

2023-252 Bijlage

AUDIT INFORMATIEBEVEILIGING KEY2FINANCIËN



Sparrenheuvel 32, 3708 JE Zeist | (030) 2 270 500 | info@mxl.nl | www.mxl.nl

Project 21242

Versie 1.0

24 mei 2023

ing. Edwin Mooij MISM

ICT in perspectief

M&I/Partners/

adviseurs voor management en informatie

MANAGEMENTSAMENVATTING

In opdracht van de Gemeente Nieuwegein heeft M&I/Partners in april 2023 een audit op informatiebeveiliging uitgevoerd op het systeem Key2Financiën.

Het doel van deze beoordeling is het uitvoeren van een audit, conform het vooraf opgestelde normenkader, gerelateerd aan een subset van de beheersmaatregelen zoals gedefinieerd in de Baseline Informatiebeveiliging Overheid (BIO). Door middel van deze audit wenst de Gemeente Nieuwegein inzicht te verkrijgen of de informatiebeveiligingsmaatregelen afdoende zijn in het systeem Key2Financiën.

Het toepassingsgebied van deze beoordeling omvat:

- De audit opdracht 2023;
- Het opgestelde normenkader.

Deze audit is volledig volgens het auditplan uitgevoerd.

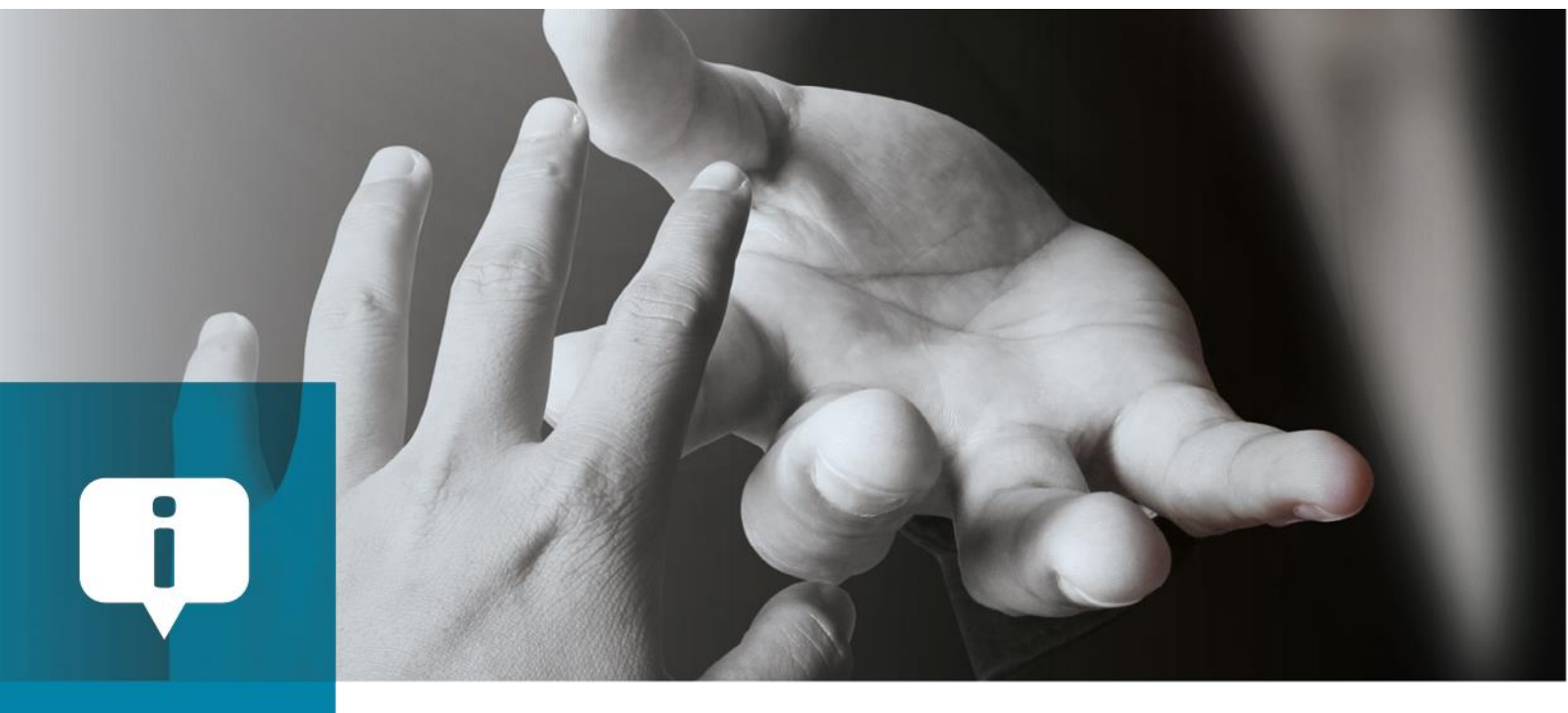
Samengevat zijn onze bevindingen als volgt:

