Controle op controle

Informatiebeveiliging staat steeds meer op de gemeentelijke agenda. Terecht want de afhankelijkheid van ICT is fors toegenomen. De bedreigingen nemen ook toe. Het antwoord zou moeten zijn dat we beveiliging steeds meer benaderen vanuit perspectief van risicomanagement, niet in nog meer externe controles.

In de praktijk nemen echter het aantal audits, zelfevaluaties en vragenlijsten over informatiebeveiliging fors toe. Tilburg heeft tien externe en drie zelf opgelegde audits. Informatiebeveiliging verzandt daarmee.

De essentie van auditing is controle achteraf door objectieve buitenstaanders. De energie zou beter in het tijdig signaleren, het voorkomen van en het adequaat reageren op incidenten moeten zitten. De meeste audits zijn niet gericht op toetsing van de werking. Audits zijn gericht op de toets of op papier (opzet) aangetoond is dat de processen administratief juist verlopen (bestaan). Of er ook echt doorlopend in de praktijk naar gehandeld wordt (werking), is lastiger en buiten scope. Veel audits toetsen de administratieve en niet de technische processen. Risico's worden echter steeds meer door ICT bepaald en begrensd. Daarom is het nemen van technische beveiligingsmaatregelen doorgaans effectiever.

Waarom lukt de risicobenadering niet? Daar is een aantal redenen voor.

- ICT is lastig te doorgronden en complex. De politieke top wil toch zekerheden inbouwen; imagoschade moet worden voorkomen. Een externe audit geeft houvast.
- Het overheidsapparaat toont risicomijdend gedrag. Vluchten in regels en toezicht is een standaardoplossing. Het uitvoeren van risico analyses is lastig en vooral het accepteren van risico's, omdat dit een goed instrumentarium vergt.
- Verzet vanuit de werkvloer. Gemeenten hebben een complexe architectuur en dynamisch IT infrastructuur. De mensen die dit draaiend moeten houden, zitten niet op extra werk te wachten.
- Ministeries decentraliseren taken naar gemeenten maar vertrouwen niet op de kwaliteit van de uitvoering. Ministeries verlangen daarom audits en zelfevaluaties.

Onze conclusie is dat een vorm van externe onafhankelijke toetsing onontkoombaar is. Het is zaak om die zo effectief mogelijk te maken. Gemeenten hebben de BIG geadopteerd. De Informatie Beveiligingsdienst (=IBD) van het Kwaliteitsinstituut Nederlandse Gemeenten (= KING) beproeft nu een systeem van *single auditing* op haalbaarheid. Is dit dan de gewenste oplossing?

Het is een lofwaardig initiatief maar als risicomanagement geen uitgangspunt is, voorspellen we een teleurstelling,
De BIG is zo veelomvattend dat een beschrijving van de administratieve organisatie noodzakelijk wordt op alle ICT processen. Dat vergt enorme inspanning, niet alleen om dit tot stand te brengen, maar ook qua onderhoud. De scope is namelijk veel breder dan de huidige optelsom van audits. Mogelijk dat de markt hierin voorziet, maar hiermee wordt het "paard achter de wagen gespannen". De aanpak die de IBD nu ontwikkelt, resulteert voorlopig alleen in nieuwe vragenlijsten en hogere auditlast.

Wat is de oplossing? Op management niveau risicomanagement centraal stellen. De BIG niet klakkeloos invoeren als een absolute norm zoals gangbaar. Nee, het management bepaalt op basis van een risico-analyse wat relevant is. In Tilburg hanteren we de baseline daarom als leidraad en niet als norm. Vervolgens selecteer je uit de BIG de relevante beveiligingsmaatregelen. Deze keuzes moeten niet door IT worden gemaakt maar door proceseigenaren. Zorg dat je "in control" bent. Zorg er voor dat de proceseigenaren zeggen wat ze gaan doen, doen wat ze zeggen, laten zien dat ze gedaan hebben wat ze hebben beloofd. Werk aan je verbetercyclus. Wanneer je vaststelt dat een kwetsbaarheid een bedreiging vormt, neem dan maatregelen. Kijk steeds of het beter kan.

Ondanks het wantrouwen vanuit de rijksoverheid en druk van accountants, moeten we blijven inzetten op zelfregulering en visitatie. Het is daarom van belang dat we zorgen dat gemeenten en auditors *samen* nagaan of alle wezenlijke risico's adequaat zijn afgedekt.

Rob Bots, security officer gemeente Tilburg
René IJpelaar, IT auditor BKBO

De rubriek opinie staat open voor leesbare, opiniërende bijdragen die betrekking hebben op actuele zaken in het openbaar bestuur. De maximale lengte voor inzendingen is 600 woorden. Inzendingen graag naar: info@binnenlandsbestuur.nl o.v.v. "Rubriek Opinie". Via dit email adres kunt u ook reageren.