

Rapportage ***Beheer en beveiliging*** ***Negometrix***

Definitief

Deze rapportage bij voorkeur digitaal lezen 
of in kleur printen 

Concerncontrol
Juli 2018



Inhoud

1. Inleiding

1.1 Aandachtsgebieden bij onze audit

2. Wat rapporteren wij per aandachtsgebied?

3. Conclusie en overzicht aanwijzingen en aanbevelingen

3.1 Aanwijzingen

3.2 Aanbevelingen

4. Overzicht bevindingen

4.1 Beheer

4.2 Beveiliging

4.3 Gebruik

Bijlagen

I. Analyse gebruikers Negometrix dd april 2018

II. Lijst geïnterviewden

III. Advies CC compenserende maatregelen

1. Inleiding

Aanleiding voor de audit

In 2017 is Negometrix (NM) in gebruik genomen door de organisatie. Het systeem wordt als aanbesteding ondersteunend systeem gebruikt door het domein Bedrijfsvoering (o.a. de sector FAO) het Sociaal Domein en in het Ruimtelijk domein door de sector MVS. Binnen het SD wordt NM daarnaast ook nog als contractmanagementsysteem gebruikt.

Concerncontrol ziet een aantal risico's op het gebied van beheersing van Negometrix en vindt het van belang deze in beeld te brengen richting direct betrokkenen, zodat we gezamenlijk kunnen bekijken waar we de organisatie en het beheer kunnen verbeteren (lerende organisatie). Het doel van de audit op Negometrix is derhalve aanvullende zekerheid te verkrijgen over de beheersing van de risico's die samenhangen met het gebruik van deze applicatie.

Aandachtspunten tijdens de audit liggen in eerste instantie op het gebied van:

- Eigenaarschap in de breedste zin van het woord (applicatie en gegevens), rollen en verantwoordelijkheden;
- Contracten en overeenkomsten;
- Data/AVG
- Beveiliging (onder andere logische toegangsbeveiliging, application controls, autorisatiebeheer, logging, documentatie, wijzigingsbeheer);
- Continuïteit;
- Gegevensoverdracht (koppelingen).

Scope

Negometrix, hierbij hebben we de koppeling met Suites betrokken.

Volledigheidshalve benadrukken we dat de functionaliteit van Negometrix buiten de scope van ons onderzoek valt. Deze is niet door ons onderzocht.

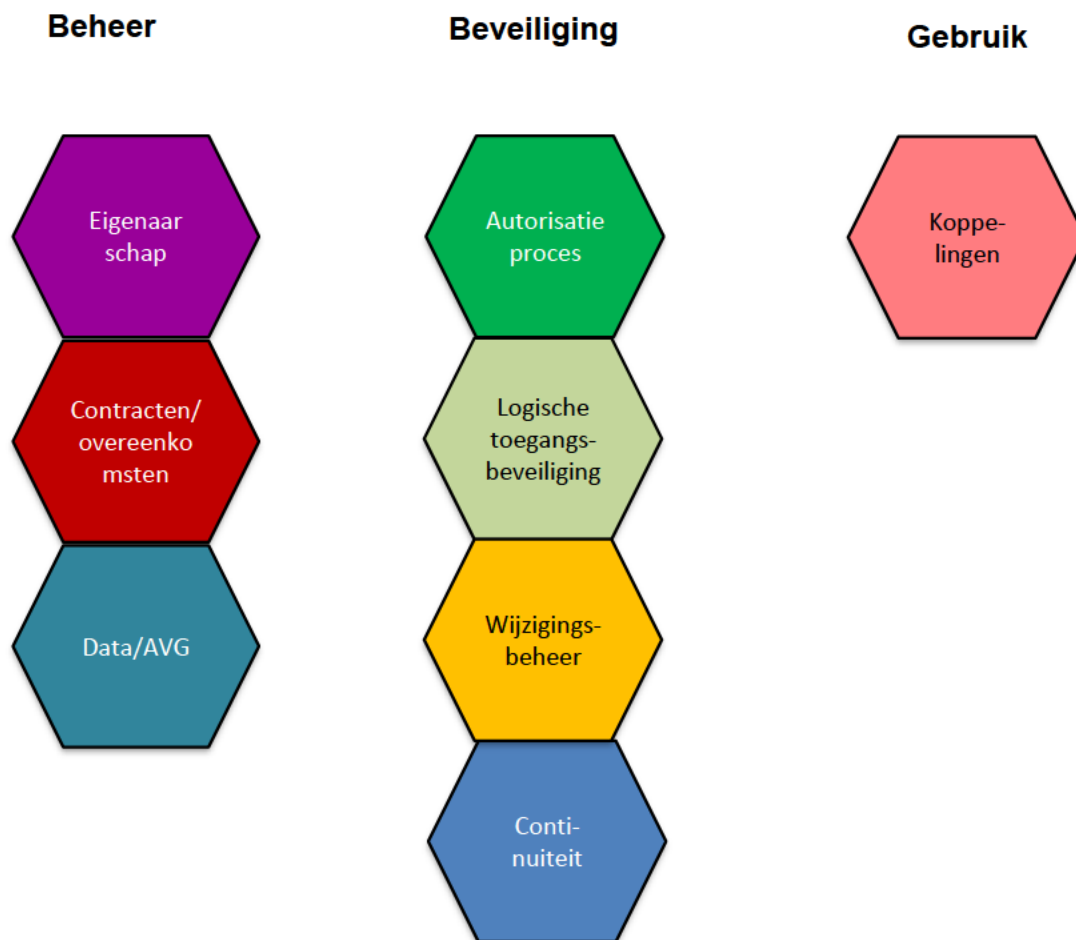
Gehanteerde criteria

Voor het onderzoek hebben wij een normenkader opgesteld gebaseerd op de geldende standaarden voor de inrichting en het beheer van applicaties. Dit normenkader is op te vragen bij Concerncontrol.