Aantal Significante afwijkingen	0
Aantal Incidentele afwijkingen	8
Aantal Observaties	4



INHOUDSOPGAVE

1	INLEIDING	4
1.1	Opdracht	4
1.2	Doelstelling	5
1.3	Toepassingsgebieds- en auditoverwegingen	5
1.4	Bevindingen	6
1.5	Verbeterplan	7
2	AUDIT BEVINDINGEN (2023)	8
2.1	Bevindingen	9
2.2	Significante afwijkingen	13
2.3	Incidentele afwijkingen	13
2.4	Observaties	15
3	OPMERKINGEN	18



1 INLEIDING

1.1 OPDRACHT

Gemeente Nieuwegein heeft M&I/Partners gevraagd een audit uit te voeren op een deel van de beheersmaatregelen, gerelateerd aan de Baseline Informatiebeveiliging Overheid (BIO), ten behoeve van het systeem Key2Financiën. Key2Financiën wordt door de gemeente gebruikt als financieel systeem.

Het doel van deze beoordeling is het uitvoeren van een audit, conform het vooraf opgestelde normenkader, vergelijkbaar met een subset van de maatregelen zoals gedefinieerd in de Baseline Informatiebeveiliging Overheid (BIO).

De Baseline Informatiebeveiliging Overheid (BIO) beschrijft het basisniveau voor informatiebeveiliging. De BIO wordt gehanteerd binnen de Nederlandse overheid, door het Rijk, Gemeenten, Waterschappen en Provincies. Dit is één basisniveau voor informatiebeveiliging, één gezamenlijke taal voor alle overheidsorganisaties.

Het doel van de BIO norm is de informatie(-systemen) bij alle bestuurslagen en bestuursorganen van de overheid te beschermen. Alle bestuursorganen van de overheid dienen erop toe te zien dat onderling uitgewisselde gegevens beveiligd zijn, in overeenkomst met wet- en regelgeving.

1.2 DOELSTELLING

Dit rapport is opgesteld door Edwin Mooij van M&I/Partners en heeft betrekking op de onderstaande beoordelingsactiviteit:

Soort Audit/Datum/Duur	Standaard(en)	Locatie
Audit 17 april 2023 1 dag	Subset normenkader BIO	Gemeente Nieuwegein Stadsplein 1 3431 LZ Nieuwegein

Het doel van deze beoordeling is het uitvoeren van een audit, conform het vooraf opgestelde normenkader, gerelateerd aan een subset van de beheersmaatregelen zoals gedefinieerd in de Baseline Informatiebeveiliging Overheid (BIO). Door middel van deze audit wenst de Gemeente Nieuwegein inzicht te verkrijgen of de informatiebeveiligingsmaatregelen afdoende zijn in het systeem Key2Financiën.

1.3 TOEPASSINGSGEBIEDS- EN AUDITOVERWEGINGEN

Het toepassingsgebied van deze beoordeling omvat:

- De audit opdracht 2023;
- Het door Gemeente Nieuwegein opgestelde normenkader:

