Auteur: Renco Schoemaker is senior adviseur informatiebeveiliging en privacy en werkt als zelfstandige onder de naam `qeep IT safe' voor (lokale) overheden. Hij is bereikbaar via r.schoemaker@qeep.nl.

Aanbesteden en informatiebeveiliging – drie smaken

Aanbesteden is een vak op zich omdat het gebonden is aan de nodige regels. Als CISO wil je graag dat informatiebeveiligingseisen aan het begin van het (inkoop)proces worden meegenomen: security-by-design. In de praktijk van de afgelopen jaren zie ik dat opdrachtgevers vrij veel tijd kwijt zijn met het bedenken van (dezelfde) eisen of zeer gedetailleerde eisen stellen. In dit artikel werk ik drie smaken uit van het opnemen van informatiebeveiliging in een aanbesteding.

In overheidsland wordt er heel wat aanbesteed. Aanbesteden is een vaak wettelijke verplichte methode van inkoop waarbij de opdrachtgever kenbaar maakt welke opdracht er aan komt. Een aanbesteding gaat gepaard met een programma van eisen waar inschrijvers aan moeten voldoen indien zij een offerte wensen in te dienen. Aan het einde van de rit wordt de opdracht gegund aan één inschrijver.
Het idee achter aanbesteden is dat uiteenlopende aanbieders (groot én klein) overheidsopdrachten kunnen binnenhalen en overheden een grotere kans hebben op een optimale prijs-kwaliteitverhouding. Of dat lukt valt te bediscussiëren, maar liever zoom ik in op informatiebeveiliging. Wordt daar een optimale prijs-kwaliteit behaald? Aan welke knoppen valt te draaien om zo invloed op die prijs-kwaliteit uit te oefenen?

De drie smaken

Het van toepassing verklaren van de juiste inkoopvoorwaarden en format verwerkersovereenkomst is het eenvoudige werk. Hoe ga je als opdrachtgever, informatiebeveiliging opnemen in het programma van eisen? Dat kan op de volgende drie manieren:

1. **Geschiktheidseisen**: met geschiktheidseisen toetst een opdrachtgever of een inschrijver geschikt is om de opdracht uit te voeren. Dit zijn dus eisen die gesteld worden aan een bedrijf.
2. **Gunningseisen**: met gunningseisen toets een opdrachtgever of de IT-oplossing van de inschrijver voldoet aan het gewenste 'niveau'. Dit zijn dus eisen die gesteld worden aan de IT-oplossing.
3. **Gunningscriteria**: met gunningscriteria toetst een opdrachtgever bij het Beste Prijs-KwaliteitsVerhouding (BPKV) criterium wat de beste inschrijving is. Dit zijn dus geen eisen waaraan moet worden voldaan, maar (selectie)criteria voor gunning.

Smaak 1: Geschiktheidseisen

Dit zijn eisen die gesteld worden aan een bedrijf, ofwel de inschrijver. Andersom kunnen dit dus geen eisen aan de IT-oplossing zijn die wordt aangeboden. Toegepast op informatiebeveiliging is mijn advies om als geschiktheidseis het hebben van een managementsysteem voor informatiebeveiliging dat voldoet aan de eisen van ISO 27001, NEN 7510 of gelijkwaardig op te nemen. Dat is bewust wat voorzichtig geformuleerd omdat de wetgever heeft bepaald dat 'of gelijkwaardig' moet worden toegevoegd en daarom kan je niet alleen als geschiktheidseis het hebben van bijv. een ISO 27001 certificaat opnemen.
Voldoen aan deze eis voor een 'managementsysteem voor informatiebeveiliging' gaat natuurlijk het eenvoudigst door het overleggen van een ISO 27001 of NEN 7510 certificaat. Enkele aandachtpunten daarbij:

- het moet gaan om een managementsysteem bij de inschrijver zelf;
- het certificaat dient te zijn afgegeven door een daartoe geaccrediteerde organisatie;
- de bijbehorende Verklaring van Toepasselijkheid (VVT) mag niet ontbreken.

Eventueel kun je op voorhand aangeven welke beheersmaatregelen wel/niet 'buiten scope' mogen zijn in de VVT. Tot slot is het van belang te definiëren op welke wijze de opdrachtgever vaststelt hoe het managementsysteem voldoet aan de eisen van ISO 27001 of NEN 7510 zónder dat de inschrijver één van beide certificaten kan tonen. Het managementsysteem heeft wat mij betreft minimaal een actueel en compleet kwaliteitshandboek informatiebeveiliging, een beveiligingsorganisatie en een jaarlijkse, onafhankelijke toetsing op de getroffen beveiligingsmaatregelen.
Ik zie te weinig dat informatiebeveiliging is opgenomen als geschiktheidseis bij aanbestedingen, terwijl het wel vaak als

Inkoopvoorwaarden en verwerkersovereenkomst

Het van toepassing verklaren van de ARBIT (rijksoverheid) GIBIT (gemeenten) als inkoopvoorwaarden voor IT-opdrachten lijkt me een open deur. Dat moet je zeker doen indien het hoofdonderwerp van de aanbesteding dat toelaat. Niet iedereen zal positief reageren op dit standpunt en ik kan het boek 'Reset de gemeentelijke ICT' van Kees Groeneveld en Herman Timmermans in dat licht aanbevelen.
Indien er persoonsgegevens worden verwerkt binnen de opdracht die wordt aanbesteed, stel dan een format verwerkersovereenkomst verplicht. Een tweede open deur gezien het verplichtende karakter van het VNG-format voor gemeenten. Voor de rijksoverheid is er een model dat aansluit op de ARBIT, maar het gebruik daarvan is niet verplicht.

