REKENINGKUNDIGE BEHEER IN ELEKTRONIESE HANDEL

Johannes Elias William Carstens

B.Com. Hons. M.Com.

G.R. (S.A.)

Proefskrif voorgelê vir die graad

Philosophiae Doctor

In die Skool vir Ekonomiese Wetenskappe aan die

Potchefstroomse Universiteit vir Christelike Hoër Onderwys

Promotor: Prof. dr. P. Lucouw

VANDERBIJLPARK

2003

DANKBETUIGINGS

Ek betuig graag my dank en waardering aan almal wat, in 'n mindere of meerdere mate, meegehelp het tot die bereiking van hierdie doelwit.

Alle dank en eer kom Hom toe wat talente gee, geleenthede daarstel en voorsien in alles wat ons nodig het.

Aan my ouers en skoonouers vir hulle belangstelling en aanmoediging.

Aan my kollegas en vriende vir hulle hulp en motivering.

Aan my promotor vir sy insig, raad en leiding.

Aan my eggenote vir haar aanmoediging en opofferings.

ABSTRACT

ACCOUNTING CONTROL IN ELECTRONIC COMMERCE

Accounting Control includes the disciplines of the accountant and the auditor and has over the centuries evolved as a gradual process to find a suitable accounting approach to an accounting problem.

With the advent of the Internet, the world market is being delivered to the user. Electronic commerce (e-commerce) can take place via the Internet with no borders to prohibit trade.

The advantages of e-commerce however also brought challenges and fears with relation of conducting transactions over the Internet. The safety of such transactions is the concern of Accounting Control.

Accounting Control encompasses the recording of transactions, the control thereof to ensure the safety of information, the limitation of fraud, defining the liability for the loss of goods and funds and the international acceptance of the legality of transactions.

The aim of this study is to quantify accounting control in electronic commerce and to make recommendations where there are shortcomings.

The field of this study has been narrowed down to quantify the broader aspects of accounting control and the process followed to develop and implement those controls within electronic commerce to safeguard and report information.

The research has shown that the principles applicable to traditional businesses are also valid in electronic commerce. Furthermore, that the application of sound accounting control and the control that evolved around electronic commerce, together with the compliance of generally accepted accounting practice, auditing standards, the companies act, the rules of the JSE Securities Exchange, the Code of Corporate Conduct and the Electronic Communications and Transactions Act, can lower the risk of corruption and fraud and protect the accuracy of information.

It is however necessary to continually revisit the accounting and internal control measurements, the accurate processing of transactions, taxation matters, the legal process and regulations, accounting principles and strategy, to successfully address new challenges at an early stage.

It is recommended that further research is conducted in the legal field, especially with regards to the enforcement of the jurisdiction of agreements and the prosecution of cyber criminals. This may lead to an international e-court!

It is further recommended that research should be done into the feasibility of e-tax, on an international basis to ensure that all parties concerned i.e. individuals, organisations and governments, are fairly treated.

Lastly, the success of e-commerce will depend on the depth of knowledge and the skill base of individuals to develop and implement controls to safeguard information. Continuous research is necessary to establish the degree to which accounting control must form part of the field of study.

OPSOMMING

REKENINGKUNDIGE BEHEER IN ELEKTRONIESE HANDEL

Rekeningkundige beheer sluit die dissipline van die rekenmeester en dié van die ouditeur in en het oor die eeue heen ontwikkel as 'n geleidelike proses om geskikte rekeningkundige benaderings vir rekeningkundige probleme te vind.

Met die intrede van die internet, is die wêreldmark aan die gebruiker gelewer. Elektroniese handel (e-handel) kan deur middel van die internet plaasvind met geen perke wat handel verbied nie.

Die voordele van e-handel het egter ook uitdagings en vrese met betrekking tot die uitvoer van transaksies oor die internet gebring. Die veiligheid van sulke transaksies is die besorgdheid van rekeningkundige beheer.

Rekeningkundige beheer behels die aanteken van transaksies, die beheer daarvan om die veiligheid van inligting te verseker, bedrog te beperk, die aanspreeklikheid vir die verlies van goedere en fondse te definieer en die internasionale aanvaarding van die regsaanspreeklikheid van transaksies.

Die doel van hierdie studie is om rekeningkundige beheer in e-handel te kwantifiseer en om aanbevelings te maak waar daar tekortkominge is.

Die studieveld is beperk tot die kwantifisering van die breër aspekte van rekeningkundige beheer en die proses wat gevolg is in die ontwikkeling en implementering van die beheermaatreëls in e-handel om inligting te beskerm en te rapporteer.

Die navorsing het getoon dat dieselfde beginsels wat van toepassing is op tradisionele besighede, ook geldig is in e-handel. Voorts, dat die toepassing van gesonde rekeningkundige beheer en die beheer wat rondom e-handel ontwikkel het, tesame met die nakoming van die algemeen aanvaarde rekeningkundige praktyk, ouditstandaarde, die Maatskappyewet, die reëls van die Johannesburgse Sekuriteitebeurs, die Kode van

Korporatiewe Gedrag en die Wet op Elektroniese Kommunikasie en Transaksies, die risiko van korrupsie en bedrog kan verlaag en die akkuraatheid van inligting beskerm.

Dit is egter nodig om voortdurend die rekeningkundige en interne kontrole- maatreëls, die akkurate prosessering van transaksies, belastingaangeleenthede, die regsproses en regulasies, asook rekeningkundige beginsels en strategieë na te gaan om vroegtydig nuwe uitdagings suksesvol die hoof te bied.

Daar word aanbeveel dat verdere navorsing gedoen moet word in die regsveld, spesifiek met betrekking tot die afdwingbaarheid van die jurisdiksie van ooreenkomste en die vervolging van kubermisdadigers. Dit mag lei tot die totstandkoming van 'n e-hof.

Verder word aanbeveel dat navorsing gedoen moet word ten opsigte van e-belasting om op 'n internasionale basis te verseker dat alle betrokke partye, naamlik individue, organisasies en regerings regverdig behandel word.

Ten slotte, die sukses van e-handel sal afhang van die diepte van die kennis en die vlak van bekwaamheid van individue om kontroles te ontwikkel en te implementeer om inligting te beveilig. Voortdurende navorsing is nodig om die mate te bepaal waartoe rekeningkundige beheer deel moet uitmaak van die studieveld.

AKRONIEME EN AFKORTINGS

AARF	:	Australiese Rekeningkundige Navorsingstigting (Australian Accounting Research Foundation)
AARP (GAAP)	:	Algemeen Aanvaarde Rekeningkundige Praktyk (General Accepted Accounting Practice)
ACL	:	Access Control List
ADV (ASP)	:	Aanwendingsdiensverskaffer (Application Service Provider)
AGS	:	Auditing and Assurance Guidance Statement (Australia -CPA)
AICPA	:	American Institute of Certified Public Accountants
ARPA	:	Advanced Research Project Agency
B2B	:	Besigheid-tot-Besigheid (Business to Business)
B2G (B2C)	:	Besigheid-tot-Gebruiker (Business to Consumer)
BEE	:	Black Economic Empowerment (Swart ekonomiese bemagtiging)
BTW	:	Belasting op Toegevoegde Waarde
CA	:	Certification Authority
CAAT	:	Computer Assisted Audit Techniques
CERT	:	Computer Emergency Response Team
CFE	:	Controlled Foreign Entities
CGI	:	Algemenepoort-koppelvlakskrif
CPA	:	Certified Public Accountant
CYBER CASH	:	CyberCash Secure Internet Payment System
DES	:	Data-enkripsiestandaarde

