

Managementletter

Gemeente Goes
Boekjaar 2023

Aan het college van burgemeester en
wethouders van de gemeente Goes
Postbus 2118
4460 MC GOES

ONDERWERP:
Managementletter 2023

Geacht college,

Als onderdeel van de controle van de jaarrekening 2023 van de gemeente Goes hebben wij de administratieve organisatie en de daarin opgenomen maatregelen van interne beheersing beoordeeld, teneinde onze controlewerkzaamheden in overeenstemming met Nederlands recht waaronder de controlestandaarden te kunnen bepalen.

De opzet, het bestaan en in voorkomende gevallen de werking van de interne beheersingsmaatregelen van de belangrijkste bedrijfsprocessen, inclusief de geautomatiseerde gegevensverwerking, in uw gemeente zijn beoordeeld en getoetst, zodat we een terugkoppeling kunnen geven over de betrouwbaarheid van de interne informatievoorziening en de jaarrekening.

Onze bevindingen zijn gebaseerd op de normale werkzaamheden in het kader van de jaarrekeningcontrole. Deze brief bevat daardoor niet alle onvolkomenheden in uw organisatie, die bij een eventueel uitgebreid en hierop specifiek gericht onderzoek naar voren zouden kunnen komen. Zoals u zult begrijpen, is de managementletter van nature kritisch. Wij rapporteren over de eventuele leemtes of mogelijkheden ter verbetering van de financiële en administratieve processen, de administratieve organisatie daarvan en de daarin opgenomen maatregelen van interne beheersing.

Op uw verzoek geven wij in deze managementletter aan op welke wijze verbeteringen van de administratieve organisatie en de daarin opgenomen maatregelen van interne beheersing kunnen worden gerealiseerd. De aanbevelingen en oplossingsrichtingen, zoals beschreven in deze managementletter bieden u handvatten voor deze uitwerking. Wij hebben de concept managementletter toegelicht en besproken met een afvaardiging van de ambtelijke organisatie.

Deze managementletter is door ons opgesteld voor uw informatie en mag niet zonder onze uitdrukkelijke toestemming geheel of gedeeltelijk aan derden ter beschikking worden gesteld.

Wij danken u en uw medewerkers voor de samenwerking en zijn graag bereid tot het verstrekken van nadere toelichting.

Hoogachtend,
Baker Tilly (Netherlands) N.V.

Was getekend
drs. A.R.M. Peelen RA
Partner

Was getekend
D. Eijke MSc RA
Senior Manager

Inhoudsopgave

CONTACT

drs. A.R.M. Peelen RA
Partner
r.peelen@bakertilly.nl

D. Eijke MSc RA
Senior Manager
d.eijke@bakertilly.nl

R. Buijze MSc RA
Manager
r.buijze@bakertilly.nl

KANTOORGEGEVENS
Baker Tilly (Netherlands) N.V.
Stationspark 8b
4462 DZ Goes

Postbus 85
4460 AB Goes
0113 – 24 20 00



1. Bestuurlijke samenvatting



2. Interne beheersing



3. Voorbereiding controle



4. Actualiteiten



Bijlage 1: Detailbevindingen



Bijlage 2: IT-Bevindingen

1. Introductie

Doel van de managementletter

Deze managementletter bevat onze bevindingen ten aanzien van de interne beheersing (inclusief de IT-omgeving), die zijn gebaseerd op onze werkzaamheden in het kader van de jaarrekeningcontrole 2023. Deze werkzaamheden zijn dan ook niet gericht op het geven van een oordeel over de interne beheersing van uw organisatie als geheel.

Een goede interne beheersing maakt dat de risico's voor de organisatie beter beheersbaar zijn en de jaarrekeningcontrole effectiever en efficiënter kan plaatsvinden. Vanuit onze natuurlijke adviesfunctie willen wij bijdragen aan verbetering van uw bedrijfsvoering, onder andere door het analyseren van de IT-omgeving en de bedrijfsprocessen.

Voorgaande jaren hebben wij onze bevindingen eveneens met u gedeeld. In deze managementletter geven wij u een update van onze bevindingen.

Bestuurlijke samenvatting

In het volgende overzicht (zie de volgende twee pagina's) hebben wij voor u een bestuurlijke samenvatting opgenomen. Deze punten worden in detail besproken in de hierop volgende paragrafen.

1. Bestuurlijke samenvatting

1. Bestuurlijke samenvatting



Timing van werkzaamheden: Onze bevindingen in de managementletter zijn gebaseerd op de door ons uitgevoerde interim-controle tot en met begin november 2023. Eventuele ontwikkelingen die hierna hebben plaatsgevonden zijn daarom niet meegenomen in deze managementletter.



Algemene conclusie interne beheersing: Uw interne beheersing is in de basis op orde. Wel geven we in deze managementletter een aantal aanbevelingen om processen verder te optimaliseren. Daarnaast rapporteren we aanbevelingen omtrent het verder ontwikkelen van de algehele beheersomgeving en verdere verbetermogelijkheden binnen uw IT-beheersing.



Interne beheersing en interne controles: We constateren dat de gemeente Goes haar processen met name beheerst door middel van interne controles achteraf. We stellen vast dat deze controles met voldoende diepgang, tijdig en op kritische wijze worden uitgevoerd. Wel adviseren we om meer (zichtbare) interne beheersmaatregelen aan te brengen in de primaire processen, om zo de hoeveelheid aan (formele) bevindingen die uit (interne) controles blijken terug te brengen.

Daarnaast constateren we dat voor de meeste controleprocessen een tweedelijscontrole ontbreekt. Hierdoor dient de interne controleafdeling relatief veel werkzaamheden uit te voeren. We adviseren om meer tweedelijscontroles uit te voeren. Een voorbeeld hiervan is een (tussentijdse) controle op naleving van de Europese aanbestedingswet door Inkoop.



Ontwikkeling interne beheersing: We constateren dat de gemeente Goes de managementletterpunten uit boekjaar 2022 nog niet volledig heeft opgevolgd. De gemeente heeft aangegeven dat een aantal punten nog niet volledig is opgevolgd door een beperkte personeelscapaciteit in combinatie met de aanvullende werkzaamheden in het kader van de rechtmatigheidsverantwoording 2023.

De gemeente Goes heeft wel stappen gezet op het gebied van frauderisicobeheersing, door het opstellen van formele frauderisicoanalyses. Daarnaast heeft de gemeente haar interne beheersing o.a. verbeterd door het opstellen van een concept procesbeschrijving voor het inkoop- en aanbestedingsproces en het opstellen van beleid omtrent de vastlegging van de prestatie-akkoordverklaring in het financiële pakket. Ook constateren we dat er richtlijnen zijn opgesteld ter borging van een 4-ogen principe bij memoriaalboekingen en stellen we vast dat IC de naleving hiervan periodiek toetst. Tevens voert de gemeente periodieke controles uit op het 4-ogen principe binnen de inkoopstraat. Dit achten we positieve ontwikkelingen.

Tegelijkertijd constateren we, conform voorgaand boekjaar, een aantal bevindingen ten aanzien van het subsidieproces en het inkoop- en aanbestedingsproces. We hebben vernomen dat de gemeente hiervoor taskforces heeft opgericht en maatregelen hieromtrent heeft genomen. Het effect hiervan zal in de komende jaren tot uiting komen. We vragen daarbij onder andere aandacht voor de uitvoering van tussentijdse aanbestedingsanalyses, het implementeren van een subsidieregister in het primaire proces en het borgen van de volledigheid van de registratie van contracten en verplichtingen.

1. Bestuurlijke samenvatting



Rechtmatigheidsverantwoording: Vanaf 2023 dient het college van burgemeester en wethouders zelfstandig verantwoording af te leggen over de rechtmatigheid. De gemeente ligt op schema voor de verantwoording. De gemeente zal belangrijke beleidskaders 21 december 2023 vaststellen, zoals de nieuwe financiële verordening en de controleverordening. We hebben vernomen dat het normenkader 2023 begin 2024 wordt vastgesteld. Daarnaast is er een interne controleplan 2023 opgesteld en met ons afgestemd, waarin de periodieke controles van de belangrijkste financiële processen opgenomen zijn. We vragen de gemeente om bij bevindingen in het kader van de rechtmatigheid tijdig met ons te schakelen om op voorhand hierover afstemming te hebben.



IT omgeving: In het kader van onze jaarrekeningcontrole hebben we de interne beheersing rondom uw IT onderzocht. Wij hebben in dat kader de belangrijkste applicaties binnen uw gemeente onderzocht en conclusies en aanbevelingen opgenomen in het daartoe beschikbare hoofdstuk van deze managementletter. We constateren geen significante tekortkomingen. Wel constateren we een aantal verbeterpunten.

In het kader van logische toegangsbeveiliging binnen het netwerk en de applicatie adviseren we de gemeente maatregelen te treffen op het gebied van autorisatiebeheer en periodieke review van accounts met hoge rechten. Ook adviseren we om een procedurebeschrijving omtrent wijzigingsbeheer op te stellen en testwerkzaamheden formeel vast te leggen alvorens systeemwijzigingen worden doorgevoerd.

Verder adviseren we om in het kader van IT-continuïteit aanvullende maatregelen te treffen in overleg met de GR de Bevelanden. Zo adviseren we om een jaarlijkse IT-penetratietest uit te (laten) voeren.



Vooruitblik richting jaarrekeningcontrole 2023: We hebben met uw gemeente goede afspraken over de planning van de jaarrekeningcontrole gemaakt. Op voorhand identificeren we een aantal aandachtsgedebieden met verhoogde aandacht in onze controle. Dit betreffen met name de controle op de waardering van de grondexploitaties, de controle op de getrouwheid van de rechtmatigheidsverantwoording en de controle op de naleving van de Wet Normering Topinkomens. Wij vragen u, indien er sprake is van mutaties in de WNT-verantwoording, deze tijdig met ons te delen.



Tot slot hebben we vanuit het oogpunt van onze **natuurlijke adviesfunctie** in deze managementletter een hoofdstuk opgenomen met actuele ontwikkelingen. Belangrijke elementen zijn hier onder andere de update Bado, de notitie overhead en het tijdspad van te verwachten IT audits binnen de overheid.

