Certificering tegen de Code voor Informatiebeveiliging bij het CAK-BZ

In 1994 kwam de Nederlandse vertaling van de British Standard 7799, de Code voor Informatiebeveiliging, ter beschikking. Naast het gebruik als leidraad voor implementatie kan de Code gebruikt worden als maatstaf voor de kwaliteit van de beveiliging bij informatie-uitwisseling tussen organisaties. Het beoordelen van deze kwaliteit met als norm de Code voor Informatiebeveiliging werd mogelijk na het beschikbaar komen van een certificatieschema door ICIT en door het aanstellen van een tweetal certificeerders (KEMA en KPMG) door de Raad voor Accreditatie. Het aantal gecertificeerde organisaties is relatief klein maar dit zal in de nabije toekomst veranderen omdat diverse organisaties reeds bezig zijn met het implementatie- en certificatietraject. In dit artikel wordt een dergelijk implementatietraject, inmiddels met succes afgesloten met certificatie door KEMA Registered Quality BV, besproken. De organisatie in kwestie is daarmee de eerste in het MKB in Nederland gecertificeerde organisatie[1].

Invoering bij het MKB kan dus toch!

Op de door het NGI eind 1994 georganiseerde bijeenkomst in Amsterdam waar de Code voor Informatiebeveiliging werd geïntroduceerd verzuchtte de heer E. Kruiderink, toenmalig algemeen directeur van het Instituut voor het Midden- en Kleinbedrijf (IMK) al dat kleinere ondernemingen niet de mogelijkheden hebben ingewikkelde procedures in te voeren. Daarom is een op het middenbedrijf gerichte Code nodig. "Het moet met die Code niet gaan als met die ISO-9000-regelingen die de ondernemer enorm veel tijd kosten om te implementeren"[2].
Na hem sprak de heer G. Kusters van Kusters Engineering welke bevestigde dat implementatie aldaar een kwestie van jaren was. (Voor de ervaringen zie het artikel genoemd in voetnoot 1.)

De organisatie

Het Centraal Administratie Kantoor Bijzondere Zorgkosten (het CAK-BZ) te Den Haag verricht als uitvoerder namens de overheid de betaling van bedragen aan inrichtingen voor het verlenen van AWBZ-verstrekkingen. Ook registreert het CAK-BZ de vaststelling en de betaling van de zogenoemde eigen bijdragen voor de AWBZ. Voor een groot deel van de aanspraak op thuiszorg geldt een inkomensafhankelijke eigen bijdrage per uur waarvan het CAK-BZ de hoogte bepaalt en de inning verzorgt.

Zoals de laatste tijd al uit de media duidelijk wordt gaat er in dit circuit veel geld om. Het jaarverslag van het CAK-BZ over 1998 spreekt over een totale geldstroom van ruim 20 miljard gulden. Ongeveer 400 miljoen gulden per week dus! Voorts is het aantal cliënten van de thuiszorg bijzonder groot; in 1998 kende het CAK-BZ alleen al ruim 227.000 bijdrageplichtigen waarmee 2,3 miljard per jaar gemoeid is. Er worden t.b.v. de eigen bijdrage thuiszorg bijna 5 miljoen nota's per jaar verzonden. Het mag dus duidelijk zijn dat de informatie rond deze bedrijfsprocessen goed beveiligd moet worden.

Vanaf januari 1997 werd het CAK-BZ door de overheid verantwoordelijk gesteld voor de inning van de eigen bijdrage voor thuiszorg. In enkele maanden tijd groeide de organisatie van 30 naar ruim 150 mensen. Er moest een callcenter komen en de bedrijfsprocessen en de ondersteunende ICT werden totaal vernieuwd. De nieuwe adjunct-directeur ICT realiseerde zich dat met deze nieuwe, sterk toegenomen sociale en politieke verantwoordelijkheid van het CAK-BZ met name de beschikbaarheid van de informatiesystemen de allerhoogste prioriteit diende te krijgen. Een storing in de bedrijfsprocessen zou bijvoorbeeld vrij snel tot kamervragen kunnen leiden.

