Het nut van de GBA-audit: een terugblik en een voorstel tot verandering

In september 2004 bestaat de periodieke GBA-audit vijf jaar. In het eerste lustrum van haar bestaan heeft de audit haar nut als instrument om de kwaliteit van de GBA te verhogen ruimschoots bewezen. Toch is de vraag gerechtvaardigd of het instrument niet aan revisie toe is: is bij handhaving van de huidige uitvoeringswijze nog wel verdere kwaliteitswinst te behalen? In dit artikel wordt deze vraag ontkennend beantwoord. De grondslag hiervoor ligt in een nadere analyse van de resultaten bij de door BMC uitgevoerde audits. Om de discussie te openen over bijstelling van de regeling periodieke GBA-audits voorafgaand aan de volgende ronde worden in dit artikel tevens voorstellen gedaan voor een alternatieve aanpak van de audit.

Ontwikkeling van het audit-instrument

Tot dusver zijn de eisen bij de GBA-audit vanaf de introductie van dit instrument twee keer bijgesteld. In januari 2001 werd de tot dan toe facultatieve toets op de privacy-aspecten een verplicht onderdeel van de audit. Vanaf de start van de tweede ronde GBA-audits in september 2002 werden de eisen ten aanzien van het procesgedeelte aanzienlijk verzwaard. Tegelijk trad een verlichting op van de eisen bij het inhoudelijke deel doordat de aanvraagformulieren voor reisdocumenten niet langer getoond hoefden te worden bij de audit. Gesteld kan worden dat er in de eerste vijf jaar een verschuiving heeft plaatsgevonden van een toets op uitvoeringsaspecten naar een toets op beheeraspecten rond de GBA. Dat is in relatie tot de kwaliteitsaspecten die bij de audit een rol spelen ook zonder meer verklaarbaar. De juistheid van een inhoudelijk gegeven op de persoonslijst is slechts één aspect van de betrouwbaarheid (integriteit) van de GBA. Integriteit op haar beurt is slechts één kwaliteitsaspect, naast beschikbaarheid en vertrouwelijkheid van de GBA-gegevens. Die laatste aspecten zijn met name het object van de proces- en privacy-audit.

Het inhoudelijke deel van de GBA-audit

De eerste vraag die naar onze mening beantwoord moet worden is de volgende: geeft een controle van een beperkt aantal persoonslijsten een volledig beeld van de betrouwbaarheid van een GBA-gegevensbestand? Een statisticus kan deze vraag van een sluitend antwoord voorzien, maar gezond boerenverstand maakt het ook wel mogelijk in te zien dat in de beperking van de steekproef een inherente zwakte schuilt van de huidige toets als middel om de integriteit van alle gegevens te toetsen. Daarbij komt dat de toets zich beperkt tot een controle op administratieve juistheid van de gegevens en niets zegt over de feitelijke juistheid van deze gegevens.
Voor een oordeel over de integriteit is naast de juistheid ook de tijdigheid en volledigheid van de gegevensverwerking van belang. Deze laatste aspecten worden met het streven naar online gegevensverstrekking aan afnemers extra belangrijk. Met de introductie van TCP/IP kan het berichtenverkeer wel versneld worden, maar de daarmee behaalde winst gaat verloren als gemeenten bijvoorbeeld complexere mutaties slechts één keer per week verwerken.
Het verdient daarom ook aandacht om te kijken naar de tijdigheid, volledigheid en juistheid van de administratieve afhandeling van mutaties, van aangifte tot GBA bericht bij Burgerzaken. Dit zou uitstekend steekproefsgewijs kunnen gebeuren bij de GBA audit.
Bij verdere aanpassing van de regeling periodieke GBA-audit moet naar onze mening met name gezocht worden naar een methodiek om de inherente zwakheden van de huidige toets op te heffen dan wel te verminderen. Een mogelijke oplossingsrichting is een geautomatiseerde controle van het volledige GBA-bestand van een gemeente (waarvoor goede instrumenten ter beschikking staan), gekoppeld aan een audit op (een deel van) de verwerkingsprocessen van GBA-gegevens.

