Rapportage behoefteonderzoek cloudondersteuning

Enquête onder gemeenten

Vereniging van Nederlandse Gemeenten

Nassaulaan 12
2514 JS Den Haag

Auteurs: Geeske Logtmeijer, Paula Graafland, Pieter-Bas Nederkoorn
Datum: 17 maart 2023

Versie	Datum	Auteur	Belangrijkste wijzigingen
0.1	17-03-2023	Geeske Logtmeijer	Initiële versie
0.2			
1.0			

Inhoud

1. Aanleiding en probleemstelling

Digitalisering is explosief gegroeid: dat vraagt onder andere flexibilisering in opschaling, meer kennis van beheer, hogere eisen aan beveiliging. Daarom besteden steeds meer gemeenten hun software- en infrastructuurbeheer uit aan clouddienstverleners. Vraagstukken waar gemeenten bijvoorbeeld tegenaan lopen zijn:

- Hoe borg ik de informatiebeveiliging en privacybescherming; mag een gemeente bijvoorbeeld de persoonsgegevens van haar burgers opslaan in een publieke cloud omgeving zoals Azure? De recente publicatie Rijksbreed cloudbeleid 2022 ondersteunt het gebruik van public cloud en stipt daar een aantal risico's bij aan.
- Hoe houd ik grip op financiën; hoe belast je generieke "cloudkosten" door aan de interne afdelingen?
- Hoe ga ik om met leveranciersafhankelijkheid; wat zijn de risico's als alle Nederlandse gemeenten gebruik zouden gaan maken van één leverancier?

Om goed te kunnen bepalen welke behoefte er is aan ondersteuning vanuit VNG is onderzocht wat de status is van cloud onder gemeenten en welke zorgen en risico's zich voordoen. Ook is onderzocht welke kansen er liggen. Dit is onderzocht middels een gemeentebrede enquête, diepte-interviews met een aantal gemeenten en leveranciers, onafhankelijk benchmarkonderzoek, een architectuuranalyse en interdisciplinaire expertconsultatie binnen VNG en VNG Realisatie.
Voorliggend document beschrijft de resultaten van de gemeentebrede enquête.
Leidend bij de enquête zijn de hoofdvragen

- Waar gemeenten staan in de Cloud transitie.
- Waar gemeenten tegenaanlopen.
- Wat gemeenten van de VNG verwachten t.a.v. de Cloud ondersteuning.

2. Onderzoeksmethode

Eén van de deelonderzoeken om de behoefte van gemeenten in kaart te brengen betreft een enquête. Hiervoor is gekozen omdat dit alle gemeenten in staat stelt om hun input bekend te maken en omdat dit, door de omvang, het mogelijk maakt om met een hoge betrouwbaarheid een aanname te doen over de behoeften van alle gemeenten.
Hoewel er ruimte was voor eigen inbreng is de enquête vooral kwantitatief van opzet. Hiermee zijn stellingen getoetst en is een beeld ontstaan van de prioriteiten van deelnemers.
Het onderzoek is verstuurd aan bestaande mailinglijsten gemeentesecretarissen, CIO's en via de mailinglijsten GT, SCG, VIAG en IMG 100.000+.
De enquête bevatte geen verplichte antwoorden, het was mogelijk om de enquête anoniem in te vullen.

3. Enquêteresultaten

3.1. Respons

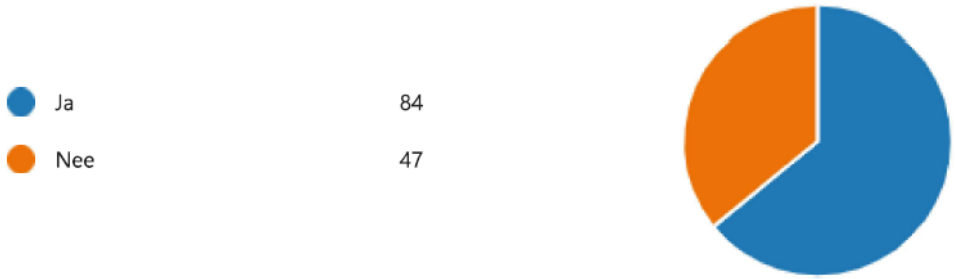
De enquête is ingevuld door 131 respondenten. Daarbinnen is 57% herleidbaar naar een gemeente. Daardoor was het bijvoorbeeld mogelijk om de resultaten te koppelen aan omvang van een gemeente.

Respons naar omvang:

Klein: 17%	Van de 273 kleine gemeenten (<60.000 inwoners) heeft 47 | 17% identificeerbaar de enquête ingevuld
Middelgroot: 38%	Van de 37 middelgrote gemeenten (60.000-100.000) heeft 14 | 38% identificeerbaar de enquête ingevuld
Groot: 40%	Van de 32 grote gemeenten (>100.000) heeft 13 | 40% identificeerbaar de enquête ingevuld

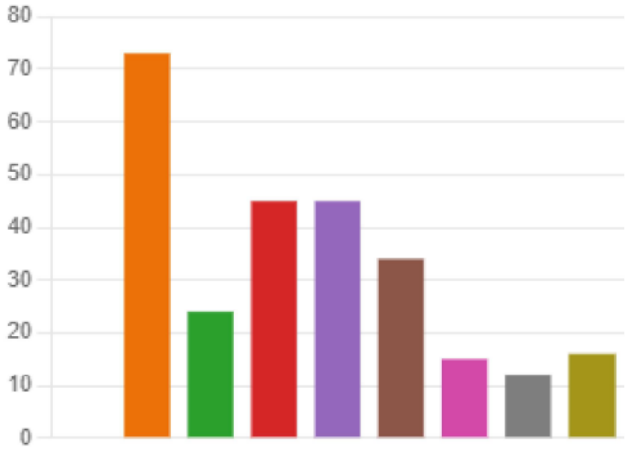
3.2. Huidige situatie

1. **Onze organisatie heeft een cloudbeleid en/of -strategie opgesteld.**



2. **De volgende onderwerpen zijn hierin uitgewerkt**:

Zo min mogelijk cloud	0
SaaS-first	73
Leveranciersafhankelijkheid	24
Eigenaarschap (o.a. van Data)	45
Exitstrategie	45
Compliance verantwoording	34
(IaaS/PaaS): Single-platform	15
(IaaS/PaaS): Multi-platform	12
Andere	16

