Gemeente Amsterdam

Auditrapport

Derde partijen (third parties)

Third Party Management voor Regiepartijen en SaaS-oplossingen

Referentie: VIC2023/audit 27 AJP

Opdrachtgever: Concerncontroller

Auteur: IA&BO

Proceseigenaar: Directie Digitale Voorzieningen

23 februari 2024 (Definitief)

1 Inleiding

Op basis van het auditjaarplan 2023 heeft de afdeling Interne Audit & Beleidsonderzoek een audit uitgevoerd rondom het proces contractbeheer en leveranciersmanagement voor IT-middelen (verder contractbeheer). Dit proces valt onder de verantwoordelijkheid van directie Digitale Voorzieningen.

Het onderwerp van deze audit is in overeenstemming met de directeur digitale voorziening gedefinieerd op contractbeheer van uitbestede IT-taken en buiten de gemeente gehoste applicaties. Contractbeheer is essentieel voor beheersing van risico's op het gebied van informatiebeveiliging bij buiten de gemeente gehoste applicaties.

Wij hebben deze audit uitgevoerd conform het Audit Charter 2023, welke is ondertekend door onze opdrachtgever, de Gemeentesecretaris. Hierin staat de reikwijdte van onze werkzaamheden en bevoegdheden beschreven en is te vinden op onze intranetpagina van IA&BO. Onze werkzaamheden worden uitgevoerd in overeenstemming met de normen van de beroepsgroep voor interne auditors. Dit is het Instituut voor Interne Auditors (IIA). Sinds september 2022 is IA&BO gecertificeerd.

Op 4 oktober jl. hebben wij u onze auditbrief verstuurd met hierin de gemaakte afspraken ten behoeve van de uitvoering van deze audit.

Doelstelling en centrale vraag:
De audit is gericht op het identificeren en prioriteren van verbetermogelijkheden voor contractbeheer voor IT-middelen. Hiervoor onderzoeken wij de centrale vraag: In welke mate is de gemeente in control voor uitbesteding van IT-dienstverlening?

Scope:
De audit richt zich op onderzoek van contractbeheer voor regiepartijen en leveranciers van Software as a Service (verder (SaaS-leveranciers) welke geen onderdeel van de jaarrekeningcontrole vormen. We doen onderzoek naar beheer en handhaving van de naleving van de contractuele voorwaarden met expliciet aandacht voor informatiebeveiliging, financiële afspraken en afspraken die overig gemeentelijk beleid weerspiegelen zoals duurzaamheid.

Niet in scope:
In de auditbrief was aangegeven dat we ook onderzoek zouden doen naar omgang met generieke voorzieningen en toegang voor leveranciers. Wegens complicaties omtrent de beschikbaarheid van medewerkers en informatie hebben we de scope van de audit op deze punten alsnog moeten beperken.

In onze audit hebben wij geen aandacht besteed aan activiteiten op het gebied van inkopen & aanbesteden, contactbeheer van niet-IT-middelen en contractbeheer van andere IT-middelen dan benoemd onder de scope.

Openbaar maken van rapporten:
Alle definitieve auditrapporten worden 6 maanden na bespreking in het Risk en Audit Comité (RAC) openbaar gemaakt.

In hoofdstuk 2 hebben wij de samenvatting en conclusies opgenomen. In hoofdstuk 3 zijn onze uitgevoerde werkzaamheden en bevindingen opgenomen. In de bijlagen hebben wij deze bevindingen nader uitgewerkt.

Wij bedanken de medewerkers die bij dit onderzoek betrokken zijn geweest voor de open en constructieve samenwerking bij het verrichten van onze werkzaamheden. Tot het verstrekken van nadere toelichting zijn wij uiteraard bereid.

2 Samenvatting en conclusies

De audit Derde partijen is uitgevoerd in het kader van het auditjaarplan 2023 en richt zich op third party management voor regiepartijen en SaaS-oplossingen.

Wij hebben onderzoek gedaan naar contractbeheer en leveranciersmanagement met aandacht voor licentiebeheer, contractbeheer, risicobeheer van leveranciers en bijbehorende governance-aspecten. Ons onderzoek richtte zich op leveranciersmanagement voor SaaS-partijen welke buiten de ACAM-controle vallen en regiepartijen.

Wij hebben de belangrijkste risico's en de getroffen beheersmaatregelen geïdentificeerd. Wij zijn nagegaan of deze interne beheersmaatregelen zijn beschreven en bestaan. De audit heeft betrekking op 2023.

Conclusie t.a.v. Regiepartijen

De risico's voor contractbeheer en leveranciersmanagement voor regiepartijen worden in grote mate beheerst.

Conclusie t.a.v. SaaS-partijen

De risico's voor contractbeheer en leveranciersmanagement t.b.v. SaaS-partijen welke buiten de ACAM-controle vallen worden beperkt oftewel onvoldoende beheerst. De huidige inrichting van beheersmaatregelen binnen het proces bieden deels houvast, maar er is zeker nog ruimte voor verbetering.

* Betekenis kleuren voor de conclusie:
- Groen: goed
- Geel: redelijk/voldoende
- Oranje: beperkt/onvoldoende

De belangrijkste bevindingen (d.i. met prioriteit 1 en 2) zijn:

- Onvoldoende integrale centrale opslag en beschikbaarheid van overeenkomsten.
- Onvoldoende structurele en tijdige ontvangst en analyse van third party mededelingen.
- Onvoldoende integraal en structureel Service Level Management.
- Ontbreken van structurele herevaluatie van integriteit van leveranciers bij grote wijzigingen bij de leverancier.
- Onvoldoende structureel inzicht in de financiële afspraken opgenomen in het contract (oudere contracten)]

Als gevolg van deze bevindingen loopt de gemeente Amsterdam voor SaaS-partijen, welke buiten de ACAM-controle vallen, het risico van onduidelijkheden over de gewenste dienstverlening, levering van slechtere dienstverlening dan contractueel overeengekomen, verminderde beveiliging van (vaak gevoelige) gegevens en het risico dat zaken worden gedaan met partijen welke niet of niet meer voldoen aan de integriteitsvoorwaarden van de gemeente Amsterdam.

Ten slotte melden wij u dat het definitieve auditrapport wordt toegestuurd aan de concerncontroller, de Stedelijk Directeur, de manager Control, de (proces)controller en ACAM. Wanneer ACAM erom verzoekt, verstrekken wij hen ook toegang tot ons dossier. De conclusies en belangrijkste bevindingen worden opgenomen in onze voortgangsrapportage die aan het GMT worden toegestuurd.

Managementreactie Directie Digitale Voorzieningen

Directie Digitale Voorzieningen heeft op 23-02-2024 een managementreactie gegeven op dit rapport. Samengevat heeft directie als reactie aangegeven:

“ Dank voor het delen van het auditrapport. De Directie Digitale Voorzieningen heeft kennisgenomen van het rapport en de daarin opgenomen aanbevelingen. We zijn in de aanbevelingen meegenomen en delen het beeld van de auditor, zien ruimte voor verbetering en zullen de aanbevelingen van de auditor opvolgen.

Voor de volledige managementreactie per bevinding verwijzen wij naar bijlage 1 van ons rapport.

3 Werkzaamheden en bevindingen

Werkzaamheden

In de audit is onderscheidt gemaakt tussen twee types contractmanagement:

- de regiepartners (casus HenT);
- de SaaS-partijen (casussen MijnLenO en Khonraad-Visma*).

