

Interne IT Audit 2020 Q4

Bevindingen rapportage



Datum: 10-02-2021

Gemeente Almere



Inleiding

Doel en Scope

Gedurende 2020 wordt elk kwartaal een interne IT-audit uitgevoerd op basis van het geldende IT –control framework. Hiermee wordt getracht om in control te komen met betrekking tot:

- de cultuur inclusief houding en gedrag ('de IT-audit hoort bij het reguliere werkproces').
- verhogen van het belang en bewustzijn van de IT-audit.
- tussentijdse sturing en monitoring zodat de kwaliteit continu geborgd wordt.
- de voorbereiding voor de externe audit door de externe accountant.

De IT-control maakt onderdeel uit van het gedachtengoed van het gemeentebrede internal control framework, waarbij wordt uitgegaan van de Three Lines of Defence. In het kader van IT-control definiëren we de 1e lijn als het reguliere business proces van de afdeling ICTAR, de 2e lijn wordt uitgevoerd door diverse (control) medewerkers van ICTAR die periodiek controles uitvoeren (conform het IT-control framework). De derde lijn wordt gevormd door team Audit die vaststelt of afspraken worden nagekomen, of controles periodiek worden uitgevoerd, of opvolging wordt gegeven aan bevindingen en of processen worden aangepast en/of geoptimaliseerd.

De interne IT-audit werkzaamheden zijn verricht omtrent de opzet, het bestaan en de werking van de algemene IT beheersmaatregelen in- en rondom EnterpriseOne. Daarbij zijn de volgende IT elementen meegenomen:

- EnterpriseOne
- Linux
- Oracle
- Windows Active Directory

Daarnaast hebben wij tevens de getroffen beheersmaatregelen omtrent Continuïteit & Security getoetst.

Management samenvatting

In 2020 heeft team Audit & Risk diverse audits uitgevoerd op de IT General Controls (opzet, bestaan en werking) over de gehele periode 2020.

Sinds de vorige IT audit heeft ICTAR de volgende acties ondernomen:

- Aanpassen van controle rapportages naar een maandelijkse frequentie.
- Aanscherpen van maandelijkse controles 2^e lijn op EnterpriseOne.

BELANGRIJKSTE OBSERVATIES EN VERBETERPUNTEN

In overeenkomst met 2019 hebben wij vastgesteld dat de kwaliteit van de 2^e lijn verder kan worden verbeterd. Ondanks de aanwezigheid van formele procedures kan de uitvoering van de 2^e lijn controles worden versterkt op het gebied van nauwkeurigheid, tijdigheid, uitvoerigheid en pro activiteit. Wij willen management expliciet benadrukken dat de controles van groot belang zijn binnen het controlemodel van de gemeente waarbij de interne én externe auditor gebruik maakt van de door de 2^e lijn verrichte werkzaamheden. Temeer omdat voor 2021 afspraken zijn gemaakt dat Deloitte gaat steunen op de werkzaamheden.

Binnen wijzigingsbeheer hebben wij vastgesteld dat het akkoord van de proceseigenaar ontbreekt in de wijzigingsaanvraag. Daarnaast is in het TopDesk ticket onduidelijk of een acceptatietest is vereist en uitgevoerd.

Door een upgrade aan EnterpriseOne zijn een aantal controlerapportages niet meer operationeel en dienen te worden aangepast.

Binnen de Windows Active Directory en Oracle worden de periodieke reviews op de juistheid van de gebruikers en toegekende rechten niet uitgevoerd.

De maximale wachtwoordduur binnen de Windows Active Directory wijkt af van de gestelde norm en de Baseline informatiebeveiliging Overheid (BIO).

Overzicht van bevindingen

#	Omschrijving	Categorie	2019	2020	Pagina
1	Uitdienstcontrole is niet uitgevoerd	EnterpriseOne	●	●	5
2	Controle op doorstroom is niet tijdig uitgevoerd	EnterpriseOne	●	●	6
3	Controle op toegekende autorisaties is niet volledig uitgevoerd	EnterpriseOne	●	●	7
4	Vastlegging werkzaamheden op doorgevoerde wijzigingen onvolledig	EnterpriseOne	●	●	8
5	Rapportages voor gebruikersreview zijn niet beschikbaar	EnterpriseOne	●	●	9
6	Review op Windows AD accounts niet maandelijks uitgevoerd	Windows	●	●	10
7	Wachtwoordinstellingen wijken af van beleid	Windows	-	●	11
8	Ontbreken van gebruikersreview op Oracle	Oracle	●	●	12