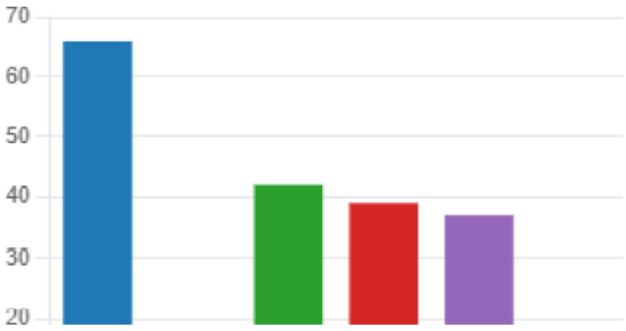


3. **Onze organisatie maakt gebruik van IaaS of PaaS diensten.**

Ja	89
Nee	42

4. **Onze organisatie maakt gebruikt van IaaS/PaaS voor:**

Hosting productie-omgeving pr...	66
Softwareontwikkeling	12
Back-up en/of recovery	42
Storage	39
Remote werkplekken	37



5. **Via welke CSP neemt u deze diensten af?**

Microsoft Azure	81
Amazon AWS	9
Google Cloud Platform	2
Andere	13

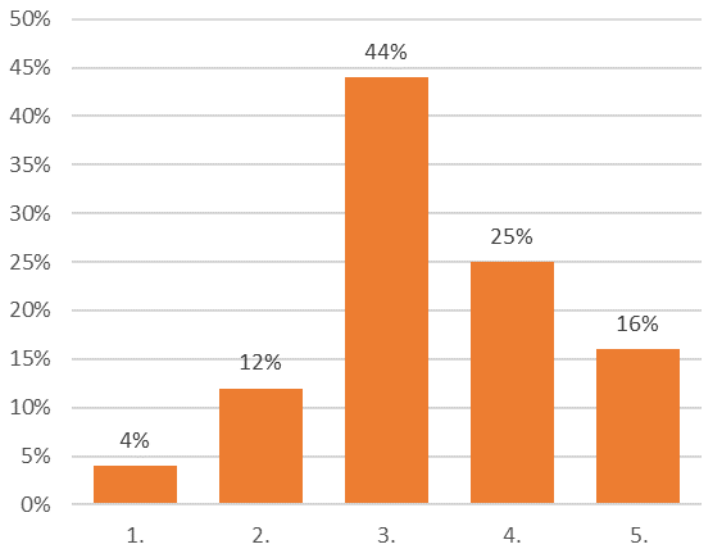
6. **Hoe is uw back-up en restore van de IaaS/PaaS geregeld?**

Bij dezelfde CSP	52
Bij een andere CSP	10
On Premises	15
Andere	10

7. **Wij zijn in control (BIO, AVG) op onze IaaS/PaaS in de Cloud**

3.39

Gemiddelde beoordeling



8. **Wilt u dit toelichten**

57 Antwoorden

Aan de voorkant regelen we dit bij de contractvorming, bij bestaande contracten minder in control
Afspraken binnen gt microsoft
Alles vooraf duidelijk afgesteld, SLA is helder, uitvallocaties zijn bekend, alles is in Nederland gehost, etc.
Bij de aanbesteding zijn de eisen vanuit Informatiebeveiliging en Privacy meegenomen.
Bij de inrichting van IaaS/PaaS is aandacht voor BIO en AVG
Bij IaaS/Saas is de CISO onvoldoende tijdig bij betrokken met gevolg dat het ook onvoldoende in beeld is.
BIO / AVG als vast onderdeel PvE en daarmee onderdeel van de overeenkomst
compliance via contract, tot nu toe geen eigen audits uitgevoerd op werking
Continue aandacht voor, omgeving wordt regelmatig door externen getoetst, Dataclassificatie kan nog beter.
De reden voor deze iaas dienst is puur juridisch want voor 4 gemeenten samen zonder 1 jur identiteit, wat lic problemen geeft als 1 voor de 3 andere host..
Deels maatregelen genomen, nog niet afdoende
Een servicegemeente voert deze taken uit.
eigen plan en apart team
Er is altijd ruimte voor verbetering. Tevens zijn er BIO controls te mappen op Azure veiligheidsmaatregelen.
Er liggen nog wat vraagpunten / aandachtspunten die nog uitgewerkt moeten worden tav opslag documenten in onedrive en teamsomgeving.
er zijn veel onduidelijkheden nog,
geen periodieke controle/verificatie
geen toelichting
Gemeente x volgt het BIO initiative gezamenlijk met Microsoft.
Het kan altijd beter
Is meestal geen eis/factor bij overgang naar SAAS
ken gebruik van het Azure CAF met BIO compliant policies
Laatste punt op de I wordt gezet
leveranciers management contract management zeer laag volwassenheidsniveau
ligt voor groot deel bij onze externe leverancier
Met de wisselende regelgeving en multiple interpretaties blijft het lastig hier volmondig ja op te kunnen zeggen.
Neutraal - kan ik niet zeggen
Nog niet alle afspraken zijn naar onze wensen/eisen ingeregeld
op papier zeker, maar gevoelsmatig niet altijd
Regelmatig strategisch, tactisch en operationeel overleg. Regelmatig SLA rapportages. Regelmatig CISO overleg. Jaarlijkse BIO TPM.
Te vaak wisselende berichtgeving over de legitimiteit om gebruik te kunnen maken van Azure
Uit de BIO rapportages komen geen bijzonderheden / aandachtspunten.
verwachting is dat het voldoet echter meer controle nodig
Volledig compliant met BIO en AVG verwerkt in contracten