* De casussen zijn geselecteerd vanuit een export uit de Application Portfolio Management Tool (Blue Dolphin) met filtering op SaaS-module en met uitsluiting van de applicaties welke onderdeel zijn van de jaarrekeningcontrole.

We hebben ons onderzoek uitgevoerd aan de hand van gegevensgerichte toetsing van enkele cases. We hebben één casus voor regiepartners geselecteerd en drie SaaS-overeenkomsten van twee leveranciers.

Het bestaan van de beheersmaatregelen hebben wij vastgesteld aan de hand van documentatie, het houden van interviews en waarnemingen ter plaatse.

In dit hoofdstuk zullen voor contractmanagement regiepartner HenT geen bevindingen opgenomen worden, omdat dit gedeelte van de audit als goed is beoordeeld (zie H2) en er daardoor geen bevindingen naar voren zijn gekomen. Voor contractmanagement van de SaaS-partijen zijn wel bevindingen geconstateerd en in dit rapport opgenomen.

Vertrouwen

Naast dat wij hebben getoetst op meetbare en tastbare maatregelen zoals procedures en werkinstructies (hard controls), hebben wij ook naar het gedrag van medewerkers en de cultuur van het team (soft controls) gekeken. Uit de geconstateerde bevindingen blijkt dat de gemeente Amsterdam enkele cruciale aspecten van haar IT-beheer kan verbeteren om kostenbewust, kwaliteitsgericht en communicatief effectief te zijn.

Verbetering van het proces betekent voor contractbeheer effectiever kunnen uitvoeren van de ingerichte controls, geen wijziging in aantal controls. Het ontbreken van een integraal beeld over actuele IT-overeenkomsten en structurele archivering kan leiden tot onnodige kosten en kwaliteitsverlies. Het gebrek aan structurele contractuele afspraken over dienstverleningskwaliteit en informatiebeveiliging, samen met het ad-hoc uitvoeren van Service Level Management, onderstreept de behoefte aan verbeteringen in kwaliteitsbeheer. Bovendien wijzen de bevindingen op het belang van het vastleggen en naleven van communicatielijnen en samenwerkingsafspraken in contracten. Door deze aspecten te verbeteren creëert de gemeente helderheid en faciliteert uitvoerbaarheid en transparantie in de uitvoering van contractbeheer. Hiermee kan gemeente Amsterdam haar kosten verder optimaliseren, de kwaliteit van dienstverlening beter waarborgen en communicatie met leveranciers verbeteren.

Bevindingen

Naar aanleiding van de door ons uitgevoerde werkzaamheden hebben wij de volgende bevindingen.

Bevinding 1 Onvoldoende integrale opslag en beschikbaarheid van overeenkomsten

We hebben vastgesteld dat een deel van de bijlagen van de onderzochte overeenkomsten niet beschikbaar waren. Zo ontbrak de SLA en DAP van twee casussen. En ook ontbrak kennisgeving van de verlenging van één overeenkomst. Wel hebben we voor iedere casus een actuele verwerkersovereenkomst (model VNG) aangetroffen. Ook hebben we bij 2 van de drie casussen een DFA aangetroffen.

Verder constateerden we dat voor oudere overeenkomsten bijlagen, verlengingsovereenkomsten en addenda ontbraken waardoor afspraken

voor onder andere integriteitsborging, duurzaamheid en social return, maar ook de opvolging van beveiligingsincidenten mogelijk niet zijn gemaakt.

Tijdens het selecteren van de casussen/deelwaarnemingen hebben wij geconstateerd dat de informatie zoals deze is geregistreerd in Blue Dolphin ten aanzien van soort geleverde IT-oplossing niet juist waren ingevoerd.

Uit de interviews is tevens naar voren gekomen dat vanuit verschillende directies en afdelingen de mogelijkheid bestaat om een samenwerking aan te gaan met een SaaS-leverancier zonder centraal beleid te volgen.

Bevinding 2 Onvoldoende structurele en tijdige ontvangst en analyse van third party mededelingen
De gemeente vereist van SaaS-leveranciers de levering van een geldig ISO-certificaat, de levering van een jaarlijkse ISAE 3402 type 2 assurance-rapportage en een jaarlijkse pentestrapportage, gezamenlijk in dit rapport aangeduid als third party mededelingen. In ons onderzoek hebben we van 1 leverancier een alternatief voor de ISAE 3402 assurancerapportage aangetroffen (In Control Verklaring t.a.v. de naleving van de BIO van oktober 2022), maar zonder onderliggende detailrapportage. Voor de andere leverancier was geen ISAE 3402 assurancerapportage of een vervangende rapportage beschikbaar. Het ontbreken van een actuele third party-mededeling en daarop uitgevoerde analyse betekent dat de gemeente niet beschikt over actuele informatie omtrent de kwaliteit van de informatiebeveiligingsmaatregelen getroffen door de leverancier.

Bevinding 3 Onvoldoende integraal en gestructureerd Service Level Management
Het handelingskader contractmanagement van gemeente Amsterdam bevat afspraken over de uitvoering van het service level management. In het casusonderzoek constateerden we dat de naleving van het handelingskader beperkt is. Contractbeheer wordt uitgevoerd door vele verschillende functionarissen en deels op ad hoc basis. Dit is bijvoorbeeld gebleken uit het ontbreken van formele en regelmatig ontvangen service level rapportages en het ontbreken van een periodiek overleg met een vaste frequentie.

Bevinding 4 Ontbreken van structurele her-evaluatie van integriteit van leveranciers bij grote wijzigingen bij de leverancier
Eén van de geselecteerde leveranciers is recent overgenomen door een sterk groeiende buitenlandse (Noorse) partij. Het gemeentelijk beleid omvat de verplichting om bij grote wijzigingen in contractpartijen een hernieuwde evaluatie van de geschiktheid van de leverancier als gemeentelijke partner uit te voeren. Dit kan in de vorm van een zogeheten ‘basale toets’. In het dossier van de leverancier hebben we geen vastlegging van de uitvoering van een dergelijke toetsing aangetroffen. Wel hebben we geconstateerd dat de overeenkomst voor één van de twee afgenomen SaaS-modules is herzien en dat een paragraaf is opgenomen inzake integriteitsborging en naleving van de Beleidsregel Integriteit en Overeenkomsten (BIO gemeente Amsterdam).

Bevinding 5 Onvoldoende structureel inzicht in de financiële afspraken opgenomen in het contract (oudere contracten)
Voor uitvoering van goed financieel contractbeheer is inzicht in financieel gerelateerde afspraken essentieel. Voor één van de drie casussen ontbrak in de overeenkomst informatie omtrent indexatie, boeteclausules en andere financiële afspraken. Wel vermeld waren de tariefstructuur en tarieven van het jaar van aangaan van de overeenkomst (2001).

Verlengingsovereenkomsten en addenda voor deze overeenkomst ontbreken eveneens. Bij de andere twee casussen is wel informatie voor het

kunnen uitvoeren van financieel contractbeheer in de overeenkomst met bijlagen zoals DFA opgenomen.