Nr.	Onderwerp	*	Norm
1	Governance	O	Er is een vastgesteld, actueel informatiebeveiligingsbeleid.
2	Governance	O	Er is een contract en service level agreement voor Key2Financiën en Active Directory waarin afspraken zijn vastgelegd over: - verantwoordelijkheden inzake informatiebeveiliging; - wanneer en hoe de leverancier toegang tot systemen/data van de gemeente heeft; - de inhoud en frequentie van rapportages hierover (service level reporting.)
3	Governance	B	Leveranciers leveren periodiek een onafhankelijke assurance rapportage (TPM, ISAE Type 2.)
4	Governance	B	Leveranciers leveren periodiek rapportages over informatiebeveiliging (waaronder beveiligingsincidenten.)
5	Governance	B	De gemeente evalueert deze rapportages tijdig.
6	Toegang	O	Er is een actueel wachtwoordbeleid.
7	Toegang	B	De wachtwoordvereisten voor Key2Financiën worden afgedwongen.
8	Toegang	O	Er is een actuele procesbeschrijving voor indiensttreding van medewerkers.
9	Toegang	O	Er is een actuele procesbeschrijving voor doorstroom van medewerkers.
10	Toegang	O	Er is een actuele procesbeschrijving voor uitdiensttreding van medewerkers.
11	Toegang	O	In het proces indiensttreding zijn stappen opgenomen om de nieuwe medewerker gecontroleerd toegang te geven tot de systemen.

Nr.	Onderwerp	*	Norm
12	Toegang	O	In het proces doorstroom zijn stappen opgenomen om de betreffende medewerker de toegang tot de systemen te ontfeggen, tenzij die in de nieuwe functie ook nodig is.
13	Toegang	O	In het proces uitdiensttreding zijn stappen opgenomen om de vertrekkende medewerker de toegang tot de systemen te ontfeggen.
14	Toegang	B	Toegang tot de systemen wordt gecontroleerd verleend aan nieuwe medewerkers.
15	Toegang	B	Tijdelijke toegang tot de systemen wordt gecontroleerd verleend aan leveranciers.
16	Toegang	B	Tijdelijke toegang tot de systemen wordt gecontroleerd en tijdig ingetrokken.
17	Toegang	B	Bij doorstroom van medewerkers met toegang tot (een of meer van) de systemen wordt die toegang ingetrokken als zij die niet langer nodig hebben.
18	Toegang	B	Bij uitdiensttreding van medewerkers met toegang tot (een of meer van) de systemen wordt die toegang ingetrokken.
19	Toegang	B	Mutaties in de toegang tot de systemen worden met adequate frequentie, regelmatig gecontroleerd.
20	Toegang	B	Enkel accounts die nodig zijn voor het beheer hebben toegang tot de database.
21	Wijzigingsbeheer	B	Updates van Key2Financiën worden tijdig en gecontroleerd uitgevoerd.
22	Back-up/recovery	O	Er is een actueel back-up/recoveryplan voor financiële gegevens.
23	Back-up/recovery	B	De gemeente toetst periodiek de werking van het back-up/recovery mechanisme voor financiële gegevens.

Deze audit is volledig uitgevoerd volgens het auditplan en is remote uitgevoerd (MS Teams).

1.4 BEVINDINGEN

Tijdens de uitvoering van de audit kunnen er afwijkingen worden geconstateerd. Wij classificeren afwijkingen als volgt:

Type afwijking	Bevinding
Significante afwijking	Afwijking die geconstateerd is in het geval dat: - De algehele effectiviteit van het ISMS wordt beïnvloed; of - Het vermogen van de organisatie wordt beïnvloed om haar doelstelling(en) op het gebied van informatiebeveiliging te bereiken; of - Een vereist element van de ISO-standaard ontbreekt; of - Een aanzienlijke verstoring van de werking van het ISMS
Incidentele afwijking	Afwijking die geconstateerd wordt indien: Er geen invloed is op de algehele effectiviteit van het ISMS; of

Type afwijking	Bevinding
	- Afgeweken wordt van de standaard, maar dat de afwijking geen grote invloed heeft op het vermogen van de organisatie om haar doelstelling(en) op het gebied van informatiebeveiliging te bereiken; of - Het een geringe afwijking op de werking van het ISMS betreft.
Observatie	De auditor wijst erop dat elementen op dit moment wel in overeenstemming zijn met de normen, maar dicht bij een non-conformiteit zitten of dat het gemis aan bewijs in de toekomst tot een non-conformiteit kan leiden.

1.5 VERBETERPLAN

Tijdens de audit kunnen afwijkingen worden vastgesteld. Indien significante en/of incidentele afwijkingen worden vastgesteld, dan dient de Gemeente Nieuwegein een verbeterplan op te stellen voor deze afwijkingen, waarbij de volgende oplostermijnen worden gehanteerd:

Type bevinding	Oplostermijn
Significante afwijking	Moet worden opgelost binnen 3 maanden. Na 3 maanden vindt er een heraudit plaats op deze afwijkingen.
Incidentele afwijking	Moet worden opgelost binnen 1 jaar. Deze afwijkingen worden opnieuw getoetst tijdens de volgende audit.