Voor de omgeving van het Datawarehouse is een uitgebreide DPIA uitgevoerd en maatregelen getroffen. Door de FG is meegekeken met de inrichting.
Wat is in control?
We denken van wel, maar zonder diepgaande analyse/inspectie.
We eisen dat leveranciers voldoen aan de BIO en GIBIT. We schakelen steeds meer functionaliteit in om in control te komen.
We hebben aan veel gedacht maar kunnen ook zaken gemist hebben.
We hebben wel afspraken gemaakt maar komen nog niet toe aan het controleren. We controleren wel de prestaties ieder jaar.
We moeten de beide Azure Tenants nog dusdanig inrichten en het BIO policy initiatief van Microsoft er overheen gooien. On-premise toetsen we alle nieuwe systemen met o.a. de Security Impact Analyse tool. Het beantwoorden van de vragen levert een BIV classificatie op en een BBN niveau dat gekoppeld is aan de BIO en risk appetite. Maar bij bestaande omgevingen is die toets lang niet altijd uitgevoerd. Werk aan de winkel dus. Zodra de aanbesteding heeft plaatsgevonden moeten we in staat zijn om de private cloud agnostisch te koppelen aan onze Azure tenants zodat we het MS BIO initiatief ook kunnen uitrollen over die private cloud.
We monitoren doorlopend op BIO compliancy.
We slagen voor de DigiD audit in deze omgeving. Zeer sterke mate van automatisering, met daarin controls ingebouwd. Nog geen 5 bollen omdat we nog werken aan verder automatisering en verbetering
We voeren zelf beheer uit op de omgeving qua data.
We zijn afhankelijk van keuzes van leveranciers en proberen via contracten dat goed dicht te timmeren, maar we hebben hier niet genoeg invloed op als kleine gemeente.
we zitten midden in een aanbesteding
We zitten nu voornamelijk op on=prem en gaan richting cloud (nog in transitie). En BIO en AVG worden niet door deployment in ene beter ofzo.
Werken in de praktijk op basis van eigen onderzoeksteam en uitvoeren DPIA, in de geest van veilig gebruik Cloud maar nog zonder Strategiebeleid. Met de ervaringen die we opdoen wordt er langzaam wel vorm gegeven aan een strategieplan om tot -beleid te komen. Beeld begint zich te vormen maar het is nog niet echt vastgelegd wat de standaard gaat worden en tot hoever wij de eisen kunnen vastleggen.
Wij controleren KPN Werkplek op oa daadwerkelijk voldoen aan ISAE 3402 en ISO 270001. Tevens zijn de controls qua afstemming en escalatie in place en worden daadwerkelijk toegepast.
Wij doen het beheer
Wij maken nu nog zeer beperkt gebruik van IaaS/PaaS.
Wij stellen bij de aanschaf van nieuwe software die mogelijk in de cloud staat altijd duidelijk inkoopvoorwaarden op die ervoor zorgen dat de mogelijke leverancier voldoend aan de BIO/AVG
Wij werken met het Security en Privacy Control Framework dat een uitwerking is van BIO en AVG.
Wij zitten in een transitie naar de cloud, nog niet aan alle kaders en randvoorwaarden is voldaan en daarmee nog in ontwikkeling.
Wordt in essentie beheerd door onze gezamenlijke regeling
Wordt nog nader uitgezocht
zoals zoveel gemeentes zitten we momenteel midden in de transitie van VerSaaSing en verplaatsen van diensten naar de Cloud

9. **Onze organisatie ontwikkelt eigen software.**

Ja	9
Nee	78

10. **Op welke platformen?**

.Net, Python, Drupal, Mendix
azure / visual basic
Azure, Common ground
Diverse Open Source en Lowcode-platformen
E-Formulieren MOB
javascript/typescript/python zowel voor applicatiecode als voor de infra-as-code
MS (.net), Oracle (java), phyton, Mendix
Open Source Software en low code platform Outsystems (op AWS)
semi highlevel low code achtig: Oracle Apex, WeAreFrank

11. **Wij gebruiken SaaS voor één of meer primaire processen:**

Ja	127
Nee	4

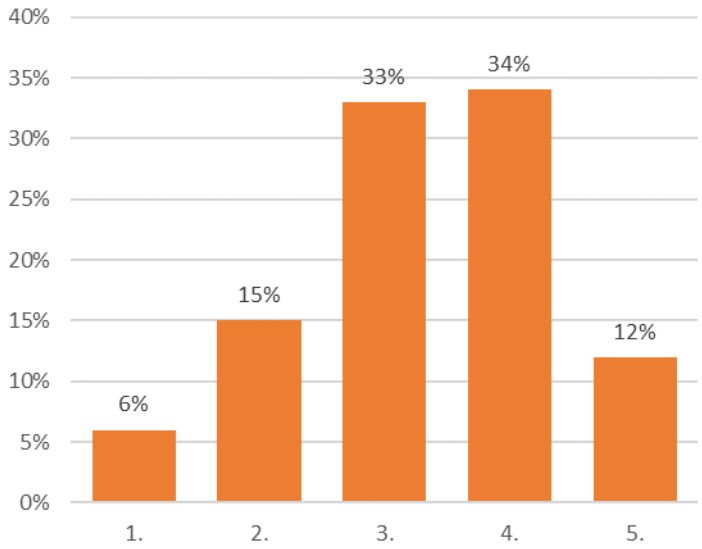
12. **Heeft u afgesproken dat de backup volledig geïsoleerd van de omgeving die geback-upt wordt?**