Aanpak

- De werkzaamheden zijn uitgevoerd op basis van documentenonderzoek en interviews met betrokken medewerkers;
- De uitkomsten van de audit zijn afgestemd met de direct betrokken medewerkers, de CPO en sectorhoofden van FAO en I&B;
- De definitieve rapportage wordt uitgebracht aan de DR en de sectorhoofden FAO, I&B, de directeur Sociaal Domein en de CIO. De aanwijzingen uit deze rapportage zullen ook in de periodieke CC rapportage worden gerapporteerd aan de Directieraad.

1.1 Aandachtsgebieden bij onze audit



2. Wat rapporteren wij per aandachtsgebied?

Bevinding De bevindingen die we hebben voor het betreffende aandachtsgebied	Onderwerp Het onderwerp dat extra aandacht vereist binnen het aandachtsgebied
Sterke punten Volgens ons is dit een werkwijze die als voorbeeld kan dienen voor de organisatie/het proces/het project.	Verbeterpunten Volgens ons is dit een punt waarop het proces verbetering behoeft en/of kan leren van andere sectoren.
Reactie verantwoordelijke De reactie van de verantwoordelijke op de aanbeveling.	Zaken die niet worden genoemd Dit rapport betreft een uitzonderings-rapportage. Indien in dit rapport niet wordt ingegaan op zaken die in hoofdstuk 1 als aandachtspunt zijn genoemd, hebben wij hierbij geen zwaarwegende bevindingen.
Aanwijzing of aanbeveling? <ul style="list-style-type: none">• Aanwijzingen: dit zijn dusdanige tekortkomingen die wij tevens aan de directieraad rapporteren.• Aanbevelingen: hierbij heeft het sector/project of procesmanagement vanuit zijn verantwoordelijkheid voor het beheer binnen de sector de vrijheid om te beslissen of een aanbeveling wordt opgevolgd of dat andere maatregelen worden getroffen om het gesignaleerde risico te beperken.	

3. Conclusie en overzicht aanwijzingen en aanbevelingen

Samenvatting bevindingen

De bevindingen ten aanzien van de inrichting en het gebruik van Negometrix (NM) zijn verontrustend. Veel basale onderwerpen op het gebied van beheersing van een webapplicatie zijn niet of onvoldoende geregeld of er is niet te achterhalen of en hoe ze zijn geregeld. Door de veranderingen in het Sociaal Domein is Negometrix als pilot daar begonnen. Vervolgens is nagelaten de pilot te evalueren en op normale wijze in productie te brengen. Ook niet bij uitbreiding van het gebruik door FAO en door MVS.

Er is geen eigenaar die verantwoordelijk is voor regie en sturing op de inrichting van de applicatie. Documentatie ontbreekt; zelfs een essentieel document als een contract is niet gevonden. Hierdoor hebben we geen inzicht in de afspraken hierover en hoe de leverancier met onze gegevens omgaat (o.a. waar staan de gegevens, worden ze gebackupped, wie hebben er toegang toe).

Er zijn geen acties uitgevoerd in het kader van de Algemene Verordening Gegevensbescherming (AVG).

Het intern autorisatieproces en de autorisaties worden momenteel opnieuw ingericht maar dit is nog niet op orde. Ook de logische toegangsbeveiliging voldoet niet aan de daar aan te stellen eisen. De logging is zeer beperkt en geeft onvoldoende inzicht in wat er gebeurt in de applicatie.

Gezien onze bevindingen zijn de risico's van het gebruik van Negometrix dusdanig hoog dat de voorgestelde verbeterpunten met prioriteit moeten worden gerealiseerd.

Daarnaast is een belangrijke vraag die de organisatie zich moet stellen: “hoe voorkomen we situaties als deze in de toekomst en hoe signaleren we dit eerder?”. Het moet niet mogelijk zijn om een dusdanig essentieel proces als inkoop te ondersteunen met een pakket zonder dat de standaardprocedures voor inkoop voor een IT-applicatie worden gevolgd.

Volledigheidshalve benadrukken we dat de uitkomsten van dit onderzoek niks zeggen over de functionaliteit van Negometrix maar gaan uitsluitend over het beheer, de beveiliging en de koppeling met Suites.

Conclusie

Om de betrouwbaarheid en rechtmatigheid van het aanbestedings- en contractproces in Negometrix te waarborgen en vast te kunnen stellen zijn aanvullende beheersmaatregelen per direct noodzakelijk.