● Hoog risico bevinding ● Medium risico bevinding ● Laag risico bevinding

1. Uitdienstcontrole is niet uitgevoerd

Laag

Observatie	Risico
Om te voorkomen dat uitdienst getreden medewerkers nog toegang hebben tot EnterpriseOne zijn er uitdienstcontroles ingericht. Op basis van een deelwaarneming hebben wij vastgesteld dat er gedurende 2020 geen uitdienstcontrole is uitgevoerd. Dit komt omdat de rapportage van uitdienststreders in de nieuwe versie van EnterpriseOne niet is ingericht. Er is geen koppeling ingericht tussen EnterpriseOne en Profit. De twee databases zijn in de nieuwe structuur gescheiden wegens privacy redenen. Wij hebben begrepen dat er, wegens Single Sign-On wordt gesteund op de effectieve werking van het IAM proces.	Risico dat er na uitdienstdatum nog gebruik wordt gemaakt van het EnterpriseOne account.
Actieplan	Management reactie
A. Geen actie omdat er wordt gesteund op de effectieve werking van IAM en Single Sign-On. Derhalve zal deze controle niet meer worden meegenomen in de 2021 testwerkzaamheden.	

2. Controle op doorstroom is niet tijdig uitgevoerd

Medium

Observatie	Risico
Maandelijks wordt vanuit AFAS Profit een overzicht gestuurd van bekende contractbeëindigingen van de komende 2 weken. Op basis van deze overzichten wordt maandelijks een controle uitgevoerd op functiewijzigingen van EnterpriseOne gebruikers. Op basis van onze controle werkzaamheden hebben wij vastgesteld dat er in het eerste kwartaal van 2020 niet voor elke maand tijdig een controle op doorstroom is uitgevoerd.	• Risico dat functiewijzigingen niet worden opgemerkt en gebruikers derhalve onterecht autorisaties bezitten
Actieplan	Management reactie
A. Inventariseer of er door het niet tijdig uitvoeren van de doorstroom rapportage een risico is ontstaan waardoor medewerkers toegang hebben gehad tot EnterpriseOne terwijl deze niet meer tot hun functie behoort.	

3. Controle op toegekende autorisaties is niet volledig uitgevoerd

Medium

Observatie	Risico
Op maandelijkse basis wordt een controle uitgevoerd op toegekende autorisaties in EnterpriseOne. De rapportage dient op basis van een maandelijkse frequentie te worden gedraaid en neemt alle toegekende autorisaties mee van die maand. Wij hebben vastgesteld dat de controles niet tijdig zijn uitgevoerd.	Risico dat ongeautoriseerde toegangsrechten tot EnterpriseOne en bijbehorende functieconflicten niet worden opgemerkt
Actieplan	Management reactie
A. Voer een analyse uit op alle missende maanden waarop geen review is uitgevoerd. B. Waarborg dat de uitgevoerde werkzaamheden en het eindoordeel in het TopDesk ticket juist en volledig worden vastgelegd.	

4. Vastlegging werkzaamheden op doorgevoerde wijzigingen onvolledig

Medium

Observatie	Risico
Op maandelijkse basis wordt door de 2^e lijn een controle uitgevoerd op doorgevoerde wijzigingen naar de EnterpriseOne productieomgeving. Door middel van een deelwaarneming hebben wij de controle van de doorgevoerde wijzigingen beoordeeld. Daarbij hebben wij vastgesteld dat in het TopDesk ticket niet wordt aangegeven of de wijzigingen conform de opzet van de beheersmaatregel zijn verlopen. Tevens ontbreken de onderliggende TopDesk tickets van de wijzigingen én een conclusie. Op basis van een analyse van de TopDesk tickets uit onze deelwaarneming vastgesteld dat het akkoord van de proceseigenaar ontbreekt in de wijzigingsaanvraag. Daarnaast is het onduidelijk of een acceptatietest is vereist en uitgevoerd.	• Risico dat een verkeerde wijziging is aangebracht in het productiesysteem door de ontwikkelaar welke impact heeft op de juistheid en volledigheid van de gegevensverwerking.
Actieplan	Management reactie
A. Pas het TopDesk ticket aan waarin de uitgevoerde review is vastgelegd en voeg de uitgevoerde werkzaamheden en conclusie toe. B. Waarborg dat de uitgevoerde werkzaamheden en het eindoordeel in het TopDesk ticket juist en volledig conform de opzet van de beheersmaatregel worden vastgelegd.	

