

Interne IT Audit 2021

Opzet voorstel



Datum: 30-11-2020

Gemeente Almere



Inleiding

Doel en Scope

Als onderdeel van het in 2018 begonnen verbeterplan voert de afdeling Audit & Risk van de Gemeente Almere interne audit werkzaamheden uit op de IT beheersmaatregelen. Daarbij wordt elk kwartaal een audit uitgevoerd op basis van het geldende IT-controle raamwerk.

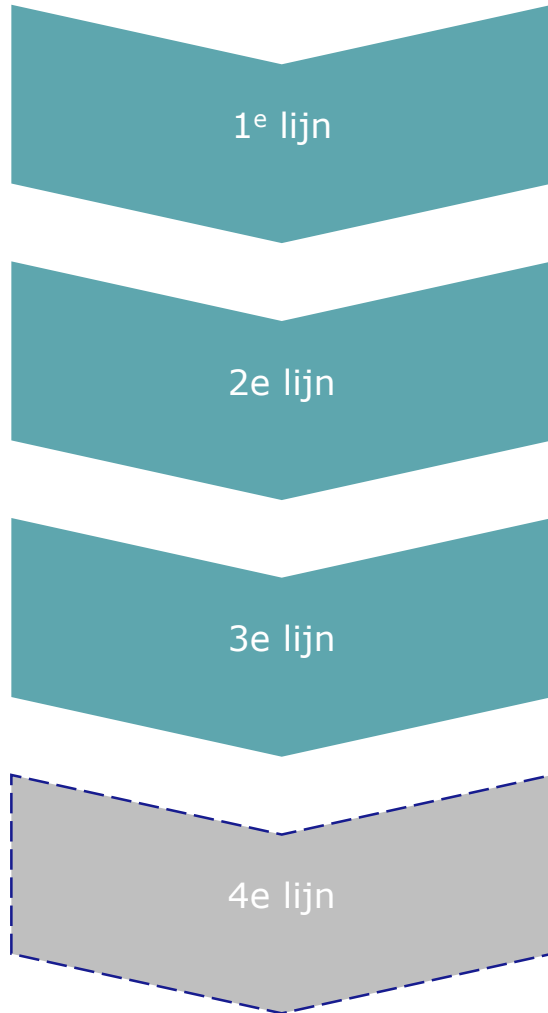
De periodieke IT audit is onderdeel van het gemeente brede interne controle raamwerk waarbij wordt uitgegaan van de Three Lines of Defence. In het kader van IT-control definiëren we de 1e lijn als het reguliere business proces van de afdeling ICTAR, de 2e lijn wordt uitgevoerd door diverse (control) medewerkers van ICTAR die periodiek controles uitvoeren (conform het IT-controle raamwerk). 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.

In het kader van efficiëntie en minimale belasting voor de interne organisatie is in november 2020 is met de externe accountant besproken om voor het boekjaar 2021 zoveel mogelijk gezamenlijk de werkzaamheden uit te voeren. Daarbij dient rekening te worden gehouden met de voor de externe accountant geldende vaktechnische (COS) eisen en beperkingen.

In dit document is een uiteenzetting gegeven van de voorgestelde planning en aanpak.



Inleiding



- Afdeling ICTAR
 - Reguliëre uitvoering van operationele processen
- Medewerkers ICTAR belegd met controle
 - Periodiek uitvoeren controles uit het IT-controle raamwerk
- Interne auditdienst Gemeente Almere
 - Vaststellen of controles 2^e lijn juist en volledig worden uitgevoerd
 - Controleren of opvolging wordt gegeven aan bevindingen en processen worden aangepast en/of geoptimaliseerd.
- Externe auditor (Deloitte)
 - Uitvoering werkzaamheden jaarrekening
 - (Deels) steunend op werkzaamheden 3^e lijn



Planning & scope



Planning

De werkzaamheden zullen na elk kwartaal worden uitgevoerd. Dit betekent dat in 2021 viermaal dezelfde cyclus van werkzaamheden zullen worden uitgevoerd.