Ja	37
Nee	29
Weet ik niet	45
Andere	14

13. **Wij zijn in control (BIO, AVG) op onze SaaS diensten**

3.32

Gemiddelde beoordeling



14. **Wilt u dit toelichten**

80 Antwoorden

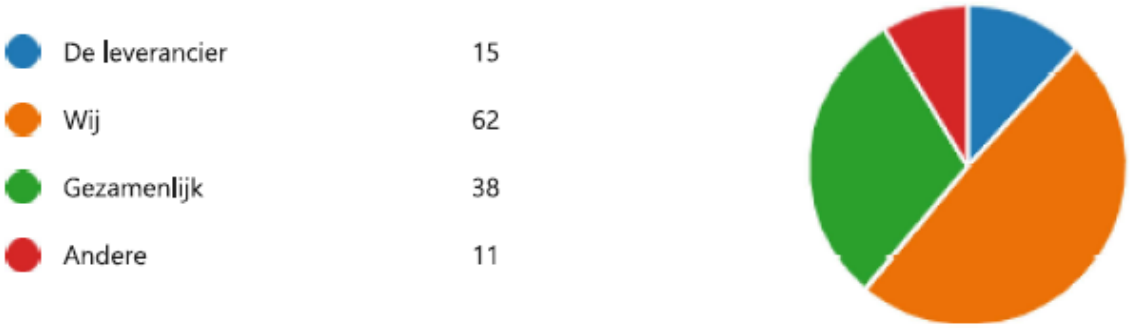
Aan de voorkant worden goede afspraken gemaakt. De controlerende taak blijft daarna achterwege. We vertrouwen op de leverancier..
Aangeboden oplossingen dienen te voldoen aan de BIO en dit wordt met een complianceverantwoording ondervangen. Vraag is of we hier hard op controleren en auditen.
Actualisatie van afspraken blijft achter
Afsluiten van verwerkerscontracten en of TPM contracten
afspraken over hoe en waar data wordt opgeslagen en dat de leverancier er niets mee kan.
Als inkoopvoorwaarden hanteren wij de Gibit 2020, welke op SaaS overeenkomsten van toepassing worden verklaard. . Alle SaaS overeenkomsten worden hieraan getoetst
Audit mogelijkheden zijn beperkt, leverancier werkt niet mee, standaard TPM is niet voldoende voor primaire processen
Audit uitgevoerd

Basic controls in orde, maar praktijk is weerbarstig
bij aanvang wordt er een goede screening gedaan
Bij een aanbesteding wordt er getoetst maar regelmatig zie je dat er weinig tussentijds getoetst wordt. Het is ook nog een uitdaging in de praktijk om uit te leggen aan de Business dat ook al is het SaaS dienst we als organisatie verantwoordelijk blijven voor de inhoud van de data, IAM en end-point security. En daarnaast is het altijd een gedeelde verantwoordelijkheid en dien je als organisatie afspraken te maken met je interne business en de dienstverlener en daarop te toetsen. SaaS wordt ook regelmatig gezien als mooi dan hoeven we nergens meer naar om te kijken en zijn we van die IV-organisatie af met al die lastige vragen en eisen.
Bij iedere SAAS dienst is een PO en ISO betrokken die de BIO/AVG aspecten adresseren
Bij Saas is de CISO onvoldoende tijdig bij betrokken met gevolg dat het ook onvoldoende in beeld is.
BIO / AVG (privacy) eisen maken onderdeel uit van PvE en de overeenkomsten die we aangaan mbt SaaS
BIO beter dan AVG. Die laatste heeft nog een lange weg te gaan.
BIO en AVG maken een vast onderdeel uit van ons inkoopbeleid (o.a. TPM, verwerkersovereenkomst). We hanteren de GIBIT bij nieuwe inkooptrajecten. Contractueel wordt een en ander dus geborgd. Het is geen 100% score omdat we als gemeenschappelijke regeling niet overal zeggenschap over hebben gehad in het verleden. Waardoor er een enkele oplossing wellicht niet helemaal voldoet aan ons huidige inkoopbeleid.
BIO vragenlijst geeft geen aandachtspunten.
compliance via contract en aanvullende voorwaarden (gibit), TPM op een aantal contracten
Contract afspraken
contracten zijn afgesloten op basis van de GIBIT toolkit, er is te weinig controle / toetsing op uitvoering
door het uitvoeren van periodieke audit door externe partners
Er is aandacht voor BIO en AVG bij SaaS migratie
Er worden geen audits uitgevoerd bij de leverancier. Alleen SLA en overeenkomsten. Geen controle dus
Er wordt met de leveranciers een DVO, inclusief Gibit en een verwerkersovereenkomst afgesloten
Er wordt naar gekeken, over nagedacht en naar gehandeld. Maar kan strakker.
Er zijn wel verwerkersovereenkomsten en contracten afgesloten onder GIBIT-voorwaarden, maar certificeringen, audits e.d. worden niet gecontroleerd,
Expertises zijn ingericht en hebben deel in de voortbrengings en monitoringsprocessen
Geen factor in de besluiten naar de SAAS
getoetst door onze eigen CISO en AVG medewerkers
GIBIT inclusief ICT kwaliteitsnormen + benodigde certificeringen (ISO ISAE etc) + aanvullende contractuele afspraken
Hebben afspraken vastgelegd met de Cloudleveranciers.
Het is lastig grip en inzicht te krijgen op de wijze waarop leveranciers beveiliging hebben geborgd
Hiertoe werken we met TPM's die de leveranciers aanleveren in geval van audits. Ook hier is ruimte voor verbetering.
Ik denk dat we niet voor alle SaaS-diensten waterdichte afspraken hebben, maar wel een eind komen.
In de aanbesteding zijn de eisen voor Informatiebeveiliging en Privacy meegenomen. Dit waren knock-out criteria.
In de offerte-uitvraag hebben we uitgebreide eisen gesteld voor zowel BIO als AVG. Er zijn verwerkersovereenkomsten afgesloten.

