Bestuurlijke verantwoordingsrapportage WOZ

Informatiebeveiliging en informatie-architectuur WOZ 2021

Gemeenten en uitvoeringsorganisaties zullen bij de interne beheersing van risico's in het WOZ-proces voldoende aandacht moeten hebben voor de beheersing van geautomatiseerde systemen. Beheersingsaspecten die te maken hebben met architectuur, informatiebeveiliging, continuïteit, beschikbaarheid en algemene IT-beheersingsmaatregelen (General IT Controls als back-up & recovery, change management), moeten voldoende worden beheerst. Door snelle ontwikkelingen op het terrein van minimale beveiligingsmaatregelen en gewenste architectuur vergen deze aspecten even snel mee-ontwikkelende beheersingsmaatregelen.

Gezien de maatschappelijke behoefte aan WOZ-waarden en WOZ-gegevens van hoge kwaliteit met de mogelijkheid tot inbreng van belanghebbenden (regie op gegevens) en gezien de ontwikkelingen rond basisregistraties en het tot stand brengen van één objectenregistratie zullen gemeenten en uitvoeringsorganisaties zich moeten realiseren dat er aanzienlijke investeringen in de komende jaren nodig zijn. Dat betreft voor een belangrijk deel investeringen in de vernieuwing van automatiseringssystemen, gericht op het benutten van geografische informatiesystemen (GIS), het benutten van AI-technieken in taxatiemodellen en de overgang naar een andere informatie-architectuur. Deze andere informatie-architectuur is nodig om mee te gaan met technische ontwikkelingen, met ontwikkelingen op het terrein van informatieveiligheid en de hiervoor geschetste ontwikkelingen rond basisregistraties en het tot stand brengen van één objectenregistratie. Maar zeker ook de communicatie met inwoners en het realiseren van "regie op gegevens" vergt op korte termijn investeringen in de ICT-infrastructuur rond het WOZ-domein. Concrete stappen zijn bijvoorbeeld vervangen van bestandsuitwisselingen door beveiligd berichtenverkeer. Tot slot is de verwachting dat voor de geobasisregistraties en de WOZ in de komende jaren verdere samenwerking aan de orde is, ook in uw gemeente. Daarbij is ook aandacht voor de datakwaliteit van groot belang.

REGIE OP GEGEVENS
Zelf gegevens delen, veilig en betrouwbaar!

BAG BGT BOR WOZ

SOR
Samenhangende objectenregistratie

Common Ground

DiS Geo
Doorontwikkeling in Samenhang

Standaard voor Ratiocontroles

VNG

Samen Organiseren

Zie ook de toolbox Samenhangende objectenregistratie en ICT-ontwikkelingen op de website van de Waarderingskamer (https://www.waarderingskamer.nl/basisregistratie-woz-lv-woz/investeringsagenda).

Datum vaststelling door College van B&W:	23 maart 2022

In onderstaande tabel zijn de uitkomsten van de WOZ-vragenlijst zoals deze binnen ENSIA zijn ingevuld voor uw organisatie samengevat. Onder het kopje ‘tips’ leest u meer over het betreffende aspect en hoe u dit, indien nodig, kunt verbeteren.

Status	Conclusie	Tips
✗	De BIO is niet volledig geïmplementeerd in de organisatie, er worden op dit moment geen controles uitgevoerd op naleving van de BIO voor de WOZ.	Elke gemeente en gemeentelijke uitvoeringsorganisatie dient te voldoen aan de BIO. Ook voor de WOZ-systemen moet daarom door de organisatie bekeken zijn, welke BIO-controls van toepassing zijn. De naleving van deze controls dient periodiek gecontroleerd te worden en de resultaten van deze beoordeling, in hoeverre de WOZ-systemen binnen de organisatie aan de BIO voldoen, dienen beschikbaar te zijn.
✓	De overgang naar Common Ground conforme architectuur voor de WOZ is gestart!	Bekijk hier (https://commonground.nl/) wat deze ingrijpende hervorming van de informatievoorziening voor uw organisatie gaat betekenen en wat u al kunt doen.
✓	Er wordt gebruikt gemaakt van de gewenste koppelvlakken (API's en/of xml-berichtenverkeer) voor de communicatie tussen de diverse applicaties voor de WOZ-uitvoering.	Gezien de privacy-gevoeligheid van (een deel van) de gegevens in de WOZ-administratie en de ontwikkelingen in de architectuur van de WOZ-informatiehuishouding is permanente aandacht voor beveiliging van de genoemde koppelvlakken en bijgewerkt (releases and patches) houden van alle betrokken systemen van groot belang.
✓	Tussen de applicaties die de uitvoering van de WOZ-processen ondersteunen vindt interactie plaats. Er is een volledig overzicht van de onderlinge relaties tussen deze systemen.	Het is raadzaam een volledig overzicht van de verschillende koppelvlakken / interfaces te hebben zodat u deze kunt beheren.
✓	Er is onderzocht of de verschillende geautomatiseerde systemen informatie juist delen met externe systemen zoals bijvoorbeeld de Landelijke voorziening WOZ (LV WOZ) en MijnOverheid.	Gemeenten moeten verifiëren of de gegevens in de LV WOZ nog overeenkomen met die van de gemeentelijke Basisregistratie WOZ. Indien dit niet gebeurt bestaat het risico dat afnemers niet de juiste gegevens krijgen, inwoners niet tijdig hun WOZ-waarde op www.wozwaardeloket.nl zien en de belastingcapaciteit per gemeente, die het CBS op basis van de LV WOZ vaststelt, niet klopt.
✓	Op terrein van de beheersing van informatiebeveiliging conform BIO is voor de WOZ-uitvoering de gewenste managementinformatie beschikbaar.	Op pagina 88 en 91 van de Waarderingsinstructie (https://www.waarderingskamer.nl/hulpmiddelen-gemeenten/waarderingsinstructie/) is onder het kopje “stuurinformatie” beschreven welke managementinformatie er belangrijk is bij het inzicht krijgen in de naleving van beveiligingsbeleid en -normen (BIO).