1. Q1 – begin april 2021
2. Q2 – begin juli 2021
3. Q3 – begin oktober 2021
4. Q4 – begin januari 2022

Tijdens elke testperiode wordt na het uitvoeren van de testwerkzaamheden een rapportage met bevindingen opgesteld en afgestemd met de betrokkenen. Vervolgens zal worden bepaald welke aanvullende werkzaamheden er dienen te worden uitgevoerd om de ontstane risico's te mitigeren.

#	Omschrijving
1	Voorbereiding en planning • Inplannen van interviews • Inrichten audit dossier
2	Uitvoeren werkzaamheden • Uitvoeren testwerkzaamheden in opzet, bestaan en werking • Interviews met betrokken personen • Inspectie en beoordelen van evidence • IPE werkzaamheden
3	Rapportage • Opstellen rapportage van bevindingen • Bespreken van rapportage
4	Remediation • Afstemming van bevindingen en actieplan met proceseigenaren • Uitvoeren herstelwerkzaamheden



Scope

Voor de IT audit van 2021 stellen wij de volgende aanpak voor:

1. Algemene IT beheersmaatregelen

Overeenkomstig aan de aanpak van 2019 en 2020 bestaat de basis van onze werkzaamheden uit het testen van de algemene IT beheersmaatregelen in en rondom EnterpriseOne. Deze werkzaamheden zullen worden uitgevoerd zodat de juistheid en volledigheid van (financiële) rapportages vanuit EnterpriseOne kan worden geborgd. Daarbij zullen de onderstaande IT elementen en deelgebieden worden gecontroleerd.

IT element	Kenmerk	Access Security	Change Management	Continuïteit
Windows AD	O/S	✓	✓	
Linux	Applicatieserver	✓	✓	
Oracle Database	Database	✓	✓	
EnterpriseOne	Applicatie	✓	✓	
Security	Deelgebied	✓		
Continuïteit	Deelgebied	✓		✓

Gemeente Almere heeft een deel van het IT beheer uitbesteed aan Fujitsu. Om de effectieve werking van de door Fujitsu uitgevoerde taken te toetsen zullen wij de ISAE 3402 Type 2 beoordelen. Deze wordt jaarlijks in februari door Fujitsu beschikbaar gesteld. Wij zullen de scoping van de werkzaamheden, het gehanteerde normenkader en bevindingen beoordelen. Daarnaast stellen wij vast of (en zo ja, welke) gebruikersoverwegingen in de verklaring van toepassing zijn.

2. Cyber

Als onderdeel van onze IT audit werkzaamheden al in 2021 ook aandacht worden besteed aan de getroffen Cyber maatregelen binnen de gemeente. Daarbij zal door middel van gesprekken en inspectie van documentatie een inventarisatie worden gedaan naar de aanwezigheid van operationele (bijv. awareness training) en technische (bijv. firewall) controles op het gebied van informatiebeveiliging.

Scope

3. Application controls

In 2021 zullen wij tevens controle werkzaamheden uitvoeren op het proces van digitale factuurwerking en de toekenning van subsidies. Dit onder de voorwaarde van een effectief stelsel van algemene IT beheersmaatregelen (zie #1).

Tijdens onze audit werkzaamheden testen wij de geautomatiseerde beheersmaatregelen rondom het registreren, toewijzen, goedkeuren en betalen van inkoopfacturen. Tevens zullen wij werkzaamheden verrichten op het proces van beoordelen, goedkeuren en toewijzen van subsidieaanvragen.

Middels een lijncontrole worden opzet en bestaan van de processen in kaart gebracht. Op basis van deze inzichten identificeren wij de geautomatiseerde (*application*) controles die vervolgens worden getoetst.