Bij twee van de drie casussen betreft het een monopolist voor de geleverde SaaS-oplossing. In één van de overeenkomsten is getracht het financieel beheer te versterken door opname van een mogelijkheid tot uitvoering van benchmarking in de overeenkomst. Een gevolg van uitvoering van financieel contractbeheer blijkt uit het memorandum van de monopolist waarbij korting op een forse tariefverhoging wordt gegeven in het eerste jaar van ingaan. De prijsverhoging was een gevolg van de implementatie van nieuwe wetgeving.

Overige constateringen

Naast de bovenstaande vijf bevindingen welke een verdere uitwerking vormen van de bevindingen genoemd in hoofdstuk twee hebben we nog enkele kleinere (prio 3) constateringen:

6. Onjuistheden in registratie Application Portfolio Management tool: Bij de selectie van casussen voor ons deelonderzoek constateerden we dat applicaties in de Application Portfolio Management tool (Blue Dolphin) foutief gelabeld waren. Een voorbeeld betreft de verschuiving tussen het label module en het label SaaS.

7. Onvoldoende aansluiting op nieuwe gemeentelijke werkwijzen: Bij twee van de drie casussen waren in de overeenkomst met bijlage afspraken opgenomen inzake doorontwikkeling en wijzigingenbeheer. Deze afspraken sluiten nog niet aan op de nieuwe gemeentelijke agile- en OWW-werkwijze.

8. Onvoldoende aansluiting IT-ondersteuning op Amsterdamse werkwijzen: Bij één van de drie casussen bleek de machtspositie van de monopolist uit de eenzijdige doorvoering van een ontwikkeling ongeacht of deze aanpassing bij de sterk gedigitaliseerde werkwijze lvan gemeente Amsterdam past (vb. printstraat BOPZ online).

9. Ontbreken van rapportages over overige contractafspraken: We hebben in de dossiers van deze drie casussen geen rapportages ten aanzien van de naleving van de afspraken omtrent duurzaamheid en social return aangetroffen.

De bevindingen zijn (met overeenkomstige nummering) nader uitgewerkt in bijlage 1. In bijlage 2 is een volledig overzicht opgenomen van alle door ons getoetste interne beheersmaatregelen met onze conclusies over de opzet, het bestaan en de effectieve werking van de getoetste beheersingsmaatregelen.

In het onderstaande schema hebben wij op basis van een risico-inschatting aangegeven welke prioriteit aan de bevindingen moet worden gegeven.

Wij maken daarbij het volgende onderscheid in de bevindingen:
Prioriteit 1: Zeer belangrijk, grote impact, urgent, opvolging direct vereist
Prioriteit 2: Belangrijk, gemiddelde impact, minder urgent, opvolging nodig
Prioriteit 3: Aandacht nodig, beperkte impact, niet urgent, opvolging niet noodzakelijk

Bevindingen met prioriteit 1 worden in de voortgangsrapportages aan het GMT opgenomen. Prioriteit 2 bevindingen worden alleen aan het GMT gemeld als er geen opvolging aan wordt gegeven en prioriteit 3 bevindingen worden enkel aan de directie en management gerapporteerd.

Bevindingen	Prioriteit 3 Laag	Prioriteit 2 Midden	Prioriteit 1 Hoog
1. Onvoldoende integrale centrale opslag en beschikbaarheid van overeenkomsten			X
2. Onvoldoende structurele en tijdige ontvangst en analyse van third party mededelingen			X
3. Onvoldoende integraal en gestructureerd Service Level Management			X
4. Ontbreken van structurele herevaluatie van integriteit van leveranciers bij grote wijzigingen bij de leverancier		X	
5. Onvoldoende structureel inzicht in financiële afspraken opgenomen in het contract (oudere contracten)		X	
6. Onjuistheden in registratie Application Portfolio Management tool	X		
7. Onvoldoende aansluiting op nieuwe gemeentelijke werkwijzen	X		
8. Onvoldoende aansluiting IT-ondersteuning op Amsterdamse werkwijzen	X		
9. Ontbreken van rapportages over overige contractafspraken	X		

Bijlage 1: Bevindingen en aanbevelingen

Bevindingen Directie Digitale Voorzieningen

1. Onvoldoende integrale centrale opslag en beschikbaarheid van overeenkomsten	PRIO 1

Achtergrond	I-domein is per 1 juli 2022 gecentraliseerd waarna gewerkt is aan uniformering van diverse stedelijke processen. Ten tijde van de audit was de uniformering van de processen voor contractbeheer en leveranciersmanagement gaande. Een handelingskader was beschikbaar, maar overdracht van alle overeenkomsten aan de centrale vakgroep was nog niet gerealiseerd. O.a. de overdracht van de IT-overeenkomsten van de GGD zijn nog niet gerealiseerd. De reorganisatie per 1 juli 2022 was een volgende stap in de ontwikkelingen ingezet bij de grote stedelijke reorganisatie van per 1 januari 2015. Daarnaast is uit gesprekken gebleken dat vanuit verschillende directies de mogelijkheid bestaat om een samenwerking aan te gaan met een SaaS-leverancier zonder centraal beleid te volgen. Bovenstaande heeft tot gevolg dat ook het contractbeheer deels centraal (samenwerking contractbeheerder met (keten)informatiemanager) en deels decentraal (samenwerking afdeling, beleid en informatiemanagement) plaatsvindt. Bevinding 1 is een samenvoeging van de resultaten van het onderzoek van de risico's. Voor een overzicht van de onderzochte risico's en beheersmaatregelen zie bijlage 2.
Bevinding	Bij het onderzoek van de drie geselecteerde casussen hebben we geconstateerd dat voor geen enkele van de drie casussen alle bijlagen, addenda en verlengingsovereenkomsten beschikbaar waren. - Casus BOPZ online (Khonraad-Visma): aanwezig zijn een overeenkomst uit 2002 met een recente verwerkersovereenkomst (juli 2022), maar geen SLA, DAP of DFA - Casus Tijdelijk Huisverbod (Khonraad-Visma): aanwezig een herziene en geactualiseerde overeenkomst (oktober 2021) voorzien van DFA en verwerkersovereenkomst, maar geen SLA of DAP.

	- Casus LenO: geen overeenkomst, wel een SLA en verwerkersovereenkomst (beiden december 2021). Deze beperkte documentlevering duidt op een zeer onvolledige archivering en daarmee onvolledig inzicht in de contractuele afspraken. Uit de overeenkomst (Tijdelijk Huisverbod) en SLA (LenO) blijken dat de overige documenten als bijlagen bij de overeenkomst wel aanwezig zouden moeten zijn. Als gevolg van deze beperkte documentatie ontbreekt inzicht in gemaakte afspraken omtrent: - Dienstverleningsniveau's (2x) - Financiële afspraken (2x) - Algemene afspraken waaronder afspraken op het gebied van duurzaamheid, naleving van de Beleidsregel Integriteit en ten aanzien van social return (2x) - Afbakening van taken, verantwoordelijkheden en overlegstructuren (3x) - Escalatieprocedures (1x) en incidentmanagement (2x)
Risico	R1. Het ontbreken van duidelijke contractvoorwaarden bemoeilijkt het contractbeheer en kan leiden tot een slechtere kwaliteit van de dienstverlening. R2. De grote inhoudelijke verschillen tussen overeenkomsten, ook meerdere overeenkomsten met dezelfde leverancier, leidt tot inefficiënt en mogelijk diffuus contractmanagement. R3. Het ontbreken van voldoende inzicht en beheersing van leverancierspresta ties kan leiden tot betaling voor niet geleverde prestaties en tot levering van kwalitatief onvoldoende prestaties.
Oorzaak	Oorzaken zijn het tot voor kort ontbreken van een formeel handelingskader voor contractbeheer. Daarnaast heeft ook de impact van de organisatiewijziging voor het I-domein in 2022 en de grote omvang van personeelswisselingen tot gevolg dat overeenkomsten slechts deels beschikbaar zijn.
Aanbeveling	Maak voor het contractbeheer van (SaaS-)overeenkomsten gebruik van de contractregistratie welke door Financiën en Inkoop ter beschikking gesteld gaat worden.