Het procesdeel van de GBA-audit

Zoals gezegd is het belangrijkste kwaliteitsaspect dat in het procesdeel van de audit wordt getoetst de beschikbaarheid (continuïteit) van de GBA. In eerste instantie is de toetsing beperkt gebleven tot een controle op de opzet van de getroffen maatregelen. Sinds medio 2002 wordt daarnaast gekeken naar bestaan en werking van de maatregelen. Het hebben van een schriftelijke procedure voor het dagelijks uitvoeren van een back-up (opzet) is bijvoorbeeld niet langer voldoende om voor de eerste eis van de vragenlijst te slagen. Door middel van het aantoonbaar maken dat een back-up dagelijks daadwerkelijk wordt uitgevoerd (bestaan) wordt aannemelijk gemaakt dat het uitvoeren van een back-up onderdeel is van de beheerprocedures. Verder wordt de werking heel beperkt getoetst. In verband met het kostenaspect wordt dit niet door de auditors zelf gedaan maar volstaat het door de gemeente zelf uitvoeren van een interne beproeving. De vastlegging van de resultaten van de beproeving en de rapportage ervan aan het management maakt het geheel enigszins controleerbaar. De meeste eisen binnen het procesdeel worden op soortgelijke wijze getoetst. Opzet, bestaan en werking van de verschillende maatregelen moeten aantoonbaar zijn om te voldoen aan de gestelde eisen. De resultaten van de audits geven aan dat gemeenten steeds beter erin slagen aan deze eisen te voldoen. Maar nadere analyse van de resultaten wijst tegelijk uit dat bij het voldoen aan de eisen veelal sprake is van 'compliance': men conformeert zich aan een door een externe instantie opgelegde norm, zonder dat sprake is van het zich eigen maken van deze norm. Bij het toetsbaar maken van opzet, bestaan en werking is er geen ander doel dan te voldoen aan de GBA-audit. Dit blijkt onder andere uit het feit dat een directe relatie tussen beveiligingsbeleid en beveiligingsplan enerzijds en de beveiligingsprocedure vaak ontbreekt, rapportages vlak voor de GBA-audit plaatsvinden en duidelijk niet het doel hebben een beeld te geven van de inhoudelijke werking van procedures, verantwoording aan verschillende managementniveaus wordt afgelegd en algemeen gesproken slechts aandacht wordt besteed aan zaken die door het agentschap BPR verplicht zijn gesteld. De verklaring hiervoor is naar onze mening dat niet de beschikbaarheid van de GBA als uitgangspunt wordt genomen voor de inrichting van de beheerprocessen, maar de vragenlijst van het agentschap BPR. De opzet van deze vragenlijst is niet direct terug te voeren op de genoemde kwaliteitsaspecten, wat ertoe leidt dat maatregelen niet in relatie tot elkaar staan en afzonderlijk van elkaar worden beschouwd, met als enig doel te slagen voor de GBA-audit. En zoals gezegd, dat lukt ook steeds beter. Navraag bij buurgemeenten maakt snel duidelijk hoe aan de auditeisen kan worden voldaan, maar het waarom van de getroffen maatregelen is natuurlijk een veel essentiëlere vraag die echter zelden wordt gesteld. Het gevaar van 'papieren tijgers' ligt bij handhaving van de huidige beoordelingssystematiek toch weer op de loer, ondanks een verbreding van de scope van de audit naar het toetsen van bestaan en werking. Inhoudelijke normen ter bepaling van de kwaliteit van een procedure of rapportage ontbreken immers.

Een oplossing voor deze constatering zou kunnen zijn de bestaande vragenlijst te vervangen door een (met het 'Handboek Toetreding tot de GBA' vergelijkbare) checklist op basis van een beperkte risico analyse, die opzet, bestaan en werking van de te treffen maatregelen op een meer begrijpelijke en hanteerbare wijze relateert aan een binnen de gemeente verankerd beleid dan nu het geval is. Dat houdt tevens in dat er een gradatie moet worden aangebracht in de verschillende maatregelen. De aanwezigheid van een informatiebeveiligingsbeleid dat eisen stelt aan beschikbaarheid, integriteit en vertrouwelijkheid van de GBA is van een wezenlijk andere orde (want voorwaardenstellend) dan de aanwezigheid van een procedure voor het ongedaan maken van verkeerde verstrekkingen (die slechts een ondergeschikt uitvoeringsaspect dekt). Het risico dat maatregelen worden genomen zonder inzicht in de samenhang kan met het bieden van een duidelijk raamwerk voor de opzet ervan naar onze mening sterk worden verkleind.