Je kunt van alles uitvragen, maar hoe controleer je de antwoorden van leveranciers? Wat zegt het als er geen audit achter hangt?
Leveranciers versturen bij uitzondering rapportages over incidenten of release updates.
ligt grotendeels bij externe dienstverlener
Loopt nu, nog niet geregeld
Meeste gebieden wel, maar niet alles bekend
Met verwerkingsovereenkomst
Niet voor alle SaaS-diensten is dit in place
Nog enkele diensten niet onderzocht
Nog geen goed overzicht
Nog niet alle afspraken zijn naar onze wensen/eisen ingeregeld
onvoldoende centraal inzicht in stavaza van backup en performance etc.
onvoldoende in beeld, dus voorzichtige tot pessimistische schatting
Ook hier geldt dat er nog veel in ontwikkeling is en we steeds meer de regie pakken om in control te komen.
Op Saas is de invloed beperkt. Waar interne audits eenvoudig zijn ligt dit bij Saas anders. Wanneer een Saas leverancier besluit van hostingpartij te veranderen kom je daar pas achter bij een incident zoals log4j.
Servicegemeente voert dit uit.
Teveel fragmentatie in kwaliteit aanbieders, nog teveel zoekende naar een uniforme uitvraag, wensen/eisen aanbestedingen niet altijd het juiste instrument, controle na gunning ook lastig
Via een checklist Informatieveiligheid.
Volgens mij is er alleen in de inkoopstrategie iets opgenomen qua bio en avg, Actieve controle vind plaats binnen de applicatie, qua backup niet.
Volgt uit GAP analyse
Voor alle belangrijke processen sowieso. Voor niet alle kleine diensten is het zo ver uitgewerkt. Dat kan dus wat beter, maar de risico's zijn hanteerbaar. Kortom grotendeels in control.
We bevragen de SAAS leveranciers actief op deze onderwerpen.
We hebben verwerkersovereenkomsten met de SaaS leveranciers afgesloten
We maken met alle leverancier hier afspraken over in de SLA / DAP. Tevens ook een terugkerende toets hierop.
We stellen hierop voorwaarden bij aanschaf, maar controleren hier niet structureel op
We zijn niet leidend maar worden geleid door de visie van de leverancier.
We zijn nog niet zo ver dat we dit jaarlijks procedureel testen.
Wel contractuele eisen, maar nog niet 100% compliant.
wij bepalen zelf dat alleen software die
Wij doen het beheer
Wij houden bij de inkoop van SaaS diensten rekening met BIO en AVG compliancy
Wij moeten meer toezien op het nakomen van de SLA's. Overeenkomsten allemaal gebaseerd op de GIBIT en de BIO.
Wij sluiten standaard een verwerkersovereenkomst af met leveranciers en letten hierbij de informatie-beveiligingsaspecten. Echter beschikken wij niet over een EA-tool (voor het gewenste overzicht) en daarnaast gebeurt het ook dat er buiten Informatiemanagement om applicaties / websites worden aangeschaft waarbij controle mogelijk onvolledig is
Wij stellen eisen over IB en AVG bij de aanbesteding van SaaS diensten.

Wij stellen sinds 2019 bij alle nieuw af te nemen SaaS diensten het voldoen aan de BIO (en al veel eerder ook aan de AVG) als eis. Dus ook altijd ISAE 3402, ISO 270001 in place en GIBIT 2020 van toepassing en verwerkersovereenkomst.
Wij vragen het uit conform het PVE alleen het controleren van de leverancier hierop doen we te weinig.
Wij werken strikt vanuit een CAB met verwerkersovereenkomsten via onze privacy officer en ciso
Wij zijn in control o.a. door verwerkersovereenkomsten en het periodiek opvragen van auditrapporten.
Zowel backup als BIO/AVG nog een keer uitdiepen omdat in het verleden hier onvoldoende aandacht voor was (nu een afvinklijst bij aanbesteding)

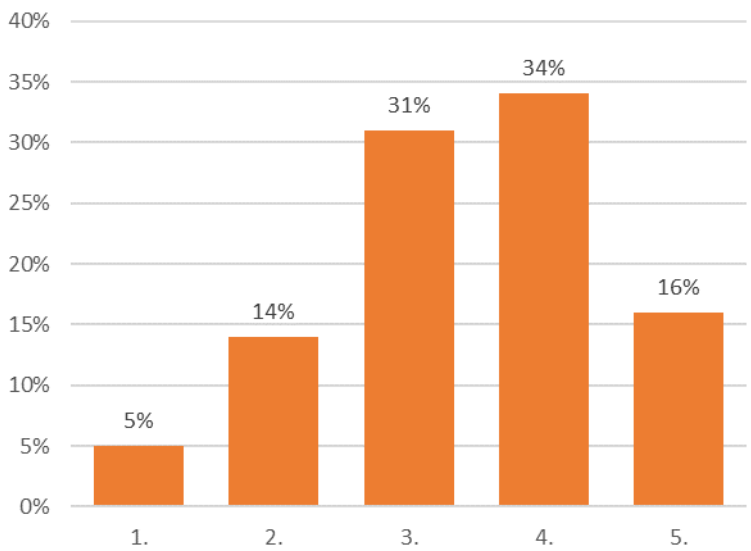
15. **Wie heeft de regierol?**



16. **De verantwoordelijkheden, tussen onze organisatie en de cloudleverancier, zijn duidelijk.**

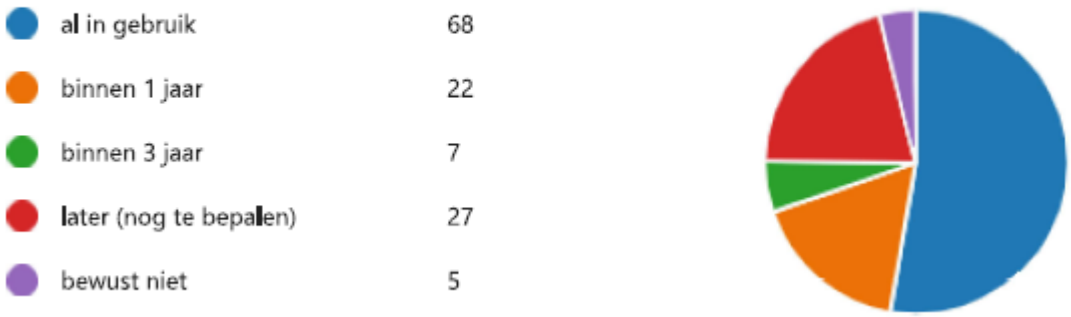
3.43

Gemiddelde beoordeling



3.3. Verwachte situatie

17. **Onze organisatie gaat binnenkort IaaS/PaaS diensten gebruiken.**

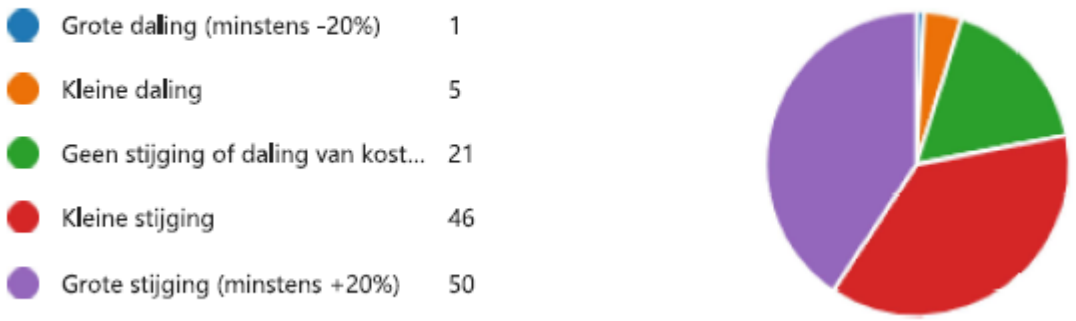


18. **Kunt u aangeven waarom er bewust geen gebruik gemaakt gaat worden van IaaS/PaaS diensten?**