3.1 Aanwijzingen

Nr.	Aandachtsgebied	Aanwijzing
1	overkoepelend	Geef sectorhoofd I&B de opdracht om gemeentebrede afspraken met betrekking tot de aanschaf van applicaties onder de aandacht te brengen en toe te zien op de naleving ervan.
2	overkoepelend	Geef sectorhoofd I&B de opdracht om actief te monitoren of er applicaties worden gebruikt die buiten I&B om zijn aangeschaft.
3	overkoepelend	Geef sectorhoofd I&B de opdracht om periodiek na te gaan van alle applicaties of ze voldoen aan de minimale eisen mbt beheer (in brede zin) en beveiliging
4	overkoepelend	Geef de CIO opdracht om voor 1 januari 2019 gemeentebrede afspraken met betrekking tot eigenaarschap van applicaties vast te leggen en vast te laten stellen door DR/DSO.
5	eigenaarschap	Geef sectorhoofd FAO opdracht om een risicoanalyse Negometrix uit te voeren en de noodzakelijke maatregelen te treffen en tot die tijd het gebruik van Negometrix te bevriezen (dwz geen nieuwe data toe te voegen aan Negometrix).
6	eigenaarschap	Geef sectorhoofd FAO de opdracht om per direct binnen de sector FAO een eigenaar aan te wijzen voor de applicatie Negometrix en uitvoering te geven aan de bijbehorende taken.
7	eigenaarschap	Geef sectorhoofd I&B de opdracht om per direct de capaciteit voor het uitvoeren van de Functioneel Beheertaken voor Negometrix af te stemmen op de hoeveelheid werk die moet worden uitgevoerd.
8	Contracten/ overeenkomsten	Geef het sectorhoofd I&B opdracht om zo snel mogelijk een gedegen contract af te sluiten met Negometrix waarin afspraken worden gemaakt over voor Cloud applicaties relevante aspecten. Maak waar mogelijk gebruik van de ervaringen van andere gemeenten hiermee.
9	Data/AVG	Geef, via sectorhoofd FAO, de eigenaar van NM opdracht om per direct na te gaan welke acties in het kader van de AVG moeten worden genomen en een plan op te stellen hoe hieraan uitvoering te geven.

3.1 Aanwijzingen

Nr.	Aandachtsgebied	Aanwijzing
10	Autorisatieproces	Geef het sectorhoofd I&B de opdracht om het autorisatieproces Negometrix in te richten conform de eisen van de organisatie.
11	Logische toegangsbeveiliging	Geef sectorhoofd I&B (functioneel beheer NM) de opdracht voor 1 december 2018 de logische toegangsbeveiliging van Negometrix in te richten conform de eisen van de organisatie.

3.2 Aanbevelingen

Nummer	Aandachtsgebied	Aanbeveling
1	wijzigingsbeheer	Geef sectorhoofd I&B (FB Negometrix) de opdracht om voor 1 december 2018 het wijzigingsbeheer in te richten voor Negometrix.

4. Bevindingen en aanbevelingen

Overkoepelende bevindingen

Tijdens een onderzoek (in dit geval naar de beheersing van Negometrix) vallen soms ook dingen op die niet specifiek betrekking hebben op de betreffende applicatie maar die gelden voor andere applicaties of processen of de hele gemeentelijke organisatie. Tijdens het onderzoek naar Negometrix is ons opgevallen dat ondanks gemeentebrede afspraken omtrent het aanschaffen van applicaties met bijbehorende waarborgen dat een applicatie voldoet aan bepaalde eisen, Negometrix toch is aangeschaft en draait binnen de organisatie. Dit zonder dat aan de minimale eisen rondom beheersing en beveiliging wordt voldaan, met alle risico's van dien. Als een dergelijk proces heeft plaatsgevonden wordt achteraf ook onvoldoende geverifieerd of aan de eisen wordt voldaan en zo nodig bijgestuurd.

Er is veel onduidelijkheid en hieruit voortkomend onenigheid over waar het eigenaarschap van applicaties is belegd en wat dit inhoudt.

Onderwerp	Verbeterpunten
Grip op aanschaf applicaties ontbreekt	Breng afspraken over aanschaf van applicaties onder de aandacht en monitor hier actief op.
	Ga periodiek na of alle bekende applicaties voldoen aan de minimale eisen op het gebied van beheer en beveiliging.

Aanwijzing 1

Geef sectorhoofd I&B de opdracht om gemeentebrede afspraken met betrekking tot de aanschaf van applicaties onder de aandacht te brengen en toe te zien op de naleving ervan en waar nodig te escaleren richting DSO-overleg.

Reactie sector I&B

Eens dat het belangrijk is dat dit onder de aandacht wordt gebracht. Sector I&B heeft dit reeds vaak gecommuniceerd en waar nodig uitgelegd. Dit in navolging en overeenstemming met het vigerende inkoopbeleid en mandaatbesluit inzake de aanschaf van ICT. Daar waar de sector I&B constateert dat er afwijkingen plaatsvinden of hebben plaatsgevonden, zal I&B in gesprek gaan met deze verantwoordelijke opdrachtgever. Indien nodig, of bij herhaling, zal escalatie / opschaling plaatsvinden naar de directeur Bedrijfsvoering.

