

MEMO

Opsteller: Sandra de Wolff
Team: Strategie, Financiën en Control
Kenmerk: D/22/050527
Datum: 27 januari 2022
Vertrouwelijkheid: Openbaar

Onderwerp: Aanbieden resultaten IT-Audit

Aanleiding: toezegging van college LTA T- 463

Memo:

Geachte leden van de Auditcommissie,

Bijgaand treft u het ISAE 3402 type 2 certificaat ter kennisgeving aan, gelet op de toezegging (LTA T-463) van de wethouder aan de auditcommissie in uw vergadering van 20 januari 2021. In de Management Letter over het jaar 2020 heeft de accountant de gemeente de aanbeveling gedaan om een IT-audit uit te voeren. De IT-audit die de gemeente heeft laten uitvoeren heet ISAE 3402. De norm staat voor International Standard for Assurance Engagements. Hierin wordt door een externe gecertificeerde auditor gekeken hoe interne beheersmaatregelen binnen de ICT-organisatie van de gemeente Woerden zijn geïmplementeerd. Dergelijke maatregelen moeten ervoor zorgen dat de IT-systemen van de gemeente betrouwbaar en integer geregeld zijn.

De auditor heeft onder andere gekeken naar de volgende punten:

- *Testen van toegang tot de systemen.* Hierbij wordt gekeken of alleen de medewerkers toegang hebben tot de systemen die ze nodig hebben. Voorbeelden hiervan zijn blokkeren van toegang tot de systemen als medewerkers uit dienst gaan of een andere functie krijgen.
- *Actualiteit van de systemen.* Hierbij wordt gekeken of de systemen op tijd worden geüpdatet en dit gebeurt via vastgestelde procedures. Bij kwetsbaarheden (mogelijkheden die zijn gevonden om systemen te misbruiken) dienen direct herstelmaatregelen worden uitgevoerd.
- *De toegang tot apparatuur.* Het is belangrijk dat alleen bevoegde personen toegang hebben tot de serverruimte.
- *Maken van backups via vastgestelde procedures.*
- *Uitvoeren van een uitwijktest (overnemen van systemen op andere locatie) voor kritische systemen.*
- *Behandelen van incidenten.* Hierbij wordt gekeken of alle gemelde incidenten worden behandeld en geëvalueerd.

Medio 2020 heeft de eerste audit plaatsgevonden waarbij vooral is gekeken naar de opzet en het bestaan van procedures. Deze audit wordt aangeduid met ISAE 3402 type 1. Hierbij is een tekortkoming geconstateerd op de toegang tot de systemen. Het rapport van de eerste audit is verspreid onder alle klanten van de ICT-organisatie van de gemeente Woerden zoals de griffies van Woerden en Oudewater, Ferm Werk, Regionaal Historisch Centrum, Inkoop en Monitoring

Utrecht West en Regionaal Bureau Leerplicht. In december 2021 heeft een tweede audit plaatsgevonden, een zogenaamde ISAE 3402 type 2 waarbij is gekeken naar de opzet, bestaan en werking van de procedures. Hierbij zijn geen tekortkomingen geconstateerd. De auditor heeft twee aanbevelingen gegeven voor verbetering, zie punt 1.2 van de samenvatting. De IT-audit is ook besproken met de accountant. De opmerkingen van de accountant op deze IT-audit worden verwerkt in de Management Letter en bestuurlijke reactie van het college en dit wordt aangeboden in een apart memo. De aanbevelingen uit het rapport van de auditor worden zo snel mogelijk opgepakt door de ambtelijke organisatie. Bijgevoegd is het certificaat en de samenvatting van de ISAE 3402 type 2 audit.