



IT-auditplan Gemeente Almere

Boekjaar 2021

Team Audit – afdeling Financiën & Control

Versie : 1.0
Datum : 9 december 2021
Auteur : H.W.P. (Peter) Niemeijer

INHOUDSOPGAVE

1	INLEIDING	3
2	KADERS	4
2.1	Doelstelling	4
2.2	Team Audit	4
2.3	Stakeholders.....	4
2.4	Werkwijze	4
2.5	Scope en uitgangspunt	5
2.6	Internal control.....	5
2.7	Stip op de horizon	6
3	PRAKTISCHE ZAKEN	7
3.1	Opdrachtgeverschap IT-audit	7
3.2	Betrokkenen	7
3.3	Planning.....	7
3.4	Communicatie.....	8
3.5	Randvoorwaarden efficiënte interne controle.....	8
3.6	Omgang met persoonsgegevens.....	8

1 Inleiding

Voor u ligt het IT-auditplan 2021 van de gemeente Almere. Dit plan is door team Audit, afdeling Financiën en Control opgesteld in nauwe samenwerking met de afdeling ICTAR. Dit auditplan vormt de basis voor de uit te voeren (interne) IT-audit voor het begrotingsjaar 2021.

Centraal staat dat de gemeente Almere een betrouwbare bedrijfsvoering nastreeft. Dit geldt in steeds belangrijkere mate voor de betrouwbaarheid van de IT-omgeving. Interessant is ook dat de bestuurlijke aandacht voor dit onderwerp toeneemt, wat maakt dat voor 2021 de ambitie wordt uitgesproken dat – voor de jaarrekening – gesteund kan worden op de IT-omgeving.

Om dit te realiseren wordt ieder kwartaal het IT-control framework (het normenkader) uitgevoerd en intern getoetst. Hierbij wordt gebruik gemaakt van de systematiek van de three-lines-of-defence, waarbij de business de eerste lijn vormt, de control medewerkers van ICTAR de tweede lijn en Audit completeert de derde lijn.

Het primaire doel van de IT-audit is het verbeteren van de interne beheersing van het IT-landschap van de gemeente Almere. Secundair willen we een betrouwbare basis creëren voor de externe IT-audit die de accountant uitvoert in het kader van de jaarrekeningcontrole. De interne beheersing van het IT-landschap kent drie belangrijke aspecten die elkaar ondersteunen en versterken. Het gaat om mensen, organisatie en techniek, zoals weergegeven in onderstaande figuur.



Willen we de ambitie realiseren dan gaat het niet alleen om de techniek en organisatie; het gaat vooral over de mens- en cultuurkant. Dit betekent extra aandacht besteden aan houding, gedrag en bewustwording. Dit realiseren we door open te communiceren over bevindingen en aanbevelingen, een centrale kick-off met betrokkenen, periodieke controles en monitoren van de voortgang. Het management van F&C en ICTAR wordt hierbij betrokken.

De IT-audit werkzaamheden richten zich op de opzet, het bestaan en werking van de algemene IT beheersmaatregelen in- en rondom Enterprise One (general IT-controls). Daarbij worden de componenten Enterprise One, Linux, Oracle en Windows Active Directory gecontroleerd. Daarnaast worden getroffen beheersmaatregelen omtrent Continuïteit & Security getoetst.

We sluiten deze managementsamenvatting af door te verwijzen naar de onderwerpen die in de onderliggende hoofdstukken worden beschreven. In hoofdstuk 2 worden de algemene kaders geschetst zoals doestelling, controleaanpak en scope. In hoofdstuk 3 worden een aantal praktische zaken beschreven zoals planning, betrokken medewerkers en het opdrachtgeverschap.

2 Kaders

2.1 Doelstelling

Met de uitvoering van de interne IT-audit wordt de kwaliteit en betrouwbaarheid van het IT-landschap beoordeeld. Specifiek wordt gekeken naar de general IT-controls (GITC) van het financiële systeem alsmede naar de onderliggende structuur. Dit doen we omdat we een betrouwbare jaarrekening willen realiseren. Om dit vast te stellen voert Audit ieder kwartaal een audit / onderzoek uit om te toetsen of de interne processen in opzet en bestaan werken. Hierover wordt na iedere controlemoment gerapporteerd.