---

[1] Een zeer lezenswaardig artikel over de pilot van implementatie binnen het MKB is gepubliceerd in IT Management [Select] nummer 4, jaargang 1996
[2] Automatisering Gids, week 50 van 1994

Automatisering bij het CAK-BZ

Het CAK-BZ heeft bijna 200 medewerkers gehuisvest in een kantoorpand in Den Haag. Vrijwel alle medewerkers gebruiken een geautomatiseerde werkplek gekoppeld aan een Unisys mainframe, Unix mini's en Windows NT servers. Er wordt gebruik gemaakt van standaard kantoor applicaties en van zelf ontwikkelde software gebaseerd op Oracle databases. Inkomende post, voornamelijk vanuit de zorgkantoren, wordt direct na binnenkomst gescand en digitaal opgeslagen. Gegevensuitwisseling met de zorgkantoren, de thuiszorginstellingen, belastingdienst en het betalingsverkeer vindt nog vrijwel uitsluitend via tapes en diskettes en papier plaats.

De eigen ontwikkelde software wordt ook aan de markt aangeboden; een aantal zorgkantoren gebruikt deze software, waarvoor een kleine ontwikkelafdeling aanwezig is. De afdeling systeembeheer ter ondersteuning van alle ICT bestaat uit 8 mensen.

De aanloop tot het project

Bij de verhuizing van een drietal kleine panden in Den Haag naar een nieuw bedrijfspand werd de kans aangegrepen om een project te starten voor de inrichting van een eigen uitwijkcentrum in één van die bestaande panden.

Medio 1998 was de inrichting van de uitwijkvoorziening en de ontwikkeling van de benodigde procedures zoals een uitwijkhandboek (ontwikkeld met de DRM Toolkit[3]) gereed.

Uiteraard is naast beschikbaarheid ook de integriteit en de vertrouwelijkheid van de informatievoorziening bij het CAK-BZ belangrijk. De inrichting van de uitwijkvoorziening maakte, evenals een eerder ontwikkeld ontruimingsplan (volgens de ARBO wetgeving verplicht), deel uit van een integraal informatiebeveiligingsplan (zie figuur).

De adjunct-directeur ICT gaf opdracht aan Getronics tot ontwikkeling van een (deel-)projectplan om ook aan de genoemde andere twee kwaliteitsaspecten zorg te besteden. Geadviseerd werd een openbare norm te kiezen bij implementatie. Omdat de verwachting is dat het CAK-BZ in de toekomst veel meer zal moeten verantwoorden aan partners dat informatie bij haar in goede handen is, werd gekozen voor de Code voor Informatiebeveiliging als norm. De Code heeft immers een breed draagvlak en is zeker bekend bij de overheid; een belangrijke partner van het CAK-BZ.

Begin 1999 gaf het directieteam van het CAK-BZ unaniem de opdracht om dit project te starten en het project af te sluiten met certificatie. Gekozen werd voor een getrapt project; in eerste instantie invoering alsmede certificatie van de 10 sleutelmaatregelen uit de Code gevolgd door een risicoanalyse (gekozen is voor CRAMM; zie ook eind van het artikel). De uit de risicoanalyse voortkomende overige meest belangrijke maatregelen worden in de laatste fase van het project aangepakt.

Kosten en doorlooptijd

Eind maart 1999 startte het project formeel. Op 22 oktober 1999 om 14:07 uur meldde Frank Otte, auditor van KEMA, dat het CAK-BZ voor certificatie in aanmerking kwam[4]. De doorlooptijd voor het project was dus precies 7 maanden.

De planning ging uit van een afronding voor de zomer en een inspanning van de externe partner van 22 consultancy dagen. Afronding was dus later; de inspanning (de voornaamste kostenpost) van de externe partner kwam uiteindelijk op 29 consultancy dagen.