DNA	:	Domain Name Authority
EDI	:	Elektroniese data-interaksie
EDU	:	Elektroniese data-uitruiling
ES	:	Kundigestelsel
FNB	:	Eerste Nasionale Bank
FV	:	First Virtual Internet Payment System
HTML	:	Hyper Text Mark-up Language
HTTP	:	Hyper Text Transfer Protocol
IAPC	:	International Audit Practice Committee
IAPS	:	International Auditing Practice Statement
ICT	:	Information and Communications Technologies
IDV (ISP)	:	Internet-diensverskaffer (Internet Service Provider)
IE	:	Intellektuele Eiendom
IFAC	:	International Federation of Accountants
IP	:	Internet Protocol
ISA	:	International Standards on Auditing (Internasionale Ouditstandaarde)
IT	:	Inligtingstegnologie
JSB	:	Johannesburgse Sekuriteitebeurs
KMMO's	:	Klein, medium en mikro-organisasies
LBS	:	Lopende betaalstelsel
MIS	:	Bestuursinligtingstelsels
MTS	:	Multilaterale handelstelsel

NCP	:	Network Control Protocol
OECD	:	Organisation for Economic Co-operation and Development
OU	:	Ouditkunde (Suid-Afrikaanse Ouditstandaarde)
PKE	:	Public Key Encription
PKI	:	Private Key Infrastructure
RE	:	Rekeningkunde (Algemeen Aanvaarde Rekeningkundige Praktyk)
RIS	:	Rekenaarinligtingstelsel
RPR	:	Rekeningkundige Praktykeraad
SAAPS	:	South Africa Audit Practice Statements
SAIGR	:	Suid-Afrikaanse Instituut van Geoktrooieerde Rekenmeesters
SAOPS	:	Suid-Afrikaanse Ouditpraktykstandpunte
SAOS	:	Suid-Afrikaanse Ouditstandaarde
SET	:	Secure Electronic Transactions
S-HTTP	:	Secure Hyper Text Transfer Protocol
SMME	:	Small Medium and Micro Enterprises
SPC	:	Software Publisher Certificate
SSL	:	Secure Socket Layer
T	:	Transaksie
TCP	:	Transmission Control Protocol
TRIPS	:	Trade Related Aspects of Intellectual Property Rights
UN/EDT FACT	:	United Nations Electronic Data Interchange for Administration, Commerce and Transport

UNITRAL	:	United Nations Commission of International Trade Law
VKA	:	Verenigde Koningkryk van Amerika
VPN's	:	Virtuele privaat netwerke
VSA	:	Verenigde State van Amerika
W3C	:	Wêreldwyeweb-konsortium
WTO	:	World Trade Organisation
WWW	:	World Wide Web

INHOUDSOPGAWE

HOOFSTUK 1

INLEIDING, PROBLEEMSTELLING EN BEPLANNING

1.1 INLEIDING

Die rekeningkunde se ontwikkeling het nie willekeurig geskied nie, maar dit het sedert die Mesopotamiese beskawing oor die eeue heen gebeur as deel van 'n langsame proses om die regte benadering te kry wat 'n rekeningkundige probleem sal bied. Rekeningkundige beheer omsluit die werksaamhede van beide die rekenmeester en die ouditeur.

Waar die rekeningkunde te make het met die bymekaarmaak van inligting (-data) en die opsomming, asook die kommunikasie daarvan, behels die ouditkunde as 'n afsonderlike dissipline 'n proses van gedetailleerde nagaan met die klem op bewyslewering en verifikasie van inligting, om sodoende beskerming aan lesers van finansiële verslaggewing te bied.

In hierdie proses van die hou en die verifikasie van rekeninge, word gebruik gemaak van kontroles om die betroubaarheid en die integriteit van inligting, die nakoming van beleid, planne, prosedures, wette en regulasies, die beveiliging van bates, die ekonomiese en effektiewe aanwending van hulpbronne en die uitvoering van neergelegde doelwitte van bedrywe en programme te verseker.

Die omgewing waarin die rekeningkunde praktiseer, het oor die afgelope dekades deur die toetreding van rekenaars radikaal verander. Daar is egter geen aanduiding dat die konsepte van rekeningkundige beheer as gevolg van die metode wat gebruik word, of dit dan handgeskrewe of gerekenariseerd is, verander het nie.

Met die ontstaan van die internet is die geleentheid geskep om elektronies handel te kan bedryf. Dieselfde beginsels wat tradisioneel op baksteen-en-beton-ondernemings van toepassing is, is eweneens van toepassing op e-handel (Ruthven, 2000). Nie net geld hierdie stelling vir die bestuur van 'n maatskappy en onderliggende sake-beginsels nie, maar sekerlik ook vir die rekeningkundige beheer van e-handelstransaksies.

Dit is egter so dat die koms van rekenaars en e-handel oor die internet 'n eiesoortige uitdaging daargestel het. Rekenaars vorm 'n integrale deel van die rekeningkunde en met die integrasie van rekenaars en stelsels, is die beheer rondom sulke integrasies van uiterste belang. Die akkuraatheid van inligting is belangrik vir die sukses in die besluitnemingsproses wat 'n uitwerking op die markpryse van aandele mag hê, asook op ekonomiese kragte.

Die risiko in e-besigheid is dieselfde as dié van die konvensionele wêreld. Dit is net groter en meer in die openbaar en moet dus met groter omsigtigheid hanteer word (Mitchell, 2000). Dit is belangrik dat sekuriteit en kontroles ingestel word om voldoende rekeningkundige beheer te bied oor die akkuraatheid van inligting, toegangsbeheer, vernietiging van data en die elektroniese omgewing waarin transaksies plaasvind en dat dit op 'n gereelde basis geëvalueer word.

1.2 PROBLEEMSTELLING

Die internet het die wêreldmark aan die voete van gebruikers geplaas. E-handel kan daarom grensloos deur middel van die internet, internasionaal plaasvind. Alhoewel die internet opwindende geleenthede vir beide die gebruikers en organisasies bied, bring dit egter ook wantroue oor die veiligheid van transaksies oor die internet teweeg. Hierdie *veiligheid van transaksies* verwys na die rekeningkundige beheer wat in en rondom die internet aanwesig is.

Rekeningkundige beheer behels nie net die aanteken van transaksies nie, maar ook die kontroles en beheer in en rondom die transaksies waarmee verseker word dat inligting veilig is, bedrog beperk word, die aanspreeklikheid vir die verlies van goedere en fondse tydens transaksies omskryf word, en ook dat daar aanvaarbare internasionale erkenning vir die regsgeldigheid van transaksies is. Terselfdertyd sal die belastingaanspreeklikheid vir e-handelstransaksies oorweeg en vasgestel moet word.

Die toekomstige sukses van e-handel sal afhang van die mate waartoe rekeningkundige beheer ingestel en toegepas word, en die vertroue wat gebruikers daarin stel.

1.3 DOELSTELLING

Die doelstelling van die navorsing is om die rekeningkundige beheer in e-handel te kwantifiseer, aanbevelings te maak waar hierdie beheer te kort skiet, en om sodoende die risiko van e-handel te minimaliseer.

1.4 ONDERSOEKGEBIED

Hierdie ondersoek na die rekeningkundige beheer in e-handel sal die breë veld van rekeningkundige beheer dek, maar in die besonder fokus op die kontroles wat tans beskikbaar is betreffende die veiligheid van e-handel om die toekomstige sukses van e-handel te verseker.