4. Bevindingen en aanbevelingen

Overkoepelende bevindingen

Aanwijzing 2

Geef sectorhoofd I&B de opdracht om actief te monitoren of er applicaties worden gebruikt die buiten I&B om zijn aangeschaft.

Reactie sector I&B

Conform mandaatbesluit moet alle aanschaf van ICT middelen via de sector I&B lopen en dit geldt dus ook onverminderd voor de aanschaf van applicaties door de sector FAO. Sector FAO kan dus niet zelf applicaties aanschaffen.

Daar waar wordt gesignaleerd dat er aanschaf plaatsvindt / heeft plaatsgevonden buiten de sector I&B om, onderneemt de sector I&B actie (zie vorige reactie op aanwijzing 1). Actief monitoren is zeker een optie. Bij de implementatie van het inkoop ondersteunend systeem (IOS) gaan we dit meenemen. Feitelijk wordt hier gevraagd dat de gemandateerde gevraagd wordt om het aan hem / haar verstrekte mandaat te monitoren / toetsen. Deze toetsing zou in eerste instantie en primair moeten plaatsvinden door de verstrekker van het mandaat. Dit geldt niet alleen voor dit mandaat maar voor alle mandaten.

Aanwijzing 3

Geef sectorhoofd I&B de opdracht om periodiek na te gaan van alle applicaties of ze voldoen aan de minimale eisen mbt beheer (in brede zin) en beveiliging

Reactie sector I&B

Wanneer het inkoopbeleid van de gemeente Eindhoven wordt gevolgd door alle betrokkenen, vindt er tijdens de intake bij I&B een toetsing plaats aan de hand van acceptatiecriteria. Deze acceptatiecriteria zijn opgesteld / gedefinieerd en gelden voor zowel on premise als SaaS oplossingen.

Met betrekking tot de minimale eisen van beheer volgt I&B de Baseline Informatiebeveiliging Gemeenten (BIG), het hieruit voortvloeiende informatiebeveiligingsbeleid van de gemeente Eindhoven en beschikbaar aanvullend beleid (kaders / richtlijnen) van de CISO.

Er voor zorgen dat er ook na initiële implementatie aan deze eisen wordt voldaan maakt onderdeel uit van de werkzaamheden van service delivery management, functioneel en technisch beheer.

Sectorhoofd I&B stelt voor om in overleg met CC een plan van aanpak op te stellen voor periodieke toetsing van met name de bedrijfskritische applicaties.

4. Bevindingen en aanbevelingen

Overkoepelende bevindingen

Er is veel onduidelijkheid en hieruit voortkomend onenigheid over waar het eigenaarschap van applicaties is belegd en wat dit inhoudt. Een vaak voorkomend misverstand is dat I&B eigenaar is van de applicaties terwijl eigenaarschap gezien de benodigde kennis van de processen die door de applicatie worden ondersteund thuishoort bij de lijn-/gebruikersorganisatie. De aanschaf van applicaties dient conform mandaat via de sector I&B plaats te vinden. Maar dit mandaat tot aanschaf staat los van het eigenaarschap van de applicatie en de gegevens die er in vastgelegd worden.

Onderwerp	Verbeterpunten
Eigenaarschap applicaties	Leg duidelijk vast waar eigenaarschap van applicaties wordt belegd en wat dit eigenaarschap inhoudt en laat dit vaststellen door het DR/DSO overleg.

Aanwijzing 4

Geef de CIO opdracht om voor 1 januari 2019 gemeentebrede afspraken met betrekking tot eigenaarschap van applicaties vast te leggen en vast te laten stellen door DR/DSO.

Reactie hoofd CIO

Akkoord na enkele (reeds verwerkte) tekstuele aanpassingen in de rapportage en onderstaande toelichting.

“Door de introductie van Negometrix door het Sociaal Domein als enige gebruiker, ligt het voor de hand dat Sociaal Domein in eerste instantie als eigenaar kan worden aangewezen. Die rol is onvoldoende waar gemaakt. Door de uitbreiding van het gebruik door andere sectoren vervaagt de eigenaarsrol. “

4.1 Beheer

Eigenaarschap

Overzicht bevindingen

Eigenaarschap in brede zin, dat wil zeggen van de applicatie en de data en de rollen en verantwoordelijkheden, is niet geregeld binnen Negometrix (NM): zowel voor de data als voor de applicatie is er geen eigenaar aangewezen. Hierdoor ontbreekt inzicht in de risico's van het gebruik van Negometrix en de regie en sturing op inrichting en gebruik van Negometrix binnen de organisatie.

Onderwerp	Verbeterpunten
Geen inzicht in risico's verbonden aan het gebruik van NM	Ga na welke risico's verbonden zijn aan het gebruik van NM en tref maatregelen om deze te beheersen.
Geen regie op inrichting en gebruik NM door ontbrekend eigenaarschap voor de applicatie NM	Beleg het eigenaarschap voor Negometrix (bij voorkeur bij de afdeling Inkoop van de sector FAO) en geef uitvoering aan de bijbehorende taken.