In het op te stellen verbeterplan dient per afwijking het volgende aangegeven te worden:

- Oorzaak van de afwijking;
- Geplande correctieve actie;
- Verantwoordelijke voor de correctieve actie;
- Tijdsplanning van uitvoering van de correctieve actie.

2 AUDIT BEVINDINGEN (2023)

Dit hoofdstuk bevat onze bevindingen t.a.v. het door Gemeente Nieuwegein opgestelde normenkader. De bevindingen zijn genummerd vanwege efficiëntie redenen.

2.1 BEVINDINGEN

Nr.	Onderwerp	*	Norm	Bevinding(en)
1	Governance	O	Er is een vastgesteld, actueel informatiebeveiligingsbeleid.	De Gemeente Nieuwegein beschikt over een gedocumenteerd Strategisch Informatiebeveiligingsbeleid 2021-2025, versie 1.1, gedateerd 1 november 2021.
2	Governance	O	Er is een contract en service level agreement voor Key2Financiën en ActiveDirectory waarin afspraken zijn vastgelegd over: - verantwoordelijkheden inzake informatiebeveiliging; - wanneer en hoe de leverancier toegang tot systemen / data van de gemeente heeft; - de inhoud en frequentie van rapportages hierover (service level reporting.)	Het systeem Key2Financiën wordt al meer dan 20 jaar door de Gemeente Nieuwegein gebruikt. De leverancier van het systeem is Centric. Er is indertijd een contract met de leverancier afgesloten met een standaard SLA. Het contract en de SLA zijn tijdens de audit niet als documentatie beschikbaar gesteld. Het systeem draait op de locatie van de Gemeente Nieuwegein en is stabiel. Vanwege de ouderdom van het contract met Centric vinden er op dit moment besprekingen plaats om het contract te actualiseren en opnieuw vast te stellen met de leverancier.
3	Governance	B	Leveranciers leveren periodiek een onafhankelijke Assurance rapportage (TPM, ISAE Type 2)	Centric levert geen periodieke onafhankelijke Assurance rapportage op. Wel is een aantal onafhankelijke beoordelingen beschikbaar die publiek toegankelijk zijn, maar geen onafhankelijke Assurance rapportage.
4	Governance	B	Leveranciers leveren periodiek rapportages over informatiebeveiliging (waaronder beveiligingsincidenten.)	Periodiek rapporteert Centric over de performance. De rapportage wordt door Centric via hun portaal (customerportal.centric.eu) ter beschikking van de klanten gegeven. Het is niet duidelijk of er over beveiligingsincidenten gerapporteerd wordt.
5	Governance	B	De gemeente evalueert deze rapportages tijdig.	Dit zou belegd moeten zijn bij de systeemeigenaar, maar daar is geen duidelijkheid over gegeven.
6	Toegang	O	Er is een actueel wachtwoordbeleid.	De Gemeente Nieuwegein beschikt over een gedocumenteerd wachtwoordbeleid, versie 0.3, gedateerd 10 februari 2021. Het wachtwoordbeleid is definitief en door DT vastgesteld in haar vergadering van 8-11-2021.
7	Toegang	B	De wachtwoordvereisten voor Key2Financiën worden afgedwongen.	In Key2Financiën zijn vreemde tekens lastig in het wachtwoord te verwerken, daarom heeft men besloten alleen op dit onderdeel af te wijken van het wachtwoordbeleid. Dit is een door de gemeente toegestane afwijking. De