2.2 Team Audit

Team Audit maakt onderdeel uit van de afdeling Financiën & Control. Vanuit rol en functie wordt de interne audit altijd vanuit objectiviteit en onafhankelijkheid uitgevoerd. Team Audit is toetsend en signalerend.

2.3 Stakeholders

De belangrijkste stakeholders voor team Audit zijn de afdelingen ICTAR en Financiën & Control. De afdeling ICTAR is dat omdat zij primair verantwoordelijk is voor de betrouwbaarheid, continuïteit en integriteit van het financiële systeem. De afdeling F&C is dat omdat zij eigenaar is van het financiële pakket (Enterprise) en verantwoordelijk is voor de juiste inrichting (zoals functiescheiding, autorisaties en procesinrichting). Andere belangrijke stakeholders zijn de wethouder financiën en de concerncontroller. Externe stakeholders zijn de accountant en de belastingdienst.

2.4 Werkwijze

In 2019 is het IT-control framework vastgesteld. Dit framework is de basis voor het toetsen van de IT-omgeving. Het IT-landschap wordt ieder kwartaal getoetst door de tweede lijn (control medewerkers ICTAR) en de derde lijn (Audit).

De uitkomsten van de IT-audit worden vastgelegd in werkprogramma's inclusief onderbouwende documentatie en vertaald naar een rapport met bevindingen en aanbevelingen. Een risicoanalyse maakt onderdeel uit van dit proces. Het rapport wordt ieder kwartaal besproken met het management van ICTAR en F&C. Monitoring van de voortgang en uit te voeren acties naar aanleiding van de audit vallen ook onder de verantwoordelijkheid van Audit.

De uitgevoerde werkzaamheden door de gemeente worden beschikbaar gesteld aan de externe accountant die deze controleert in het kader van de jaarrekeningcontrole. De accountant zal hierbij gebruikmaken van alle (intern) beschikbare controle-informatie. De externe accountant kan uit hoofde van zijn eigen verantwoordelijkheid en oordeelsvorming niet volledig steunen / gebruikmaken van de beschikbaar gestelde controle-informatie en is daarom verplicht tot het houden van interviews, het selecteren van de deelwaarnemingen en het gedeeltelijke re performen van de door Audit verrichtte en vastgelegd de werkzaamheden. Audit maakt voor de vastlegging gebruik van de door Deloitte beschikbaar gestelde formats voor vastlegging en oordeelsvorming. Deloitte trekt zelfstandig de steekproeven voor de audit van de derde lijn. Tevens maakt de derde lijn de betrouwbaarheid van de rapporten inzichtelijk.

Audit coördineert het IT-auditproces intern en in afstemming met de externe accountant.

2.5 Scope en uitgangspunt

De IT-audit werkzaamheden richten zich op de opzet, het bestaan en werking van de algemene IT beheersmaatregelen in- en rondom Enterprise One (general IT-controls) over het jaar 2021. Daarbij worden de componenten Enterprise One, Linux, Oracle en Windows Active Directory gecontroleerd. Daarnaast worden getroffen beheersmaatregelen omtrent Continuïteit & Security getoetst. Voor het boekjaar 2021 hanteert de gemeente het uitgangspunt dat gesteund kan worden op de ITGC in het kader van de jaarrekeningcontrole. De externe accountant ondersteunt dit uitgangspunt.

2.6 Internal control

Bij de totstandkoming van het normenkader is het internal control framework (ICF) als basis gebruikt. Het ICF van gemeente Almere is gebaseerd op COSO, de beste-practice voor het opzetten, analyseren en verbeteren van interne beheersingssystemen. Een goed functionerend ICF helpt de gemeente op de lange termijn, om succesvol te zijn en om de doelstellingen te realiseren.

COSO identificeert de relatie tussen risico's en het interne beheerssysteem en hanteert de gedachte dat interne beheersing een proces is dat gericht is op het verkrijgen van zekerheid over het bereiken van de doelstellingen in vier categorieën: strategisch, operationeel, verantwoording en voldoen en wet- en regelgeving.



Verder stelt COSO dat een beheersing- en controlesysteem uit 5 elementen bestaat. Deze elementen komen duidelijk terug in het IT-control framework en de gehanteerde controleaanpak.