De drie smaken zijn uitstekend met elkaar te combineren zolang je weet wat je doet; niet alle combinaties zijn logisch.

gunningseis opgenomen wordt (smaak 2). Mijn advies is hiervoor de geschiktheidseis in te zetten en níet de gunningseis. Dit omdat het managementsysteem immers primair toeziet op de inschrijvende organisatie en niet op de IT-oplossing.

Smaak 2: Gunningseisen

Dit zijn de eisen die worden gesteld aan de IT-oplossing. Hier heb je eigenlijk twee afslagen: 1) gunningseisen in aanvulling op bovengenoemde geschiktheidseis, en 2) gunningseisen zónder bovengenoemde geschiktheidseis. In het eerste geval neem je als eis nummer één op dat de IT-oplossing dient te vallen onder de reikwijdte van het al dan niet gecertificeerde managementsysteem. Vervolgens kan je eisen opnemen over bijvoorbeeld SLA, framework voor softwareontwikkeling, hardeningsrichtlijnen, logische scheiding bij cloudinfrastructuur en talloze andere, specifieke gunningseisen waar de IT-oplossing aan moet voldoen. Te denken valt aan verplichte standaarden, koppelvlakken, protocollen etc.

Ontdubbel je eisen wel met de inkoopvoorwaarden en de verwerkersovereenkomst en neem alleen specifiekere zaken op dan wat de ISO 27001 annex A al benoemt. Dus bijvoorbeeld beveiligingsmaatregelen waarvan je zeker wilt weten dat ze conform ISO ISO 2700/BIO zijn geïmplementeerd bij de IT-oplossing. Verder is het mijns inziens van (groot) belang duidelijk te benoemen (of eisen) dat de inschrijver jaarlijks middels een auditrapport – opgesteld door een onafhankelijke derde – dient aan te tonen dat de beveiligingsmaatregelen, zoals geïmplementeerd bij de IT-oplossing, werken. Indien ISO 27001/NEN 7510/gelijkwaardig als geschiktheidseis is opgenomen ben je nu klaar wat mij betreft. Heb je die geschiktheidseis (smaak 1) niet opgenomen, dan raad ik aan tenminste gunningseisen op het gebied van General IT Controls (GITC) op te nemen. Verwijs niet naar de gehele ISO27002/BIO bij de gunningseisen en ga er niet alle maatregelen uit kopiëren. Indien je ISO 27001/NEN 7510/gelijkwaardig niet of zelden als geschiktheidseis wilt opnemen, dan zou ik een standaard lijst met gunningeisen opstellen. Onthoud daarbij dat voor alle geschiktheids- en gunningseisen geldt dat níet voldoen een 'exit' betekent voor de inschrijver. Het zijn dus 'knock-out' criteria.

Smaak 3: Gunningscriteria

Zoals de naam al doet vermoeden, gaat het hier echt om iets anders. Dit zijn geen eisen aan de inschrijvende organisatie of de IT-oplossing, maar criteria waarlangs de aanbesteding gegund kan worden. Vaak zijn er uiteenlopende gunningscriteria en één of meer daarvan kan een criterium zijn op het gebied van informatiebeveiliging. Omdat er meerdere criteria zijn resulteert een slechte score op het gunningscriterium over informatiebeveiliging niet tot diskwalificatie. Sterker nog, indien deze inschrijver op andere criteria zeer goed scoort kan ze de aanbesteding winnen.

Omdat je als opdrachtgever geen zekerheid verkrijgt over informatiebeveiliging bij een gunningscriterium is het niet raadzaam informatiebeveiliging alleen op te nemen op deze wijze. Je kunt natuurlijk wel combineren met geschiktheids- en/of gunningseisen, maar voorkom overlap. In de praktijk zal natuurlijk ook hier de prijs een belangrijke factor zijn. Tezamen spreek je dan van Beste PrijsKwaliteitVerhouding (BPKV).

Smaken samenvoegen

De voornoemde drie smaken zijn uitstekend met elkaar te combineren zolang je weet wat je doet; niet alle combinaties zijn logisch en leveren derhalve een smaakvol gerecht op. Ik pleit voor meer gebruik van de geschiktheidseis op het managementsysteem volgens de eisen van ISO 27001. Uiteindelijk wil je als opdrachtgever dat de inschrijver zelf verantwoordelijkheid neemt op het gebied van informatiebeveiliging. Ik ben van mening dat je dat bereikt door genoegen te nemen met een degelijk managementsysteem dat door een geaccrediteerde organisatie is gecertificeerd, eventueel aangevuld met een pentest en/of auditrapport, en de gunningseisen echt te beperken tot het noodzakelijke. Let wel, dat kunnen nog steeds heel wat eisen zijn naar gelang de complexiteit van de uitgevraagde IT-oplossing. En benut ook de mogelijkheden van een gunningscriterium.

Inkopen is een vak, net als informatiebeveiliging. Werk daarom altijd nauw samen met een inkoopadviseur en/of aanbestedingsjurist.