1.5 ONDERSOEKMETODE

Die ondersoekmetode sal op 'n literatuurstudie gebaseer word. Die studie sal die breë konsepte dek van die rekeningkundige beheer wat nodig is om die risiko van beide die gebruiker en die organisasie in e-handel te beperk. Die studie sal bykomend voort spruit uit navorser se kennis deur die bestudering van die rekeningkunde en die ouditkunde as studievelde, jare se ondervinding in die praktiese aanwending van hierdie kennis, die bestuur van rekeningkundige beheer en 'n eie ondersoek wat plaaslik en oorsee (Arrow Electronics – New York) na die implementering van rekeningkundige beheer in e-handel uitgevoer is.

1.6 HIPOTESE

Die hipotese word gestel dat die aanwesigheid van behoorlike rekeningkundige beheer, e-handel feitlik risikoloos kan laat geskied.

1.7 AANBIEDINGSMETODE

In Hoofstuk een word die motivering vir die studie, die ondersoekgebied en die ondersoekmetode omskryf.

Die teoretiese benadering van rekeningkundige beheer word in Hoofstuk twee in oënskou geneem. Hierdie hoofstuk vestig verder die aandag op die kennis van rekeningkundige beheer, asook op aspekte rakende die bedrewenheid in hierdie beheer.

Hoofstuk drie gee 'n agtergrond oor die ontstaan van die internet as 'n medium waardeur e-handel moontlik gemaak is.

In Hoofstuk vier word die begrip elektroniese handel *(e-handel)* en die uitbreiding daarvan in meer detail omskryf.

Die sekuriteit in en rondom netwerke vir die dryf van e-handel word in Hoofstuk vyf bespreek.

In Hoofstuk ses word die regswerking van e-handel omskryf.

Hoofstuk sewe stel ondersoek in na die belastingaangeleenthede van e-handel.

In Hoofstuk agt word verskeie aspekte van die elektroniese beheer van e-handel ondersoek en bespreek.

Aangesien daar aan die einde van elke hoofstuk 'n samevatting van die betrokke hoofstuk se inhoud gegee word, dien Hoofstuk nege as 'n kort en bondige samevattende oorsig van die hele studie. Hier word ook areas vir verdere ondersoeke geïdentifiseer.

Skematiese voorstellings en die inligting ter ondersteuning van sekere aspekte wat in die bogenoemde hoofstukke bespreek is, word as bylaes tot die studie aangeheg.

HOOFSTUK 2

TEORIE VAN REKENINGKUNDIGE BEHEER

2.1 INLEIDING

Met die verandering in die manier waarop sake bedryf word en die aantekening van transaksies, ontstaan die vraag of die teorie van die rekeningkunde en die beheer daaroor nog geldig is. Is dit moontlik dat die teorie van rekeningkundige beheer sedert die veertiende eeu se dubbelinskrywingsboekhouding ongeldig of verouderd is met betrekking tot vandag se elektroniese manier van handeldryf?

'n Kort oorsig oor die ontstaan van die rekeningkunde en rekeningkundige beheer word in hierdie hoofstuk weergegee, om die voortgaande vraag en ook ander voortspruitende vrae te beantwoord.

2.2 GESKIEDENIS VAN REKENINGKUNDE

2.2.1 Inleiding

Dit is amper onmoontlik om die plek of die datum vas te stel van wanneer dubbelinskrywingsboekhouding ontstaan het. Dit wil egter voorkom dat dit in die begin van die dertiende eeu tot die einde van die veertiende eeu in Italië ontwikkel het.

Ananias C. Littleton skryf in sy boek, "Accounting Evolution to 1900", dat die vinnige ontwikkeling van handel en besigheid die evolusie van die stelsels van dubbelinskrywingsboekhouding uit daaglikse boekinskrywings versnel het en dat dubbelinskrywingsboekhouding geforseer is tot die ontwikkeling van die rekeningkunde (Kojima, 1995:34).

2.2.2 Die ontstaan van rekeningkunde

Sedert 1970 vind daar 'n oplewing plaas in die belangstelling in die geskiedenis van die finansiële rekeningkunde. 'n Vraag kan egter gevra word na die waarde van geskiedenis en veral die geskiedenis van die rekeningkunde. Volgens Edwards

(1989:1) beskryf Napoleon *geskiedenis* as 'n stel vooraf ooreengekome leuens en Herbert Spencer verwys daarna as 'n waardelose geskinder. Maar Aristoteles verklaar dat om enigiets te verstaan, jy die begin en die ontwikkeling daarvan moet waarneem.

Die waarde van die geskiedenis van die rekeningkunde is drieledig. Behalwe dat dit ontspannend en intellektueel van aard is, is dit ook waardevol in die oplossing van probleme. Waar dit ons intellektueel help om die verlede te verstaan en aan ons 'n waardering gee vir hoe die huidige praktyke en probleme ontstaan het, bied dit ook aan ons die insig om oplossings vir huidige rekeningkundige probleme te vind en om toekomstige ontwikkeling in die rekeningkunde te voorspel (Edwards,1989:3-5).

Gedurende die pre-kapitalistiese tydperk, 4000v.C. tot 1000n.C. was die rekeningkunde gemoeid met die opskryf van inligting en die produksie van bates, en nie met besluitneming en finansiële bestuur nie (Mathews *et al.*, 1996:9). Kojima (1995:25) sê die Romeinse teorie, waarna ook verwys word as *slawe-rekeningkunde*, beskryf 'n dagboek en 'n inkomste-en-uitgawe-boek wat deur slawe namens hulle eienaars bygehou is, waar die krediet van die eienaar teen die debiet van die lener gebalanseer is.

Die tweede tydperk in die ontwikkeling van die rekeningkunde dek die periode vanaf 1000 tot 1760 en dit staan bekend as die kommersiële kapitalistiese tydperk. Edwards (1989:10,12) wys daarop dat die sirkulasie van kapitaal en die investering in voorraad en handel gedurende hierdie tydperk ontstaan. Dit is ook die tydperk van die industriële revolusie en die ontstaan van vervaardigingstelsels. Die bou van fabrieke, produksielyne, asook die ontwikkeling van masjinerie en die installering daarvan, lei die volgende fase in die ontwikkeling van die rekeningkunde in, naamlik die industriële kapitalisme (1760-1830) (Mathews *et al.*, 1996:12).

Gedurende die kommersiële kapitalistiese tydperk word verskeie Italiaanse teorieë voorgestel. Die Genoa-teorie verwys na die tesourie van die Genoa-gemeenskap, wat 'n grootboek-, debiteure- en 'n goedere-rekening insluit en 'n uitgawe-, asook 'n wins-en-verliesrekening gebruik. Die "Tuscany"-teorie verwys op sy beurt na die rekeningeboek van "Champage of Rinieri Fini and Brothers of Florence", wat in 'n paragraaf-vorm

voorkom en van kruisverwysings na korresponderende krediete of debiete gebruik maak.

Melding moet gemaak word van Pacioli, 'n wiskundige en monnik wat betrokke was by die skepping van die dubbelinskrywingsboekhouding. In sy publikasie, "Summa" (1494), gee hy die volgende voordele van die dubbelinskrywingsboekhouding, naamlik dit maak die neem van groter sorg moontlik, ingestemdheid op korrektheid, maak dit moeiliker om boeke te vervals, asook om bedrog en diefstal te versin, en dit akkommodeer die verdeling van pligte en rekeningkundige kontrole via die proefbalans. (Mathews *et al.*, 1996:13; Hannay, 2003:58).