4 antwoorden

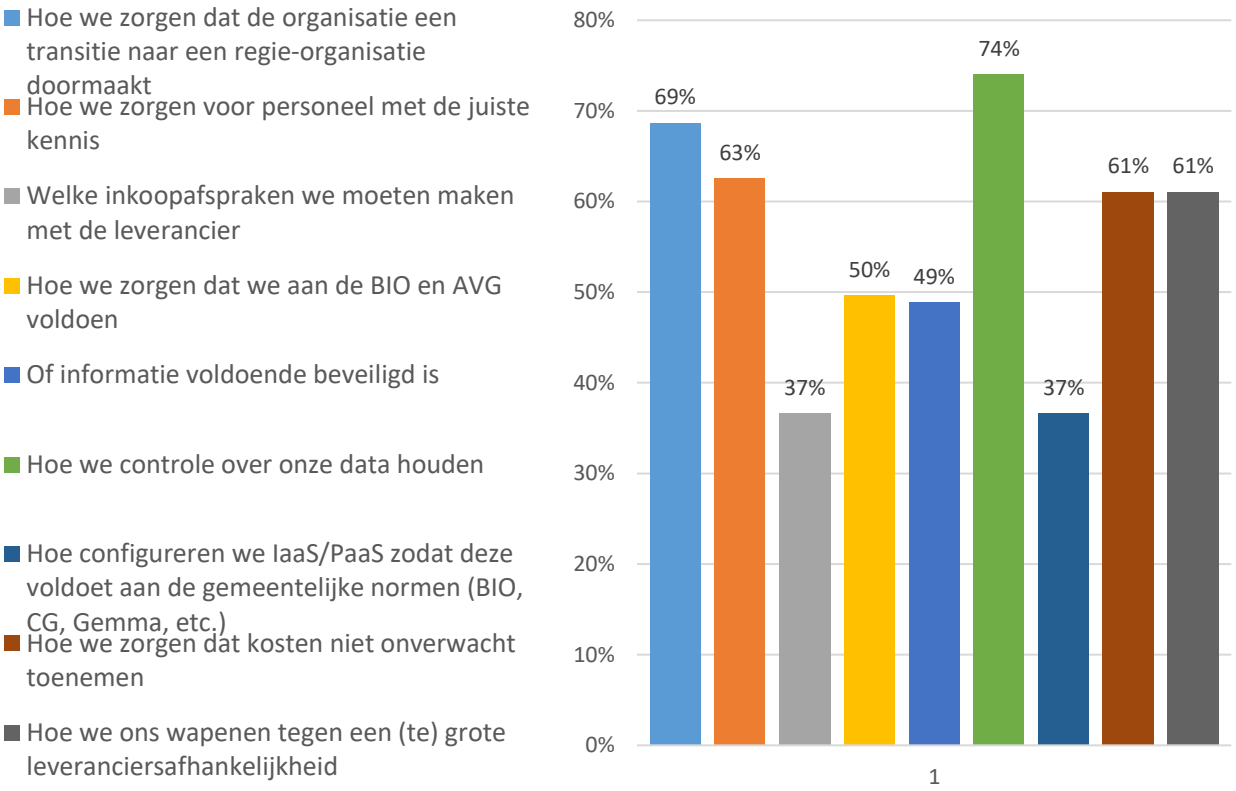
Alles is al op SaaS
Op dit moment is het voor ons als samenwerkingsorganisatie nog niet interessant genoeg om deze stap te maken. We hebben voldoende body om de benodigde infrastructuur die we nodig hebben (on-premises) zelf te kunnen faciliteren. Als de versaasing van het applicatielandschap bij onze deelnemers doorzet en daardoor de hoeveelheid (on-premises) infrastructuur af gaat nemen is dat voor ons wel reden om ons te bezinnen. De praktijk laat echter zien dat de vraag naar deze on-premises infrastructuur nog steeds groeit. Het tempo waarin dit bij gemeenten gaat is erg laag!
We hebben zelf een goed serverpark staan.
We maken bij voorkeur gebruik van door leveranciers ontwikkelde applicaties/SAAS oplossingen en ontwikkelen alleen zelf iets wanneer dat echt niet anders kan. En wanneer we wat zelf laten ontwikkelen gaat dat op een low/zero coding platform wat weer in de cloud draait. 90% van de medewerkers werkt op 1 locatie en daar hebben we een eigen datacenter (en elders een 2e actief/actief). Ondanks de move naar SAAS blijft er enige infra op die centrale locatie die toch beheerd moet worden door onze beheerders, de incrementele kosten om een aantal niet-SAAS applicaties lokaal te draaien zijn daardoor minimaal. Ik zie nog geen businesscase om de lokale applicaties naar een IAAS/PAAS over te zetten. Ook kijken we sterk vanuit een beschikbaarheidsperspectief. Diverse leveranciers (iBabs bv) maken al gebruik van Azure, wanneer daar echt wat misgaat zoals een paar maanden terug gebeurde heeft iedere Azure klant daar last van.