---

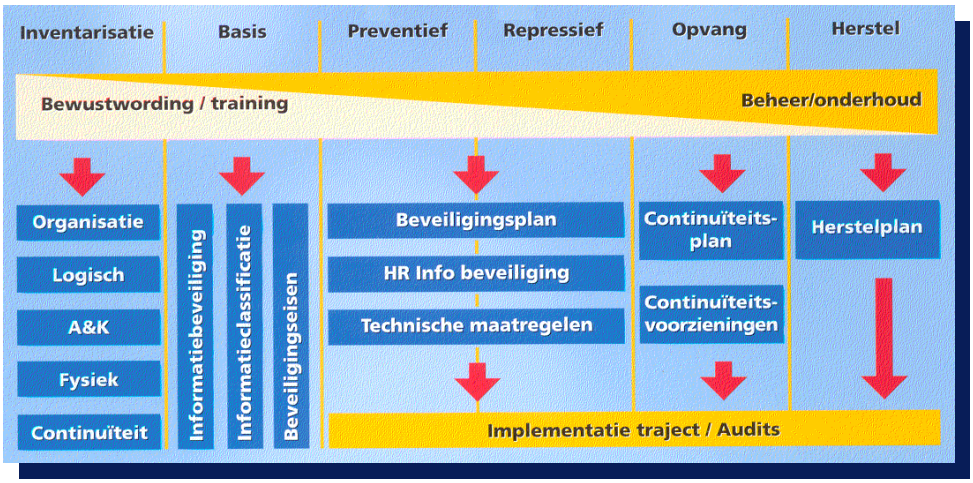
[3] Software om op basis van de Disaster Recovery Methodology van Getronics een continuïteitsplan te ontwikkelen en te onderhouden

[4] Het certificaat is door KEMA aan het CAK-BZ overhandigd tijdens de nieuwjaarsreceptie op 5 januari 2000

Bij implementatie van de Code voor Informatiebeveiliging blijkt hoofdstuk 9, continuïteitsplanning, voor veel organisaties het grote struikelblok qua benodigde inspanning. Bij het CAK-BZ was dus reeds veel aandacht voor dit onderwerp waardoor in het relatief geringe aantal dagen een project als dit mogelijk was. Wel was voor continuïteitsplanning nog zeker aandacht nodig; opzet en bestaan was gewaarborgd maar werking diende nog bewezen te worden middels gedocumenteerde uitwijktesten. Het plannen van uitwijktesten werd bemoeilijkt doordat in dezelfde periode ook millenniumtesten plaats moesten vinden. (Dat project is overigens na een audit van de Tüv - de Duitse pendant van KEMA - goedgekeurd, maar dit terzijde.)

De projectaanpak

Met MS-Project werd een projectplan ontwikkeld volgens de Getronics methodiek (zie figuur 1) waarin de resources (mensen, tijd) gebaseerd werden op empirisch bepaalde waarden uit vorige projecten.



Figuur 1 : De componenten van een integraal informatiebeveiligingsplan

De projectorganisatie bestond uit een senior consultant en een consultant van de externe partner, de adjunct-directeur ICT alsmede de manager systeembeheer en ondersteuning van het CAK-BZ.

In april zijn interviews gehouden met de proceseigenaren en is door middel van vragenlijsten de huidige status van de informatiebeveiliging, ten opzichte van het door de gekozen norm vereiste niveau, bepaald. Deze vragenlijsten, gebaseerd op de 'geest' van de Code voor Informatiebeveiliging zijn door Getronics Business Continuity voor eigen gebruik ontwikkeld. Als 'second-opinion' is ook gebruik gemaakt van de elektronische vragenlijst SecurityPAC van CPA.. In de toekomst zal de aanstaande checklist van het NGI uiteraard voor dit doel goed bruikbaar zijn.

Vrijwel elke week kwam het projectteam bij elkaar. De manager systeembeheer delegeerde waar nodig de te ontwikkelen procedures aan de systeembeheerders. Ondertussen werkten de

consultants aan het beveiligingsbeleid en het beveiligingsplan.

Deze twee documenten werden gebaseerd op in de praktijk bewezen documenten van een grootbank, een grootindustrieel, Nivra geschrift 53 en de ITIL module Security Management.

