Informatiebeveiliging: de rol van de accountant

Prof. Drs. J.C.E. van Kollenburg en J.M. Suerink

THEMA

Inleiding

In dit artikel geven wij allereerst een verdere inkadering van het begrip informatiebeveiliging, daarna behandelen we verschillende verantwoordelijkheden, die te onderkennen zijn binnen informatiebeveiliging. Ten slotte behandelen we een model, waarin de rol van de accountant wordt beschreven.

Informatiebeveiliging

Informatie is de resultante van een gegevensverwerkend proces. Dat wil zeggen wanneer we het begrip informatiebeveiliging afbakenen, dan valt hieronder het hele traject: verzamelen, opslaan, be- en verwerken, transport en distributie van gegevens/informatie. Wij maken voor wat de beveiliging betreft geen onderscheid tussen gegevens en informatie.

Beveiliging is geen doel op zich. Beveiliging heeft tot doel het handhaven van de kwaliteit c.q. het bevorderen van het bereiken van eerder geformuleerde doelstellingen, door het treffen van risicoreducerende maatregelen. Voorts dient informatiebeveiliging te worden beoordeeld als onderdeel van het totale beveiligingsbeleid van een organisatie. Dit beveiligingsbeleid zal op haar beurt deel uitmaken van het totale bedrijfsbeleid.

Prof. Drs. J.C.E. van Kollenburg RA is firmant van BDO CampsObers Registeraccountants; voorts is hij hoogleraar Accountancy aan de Katholieke Universiteit Brabant.

J.M.Suerink RE RA is firmant van BDO CampsObers Registeraccountants; voorts is hij universitair docent Organisatie van de Informatieverzorging Erasmus Universiteit Rotterdam, alsmede co-auteur Inleiding EDP-auditing.

Het beveiligingsbeleid is daarbij de resultante van het proces van risicomanagement, waarbij de leiding van de organisatie haar beveiliging zo organiseert, dat optimale condities ontstaan om eerder geformuleerde doelstellingen te realiseren. Informatiebeveiliging is een van de componenten van dat beveiligingsbeleid, voorzover kwaliteit van informatie een rol speelt bij het bereiken van die eerder genoemde doelstellingen. Wanneer het objectief van informatiebeveiliging is het handhaven van de kwaliteit van informatie, dan zullen de kwaliteitscriteria benoemd moeten worden.

NIVRA-geschrift 53 onderkent een aantal kwaliteitscriteria:
- integriteit (juistheid, tijdigheid en volledigheid)
- exclusiviteit (vertrouwelijkheid)
- beschikbaarheid (continuïteit)
- doelmatigheid (efficiency)
- doeltreffendheid (effectiviteit)
- controleerbaarheid.

De eerste afbakening betreft het gegevensverwerkend proces. In een huishouding zijn vele gegevensverwerkende processen te onderkennen. Denk bijvoorbeeld aan de verzameling van informatie over concurrenten, informatie in een ziekenhuis over patiënten en methoden van symptoombestrijding, et cetera. Al deze vormen van informatie spelen in het algemeen een cruciale rol ter realisatie van de ondernemingsdoelstellingen, en vormen daarmede object van informatiebeveiliging binnen deze organisaties. Wij zullen ons echter in dit artikel beperken tot die gegevensverwerkende processen, die gevolgen hebben voor de financiële verantwoording, aangezien deze processen binnen de certificerende functie van de accountant het primaire onderzoeksobject vormen.

Redenerend vanuit de certificerende functie van de accountant dient tevens een beperking te worden aangebracht in de kwaliteitscriteria. De accountant is niet de deskundige bij uitstek op het gebied van effectiviteit en efficiency van informatie. Wij vinden in deze opvatting steun bij de wetgever. De wetgever heeft met de Wet Computercriminaliteit art. 393 boek 2 BW uitgebreid met lid 4, waarin een rapportageplicht is opgenomen aan de Raad van Commissarissen en het bestuur van een huishouding inzake bevindingen met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking. Dit impliceert dat de wetgever de kwaliteitscriteria doelmatigheid en doeltreffendheid uitsluit. De wetgever heeft met deze bepaling geen extra financiële lasten op het bedrijfsleven willen leggen, maar eerder een stimulans aan het accountantsberoep willen geven expliciet aandacht te besteden aan betrouwbaarheid en continuïteit. Studierapport 34 van het Koninklijk NIVRA sluit hierop naadloos aan voor wat betreft de te hanteren kwaliteitscriteria voor geautomatiseerde gegevensverwerking in het kader van de jaarrekeningcontrole. Het criterium continuïteit moet daarbij vooral in verband worden gebracht met de natuurlijke adviesfunctie van de accountant. Indien het kwaliteitsaspect controleerbaarheid buiten beschouwing wordt gelaten, wordt vervolgens aansluiting gevonden bij de Code voor Informatiebeveiliging.