Aanwijzing 5

Geef sectorhoofd FAO opdracht om voor 1 december 2018 een risicoanalyse Negometrix uit te voeren en de noodzakelijke maatregelen te treffen en tot die tijd het gebruik van Negometrix te bevriezen (dwz geen nieuwe data toe te voegen aan Negometrix).

Reactie sector FAO

FAO is per direct gestopt met NM. Behalve lopende aanbestedingen, deze maken we nog in NM af en zorgen daarna dat alle dossiers binnen NM verplaatst wordt naar Edocs. Reden hiervoor is dat wij geen overtuigend toegevoegde waarde zien t.o.v. van Tenders. Bovendien is deze laatste tool gratis en NM niet. Het voornemen om te stoppen met NM heeft impact op het Sociaal Domein. Als FAO stopt met het gebruik van NM en het Sociaal Domein niet, dan zal het Sociaal Domein als hoofdgebruiker verantwoordelijk worden voor het gebruik van Negometrix en daarmee ook voor het doorvoeren van eventuele verbeteringen zoals benoemd in voorliggende rapportage. Dit komt voort uit de verdeling van verantwoordelijkheden voor ICT-tools, zoals gebruikelijk is in Eindhoven (waarvan volgens ons de vraag is of die daadwerkelijk zo is vastgelegd). Wij willen met de directeur en Leadbuyer van het Sociaal Domein in overleg om te kijken naar de mogelijkheden om te stoppen met de applicatie en hoe een overgang naar een ander systeem zo soepel mogelijk kan verlopen. Gelet op de uitdagingen binnen het Sociaal domein en de afhankelijkheid die zij hebben met het systeem NM verwachten wij geen actie op korte termijn. (Bovendien maken wij een onderscheid tussen bestuurlijk aanbesteden en aanbestedingsprocedure. Bestuurlijk aanbesteden is geen term of aanbestedingsprocedure. Het is verzamelterm voor de inkoop van voorzieningen in het sociaal domein. Waarbij onze invloed vanuit centraal inkoop gering is.

4.1 Beheer

Eigenaar-
schap

Reactie sector I&B vervolg

I&B heeft afstemming gezocht met het Sociaal domein over het mogelijk bevriezen van Negometrix. Hieruit blijkt dat Negometrix voor het Sociaal Domein van cruciaal belang is bij de uitvoering van de aan de Raad voorgelegde invoering van contract wijzigingen die per 1 januari 2019 operationeel moeten zijn. Dat betekent dat de tender op 1 november as. open moet om e.a. nog te kunnen verwerken. In de aandachtsvelden wordt gesproken over bevriezen van data tot 1 december, dat is daarmee niet mogelijk.

Ook 2019 zal in het teken staan van contractaanpassingen en gewijzigde inkoopstrategie waarbij Negometrix als middel wordt ingezet. Mocht worden overwogen om te komen tot uitfasering van deze tool dan zal dit in nauw overleg met de huidige gebruikersorganisatie dienen plaats te vinden.

Samenvattend: Negometrix is cruciaal voor het Sociaal Domein iedere wijziging leidt tot een directe bedreiging voor de bedrijfsvoering. Als zaken aanvullende maatregelen vragen zullen we dat in gezamenlijkheid op haalbaarheid en impact moeten beoordelen.

Vervolgreactie Concerncontrol tav aanvullende maatregelen

Als reactie hierop heeft Concerncontrol geadviseerd over compenserende maatregelen. Deze zijn opgenomen in Bijlage 3.

Aanwijzing 6

Geef sectorhoofd FAO de opdracht om per direct binnen de sector FAO een eigenaar aan te wijzen voor de applicatie Negometrix en uitvoering te geven aan de bijbehorende taken.

Reactie sector FAO

Gezien bovenstaand voornemen, is dit niet van toepassing. Overigens hebben wij het gebruik inmiddels deels bevroren

4.1 Beheer

Eigenaar-
schap

Overzicht bevindingen vervolg

Recentelijk is vanuit I&B een functioneel beheerder (FB) aan NM toegewezen. Deze FB is nog bezig met het opbouwen van kennis over de applicatie en het herinrichten van de applicatie. FB heeft 0,75 fte in de week beschikbaar voor het uitvoeren van de bijbehorende taken. Gezien onze bevindingen tijdens deze audit is dit veel te weinig.

Onderwerp	Verbeterpunten
Onvoldoende capaciteit voor het uitvoeren van beheer op NM	Zorg voor voldoende capaciteit voor het uitvoeren van de beheertaken van Negometrix.

Aanwijzing 7

Geef sectorhoofd I&B de opdracht om per direct de capaciteit voor het uitvoeren van de Functioneel Beheertaken voor Negometrix af te stemmen op de hoeveelheid werk die moet worden uitgevoerd.

Reactie sector I&B

De aanschaf van Negometrix heeft niet het vastgestelde en inkoopproces doorlopen. Hierdoor is er onvoldoende aandacht geweest voor de kwaliteit van het beheerproces. Hierdoor is er een incidentele beheerlast ontstaan a.g.v. achterstanden welke moet worden weggewerkt. Deze extra capaciteitsvraag moet alsnog worden geprioriteerd, de huidige beschikbare formatie (0,45 fte) wordt echter als wel als voldoende gezien m.b.t. regulier functioneel beheer en ook voor het op korte termijn wegwerken van de openstaande issues.