Gedurende die tydperk 1394-1400, is rekeningboeke van die Del Maino Bank in 'n katedraal in Milaan ontdek wat aanleiding tot Lombardy se teorie gegee het (Kojima, 1995:25). Volgens Yamey (1978:101) is dit egter die boeke van Freris Bonis van Montanbau (1339) en die munisipale boeke van Genoa (1340), wat die eerste voorbeelde van 'n dubbelinskrywingsboekhouding toon. Daar word ook na hierdie dubbelinskrywingsboekhouding verwys as sistematiese boekhouding of sistematiese rekeningkunde wat dit moontlik maak vir die kapitalistiese entrepreneur om sy doel te formuleer en sy planne vir die toekomstige aktiwiteite te bepaal (Yamey, 1978:99-100). Die voorgenoemde skrywer (1978:111-112) wys daarop dat spesifieke rekeninge ontwerp is om aan spesifieke behoeftes te voldoen, wat dan moontlik aanleiding gegee het tot 'n stelsel van rekeninge wat kon dien om verskeie areas gelyktydig te dek.

Littleton stel volgens Edwards (1989:12) sewe voorvereistes vir sistematiese boekhouding, naamlik die kuns om te skryf, rekenkuns, privaat eiendom, geld as 'n vorm van handel, eienaarskap van kommersiële aktiwiteite, kapitaal en investering, en krediet-transaksies.

Die vierde en huidige fase van rekeningkundige ontwikkeling staan bekend as die finansiële kapitalistiese periode (1830 -) (Edwards, 1989:9).

Hierdie periode behels die instelling van maatskappyeregswerking deur die instelling van die "Joint Stock Companies Registration"-wet (1844) en die daarstelling van die Vereniging van Rekenmeesters in Edinburgh, Skotland (1853). Voorts wys Edwards

(1989:13) daarop dat die periode ook byvoorbeeld die ontwikkeling van verslagdoening van resultate, verdeling van uitgawes in kapitaal en inkomste, waardasie van bates en die publikasie van finansiële state beleef. Die skrywer (1989:14) beklemtoon dat rekeningkunde aanpasbaar, maar ook behoudend is. Dit kan verander, maar verander nie sonder oorsaak en rede nie.

Individuele studies vind plaas op 'n voortdurende basis om die rekeningkunde verder te ontwikkel, onder andere deur persone soos Paton (1922), Gilman (1939), Paton en Littleton (1940) asook Grady (1965) (Mathews *et al.*, 1996:14-20).

2.2.3 Doelwit van rekeningkunde

2.2.3.1 Inleiding

Die geskiedenis van die rekeningkunde verwys na die opteken van inligting deur middel van die boekhouding van transaksies. Hierdie prosedure behels volgens Faul (1989:6) 'n verwysing na rentmeesterskap, waar die rentmeester aan sy heer verslag en verantwoording gedoen het omtrent die bates wat aan hom toevertrou is. Die inligting is beheer deur gebruik te maak van 'n boekhoudingstelsel. Droms (1990:49) wys daarop dat die dubbelinskrywingsboekhouding 'n boekhoudingstelsel is wat 'n stel tegnieke voorsien om rekeningkundige data by te hou, terwyl die waarskynlikheid van rekenkundige foute terselfdertyd uitgesluit word.

Daar word dikwels na die rekeningkunde as die *universele taal van besigheid* verwys. Die rekeningkundige proses is dus volgens Droms (1990:46) 'n finansiële inligtingstelsel wat die aantekening, klassifisering, verslagdoening en die interpretasie van finansiële data behels.

2.2.3.2 Rekeningkundige proses

Die rekeningkundige proses omvat die opneem van transaksies, die verwerking van hierdie transaksies (data) in inligting, die weergee van dié inligting in relevante, verstaanbare, betroubare, volledige, objektiewe, tydige en vergelykbare formaat aan verskeie gebruikers (vergelyk Faul, 1989:3-5, 13-14; Lambrechts, 1990:40).

Voorts bepaal die metodes en prosedures van die rekeningkunde hoe data en inligting volgens die beginsels van 'n rekeningkundige proses hanteer moet word.

Dit vorm ook die reëls waarvolgens transaksies onder verskillende omstandighede binne die raamwerk van die beginsels aangeteken en die inligting verder behandel en aangebied behoort te word (Faul, 1989:27).

Die mate waarmee sorg gedra word om die regte metode vir 'n bepaalde stel omstandighede objektief te kies, bepaal volgens Faul (1989:28) die verskil tussen 'n goeie en 'n swak rekeningkundige proses.

Faul (1989:28) wys verder daarop dat die rekeningkunde se ontwikkeling nie 'n willekeurige nie, maar 'n langsame proses is om die regte benadering te kry wat 'n rekeningkundige oplossing vir 'n rekeningkundige probleem sal bied.

Die begrip rekeningkundige *praktyk* behels die gebruik van algemeen aanvaarde praktiese reëls ten opsigte van die toepassing van 'n bepaalde metode of prosedure, en die toepassing van beleid volgens die heersende omstandighede (Faul, 1989:28).

Rekeningkunde moet na die mening van Faul (1989:4) ook binne regsbeginsels en wette fungeer wat spesifiek toepaslik is op die betrokke ekonomiese aktiwiteit wat bedryf word. Sulke regsbeginsels verwys onder andere na die Maatskappyewet, Belastingwet, hofuitsprake, aanvaarde rekeningkundige praktyke, asook die vereistes en beginsels van die Johannesburgse Sekuriteitebeurs.

Die hoekstene van die rekeningkundige proses word vervat in die funksie van boekstawing en verslagdoening. Hierdie verslagdoening behels onder andere bestuursverslae, asook interim- en jaarverslae wat die finansiële state en resultate insluit.

Die doelwit van die rekeningkunde word as 'n kommunikasieproses voorgestel, in dié opsig dat inligting deur middel van finansiële verslae aan belanghebbende gebruikers verstrek word (Vorster *et al.*, 2002:15).

2.2.3.3 Verslagdoening

Rekeningkundige praktyke is volgens Correira *et al.* (1990:3) ontwerp om verslagdoeningsprosesse te standaardiseer. As sodanig beoog rekeningkundige praktyke op finansiële state om finansiële inligting te verskaf.

Faul (1989:5) wys daarop dat die verslae deur verskeie gebruikers gelees, bewerk en aangewend word, onder meer in die ontleding en vertolking van inligting vir verskeie besluitnemings, onder andere by kredietverlening en die bepaling van belastingpligtigheid.

Aangesien daar verskillende finansiële verslae mag bestaan, moet finansiële verslae volgens Correira *et al.* (1990:146) sulke beleid uitspel.

Die toepassing van die algemeen aanvaarde rekeningkundige (GAAP) en ouditstandaarde se belangrikheid in die verslaggewingsproses word deur Droms (1990:25) beklemtoon. Hierdie standaarde is oor baie jare ontwikkel met die doel om die opstel en aanbieding van finansiële state te reguleer.

'n Raamwerk vir die opstel en aanbieding van rekeningkundige state is deur die Rekeningkundige Praktykraad van die Suid-Afrikaanse Instituut van Geoktrooieerde Rekenmeesters (SAIGR) goedgekeur en word in standpunt RE 000 vervat.