19. **Verwacht u, door cloud, de komende jaren een wijziging in uw IT kosten?**



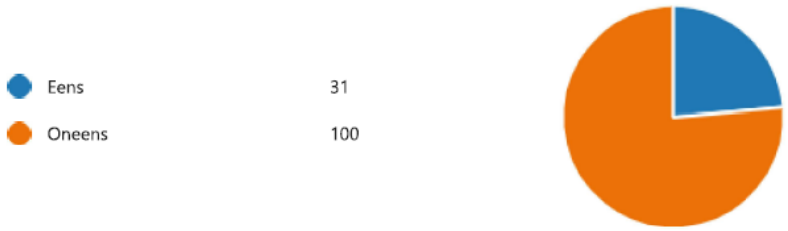
3.4. Zorgen

20. **Onze grootste zorgen met betrekking tot Cloud zijn:**

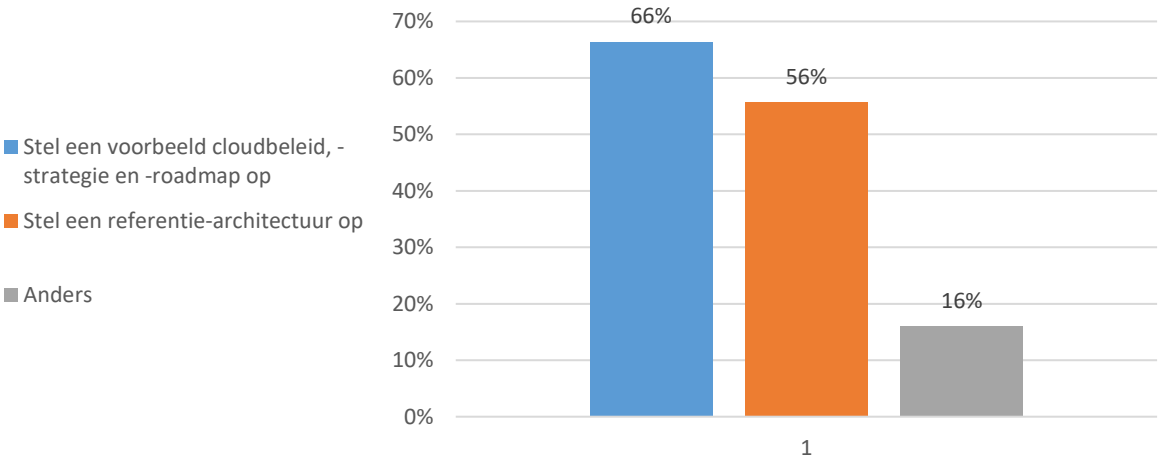


3.5. Behoefte gemeenten

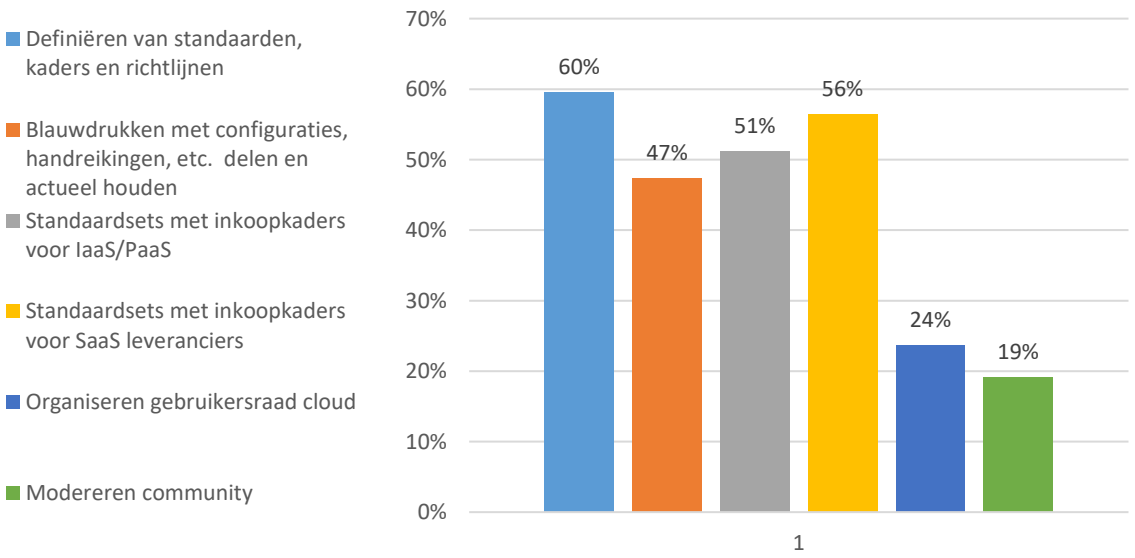
21. **Wij zien geen rol voor VNG**



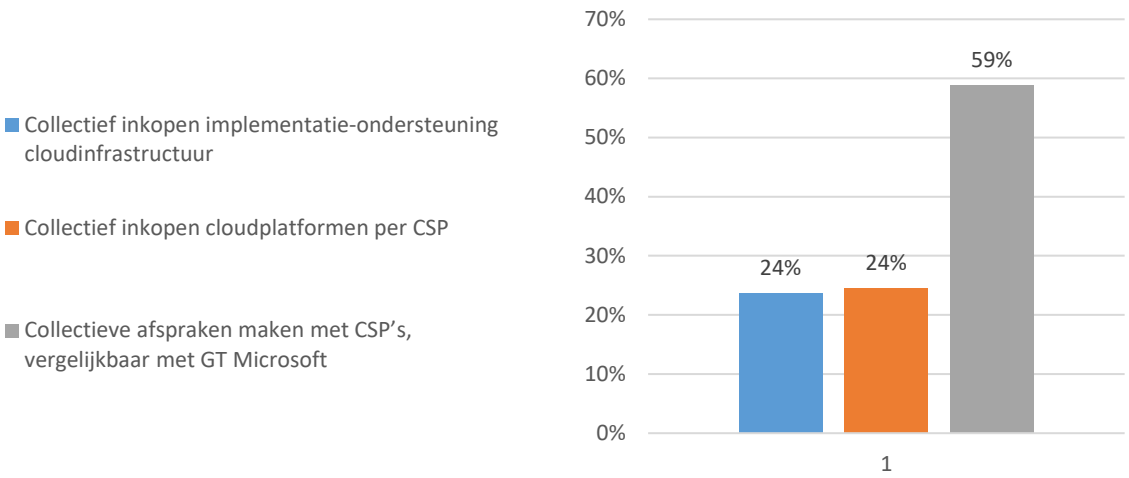
22. De VNG moet het volgende aanbieden als het gaat over beleid