4.1 Beheer

Contracten
en overeen-
komsten

Overzicht bevindingen

Er is geen contract met NM beschikbaar. De Service Level Agreement en Licentieovereenkomst zijn wel aangeleverd maar niet actueel.

Er zijn geen afspraken gemaakt over een Third Party Mededeling (TPM) verklaring waarin door een onafhankelijke derde wordt getoetst of een leverancier zich houdt aan de gemaakte (beveiligings)afspraken.

Omdat een contract ontbreekt is onder andere niet bekend:

- de logische toegangsbeveiliging en autorisaties van de leverancier;
- over de wijze waarop de data door de leverancier worden gebackupped en worden hersteld (recovery) indien noodzakelijk.
- waar de servers met de applicatie en de gegevens zich fysiek bevinden. Ook over de fysieke beveiliging bij de leverancier is niets bekend.
- In hoeverre de leverancier voldoet aan de privacy voorschriften uit de AVG.
- Of er afspraken zijn over eigenaarschap van de data en hoe er wordt gehandeld (bijv. inzake overdracht van data) in geval van beëindiging van het contract;

Aangezien deze informatie ontbreekt is het niet mogelijk in te schatten of en zo ja in welke mate de organisatie risico's loopt en of de getroffen maatregelen voldoen aan de daar aan te stellen minimale eisen.

Onderwerp	Verbeterpunten
Contract, SLA en licentieovereenkomst niet actueel en niet volledig.	Zorg voor een actueel en goed contract, SLA en licentieovereenkomst. Maak zo nodig afspraken over een TPM-verklaring om zeker te zijn dat de afspraken uit het contract worden nageleefd door de leverancier.


Aanwijzing 8

Geef het sectorhoofd I&B opdracht om zo snel mogelijk een gedegen contract af te sluiten met Negometrix waarin afspraken worden gemaakt over voor Cloud applicaties relevante aspecten. Maak waar mogelijk gebruik van de ervaringen van andere gemeenten hiermee.

Reactie sector I&B

De zorg omtrent het ontbreken van een actueel en goed contract onderschrijven wij. Echter zien wij hier, op basis van de reeds gedane uitgaven (160k), in het kader van de rechtmatigheid niet direct mogelijkheden voor en zou dit in strijd zijn met de inkoopstrategie / inkoopbeleid van de gemeente v.w.b. het rechtmatig inkopen. Nadere afstemming met de eigenaar is hierin noodzakelijk.

4.1 Beheer



Contracten
en overeen-
komsten

Reactie sector I&B - vervolg

Sector FAO heeft aangegeven per direct te stoppen met het gebruik van Negometrix. Zie reactie sectorhoofd FAO. Hierdoor wordt Sociaal Domein Inkoop de enige gebruiker. Omdat de bestuurlijke aanbestedingen hierin zijn ondergebracht blijft Negometrix voor het Sociaal Domein (tot in 2020) voorlopig nog in gebruik. Uitgangspunt is dat door het afsluiten van een nieuw contract geen onrechtmatigheid mag ontstaan. De aanbestedingsjurist zal hierbij worden betrokken.

Reactie CIO

De leverancier is overigens marktleider in zijn segment, stelt op zijn website aan alle relevante eisen te voldoen en onder andere defensie is bij hun klant. Daarmee is de verwachting dat de meeste beveiligingszaken wel geregeld zullen zijn, alleen weten we dat niet zeker en hebben we er ook geen afspraken over gemaakt.

4.1 Beheer

Data/AVG

Overzicht bevindingen

Negometrix bevat vertrouwelijke data omtrent aanbestedingen (aanbieders, prijzen, contracten). Onbekend is wie bij de leverancier allemaal toegang hebben tot deze data. Aangezien Negometrix ook door veel andere partijen (in binnen- en buitenland) wordt gebruikt beschikt de leverancier hiermee over voor derden zeer interessante (markt)informatie.

Er is niets geregeld over hoe de gemeente de eigen data (waaronder de contracten in het Sociaal Domein) terugkrijgt in geval van overstap naar een andere leverancier of faillissement van Negometrix. De vraag is of er überhaupt afspraken zijn gemaakt over eigenaarschap van de data.

Binnen de organisatie is niet bekend in hoeverre er voor Negometrix (NM) iets geregeld is of nog moet worden in het kader van de AVG. Hierdoor is niet duidelijk of er bijvoorbeeld een verwerkersovereenkomst of een Privacy Impact Assessment moet worden uitgevoerd.

Onderwerp	Verbeterpunten
Niets geregeld in het kader van de AVG	Ga na of er in het kader van de AVG dingen moeten worden geregeld (zowel aan de kant van de gemeente als aan de kant van de leverancier)
Niets geregeld over overdracht van data bij einde contract	Maak afspraken met de leverancier over eigenaarschap van de data en over overdracht van gegevens aan het einde van het contract (zie Aanwijzing 6).