2. Interne beheersing

2. Interne beheersing

Inleiding

In dit hoofdstuk behandelen wij onze bevindingen ten aanzien van de interne beheersing.

Achtereenvolgens worden de volgende onderwerpen besproken:

- *Algemeen*
In dit onderdeel behandelen wij het doel en de reikwijdte van de jaarrekeningcontrole, evenals onze risicoanalyse.
- *Evaluatie interne beheersing*
In dit onderdeel behandelen wij de belangrijkste bevindingen ten aanzien van de IT-omgeving, de primaire processen en de gevolgen van onze bevindingen voor de controleaanpak.
- *Controleomgeving – Ontwikkeling van de (V)IC*
De controleomgeving vormt de basis voor de interne beheersing. In dit onderdeel rapporteren wij onze waarnemingen ten aanzien van de elementen van de controleomgeving, waaronder de (Verbijzonderde) Interne Controle (VIC).
- *Rechtmatigheidsverantwoording*
In dit onderdeel gaan we in op de onderdelen van de rechtmatigheidsverantwoording, die voor het eerst zal worden afgegeven door het college in boekjaar 2023.
- *Frauderisicoanalyse en beheersing frauderisico's*
In dit onderdeel beschrijven wij de belangrijkste frauderisico's, de bijbehorende beheersingsmaatregelen en onze inschatting van het restrisico, rekening houdend met de getroffen maatregelen.
- *Data-analyse*
In dit onderdeel geven wij een overzicht van de geplande data-analyses en het effect hiervan op de controle.
- *IT-omgeving*
In dit onderdeel geven wij een visuele weergave van de IT-omgeving. Daarnaast geven wij aan welke applicaties binnen onze jaarrekeningcontrole betrokken worden, in hoeverre hierop kan worden gesteund en wat de gevolgen zijn als onvoldoende op de applicatie kan worden gesteund.

2. Interne beheersing

2.1 Algemeen

Doel en reikwijdte

Het doel van onze jaarrekeningcontrole is het vormen van een oordeel over de getrouwheid van de jaarrekening (waaronder inbegrepen de rechtmatigheidsverantwoording) als geheel, zoals bedoeld in het Besluit Accountantscontrole Decentrale Overheden (Bado). Vanuit de jaarrekeningcontrole beoordelen wij de kwaliteit van de administratieve organisatie en interne beheersing voor zover relevant voor onze oordeelsvorming en geven wij geen zelfstandig oordeel over de kwaliteit van de administratieve organisatie en interne beheersing. De controle van de jaarrekening omvat het uitvoeren van controlewerkzaamheden, waaronder risicoanalyse, cijferanalyses, beoordeling van de administratieve procedures en het daarmee samenhangende systeem van interne beheersingsmaatregelen en gegevensgerichte controlewerkzaamheden. De samenstelling en omvang van die werkzaamheden zijn noodzakelijk voor het verkrijgen van voldoende controle-informatie ter onderbouwing van ons oordeel.

Risicoanalyse

Onze risicoanalyse richt zich op een betrouwbare totstandkoming van de jaarrekening. Dit betekent dat wij niet alle risico's die voor u als gemeente relevant zijn in onze controle meenemen. De risicoanalyse is een continue proces en stellen wij gedurende de controle indien nodig bij. De belangrijkste bij uw gemeente onderkende risico's / kernpunten in de controle zijn:

- Waardering van uw grondexploitaties;
- Getrouwheid van de rechtmatigheidsverantwoording;
- Lasten zijn niet nauwkeurig verantwoord doordat de inkoopfactuur niet in overeenstemming is met de geleverde prestatie;
- Onterechte betalingen waardoor de lasten ten onrechte zijn verantwoord;
- Risico dat het management van de gemeente de procesafspraken doorbreekt, hetgeen een standaard risico is vanuit onze beroepsregels. Dit risico ziet bij uw gemeente met name toe op de schattingsposten in de grondexploitaties Deltaweg Fase 2 en Goes-West Masterplan.

In ons verslag van bevindingen rapporteren wij naar aanleiding van de jaarrekeningcontrole over bovenstaande punten. In 2023 is het risico inzake de rechtmatigheidsverantwoording toegevoegd. Daarnaast is het risico omtrent aanbestedingsrechtmatigheid niet meer van toepassing, deze verantwoordelijkheid ligt nu bij het college.

2. Interne beheersing

2.2 Evaluatie interne beheersing

Interne beheersing

Om alle financiële uitdagingen voor uw gemeente in de komende tijd in goede banen te leiden worden hoge eisen aan het planning- en control instrumentarium, alsmede het interne beheersingssysteem gesteld. De invoering van de rechtmatigheidsverantwoording door het college stelt hogere eisen aan het interne beheersingssysteem. De aanwezigheid van een adequaat intern (financieel) beheersingssysteem is daarbij een essentiële randvoorwaarde om te kunnen bijsturen en de betrouwbaarheid van financiële informatie en verslaglegging is van groot belang om dit tijdig en goed te kunnen doen.

Basis op orde echter beheersmaatregelen nog onvoldoende (zichtbaar)

Wij constateren dat op dit moment de processen in de basis op orde zijn en dat primaire functiescheiding is ingeregeld. Daarentegen zijn op onderdelen de interne beheersingsmaatregelen in het proces nog onvoldoende verankerd danwel onvoldoende zichtbaar. In die laatste situatie kan achteraf niet vastgesteld worden of de afgesproken procedures en interne controles wel bestaan en werken. Een voorbeeld hiervan is de controle op de prestatielevring binnen het inkoopproces, waarbij niet expliciet blijkt op basis waarvan een akkoord is gegeven. De (verbijzonderde) interne controlefunctie kan in deze gevallen niet systeemgericht controleren en wij als accountant ook niet. Hierdoor is het risico op fouten en onrechtmatigheden ook hoger ten opzichte van processen met veel zichtbare interne beheersingsmaatregelen. Wij adviseren de zichtbaarheid van de interne beheersingsmaatregelen te vergroten om u in staat te stellen bestaan en werking van de beheersingsmaatregelen te monitoren. Dit stelt uw gemeente in staat verder "in control" te komen. Daarnaast vermindert dit de werkdruk op uw interne controle afdeling, doordat er minder gegevensgerichte testwerkzaamheden (achteraf) plaats hoeven te vinden.

Procesbeschrijvingen

Uw gemeente beschikt momenteel over procesbeschrijvingen met betrekking tot grondaankopen, grondverkoop, het subsidieproces en het inkoop- en aanbestedingsproces. We achten het een positieve ontwikkeling dat twee belangrijke controleprocessen zijn beschreven. Tegelijkertijd vragen we aandacht voor het beschrijven van overige belangrijke controleprocessen. Het is namelijk van belang dat de gemeente beschikt over procesbeschrijvingen voor de belangrijkste controleprocessen, waaruit blijkt hoe interne beheersmaatregelen er precies uitzien. Om dit scherp in beeld te brengen is het belangrijk procesbeschrijvingen op te stellen voor de belangrijkste controleprocessen en waar deze reeds voorhanden zijn, deze te verfijnen voor de "key-controls". Deze "key-controls" worden vaak uitgevoerd door functionarissen met een controlerende of beschikkende functie. Belangrijk hierbij is om de "key-controls" zo scherp mogelijk te beschrijven aan de hand van de 6W's (wie, wat, waarom, wanneer, met welke informatie en wat wordt vastgelegd) zodat iedere betrokken functionaris weet wat er van hem of haar verwacht wordt. Daarnaast adviseren wij u blijvend aandacht te besteden aan het up-to-date houden van deze procesbeschrijvingen.

Transformatie van controle achteraf naar beheersing vooraf

Een adequate beschrijving en toereikende inrichting en werking van de interne beheersing vormt de basis om voor de (verbijzonderde) interne controle en door ons als accountant over te gaan van een gegevensgerichte naar een organisatiegerichte controlestrategie. Hierdoor wordt het mogelijk om te steunen op de maatregelen van interne beheersing waardoor minder gegevensgerichte detailcontroles hoeven te worden uitgevoerd. Daarnaast biedt een toereikende inrichting en werking van de interne beheersing ook een goede grondslag voor de rechtmatigheidsverantwoording door het college.

2. Interne beheersing

2.3 Overzicht bevindingen interne beheersing

Deze managementletter bevat onze bevindingen die zijn gebaseerd op onze werkzaamheden in het kader van de jaarrekeningcontrole voor het jaar eindigend op 31 december 2023. Deze werkzaamheden zijn dan ook niet gericht op het geven van een oordeel over de interne beheersing van uw organisatie als geheel.

Voorgaand jaren hebben wij tijdens onze besprekingen met u diverse aanbevelingen benoemd ter verdere optimalisering van de bestaande administratieve organisatie en interne beheersing. In deze managementletter geven wij u een schriftelijke update van onze bevindingen.

In de tabel rechts is een totaal overzicht opgenomen van het totaal aantal detailbevindingen. De bevindingen en onze aanbevelingen worden op de volgende pagina's van deze managementletter uitgebreider toegelicht.

De kleur van het symbool geeft de status van de constatering aan.

- = opgelost in 2023
- = actie ondernomen, maar nog niet afgerond in 2023
- = geen actie ondernomen in 2023
- = nieuwe bevinding in 2023

Ontwikkeling aanbevelingen in 2023

Aanbevelingen uit voorgaande jaren	10
Waarvan opgelost in 2023	2
Aantal nieuwe aanbevelingen in 2023	0
Totaal aanbevelingen in 2023	8
Waarvan reeds acties zijn ondernomen, maar nog niet zijn afgerond	5
Waarvan nog geen acties zijn ondernomen	3

#	Proces	Bevinding	Status	Prioriteit 2023	Prioriteit 2022
1	Algehele beheersomgeving	Geen (actuele) procesbeschrijvingen	●	Laag	Laag
2	Inkopen en aanbestedingen	Onderbouwing prestatielevering	●	Gemiddeld	Gemiddeld
3	Inkopen en aanbestedingen	Geen zichtbare interne beheersing (4-ogen principe) bij start inkoop- en aanbestedingsproces	●	Laag	Laag
4	Inkopen en aanbestedingen	Contractenregister is onvolledig	●	Gemiddeld	Gemiddeld
5	Inkopen en aanbestedingen	Verplichtingenadministratie is niet aanwezig	●	Gemiddeld	Gemiddeld
6	Inkopen en aanbestedingen	Aanbestedingsproces wordt niet structureel eenduidig uitgevoerd en vastgelegd.	●	Hoog	Hoog
7	Subsidies	Rechtmatigheidsfouten in subsidieproces	●	Gemiddeld	Gemiddeld
8	Inkopen en aanbestedingen	Tussentijdse aanbestedingsanalyse	●	Gemiddeld	Gemiddeld
	Memoriaalboekingen	Ontbrekende beheersmaatregelen bij het boeken van memorialen	●	-	Gemiddeld
	Automatisering	(Technische borging) digitale factuurstraat	●	-	Gemiddeld

2. Bevindingen en aandachtspunten

2.4 Rechtmatigheidsverantwoording

Is gemeente Goes klaar voor de rechtmatigheidsverantwoording?