Managementreactie	Wij onderschrijven de oorzaak en maken graag gebruik van het contractmanagementsysteem dat door directie F&I beschikbaar gesteld zal worden. Inrichten en Ingebruikname nieuw CMS.	voorlopige planning is 01-10-24 in productie Q4 2024 Follow-up audit: ja	Verantwoordelijke directie: F&I voor levering Ingebruikname DV

2. Onvoldoende structurele en tijdige ontvangst en analyse van third party mededelingen	**PRIO 1**

Achtergrond	In de overeenkomst en de bijbehorende verwerkersovereenkomst zijn afspraken opgenomen omtrent borging van informatiebeveiliging en privacyborging. De leverancier toont de naleving van de gemaakte afspraken aan door levering van een geldig certificaat ISO 27001 en NEN 7510. Daarnaast levert de leverancier jaarlijks een ISAE 3402 type 2 assurancerapportage en wordt jaarlijks een pentest [hacktest] uitgevoerd waarvan de resultaten met de gemeente gedeeld moeten worden. Deze rapportage worden ook wel aangeduid als third party mededelingen.
Bevinding	Op basis van interviews en documentatie onderzoek met betrekking tot de geselecteerde deelwaarnemingen zijn de volgende bevindingen vastgesteld: Leverancier 1 - 1 SaaS-module Onbekend is welk type rapportage is gevraagd. Een Assurancerapportage is niet ontvangen. Ook het ISO-certificaat is niet ontvangen. Leverancier 2 - 2 SaaS-modules De leverancier levert certificaten en rapportages voor de applicatie als geheel waarmee deze van toepassing zijn op beide afgenomen modules. Geleverd zijn een geldig ISO-certificaat en een geldig NEN-certificaat. In de overeenkomst is voor één van de modules een ander type rapportage gevraagd dan vermeld in het gemeentelijk beleid. In de overeenkomst voor de tweede module ontbreekt een verplichting tot levering van een assurance-rapportage. Door de leverancier is invulling gegeven aan de contractuele passage in één van de twee overeenkomsten door levering van een Statement of Compliancy: In Control Verklaring te leveren afgegeven door Audit orde B.V. voor specifiek benoemde BIO-hoofdstukken. Het gekozen alternatief is niet gelijk aan de door de gemeente vereiste

	assurance rapportage, maar bevat wel een gemeente-specifieke invulling. De ontvangen ICV is van oktober 2022 en heeft betrekking op de periode oktober 2021-september 2022. Een recentere ICV was ten tijde van afronding van de audit nog niet beschikbaar. De scope van de ICV heeft betrekking op de hoofdstukken 6 en 8 tot en met 18. Dit betekent dat de hoofdstukken 5 Informatiebeveiligingsbeleid en 7 Veilig personeel buiten de scope van deze ICV zijn gehouden. Er is geen bevestiging van de gemeente dat deze scope voor het ICV is overeengekomen tussen gemeente en leverancier. De ICV van 3 oktober 2022 geeft een gemiddelde score van 2,862 bij een maximumscore van 3,0. De laagste score, 2,5, is op H15 (Leveranciersrelaties). De hoofdstukken 8 (beheer van bedrijfsmiddelen), 10 (Cryptografie), 14 (Acquisitie, ontwikkeling en onderhoud IS-systemen) en 18 (Naleving) hebben de maximale score van 3,0. De overige hoofdstukken hebben scores van 2,8 en 2,9. Uit de ontvangen documentatie blijkt niet welke follow up de gemeente heeft gegeven aan deze rapportage. De rapportage met detailgegevens behorende bij deze score is opgevraagd, maar niet ontvangen. Hierdoor ontbreekt ook inzicht in de analyse en vervolgacties naar aanleiding van deze score op de BIO. Voor MijnL&O is er tevens geen assurance rapport en/of ISO cerficaat gedeeld en beschikbaar. Deze verwachtingen staan wel formeel gedocumenteerd in het verwerkingsovereenkomst.
Risico	R1. De gemeente doet zaken met partijen welke niet compliant zijn met van toepassing zijnde wet- en regelgeving. R2. Het risico is aanwezig dat de gemeente onopgemerkt bloot staat aan een groter risico op datalekken en schending van de vertrouwelijkheid.
Oorzaak	Oorzaken zijn het tot voor kort ontbreken van een formeel handelingskader voor contractbeheer. Daarnaast heeft ook de impact van de organisatiewijziging voor het I-domein in 2022 en de grote omvang van personeelswisselingen tot gevolg dat overeenkomsten slechts deels beschikbaar zijn waardoor aandacht voor third party mededelingen verder verslapte. Ook was voorafgaand aan de organisatiewijziging de verantwoordelijkheid voor ontvangst, analyse en terugkoppeling van de third party mededelingen versnipperd belegt binnen de organisatie. De verantwoordelijken konden zijn de security officer, de informatiemanager of de contractbeheerder.
Aanbeveling	1. Besteed bij de implementatie van het nieuwe handelingskader expliciet aandacht aan de rol van contractbeheer ten aanzien van borging van naleving van contractuele afspraken waar voor software-overeenkomsten uitdrukkelijk ook de levering van assurancerapportages (Third party mededelingen, TPM) bij hoort. Borg daarmee dat de contractbeheerder ten aanzien van de ontvangst en verwerking van TPM- assurancerapportagess zijn verantwoordelijkheid kan nemen.

	2. Train de contractmanagers in basiskennis van lezen en begrijpen van TPM-assurancerapportages en neem daarbij mee in welke situaties in ieder geval een security officer moet worden ingeschakeld.		
Managementreactie	Wij zien ruimte voor verbetering en zullen de aanbevelingen van de auditor hierover opvolgen Implementatie handelingskader en toepassing – door ICLM	Q3-Q4 Q4-2024 Follow-up audit: ja/nee	Verantwoordelijke directie: DV