Reeds in 1973 het die Amerikaanse Instituut van Gesertifiseerde Publieke Rekenmeesters (AICPA) egter die "Trueblood"-verslag onderskryf, waarmee twaalf doelstellings van finansiële verslaggewing voorgelê is. Dit sluit onder meer die besluitnemings- proses in, die opstel van finansiële state, kontantvloei-state, verdienste, openbaarmaking en sosiale besorgdheid (Williamson, 2003).

Correira *et al.* (1990:145-146) wys daarop dat finansiële state en die ontleding daarvan afhanklik is van rekeningkundige gegewens. Sulke gegewens poog om hoogs ingewikkelde en uiteenlopende ekonomiese gegewens en gebeure op skrif te stel. Groot gedeeltes van hierdie finansiële data in finansiële state is gegrond op subjektiewe eerder as objektiewe kriteria. Die subjektiwiteit spruit voort uit die raming en die oordeel

van rekenmeesters. Aangesien verskillende beleide toegepas kan word en dit nie eenvormig en onvergelykbaar is nie, moet rekeningkundige beleid verklaar en openbaar word.

2.3 ONTWIKKELING VAN OUDITKUNDE

Die ouditkunde het soos die finansiële rekeningkunde sy beslag in die ontwikkeling van die entiteit as 'n afsonderlike eenheid gevind. Faul *et al.* (1989:8) beklemtoon dat die openbare ouditeur se statutêre pligte deur wetgewing vasgelê word, naamlik die Maatskappyewet No. 61 van 1973 soos gewysig, waar onder andere 'n verslag oor sy werksaamhede uitgebring moet word. Verder word sodanige gerig deur die riglyne wat neergelê is in algemeen rekeningkundige en ouditstandaarde.

Die ouditkunde het ontwikkel deur 'n proses van die gedetailleerde nagaan van gegewens en het ontstaan as 'n neweproduk van die regsveld, asook van gebruike met voorgeskrewe vorme en prosedures. Die teorie van die ouditkunde bevat sekere tegnieke, prosedures, beginsels en die aanvaarding van standaarde.

Die filosofie van die ouditkunde is om ons terug te neem na die basiese of eerste beginsels, dit is besorg oor die sistematiese organisering van kennis en dit voorsien 'n basis waarvolgens sosiale verhoudinge ontwikkel en verstaan word (Mautz *et al.*, 1961:1-9). Die woord *ouditeur* is dan ook afgelei van die Latynse woord "audire", wat beteken *om te hoor*. Dit impliseer iemand wat homself tevrede stel met betrekking tot die waarheid van die rekenskap van iemand anders (Puttick *et al.*, 1998:2).

Waar die rekeningkunde te make het met die bymekaarmaak van inligting, asook die klassifikasie, opsomming en die kommunikasie daarvan, oorweeg die ouditkunde die besigheidsgebeure en-toestande. Dit oorweeg die maatstawwe wat gebruik is en die kommunikering van die rekeningkunde. Mautz *et al.*, (1961:10-19) bespreek die voorgaande en lig die hieropvolgende punte betreffende die ouditkunde, naamlik :

- dit is oudities, krities en ondersoekend;
- dit lê klem op die bewyslewering en verifikasie van feitlike gegewens (inligting en data);

- dit is 'n gespesialiseerde kennisveld en
- dit is 'n toegepaste dissipline.

Die tentatiewe postulate van die ouditkunde is volgens Mautz *et al.* (1961:49-59) dat finansiële state en finansiële data verifieerbaar is. Voorts dat daar geen konflik van belange bestaan tussen die ouditeur en die bestuur van 'n organisasie waar die oudit plaasvind nie; dat die finansiële state en ander inligting aangebied vir verifikasie, vry van korrupsie en onregmatigheid is; dat aanvaarbare stelsels van interne kontrole bestaan en dit die moontlikheid van onregmatigheid elimineer; dat die konsekwente toepassing van AARP in die redelike aanbieding van die finansiële posisie en die resultate van bedrywe konsekwent geskied; dat dit wat in die verlede waar was, ook in die toekoms geldig is waar voldoende bewys ontbreek, en dat die ouditeur ten alle tye sy onafhanklikheid behou.

Mautz *et al.* (1961:83) beskou die lewering van bewyse, die neem van behoorlike ouditsorg, redelike aanbieding, onafhanklikheid en etiese gedrag, as die basiese konsepte van die ouditkunde. Aangesien die ouditkunde volgens die voorgenoemde skrywers (1961:94) besorg is met die beskerming van lesers van finansiële state, het dit ten doel om sekere standaarde van akkuraatheid, deursigtigheid en volledigheid te handhaaf.

Die betrokke skrywers (1961:104-105) konstateer dat bewyslewering van 'n natuurlike aard kan wees, ontwikkel word, of deur middel van logiese denke aangebied word. Dit kan fisies van aard wees, standpunte van derde partye en gemagtigde dokumentasie insluit of na voldoende interne kontroleprosedures verwys.

Die ondervinding en bekwaamheid van die ouditeur speel uiteraard 'n belangrike rol in die verkryging en aanvaarding van bewyse (Mautz *et al.*,1961:109). Die voorgaande geld volgens die betrokke skrywers (1961:135-142) ook by die neem van behoorlike ouditsorg en die aanvaarding van verantwoordelikheid ten opsigte van die effek wat onreëlmatighede op finansiële state mag hê.

Alhoewel die ouditkunde en die rekeningkunde in noue verband tot mekaar staan, is die ouditkunde 'n dissipline in sy eie reg en logika (Mautz *et al.*,1961:191). Hierdie eiereg

van die ouditkunde sluit dan aan by die konsep van onafhanklikheid, wat op sy beurt volgens die skrywers (1961:246) noodsaaklik is om te verseker dat 'n ouditeur se mening waarde het.

Die laaste konsep van die ouditkunde verwys na etiese gedrag, wat veral teenoor kliënte, die gemeenskap en die ander lede van die professie geopenbaar moet word.

2.4 REKENINGKUNDIGE KONTROLE

Kontrole "control" word in "The Concise Oxford Dictionary of Current English" (1990) omskryf as die aanwys van rigting, die gee van leiding of die inhou van mag, en die fondasie van kontrole is volgens Lamperti *et al.* (1953:24) toesighouding. Die objektiwiteit van kontroles lê in die betroubaarheid en die integriteit van inligting, die nakoming van beleid, planne, prosedures, wette en regulasies, die beveiliging van bates, die ekonomiese en effektiewe aanwending van hulpbronne en die uitvoering van neergelegde doelwitte van bedrywe en programme (Ratliff *et al.,* 1996:12).

Inligtingstelsels word in twee aspekte verdeel, naamlik rekeningkundige inligting en operasionele inligting, en kontroles moet beide hierdie aspekte dek. Om behoorlike kontrole uit te oefen, moet die bestuur beleid, planne en prosedures instel, en moet dit geëvalueer word of dit voldoende is en wel toegepas word. Hier speel die interne oudit 'n belangrike rol in die kontroleproses. Eksterne kontrole word volgens Ratliff *et al.* (1996:99) deur regswerking en regulasies, byvoorbeeld die Maatskappyewet en die rekeningkundige standaarde opgelê.

Kontroles kan verder voorkomend, ontdekkend, korrektief, voorskriftelik en kompenserend van aard wees. Daarenteen, word operasionele kontrole vervat in beplanning, 'n begrotingsproses, rekeningkundige en inligtingstelsels, dokumentasie, bemagtiging, asook beleid en prosedures (Ratliff *et al.*, 1996:101-110).