De verantwoordelijkheden ten aanzien van informatiebeveiliging

De recente discussie rond corporate governance (Cadbury rapport) laat zien, dat er verschillende verantwoordelijkheden te onderkennen zijn, ook ten aanzien van informatiebeveiliging.

Allereerst het management, deze heeft tot taak een adequaat stelsel van internal control, waar informatiebeveiliging een niet onbelangrijk deelaspect van uitmaakt, op te zetten. Het rapport van de Committee of Sponsoring Organizations of the Treadway Commission (COSO) biedt een adequate handreiking voor de methode waarmee een dergelijk systeem ontworpen en geïmplementeerd dient te worden. Grofweg houdt de methode in dat rekening houdend met de beheersomgeving (control environment) via bedreigingenanalyse (risk assesment) een stelsel van interne controlemaatregelen moet worden ontwikkeld (control activities), waarbij informatie en communicatie een vitale rol spelen. Als sluitstuk dient het geïmplementeerde systeem bewaakt te worden, zodat steeds bijstelling mogelijk is (monitoring en feed back).

Het management vindt steun bij het bepalen welke maatregelen getroffen moeten worden in bijvoorbeeld de Code voor Informatiebeveiliging. De Code voor Informatiebeveiliging is een codificering van de 'best practice' bij vooraanstaande internationale bedrijven. De Code heeft de status van NNI-norm.

De Rijksoverheid beschikt over het Besluit voorschrift informatiebeveiliging rijksoverheid 1994, waarin verantwoordelijkheden, vorm en inhoud van het informatiebeveiligingsbeleid en implementatie-, monitoring- en feedbackmodellen zijn geschetst.

Op de tweede plaats ligt er een verantwoordelijkheid voor informatiebeveiliging bij het 'interne' toezichthoudende orgaan. Het behoort tot een van de taken van de Raad van Commissarissen om inhoudelijk het informatiebeveiligingsbeleid te toetsen en aan zich te laten rapporteren over de uitkomsten van dat beleid. Deze verantwoordelijkheid vloeit enerzijds voort uit haar toezichtfunctie op het beleid en de algemene gang van zaken (artikel 140/250 boek 2 BW) en wordt nog eens extra geaccentueerd door de aansprakelijkheid van de commissaris voor misleidende jaarrekeningen (artikel 150/260 boek 2 BW). Daarnaast ontvangt de RvC op basis van artikel 393 lid 4 boek 2 BW bevindingen uit de jaarrekeningcontrole met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking.

Soms ligt er ook een verantwoordelijkheid op het gebied van informatiebeveiliging bij de externe toezichthouders. Als voorbeeld moge dienen De Nederlandsche Bank, die reeds op 20 september 1988 een Memorandum liet verschijnen omtrent de betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking in het bankwezen. Het model waarvoor DNB heeft gekozen komt kortweg hierop neer, dat de kredietinstelling een extra opdracht geeft aan zijn accountant en dat de externe toezichthouder zich laat informeren over de uitkomsten van het onderzoek naar de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking.