Met ingang van 1 januari 2023 moet gemeente Goes zelf een rechtmatigheidsverantwoording in de jaarrekening opnemen. Voorheen vormde de accountant een oordeel over de rechtmatigheid en bracht hierover verslag uit. Met ingang van boekjaar 2023 wordt het een verplichting voor het college van Burgemeester & Wethouders om een rechtmatigheidsverantwoording af te geven. De van toepassing zijnde wet- en regelgeving (Besluit begroting en verantwoording en Besluit Accountantscontrole Decentrale overheden) is op dit moment in revisie / in consultatie. De verwachting is dat de deze formalisatie begin 2024 gaat plaatsvinden.

De rechtmatigheidsverantwoording ziet primair toe op de volgende aspecten:

- Begrotingscriterium
 - Begrotingsrechtmatigheid
 - Kredietrechtmatigheid
- Voorwaardencriterium
 - Aanbestedingsrechtmatigheid
 - Overige aspecten (treasury, subsidies, uitkeringen)
- M&O (Misbruik & Oneigenlijk) – gebruik criterium
 - Vaststellen dat college M&O-beleid heeft nageleefd

Op deze drie dossiers dient het college in het jaarrekeningdossier rekening te houden dat op deze aspecten er een toereikend onderbouwd oordeel beschikbaar dient te zijn inclusief het onderliggende interne controledossier. Dit dossier dient door de gemeente dusdanig aan ons als accountant gerapporteerd te worden, zodat wij dit als onafhankelijke derde zelfstandig moeten kunnen reviewen en beoordelen. De eisen die aan deze dossiers gesteld worden zijn dus hoger dan voorgaande jaren.

Op basis van onze gesprekken met de gemeente stellen we vast dat de gemeente in opzet haar (interne) controlewerkzaamheden op toereikende wijze gepland heeft om in beginsel een betrouwbare rechtmatigheidsverantwoording te waarborgen. Wel vragen we aandacht voor de beschikbare capaciteit om deze controles uit te voeren, gezien deze verplichte verantwoording leidt tot aanvullende werkzaamheden voor de organisatie.

2. Interne beheersing

2.5 Controleomgeving – Ontwikkeling van de (V)IC

Organisatie

Als voorbereiding op de interim-controle hebben wij een evaluatie gedaan van het controleproces van voorgaand jaar en zijn er tussen ons en de gemeentelijke organisatie heldere afspraken gemaakt over de verwachtingen voor het controleproces van 2023 (bijvoorbeeld ten aanzien van inkopen en aanbestedingen, mede in het kader van de rechtmatigheidsverantwoording). Tijdens de interim-controle hebben wij in een prettige en constructieve wijze samengewerkt met de gemeente. Belangrijke elementen in de samenwerking hierbij zien onder andere toe op:

- proactieve afstemming van bijzonderheden en/of belangrijke aandachtsgebieden bijvoorbeeld ten aanzien van de opvolging van aanbevelingen uit de management letter voorgaand jaar en grondexploitaties.
- inspanning om te zorgen dat alle gewenste informatie op een adequate wijze en voor aanvang van de controle aanwezig is.
- bereidheid en beschikbaarheid van medewerkers om onze vragen op een adequate wijze en tijdig te beantwoorden.

Inrichting en kwaliteit VIC

Een belangrijk onderdeel van de interne beheersing is de (verbijzonderde) interne controlefunctie. Deze werkt op dit moment vanuit een geformaliseerd en gestructureerd actueel controleplan. We stellen vast dat interne controles met voldoende diepgang, tijdig en op kritische wijze worden uitgevoerd. Daarnaast constateren we dat de interne controle ook nauw betrokken is bij het opstellen van interne frauderisicoanalyses. Hierdoor sluiten de IC werkzaamheden beter aan op de onderkende risico's binnen de organisatie. Op deze wijze wordt de (verbijzonderde) interne controle volwaardiger en volwassener. De frauderisicoanalyses bespreken we op de volgende pagina.

We constateren ten aanzien van interne controles nog een aantal verdere verbetermogelijkheden. Deze zien toe op:

- Het uitvoeren van een tussentijdse aanbestedingsanalyse.
- Het opstellen van een intern controleplan voor de werkzaamheden omtrent SiSa regelingen.

Tweedelijscontroles

Daarnaast constateren we dat voor de meeste controleprocessen een tweedelijscontrole ontbreekt. Hierdoor dient de interne controleafdeling relatief veel werkzaamheden uit te voeren. We adviseren om meer tweedelijscontroles uit te voeren. Een voorbeeld hiervan is een (tussentijdse) controle op naleving van de Europese aanbestedingswet door de afdeling inkoop.

Tijdigheid VIC werkzaamheden

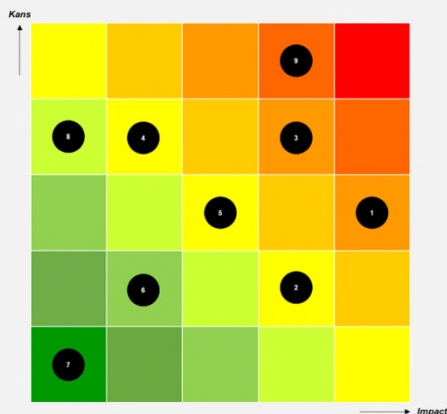
Tot slot constateren we dat de werkzaamheden op de uit te voeren steekproeven tot op heden tijdig worden afgerond. Conform voorgaand jaar zijn strakke afspraken gemaakt met de interne controle afdeling die worden nagekomen. Gezien de rechtmatigheidsverantwoording leidt tot aanvullende werkzaamheden voor de organisatie en met name voor de interne controle afdeling, vragen we tijdig met ons te communiceren wanneer de gemeente voorziet dat eventuele deadlines niet gehaald kunnen worden.

Tijdigheid van werkzaamheden is niet alleen van belang voor het verkrijgen van zekerheid over de beheersing van deze processen. Niet tijdige aanlevering heeft ook gevolgen voor de planning van onze jaarrekeningcontrole. We kunnen dan mogelijk geen gebruikmaken van de resultaten en zijn genooddaakt om extra werkzaamheden uit te voeren. Dit leidt tot extra kosten en extra werkdruk voor de medewerkers. Daarmee benadrukken we de urgentie voor het adequaat naleven van dit proces.

2. Interne beheersing

2.6 Frauderisicoanalyse en beheersing frauderisico's

Fraude- en corruptierisico's



Frauderisicoanalyse

De primaire verantwoordelijkheid voor het voorkomen en detecteren van fraude (waaronder corruptie) berust bij het college van burgemeester en wethouders. Deze verantwoordelijkheid betreft ook het onderhouden van een zodanige interne beheersing om het opmaken van de jaarrekening mogelijk te maken, zonder dat deze afwijkingen van materieel belang bevat als gevolg van fraude of fouten.

Voor het opstellen van een frauderisicoanalyse heeft de gemeente Goes een helder en gestructureerd template gebruikt. Hierin zijn voor de belangrijkste controleprocessen inzichtelijk gemaakt:

- welke frauderisico's de gemeente onderkent;
- wat de geschatte kans en impact van deze frauderisico's is;
- wat de risicorespons van de gemeente is, idealiter afgestemd op de risicobereidheid van de gemeente, zoals vastgelegd in frauderisicobeleid;
- welke interne beheersmaatregelen reeds getroffen zijn om onderkende frauderisico's te mitigeren;
- welke eventuele restrisico's/leemtes in de interne beheersing resteren en hoe de gemeente deze ondervangt (bijvoorbeeld via interne controles).

De kans- en impactweging van frauderisico's is via een risicomatrix weergegeven om op basis daarvan prioriteiten te stellen in de wijze waarop met risico's wordt omgegaan. De opzet van de risicomatrix is conform de afbeelding hiernaast.

Voor de duidelijkheid benoemen we dat er een relatie is tussen fraude en misbruik en oneigenlijk gebruik (M&O). M&O is namelijk een vorm van fraude waarbij de nadruk ligt op handelingen van derden in relatie tot het verkrijgen van overheidsbijdragen dan wel het betalen van heffingen. Wij constateren dat u bij het opstellen van de frauderisicoanalyses ook expliciet aandacht heeft besteed aan M&O-risico's, conform de 'Kadernota Voorkomen en Bestrijden Misbruik en Oneigenlijk gebruik 2023'.

Tot slot merken wij op dat het uitvoeren van een frauderisicoanalyse en het treffen van interne beheersmaatregelen, onderdeel vormen van het bredere 'frauderisicomanagement'. Frauderisicomanagement omvat namelijk ook het opstellen van frauderisicobeleid (waar M&O-beleid al dan niet onderdeel van kan vormen), het opstellen van een frauderesponsplan voor situaties dat een vermoeden van fraude bestaat en het periodiek intern evalueren in hoeverre frauderisicomanagement voldoende is ingericht en toereikend werkt binnen de organisatie. Wij adviseren de gemeente een frauderesponsplan op te stellen, in het verlengde van de reeds opgestelde frauderisicoanalyses. Onder andere middels interne controles toetst de gemeente periodiek de inrichting en de werking van het frauderisicomanagement binnen de organisatie.