Middels levendige e-mail uitwisselingen via alle moderne communicatiemogelijkheden (o.a. GSM<->laptop koppelingen) werden de partijen op de hoogte gehouden van de laatste ontwikkelingen.

De gehouden interviews met de proceseigenaren resulteerden in een goed overzicht van de te ondernemen acties. Hoogste prioriteit diende te krijgen:

- documentatie van het beveiligingsbeleid;
- schriftelijk vastleggen van alle reeds aanwezige procedures en werkinstructies; met name rond viruscontrole;
- uitwijktesten;
- inrichting van een beveiligingsorganisatie en training van de betrokken medewerkers;
- bewustwording en voorlichting aan de medewerkers.

Enthousiasme voor informatiebeveiliging; ook dat kan!

Gezien het enthousiasme binnen de organisatie was het mogelijk de externe partner als kennisbron te gebruiken; monitoring van de dagelijks voortgang van de onderkende acties was uitstekend te beleggen binnen de organisatie zelf. Het mag duidelijk zijn dat in andere organisaties het trekken van een project als dit veel meer aandacht kan vergen. Dit enthousiasme kwam tot stand doordat de sector ICT nu een directe kans kreeg haar kwaliteit te bewijzen aan de rest van de organisatie. Te vaak staat een ICT afdeling onder vuur bij snelle veranderingen binnen een organisatie en dan kan een project als dit dus een enorme motivatie teweeg brengen. Na alle publicaties met als onderwerp het moeilijk motiveren van medewerkers voor dit onderwerp eens een welkome afwisseling.

Specifieke problemen gedurende het project.

Hoewel gesteld mag worden dat de eerste fase van dit project (de 10 sleutelmaatregelen inclusief certificatie) zonder meer zeer succesvol is afgesloten zijn er uiteraard een aantal problemen en knelpunten geweest.

De enorme groei van het CAK-BZ betekent dat een aantal benodigde documenten om een goed beveiligingsbeleid te formuleren, denk aan een informatiebeleid, een ondernemingsbeleid en procesbeschrijvingen, niet, of slechts in conceptvorm, aanwezig waren. Hierdoor zijn uiteindelijk negen versies van het informatiebeveiligingsbeleid noodzakelijk geweest voordat consensus over de inhoud verkregen werd.

De leesbaarheid van het uiteindelijke document liet op een gegeven moment te wensen over waardoor besloten is het document te splitsen in een apart beleidsdocument en een implementatieplan.

Een structuurprobleem bij de Code voor Informatiebeveiliging is dat het documenteren van 'opzet en bestaan' van een aantal maatregelen (zoals beleid en toewijzing van verantwoordelijkheden) dan in het beleidsdocument en implementatie van de overige maatregelen in het implementatieplan terechtkomt. Het ene document kan daardoor helaas niet meer volledig los gelezen worden van het andere en er ontstaan doublures hetgeen tot een onderhoudsprobleem leidt.

Een cliché maar toch weer een verrassing was de grote benodigde inspanning om elke medewerker te doordringen van het belang van dit project. Sprekende voorbeelden spelen dan een belangrijke rol ("Hoe zou je het zelf vinden als je het geld waar je recht op hebt niet krijgt door een computerstoring?" en "Wat is het risico als je aan de telefoon de NAW gegevens van gescheiden partners zo maar zou verstrekken?"). Gekozen werd voor een aantal artikelen in het personeelsblad en de inrichting van een multidisciplinaire beveiligingscommissie. Ook zijn richtlijnen voor een ieder in het personeelshandboek opgenomen.

Met name de laatste maanden voor de certificering is de belangstelling voor dit project onder alle medewerkers enorm gegroeid door er veel aandacht aan te besteden tijdens het werkoverleg en door diverse presentaties door het projectteam.

Ondanks volledig commitment vanuit het directieteam bleek tijdens de proefaudit van KEMA dat kennis en absorptie van het beveiligingsbeleid en -plan nog niet op het juiste niveau was beland.