- de interne controleomgeving (houding en gedrag, normen en waarden, competenties)
- risicobeoordeling (identificatie en analyse van risico's - risicomanagement)
- beheersingsmaatregelen (regels en procedures om beleid uit te voeren en te controleren)
- informatie en communicatie (vastlegging van informatie en communicatie erover ter beheersing)
- monitoring (bewaken goede werking)

Een belangrijk element van het ICF is de zogenaamde three-lines-of-defence. De kern hiervan is dat het afdelingsmanagement integraal verantwoordelijk is voor hun eigen proces, de beheersing, de kwaliteitstoets en de verantwoording daarover.

In de gemeente Almere is de eerste lijn het primaire proces van een afdeling. Daarnaast zijn er functies in een afdeling die de eerste lijn ondersteunen, adviseren en bewaken of de afdelingsmanager zijn verantwoordelijkheden neemt. Dit is de tweede lijn. De derde lijn is de functie die controleert of het samenspel tussen de eerste en tweede lijn soepel functioneert en daarover een objectief, onafhankelijk oordeel velt met mogelijkheden tot verbetering. In Almere wordt de derde lijn uitgevoerd door team Audit. De 3 lines of defence kent verschillende verschijningsvormen maar wordt het beste als volgt weergegeven:



2.7 Stip op de horizon

In 2021 ligt de focus nog op het toetsen van de kwaliteit van de GITC in het kader van de jaarrekening. Cyberrisico's zullen daarin betrokken worden, bijvoorbeeld op basis van de NBA cyber health check. Tevens wordt voor 2021 geïnventariseerd welke application controls reeds in het financiële pakket zijn ingericht en welke kunnen worden gebruikt ter vervanging van de huidige (handmatige) controles. Naast de application controls in het financiële pakket is het de ambitie van Almere om ook het subsidieproces te toetsen op basis van application controls. Dit lijkt een logische en realistische stap omdat de subsidiemodule onderdeel uitmaakt van het financiële systeem (Enterprise One).

Daarnaast zal worden onderzocht of andere werkzaamheden mogelijk efficiënter zijn in uitvoering, maar toch dezelfde betrouwbaarheid als application controls opleveren. Deze uitkomsten worden dan ook betrokken in het normenkader.

Eind 2020 zal worden geïnventariseerd welke application controls reeds in het financiële pakket zijn ingericht en welke kunnen worden gebruikt ter vervanging van de huidige (handmatige) controls. In 2021 zal tevens worden onderzocht op welke wijze deze audit te verbreden is naar systemen (zoals de systemen die worden gebruikt voor subsidies, grondverkoop en belastingen).

3 Praktische zaken

3.1 Opdrachtgeverschap IT-audit

Het opdrachtgeverschap voor de IT-audit is dual belegd bij zowel de afdelingsmanager ICTAR als de afdelingsmanager F&C. ICTAR is opdrachtgever vanwege de primaire verantwoordelijkheid voor de gemeentebrede IT-omgeving, F&C omdat zij eigenaar is van het financiële systeem. Beide afdelingen hebben belang bij een adequate inrichting van de IT-audit en een positieve uitkomst. Het is evident dat beide afdelingsmanagers instemmen met dit IT-auditplan (akkoord via mail).

3.2 Betrokkenen

De teammanager Audit is eindverantwoordelijk voor de kwaliteit van de uitgevoerde IT-audit. Bij de daadwerkelijke uitvoering zijn diverse medewerkers betrokken.

Wie	Rol	Moment betrokkenheid
Raad	Toezichthouder	Informeren politieke markt
Wethouder Financiën	Bestuur	Definitief rapport
Concerncontroller	Toetsend en signalerend	Plan en definitief rapport
Afdelingsmanager ICTAR	Integraal verantwoordelijk IT	Plan en definitief rapport
Afdelingsmanager F&C	Integraal verantwoordelijk Enterprise	Plan en definitief rapport
Teammanager ICTAR	Verantwoordelijk IT-audit ICTAR	Plan en rapporten
Teammanager Audit	Verantwoordelijk IT-audit Audit – 3 ^e lijn	Plan en rapporten
IT-auditor	Toets IT-control framework – 3 ^e lijn	Volledige controleperiode
Functioneel beheer	Uitvoeren werkzaamheden – 2 ^e lijn	Ieder kwartaal
Security medewerker	Uitvoeren werkzaamheden – 2 ^e lijn	Ieder kwartaal
Control medewerker	Uitvoeren werkzaamheden – 2 ^e lijn	Ieder kwartaal

De wethouder financiën, de concerncontroller en de afdelingsmanagers ICTAR en F&C ontvangen na afronding van de IT-audit de definitieve rapportage.