2. Interne beheersing

2.6 Frauderisicoanalyse en beheersing frauderisico's

Fraude- en corruptierisico's

Frauderisicoanalyse (vervolg)

Op basis van onze uitgevoerde interim-controle stellen wij vast dat er binnen de gemeente aandacht is voor frauderisico's en de preventie daarvan. Daarnaast constateren we dat de gemeente een formele frauderisicoanalyse heeft opgesteld, waarin ook aandacht is voor risico's omtrent Misbruik en Oneigenlijk gebruik (M&O). We concluderen dat uw gemeente daarmee concrete stappen onderneemt om frauderisico's in kaart te brengen en op deze risico's in te spelen. Mede hierdoor bent u beter in staat om vanaf huidig jaar te rapporteren over misbruik en oneigenlijk gebruik als onderdeel van de rechtmatigheidsverantwoording.

Onze frauderisicoanalyse

Op basis van de bedrijfsverkenning en de interim-controle onderkennen wij het volgende frauderisico bij onze jaarrekeningcontrole:

- Risico dat het management van de gemeente de procesafspraken doorbreekt, hetgeen een standaard risico is vanuit onze beroepsregels. Wij zien dit risico op voorhand bij de schattingsposten in de grondexploitaties Deltaweg Fase 2 en Goes-West Masterplan.

De passages die wij voornemens zijn op te nemen in de controleverklaring stemmen wij tijdig met u af en zullen wij bij de bespreking van het accountantsverslag met u doornemen.

2. Interne beheersing

2.7 Data-analyse

Gebruik van data-analyse in de controle

Om te komen tot een efficiënte en effectieve controle maken wij gebruik van data-analyse.

Onderstaand hebben wij een overzicht opgenomen van de geplande data-analyses. Afhankelijk van de bevindingen naar aanleiding van de data-analyses, voeren wij waar nodig aanvullende (gegevensgerichte) werkzaamheden uit.

Analyse	Effect op de controle
Controle memoriaalboekingen	Door het analyseren van de auditfile, krijgen wij snel en diepgaand inzicht in de financiële transacties binnen uw organisatie.
Bankanalyse uitgaande betalingen	Door het analyseren van de CAMT.053 en SEPA bestanden, krijgen wij snel en diepgaand inzicht in alle uitgaande betalingen die zijn verricht vanuit de betaalomgeving van de bankapplicatie.
Analyse werkstroom inkoopfacturen	Door het verkrijgen van de juiste extractie uit Key2Financiën krijgen wij een inzicht in de workflow van inkoopfacturen en kunnen wij analyseren of verantwoorde inkoopfacturen in functiescheiding tot stand zijn gekomen gedurende het jaar.
Analyse werkstroom crediteurenstamgegevens	Door het verkrijgen van de juiste extractie uit Key2Financiën krijgen wij een inzicht in de workflow van de crediteurenstamgegevens (specifiek gericht op de bankrekeningnummers) en kunnen wij beoordelen of de doorgevoerde mutaties in crediteurenstamgegevens in functiescheiding tot stand zijn gekomen.

2. Interne beheersing

2.8 Detailbevindingen IT-beheersing - Samenvatting

De tabellen op deze pagina geven een overzicht van onze bevindingen ten aanzien van de processen en de IT aandachtsgebieden binnen uw organisatie. De detailbevindingen vindt u in bijlage 2. De mate van risico die u als organisatie loopt bij constatering verschilt per IT aandachts-gebied. Een inschatting van de impact op de controle en op uw organisatie vindt u in de afbeelding rechts.

De kleur van de het symbool geeft de status van de constatering aan.

-  Benodigd, verbetering op (korte) termijn
-  Adviespunt, verdere aanscherping mogelijk
-  Op dit moment voldoende

Onderstaande symbolen geven de status van onze bevindingen ten aanzien van de overige processen aan.

-  Opgelost
-  Actie ondernomen, maar nog niet afgerond
-  Geen actie ondernomen
-  Niet oplosbaar door omvang organisatie
-  Nieuwe bevinding
- 

Belangrijkste bevindingen IT beheersing



Omgeving	Toegangs-beveiliging	Wijzigings-beheer	Continuïteit	Proces
Netwerk		n.v.t.		
Key2Financiën				Financieel

Belangrijkste bevindingen en aanbevelingen interne beheersing

#	Proces	Bevinding	Jaar van Constateren	Status	Kans	Impact
1	Financieel	Hoge rechten bij 2 medewerkers die direct betrokken zijn bij het primaire (financiële) proces van de applicatie.	2022		Middel	Middel
2	Financieel	Wijzigingsbeheer: er worden testen uitgevoerd maar de controleerbare vastlegging ontbreekt. Daardoor voeren wij extra werkzaamheden uit op betrouwbaarheid lijstwerk.	2022		Laag	Middel
3						
4						
5						
6						

3. Voorbereiding jaarrekeningcontrole



3. Voorbereiding jaarrekeningcontrole

3.1 Planning en afspraken

Om aan uw behoeften te kunnen voldoen en om het proces voor de jaareinde controle verder te kunnen verbeteren vinden wij het belangrijk om vooraf afspraken te maken, het proces regelmatig te evalueren en onze bevindingen met u te delen. Om achteraf verrassingen te voorkomen willen wij de volgende werkafspraken met u maken:

Voorbereiding voor de jaareinde controle 2023

Onderwerp	Toelichting
Planning	Wij starten met de jaarrekeningcontrole op 15 april 2024. Om de jaarrekeningcontrole efficiënt te laten verlopen is het belangrijk dat vóór deze datum een concept jaarrekening inclusief sluitende brugstaat en controledocumentatie aanwezig is. Voor de benodigde controledocumentatie (het balansdossier) leveren wij een lijst 'met op te leveren stukken' aan, inclusief deadlines voor de aanlevering van de documentatie.
Deelwaarnemingen en gegevensgerichte werkzaamheden	Voor aanvang van de jaareinde controle zullen wij de belangrijkste deelwaarnemingen uitzetten. Hiervoor is het noodzakelijk dat u tijdig de administratie(s) afsluit en de auditfile(s) aan het controleteam verstrekt. Het vooraf uitzetten van onze selecties heeft als bijkomend voordeel dat uw medewerkers de benodigde controle documentatie op een door hun gekozen moment (voor aanvang van de controle) kunnen verzamelen.
Kwaliteit van cruciaal belang	Voor een efficiënte controle en korte doorlooptijd is van cruciaal belang om een interne kwaliteitscheck uit te voeren op de door uw medewerkers aangeleverde stukken. Dit voorkomt onnodige vragen en uitzoekwerk gedurende de jaarrekeningcontrole.
Onze verwachtingen	Om een kwalitatief goede en efficiënte controle uit te voeren verwachten wij van u: - Complexe vraagstukken worden vooraf met ons afgestemd op basis van uw eigen standpunt; - Tijdige aanlevering van de (volledige) jaarrekening inclusief rechtmatigheidsverantwoording aansluitend met uw administratie; - Maximaal twee versies van de jaarrekening (concept en definitief); - Tijdige en volledige aanlevering van het balansdossier volgens de op te leveren stukkenlijst; - Uw medewerkers zijn voldoende beschikbaar om vragen (tijdig) te beantwoorden; - Na het opmaken van de jaarrekening wordt niet meer geboekt in de administratie van het te controleren boekjaar.

4. Actualiteiten

4. Actualiteiten

4.1 Aankomende wetswijzigingen in BBV en Bado

Afgelopen zomer heeft het Rijk enkele wijzigingen op het Besluit Begroting en Verantwoording provincies en gemeenten (BBV) en het Besluit Accountantscontrole Decentrale Overheden (Bado) voorgesteld. Samenvattend zijn de belangrijkste voorgestelde wijzigingen opgenomen:

Aanpassing Bado

Met ingang van mogelijk 2025 veranderen de goedkeurings-toleranties voor de jaarrekeningcontrole. Voorheen werd voor fouten uitgegaan van 1% van de totale lasten inclusief dotaties aan de reserves en voor onzekerheden 3%. Vanaf 2025 worden fouten en onzekerheden samengevoegd en wordt de goedkeuringsgrens gesteld op 2% van de totale lasten (dus zonder toevoeging reserves). Deze wijziging kan een belangrijke impact hebben. Wij adviseren u te evalueren wat dit voor uw situatie betekent en welke stappen gezet dienen te worden ter waarborging dat de fouten en onzekerheden binnen de goedkeuringstoleranties blijven vanaf 2025.

Ten aanzien van de SISa-bijlage houdt de accountant de verantwoordelijkheid om ook de rechtmatigheid vast te stellen.

De volgende tabel zal gehanteerd worden t.b.v. het oordeel:

Materialiteit	Goedkeurende verklaring	Verklaring met beperking	Verklaring van oordeelonthouding /afkeurende verklaring
Fouten in de jaarrekening en onzekerheden in de controle	≤2%	>2% - ≤4%	> 4%

Controleverklaring bij de jaarrekening

Vanuit onze beroepsvereniging NBA is aangegeven dat in het BBV duidelijkheid moet worden gegeven over de publicatie van de controleverklaring in de jaarstukken van decentrale overheden. In het BBV is nu niet opgenomen dat deze verklaring onlosmakelijk deel uitmaakt van de jaarrekening en dat noch de definitieve jaarrekening en / of de jaarstukken noch de controleverklaring separaat gepubliceerd mogen worden. Hierdoor komt het voor dat jaarstukken van decentrale overheden worden gepubliceerd zonder de daarbij afgegeven controleverklaring.

Het is in het publiek belang dat de jaarstukken altijd met inbegrip van de controleverklaring toegankelijk worden voor het maatschappelijk verkeer, zoals raadsleden, burgers en andere belanghebbenden. Om dit te borgen heeft onze beroepsvereniging suggesties opgenomen ter aanpassing van artikel 24 lid 3 van het BBV, door daarin 'overige gegevens' toe te voegen waarin de controleverklaring wordt opgenomen.

Wij adviseren u om vooruitlopend op deze aanpassing deze werkwijze alvast toe te passen voor de jaarrekening 2023.