3. Onvoldoende integraal en gestructureerde Service Level Management	PRIO 1

Achtergrond	Als gevolg van het ontbreken van structurele en eenduidige archivering van overeenkomsten met alle bijbehorende documenten komt het ook voor dat de SLA en daarmee de basis voor uitvoering van het service level management niet beschikbaar is. Daarnaast is ook de DAP en daarmee de afspraken over taakverdelingen, processen en communicatielijnen niet altijd beschikbaar. Leverancier 2 betreft een monopolist voor de IT-ondersteuning geleverd met de twee SaaS-modules betrokken in ons onderzoek. Voor beide SaaS-modules zijn afzonderlijke overeenkomsten afgesloten.
Bevinding	Generiek Met iedere leverancier zijn overlegstructuren aangetroffen. De deelname aan en de frequentie van de diverse overleggen is divers en varieert van beleidsmedewerkers tot lijnmanagement, informatiemanagers en leveranciersmanagers. Een voorbeeld van actief SLM bleek uit de opmerking van de leveranciersmanager over verzending van een brandbrief naar een CEO van leverancier anders dan de geselecteerde casussen (communicatie +). De inrichting van het service level management is verschillend per overeenkomst. De verschillen hebben betrekking op verschillen in gemeentelijke functies verantwoordelijk voor de uitvoering, wel of niet structureel en periodiek ontvangen en verwerken van geformaliseerde rapportages, ontbreken van third party mededelingen en bijbehorende detailrapportages. Hiermee ontstaat een indruk van ad hoc en diverse uitvoering van service level management voor kleinere SaaS-overeenkomsten en daarmee verminderde prestatie(mogelijkheden) voor het gedragsaspect kwaliteitsgericht (kwaliteitsgericht -) Leverancier 1 – 1 SaaS-module Een formele en uitgebreide service level rapportage (SLR) is geleverd en is in overeenstemming met de afspraken in de eveneens beschikbare SLA. Leverancier 2 – 2 SaaS-modules Voor beide modules waren geen formele periodieke service level rapportages (SLR) beschikbaar. Voor één van de twee modules is ten behoeve van de audit een SLR opgevraagd bij de leverancier. Ontvangen is een mail met daarin getypte informatie over service levels in de periode 1 januari tot 21 november 2023. Dit is beoordeeld als een informele melding over een willekeurige periode en daarmee niet gelijk te stellen met een formele periodieke SLR. Uit gesprekken is gebleken dat er geen sprake is van een vaste frequentie voor overleggen. De laatste jaren zijn overleggen naar behoefte gepland. Ook ontbreken heldere en eenduidige afspraken omtrent rapportering en opvolging van beveiligingsincidenten in één van de twee overeenkomsten. Een positief punt is het gebruikersoverleg

	dat door de leverancier wordt gevoerd met een vertegenwoordiging van al hun klanten (gemeenten, ggz-instellingen) en de samenwerking in VNG-verband.
Risico	R1. Als gevolg van de ad hoc uitvoering van service level management en het ontbreken van tijdig en structureel periodiek ontvangen van formele service level rapportages, third party mededelingen met bijbehorende detailrapportages loopt de gemeente het risico dat, veelal gevoelige, gegevens opgeslagen in de databases van de betreffende SaaS-oplossingen onvoldoende beschermt zijn tegen toegang door onbevoegden zonder dat de gemeente hiervan op de hoogte is. Het ontbreken van informatie betekent dat de gemeente niet in staat is om tijdig aanvullende of vervangende maatregelen te treffen ter bescherming van deze gegevens. Toegang door onbevoegden kan resulteren in gijzeling of verminking van data. Ook kunnen datalekken het gevolg zijn. R2. Een ander risico van ad hoc uitvoering van service level management zonder integrale overkoepelende informatiestroom is dat de gemeente niet beschikt over een integraal beeld van de kwaliteit van de informatiebeveiliging voor alle uitbestede IT-diensten gezamenlijk.
Oorzaak	Oorzaken zijn het tot voor kort ontbreken van een formeel handelingskader voor contractbeheer. Daarnaast heeft ook de impact van de organisatiewijziging voor het I-domein in 2022 en de grote omvang van personeelswisselingen tot gevolg dat overeenkomsten slechts deels beschikbaar zijn. Voor effectieve uitvoering van service level management is het essentieel om te beschikken over de volledige overeenkomst met bijlagen waarbij in ieder geval de afspraken veelal opgenomen in de service level afspraken (SLA) en dossier afspraken en procedures (DAP) noodzakelijk zijn.
Aanbeveling	Besteed bij de implementatie van het nieuwe handelingskader expliciet aandacht aan de rol van contractbeheer ten aanzien van borging van naleving van contractuele afspraken over uitvoering van service level management.

Managementreactie	Wij zullen de aanbevelingen van de auditor hierover opvolgen Implementatie handelingskader met nadruk naleving van afspraken SLM – door ICLM	Q3-Q4 Q4-2024 Follow-up audit: ja/nee	Verantwoordelijke directie: DV

4. Ontbreken van structurele herevaluatie van integriteit van leveranciers bij grote wijzigingen bij de leverancier	PRIO 2

Achtergrond	In het handelingskader is aangegeven dat borging van naleving van de Beleidsregel Integriteit en Overeenkomsten gemeente Amsterdam (BIO gemeente Amsterdam) ook gedurende de looptijd van de overeenkomst uitgevoerd dient te worden. De borging van de naleving bestaat uit handhaving van de contractuele afspraken en her-evaluatie van de leverancier bij grote veranderingen zoals wijzigingen in de bedrijfsvoering of organisatiestructuur. Voor uitvoering van deze her-evaluatie zijn instructies aanwezig.
Bevinding	Vastgesteld is dat één van de beide leveranciers betrokken in het onderzoek in de afgelopen twee jaar een grote verandering heeft meegemaakt, namelijk overname door een grote Europese (niet-EU) partij. In het dossier van de leverancier is geen her-evaluatie van de integriteit van de leverancier aangetroffen. Wel hebben we geconstateerd dat voor één van de beide afgenomen SaaS-modules in 2020 een nieuwe overeenkomst is afgesloten waarin een hoofdstuk over borging integriteit met naleving van de beleidsregel is opgenomen. De overeenkomst voor de andere SaaS-module dateert uit 2002 en bevat geen afspraken omtrent borging integriteit en eventueel van toepassing zijnde wet- en regelgeving. Voor beide modules is in 2022 de verwerkersovereenkomst (model VNG) vernieuwd.
Risico	Het niet uitvoeren van een integriteitstoets bij grote wijzigingen van de leverancier kan tot gevolg hebben dat de gemeente zaken doet met een leverancier welke op basis van het gemeentelijk integriteitsbeleid niet in aanmerking komt als contractpartij. In de meest extreme situatie kan dit leiden tot zakelijke relaties met partijen welke gebruik maken van dubieuze financiering. Omdat het hier gaat over levering van een SaaS-dienst kan dit ook betekenen dat gegevens van kwetsbare burgers in handen kunnen komen van daarvoor ongeschikte partijen.
Oorzaak	Oorzaken zijn het tot voor kort ontbreken van een formeel handelingskader voor contractbeheer. Daarnaast heeft ook de impact van de organisatiewijziging voor het I-domein in 2022 en de grote omvang van personeelswisselingen tot gevolg dat overeenkomsten slechts deels beschikbaar zijn. Het uitvoeren van een periodieke herevaluatie van de leverancier in het kader van de Beleidsregel gemeente Amsterdam is tevens een recente toevoeging aan de activiteiten welke vallen onder contractbeheer.