De rol van de accountant

De accountant kan velerlei rollen vervullen. Wij beschouwen in dit artikel vooral zijn rol in de certificerende functie, dat wil zeggen in het kader van de wettelijke controle van de jaarrekening. De wet werkt die rol nader uit in artikel 393 boek 2 BW. De accountant heeft daarbij tot taak om te onderzoeken of de jaarrekening een zodanig inzicht geeft, dat een verantwoord oordeel kan worden gevormd omtrent het vermogen en het resultaat. Zijn bevindingen behoort de accountant te rapporteren aan de raad van commissarissen en het bestuur. Met de invoering van de Wet Computercriminaliteit is hieraan toegevoegd, dat de accountant daarbij ten minste melding moet maken van zijn bevindingen met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking. Uit de totstandkoming van deze wet kan worden afgeleid, dat de wetgever hierbij geen aanvullend onderzoek door de accountant voor ogen heeft gestaan, maar wel voorschrijft om bevindingen op het gebied van informatiebeveiliging te rapporteren, voor zover de uitgevoerde controlewerkzaamheden hiertoe aanleiding geven.

Nog belangrijker dan de wettelijk gecodificeerde taak zijn de verwachtingen, die bij het gebruikersverkeer in enge en ruime zin leven ten aanzien van de rol, die de accountant bij informatiebeveiliging dient te spelen en vervolgens de rol die accountants zelf willen en kunnen spelen op het gebied van informatiebeveiliging. Over de verwachtingen, toegespitst op informatiebeveiliging, van gebruikers van accountantsdiensten, zoals directeuren, commissarissen, aandeelhouders, kredietverschaffers et cetera is slechts zeer gebrekkige informatie ter beschikking. In het algemeen wijst deze informatie in de richting van hoger gespannen verwachtingen dan de accountant waarmaakt of waar kan maken. Recente ontwikkelingen rond corporate governance geven de indruk dat althans in kwalitatieve zin de verwachtingen nu meer expliciet worden geformuleerd, waarbij een tendens valt waar te nemen in de richting van een meer prominente rol van de accountant op het gebied van informatiebeveiliging.

Het Koninklijk NIVRA heeft vele publicaties gewijd aan de wijze waarop de accountant aandacht dient te schenken aan de geautomatiseerde gegevensverwerking, recentelijk nog het studierapport inzake normatieve maatregelen voor de geautomatiseerde gegevensverwerking in het kader van de jaarrekeningcontrole. Alvorens in te gaan op de wijze waarop de accountant tijdens de uitvoering van de controleopdracht aandacht besteedt aan informatiebeveiliging is het nuttig eerst de rol en verantwoordelijkheden van de accountant ten aanzien van informatiebeveiliging verder uit te diepen.

Het is daarbij zinvol om als uitgangspunt te nemen de rol van de accountant, zoals het NIVRA deze schetst in haar beleidsplannen. Zij ziet de kern van de accountantsfunctie als zijnde de voorziening in de behoefte aan zekerheid omtrent (financiële) informatie ten behoeve van besluitvorming, beheersing en verantwoording. Zo geformuleerd spreekt daaruit een grote betrokkenheid met informatiebeveiliging. Of dit door praktijkbeoefenaren ook zo beleefd wordt is nog maar de vraag.

Illustratief is de discussie tussen Schilder en Van Zanten in de Accountant van juli/augustus en november 1994 over de vraag of de verklaring bij de jaarrekening tevens een uitspraak impliceert over de juiste werking van de administratieve organisatie en daarmede over het stelsel van maatregelen dat de kwaliteit van informatie borgt (lees informatiebeveiliging). Geen verschil van mening bestaat tussen hen over het feit, dat een goedkeurende verklaring een minimumniveau AO/IC omvat. Dit minimumniveau kan worden omschreven als de AO/IC, die bij afwezigheid een objectieve verhindering vormt bij het komen tot een goedkeurende verklaring. Het minimumniveau is veelal vereist als controlemiddel voor de negatieve controle op de volledigheid van de opbrengstverantwoording. Van Zanten onderkent naast dit minimale niveau, niveau A, evenwel ook nog een niveau B (=minimumniveau plus ingebouwde waarschuwingscapaciteit voor bedreigingen) en een niveau C (=niveau B plus optimalisering van kosten en opbrengsten).

Een complicerende factor, die onvoldoende door van Zanten in de discussie betrokken is, is het feit dat de jaarrekeningcontrole de laatste jaren steeds meer wordt gezien als een commodity. Dit heeft tot gevolg, dat accountantskantoren hun werkprocessen steeds verder stroomlijnen.