4. Actualiteiten

4.1 Aankomende wetswijzigingen in BBV en Bado

Afgelopen zomer heeft het Rijk enkele wijzigingen op het Besluit Begroting en Verantwoording provincies en gemeenten (BBV) en het Besluit Accountantscontrole Decentrale Overheden (Bado) voorgesteld. Samenvattend zijn de belangrijkste voorgestelde wijzigingen opgenomen:

Uitbreiding inhoud jaarrekening

De voorgeschreven inhoud van de jaarrekening wordt uitgebreid met de rechtmatigheidsverantwoording. Hiermee bestaat de jaarrekening uit:

- het overzicht van baten en lasten in de jaarrekening en de toelichting;
- de balans en de toelichting;
- de rechtmatigheidsverantwoording;
- de bijlage met de verantwoordingsinformatie over specifieke uitkeringen;
- een bijlage met het overzicht van de gerealiseerde baten en lasten per taakveld.

De volgende eisen worden gesteld aan de rechtmatigheidsverantwoording:

1. In de jaarrekening is een rechtmatigheidsverantwoording opgenomen, met inachtneming van de verantwoordingsgrens.
2. De rechtmatigheidsverantwoording bevat een toelichting op de rechtmatige totstandkoming van de baten, lasten en balansmutaties.
3. De gemeenteraad en provinciale staten stellen de verantwoordingsgrens vast. De verantwoordingsgrens valt binnen 0 tot 3% van de totale lasten, exclusief de dotaties aan de reserves.
4. Indien het eindbedrag hoger is dan de verantwoordingsgrens licht het college van burgemeesters en wethouders of gedeputeerde staten deze afwijking toe in de rechtmatigheidsverantwoording.

De commissie BBV stelt een modeltekst voor de rechtmatigheidsverantwoording op.

Notitie Overhead

De Notitie Overhead van de commissie BBV is in het voorjaar 2023 geactualiseerd en ter consultatie gepubliceerd. Ten opzichte van de notitie overhead 2016 is een belangrijke aanpassing de definitie van het begrip overhead zelf. Deze wordt als volgt gedefinieerd:

“Het geheel van functies gericht op de sturing en ondersteuning van de medewerkers in het primaire proces. Hiertoe behoren ook de systemen en aanverwante lasten die deze functies ondersteunen.”

Daarnaast doet de commissie BBV de volgende stellige uitspraken, welke overigens al bestonden.

- De methodiek voor het toerekenen van overhead, zoals opgenomen in het overzicht overhead, aan lokale heffingen en rechten mag niet afwijken van de overige methodieken voor het toerekenen van overhead aan gemeentelijke taakvelden.
- Bij de berekening van de tarieven voor lokale heffingen moet de methodiek voor de toerekening van overhead worden opgenomen in de financiële verordening.

Ook zijn er voorbeelden toegevoegd die antwoord geven op actuele vraagstukken. De notitie treedt na publicatie naar verwachting in werking vanaf begrotingsjaar 2025.

4. Actualiteiten

4.1 Aankomende wetswijzigingen in BBV en Bado

Afgelopen zomer heeft het Rijk enkele wijzigingen op het Besluit Begroting en Verantwoording provincies en gemeenten (BBV) en het Besluit Accountantscontrole Decentrale Overheden (Bado) voorgesteld. Samenvattend zijn de belangrijkste voorgestelde wijzigingen opgenomen:

Paragraaf Openbaarheid

Paragraaf Openbaarheid moet ten minste inzicht verschaffen in:

- a. de informatie die op grond van de artikelen 3.1, 3.3 en hoofdstuk 4 van de Wet open overheid openbaar is gemaakt;
- b. de informatiehuishouding;
- c. het aanwijzen en in dienst hebben van een contactpersoon als bedoeld in artikel 4.7 van de Wet open overheid;
- d. de besteding van subsidie voor de uitvoering van de Wet open overheid;
- e. de eventuele andere activiteiten benodigd ter uitvoering van de Wet open overheid;

De op grond van artikel 3.3, eerste en tweede lid, van de Wet open overheid openbaar gemaakte informatie bevat per categorie van informatie ten minste:

- a. op grond van welk artikel van de Wet open overheid de informatie openbaar is gemaakt;
- b. het jaar waarin de openbaarmaking van de informatie naar verwachting verplicht is;
- c. een omschrijving van de verstrekte informatie;
- d. het aantal documenten dat openbaar is gemaakt;
- e. het platform waarop de documenten openbaar zijn gemaakt.

Het inzicht in de besteding van de subsidie bedoeld in het eerste lid, onderdeel d, bevat ten minste een omschrijving van de wijze waarop de subsidie is besteed.

Paragraaf Bedrijfsvoering

Daarnaast worden de eisen t.a.v. de paragraaf bedrijfsvoering worden uitgebreid. Tot en met 2023 is de eis:

“De paragraaf betreffende de bedrijfsvoering geeft ten minste inzicht in de stand van zaken en de beleidsvoornemens ten aanzien van de bedrijfsvoering.”

Na goedkeuring van de voorgestelde wijziging verlangt de wetgever de volgende toelichting in deze paragraaf:

De paragraaf betreffende de bedrijfsvoering bevat ten minste:

- a. De stand van zaken van de bedrijfsvoering;
- b. De beleidsvoornemens ten aanzien van de bedrijfsvoering;
- c. Informatie over de financiële rechtmatigheid;
- d. Welke actie wordt ondernomen om afwijkingen van de financiële rechtmatigheid te voorkomen.

4. Informatieveiligheid

4.2 Is uw gemeente klaar voor de verplichte IT audits die wij in de publieke sector verwachten?

Binnen de publieke sector is informatieveiligheid een hot topic. Gemeenten halen regelmatig negatief het nieuws vanwege incidenten met betrekking tot informatieveiligheid, zoals hacks, CEO-fraude en datalekken. De komende jaren treden verschillende nieuwe wetten op het gebied van informatieveiligheid in werking waar ook uw gemeente mee te maken krijgt.

Van gemeentelijke colleges wordt verwacht dat de ambtelijke organisatie wordt gefaciliteerd bij de implementatie van deze richtlijnen en wetten. Doel van deze wetten en richtlijnen is dat uw gemeente weerbaarder wordt op het gebied van informatieveiligheid. Daarnaast zal de toezichthoudende rol van de gemeenteraad op het dossier informatieveiligheid ook worden uitgebreid. Verder is het onze verwachting dat de auditlast in relatie tot nu al verplichte IT-audits zal toenemen en dat nieuwe IT-audits hun opwachting zullen maken.

Wij adviseren u, in overleg met GR de Bevelanden, in beeld te brengen in hoeverre deze ontwikkelingen voor uw ambtelijke organisatie zijn gefaciliteerd en op basis daarvan vervolgstappen te nemen.

Huidige situatie

Jaarlijks legt het college middels de **ENSIA** collegeverklaring onder andere verantwoording af over informatieveiligheid ten aanzien van DigiD en Suwinet. Van gemeenten wordt verwacht dat ieder jaar een interne audit **Wpg** (Wet Politiegegevens) wordt uitgevoerd. Eén keer in de vier jaar wordt een externe Wpg-audit uitgevoerd.

Vanaf 2024 – wijzigingen ENSIA

Tot op heden is de diepgang van de jaarlijkse **ENSIA-audit** beperkt tot 'opzet' en 'bestaan' (beleid en implementatie van het beleid middels beheersingsmaatregelen). Vanaf 2024 wordt op een aantal onderdelen ook 'werking' van beheersingsmaatregelen getoetst in de jaarlijkse ENSIA-audit. Dit vraagt van uw organisatie dat beheersingsmaatregelen gedurende het jaar consequent en aantoonbaar worden uitgevoerd.

Vanaf 2026 – Wet Digitale Overheid

Vanaf 2026 is ook de tweede tranche van de **Wet Digitale Overheid** van toepassing. Dit deel van de wet vraagt van organisaties dat de governance rondom de verschillende basisregistraties en het delen van persoonsgegevens op orde is.

Vanaf 2023 – Wet Digitale Overheid

Met ingang van 2023 treedt het eerste deel (eerste tranche) van de **Wet Digitale Overheid** (WDO) in werking. De Wet Digitale Overheid is gebaseerd op de Europese eIDAS-richtlijn en regelt dat burgers veilig kunnen inloggen bij de overheid. Vanaf 2023 is het gebruik van HTTPS en HSTS verplicht. HTTPS configuraties dienen daarnaast te voldoen aan de laatste TLS-richtlijnen.

Vanaf 2024 – NIS2-richtlijn

Naar verwachting is vanaf eind 2024 de Europese **NIS2-richtlijn** (Network and Information Security Directive) van toepassing. De verwachting is dat de Baseline Informatiebeveiliging Overheid wordt uitgebreid met een aantal verplichte elementen. Vanuit de NIS2-richtlijn heeft uw organisatie een **zorgplicht** en **meldplicht** ten aanzien van informatieveiligheid. Daarnaast zal een toezichthouder **toezicht** houden op naleving van de NIS2-richtlijn middels (externe) IT-audits.

Bijlagen

Bijlage 1: Detailbevindingen

Detailbevindingen interne beheersing - Bevindingen per proces

Hierna zijn de detailbevindingen en aanbevelingen ten aanzien van de belangrijkste processen opgenomen.

Per pagina is een bevinding opgenomen met daarbij het risico en de aanbeveling. Bij elke bevinding staat het jaar van de eerste vermelding aangegeven evenals de geschatte kans van voorkomen en impact op uw organisatie.

Per bevinding geven wij aan welke alternatieve werkzaamheden wij zullen uitvoeren om het geconstateerde risico (gegevensgericht) te ondervangen.

Per bevinding verzoeken wij de gemeente om commentaar te geven.

Aan het eind van dit hoofdstuk geven wij (voor zover van toepassing) voor bestaande bevindingen een update van de status van deze bevinding in het huidige boekjaar.

Constatering

In dit blok wordt aangegeven wat gedurende de accountantscontrole is geconstateerd en waarvan wij u graag op de hoogte willen brengen.



Applicatie

Relevante IT systemen

Bevinding	TITEL BEVINDING	Kans: Hoog/midden/laag
Jaar van constatering	Boekjaar eerste vermelding	Impact: Hoog/midden/laag
Status bevinding:	Mate waarin door de organisatie opvolging is gegeven aan de constatering	
 Risico	Hierbij geven wij aan wat de risico's zijn van de bevinding en wat de gevolgen voor de gemeente Goes kunnen zijn.	
 Aanbeveling	Hier geven wij u aanbevelingen met betrekking tot de bevinding. Deze aanbeveling is een mogelijke oplossing voor de bevinding.	
 Gevolgen jaarrekening-controle	Hier geven wij een update van de bevinding wanneer deze in een eerde boekjaar is geconstateerd. Tevens kan de bevinding gevolgen hebben voor de controleaanpak en de omvang van onze controlewerkzaamheden. Op deze plaats maken wij hier eveneens vermelding van.	
 Management commentaar	Na het bespreken van de concept managementletter krijgt u de mogelijkheid om hier uw commentaar op geven.	