5. Rapportages voor gebruikersreview zijn niet beschikbaar

Laag

Observatie	Risico
Elk kwartaal wordt door de verantwoordelijke leidinggevende een review uitgevoerd op toegekende rollen binnen een afdeling. Wij hebben begrepen dat de review door de verantwoordelijk leidinggevenenden niet is uitgevoerd omdat de rapportages vanwege de EnterpriseOne upgrade nog moeten worden aangepast. Een review op beheer is wel uitgevoerd. Als mitigerende controle is eind 2020 een review uitgevoerd op de juistheid van budgethouders binnen EnterpriseOne.	• Risico dat ongeautoriseerde toegangsrechten tot EnterpriseOne en bijbehorende functieconflicten niet worden opgemerkt
Actieplan	Management reactie
A. Ontwikkel een rapportage met alle gebruikers en bijbehorende rollen in EnterpriseOne per afdeling B. Borg dat de review elk kwartaal wordt uitgevoerd met expliciete bevestiging van de leidinggevende.	

6. Review op Windows AD accounts niet maandelijks uitgevoerd

Laag

Observatie	Risico
Op maandelijkse basis dienen controles te worden uitgevoerd op toegekende autorisaties binnen de Windows Active Directory: (1) een controle op alle nog actieve Windows Active Directory accounts van uitdiensttrekkers; (2) toegekende A en LSD accounts met hoge rechten, en (3) review op toegekende rechten binnen de Windows AD. Wij hebben begrepen dat een rapportage voor het uitvoeren van de controle op toegekende autorisaties binnen de Windows Active Directory niet is ingericht. Er wordt daarmee gesteund op de effectieve werking van IAM.	• Risico dat ongeautoriseerde toegangsrechten tot Windows Active Directory en bijbehorende functieconflicten niet worden opgemerkt
Actieplan	Management reactie
A. Onderzoek of de rapportage op toegekende autorisaties binnen de Windows Active Directory nog dient te worden ingericht of dat er wordt gesteund op de geautomatiseerde controle binnen IAM.	

7. Wachtwoordinstellingen wijken af van beleid

Laag

Observatie	Risico
Gemeente Almere beschikt over een wachtwoordbeleid waarin de binnen de gemeente geldende wachtwoordeisen staan beschreven. Op basis van inspectie van het document hebben wij begrepen dat de volgende eisen worden gesteld: - Wachtwoorden bestaan uit minimaal 8 karakters - Het wachtwoord moet bestaan uit tenminste 1 hoofdletter, 1 cijfer en/ of 1 vreemd teken. - Wachtwoorden zijn maximaal 60 dagen geldig en mogen niet binnen 10 keer herhaald worden. - Maximaal 5 pogingen bij foutieve wachtwoorden Op basis van inspectie van de Windows AD wachtwoordinstellingen hebben wij vastgesteld dat de maximale wachtwoordduur is ingesteld op 90 dagen. Dit is in strijd met het door de gemeente opgestelde wachtwoordbeleid. Wij hebben begrepen dat de gemeente dit vanwege de Corona maatregelen heeft aangepast. Doordat er minder wachtwoorden worden gewijzigd wordt het aantal meldingen aan de Servicedesk beperkt en hoeven laptopgebruikers niet elke 60 dagen naar kantoor om het wachtwoord te wijzigen.	• Risico dat het wachtwoord van de gebruiker kan worden achterhaald en daarmee ongeautoriseerd toegang kan worden verkregen tot de IT omgeving.
Actieplan	Management reactie
A. Onderzoek of de aanpassing van de maximale wachtwoordduur nog benodigd is en of dit weer conform beleid kan worden ingesteld.	

8. Ontbreken van gebruikersreview op Oracle

Medium

Observatie	Risico
Periodiek dient er een User Access Review te worden uitgevoerd op de Oracle database. Daarbij dient te worden gekeken of de juiste gebruikers (medewerkers, beheerders, systeemaccounts en leveranciers) toegang hebben tot het systeem én of deze zijn gekoppeld aan de juiste profielen. Wij hebben vastgesteld dat deze review op de juistheid van toegekende rechten binnen Oracle database op de EnterpriseOne server (PCDR2) over het eerste semester van 2020 niet is uitgevoerd. De review in het tweede semester is uitgevoerd.	Risico dat ongeautoriseerde toegangsrechten tot Oracle niet worden opgemerkt
Actieplan	Management reactie
A. Voer periodiek een review uit op de juistheid van toegekende rechten binnen Oracle waarbij eventuele bevindingen tijdig worden opgevolgd B. Leg de resultaten van de controle vast in TopDesk	

Appendix

Appendix A: Overzicht geïnterviewde personen

Naam	Functie
Björn Dietrich	Functioneel beheerder EnterpriseOne
Anuschka Stevens	Functioneel beheerder EnterpriseOne
Yvonne Boonstra	Senior Medewerker Serviceorganisatie ICT
Frankla Huistra	Senior Medewerker Serviceorganisatie ICT
Gary King	Technisch Architect
Randy Snellenburg	Technisch Security Specialist
Marlous Weber	Functioneel beheerder AFAS Profit