Dit gebeurt onder andere door gebruik te maken van kennissystemen. Een controleaanpak

gebaseerd op risicoanalyse neemt daarbij per definitie niet meer 'alles' in beschouwing, maar richt zich op die 'key controls', die van materieel belang zijn voor de jaarrekening.

In de huidige situatie moeten wij, met Schilder, concluderen dat een goedkeurende verklaring geen uitspraak impliceert over een adequaat stelsel van AO/IC en daarmede over de toereikendheid van informatiebeveiliging.

Ogenschijnlijk verkeert de accountant in een prisoner's dilemma. Als in de optiek van de accountant het minimumniveau AO aanwezig is (om één van de kwaliteitscriteria in casu betrouwbaarheid van informatie te garanderen) en hij met inzet van overige controlemiddelen een uitspraak kan doen over de jaarrekening, hoe moet hij dan duidelijk maken aan het maatschappelijk verkeer dat de informatiebeveiliging op de overige kwaliteitscriteria niet onderzocht is ? En dit terwijl de beroepsorganisatie zich profileert als deskundige op het gebied van de controle van kwaliteit van informatie, en andere belanghebbenden bij de onderneming vragen om een bredere verantwoording over, toezicht op en controle van beheerstaken, ofwel corporate governance.

De oplossing ligt in een actieve opstelling van de accountant en het accountantsberoep.

De verantwoordelijkheid voor een adequaat stelsel van informatiebeveiliging (binnen het groter geheel van internal control) ligt bij het management. De discussie over corporate governance en zelfregulering van huishoudingen zou kunnen uitmonden in een separate verantwoording van het management over de kwaliteit van internal control. Wij denken hierbij aan maatwerk. Voor die omgevingen, waar informatiebeveiliging cruciaal is (denk aan financiële instellingen, ziekenhuizen, organisaties, waar bedrijfsprocessen tot stilstand komen als de IT-functie uitvalt) zou in ieder geval de RvC moeten eisen, dat het management zich verantwoordt over het stelsel van maatregelen, dat de informatiebeveiliging moet waarborgen.

De RvC zou kunnen overwegen deze verantwoording door een onafhankelijke instantie te laten toetsen. De vraag of ook 'publiek' verantwoording moet worden afgelegd hangt af van de maatschappelijke ontwikkelingen. De wetgever heeft een en ander overwogen bij de uitbreiding met lid 4 van artikel 393 van boek 2 BW en toen deze optie verworpen.

Informatiebeveiliging procesmatig bezien

Nu de contouren van de rol van de accountant met betrekking tot informatiebeveiliging zijn verkend, rest ons de vraag op welke wijze de accountant invulling kan geven aan deze rol. Hiervoor hebben we het proces van informatiebeveiliging in de cliëntomgeving gekoppeld aan het controleproces van de accountant en nader uitgewerkt in een model (zie figuur 1 op p. 594).

Het management heeft als primair aandachtsgebied de realisatie van de organisatiedoelstellingen: effectiviteit. Bij het bereiken van die organisatiedoelstellingen heeft de organisatie een administratieve organisatie nodig ten behoeve van het besturen (managementinformatie), het doen functioneren (transactie-informatie) en ten behoeve van de verantwoording, die over het besturen moet worden afgelegd (verantwoordingsinformatie).