In de bijlage zijn de complete vraagteksten en de namens uw organisatie opgegeven antwoorden terug te vinden.

Daar vindt u ook welke **conclusies** uw WOZ-specialist heeft getrokken over de rol en invloed van IT op de WOZ-uitvoering binnen uw organisatie en welke **verbetermaatregelen** in 2021 reeds zijn getroffen ten aanzien van informatieveiligheid en informatie-architectuur in het kader van de WOZ-uitvoering.

Aan het bestuur van uw organisatie worden door de invullers (ENSIA-coördinator en/of WOZ-specialist) de volgende aanbevelingen gedaan:

Op het gebied van informatieveiligheid zijn door BSOB de volgende maatregelen uitgevoerd in 2021:

1. Implementatie van de BIO met de volgende projectstappen:
    a. Het uitvoeren van een GAP-analyse op de organisatiebrede informatiebeveiliging.
    b. Het uitvoeren van een risicoanalyse op basis van dreigingen en de GAP-analyse. Deze risicoanalyse is uitgevoerd door met proceseigenaren en de ICT service provider (Waterschap Aa en Maas) de huidige stand van zaken te bespreken.
    c. Het bepalen van de top 10 risico's.
2. In juli 2021 zijn kwetsbaarheidsonderzoeken (penetratietest en blackbox applicatieonderzoek) uitgevoerd. Voor de BSOB website en portalen zijn geen kwetsbaarheden gevonden. Het kwetsbaarhedenonderzoek van het interne netwerk leverde een aantal bevindingen op. Deze zijn direct samen met ICT Waterschap Aa en Maas opgepakt en gemitigeerd.
3. Voor het continu werken aan bewustwording bij medewerkers zijn een tweetal phishing tests uitgevoerd.

Door BSOB zijn voor 2022 de volgende maatregelen ingepland:

BSOB wil de interne organisatie, op het gebied van informatiebeveiliging, naar een hogere volwassenheid brengen. Hiervoor zijn in een voorgaand project de top 10 risico's inzichtelijk gemaakt met daarbij de maatregelen vanuit de BIO die hier tegenover gezet kunnen worden om de risico's de mitigeren. Tijdens de presentatie hierover aan het managementteam (op 20 januari 2022) is aangegeven dat BSOB wil toewerken naar een systematiek (ISMS in de breedste zin) waarbij de verantwoordelijkheden met betrekking tot informatiebeveiliging op het juiste niveau wordt belegd en waar verantwoording over wordt afgelegd op structurele (en pragmatische) wijze.

Met behulp van externe ondersteuning worden de volgende werkzaamheden uitgevoerd:

1. Op basis van geselecteerde maatregelen (onderliggend aan de top 10 risico's) een nulmeting uitvoeren over de status van implementatie.
2. Aan de hand van de uitkomsten van deze nulmeting, een adviesrapport in de vorm van een plan van aanpak opstellen voor de verdere implementatie van de maatregelen.
3. De eerste lijn (lijnverantwoordelijken) handreikingen geven hoe diverse controles uitgevoerd kunnen worden. Dit omvat trainingen, ondersteuning en templates.
4. Inrichting van ISMS tooling.