In die kontroles oor handelstelsels by die opsporing en voorkoming van bedrog, word op organisatoriese fokus, bestuursbetrokkenheid en betragting, verdeling van pligte en die beoefening van oordeel vertrou.

In rekenaarstelsels, die sentrale deponeerplek van inligting, verander die pligte van 'n gebruiker na die van 'n voorbereider en 'n verwerker van data asook na 'n gebruiker van die afvoer. 'n Ramp in die rekenaarstelsel kan nie net 'n stelsel uitwis nie, maar ook al die inligting van 'n organisasie.

Voorkomende kontroles ten opsigte van die magtigingsproses, vaslegging van data en die veilige bewaring van bates en die opsporing van foute en onreëlmatighede by die rekonsiliasie- en waardasiehandelinge, moet noukeurig na omgesien word (Lay *et al.*, 1987:3-14).

'n Aanvaarbare rekeningkundige stelsel moet volgens Lamperti *et al.* (1953:25,125) voldoende kontroles bevat om die korrekte inligting op te neem, te verwerk en weer te gee. Terselfdertyd is die eksterne ouditeur 'n belangrike skakel in die kontroleproses.

2.5 SAMEVATTING

Ekonomiese aktiwiteite gee aanleiding tot transaksies en transaksies op hulle beurt is die grondstof van die rekeningkunde. Die rekeningkunde dui op 'n diensaktiwiteit en sy funksie is om kwantitatiewe inligting van 'n hoofsaaklik finansiële aard omtrent ekonomiese entiteite te voorsien. Sulke inligting moet in die ekonomiese besluitnemingsproses bruikbaar wees (Faul *et al.*, 1989:voorwoord, 5).

Die Engelse vertaling van *rekeningkunde* (-rekeningkundige), is "accounting". Die woord "accounting" word in "The Concise Oxford Dictionary of Current English" (1990) omskryf as "the process of or skill in keeping and verifying accounts". Nie net impliseer dit dus die hou van inligting nie, maar ook die vasstel van die waarheid of korrektheid daarvan by wyse van 'n ondersoek of 'n demonstrasie. Rekeningkundige beheer omsluit dus die werksaamhede van beide die rekenmeester en die ouditeur.

Die geskiedenis van die rekeningkunde dateer uit die Mesopotamiese beskawing en aangesien dit aanpasbaar is, het dit oor die eeue heen sodanig ontwikkel om vandag nog steeds toepaslik en geldig te wees.

HOOFSTUK 3

DIE INTERNET EN WEBTERREINE

3.1 DIE INTERNET

3.1.1 Ontstaan

Die RAND Korporasie, 'n vooraanstande Amerikaanse organisasie vir die strategiese beplanning van koueoorlogvoering, het reeds ongeveer agt-en-dertig jaar gelede begin om 'n oplossing te vind vir die daarstel van 'n beheer-en-kontrolestelsel wat kommunikasie in Amerika moontlik sou maak en wat bestand sou wees teen 'n kernoorlog tydens so 'n oorlog en daarna.

'n Oplossing hiervoor is in 1964 bekend gemaak en dit is die "RAND"-voorstel genoem. Behalwe dat die stelsel geen sentrale gesag het nie, sou dit in 'n onstabiele omgewing opereer en boodskappe sou in pakkette hulle eie weg op 'n individuele basis deur die stelsel vind.

Die eerste toetsnetwerk is in 1968 deur die "National Physical Laboratory" in die Verenigde Koninkryk opgestel, en dit is kort daarna deur die "Pentagon's Advance Research Projects Agency" met 'n tweede en groter projek opgevolg.

Teen Desember 1969 was daar vier nodes geïnstalleer in 'n netwerk wat ARPANET genoem is. Die vier rekenaars kon data deur toegewyde hoë-spoed transmissielyne stuur en kon ook van ander rekenaars geprogrammeer word, wat dit moontlik gemaak het dat wetenskaplikes en navorsers nou mekaar se rekenaarfasiliteite oor lang afstande kon deel. Teen 1971 het die vier nodes tot vyftien vermeerder.

Dit het egter op 'n verrassende wyse duidelik geword dat ARPANET nie slegs vir langafstandrekenarisering gebruik is nie, maar dat nuus en persoonlike boodskappe die hoofverkeer geword het. Persoonlike adresse vir elektroniese pos het ontstaan en posadreslyste het toegelaat dat 'n boodskap aan meer as een netwerkintekenaar gestuur kon word.

Die oorspronklike kommunikasiestandaard, NCP ("Network Control Protocol"), is vervang deur meer gevorderde standaarde, bekend as TCP en IP ("Transmission Control Protocol" en "Internet Protocol") wat tot gevolg gehad het dat ander netwerke met ARPANET kon inskakel.

Aangesien TCP en IP publieke domeine was, was dit moeilik om mense te verhoed om met ander netwerke in te skakel. Dié vertakking van netwerke het bekend geword as "Internet". ARPANET het 'n noodsaaklikheid geword. Organisasies soos die "National Science Foundation" (1984) en die "National Institute of Health" en ook die Departement van Energie, het in die negentiger jare betrokke begin raak by die saak.

Vreemde rekenaars en sekere Amerikaanse rekenaars is gekenmerk deur hulle demografiese ligging. Die ander is gegroepeer in ses basiese internet-domeine, naamlik "gov" (regering), "mil" (militêr), "edu" (opvoeding), "com" (kommersieel), "org" (organisasies) en "net"- (deurgang of "gateway" tussen netwerke).

Die internet het uitbeweeg uit die militêre en navorsingsbasis, en behalwe vir heelparty ander velde, 'n belangrike kommersiële hulpmiddel geword.

Die internet behels dus vandag meer as net om pos te stuur, aan besprekingsgroepe deel te neem, of om lang afstandsberekening en leer-oorplasings te doen.

3.1.2 Eienaarskap en toegang

Die vryheid, gratis gebruiksmoontlikhede en ongebondenheid, maak van die internet 'n gesogte gebruikersmiddel met geen diensfooie of gebruikersfooie wat deur die internet self gehef of verhaal word nie. Elke persoon of groep is verantwoordelik vir hulle eie rekenaars en toegangslyne tot die internet.

Alhoewel verskillende groepe graag beheer oor die internet sal wil hê, byvoorbeeld die akademie om dit slegs vir navorsing en studie te gebruik, die militêre beheer slegs vir spioenasie en sekuriteit, die handel slegs vir finansiële gewin en die regering om meer regulasie daaroor uit te oefen, behoort die internet aan niemand nie, maar tog aan almal. Vandag het verskillende lande hulle eie infrastrukture en groot organisasies bedryf hulle eie private beginselvastheid vir die oordra van handelsdata.

Om toegang tot die internet te verkry, vereis 'n rekenaar en 'n modem. 'n Rekenaar dien as 'n terminaal en die telefoon as die konneksie tot 'n internet gekoppelde masjien. Hierdie toegang tot 'n internet gekoppelde masjien kan op 'n tydbasis gehuur word van organisasies wat internettoegang het, naamlik tot hoëspoedinternet-TCP/IP-lyne (Bruce, 2001:1-6).