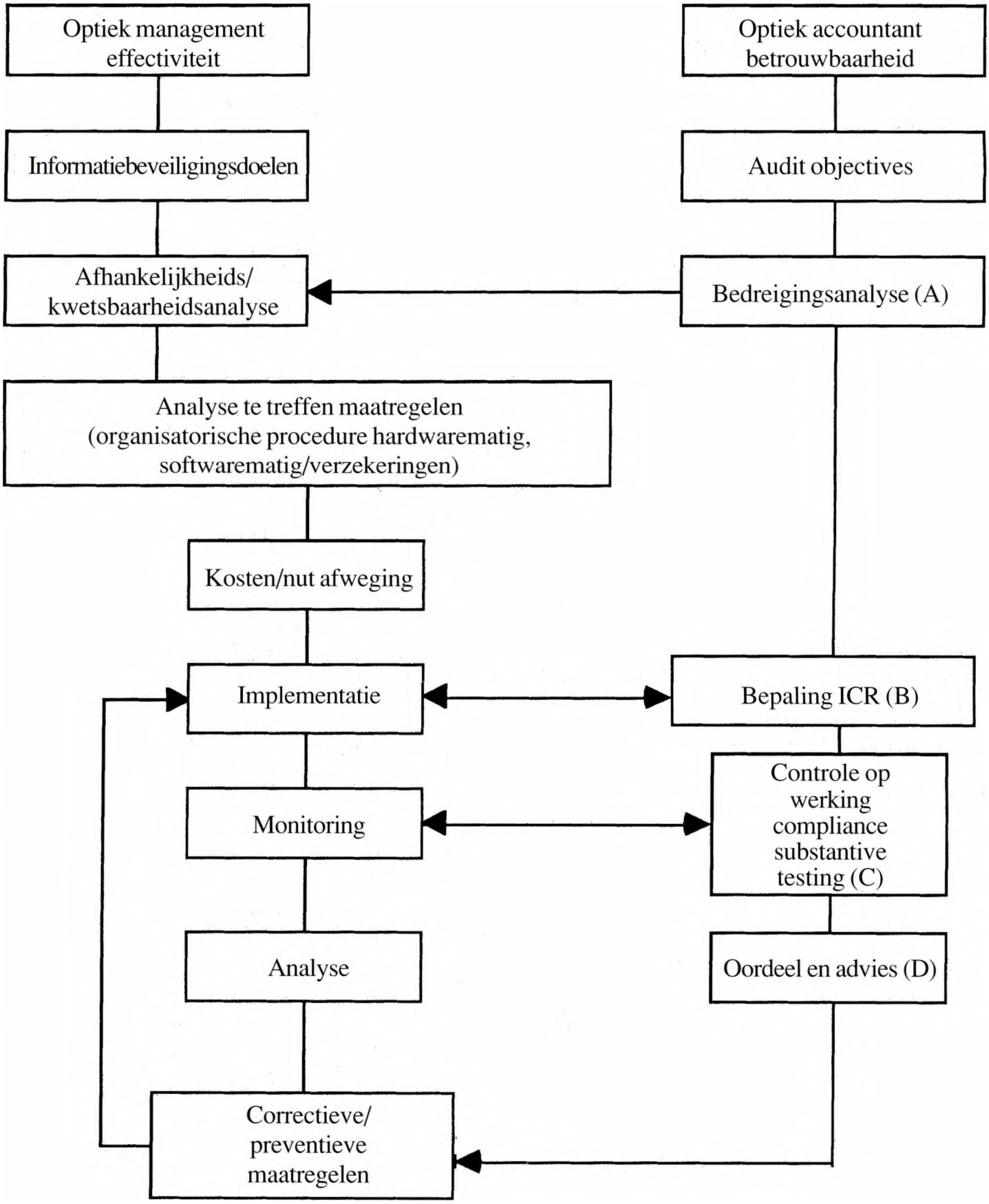
Deze informatie moet voldoen aan bepaalde kwaliteitseisen. Daarom moeten bedreigingen, die inbreuk maken op die kwaliteit, gereduceerd worden door een stelsel van maatregelen op het gebied van informatiebeveiliging. Het management zal de informatiebeveiligingsdoelen moeten formuleren om zodoende te komen tot een (informatie)beveiligingsbeleid.

De accountant heeft als missie het voldoen aan de aan hem gegeven opdracht, neergelegd in de engagement letter. Hieruit zal hij de te bereiken controledoelen afleiden (=de audit objectives).

Van de accountant mag worden verwacht, dat hij de cliënt wijst op het feit dat hij deskundig is op het gebied van de kwaliteit van internal control. Hierbij zou ook de door ons gesuggereerde verantwoording over de informatiebeveiliging aan de interne toezichthouders in de discussie kunnen worden betrokken.

