Moet ik als dienstverlener een ISO 27001 certificaat hebben

Steeds meer klanten eisen van hun dienstverleners een ISO 27001 certificaat voor informatiebeveiliging. Soms is dat terecht, maar soms ook niet. Een tweetal ontwikkelingen rechtvaardigt deze klantvraag. In de eerste plaats gaan steeds meer organisaties over tot uitbesteding van processen (administratie, contact centers, datacenters, SaaS, Cloud diensten). In de tweede plaats is er de aanscherping van de privacy wetgeving, die eist dat er bewerkersovereenkomsten zijn tussen klanten en hun dienstverleners.

Waarschijnlijk deed u als dienstverlener vroeger hetzelfde voor uw klanten als nu. Maar u deed dat toen op projectbasis of op basis van uurtje-factuurtje. De opdrachtgever was verantwoordelijk voor uw werkzaamheden, want u liet netjes alle plannen goedkeuren en bood de resultaten van uw inspanningen aan ter acceptatie. Toen klanten vaker gingen aanbesteden, werd uw bedrijfsrisico natuurlijk hoger. Dat had echter geen invloed op de eisen aan informatiebeveiliging. Maar daarop komen we verderop in dit artikel nog terug .
Als u nu nog steeds diensten levert op deze basis, dan is er geen enkele reden om ISO 27001 gecertificeerd te zijn. Slechts een ISO 9001 certificaat kan dan (vooral commerciële) waarde hebben.

Trend van uitbesteding en continuïteit in dienstverlening

De laatste decennia is de trend ontstaan dat organisaties bedrijfsprocessen uitbesteden. Onder het motto ‘back to the core business’ geldt dat vooral voor ondersteunende processen. Het begon met goed af te bakenen processen als catering, beveiliging, transport en salarisverwerking. Tegenwoordig geldt het echter ook voor complexere ondersteunende diensten als ICT, administratie, en contactcenters. Dienstverleners voeren een stukje bedrijfsproces van de klant uit en zijn daar dan ook operationeel verantwoordelijk voor. De klant verwacht wel, dat de leverancier het uitbestede proces beter en goedkoper kan leveren dan voorheen. Maar leveranciers spelen hier graag op in. Voor hen houdt dit immers in, dat er vaak langjarige business gedaan kan worden zonder acquisitiekosten.
Voor u als dienstverlener betekent dit natuurlijk wel, dat uw bedrijfsrisico wat hoger wordt. Want wilt u schaalvoordelen behalen, wanneer u uw dienst aan veel klanten kunt leveren, dan zult u moeten investeren in de standaardisatie van de dienst.
Waarschijnlijk bent u redelijk opportunistisch (anders was u immers niet ondernemer geworden). U rekent niet op problemen met het vaker verkopen van uw dienst. U zorgt in elk geval voor een scherpe prijs, zodat u omzet stijgt. En u verwacht dat dat zeker zal gebeuren, als u er ook nog wat extra salespower tegenaan gooit. En de klant is en blijft eindverantwoordelijk voor de kwaliteit van uw werk. De wet zit immers zo in elkaar, dat u alleen verantwoordelijk bent voor (een deel van) directe schade, mocht die ontstaan, en niet voor gevolgschade. De meeste van uw klanten zijn zich er helemaal niet van bewust, dat ze grote risico’s lopen als u een wanprestatie levert.

Privacy wet schudt klanten wakker

De ontwikkelingen in de Algemene Verordening Gegevensbeschering (AVG/GDPR) hebben echter veel organisaties wakker geschud. In de wet staat nadrukkelijk dat uw klant verantwoordelijk is voor iedere inbreuk op de privacy, ook al ligt de schuld daarvan bij een andere partij, bijvoorbeeld een bewerker zoals u. De boete voor dergelijke inbreuken is echter opgetrokken van € 4500 naar ruim 8 ton. Klanten beginnen zich zorgen te maken. Ze willen u aansprakelijk kunnen stellen voor fouten die u maakt en ook voor de gevolgschade van de boete. En de wet schrijft netjes voor, hoe uw klant dit moet regelen. Als verantwoordelijke moet de klant met u een verwerkersovereenkomst sluiten waarin hij onder andere aangeeft aan welke beveiligingseisen u moet voldoen bij het verwerken en opslaan van persoonsgegevens. Bovendien moet hij periodiek controleren of u die eisen naleeft. Dat

bezorgt uw klant een hoop overlast (en kosten). En u zult hier ook niet blij mee zijn. Want klanten komen allemaal met hun eigen eisen met betrekking tot de verwerking en opslag van hun gegevens en de beveiliging hiervan. En behoefte aan controle van al uw verschillende klanten, heeft u ook helemaal niet.