Nr.	Onderwerp	*	Norm	Bevinding(en)
				wachtwoordvereisten worden voor iedere gebruiker in Key2Finance afgedwongen. Key2Finance kent geen Single-sign-on functionaliteit. Het vergelijken van het wachtwoordbeleid en de wachtwoordvereisten in Key2Finance leverde 1 afwijking op: Number of passwords to keep=UNLIMITED, dit is niet conform het wachtwoordbeleid. Gemeente Nieuwegein is bezig met het invoeren van Single-sign-on. Zodra dit is ingevoerd zal dit punt komen te vervallen of moet deze worden aangepast.
8	Toegang	O	Er is een actuele procesbeschrijving voor indiensttreding van medewerkers.	In SharePoint is er een formeel proces geïmplementeerd voor de indiensttreding van nieuwe medewerkers. Door middel van automatisch gegenereerde e-mails worden de uit te voeren acties in de organisatie uitgezet. Het proces is gedocumenteerd.
9	Toegang	O	Er is een actuele procesbeschrijving voor doorstroom van medewerkers.	Autorisaties die moeten wijzigen worden nu sporadisch meegenomen in de zogenaamde maandgesprekken. Dit is onderhanden en krijgt de komende periode een verbetering.
10	Toegang	O	Er is een actuele procesbeschrijving voor uitdiensttreding van medewerkers.	In SharePoint is er een formeel proces geïmplementeerd voor de uitdiensttreding van medewerkers. Door middel van automatisch gegenereerde e-mails worden de uit te voeren acties in de organisatie uitgezet. Het proces is gedocumenteerd.
11	Toegang	O	In het proces indiensttreding zijn stappen opgenomen om de nieuwe medewerker gecontroleerd toegang te geven tot de systemen.	In SharePoint is er een formeel proces geïmplementeerd voor de indiensttreding van nieuwe medewerkers. Door middel van automatisch gegenereerde e-mails worden de uit te voeren acties in de organisatie uitgezet.
12	Toegang	O	In het proces doorstroom zijn stappen opgenomen om de betreffende medewerker de toegang tot de systemen te ontfeggen, tenzij die in de nieuwe functie ook nodig is.	Autorisaties die moeten wijzigen worden nu sporadisch meegenomen in de zogenaamde maandgesprekken. Dit is onderhanden en krijgt de komende periode een verbetering.
13	Toegang	O	In het proces uitdiensttreding zijn stappen opgenomen om de vertrekkende medewerker de toegang tot de systemen te ontfeggen.	In SharePoint is er een formeel proces geïmplementeerd voor de uitdiensttreding van medewerkers. Door middel van automatisch gegenereerde e-mails worden de uit te voeren acties in de organisatie uitgezet.

Nr.	Onderwerp	*	Norm	Bevinding(en)
14	Toegang	B	Toegang tot de systemen wordt gecontroleerd verleend aan nieuwe medewerkers.	Deze verantwoordelijkheid is belegd bij de leidinggevende van de nieuwe medewerker. De leidinggevende moet het proces initiëren voor het verlenen van toegang tot het systeem. Hiervoor is er in SharePoint een automatisch proces gedefinieerd.
15	Toegang	B	Tijdelijke toegang tot de systemen wordt gecontroleerd verleend aan leveranciers.	De leverancier Centric kan toegang verkrijgen tot Database door gebruik te maken van het programma Teamviewer. De systeembeheerder is de enige die dit voor de leverancier mogelijk kan maken. Dit is een tijdelijke, gecontroleerde toegang.
16	Toegang	B	Tijdelijke toegang tot de systemen wordt gecontroleerd en tijdig ingetrokken.	De enige tijdelijke toegang is vertrekt aan de accountant. De accountant heeft aparte inlogcode en beschikt alleen over leesrechten. Om gebruik te maken van deze toegang moet de toegang eerst geactiveerd worden door de systeembeheerder. Logging toont aan dat de accountant geen gebruik maakt van deze faciliteit. Laatste inlog is van 14 november 2019.
17	Toegang	B	Bij doorstroom van medewerkers met toegang tot (een of meer van) de systemen wordt die toegang ingetrokken als zij die niet langer nodig hebben.	Autorisaties die moeten wijzigen worden nu sporadisch meegenomen in de zogenaamde maandgesprekken. Dit is onderhanden en krijgt de komende periode een verbetering.
18	Toegang	B	Bij uitdiensttreding van medewerkers met toegang tot (een of meer van) de systemen wordt die toegang ingetrokken.	In SharePoint is er een formeel proces geïmplementeerd voor de uitdiensttreding van medewerkers. Door middel van automatisch gegenereerde e-mails worden de uit te voeren acties in de organisatie uitgezet.
19	Toegang	B	Mutaties in de toegang tot de systemen worden met adequate frequentie, regelmatig gecontroleerd.	Autorisaties die moeten wijzigen worden nu sporadisch meegenomen in de zogenaamde maandgesprekken. Dit is onderhanden en krijgt de komende periode een verbetering. Mutaties in Key2Financiën worden bij de functioneel applicatiebeheerder aangevraagd. Mutaties in de toegang tot de systemen worden niet periodiek gecontroleerd. De Logfiles worden alleen bij calamiteiten bekeken (reactief).
20	Toegang	B	Enkel accounts die nodig zijn voor het beheer hebben toegang tot de database.	Er zijn slechts 2 medewerkers (DBA'ers) die toegang hebben tot de database.