Aanbeveling	Besteed bij de implementatie van het nieuwe handelingskader expliciet aandacht aan de rol van contractbeheer ten aanzien van borging van naleving van stedelijk beleid over naleving Beleidsregel Integriteit. Daar hoort bij het instrueren van de contractmanagers in welke situatie welke integriteitstoets uitgevoerd kan worden.		
Managementreactie	Wij zullen de aanbevelingen van de auditor hierover opvolgen Handreiking aan contractmanagers over beleid en naleving – door ICLM	Q2-Q3 Q3-2024 Follow-up audit: ja/nee	Verantwoordelijke directie: DV

5. Onvoldoende structureel inzicht in de financiële afspraken opgenomen in het contract (oudere contracten)	PRIO 2

Achtergrond	Leverancier 2 (2 SaaS-modules) is een monopolist voor levering van IT-ondersteuning voor uitvoering van de wetgeving welke met de beide SaaS-modules wordt ondersteund. Bij bevinding 1 is geconstateerd dat de archivering van overeenkomsten met bijlagen, addenda en verlengingsovereenkomsten onvolledig is. Dit heeft tot gevolg dat de actuele afspraken op het gebied van financiën niet altijd beschikbaar zijn bij de functionarissen die verantwoordelijk zijn voor financieel contractbeheer.
Bevinding	De gemeente borgt financiële afspraken voor IT-middelen in de overeenkomst met de leverancier aangevuld met een bijlage Document Financiële Afspraken (DFA). De gemeente beschikt nog altijd over (oudere) overeenkomsten zonder contractpassages over contractindexering, kostencontroleclausules. In recentere contracten wordt actief gewerkt aan het beheersen van financiële risico's. Dit blijkt o.a. uit de aanwezigheid van afspraken omtrent financiële gevolgen bij constateren van disfunctioneren van de leverancier. In één van de overeenkomsten met leverancier 2 van ons onderzoek zien we bijvoorbeeld een paragraaf waarin de mogelijkheid van benchmarking is opgenomen. Een andere beheersingsmaatregel is het gezamenlijk in VNG-verband optreden van de gemeenten in relatie tot de leverancier. De gevoeligheid van deze leverancier voor dergelijke druk zien we terug in de verlening van een korting van 20% in een eerste jaar van forse prijsstijgingen naar aanleiding van de implementatie van nieuwe wetgeving wat leidde tot IT-aanpassingen. In de dossiers hebben we geen periodieke evaluatie aangetroffen van de financiële gezondheid van de IT-leveranciers betrokken in ons onderzoek naar de gemeentelijke uitvoering van leveranciersmanagement.
Risico	De gemeente loopt het risico op hogere financiële lasten dan begroot (begrotingsonrechtmatigheid) als gevolg van het niet direct en integraal beschikbaar zijn van de volledige overeenkomst met bijlagen en eventueel van toepassing zijnde verlengingsafspraken. Dit risico wordt vergroot indien ook sprake is van vergaande afhankelijkheid van één of enkele leveranciers voor uitvoering van wettelijke taken. Het ontbreken van inzicht in de financiële gezondheid van leveranciers kan, naast onverwachtse en niet overeengekomen forse tariefstijgingen, ook tot gevolg hebben dat dienstverlening onverwachts stagneert wegens financiële continuïteitsproblemen van de leverancier.

Oorzaak	Oorzaken zijn het tot voor kort ontbreken van een formeel handelingskader voor contractbeheer. Daarnaast heeft ook de impact van de organisatiewijziging voor het I-domein in 2022 en de grote omvang van personeelswisselingen tot gevolg dat overeenkomsten slechts deels beschikbaar zijn. Voor effectieve uitvoering van financieel contractbeheer is het essentieel om te beschikken over de volledige overeenkomst met bijlagen waarbij in ieder geval de financiële afspraken veelal opgenomen in het dossier financiële afspraken (DFA) noodzakelijk zijn.		
Aanbeveling	Voer periodiek een project contractrationalisatie uit.		
Managementreactie	Wij zullen de aanbevelingen van de auditor hierover opvolgen We zijn bezig met de contract hygiëne op orde te krijgen door het contract- en licentieregister te actualiseren. Dit doen we via A (Actueel), B(Betrouwbaar) en C (Compleet). Dit maakt rapportage als rationalisatie mogelijk. – door ICLM	Q1-Q3 Q3-2024 Follow-up audit: ja/nee	Verantwoordelijke directie: DV

6. Onjuistheden in registratie Application Portfolio Management tool — PRIO 3

Achtergrond	Voor samenstelling van een populatie voor het selecteren van een deelwaarneming op SaaS-applicaties was een overzicht van in gebruik zijnde SaaS-modules noodzakelijk. I-domein blijkt over drie mogelijke bronnen te beschikken, namelijk applicatielandschap, de applicatie portfolio management tool en het contractregister. Het contractregister bevat contractgegevens, maar geen kenmerken van de betreffende IT-tool. Voor de selectie is uiteindelijk gebruik gemaakt van een rapportage vanuit de applicatieportfolio managementtool.
Bevinding	Bij de selectie van casussen voor ons deelonderzoek constateerden we dat applicaties in de Application Portfolio Management tool (Blue Dolphin) foutief gelabeld waren. Dit betrof de verschuiving tussen het label module en het label SaaS. Tijdens de bespreking van de bevindingen is aangegeven dat Blue Dolphin het afgelopen jaar niet is bijgewerkt. Ten behoeve van onze audit hebben we geen aansluiting gemaakt tussen de drie bronnen voor inzicht in SaaS-applicaties.

Risico	Het ontbreken van een juist en volledig overzicht van alle IT-middelen voorzien van de juiste karakteristieken kan tot gevolg hebben dat contractbeheer niet of slechts gedeeltelijk uitgevoerd wordt voor een specifieke IT-tool.		
Oorzaak	Contractbeheer moet voor een totaaloverzicht over haar werkpakket gebruik maken van verschillende informatiebronnen (hier contractenregister, applicatielandschap en applicatie portfolio management tool) welke ieder voor een ander doel zijn ingericht en vanuit verschillende processen worden onderhouden.		
Aanbeveling	Borg dat de diverse overzichten waarin de gemeente haar applicaties registreert op elkaar aansluiten. Wees daarbij helder in de keuze over welke registratie leidend is, met welk doel een registratie wordt bijgehouden en vanuit welk proces een registratie wordt geïnitieerd. Het gaat hier over de drie registraties contractregister (deel IT-contracten), applicatieportfoliomanagement tool en applicatielandschap. Centralisatie van registraties en beperking in aantal verschillende registratielocaties heeft daarbij de voorkeur.		
Managementreactie	Wij zullen de aanbevelingen van de auditor hierover opvolgen In samenspel met de vakgroepen APM (applicatieportfolio) en vakgroep Functioneel Beheer (Applicatielandschap) willen we toewerken naar een optimale registratie – drie vakgroepen	Q3-Q4 Q4-2024 Follow-up audit: ja/nee	Verantwoordelijke directie: DV en DII

7. Onvoldoende aansluiting op nieuwe gemeentelijke werkwijzen	**PRIO 3**

Achtergrond	De gemeente is voor interne doorontwikkeling en wijzigingenbeheer bezig met de omschakeling naar Opgavegericht en Wendbaar Werken (OWW) wat is gebaseerd op de agile werkwijze. Implementatie van OWW wordt stapsgewijs doorgevoerd en heeft ook invloed op de samenwerking met de leveranciers.
Bevinding	Bij twee van de drie casussen waren in de overeenkomst met bijlage afspraken opgenomen inzake doorontwikkeling en wijzigingenbeheer. Deze afspraken sluiten nog niet aan op de nieuwe gemeentelijke agile- en OWW-werkwijze.