Met name de vraag wat in het informatiebeveiligingsbeleid geregeld moet worden stelt veel gemeenten voor problemen. Hoewel de opstelling van het beleid een binnengemeentelijke verantwoordelijkheid is, is het naar onze mening niet nodig alle gemeenten opnieuw het wiel te laten uitvinden. Een uitgewerkt voorstel als basis voor samenhang tussen de volgende stappen (uitvoeren risico-analyse, bepalen 'gap' tussen feitelijke en gewenste situatie,

inventariseren van genomen en nog te nemen maatregelen, opstellen en beheren van procedures, verantwoording regelen) kan veel gemeenten een stuk verder helpen dan nu het geval is bij de GBA-audit. En hoewel de audit primair bedoeld is als beoordelingsinstrument, de bedoeling is ook dat de gemeente met concrete aanbevelingen de kwaliteit van de GBA op een hoger plan kunnen brengen.

Het privacydeel van de GBA-audit
Het privacydeel van de GBA-audit richt zich met name op het kwaliteitsaspect vertrouwelijkheid (exclusiviteit). De te toetsen maatregelen hebben allemaal het doel het gebruik van de in de GBA vastgelegde gegevens te relateren aan de binnen de gemeentelijke organisatie te onderscheiden bevoegdheden, dit gebruik te beperken tot datgene wat voor de taakuitvoering noodzakelijk is en de rechten van de burger op vertrouwelijkheid van zijn gegevens te waarborgen. Uit de ervaringen met de audits tot nu toe blijkt dat veelal een inhaalslag noodzakelijk is geweest om de vertrouwelijkheidseisen te verankeren in formele regelgeving (beheerregeling en verordening), maar op dat terrein is inmiddels veel ten goede veranderd. Binnen de huidige norm is er naar onze mening nog wel een accentverschuiving noodzakelijk om de hanteerbaarheid van de eisen in relatie tot het te beheersen kwaliteitsaspect te vergroten. Nadruk moet dan uitgaan naar die eisen die de integriteit waarborgen, in termen van de huidige vragenlijst eis 11 (gegevensverwerking), eis 12 (verordening), eis 14 (beheerregeling GBA) en eis 17 (autorisatie binnengemeentelijke afnemers). Bij eis 11 kan gedacht worden aan een relatie met de inhoudelijke audit door de betrouwbaarheid van de gegevensverwerking te toetsen aan de binnen een verwerkingsproces aangebrachte functiescheiding. Een en ander mag wat ons betreft ten koste gaan van de eisen ten aanzien van protocollering, inzagerecht en geheimhouding van gegevens. Het vastleggen van deze rechten in binnengemeentelijke procedures voegt naar onze mening weinig tot niets toe aan de mogelijkheid voor de burger om van deze rechten gebruik te maken (wat overigens zelden gebeurt).

Tot slot
De GBA-audit is volgens ons duidelijk aan een grondige revisie toe. Niet omdat het instrument haar waarde niet heeft bewezen, maar omdat de grenzen van de mogelijkheden om binnen de huidige opzet van de audit de kwaliteit van de GBA te verbeteren wel zijn bereikt. Daarbij moet uiteraard wel worden bedacht dat de audit als instrument altijd een compromis zal blijven tussen datgene wat uit oogpunt van controleerbaarheid van de kwaliteitsaspecten wenselijk is en wat uit kostenoverwegingen mogelijk is. De grootste winst is naar onze mening te behalen uit een opzet die meer verband legt tussen de tot nu toe relatief van elkaar onderscheiden onderdelen (inhoud, proces en privacy) van de audit door deze onderdelen te relateren aan een informatiebeveiligingsbeleid, dat de in dit artikel genoemde kwaliteitsaspecten volledig onderbouwt.

In dit artikel is op verschillende plaatsen een voorzet gedaan om te komen tot een verbetering van de GBA-audit als toetsinstrument voor de kwaliteit. Daarbij hebben wij onze ervaring bij de uitvoering van GBA-audits gebruikt om een aanzet te geven tot verdere discussie, die hopelijk navolging krijgt binnen de tijd die ons rest tot een natuurlijk moment daar is om de regelgeving bij te stellen. Dat moment komt in september 2005, als de derde ronde audits start. U bent van harte uitgenodigd om voor die tijd een bijdrage te leveren aan deze discussie.

Drs. G. Lütter CISA is bij BMC manager van de marktgroep Persoonsinformatie, die zich onder andere bezighoudt met de uitvoering van GBA-audits en het opstellen van (gemeentebreed) beveiligingsbeleid en -plannen. Drs. M.B.H. IJpelaar CISA is mede verantwoordelijk voor de beoordeling van de resultaten met betrekking tot het proces- en privacydeel van de door BMC uitgevoerde GBA-audits.