Bijlage 1: Detailbevindingen

1. Geen (actuele) procesbeschrijvingen

Bevinding Wij constateren dat de gemeente Goes geen (actuele) procesbeschrijvingen heeft. De gemeente heeft software (Engage) aangeschaft om procesbeschrijvingen op te stellen en vast te leggen. Echter, heeft dit nog niet geleid tot afgeronde procesbeschrijvingen, behoudens voor het proces van grondverkoop in boekjaar 2022. Update 2023 Gemeente Goes heeft in 2023 een concept procesbeschrijving opgesteld voor het proces inkopen en aanbestedingen. Daarmee heeft de gemeente stappen ondernomen ten aanzien van deze bevinding. Echter zijn er voor de overige belangrijke processen nog geen procesbeschrijvingen opgesteld. We hebben vernomen dat verdere opvolging hiervan in 2024 zal plaatsvinden.  - Niet van toepassing Applicatie(s)	Bevinding Geen (actuele) procesbeschrijvingen Kans: Laag
	Jaar van constatering 2017 Impact: Laag
	 Risico Het risico bestaat dat processen en interne beheersmaatregelen niet op een eenduidige wijze worden uitgevoerd of dat de aanwezige procesbeschrijvingen niet meer aansluiten bij de huidige situatie.
	 Aanbeveling Wij adviseren het college om procesbeschrijvingen op te stellen voor de belangrijkste controleprocessen binnen de gemeente Goes. Daarbij is het van belang dat (1) een gedetailleerde beschrijving is opgenomen van de interne beheersmaatregelen en (2) ingegaan wordt op de (financiële) verwerking van de processtappen. Wij adviseren daarbij om de belangrijkste interne beheersmaatregelen (key-controls) uit te werken aan de hand van de 6W's (wie, wat, waarom, wanneer, met welke informatie en wat wordt vastgelegd), zodat iedere betrokken functionaris weet wat er van hem of haar verwacht wordt. Daarnaast adviseren we om belangrijke processtappen periodiek te blijven toetsen, zodat de opzet van de processen continue getoetst wordt. Dit advies is ter beheersing en naleving van de voorgeschreven procedures/procesbeschrijvingen, maar ook om op termijn meer systeemgericht te kunnen controleren.
 Gevolgen voor de jaarrekening-controle Niet van toepassing.	

Bijlage 1: Detailbevindingen

2. Onderbouwing prestatielevering

Bevinding

De functiescheiding tussen prestatieakkoord verklaarder en de budgethouder is sinds dit boekjaar geborgd in het nieuwe financiële pakket Key2Finance. Deze functiescheiding is zichtbaar in een workflow. We hebben daarbij wel geconstateerd dat enkele medewerkers met te ruime applicatiebeheerrechten de systeeminstelling omtrent functiescheiding kunnen uitzetten. Deze mogelijke handeling wordt niet gelogd, waardoor deze actie niet traceerbaar is.

We constateren verder dat er geen eenduidige vastlegging (inclusief brondocumentatie) aanwezig is van de prestatielevering in de financiële applicatie. Hierdoor is op basis van de informatie uit het systeem niet duidelijk op basis waarvan de prestatielevering is vastgesteld.

Update 2023

In boekjaar 2023 heeft de gemeente Goes een notitie prestatielevering opgesteld, waarin onder andere staat dat voor inkopen vanaf € 1.000 in beginsel de overwegingen / documentatie omtrent de prestatielevering vastgelegd moeten worden in het financiële pakket. Uit verkregen inlichtingen blijkt dat deze interne regelgeving per 01-01-2024 zal gaan gelden.



- Centric Key2Financiën

Applicatie(s)

Bevinding	Onderbouwing prestatielevering	Kans:	Midden
Jaar van constatering	2017	Impact:	Midden
 Risico	Indien de prestatieverklaring onvoldoende gedocumenteerd is, kan niet worden aangetoond dat een betaling getrouw en rechtmatig plaatsvindt. Dit kan resulteren in een onzekerheid voor zowel getrouwheid als rechtmatigheid. Tevens levert dit een verhoogd beheersings- en mogelijk frauderisico binnen uw organisatie op.		
 Aanbeveling	Wij adviseren u om maatregelen te nemen om te voorkomen dat de systeeminstelling omtrent functiescheiding kan worden uitgezet. Indien dit niet mogelijk is, adviseren we periodiek te controleren of de systeeminstelling omtrent functiescheiding (tijdelijk) is uitgezet. We adviseren verder om de vastlegging van de prestatielevering systeemtechnisch te borgen. Een andere mogelijkheid is het monitoren van de naleving van de richtlijnen. Indien geconstateerd wordt dat procesafspraken niet nageleefd worden, dient de gemeente aanvullende aandacht te besteden aan gedrag en cultuur binnen de organisatie (softcontrols).		
 Gevolgen voor de jaarrekening-controle	Met betrekking tot de eindejaarscontrole vragen wij u om inzichtelijk te maken dat de prestatie-akkoordverklaring (PAV) is vastgelegd voor alle inkoopfacturen. We vragen u een uitzonderingenlijst op te stellen, en op basis daarvan (in overleg) aanvullende werkzaamheden te verrichten op facturen zonder PAV. Verder is het noodzakelijk dat voor de door ons geselecteerde facturen de prestatielevering aangetoond kan worden door gemeente Goes.		

Bijlage 1: Detailbevindingen

3. Geen zichtbare interne beheersing (4-ogen principe) bij start inkoop- en aanbestedingsproces

Bevinding

Alvorens een inkoop plaatsvindt, wordt een inschatting gemaakt van de omvang van de inkoop. Op basis van deze inschatting wordt een te volgen aanbestedingsprocedure bepaald. Hiervoor dient een inkoopformulier voor rechtmatigheid te worden ingevuld door de medewerker die de inkoop verricht. Deze verplichting geldt voor opdrachtwaarden vanaf € 30.000 voor diensten en leveringen en vanaf € 50.000 voor werken.

Het formulier dient te worden toegevoegd aan het inkoopdossier. Er vindt nog geen structurele zichtbare controle plaats op het inkoopformulier voordat de bestelling geplaatst wordt. Tevens is niet geborgd dat voor elke inkoop een inkoopformulier wordt gebruikt.

Update 2023

Uit verkregen inlichtingen blijkt dat het proces niet gewijzigd is in boekjaar 2023. We hebben vernomen dat de gemeente met de toekomstige invoering van een verplichtingenadministratie en het investeren in contractbeheersing het risico op onrechtmatige aanbestedingen wilt mitigeren.



Applicatie(s)

- Niet van toepassing

Bevinding	Geen zichtbare interne beheersing (4-ogen principe) bij start inkoop- en aanbestedingsproces	Kans: Laag
Jaar van constatering	2015	Impact: Midden
Risico	Het risico van het niet naleven van het vastgestelde inkoop- en aanbestedingsbeleid is dat inkopen en aanbestedingen op andere wijze plaatsvinden dan wenselijk of wellicht noodzakelijk is. Dit leidt vervolgens tot een risico op rechtmatigheidsfouten.	
Aanbeveling	Wij adviseren u een zichtbaar vier-ogen principe toe te passen bij de start van het inkoop- en aanbestedingsproces. Daarnaast adviseren we u middels periodieke interne controles het juiste en volledige gebruik van het inkoopformulier te blijven monitoren, tot het moment dat nieuwe beheersmaatregelen het onderkende risico afdekken.	
Gevolgen voor de jaarrekening-controle	Wij zetten in samenspraak met de gemeente door middel van een statistische steekproef werkzaamheden op om achteraf vast te stellen dat de aanbestedingen rechtmatig hebben plaatsgevonden.	

Bijlage 1: Detailbevindingen

4. Contractenregister is onvolledig

Bevinding

We hebben vernomen dat de volledigheid van het contractenregister nog niet geborgd is. Wel hebben we vernomen dat inkoopadvies bezig is om het contractregister volledig te krijgen, onder andere door het uitvragen van informatie bij afdelingen.

Daarnaast hebben we vernomen dat inkoopadvies periodiek contact heeft de interne controle afdeling omtrent de volledigheid van het contractenregister.

Verder hebben we vernomen dat het contractenregister in de module beperkt is geworden qua functies, waardoor de gemeente een minder goed inzicht heeft in haar contracten en openstaande verplichtingen.

Update 2023

De gemeente heeft in 2023 een contractenregister-taskforce opgericht. We hebben verder vernomen dat er een plan van aanpak is opgesteld en gesprekken in de organisatie worden gehouden om contractbeheersing te vergroten. Het effect hiervan zal in de komende jaren tot uiting komen.



Applicatie(s)

- Niet van toepassing

Bevinding	Contractenregister is onvolledig	Kans:	Midden
Jaar van constatering	2018	Impact:	Midden
 Risico	Het ontbreken van adequaat werkende procedures rondom de continue (centrale) volledigheid van het contractmanagementsysteem leidt tot het risico dat de inkopen niet conform de geldende wet- en regelgeving worden aanbesteed. Ten aanzien van de jaarrekening bestaat het risico dat de door de gemeente aangegane verplichtingen per balansdatum niet volledig zijn opgenomen dan wel zijn toegelicht in de jaarrekening.		
 Aanbeveling	Wij adviseren u procedures en richtlijnen in te stellen die de (continue) volledigheid van het contractmanagementsysteem waarborgen.		
 Gevolgen voor de jaarrekening-controle	In het kader van de jaarrekening 2023 is het van belang om de totale verplichtingen uit contracten in kaart te brengen en te verantwoorden als kortlopende verplichting of als niet uit de balans blijkende verplichtingen. Ten aanzien van aanbestedingsrechtmatigheid dient de gemeente door middel van een statistische steekproef werkzaamheden uit te voeren om achteraf vast te stellen dat de aanbestedingen rechtmatig hebben plaatsgevonden.		