3.3 Planning

De controle heeft betrekking op het begrotingsjaar 2021 maar wordt gedurende het jaar uitgevoerd. De afronding vindt plaats in 2022. De planning op hoofdlijnen ziet er als volgt uit.

Wat	Wanneer	Wie
Kick-off IT-audit 2021	Januari 2021	Team Audit / ICTAR
IT-audit – 1 ^e kwartaal	April 2021	IT-auditor
Bespreken rapport	Mei 2021	Teammanager Audit / ICTAR
IT-audit – 2 ^e kwartaal	September 2021	IT-auditor
Bespreken rapport	Oktober 2021	Teammanager Audit / ICTAR
Externe IT-audit (tussentijds)	Oktober 2021	Deloitte (<i>input voor de boardletter</i>)
IT-audit – 3 ^e kwartaal	November 2021	IT-auditor
Bespreken rapport	December 2021	Teammanager Audit / ICTAR
IT-audit – 4 ^e kwartaal (follow-up)	Januari 2022	IT-auditor
Bespreken definitief rapport	Februari 2022	Audit/ICTAR/wethouder/CC

De tweede lijnwerkzaamheden door control medewerkers van ICTAR worden wekelijks of maandelijks uitgevoerd. De derde lijn voert haar werkzaamheden ieder kwartaal uit.

3.4 Communicatie

Het controlejaar kent vele communicatiemomenten; bij de afstemming van de planning, de uitvoering van de audits en het opstellen van de rapportages. Alle betrokkenen worden tijdig geïnformeerd (via agendaverzoek, mail). Als sprake is van te bespreken stukken dan worden deze tijdig beschikbaar gesteld, zodat er ruim voldoende tijd is voor hoor en wederhoor.

3.5 Randvoorwaarden efficiënte interne controle

Om de IT-audit zo efficiënt en effectief mogelijk uit te kunnen voeren en de juiste conclusies te kunnen trekken is uitgegaan van de volgende randvoorwaarden:

- Medewerking vanuit ICTAR
 - aanlevering van dossiers, lijstwerk et cetera
 - beschikbaar voor eventuele inhoudelijke vragen en toelichtingen.
 - toegang tot relevante applicaties
 - aanleveren van dossiers, lijstwerk et cetera
 - beschikbaar voor vragen en informatie
- Medewerking vanuit financieel beheer
 - aanleveren van informatie
 - beschikbaar voor vragen en informatie
- Medewerking van de afdelingsmanagers en teammanagers in het kader van de bespreking van het controleplan en het controlerapport

3.6 Omgang met persoonsgegevens

Uit hoofde van hun rol krijgt Audit bij de uitvoering ook (persoons) informatie te zien. Met deze informatie wordt zeer zorgvuldig omgegaan. Wij zijn ons zeer bewust van de (mogelijke) gevoeligheid van deze informatie. Bij twijfel over het gebruik van informatie stemmen we dit collegiaal met elkaar en met de privacy-coördinator af. De verbijzonderde interne controle hanteert de volgende uitgangspunten bij het omgaan met informatie:

- we passen het proportionaliteitsbeginsel toe: dit houdt in dat we ons altijd afvragen of het gebruik van persoonsgegevens in verhouding staat tot het doel waar het voor wordt gebruikt. Dat betekent dat alleen die persoonsgegevens worden gebruikt die noodzakelijk zijn voor een vooraf bepaald en duidelijk omschreven doel
- waar mogelijk maken wij gebruik van lijstwerk/bestanden die zo min mogelijk herleidbare informatie bevatten. Als er bijvoorbeeld sprake is van unieke cliëntnummers, dan is het niet nodig om een kolom met BSN-nummers (of zelfs NAW) op te nemen
- mocht het toch nodig zijn om per mail gegevens uit te wisselen
 - anonimiseren we persoonsgegevens
 - versleutelen we de mail
- waar dit handig is delen we informatie of wisselen we informatie uit via de T-schijf. Dit doen we door het geven van rechten voor bepaalde folders. Dit is veiliger dan mailen
- voor overdracht van grote bestanden (waar mogelijk ook persoonsgegevens in staan) maken we gebruik van een beveiligde omgeving (ook richting de externe accountant).