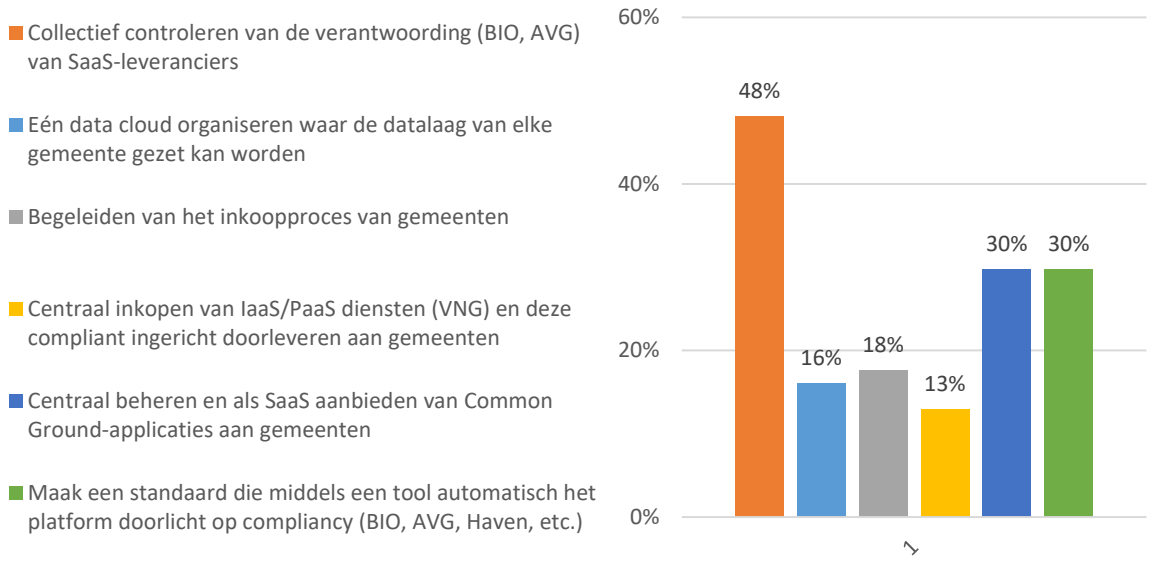
23. De VNG moet het volgende aanbieden als het gaat over kennisdeling



24. **De VNG moet het volgende aanbieden als het gaat over collectieve inkoop**



25. **Als VNG de volgende collectieve dienstverlening aanbiedt gaan wij dit binnen 1 jaar gebruiken**



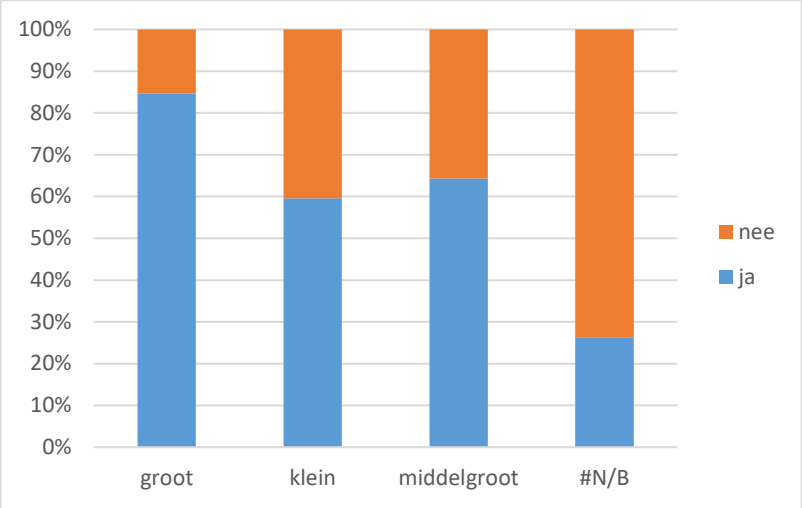
Verdeling naar omvang van gemeente

Voor enkele behoeften uit vraag 25 is geanalyseerd of de omvang van een gemeente effect heeft op de behoefte.

Qua score van de behoefte hebben we specifiek gekeken naar: 1. De vraag over certificeren SaaS-leveranciers, 2. De vraag over een collectief PaaS-platform, 3. De vraag over het als SaaS aanbieden van CG-applicaties. Conclusie is dat de uitkomsten niet significant worden beïnvloed door de beantwoording in een bepaalde groep.

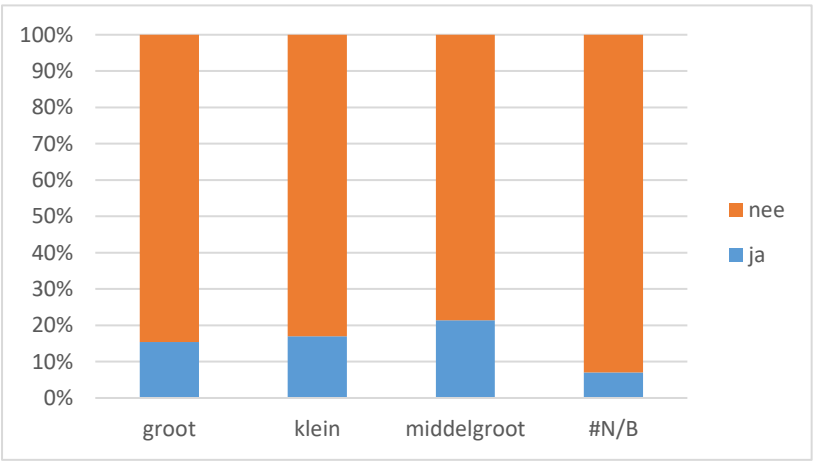
25a. Collectief controleren van de verantwoording (BIO, AVG) van SaaS-leveranciers

Rijlabels	ja	nee	Eindtotaal
groot	11	2	13
klein	28	19	47
middelgroot	9	5	14
#N/B	15	42	57
Eindtotaal	**63**	**68**	**131**



25b. **Centraal inkopen van IaaS/PaaS diensten (VNG) en deze compliant ingericht doorleveren aan gemeenten**

Rijlabels	ja	nee	Eindtotaal
groot	2	11	13
klein	8	39	47
middelgroot	3	11	14
#N/B	4	53	57
Eindtotaal	**17**	**114**	**131**



25c. **Centraal beheren en als SaaS aanbieden van Common Ground-applicaties aan gemeenten**

Rijlabels	ja	nee	Eindtotaal
groot	7	6	13
klein	18	29	47
middelgroot	5	9	14
#N/B	10	47	57
Eindtotaal	**40**	**91**	**131**