3.1.3 Samevatting

Die ontstaan en geskiedenis van die internet kan soos volg saamgevat word:

1962	Die RAND Korporasie begin navorsing in 'n growwe distribusie-kommunikasienetwerk vir militêre gesag en beheer.
1962-1969	Onder leierskap van die "Defence Advanced Research Project Agency" (ARPA) ontwikkel 'n klein netwerk, ARPANET, vir die gebruik van "super"-rekenaars tussen navorsers in die Verenigde State van Amerika.
1968	Die eerste generasie van hardeware en sagteware word ontwerp.
1969	ARPANET konnekteer vier universiteite, naamlik Stanford, UCLA, UC Santa Barbara en UTAH.
1970-1973	Alhoewel ARPANET ontwikkel is vir die uitruil van data, word die stuur van pos (e-pos) die gewildste aanwending.
1971	Drie-en-twintig universiteite en regeringsinstansies gekoppel deur ARPANET.
1972	"The Internetworking Working Group" is die eerste organisasie om die daarstelling van standaarde vir die netwerk te monitor.
1973	ARPANET beweeg buite die Verenigde State van Amerika, na London.
1974	Die eerste kommersiële weergawe van ARPANET word deur Telenet geopen.
1979	Die eerste gebruikersnuusgroep word daargestel, naamlik USENET.

1982	Die term *internet* word vir die eerste keer gebruik.
1982-1987	TCP/IP, die algemene taal vir internetrekenaars, word ontwikkel.
1983	Die term "Cyberspace" (kuberruimte) ontstaan (William Gibson).
1988	Die eerste Internet-wurm/virus, verskyn.
1988-1990	Terme soos "hacker", "cracker" en "electronic break-in" ontstaan.
1988	CERT ("Computer Emergency Response Team") word gevorm om sekuriteit gebreke aan te spreek wat deur wurms veroorsaak word.
1989	ARPANET word gekommersialiseer.
1990	Die "WorldWideWeb", (www) (Wêreldwye Web), word "gebore".
1995	Die internetprogrammateurtaal, JAVA, word vrygestel.
1996	Die internet word 25 jaar oud en huisves ongeveer 40 miljoen gebruikers.

3.2 WEBTERREINE

Die internet, 'n rekenaarnetwerk van netwerke, stel 'n infrastruktuur daar wat rekenaars toelaat om met mekaar te skakel deur die gebruik van standaardprotokolle, naamlik TCP/IP, wat veroorsaak dat verskillende tipe rekenaars wat verskillende sagteware gebruik met mekaar kan kommunikeer.

Tim Berners-Lee het in 1980 'n program die "Enquire", geskryf om homself te help om inligting te onthou betreffende mense en projekte in die laboratorium van CERN ("European Particle Physics Laboratory" – Geneva).

Hy ontwikkel 'n sagtewareprogram, "Hypertext", wat toelaat dat dokumente gekoppel kan word en hiermee as basis, ontwikkel hy die "Hypertext Transfer Protocol" (HTTP), die taal wat rekenaars sou gebruik om hiperteks-dokumente oor die internet te laat kommunikeer. Hy noem dit voorgenoemde die "WorldWideWeb" (www), 'n naam vir al die inligting wat aanlyn beskikbaar is en deel vorm van die internet.

Die Web word universeel en op 24 Mei 1994 is die eerste www-konferensie gehou. Dit is saamgeroep omdat vrees bestaan het dat die Web tot destruktiewe kompetisie sal lei wat die 'oop beginsel' van die Web skade sou aandoen.

Later dieselfde jaar is die www-konsortium (W3C) gestig. Die doel hiervan was dat enige organisasie daaraan kan behoort en tegniese spesifikasie gratis vrygestel word wat tot die ontwikkeling van die Web sal bydra.

3.3 TERMINOLOGIE

In die "Fortune", Vol. 142 No. 1 se spesiale advertensie-seksie, word verwys na e-lewering wat nuwe vrae laat ontstaan na onder andere standaarde, kulture, belasting, regsaspekte en dat die koms van die internet en e-handel nuwe woorde en terminologie voortgebring het.

Die meer algemene gebruikte name word hierna in Engels en Afrikaans en in 'n kort beskrywing weergegee. 'n Nuwe bygewerkte weergawe van rekenaartaal deur Samuel Murray-Smit kan op http://groups.yahoo.com/ group/ rekenaarterme, afgehaal word.

Application Service Provider (ASP) / Aanwendingsdiensverskaffer (ADV)

Dit is 'n organisasie wat sagteware huisves op bedieners binne sy eie fasiliteite. Kliënte mag dit deur middel van privaat lyne of die internet binnegaan.

Authentication / Stawing (Bekragtiging)

Dit is die proses om 'n gebruiker se identiteit te verifieer.

B2B / B2B

Besigheid-tot-Besigheid

B2G / B2C

Besigheid-tot-Gebruiker

Backbone / Hoofstruktuur

Dit is die boonste vlak in 'n hiërargiese netwerk.

Bandwidth / Bandwydte

Die hoeveelheid data wat deur 'n kommunikasiebaan per sekonde gestuur kan word.

Browser / Blaaier

'n Program wat 'n persoon toelaat om hiperteks te lees.

Client / Kliënt

'n Rekenaarstelsel of proses wat 'n diens aanvra van 'n ander stelsel of proses ('n bediener).

Data Encryption / Data-enkripsie

Data-enkripsie is 'n hoogs veilige metode om sensitiewe inligting wat oor die Internet beweeg, te skerm deur die data te enkodeer en te krabbel (deurmekaar te maak).

Dot-com / Dot-com

Word ook nuwe-ekonomie-maatskappye genoem waarvan die primêre besigheid e-handel is.

Data Warehouse / Datastoor

'n Generiese term vir 'n stelsel om groot hoeveelhede data te stoor, herwin en te bestuur.

Digital Signature / Digitale handtekening

Addisionele data aangeheg aan 'n boodskap om die afstuurder en boodskapdata te identifiseer en te staaf deur gebruik te maak van 'n publieke-sleutel-enkripsie.

Domain / Domein

Op die internet verwys dit na 'n groep rekenaars waarvan die gasheername 'n gemeenskaplike suffiks (agtervoegsel) deel, naamlik die domeinnaam.

E-business / E-besigheid

E-besigheid omvat internet en e-handel en die integrasie van stelsels om 'n elektroniese verbinding met die besigheid se prosesse na die buite-wêreld te skep.

E-Commerce / E-handel

Sluit alle vorms van internethandel in, asook alle ander vorms van elektroniese handel oor private netwerke en sluit ook elektroniese data-interaksie in (EDI).

Eletronic Data Interchange (EDI) / Elektroniese data-interaksie (EDI)

'n Standaardformaat om besigheidsdata oor en weer te stuur.

Electronic Banking / Elektroniese bankwese

Sluit alle elektroniese bankfasiliteite in deur banke aangebied.

E-mail address / E-posadres

Die string wat gebruik word om die bron of destinasie van 'n elektroniese boodskap te spesifiseer.

Encryption / Enkripsie

Enige prosedure gebruik in kriptografie om gewone teks na syferteks om te skakel, om daarmee te verhoed dat iemand anders, behalwe die bedoelde ontvanger die data lees.

Extranet / Ekstranet

Dit is die verlenging van 'n maatskappy se intranet na die internet sodat kliënte, leweransiers en mobiele werkers toegang tot die maatskappy se data kan kry deur die Wêreldwye Web.

Firewall / Brandmuur (Skutmuur)

'n Alleenstaande deurgangmasjien met sekuriteitsvoorsorg om buite-netwerkskakelings en inskakellyne te diens.