Bijlage 1: Detailbevindingen

5. Verplichtingenadministratie is niet aanwezig

Bevinding

Wij hebben geconstateerd dat binnen de gemeente Goes geen verplichtingenadministratie aanwezig is. Hierdoor heeft de gemeente geen actueel beeld van aangegane verplichtingen, wat de budgetbewaking bemoeilijkt.

Update 2023

We hebben geconstateerd dat er ten aanzien van deze bevinding geen wijzigingen zijn doorgevoerd in boekjaar 2023.

De gemeente verwacht de verplichtingenadministratie in komende boekjaren te implementeren binnen het inkoopproces. Daarbij hebben we vernomen dat het onderzoek naar de (inrichting van de) verplichtingenadministratie nog plaats dient te vinden.



Applicatie(s)

- Niet van toepassing

Bevinding	Verplichtingenadministratie is niet aanwezig	Kans:	Midden
Jaar van constatering	2018	Impact:	Midden
 Risico	Met betrekking tot het ontbreken van een verplichtingenadministratie bestaat het risico dat de budgethouders geen volledig inzicht hebben in de stand van hun restantbudgetten. Dit kan leiden tot ongeautoriseerde budgetoverschrijdingen. Ten aanzien van de jaarrekening bestaat het risico dat verplichtingen en schulden per balansdatum niet volledig zijn opgenomen.		
 Aanbeveling	Wij adviseren u gebruik te maken van een verplichtingadministratie.		
 Gevolgen voor de jaarrekeningcontrole	In het kader van de jaarrekening 2023 verzoeken wij u (in overleg) een voortgezette controle uit te voeren om de volledigheid van de verplichtingen per 31 december 2023 vast te stellen.		

Bijlage 1: Detailbevindingen

6. Aanbestedingsproces wordt niet structureel eenduidig uitgevoerd en vastgelegd

Bevinding

Uit de uitgevoerde (interne) controles in de afgelopen jaren kwamen relatief veel formele rechtmatigheidsfouten en enkele financiële rechtmatigheidsfouten. De fouten worden met name veroorzaakt doordat het aanbestedingsproces decentraal wordt uitgevoerd en vastgelegd. Daarbij bestaat er geen centraal overzicht waaruit blijkt dat alle aanbestedingen via TenderNed worden behandeld.

Wel hebben we van de interne controle afdeling vernomen dat er in de afgelopen jaren een verbetering waarneembaar is binnen het aanbestedingsproces. Afwijkingen van het interne inkoop- en aanbestedingsbeleid dienen voorzien te zijn van een advies van een inkoopadviseur en er is sprake van gestandaardiseerde dossiervorming.

Update 2023

Bij onze jaarrekeningcontrole 2022 constateerden we dat voor € 2,4 miljoen aan inkopen het gemeentelijke inkoop- en aanbestedingsproces niet was gevolgd. Daarnaast constateerden we € 0,3 miljoen aan financiële rechtmatigheidsfouten.

Vanuit verkregen inlichtingen hebben we vernomen dat ten aanzien van het aanbestedingsproces een verbetering gemaakt is, mede door het oprichten van een taskforce hieromtrent. Het aanbestedingsproces is echter in boekjaar 2023 nog niet getoetst door middel van (interne) controles, waardoor we de resultaten van de ondernomen acties nog niet kunnen vaststellen.



Applicatie(s)

- Niet van toepassing

Bevinding	Aanbestedingsproces wordt niet structureel eenduidig uitgevoerd en vastgelegd	Kans: Hoog
Jaar van constatering	2019	Impact: Midden
 Risico	Het risico bestaat dat de aanbestedingen niet voldoen aan de interne en externe wet- en regelgeving. Dit leidt vervolgens tot een risico op rechtmatigheidsfouten.	
 Aanbeveling	We adviseren om het aanbestedingsproces verder te formaliseren. Daarbij is het van belang om, in het verlengde van de opgestelde procesbeschrijving, de belangrijkste interne beheersmaatregelen (key-controls) verder uit te werken.	
	Verder adviseren we om naleving van inkoopprocedures (waaronder het hanteren van de gestandaardiseerde dossiervorming) periodiek te (blijven) toetsen om vast te stellen of ingevoerde procedures nageleefd worden.	
	Daarnaast adviseren we om de zichtbare betrokkenheid van inkoopadviseurs structureel te borgen.	
 Gevolgen voor de jaarrekeningcontrole	Ten aanzien van aanbestedingsrechtmatigheid dient de gemeente door middel van een statistische steekproef werkzaamheden uit te voeren om achteraf vast te stellen dat de aanbestedingen rechtmatig hebben plaatsgevonden.	

Bijlage 1: Detailbevindingen

7. Rechtmatigheidsfouten in subsidieproces

Bevinding

In de afgelopen boekjaren zijn interne controles verricht op de subsidieverstrekkings. Hieruit kwam een relatief groot aantal formele rechtmatigheidsfouten. Deze fouten hebben geen invloed gehad op onze controleverklaring.

Daarnaast stellen we vast dat, conform vorig jaar, sprake kan zijn van financiële rechtmatigheidsfouten ten aanzien van het reservecriterium zoals opgenomen in de subsidieverordening. Er is voor boekjaar 2023 nog geen gebruik gemaakt van de hardheidsclausule. Indien de subsidieaanvrager beschikt over reserves die gezamenlijk meer bedragen dan 5% van de ingediende exploitatiebegroting, dan is er sprake van een weigeringsgrond. Hierop wordt door de gemeente niet structureel getoetst.

Daarnaast hebben we vastgesteld dat aanvraagformulieren en checklists voor subsidies slechts in beperkte mate worden gehanteerd. Ook worden subsidiebelastingen niet structureel op de juiste kostensoort verantwoord.

Verder merken we op dat het jaarlijkse subsidieregister niet in het primaire proces wordt bijgehouden maar achteraf wordt opgesteld. We adviseren om het gebruik van het subsidieregister in het primaire proces te borgen.

Update 2023

We hebben vernomen dat er een taskforce is opgericht, er voorlichtingssessies zijn gehouden, er een extern onderzoek heeft plaatsgevonden en dat het verdere instrumentarium (zoals formulieren) is verbeterd om de interne beheersing ten aanzien van subsidieverstrekkings te verbeteren. De effecten van deze maatregelen zullen naar verwachting vanaf 2024 zichtbaar worden.

Daarnaast hebben we geconstateerd dat er in september 2023 een nieuwe subsidieverordening is vastgesteld waarin de uitsluitingsgrond 'reservecriterium' aangepast is. Deze verordening treedt vanaf boekjaar 2024 in werking. Daarbij hebben we vastgesteld dat er tevens een beleidsnotitie m.b.t. het reservecriterium is vastgesteld.



Applicatie(s)

- Niet van toepassing

Bevinding	Rechtmatigheidsfouten in subsidieproces	Kans:	Midden
Jaar van constatering	2018	Impact:	Midden
 Risico	Het risico bestaat dat de organisatie niet handelt conform de interne richtlijnen en procedures, waardoor het risico bestaat op formele en financiële rechtmatigheidsfouten.		
 Aanbeveling	Wij adviseren u om voor het einde van 2023 beargumenteerd een collegebesluit te nemen omtrent het niet toepassen van de uitsluitingsgrond 'reservecriterium', zoals opgenomen in de subsidieverordening. Tevens adviseren we u de genoemde aanbevelingen omtrent het subsidieproces uit eerdere interne controle rapporten op te volgen. We adviseren daarnaast het gebruik van het subsidieregister binnen het primaire proces te borgen, zodat deze continue up-to-date is. Op die manier bestaat er een centraal overzicht van subsidieaanvragen, waardoor het proces beheersbaarder wordt en rechtmatigheidsfouten kunnen worden voorkomen.		
 Gevolgen voor de jaarrekening-controle	Als het college tijdig en gemotiveerd besluit waarom geen gebruik is gemaakt van de uitsluitingsgrond 'reservecriterium', dan tellen de betreffende lasten niet mee als financiële rechtmatigheidsfouten.		

Bijlage 1: Detailbevindingen

8. Tussentijdse aanbestedingsanalyse

Bevinding

We hebben geconstateerd dat de gemeente geen tussentijdse aanbestedingsanalyse heeft uitgevoerd.

Update 2023

We constateren geen wijzigingen ten opzichte van boekjaar 2022.

Bevinding

Tussentijdse aanbestedingsanalyse

Kans:

Midden

Jaar van constatering

2022

Impact:

Midden



Risico

Het risico bestaat dat inkopen niet op de juiste wijze worden aanbesteed, hetgeen leidt tot rechtmatigheidsfouten in het aanbestedingsproces.



Aanbeveling

We adviseren de gemeente om periodiek een tussentijdse aanbestedingsanalyse uit te laten voeren door een inkoopadviseur. Op die manier kan de gemeente risicogericht eventuele naderende rechtmatigheidsfouten tijdig signaleren en hierop inspelen.



Gevolgen voor de jaarrekening-controle

Wij zetten in samenspraak met de gemeente door middel van een statistische steekproef werkzaamheden op om achteraf vast te stellen dat de aanbestedingen rechtmatig hebben plaatsgevonden.



Applicatie(s)

- Niet van toepassing

Bijlage 2: IT-bevindingen

Detailbevindingen interne beheersing - IT General Controls

IT General Controls

Veel handelingen die binnen organisaties plaatsvinden, worden geregistreerd door middel van automatisering. Daarbij zijn diverse interne beheersingsmaatregelen steeds vaker geautomatiseerd in softwarepakketten. Wij onderzoeken daarom de beheersing van uw IT-omgeving en rapporteren daarover in deze managementletter.

Op basis van de door ons uitgevoerde werkzaamheden hebben wij onze inschatting van de kwaliteit van uw IT-systeem en/of applicaties opgenomen. Hierbij hebben wij de volgende onderverdeling gemaakt om de kwaliteit weer te geven:

-  Benodigd, verbetering op (korte) termijn
-  Adviespunt, verdere aanscherping mogelijk
-  Op dit moment voldoende

Bij het uitvoeren van onze werkzaamheden hebben wij gekeken naar de algemene onderwerpen rondom de beheersing van uw IT-omgeving, zoals in de tabel rechts opgenomen. Op de navolgende pagina's zullen wij onze bevindingen rapporteren.