Nr.	Onderwerp	*	Norm	Bevinding(en)
21	Wijzigingsbeheer	B	Updates van Key2Financiën worden tijdig en gecontroleerd uitgevoerd.	1 à 2 keer per jaar wordt een update uitgevoerd. Via de portaal van Centric komen hiervan meldingen. Updates worden door de gemeente zelf uitgevoerd, omdat men bekend is met het systeem. Bij sommige updates dwingt Centric af om de update zelf uit te voeren.
22	Back-up/ recovery	O	Er is een actueel back-up/recoveryplan voor financiële gegevens.	Tijdens de audit heeft de gemeente aangetoond dat er ruime backup-voorzieningen zijn getroffen. Oracle Enterprise manager geeft een melding indien de backup niet gelukt is, zodat een technisch systeembeheerder kan ingrijpen op het proces. Het ontbreekt echter aan een recoveryplan. Zekerheid over de betrouwbaarheid van de backup wordt verkregen doordat (bij nieuwe releases/updates) de actuele database in de testomgeving wordt gekopieerd vanaf een backup.
23	Back-up/ recovery	B	De gemeente toetst periodiek de werking van het back-up/recovery mechanisme voor financiële gegevens.	Tijdens de audit heeft de gemeente aangetoond dat er ruime backup-voorzieningen zijn getroffen. Oracle Enterprise manager geeft een melding indien de backup niet gelukt is, zodat een technisch systeembeheerder kan ingrijpen op het proces. Het ontbreekt echter aan een recoveryplan. Zekerheid over de betrouwbaarheid van de backup wordt verkregen doordat (bij nieuwe releases/updates) de actuele database in de testomgeving wordt gekopieerd vanaf een backup.

2.2 SIGNIFICANTE AFWIJKINGEN

Er zijn geen significante afwijkingen vastgesteld.

2.3 INCIDENTELE AFWIJKINGEN

Er is 8 incidentele afwijkingen vastgesteld:

Incidentele Afwijking #01		
Normenkader:	Zie paragraaf 1.3	
Clausule:	2	Governance
Beheersmaatregel:		
Er is een contract en service level agreement voor Key2Financiën en ActiveDirectory waarin afspraken zijn vastgelegd over: - verantwoordelijkheden inzake informatiebeveiliging; - wanneer en hoe de leverancier toegang tot systemen/data van de gemeente heeft; - de inhoud en frequentie van rapportages hierover (service level reporting.)		
Bevinding:		
Het systeem Key2Financiën wordt al meer dan 20 jaar door de Gemeente Nieuwegein gebruikt. De leverancier van het systeem is Centric. Er is indertijd een contract met de leverancier afgesloten met een standaard SLA. Het contract en de SLA zijn tijdens de audit niet als documentatie beschikbaar gesteld. Het systeem draait op de locatie van de Gemeente Nieuwegein en is stabiel. Vanwege de ouderdom van het contract met Centric vinden er op dit moment besprekingen plaats om het contract te actualiseren en opnieuw vast te stellen met de leverancier.		
Aanbeveling:		
Finaliseer het nieuwe contract en SLA met Centric. Leg ook vast dat Centric periodiek een onafhankelijke Assurance rapportage oplevert aan de Gemeente Nieuwegein en ook rapporteert over informatiebeveiliging.		

Incidentele Afwijking #02		
Normenkader:	Zie paragraaf 1.3	
Clausule:	3	Governance
Beheersmaatregel:		
Leveranciers leveren periodiek een onafhankelijke Assurance rapportage (TPM, ISAE Type 2.)		
Bevinding:		
Centric levert geen periodieke onafhankelijke Assurance rapportage op. Wel is een aantal onafhankelijke beoordelingen beschikbaar die publiek toegankelijk zijn, maar geen onafhankelijke Assurance rapportage.		
Aanbeveling:		
Finaliseer het nieuwe contract en SLA met Centric. Leg ook vast dat Centric periodiek de een onafhankelijke Assurance rapportage oplevert aan de Gemeente Nieuwegein en ook rapporteert over informatiebeveiliging.		