ISO 27001 als praktische oplossing

Als u als dienstverlener niets doet, dan kunt u erop rekenen dat vrijwel iedere klant in de komende jaren u een verwerkersovereenkomst laat tekenen en de naleving daarvan komt controleren. De standaardisatie van uw dienst en de beoogde schaalgrootte kunt u dan wel vergeten. U zult ook die verwerkersovereenkomst en die controle moeten standaardiseren. Een ISO 27001 certificaat voor informatiebeveiliging biedt dan uitkomst. In uw ISO 27001 management systeem legt u vast aan welke beveiligingseisen u voldoet en vervolgens beoordeelt een onafhankelijke auditor of u inderdaad de door u gekozen maatregelen binnen de door u gekozen scope naleeft en hij rapporteert hierover aan u. U stelt vervolgens op basis hiervan een bewerkersovereenkomst op, die u voorlegt aan al uw klanten. Op deze manier heeft de klant zijn privacy risico afgedekt en hoeft hij ook niet meer zelf de controle op naleving te doen. Die controle wordt immers gedaan door de auditor.
Misschien schrikt u even, dat ik ISO 27001 naar voren schuif als praktische oplossing. Maar ondanks alle indianenverhalen over ISO certificaten gaat het er om in control te zijn en in de basis is dat heel eenvoudig. Het komt neer op: “Zeg wat je doet, doe wat je zegt en laat zien dat je dat gedaan hebt”. ISO-normen van tegenwoordig gaan met name over dat laatste: de aantoonbaarheid van wat je doet binnen de door jezelf bepaalde scope. Het enige, wat de norm eist is dat je in control bent ofwel dat je je afspraken nakomt, ook wat betreft de bewerkersovereenkomst. En uiteraard word je alleen geaudit op maatregelen die relevant voor je diensten zijn.

Scope van uw ISO 27001

Natuurlijk zijn er meerdere bedrijfsactiviteiten, waarbij u werkt met informatie van klanten/leveranciers/personeel/andere. Deze kunt u deels buiten de scope van ISO 27001 houden. Advies, ondersteuning en projecten doet u vaak onder verantwoordelijkheid van de klant. De klant is en blijft verantwoordelijk voor de informatiebeveiliging op deze gebieden. U bent daarvoor niet verantwoordelijk. Mogelijk zal wel een geheimhoudingsovereenkomst (NDA) getekend moeten worden. Maar dat is niet nieuw.
Vaak komt er in projecten vertrouwelijke informatie op tafel. Van belang is dat hier netjes mee omgegaan wordt en dat dit ook contractueel wordt vastgelegd.
Er zijn meestal 2 soorten van informatie te onderscheiden.

1. vertrouwelijke informatie van de klant;
2. vertrouwelijkheid van projectresultaten.

Het eerste punt is hard en moet beveiligd worden conform de standaards van de klant. Als u deze informatie opslaat in uw eigen netwerk, dan geldt ook daarvoor de bewerkersovereenkomst en valt dit dus binnen de scope van ISO 27001. Voor de tweede soort geldt, dat deze in feite nog geen status heeft, zolang het projectresultaat niet geaccepteerd is door de opdrachtgever. Tot die tijd kunt u dit projectresultaat in een eigen directory bewaren, die onder het beheer van uw organisatie valt. Het valt dan nog niet binnen de scope van ISO 27001. Zodra de opdrachtgever de resultaten geaccepteerd heeft, dan krijgt de informatie een andere status en als u het dan niet verplaatst naar een veilige omgeving, dan betekent dit dat ook de totale directory structuur binnen de scope valt van ISO 27001. En dat wilt u uiteraard niet. U wilt immers bij het werken in die directory structuur u vooral veel vrijheid hebben.
De kortste klap is om een aparte projectomgeving te creëren, die voldoet aan de eisen van de klant

en waarvoor de klant dan ook verantwoordelijk is. Deze omgeving valt dan niet binnen uw scope van ISO 27001. Alle mensen, die werken aan het project hebben toegang tot die omgeving en kunnen informatie uploaden en onder condities bewerken. Als deze omgeving gebaseerd is op een document management systeem, dan heeft u automatisch alle functionaliteit, die nodig is om dit adequaat te beveiligen. Azure (de cloud oplossing van Microsoft) voldoet hier bijvoorbeeld aan. Voor een paar euro extra kunt u daarin Sharepoint in draaien. Maar ook een projectomgeving op de infrastructuur van de klant is natuurlijk goed. Bijkomend voordeel is dat vertrouwelijk informatie niet meer per mail gestuurd hoeft te worden, zodat ook mobieltjes, tablets en laptops, waarop u ook vaak zakelijke mails ontvangt, buiten de scope van ISO 27001 kunnen blijven.
Aan het einde van het project worden de projectresultaten dan overgedragen aan de beheerorganisatie en kan de projectomgeving opgeheven worden. Natuurlijk valt die beheerorganisatie wel binnen de scope van ISO 27001. Het is dus zaak om voor die beheerorganisatie een eigen omgeving te creëren, waarop uiteraard security by design wordt toegepast, zodat de beveiligingskosten minimaal kunnen blijven.

Diensten die wel altijd binnen de scope van uw ISO 27001 vallen zijn:

- gegevensverwerking voor klanten op een platform, dat uw eigendom is;
- beheer van platformen die eigendom zijn van de klant;
- gebruik van uw bronbestanden door de klant.