Bijlage

Vraag	Antwoord
Worden er controles uitgevoerd of de BIO wordt nageleefd voor de WOZ-uitvoering?	Nee, de BIO is nog niet volledig geïmplementeerd in de organisatie
Geef een korte toelichting hoe deze controles eruitzien of waarom de BIO niet of nog niet volledig is geïmplementeerd.	We hebben wel een normenkader gedefinieerd, proceseigenaren toegekend en een GAP wordt momenteel uitgevoerd, met hulp van een derde ondersteunende partij. Onze tooling ISMS (van SEP/Inergy) is gevuld met normenkaders, rollen en verantwoordelijkheden. Nu moet nog volgen per norm, rol of verantwoordelijkheid of BSOB compliant is, en of hier vastleggingen van zijn. Dit nalopen (afvinken) moet nog gebeuren, wat niet wil zeggen dat BSOB niet voldoet.
Is de overgang naar Common Ground conforme architectuur voor de WOZ gestart?	Ja
Geef een korte toelichting op de stand van zaken.	We hebben zowel BGT, BAG als WOZ samengebracht in de applicatie Way2Go om door bij muteren ' door ' de basisregistraties heen te kunnen muteren. Deze informatie wordt live gekoppeld met ons belastingpakket en andersom conform de landelijke voorgeschreven standaarden. Data komt binnen, en verlaat de organisatie ook weer conform de landelijk interactieafspraken. Datalagen worden steeds meer in de common ground gedachte opgebouwd binnen BSOB, welke steeds meer middels API's ontsloten kunnen worden. Nu moeten we de informatie nog kwijt kunnen middels diezelfde API's. (Het opbouwen van de Service-laag.) Door afspraken te maken met de deelnemers kunnen we ook de integratielaag gaan opbouwen.
Maakt uw organisatie gebruik van standaard koppelvlakken voor de communicatie tussen de diverse applicaties voor de WOZ-uitvoering?	Ja, zowel API’s als xml (StUF woz 03.12)
Geef een korte toelichting op uw gegeven antwoord.	Tussen waarderingsapplicatie en belastingapplicatie ligt een database koppeling die verrijkt is met entiteiten uit het XML model. De burger bevraagt zijn WOZ-object bijvoorbeeld via een API in het taxatieverslag.
Heeft uw organisatie een volledig overzicht van de verschillende koppelvlakken/interfaces tussen de diverse applicaties die de uitvoering van de WOZ-processen ondersteunen?	Ja
Geef een korte toelichting op uw gegeven antwoord.	Ons applicatielandschap is in beeld gebracht, en vastgelegd. Dit mag eventueel nog naar een hoger detailniveau.

Zijn er audits uitgevoerd om te beoordelen of de verschillende geautomatiseerde systemen informatie juist delen met externe systemen (als bijv. LVWOZ en de landelijke voorzieningen van de diverse basisregistraties.	Ja, onderzoek door eigen medewerkers en externe partij
Geef hier aan voor welke systemen dit het geval is.	Het betreft GOUWIT (belastingen) voor de registraties benoemd in het opmerkingenveld.
Zijn er audits uitgevoerd om te beoordelen of alle voor de WOZ-uitvoering gebruikte systemen de gegevens uit interne systemen juist verwerken? (Tot de "interne" systemen rekenen we ook systemen die in service beheerd worden door een andere gemeente, door een dienstverlener, een cloud-oplossing of systemen die als SaaS beschikbaar zijn).	Ja, onderzoek door eigen medewerkers en externe partij
Geef hier aan voor welke systemen dit het geval is.	Er wordt zowel door eigen medewerkers als door de accountant beoordeeld of de systemen GOUWIT (belastingen) en ORTAX (waarderen) en synchroon lopen. Door eigen medewerkers wordt ook gecontroleerd of dit synchroon loopt met Way2Go.
Is vanuit de WOZ-systemen de gewenste managementinformatie beschikbaar?	Ja
Geef een korte toelichting op uw gegeven antwoord.	We hebben een intern Datawarehouse van waar uit we in Qlikview management informatie verzamelen en tonen.
Geef beknopt aan welke conclusies u, in het kader van de interne beheersing op basis van de stuurinformatie, heeft getrokken over de rol en invloed van IT op de WOZ-uitvoering.	BSOB is zich bewust van de relevantie van normenkaders, rollen en verantwoordelijkheden en heeft deze ook beschreven. Echter in toenemende mate wordt is rol van IT steeds belangrijker geworden en dat zal zich ook zo blijven ontwikkelen. De koppelvlakken niet alleen intern maar ook extern worden steeds omvangrijker. Het borgen van de volledigheid en juistheid van overdracht van gegevens is vanwege de complexiteit van de koppelvlakken een IT verantwoordelijkheid geworden. Daar hoort vanzelfsprekend ook de informatieveiligheid bij, nu koppelvlakken per definitie een verhoogd risico opleveren.
Geef kort aan welke verbetermaatregelen u in 2021 heeft getroffen ten aanzien van informatieveiligheid en informatie-architectuur in het kader van de WOZ-uitvoering.	Buiten de doorontwikkeling van ons eigen interne controleprogramma trekken we actiever op met afnemers en leveranciers. BSOB ontwikkelt samen met bijv. CBS, kadaster, waarderingskamer, GOUW IT en haar deelnemers slimmere en efficiëntere oplossingen om beter en sneller de volledigheid en juistheid van onze gegevensuitwisseling te controleren. Dit levert een meer volledig en juist gegevensbestand op. Een sprekend voorbeeld is het onderzoek naar de synchroniteit van de LV-WOZ in samenwerking met het CBS. Dit heeft geleid tot een aanpassing van de landelijke voorziening en het opwerken van foutieve data aan de kant van BSOB. Zo werden diverse API

	ontwikkelt, XML-koppelvlakken ontwikkelt en op het gebied van veiligheid werden pentesten uitgevoerd en ethisch hackers ingezet om te controleren of BSOB bestand was tegen aanvallen. Daarnaast werken we aan IB bewustwording bij medewerkers en hebben daar het afgelopen jaar o.a. een e-learning workshop en phishing test voor ingezet.