De accountant zal via een bedreigingenanalyse (risk analysis) vaststellen, welke bedreigingen van buitenaf, maar samenhangend met de bedrijfsprocessen, invloed kunnen hebben op de financiële verantwoording (A). Indien het management op een gestructureerde wijze haar AO/IC heeft ontworpen, dan zal zij een afhankelijkheidsanalyse (welke bedrijfsprocessen zijn afhankelijk van informatietechnologie) en kwetsbaarheidsanalyse (welke informatieprocessen zijn kwetsbaar voor

Figuur 1


Optiek management effectiviteit
Optiek accountant betrouwbaarheid
Informatiebeveiligingsdoelen
Audit objectives
Afhankelijkheids/ kwetsbaarheidsanalyse
Bedreigingsanalyse (A)
Analyse te treffen maatregelen (organisatorische procedure hardwarematig, softwarematig/verzekeringen)
Kosten/nut afweging
Implementatie
Bepaling ICR (B)
Monitoring
Controle op werking compliance substantive testing (C)
Analyse
Oordeel en advies (D)
Correctieve/ preventieve maatregelen

welke bedreigingen) uitgevoerd hebben.

De vergelijking van de drie analyses, vanuit verschillende invalshoeken, kan voor beide partijen (management en accountant) nieuwe gezichtspunten aan het licht brengen met betrekking tot de meest gewenste (informatie)-beveiligingsstructuur.

Vervolgens zal het management, op basis van bestaande mogelijkheden en kosten/nut-afweging, overgaan tot ontwerp en implementatie van een stelsel van maatregelen AO/IC, waarvan informatiebeveiliging een aspectsysteem vormt.

De accountant zal dit stelsel onderwerpen aan een beoordeling, teneinde vast te stellen in hoeverre de AO/IC een afdekking biedt voor de onderkende risico's (B). Hij vindt hierbij steun in het reeds eerder gememoreerde studierapport 34, dat een normatief kader biedt voor de kwaliteitscriteria exclusiviteit, integriteit, controleerbaarheid en beschikbaarheid. Deze beoordeling kan tevens een oordeel inhouden over de effectiviteit van de informatiebeveiliging, voorzover het bovengenoemde kwaliteiscriteria betreft.

Deze werkzaamheden worden enerzijds uitgevoerd tijdens de voorbereiding van de controle in het kader van het onderzoek van de controleomgeving en vormen de basis voor de inschatting van het inherente risico. De aandacht is daarbij gericht op general controls zoals de logische toegangbeveiliging, het change-management en testprocedures. In het kader van de natuurlijke adviesfunctie zal ook de opzet van maatregelen op het gebied van fysieke beveiliging, back-up, recovery en uitwijk worden beoordeeld. Ten behoeve van de bepaling van de controleaanpak en de inschatting van het intern controlerisico (C) zal voorts aandacht worden besteed aan de opzet van de in de geautomatiseerde gegevensbewerkende processen opgenomen geprogrammeerde controles (application controls). Later zullen in het kader van de uitvoering van de controle bestaan en werking van de eerder beoordeelde general controls en application controls worden vastgesteld. De uitkomsten van deze werkzaamheden van de accountant, veelal neergelegd in een management letter (D), kunnen voor het management aanleiding zijn voor het nemen van additionele maatregelen op het gebied van informatiebeveiliging. Hiermede is tevens de basis gelegd voor de rapportage aan het toezichthoudend orgaan, in de vorm van een accountantsverslag, waarbij inhoudelijk kan worden ingegaan op de bevindingen met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking, zoals bedoeld in de Wet Computercriminaliteit.

Toekomstverkenning en conclusie

Hiervoor is tot nu toe op vrij statische wijze invulling gegeven aan de rol die de accountant in het kader van informatiebeveiliging zou moeten en kunnen spelen. Belangrijker is echter om een en ander in het perspectief van de toekomst uit te werken.

De laatste jaren is een tendens waar te nemen dat betrokkenen bij ondernemingen behoefte hebben aan een bredere verantwoording door het management. Met name aandeelhouders stellen zich bij de optimalisatie van hun shareholdersvalue niet langer tevreden met een vooral financieel getinte jaarrekening. Om hun portfolio effectiever te kunnen beheren en verrassingen zoals déconfitures zoveel mogelijk uit te sluiten dringen zij aan op een meerdimensionale verantwoording waarin ook aandacht wordt besteed aan aspecten als interne beheersing, milieu en meer stellige uitspraken over de toekomst. Ook van de accountant wordt in dit verband een bredere taakopvatting verwacht, in die zin dat hij de geloofwaardigheid van deze additionele verantwoordingen bekrachtigt.