Incidentele Afwijking #03		
Normenkader:	Zie paragraaf 1.3	
Clausule:	4	Governance
Beheersmaatregel:		

Leveranciers leveren periodiek rapportages over informatiebeveiliging (waaronder beveiligingsincidenten).
Bevinding:
Periodiek rapporteert Centric over de performance. De rapportage wordt door Centric via hun portaal (customerportal.centric.eu) ter beschikking van de klanten gegeven. Het is niet duidelijk of er over beveiligingsincidenten gerapporteerd wordt.
Aanbeveling:
Finaliseer het nieuwe contract en SLA met Centric. Leg ook vast dat Centric periodiek een onafhankelijke Assurance rapportage oplevert aan de Gemeente Nieuwegein en ook rapporteert over informatiebeveiliging.

Incidentele Afwijking #04		
Normenkader:	Zie paragraaf 1.3	
Clausule:	5	Governance
Beheersmaatregel:		
De gemeente evalueert deze rapportages tijdig.		
Bevinding:		
Dit zou belegd moeten zijn bij de systeemeigenaar, maar daar is geen duidelijkheid over gegeven.		
Aanbeveling:		
Leg duidelijk de rollen en verantwoordelijkheden vast, bijvoorbeeld in een RACI matrix.		

Incidentele Afwijking #05		
Normenkader:	Zie paragraaf 1.3	
Clausule:	9	Toegang
Beheersmaatregel:		
Er is een actuele procesbeschrijving voor doorstroom van medewerkers.		
Bevinding:		
Autorisaties die moeten wijzigen worden nu sporadisch meegenomen in de zogenaamde maandgesprekken. Dit is onderhanden en krijgt de komende periode een verbetering.		
Aanbeveling:		
Richt het proces doorstroom van medewerkers adequaat in, documenteer het proces en implementeer het in de organisatie.		

Incidentele Afwijking #06		
Normenkader:	Zie paragraaf 1.3	
Clausule:	12	Toegang
Beheersmaatregel:		
In het proces doorstroom zijn stappen opgenomen om de betreffende medewerker de toegang tot de systemen te ontfangen, tenzij die in de nieuwe functie ook nodig is.		
Bevinding:		
Autorisaties die moeten wijzigen worden nu sporadisch meegenomen in de zogenaamde maandgesprekken. Dit is onderhanden en krijgt de komende periode een verbetering.		
Aanbeveling:		
Richt het proces doorstroom van medewerkers adequaat in, documenteer het proces en implementeer het in de organisatie.		

Incidentele Afwijking #07		
Normenkader:	Zie paragraaf 1.3	
Clausule:	17	Toegang
Beheersmaatregel:		
Bij doorstroom van medewerkers met toegang tot (een of meer van) de systemen wordt die toegang ingetrokken als zij die niet langer nodig hebben.		
Bevinding:		
Autorisaties die moeten wijzigen worden nu sporadisch meegenomen in de zogenaamde maandgesprekken. Dit is onderhanden en krijgt de komende periode een verbetering.		
Aanbeveling:		
Richt het proces doorstroom van medewerkers adequaat in, documenteer het proces en implementeer het in de organisatie.		

Incidentele Afwijking #08		
Normenkader:	Zie paragraaf 1.3	
Clausule:	19	Toegang
Beheersmaatregel:		
Mutaties in de toegang tot de systemen worden met adequate frequentie regelmatig gecontroleerd.		
Bevinding:		
Autorisaties die moeten wijzigen worden nu sporadisch meegenomen in de zogenaamde maandgesprekken. Dit is onderhanden en krijgt de komende periode een verbetering. Mutaties in Key2Financiën worden bij de functioneel applicatiebeheerder aangevraagd. Mutaties in de toegang tot de systemen worden niet periodiek gecontroleerd. De Logfiles worden alleen bij calamiteiten bekeken (reactief).		
Aanbeveling:		
Richt het proces controle mutaties in autorisaties adequaat in, documenteer het proces en implementeer het in de organisatie.		