Aanwijzing 9

Geef, via sectorhoofd FAO, de eigenaar van NM opdracht per direct na te gaan welke acties in het kader van de AVG moeten worden genomen en een plan op te stellen hoe hieraan uitvoering te geven.

Reactie sector FAO

I&B is bezig met het opstellen van een verwerkersovereenkomst met Negometrix. Naar verwachting wordt deze binnenkort ondertekend door de mandaathouder I&B.

4.2 Beveiliging

Autorisatie
proces

Overzicht bevindingen

Het autorisatieproces wordt op dit moment door FB opnieuw ingeregeld maar was ten tijde van het onderzoek nog niet op orde. De autorisatietabel is niet actueel en autorisaties zijn te ruim ingesteld (zie bijlage I). Het is niet met 100% zekerheid te zeggen maar het lijkt er op dat medewerkers van buiten de eigen organisatie toegang hebben tot interne (vertrouwelijke) aanbestedingsinformatie. Daarnaast is onbekend hoeveel medewerkers bij de leverancier toegang hebben tot deze (vertrouwelijke) aanbestedingsinformatie. Gezien het feit dat Negometrix een beleid heeft dat alle eigen medewerkers voor de Helpdesk werken is dit waarschijnlijk een groot aantal mensen. Kennis en inzicht ontbreken momenteel nog. Binnen de eigen organisatie hebben twee functioneel beheerders vergevorderde rechten. Er is geen logging en controle op het gebruik van deze rechten. Ook bij de leverancier zijn er gebruikers met vergevorderde rechten in ons deel van NM, onbekend is hoeveel gebruikers dit zijn en of er controle is op het gebruik van deze rechten.

Onderwerp	Verbeterpunten
Het autorisatieproces is onvoldoende ingeregeld.	Vergaar kennis over mogelijkheden voor autorisatiebeheer binnen Negometrix. Stel op basis hiervan een autorisatiematrix op met verschillende profielen en hanteer hierbij het “need to know” principe van minimale noodzakelijke autorisaties.
	Schoon de autorisatietabel op conform de hierboven beschreven autorisatiematrix. Besteed extra aandacht aan rechten van externe medewerkers (incl. de leverancier).
	Richt een autorisatieprocedure in om de autorisaties actueel te houden. Leg een link met de joiners/movers/leavers procedure.
Vergevorderde rechten	Ga na welke (vergevorderde) rechten de leverancier heeft en hoe wordt toegezien op het gebruik hiervan. Richt intern een proces in (incl. logging) om het toekenning en gebruik van deze rechten te controleren.

Aanwijzing 10

Geef het sectorhoofd I&B de opdracht om voor 1 december 2018 het autorisatieproces Negometrix in te richten conform de eisen van de organisatie.

Reactie sector I&B

Het autorisatieproces berust in hoge mate op het beleid omtrent informatiebeveiliging en het nog in ontwikkeling zijnde beleid m.b.t. identiteits – en toegangsbeheer.

4.2 Beveiliging

Autorisatie
proces

Reactie sector I&B - vervolg

Dit beleid is nog in voorbereiding en moet nog worden vastgesteld. Nieuw beleid zal zeker gevolgen hebben en zal geïmplementeerd moeten worden. Zonder beleid is het voor I&B niet mogelijk "om in te richten conform de eisen van de organisatie." Die worden immers bepaald door het nog vast te stellen beleid.

Dit betekent niet dat we niet gaan doen wat kan

Volgende punten zijn reeds opgepakt / afgerond:

- Kennis autorisatiebeheer is inmiddels aanwezig
- Op basis van functies / werkzaamheden zijn (voor SD) gebruikersrollen en groepen ingericht. Rechten worden toegekend aan gebruikersgroepen i.p.v. aan medewerkers.
- De autorisatietabel is voor interne / externe gebruikers opgeschoond, o.b.v. last logon date zijn betreffende accounts op inactief gezet.
- Vraag wordt uitgezet bij Negometrix welke medewerkers bij leverancier welke rechten hebben

4.2 Beveiliging

Logische
toegangs
beveiliging

*** en

Overzicht bevindingen logische toegangsbeveiliging

Negometrix is een webapplicatie en bereikbaar vanaf elke locatie. Dit is noodzakelijk omdat ook vanuit de regiogemeenten mensen autorisaties hebben. Hierdoor is een goede logische toegangsbeveiliging extra belangrijk.

De logische toegangsbeveiliging van Negometrix is onvoldoende. De wachtwoordinstellingen voldoen weliswaar aan de minimale

[Redacted text block]

Onderwerp	Verbeterpunten
Logische toegangsbeveiliging is niet goed geregeld	Verbeter de instellingen mbt logische toegangsbeveiliging en zie actief toe op de toegang tot en het gebruik van Negometrix.

Aanwijzing 11

Geef Sectorhoofd I&B (functioneel beheer NM) de opdracht voor 1 december 2018 de logische toegangsbeveiliging van Negometrix in te richten conform de eisen van de organisatie.