De informatisering is bezig om steeds meer buiten de grenzen van de eigen organisatie te treden. Steeds vaker wisselen ondernemingen op elektronische wijze met elkaar berichten uit en verlenen zij toegang tot elkaars bestanden. Deze laatste ontwikkeling kan alleen plaatsvinden indien over en weer door de handelspartners voldoende informatiebeveiligingsmaatregelen worden genomen. Handelspartners zullen hierover zekerheid wensen, waaruit de behoefte ontstaat tot oordelen over informatiebeveiliging door bijvoorbeeld accountants. In het verlengde hiervan valt een ontwikkeling waar te nemen dat financiële gegevens van ondernemingen steeds vaker en frequenter in elektronisch formaat worden aangeboden. De eerste jaarrekeningen op internet zijn al een feit en deze lijn doortrekkend is het niet moeilijk om zich voor te stellen dat binnen niet al te lange tijd ondernemingen delen van hun databa-

se met voor openbaarmaking geschikte gegevens beschikbaar zullen stellen aan aandeelhouders, obligatiehouders, beleggingsanalisten, journalisten, financiers en leveranciers om daaruit hun eigen informatiepakket samen te stellen. De functie van de traditionele jaarrekening zal daarmede afnemen en langzaam maar zeker plaatsmaken voor deze database. Als accountants tijdig inspelen op deze ontwikkeling dan zal hun rol worden verlegd naar een continu elektronisch betrouwbaarheidscertificaat bij deze database. Het is duidelijk dat informatiebeveiliging hierin een cruciale rol speelt, met name waar het de continue werking van het systeem van informatiebeveiliging betreft.

Het antwoord op de vraag welke rol de accountant in het kader van informatiebeveiliging moet gaan spelen, is daarmede duidelijk. Van de accountant mag worden verwacht, dat hij ten aanzien van informatiebeveiliging een pro-actieve rol speelt. Enerzijds door in te haken op maatschappelijke ontwikkelingen inzake corporate governance, anderzijds door het goed vervullen van zijn natuurlijke adviesfunctie, met name richting management en toezichthoudende organen. Hierbij heeft de accountant zeker geen exclusiviteit aangezien er zich meer deskundigen in dit speelveld bevinden. Van de accountant mag echter wel een vooraanstaande rol worden verwacht bij het toetsen van ten minste de opzet en het bestaan van informatiebeveiliging aan de kwaliteitscriteria, die in het verlengde van de jaarrekeningcontrole liggen, en het signaleren van tekortkomingen in dit vlak. Voor de nabije toekomst zal die rol met betrekking tot de jaarrekeningcontrole worden omgezet in certificering van de verantwoordingsdatabase. Deze positie willen innemen betekent evenwel dat de claim van deskundigheid ook moet worden waargemaakt, met als uitvloeisel eisen aan de kennis van informatie-technology en dus (permanente) educatie.

LITERATUUR

Automatisering en controle, Deel VII Kwaliteitsoordelen over informatievoorziening, (1989), NIVRA-geschrift 53, Kluwer, Deventer.

Cadbury rapport, (1992), Committee on the financial aspects of corporate governance.

Code voor Informatiebeveiliging, (1994), Ministerie van Economische Zaken/NNI.

Schilder, A. (1994), Na 100 jaar opnieuw? De functie van de accountant, *De Accountant*, november, met weerwoord van J.H. van Zanten.

Elliott Robert K., (1995), The future of assurance services: Implications for academia. *Accounting Horizons*, december.

Normatieve maatregelen voor de geautomatiseerde gegevensverwerking in het kader van de jaarrekening controle, (1995), Studierapport 34 NIVRA, Amsterdam.

Managementletter en accountantsverslag, (1994), Studierapport 31 NIVRA, Amsterdam.

Kollenburg J.C.E. van, (1991), *De deugd in het midden*, Oratie Katholieke Universiteit Brabant, 6 september.

Wallage Ph., (1995), *Corporate governance en de rol en functie van de accountant*, Oratie Universiteit van Amsterdam, 27 oktober.