewerkers. Geconstateerd wordt dat in onvoldoende mate toezicht wordt gehouden op het risico van mogelijk misbruik van langdurig niet of nooit gebruikte accounts. *De IT organisatie is bezig dit proces van dichtzetten van niet of langdurig ongebruikte accounts te verbeteren.*
8. Risico's van de vervuiling van de Active Directory (AD)
Bij deze IT-audit zijn een aantal bevindingen geconstateerd in de AD. *Met het vernieuwde en snellere wifi netwerk in september 2019 is dit opgelost en voorkomen we nieuwe vervuiling.*
9. Instroom, doorstroom en uitstroom
Geconstateerd wordt dat het proces voor uitstroom nog niet effectief is, waardoor er nog veel risicovolle 'ongebruikte' accounts bestaan. Hierbij is sprake van risico's voor ongemerkt misbruik van dergelijke accounts. *De IT organisatie is bezig dit proces van uitstroom met Role based user management dusdanig te reguleren dat dit proces m.b.t. autorisatiewijzigingen en 'ongebruikte'*

accounts wordt verbeterd. De verwachting is dat Role based user management in de loop van 2020 gereed is.

10. Wachtwoordbeleid

De gemeente Hilversum heeft een wachtwoordbeleid. Geconstateerd wordt echter dat het technisch bewaren van slechts 3 voorgaande wachtwoorden in combinatie met 0 dagen als minimum wachtwoordwijzigingsperiode gebruikers de mogelijkheid biedt om oude wachtwoorden te herhalen. *Door Informatiemanagement is een wachtwoord beleid opgesteld en deze wordt nu geïmplementeerd.*

11. Logging en Monitoring

De gemeente Hilversum heeft geen beleid voor logging van activiteiten en gebeurtenissen in de infrastructuur, servers en besturingssystemen. Geconstateerd wordt dat door de afwezigheid van logging het natrekken van incidenten of inbreuken wordt belemmerd, aangezien de daarvoor relevante informatie niet is vastgelegd. *Na vaststelling van het nieuwe wachtwoorden beleid (zie punt 9) wordt dit opgepakt.*

12. Configuratie Management

De Configuratie Management Database (CMDB) zit in TOPdesk. Geconstateerd wordt dat de CMDB op dit moment nog incompleet is. *In 2018 is er een project uitgevoerd gericht op het proces rondom configuratiemanagement en deze is afgerond waardoor deze weer actueel is.*

13. Change Management

De gemeente Hilversum heeft een Change Advisory Board (CAB). Deze behandelt in de praktijk alleen echte wijzigingen. Het proces verloopt nog niet helemaal vlekkeloos. Geconstateerd wordt dat er behoefte is aan een proces waarbinnen onder andere impactanalyses worden uitgevoerd en business cases worden beoordeeld, voorafgaande aan de besluitvorming door de CAB. *Hiertoe is het zogenaamde SPIN-overleg ingericht waardoor wijzingen in de architectuur en software omgeving integraal afgewogen kunnen worden en beheerst. De komende maanden zal dit wijzigingsproces nog verder worden verbeterd.*

14. Incident en Probleem Management

De processen wijzigingsbeheer, configuratiemanagement en incidentbeheer worden op een projectachtige wijze verder verbeterd. Geconstateerd wordt dat de gemeente Hilversum in januari 2018 is gestart met het documenteren van het proces voor Probleem Management, maar vervolgens niet is overgegaan tot realisatie van dit proces. *De IT organisatie heeft dit opgepakt en is in progressie. Het proces voor Probleem Management is er in concept en wordt nu gescreend op werking en volledigheid.*

15. Testgegevens

Er is een overtreding van de BIG en AVG geconstateerd door het gebruik van niet-geanonimiseerde productiegegevens voor test- en acceptatiedoelinden. *Dit is alleen voor de test omgeving waar alleen beheerders toegang toe hebben. Met het nieuwe privacy beleid zal dit actief worden aangepakt.*

16. Applicaties beheerd door de business

Er is een gebrek aan regie geconstateerd bij het beheer van contracten voor applicaties en SLA's binnen de afdelingen van de business, waardoor de gemeente mogelijk niet over de bedrijfseconomisch meest aantrekkelijke applicatieve ondersteuning beschikt. *Het College heeft besloten om het contractmanagement en sturing op prestaties van de afgesloten contracten te centraliseren. Het College heeft in de kadernota en begroting 2020 extra geld hiervoor vrijgemaakt om contractmanagement voor de grote kernapplicaties met 1 fte op peil te brengen.*

17. Recovery

De gemeente Hilversum maakt gebruik van klassieke back-ups. Er wordt regelmatig een restore aangevraagd, maar er wordt geen testplan gehanteerd. Geconstateerd wordt dat door het ontbreken van restore-testen het niet aantoonbaar is dat een back-up kan worden gebruikt na een calamiteit. *Restore vindt plaats maar generiek proces voor testen is er niet. De IT organisatie zal dit jaar een restore-test voor een grote kernapplicatie doorlopen waarna een generiek proces voor alle restores wordt uitgeschreven.*