Reactie sector I&B

De wachtwoordinstellingen kunnen niet door de functioneel beheerder zelf worden gewijzigd / aangepast. In opdracht van functioneel beheerder zijn de wachtwoordinstellingen inmiddels wel aangescherpt / doorgevoerd door Negometrix. Verdere aanscherping wordt momenteel onderzocht. Zie ook de reactie bij aanwijzing 10.

4.2 Beveiliging

Wijzigings-
beheer

Overzicht bevindingen wijzigingsbeheer

Negometrix is een SAAS-oplossing. Dit betekent dat updates automatisch vanuit Negometrix worden geïnitieerd. De gemeente ontvangt na een update bericht van de leverancier dat wijzigingen zijn doorgevoerd. Gebruikers kunnen zich vooraf laten informeren door zich te abonneren op de nieuwsbrief van Negometrix. Het is niet duidelijk of alle gebruikers dit abonnement hebben.

Er wordt binnen de organisatie niet gecommuniceerd over aankomende wijzigingen of nagegaan welke invloed wijzigingen hebben op bestaande werkwijzen/processen.

Er wordt niet getest door de gemeente. Alle testen worden door Negometrix uitgevoerd.

De ontwikkelorganisatie van Negometrix bevindt zich in Bulgarije. Contacten verlopen via een Nederlandse Helpdesk.

In het kader van regionale samenwerking binnen het SD neemt de gemeente deel aan het regionale gebruikersoverleg van Negometrix. Vanuit dit overleg worden soms wijzigingen aangevraagd bij Negometrix. De gemeente heeft weinig invloed op de planning van Negometrix en of wijzigingen worden doorgevoerd.

Binnen Eindhoven zelf is er geen gebruikersoverleg Negometrix.

Onderwerp	Verbeterpunten
Wijzigingsbeheer is niet geregeld	Richt een intern wijzigingsproces in waarbij beoordeeld wordt wat de gevolgen zijn van de door Negometrix aangekondigde wijzigingen voor de bestaande werkwijze. Bespreek dit in een intern gebruikersoverleg.

Aanbeveling 1

Geef sectorhoofd I&B (FB Negometrix) de opdracht om voor 1 december 2018 het wijzigingsbeheer in te richten voor Negometrix.

Reactie sector I&B

Momenteel wordt er gewerkt aan het inrichten van het wijzigingsproces (via Topdesk) voor Negometrix.

Gezien het stoppen door de sector FAO met het gebruik van Negometrix is een intern gebruikersoverleg niet meer relevant.

4.3 Gebruik

Koppe-
lingen

Overzicht bevindingen wijzigingsbeheer

Negometrix heeft koppelingen met Suites, Steunwijzer en het WIJ portaal. Alleen de koppeling met Suites is in ons onderzoek betrokken. Deze koppeling vindt plaats door middel van een export. De export wordt door NM op een beveiligde server afgeleverd en dan door databasebeheer Suites met scripts ingelezen in een database van waaruit deze in Suites wordt ingelezen. Voordat de export in Suites wordt ingelezen wordt een vergelijking van de oude en nieuwe versie van het exportbestand gemaakt en vervolgens gecontroleerd (oa. onbekende aanbiederscode, fout in AGB-code, wijzigingen in IBAN, wijziging in NAW gegevens en wijziging NAW gegeven crediteuren) door SD/Inkoop en Steunwijzer.

Als er geen problemen uit de controle komen worden de gegevens mbv een script ingelezen in Suites. Er is geen melding dat het inlezen goed is gegaan. Binnen Suites is zichtbaar dat een mutatie afkomt van NM (virtuele gebruiker NM).

Sterk punt

Zichtbaar vastgelegde controle op de export uit Negometrix voordat deze wordt ingelezen in Suites.

Onderwerp	Verbeterpunten
Handmatige koppeling tussen Negometrix en Suites brengt risico's met zich mee.	Een handmatige koppeling brengt het risico van fouten met zich mee. Een geautomatiseerde koppeling heeft de voorkeur.

Bijlagen

- I. Analyse autorisaties in
Negometrix dd april 2018**
- II. Lijst geïnterviewden**
- III. Advies CC compenserende
maatregelen**

I. Analyse autorisaties Negometrix dd april 2018

*** en

Gebruikersprofielen			
herkomst e-mailadres		aantal	
[redacted]		[redacted]	
[redacted]		[redacted]	
[redacted]		[redacted]	
[redacted]		[redacted]	
bevinding		aantal	
[redacted]		[redacted]	
[redacted]		[redacted]	
[redacted]		[redacted]	
[redacted]		[redacted]	
Laatste login		Aantal	Aantal status actief
voor 2017		[redacted]	[redacted]
in 2017		[redacted]	[redacted]
2018		[redacted]	[redacted]
geen login (veld leeg)		[redacted]	[redacted]
totaal		[redacted]	[redacted]

II. Lijst geïnterviewden

Naam	Functie	Sector
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

III. Advies CC compenserende maatregelen

*** en

Advies Concerencontrol inzake compenserende maatregelen

[Redacted text block containing multiple paragraphs of text, all obscured by black bars.]

III. Advies CC compenserende maatregelen

*** en

Advies Concerncontrol inzake compenserende maatregelen - vervolg

[Redacted text block containing multiple lines of blacked-out content]