Hiertoe werden de verantwoordelijkheden voor de diverse betrokken partijen in het beveiligingsbeleid nog sterker gedocumenteerd en werd middels een voorlichtingssessie waarbij ook het voltallige directieteam aanwezig was door de projectgroep zeker gesteld dat ditmaal een ieder zijn of haar verantwoordelijkheden kende en onderkende. Ook werd expliciet gekozen voor het bieden aan elke medewerker van de mogelijkheid tot inzien van de ontwikkelde documenten middels een snelkoppeling in het Startmenu van Windows naar de documenten in Acrobat Portable Document Format (PDF). Ook krijgen gebruikers regelmatig hints dat deze documenten bestaan tijdens het aanmelden aan de werkplek.

In een eerste fase van een project als deze is het vrij moeilijk om een externe partner 'beleid' te laten ontwikkelen. Het was noodzakelijk dit uit te besteden gezien de onbekendheid van de organisatie met de materie (zeker aan de start van het project) maar uiteindelijk dient de organisatie uiteraard zelf haar beleid te documenteren. Hierdoor ademt de eerste versie van de ontwikkelde documenten nog te veel de door de externe partij geadopteerde methodiek uit en is het nu aan het CAK-BZ om toekomstige versies van het informatiebeveiligingsbeleid en de gekozen implementatie meer eigen aan de organisatie te maken. Daartoe is een beveiligingscommissie ingericht welke regelmatig beleidsvoorstellen zal doen aan de directie. Doordat de leden in die commissie komen uit de (drie) sectoren van het CAK-BZ is dit geborgd.

De beveiligingscommissie heeft ook als taak regelmatig risicoanalyses uit te voeren en het bewustzijn van werknemers m.b.t. informatiebeveiliging te meten en waar nodig te verbeteren. Een literatuurstudie leverde enige bruikbare methodieken hiervoor maar met name de NGI publicatie 'Beveiligingsbewustzijn bij gegevensbescherming' zal hierbij als leidraad dienen.

Een organisatie in beweging creëert elke dag uitdagingen met hoge prioriteiten voor haar managers en medewerkers. Het blijven motiveren van de managers om aan een project als dit aandacht te besteden bleek geen sinecure. Zeker is dat certificatie als 'stok achter de deur', hoewel absoluut geen doel op zich, daar een positieve bijdrage aan kan leveren.

Het nut van uitwijktesten maar weer eens bewezen …

Een medewerker verzuchtte dat het project geen meerwaarde bood want er werd uiteindelijk alleen maar beschreven wat men eigenlijk al lang tot routine had gemaakt. Tijdens de eerste uitwijktest bleek hoe belangrijk vastgelegde procedures echter kunnen zijn.

Anekdotisch was deze eerste volledige uitwijktest van de thuiszorg applicatie op het Unisys Unix systeem naar het uitwijksysteem. Op de bewuste vrijdagavond, na afsluiten van de productiedatabases, bleek dat het kopiëren van de datasets stuk liep (en veel langer duurde dan verwacht!) door verschillende versies van het gebruikte Unix copy script.

Het bewuste copy script gaf een schrijffout op het uitwijksysteem en hing het productiesysteem daardoor op (en Unix adepten maar volhouden dat Windows NT een slecht besturingssysteem is!). Na afbreken van de test bleek het productiesysteem ook niet meer herstartbaar (uiteindelijk bleek een slecht mechanisch contact van een harddisk de boosdoener). Een voorbeeld van operatie geslaagd (een test welke een onvolkomenheid duidelijk maakt) maar patiënt overleden! Doordat de boot image van de harddisk in een RAID configuratie opgeslagen was, was het mogelijk een tweede image te gebruiken; enkele uren later was het productiesysteem weer volledig gereed voor de productie van de maandag na het weekend.