4. Data analyse

Ter aanvulling op de (preventieve) application controls kunnen wij data analyse werkzaamheden uitvoeren op de beschikbare audit-trail binnen EnterpriseOne. Daarbij kan worden gedacht aan de volgende detectieve analyses:

- Functiescheiding crediteuren:
 - vaststellen dat er functiescheiding aanwezig is tussen het registreren, goedkeuren en betalen van de factuur.
 - Vaststellen dat facturen zijn geaccordeerd door daartoe gemachtigde personen.
- Dubbele facturen: vaststellen dat de factuur niet dubbel is betaald
- Functiescheiding subsidies:
 - vaststellen dat er functiescheiding aanwezig is tussen het registreren, goedkeuren van de beschikking.
 - Vaststellen dat subsidieaanvragen zijn geaccordeerd door daartoe gemachtigde personen.

Aanpak



Aanpak

Normenkader

Voor het uitvoeren van de interne IT audit werkzaamheden zal gebruik worden gemaakt van het door de gemeente opgestelde raamwerk. Voorafgaand aan de werkzaamheden in het 1^e kwartaal zal met Deloitte worden afgestemd of dit raamwerk afdoende is.

Test aanpak en deelwaarneming

Het gehanteerde controleraamwerk is opgedeeld in verschillende controles:

1. Geautomatiseerde controles (bijvoorbeeld wachtwoordinstellingen)
2. Procedurele controles 1^e lijn (niet in scope 2^e lijn)
3. Procedurele controles 1^e lijn (wel in scope 2^e lijn)

De deelwaarnemingen zullen door Deloitte worden geselecteerd en vervolgens door de gemeente worden getoetst. Zie document 'Risk & Control Matrix - v1.0 - Opzet IT Audit 2021' voor de (D&I en/of OE) testaanpak per beheersmaatregel en bijbehorende deelwaarneming.

Interviews

Tijdens de uitvoering zullen verschillende interviews worden gehouden met de uitvoerders van de beheersmaatregel en/of proceseigenaren. De gemeente geeft Deloitte de mogelijkheid om deel te nemen aan de interviews.

De gesprekken voor het testen van opzet en bestaan van de beheersmaatregelen zullen plaatsvinden in april 2021. Na elk interview zal de IAD een gespreksverslag opstellen welke zowel met de geïnterviewde als Deloitte zal worden afgestemd.

Vastlegging

Voor de in 2021 uit te voeren werkzaamheden zal de gemeente voor de vastlegging gebruik maken van het door Deloitte beschikbaar gestelde template. Dit heeft als voordeel dat Deloitte geen of beperkte aanvullende vastlegging hoeft uit te voeren ten opzichte van reeds door de gemeente uitgevoerde werkzaamheden.



Aanpak

Interviewschema

#	Onderwerp	Aandachtsgebied	IT element	Contactpersoon
1	• Access security • Toegangsbeveiliging • Change management	• Indienstproces • Uitdienstproces • Doorstroomproces • Wijzigingsproces • Hoge rechten accounts • Review op aanwezige gebruikers • Review op directe mutaties database • Wachtwoordinstellingen	• EnterpriseOne	Frankla Huistra - Senior Medewerker Serviceorganisatie ICT
2	• Change management • Access security	• Patch management • Wachtwoordinstellingen • Audit trail instellingen	• Windows • Unix • OracleDB	Gary King - Technisch architect
3	• Access security	• Hoge rechten accounts • Review op aanwezige gebruikers	• Windows • Unix • OracleDB	Randy Snellenburg - Technisch Security Specialist
4	• Continuïteit • Interfaces	• Toegang tot datacentrum • Back-up schema • Back-up monitoring • Interface monitoring	• EnterpriseOne • Windows • Unix • OracleDB	Gary King - Technisch architect
5	• IPE rapportages	• Totstandkoming rapportages 2e lijn EnterpriseOne	• EnterpriseOne	Björn Dietrich – Functioneel beheerder EnterpriseOne
6	• IPE rapportages	• Totstandkoming doorstroom rapportage	• Profit	Marlous Weber – Functioneel beheerder AFAS Profit