Risico	Het ontstaan van een mismatch tussen de werkwijze van gemeente Amsterdam (in wijzigingenbeheer en/of in het ondersteunde proces) en de door de dienstverlener ondersteunde procesinrichting.
Oorzaak	Oorzaken zijn het tot voor kort ontbreken van een formeel handelingskader voor contractbeheer. Daarnaast heeft ook de impact van de organisatiewijziging voor het I-domein in 2022 en de grote omvang van personeelswisselingen tot gevolg dat overeenkomsten slechts deels beschikbaar zijn. Voor effectieve realisatie van doorontwikkeling en wijzigingen als onderdeel van de uitvoering van effectief contractbeheer is het essentieel om te beschikken over de volledige overeenkomst met bijlagen waarbij in ieder geval de afspraken veelal opgenomen in het dossier afspraken en processen (DAP) noodzakelijk zijn. Uit deze afspraken moet blijken op welke wijze gemeente en leverancier met elkaar samenwerken rekening houdend met de wederzijdse ontwikkelingen ten aanzien van agile werken (generiek) en OWW-werken (gemeentelijke invulling).
Aanbeveling	Besteed bij de implementatie van het nieuwe handelingskader expliciet aandacht aan de wijze waarop de gemeente omgaat met nieuwe werkwijzen ten opzichte van bestaande overeenkomsten waar agile werken en OWW-werken nog geen plaats in de overeenkomst heeft.

Managementreactie	Wij zien ruimte voor verbetering daar waar de kanteling heeft plaatsgevonden werken we met de nieuwe werkwijze. Nieuwe werkwijze vertaalt zich naar overeenkomsten binnen de opgaven, via training en presentaties zullen we hier meer aandacht voor vragen – door opgaveteams / ICLM	Q2-Q4 Q4-2024 Follow-up audit: ja/nee	Verantwoordelijke directie: DV

8. Onvoldoende aansluiting IT-ondersteuning op Amsterdamse werkwijzen — PRIO 3

Achtergrond	SaaS-applicaties worden gebruikt ter ondersteuning van veelal wettelijke taken. Effectieve inzet van IT-tools zoals SaaS-applicaties betekent ook een goede integrale aansluiting tussen de procesinrichting en de procesuitvoering in de applicatie. De integrale aansluiting wordt gecompliceerd doordat een SaaS-applicatie veelal wordt gebruikt door meerdere gemeenten voor dezelfde wettelijke taken waarbij de leverancier vanuit beheersoogpunt voor alle gemeentelijke afnemers dezelfde inrichting wil hanteren en daarmee veelal één werkwijze ondersteunt.

Bevinding	Gedurende onze audit hebben we voor één casus vastgesteld dat de leverancier wegens de implementatie van nieuwe wetgeving forse wijzigingen in de applicatie heeft doorgevoerd. Eén van de wijzigingen betrof de inrichting van een fysieke printstraat hetgeen strijdig is met het Amsterdamse beleid om de burger primair digitaal te informeren. De aanwezigheid van de fysieke printstraat heeft genoodzaakt tot inrichting van een alternatieve werkwijze ter voorkoming van te late kennisgeving en verkeerde bezorging van kennisgeving. De leverancier is een monopolist voor de ondersteuning op deze wettelijke taak.		
Risico	Toepassing van een fysieke printstraat in dit proces kan in dit proces tot een verhoogd risico heeft tot gevolg dat de formele schriftelijke kennisgeving te laat en mogelijk zelfs verkeerd geadresseerd wordt bezorgd.		
Oorzaak	Oorzaken zijn het tot voor kort ontbreken van een formeel handelingskader voor contractbeheer. Daarnaast heeft ook de impact van de organisatiewijziging voor het I-domein in 2022 en de grote omvang van personeelswisselingen tot gevolg dat overeenkomsten slechts deels beschikbaar zijn.		
Aanbeveling	Besteed bij de implementatie van het nieuwe handelingskader expliciet aandacht aan de rol van contractbeheer ten aanzien van borging goede aansluiting tussen werkprocessen van de lijndirecties en de IT-ondersteuning die door de leverancier ter beschikking wordt gesteld.		
Managementreactie	Wij zullen de aanbevelingen van de auditor hierover opvolgen Aandacht bij implementatie van het handelingskader met nadruk aansluiting tussen de werkprocessen – door ICLM	Q3-Q4 Q4-2024 Follow-up audit: ja/nee	Verantwoordelijke directie: DV

9. Ontbreken van rapportages over overige contractafspraken — PRIO 3

Achtergrond	Het gemeentelijk beleid bevat voor haar contractpartners steeds meer aanvullende zaken waar de gemeente met iedere leverancier afspraken over wil maken. Dit zijn afspraken welke niet specifiek voor het soort dienst of levering zijn, maar wel door de gemeente generiek van belang worden geacht. De naleving van deze afspraken vormt onderdeel

	van contractbeheer. Op dit moment gaat het om afspraken op het gebied van naleving van de Beleidsregel Integriteit en Overeenkomsten gemeente Amsterdam welke in bevinding 4 al is genoemd. Daarnaast betreft het ook afspraken op het gebied van Duurzaamheid en Social Return.		
Bevinding	We hebben in de dossiers van deze drie casussen geen rapportages ten aanzien van de naleving van de afspraken omtrent duurzaamheid en social return aangetroffen. Hierdoor hebben we niet kunnen vaststellen in welke mate handhaving van de gemaakte afspraken op deze onderwerpen plaatsvindt. Daarnaast hebben we vastgesteld dat in de overeenkomst van één van de drie casussen afspraken op het gebied van duurzaamheid en social return ontbreken.		
Risico	Het risico is aanwezig dat een leverancier voor één of meer van deze onderwerpen niet voldoet aan de overeengekomen afspraken wat tot gevolg heeft dat de gemeente haar beleidsdoelstellingen niet volledig kan realiseren.		
Oorzaak	Oorzaken zijn het tot voor kort ontbreken van een formeel handelingskader voor contractbeheer. Daarnaast heeft ook de impact van de organisatiewijziging voor het I-domein in 2022 en de grote omvang van personeelswisselingen tot gevolg dat overeenkomsten slechts deels beschikbaar zijn. Voor effectieve uitvoering van contractbeheer is het essentieel om te beschikken over de volledige overeenkomst met bijlagen waaruit blijkt welke verdere afspraken zijn gemaakt. Dit soort afspraken is veelal opgenomen in de hoofdtekst van de overeenkomst. En daarnaast is het essentieel om te beschikken over volledige informatie omtrent ontvangen rapportages en wie over deze rapportages beschikt.		
Aanbeveling	Besteed bij de implementatie van het nieuwe handelingskader expliciet aandacht aan de rol van contractbeheer ten aanzien van borging van naleving van contractuele afspraken over levering van overige rapportages zoals op het gebied van duurzaamheid.		
Managementreactie	Wij zullen de aanbevelingen van de auditor hierover opvolgen We zijn bezig met de contract hygiëne op orde te krijgen door het contract- en licentieregister te actualiseren. Dit doen we via A (Actueel), B(Betrouwbaar) en C (Compleet). Dit maakt rapportage als rationalisatie mogelijk. – door ICLM	Q1-Q3 Q3-2024 Follow-up audit: ja/nee	Verantwoordelijke directie: DV

Bijlage 2: Overzicht van gecontroleerde beheersmaatregelen

Symbool	Betekenis
V	Opzet, Bestaan en/of Effectieve Werking is vastgesteld.
O	Opzet, Bestaan en/of Effectieve Werking is gedeeltelijk vastgesteld.
X	Opzet, Bestaan en/of Effectieve Werking is niet vastgesteld.
—	Opzet, Bestaan en/of Effectieve Werking is getoetst.