Uiteraard heeft deze eerste uitwijktest geresulteerd in aanpassing van een aantal procedures en een herhaalde uitwijktest enkele weken later. Deze test, alsmede de test weer een maand later, voldeed wel volledig aan de verwachtingen. Niet tevergeefs; tijdens de zomermaanden 'ontplofte' een elektra schakelkast waardoor er volledige stroomuitval optrad. De oorzaak was waterlekkage vanuit het parkeerdek naar de direct daaronder gelegen schakelkast. Binnen enkele uren daarna was het CAK-BZ weer volledig operationeel. (En heeft de installateur uiteindelijk dit single-point-of-failure opgelost.)

Baten

Direct kan gesteld worden dat het CAK-BZ nu meer dan ooit bewust is van het belang van informatiebeveiliging. Het is door certificatie zeker dat het gewenste niveau ook bereikt is.

De manager Systeembeheer en Ondersteuning, Dennis Vrolijk, vond het een uitdaging om als projectleider namens het CAK-BZ te fungeren gedurende dit traject; "Dit project was namelijk voor de afdeling en mijzelf de kans om, niet alleen intern, maar ook naar buiten toe, te laten zien wat wij als ICT-afdeling qua technische kennis en middelen in huis hebben. De waardering door bekwame externen, zoals KEMA Registered Quality B.V., door het toekennen van een certificaat, werd als een enorme stimulans gezien."

Figuur 2 : Het KEMA kwaliteitsstempel

Het CAK-BZ kan nu met onderbouwing richting overheid en haar klanten bewijzen er alles aan te doen dat informatie bij haar in goede handen is. Het is absoluut te verwachten dat het CAK-BZ geconfronteerd zal worden met een vraag naar externe koppelingen met zorgverzekeraars, thuiszorginstellingen en andere partijen.

Door nu al aandacht te besteden aan beveiliging van het netwerk en de daarop aanwezige informatie is de organisatie daar klaar voor.

Het CAK-BZ heeft een convenant met de Belastingdienst en is nu in staat aan een dergelijke partij haar inspanningen op privacy gebied rond inkomensgegevens te bewijzen. Bij certificatie van Shell in 1997 werd al erkend dat certificering door onafhankelijke experts voor een internationale, openbare standaard meer betekent dan een interne poging om aan interne regels te voldoen[5].

Indirect heeft dit project gezorgd voor een horizontale communicatie tussen afdelingen en begrip voor elkaar. Het is voor het eerst dat, door dit onderlinge samenwerkingsverband, een dergelijk zichtbaar resultaat wordt bereikt. Iedereen binnen het CAK-BZ heeft de ICT afdeling dan ook complimenten overgebracht. Dennis Vrolijk; " Ik heb de afgelopen maanden geleerd dat met samenwerken en een goede onderlinge communicatie een heleboel bereikt kan worden binnen een organisatie."

Conclusies:

1. Implementatie van de Code voor Informatiebeveiliging bij het "middenbedrijf" is mogelijk gebleken; twijfel over het "kleinbedrijf" blijft.
2. Eerst invoeren van de tien sleutelmaatregelen lijkt sterk aan te bevelen.
3. Het betrekken van alle medewerkers dient de allerhoogste prioriteit te krijgen.
4. De Code voor Informatiebeveiliging bevat nog veel subjectieve omschrijvingen; in de aanstaande revisie is veel zorg nodig om deze onvolkomenheid weg te nemen.
5. Invoeren van de Code voor Informatiebeveiliging leert een onderneming veel over zichzelf en leert de betrokken medewerkers veel over de eigen verborgen capaciteiten.
6. Het zou zeer behulpzaam zijn als er specifiek op de Code gericht gereedschap zou bestaan voor de selectie van maatregelen zoals een risicoanalyse en management product; CRAMM lijkt, zeker voor een kleinere organisatie, 'overkill'.
7. Informatiebeveiliging en kwaliteitsmanagement hebben zeer veel met elkaar te maken; een koppeling tussen ISO9000 en de Code (wellicht als ISO norm) is dus wenselijk.

Dit heeft nu direct geresulteerd in het onderkennen van het belang van kwaliteitsmanagement en het vrijmaken van een arbeidsplaats daarvoor. Hierdoor wordt ISO certificatie aan de horizon zichtbaar, waarbij informatiebeveiliging wellicht in het kwaliteitssysteem te borgen is.