Onderwerp



Toegangs-beveiliging

Bij het toetsen van 'toegangsbeveiliging' wordt onderzocht of de inrichting van de IT-omgeving de authenticiteit van de gebruiker van een gebruikersaccount borgt. Vervolgens onderzoeken wij de mogelijkheden voor het 'steunen' op autorisaties en de processen rondom het verstrekken, muteren en ontnemen van autorisaties binnen de omgeving. Wanneer de randvoorwaarden hiervoor voldoende aanwezig zijn, kunnen wij in de controle gebruikmaken van ingerichte functiescheiding in het systeem. Een adequate inrichting kan preventief risico's voor uw organisaties beperken en tegelijkertijd efficiencyvoordelen opleveren in de controle.



Wijzigings-beheer

Bij het toetsen van 'wijzigingsbeheer' ofwel change management wordt vastgesteld dat wijzigingen aan de applicatie op gestructureerde en gecontroleerde wijze worden doorgevoerd. Voor uw organisatie heeft wijzigingsbeheer ten doel om te voorkomen dat applicaties zich niet gedragen zoals u verwacht na een wijziging in de software, resulterend in, wellicht niet opgemerkte, (financiële) gevolgen.



Continuïteits-maatregelen en beveiliging

Onder de noemer continuïteit en beveiliging krijgen wij inzicht in uw beheersing van risico's gericht op continuïteit van uw bedrijfsvoering. Hierbij kan discontinuïteit worden veroorzaakt door menselijk of technisch falen, maar ook door interne of externe kwaadwillenden. Voor continuïteit zijn met name het punt in de tijd tot waar u gegevens bij discontinuïteit kunt herstellen en de tijd die het kost om tot een normale bedrijfsvoering te komen bij discontinuïteit van belang. Hiernaast schatten wij uw beheersing van cyber risico's in.



Adviespunten zonder directe impact

Het is voor ons van belang om inzicht te krijgen in de verantwoordelijkheden die binnen de organisatie zijn ingericht – of met andere organisaties overeen zijn gekomen (uitbesteding) – ten aanzien van de beheersing van de IT-omgeving. Hierbij kijken wij naar beleidsstukken ten aanzien van IT-strategie, beveiliging en functiescheiding. Ook de interne beheersingsmaatregelen die al dan niet zijn ingericht binnen de IT-omgevingen zijn onderdeel van onze scope. Indien maatregelen periodiek worden uitgevoerd, kunnen wij hier gebruik van maken in de jaarrekeningcontrole. Deze adviespunten hebben niet een directe impact op onze controlewerkzaamheden, maar zijn wel wenselijk.

Bijlage 2: IT-bevindingen

Detailbevindingen interne beheersing - Toegangsbeveiliging Netwerk

2022	Authenticatie	Autorisatie	2023	Authenticatie	Autorisatie
	  	  		  	  

	Authenticatie	Autorisatie
 Bevinding	Gebruikers worden uniek geïdentificeerd. De wachtwoordinstellingen zijn van voldoende niveau. Systeemtechnisch wordt geen lock-out (timer) afgedwongen. Daarnaast zijn er 454 gebruikers in het netwerk voor gemeente Goes aanwezig die zijn uitgezonderd van het periodiek wijzigen van wachtwoorden. Deze tekortkomingen worden echter gecompenseerd door het feit dat een extra factor bij inloggen (multi factor) wordt afgedwongen voor toegang tot het netwerk. Daarmee is authenticatie op orde.	De hoge rechten in de Windows Active Directory zijn beperkt tot onafhankelijke functionarissen. Er zijn echter geen procedures beschreven voor o.a. het muteren van gebruikers en rechten aan de hand van een functie-autorisatiematrix. Daarnaast vindt er ook geen periodieke controle plaats op de gebruikers en rechten op het netwerk.
 Risico	Door het ontbreken van een lock-out (timer) is de kans aanwezig dat als kwaad willenden de MFA omzeilen ze daarna relatief eenvoudig via een zogenaamde "Brute-force attack" toegang proberen te krijgen tot een gebruikersaccount. Een lock-out (timer) voorkomt dit door het account na een bepaald aantal pogingen of een bepaalde periode tijdelijk te blokkeren.	Het risico bestaat dat bij toekenningen van autorisaties verkeerde rechten worden toegekend of rechten te lang open blijven staan. Hierdoor kunnen gebruikers mogelijk meer dan volgens de functie benodigd is. Wegens het ontbreken van een controle hierop is de kans aanwezig dat deze autorisaties niet gecorrigeerd worden.
 Aanbeveling	Wij adviseren om systeemtechnisch een lock-out (timer) in te schakelen.	Wij adviseren om een functie-autorisatiematrix te creëren welke als leidraad dient voor het toekennen van autorisaties en de periodieke controle hierop.
 Gevolgen voor de jaarrekening-controle	Wij hebben aanvullende gegevensgerichte controles uitgevoerd op autorisaties en daarbij geen relevante uitzonderingen aangetroffen voor de controleperiode. Er is derhalve geen impact voor de jaarrekeningcontrole.	

Bijlage 2: IT-bevindingen

Detailbevindingen interne beheersing - Toegangsbeveiliging & wijzigingsbeheer Key2Financiën

2022	Authenticatie	Autorisatie	Wijzigingsbeheer	2023	Authenticatie	Autorisatie	Wijzigingsbeheer
	  	  	  		  	  	  

	Authenticatie	Autorisatie	Wijzigingsbeheer
 Bevinding	Er wordt ingelogd in de applicatie middels Single Sign On (SSO). Hierdoor zijn de wachtwoordinstellingen van het netwerk leidend. De ingestelde wachtwoordeisen op het netwerk in combinatie met extra factor zijn van voldoende niveau om op de authenticatie van gebruikers te kunnen steunen.	Binnen de applicatie hebben wij 7 gebruikers met hoge rechten in de applicatie geïdentificeerd. Twee van deze gebruikers zijn direct betrokken bij het primaire (financiële) proces van de applicatie.	Wijzigingen worden getest alvorens deze in productie worden genomen. Deze testwerkzaamheden worden echter niet gedocumenteerd en door de applicatiebeheerder goedgekeurd. De testinspanningen zijn daarom voor ons niet controleerbaar.
 Risico	-	Het risico bestaat dat bedoelde functiescheiding binnen de applicatie wordt doorbroken. Gebruikers met hoge rechten kunnen gebruikers aanmaken en rechten en rollen toekennen om zo functiescheiding te omzeilen.	De kans bestaat dat er onvoldoende testwerkzaamheden worden uitgevoerd waardoor mogelijk wijzigingen worden doorgevoerd met impact op de betrouwbare gegevensverwerking van de applicatie.
 Aanbeveling	-	Wij adviseren om hoge rechten te beperken en deze te beleggen bij onafhankelijke functionarissen.	Wij adviseren om een change management procedure op te zetten waarbij (impactvolle) wijzigingen in een testomgeving worden getest en dit wordt gedocumenteerd. De applicatiebeheerder dient hier een formeel akkoord op te geven alvorens deze wijziging wordt doorgevoerd.
 Gevolgen voor de jaarrekeningcontrole	Gezien de beperkingen ten aanzien van autorisaties en wijzigingsbeheer kan er in de controle niet zonder meer gesteund worden op het lijstwerk uit de applicatie. Er zullen aanvullende gegevensgerichte werkzaamheden moeten worden uitgevoerd om de betrouwbaarheid van lijstwerken vast te stellen.		

Bijlage 2: IT-bevindingen

Detailbevindingen interne beheersing - Continuïteitsmaatregelen en beveiliging

Let op: de onderwerpen volgen uit interviews en hierop zijn door ons over het algemeen geen testwerkzaamheden uitgevoerd om vast te stellen dat de IT-omgeving is ingericht zoals ons voorgesteld is. Dit beperkt de zekerheid die u kunt ontleen aan de door ons beschreven aandachtspunten.



Back-ups: Back-ups worden door GR De Bevelanden en de systeemleveranciers periodiek en incrementeel gemaakt en extern opgeslagen. Er wordt overdag elk uur een back-up gemaakt, waardoor het dataverlies maximaal 1 uur is.

Recovery: De recoverytest en uitwijktest staan op de planning voor het einde van het jaar.

Uitwijk: Een uitwijklocatie is ingericht voor GR De Bevelanden en deze wordt periodiek getest, zie hiervoor ook bovenstaand. De capaciteit van de uitwijklocatie is verhoogd naar 30%. Wij hebben vernomen dat dit in de toekomst naar 70% verhoogd zal worden. Uitwijk is vooral bedoeld om de juiste verbindingen naar de externe applicaties te waarborgen.



Beveiliging

De beveiliging van de IT-omgeving delen wij op in verschillende aspecten, welke wij hieronder hebben weergegeven.

Fysieke beveiliging: De servers van GR De Bevelanden zijn ondergebracht in een daarvoor ingerichte serverruimte afgesloten van de rest van het gebouw. Deze serverruimte beschikt over de benodigde fysieke toegangsbeveiliging.

Remote access: Voor extern inloggen wordt gebruik gemaakt van een VPN verbinding, waarbij met een combinatie van gebruikersnaam en wachtwoord ingelogd wordt en een unieke SSL sleutel benodigd is. Het risico dat externen zich toegang verschaffen tot de Windows omgeving is hierdoor beperkt.

Hiernaast is two-factor authenticatie ingesteld voor inloggen op de Active Directory omgeving. Hiermee wordt toegang verschaffen tot deze omgeving aanvullend beschermd.

Vervolg beveiliging

Preventie: Een firewall en virusscanner is aanwezig en wordt zelf actief beheerd. Er is geen awareness training uitgevoerd onder de medewerkers van gemeente Goes, waarmee het risico op fouten door menselijk handelen verminderd zou kunnen worden.

Monitoring: Er is het afgelopen jaar geen periodieke kwetsbaarheidsscan of penetratietest uitgevoerd.



Kantoorgegevens:

Baker Tilly (Netherlands) N.V.
Stationspark 8b
4460 DZ Goes
Postbus 85
T: 0113-24 20 00