Risico	Beheersmaatregelen	Regiepartij	SaaSoplossing	Toelichting
R1 Onvoldoende informatiebeveiliging bij de derde partijen waardoor vertrouwelijke gegevens kwetsbaar kunnen zijn voor ongeautoriseerde toegang, verlies of diefstal.	IB1 Uitvoering van een grondige beoordeling van de beveiligingsmaatregelen van leveranciers van SaaS-toepassingen en regiepartijen. Dit aan de hand van door de leveranciers geleverde rapportages.	V	O	**Bevinding 2**
R2 Verlies van controle door overdracht applicatiebeheer aan derden wat kan leiden tot niet volledig aansluiten bij de behoeften en doelstellingen van de gemeente ten aanzien van servicekwaliteit, beschikbaarheid en continuïteit van de dienstverlening.	IB2 In de overeenkomst met bijlagen waaronder de SLA zijn de vereiste kwaliteitsnormen opgenomen waarover de leverancier verantwoording aflegt in periodieke formele rapportages. Dit betreft o.a. kwaliteitsnormen zoals uptime, responsetijden en hersteltijden.	V	O	**Bevinding 3** **Bevinding 6**

Risico	Beheersmaatregelen	Regiepartij	SaaSoplossing	Toelichting
R3 Geen aandacht voor doorontwikkeling en wijzigingenbeheer waardoor de dienstverlening niet toekomstbestendig is.	IB3 Goede inrichting van taken en verantwoordelijkheden van beide partijen in de samenwerking met daarin aandacht voor de vormgeving van doorontwikkeling en wijzigingenbeheer.	V	X	**Bevinding 3** **Bevinding 7** **Bevinding 8**
R4 Leverancier voldoet niet aan gestelde kwaliteitseisen, juridische eisen en compliance eisen.	IB4 Naleving van gemeentelijk beleid t.a.v. o.a. informatiebeveiliging door de leveranciers, geborgd via de contractuele afspraken.	V	X	**Bevinding 2**
R5 Hogere financiële lasten dan begroot.	IB5 Toepassing van contractuele bescherming met in ieder geval afspraken over indexeringen, boeteclausules bij niet leveren van de afgesproken kwaliteit en periodieke herevaluatie van de (financiële) stabiliteit van de leverancier.	V	O	**Bevinding 5**
R6 Onduidelijkheid over contractvoorwaarden kan leiden tot interpretatieverschillen en misverstanden met uiteindelijk gebrekkige naleving.	IB6 Heldere toewijzing van verantwoordelijkheden voor de diverse aspecten van contractmanagement waarbij effectieve uitvoering wordt bevorderd door toepassing van een centraal	V	O	**Bevinding 3**

Risico	Beheersmaatregelen	Regiepartij	SaaSoplossing	Toelichting
	contractbeheersysteem waarin alle contracten voorzien van bijlagen, addenda en verleningsovereenkomsten integraal toegankelijk zijn en ook de door de leverancier geleverde rapportages (SLR's, ISAE 3402-rapportages, ISO-certificaten etc) worden opgenomen.			
R7 Onvoldoende monitoring en opvolging van beveiligingsincidenten waardoor de gemeente langer bloot wordt gesteld aan kwetsbaarheden.	IB7 Handhaving van de afspraken welke in de overeenkomst met bijlagen zijn opgenomen omtrent herstelverplichting (met beperking van toegestane tijdsduur), meldingsplicht en communicatielijnen bij constatering van beveiligingsincidenten.	V	O	**Bevinding 2** **Bevinding 3**
R8 Afhankelijkheid van één leverancier voor uitvoering van wettelijke of overige taken kan leiden tot ernstige verstoringen van de bedrijfsvoering als de leverancier niet aan de verwachtingen voldoet.	IB8 Uitvoeren van periodieke evaluatie van mate van afhankelijkheid van IT-leveranciers, vaststellen van alternatieven (uitwijk, noodherstelplan, vervangende werkwijzen) en uitvoeren van	V	X	**Bevinding 5**

Risico	Beheersmaatregelen	Regiepartij	SaaSoplossing	Toelichting
	regelmatige prestatiebeoordelingen			
R9 Niet of gebrekkige naleving van wet- en regelgeving door derde partijen kan leiden juridische, financiële en reputatieschade voor de gemeente.	IB9 Periodieke herevaluatie van de kwaliteit, compliance en ethische praktijken van de leverancier met toetsing op aanwezigheid van certificaten	V	O	**Bevinding 2** **Bevinding 3**
R10 Niet naleven van gemeentelijk beleid op het gebied van integriteit, duurzaamheid en social return (ethische uitdagingen).	IB10 Monitoring op naleving door de leverancier van de contractuele afspraken op het gebied van integriteit, duurzaamheid en social return (ethische uitdagingen) met waar nodig toepassing van de contractuele clausules t.b.v. de handhaving van contractuele afspraken.	V	O	**Bevinding 4** **Bevinding 9**
R11 Datalekken en onvoldoende borging van de vertrouwelijkheid wat kan leiden tot ongeoorloofde toegang, verlies of diefstal van gevoelige gegevens onder beheer bij derde partijen.	IB11 Toezien op naleving van de contractuele afspraken op het gebied van gegevensbeveiliging en borging van privacy. Deze contractuele afspraken betreffen o.a. implementatie van gegevensversleuteling en goedkeurende assurancerapportages.	V	O	**Bevinding 2**

Risico	Beheersmaatregelen	Regiepartij	SaaSoplossing	Toelichting
R12 Onvoldoende beheersing van leverancierspresteaties en escalatie.	IB12 Handhaving van nakoming van de contractueel overeengekomen prestatie-niveau's door de leverancier.	V	O	**Bevinding 3**
R13 Discontinuïteit van de bedrijfsvoering als gevolg van problemen bij contractpartijen.	IB13 Monitoring en toetsing van de contractuele afspraken op het gebied van borging van continuïteit (back-up en recovery, uitwijk, periodiek testen van restore).	V	O	**Bevinding 3**
R14 Gebrekkige communicatie (soft control).	IB14 Stimuleren van een cultuur van open communicatie waarbij medewerkers worden aangemoedigd om belangrijke informatie te delen en te begrijpen en problemen, zorgen en feedback te delen.	V	O	**Bevinding 3** **Bevinding 7** **Bevinding 9**
R15 Onvoldoende kwaliteitsgerichtheid (soft control), kwaliteitsgerichtheid bevordert hoogwaardige prestaties en resultaten binnen de organisatie.	IB15 opstellen, communiceren en handhaven van duidelijk kwaliteitsnormen en -doelen welke bestaan uit specifieke criteria en meetbare indicatoren.	V	O	**Bevinding 2** **Bevinding 3** **Bevinding 9**
R16 Onvoldoende kostenbewust (soft control) kan leiden tot verminderde efficiëntie en verminderde financiële verantwoordelijkheid.	IB16 Toezien op het behoud van de balans tussen kostenbesparing en kwaliteitsbehoud met o.a. monitoring van prestaties,	V	O	**Bevinding 5**

Risico	Beheersmaatregelen	Regiepartij	SaaSoplossing	Toelichting
	uitvoeren van kwaliteitscontroles en borgen van medeneming van de gevolgen voor de kwaliteit bij het nemen van kostenbesparende besluiten.			