Ervaringen van de externe partner met het CAK-BZ en met het certificatieproces
Een project als dit bezorgt een onderneming niet in eerste instantie baten maar wel kosten. Een motivator is dan absoluut een perfecte samenwerking tussen alle betrokken partijen. Dit vereist van een externe consultant een open instelling in de problematiek, markt maar ook cultuur van een organisatie.

[5] Mr. P. van Dijken - Compact 1998/3

Certificatie tegen de Code voor Informatiebeveiliging wordt door KEMA absoluut professioneel uitgevoerd. Confrontatie blijkt dan soms nodig om scherp te blijven. Dit vereist een open instelling ook bij een externe partij.

De Code voor Informatiebeveiliging en certificatie daartegen staat nog steeds relatief in de kinderschoenen. Beiden zijn niet perfect. De Code is een leidraad met hier en daar een niet altijd logische structuur en op veel plaatsen is de Code te subjectief en wellicht vaag. Een certificeerder kan daarmee niet altijd uit de voeten. Zo zijn bij het CAK-BZ de bedrijfsprocessen bijzonder goed in kaart gebracht uitgaande van een input/output model. Alle informatiestromen zijn daardoor bekend en gedocumenteerd. De Code beschrijft in paragraaf 10.1.2 echter het *"Bijhouden van een overzicht van belangrijke informatiebronnen".* Dit leidde tot discussies of procesbeschrijvingen nu een dergelijk overzicht vormen (de mening van het projectteam) of dat in een apart document een dergelijk overzicht opgenomen zou moeten zijn (de mening van de certificeerder). Dergelijke discussies over de inhoud van de norm zijn niet aan de orde tijdens een certificatie-audit maar dienen binnen de normcommissie wellicht een plaats te krijgen.

Voor het MKB 'ligt de lat hoog' met betrekking tot de Code voor Informatiebeveiliging. In de wetenschap dat met de komende revisie van de Code het aantal maatregelen groter wordt[6] en (nog) meer nadruk zal komen te liggen op een managementsysteem voor informatiebeveiliging zal die lat nog hoger te komen liggen, hetgeen brede acceptatie van de Code er helaas niet makkelijker op maakt.

Certificeren en het begeleiden van een organisatie is nog een leertraject. Het is te verwachten dat in een relatief kort tempo een groter aantal organisaties met de Code en met certificatie zullen aanvangen. Het is voor alle betrokken partijen, gezien het leertraject, noodzakelijk om daar waar mogelijk over dergelijke projecten te publiceren. Dit vereist ondanks de concurrentie op de markt een open instelling van de betrokken organisaties.

Als laatste opmerking mag gelden dat ondergetekende het bijzonder nadelig vindt dat een sterk aan de overheid gelieerde onderneming als het CAK-BZ niet in aanmerking kan komen voor de door de overheid ontwikkelde ESAKa risicoanalyse software. Een breder draagvlak voor ESAKa lijkt noodzakelijk wil het gedachtegoed van de A&K analyse zowel door overheid als bedrijfsleven gedragen worden. Reeds vanaf 1994 bij het ontstaan van de Code en nu bij de revisie ervan werken overheid en bedrijfsleven samen aan gereedschappen; ESAKa zou daar prima in passen. Bij de risicoanalyse zal nu waarschijnlijk CRAMM gebruikt worden.

Met vooral veel dank aan alle medewerkers van het CAK-BZ. Jullie zijn met recht trots op jullie zelf en op jullie organisatie!

Ernst J. Oud, senior consultant bij Getronics Business Continuity (e.j.oud@getronics.nl),
Ronald E. de Groot, consultant bij Getronics Business Continuity (r.e.degroot@getronics.nl) en
Dennis Vrolijk, manager systeembeheer en ondersteuning bij het CAK-BZ (dvrolijk@cak-bz.nl).

[6] Zie 'Code voor Informatiebeveiliging herzien' in Informatiebeveiliging Praktijkjournaal, april 1999