2.4 OBSERVATIES

Er zijn 4 observaties vastgesteld:

Observatie #01		
Normenkader:	Zie paragraaf 1.3	
Clausule:	6	Toegang
Beheersmaatregel:		
Er is een actueel wachtwoordbeleid.		
Bevinding:		
De Gemeente Nieuwegein beschikt over een gedocumenteerd wachtwoordbeleid, versie 0.3, gedateerd 10 februari 2021. Het wachtwoordbeleid is definitief en door DT vastgesteld in haar vergadering van 8-11-2021.		
Aanbeveling:		
Maak het concept Wachtwoordbeleid definitief.		

Observatie #02		
Normenkader:	Zie paragraaf 1.3	
Clausule:	7	Toegang
Beheersmaatregel:		
De wachtwoordvereisten voor Key2Financiën worden afgedwongen.		
Bevinding:		
In Key2Financiën zijn vreemde tekens lastig in het wachtwoord te verwerken, derhalve heeft men besloten alleen op dit onderdeel af te wijken van het wachtwoordbeleid. Dit is een door de gemeente toegestane afwijking. De wachtwoordvereisten worden voor iedere gebruiker in Key2Finance afgedwongen. Key2Finance kent geen Single-sign-on functionaliteit. Het vergelijken van het wachtwoordbeleid en de wachtwoordvereisten in Key2Finance leverde 1 afwijking op: Number of passwords to keep=UNLIMITED, dit is niet conform het wachtwoordbeleid.		
Aanbeveling:		
Leg de geconstateerde afwijking formeel vast en wijzig de parameter "Number of passwords to keep" naar de waarde zoals deze is opgenomen in het Wachtwoordbeleid.		

Observatie #03		
Normenkader:	Zie paragraaf 1.3	
Clausule:	22	Toegang
Beheersmaatregel:		
Er is een actueel back-up/recoveryplan voor financiële gegevens.		
Bevinding:		
Tijdens de audit heeft de Gemeente aangetoond dat er ruime backup-voorzieningen zijn getroffen. Oracle Enterprise manager geeft een melding indien de backup niet gelukt is, zodat een technisch systeembeheerder kan ingrijpen op het proces. Het ontbreekt echter aan een recoveryplan. Zekerheid over de betrouwbaarheid van de backup wordt verkregen doordat de gemeente periodiek (bij nieuwe releases/updates) de actuele database in de testomgeving wordt gekopieerd vanaf een backup.		
Aanbeveling:		
Leg formeel vast dat het restoren van de database in de testomgeving 2 keer per jaar, wordt gebruikt als recoveryplan voor Key2Financiën.		

Observatie #04		
Normenkader:	Zie paragraaf 1.3	
Clausule:	23	Toegang
Beheersmaatregel:		
De gemeente toetst periodiek de werking van het back-up/recovery mechanisme voor financiële gegevens.		
Bevinding:		
Tijdens de audit heeft de gemeente aangetoond dat er ruime backup-voorzieningen zijn getroffen. Oracle Enterprise manager geeft een melding indien de backup niet gelukt is, zodat een technisch systeembeheerder kan ingrijpen op het proces. Het ontbreekt echter aan een recoveryplan. Zekerheid over de betrouwbaarheid van de backup wordt verkregen doordat de gemeente periodiek (bij nieuwe releases/updates) de actuele database in de testomgeving wordt gekopieerd vanaf een backup.		

Aanbeveling:

Leg formeel vast dat het restoren van de database in de testomgeving 2 keer per jaar, wordt gebruikt als recoveryplan voor Key2Financiën.

3 OPMERKINGEN

- De audit is gebaseerd op informatie die door de beoordeelde organisatie wordt verstrekt en/of gedeeld.
- Tot verstrekte en/of gedeelde informatie wordt gerekend: documenten (papier en/of elektronisch), administratie (papier en/of elektronisch) en/of mondeling (interviews) verstrekte informatie.
- De beoordeelde organisatie is verantwoordelijk voor het verstrekken en/of delen van informatie die daadwerkelijk, correct en volledig is.
- De audit is gebaseerd op steekproeven en daarom kunnen er niet-conformiteiten bestaan die niet zijn geïdentificeerd.
- Het management van de beoordeelde organisatie is verantwoordelijk voor het beheren van de corrigerende maatregelen om te controleren of de corrigerende maatregelen om een worden uitgevoerd zoals gepland.
- Dit rapport is opgesteld als audit voor de beoordeelde organisatie, en voor geen ander doel.
- M&I/Partners houdt alle informatie vertrouwelijk met betrekking tot de beoordeelde organisatie en deelt geen informatie met derden.