Hypertext / Hiperteks

'n Term vir 'n aantal dokumente wat kruisverwysings of skakels bevat en met die hulp van 'n interaktiewe deurblaaiprogram die gebruiker toelaat om maklik van een dokument na 'n ander te gaan.

Hypertext Mark-up Language (HTML) / Hiperteksbyvoegingstaal

'n Hiperteksdokument in 'n formaat wat op die Web gebruik word.

Hypertext Transfer Protocol (HTTP) / Hiperteksoordragprotokol

Die kliëntbediener se TCP/IP-protokol op die Wêreldwye Web vir die uitruil van HTML-dokumente.

Internet / Internet

Die internet is die TCP/IP-basis van intergekonnekteerde bedieners wêreldwyd, wat kommunikasie en aanwendingsdienste aan 'n internasionale basis van besighede, gebruikers, opvoedkunde en navorsing van ander organisasies voorsien.

Internet Service Provider (ISP) / Internetdiensverskaffer (IDV)

Dit is 'n persoon, maatskappy of organisasie wat toegang tot die internet verskaf.

Intranet / Intranet

'n Netwerk wat soortgelyke dienste lewer binne 'n maatskappy, maar wat nie noodwending aan die internet gekoppel is nie.

Packet / Pakket

Die data-eenheid oor 'n netwerk gestuur.

Protocol /Protokol

'n Stel formele reëls wat beskryf hoe om data oor 'n netwerk te stuur.

Router / Roteerder

'n Toestel wat pakkette tussen netwerke aanstuur.

Secure Sockets Layer / Sekuriteitsoklaag

'n Protokol ontwerp deur "Netscape Communications Corporation" om veilige kommunikasie oor die internet te voorsien.

TCP/IP

Oorsendingskontroleprotokol oor internetprotokol.

Web page / Webbladsy

'n Blok data beskikbaar op die Wêreldwye Web.

Web Server / Webbediener

'n Bedienerproses wat op 'n webtuiste hardloop en webbladsye uitstuur in rekasie op HTTP-versoeke van afgeleë snuffelaars.

Web Site / Webtuiste

Enige rekenaar op die internet wat 'n www bedienerproses loop.

World Wide Web (www) / Wêreldwye Web (www)

'n Internet-kliëntbediener wat 'n herwinningstelsel van hiperteks verspreide inligting daarstel en wat sy oorsprong van CERN in Geneva het.

3.4 DOMEINNAME

Die internet is die wêreld se grootste kommersiële hulpmiddel vir die stoor en oorstuur van inligting. Om deel te hê hieraan, moet 'n organisasie die internet betree, óf deur sy

eie domeinnaam te registreer óf deur 'n internet-diensverskaffer se domeinnaam. Hierdie domeinnaam of rekenaaradres is ook bekend as 'n IP-adres en word deur die rekenaar as 'n internasionale telefoonnommer herken. Wanneer 'n domeinnaam in die rekenaar gesleutel word, skakel die internetsagteware outomaties die domeinnaam om na die genommerde adres.

'n Domeinnaam moet uit ten minste twee vlakke bestaan, 'n topvlak-domeinnaam en 'n tweede vlak-domeinnaam. Die topvlak is die .co.za. Daar is twee tipes topvlak-domeine, nasionaal en internasionaal, waar die nasionale domeine twee letters bevat, naamlik byvoorbeeld za vir Suid- Afrika, uk vir Verenigde Koninkryk, zw vir Zimbabwe, nz vir New Zealand, ensovoorts.

Daarenteen, verwys die internasionale vlak na generiese kategorieë, .com staan byvoorbeeld vir kommersieel, .org vir organisasie, .net vir netwerk. Die topvlak-domeinname, .mil (militêr), .edu (opvoedkunde) en .gov (regering), is gereserveerde name.

Die tweedevlak-domein van domeinname bevat dan die handelsnaam of die houernaam van die domeinnaam. In Suid-Afrika word co.za gebruik deur kommersiële organisasies (co = com) en ac.za deur navorsing en akademiese instellings. Org.za is vir nie-kommersiële organisasies en nom.za vir individue en persoonlike name. Die maklikste manier om 'n domeinnaam te registreer, is om deur 'n internetdiensverskaffer te werk.

3.5 SAMEVATTING

Alhoewel die internet reeds indirek in 1962 ontwikkel is, is dit heelwat later, naamlik in 1974 gekommersialiseer.

Die Wêreldwye Web (www) is deur Tim Berners-Lee ontwikkel wat deur middel van HTTP, rekenaars oor die internet laat kommunikeer.

Dit het nuwe moontlikhede daargestel, onder andere die gebruik van die internet om besigheid te doen, e-handel.

Die sukses van hierdie nuwe manier van besigheid doen, sal afhang van die integriteit en vertroue wat die kanaal aan alle gebruikers wêreldwyd sal bied. Die aantal gebruikers wat aankope elektronies doen, neem egter reeds toe.

Yahoo se aanlyndiens het met 86% gestyg gedurende die 2001-Kersseisoen, vergeleke met die ooreenstemmende tydperk die vorige jaar. So, het "The Shopping Matrix.com" verklaar dat nuwe kliënte vir 38% van die transaksies in die vierde kwartaal in 2001 verantwoordelik was ("Sake-Beeld", Dinsdag 15 Januarie 2002, bladsy 5).

Daar word verwag dat e-handel teen 2005 verantwoordelik sal wees vir 7 miljard dollar se verkope ("Business Day Survey", Donderdag 5 Oktober 2000). Daar is dus geen twyfel dat e-handel 'n toenemende invloed op die wêreld-ekonomie sal hê nie.

HOOFSTUK 4

ELEKTRONIESE HANDEL

4.1 INLEIDING

Elektroniese handel, of beter bekend as e-handel, kan omskryf word as die gebruik van elektroniese netwerke om inligting uit te ruil in die verkoop van produkte en dienste, en vir die betaling van sulke transaksies.

Hierdie metode vorm 'n teenstelling met die tradisionele manier van sake doen, waar 'n gebruiker fisies 'n besigheid sal besoek om sake te doen, betaling per tjek of kontant (kredietkaart) sàl geskied en waar rekeningkundige data handgeskrewe of aflyn plaasvind.

E-handel kan geskied tussen besighede (B2B), tussen besighede en gebruikers (B2C), tussen besighede en regeringsinstansies, tussen regeringsinstansies en gebruikers, asook tussen gebruikers.

4.2 ELEKTRONIESE NETWERKE

4.2.1 Inleiding

"E-commerce, as a term, has come to mean trading over the Internet" (Davies, 1998:14).

Hierdie stelling veronderstel dat e-handel reeds vroeër in 'n ander vorm bestaan het en beoefen is.

4.2.2 Elektroniese data-uitruiling

Elektroniese data-uitruiling ("Electronic Data Interchange" of EDI) is al 'n geruime tyd in gebruik tussen organisasies en veral in die verskaffing van goedere.

Die Suid-Afrikaanse Instituut van Geoktrooieerde Rekenmeesters het in 'n heruitgawe in 1995 in 'n artikel, "Paperless Business Transactions. An introduction to the Risks and Controls", elektroniese data-uitruiling (EDU) as 'n metode van besigheid bespreek.

4.2.2.1 Oorwegings vir elektroniese data-uitruiling (EDU)

Alvorens 'n entiteit elektroniese data-uitruiling instel, is/was dit nodig om oorweging te gee aan sekere faktore om die sukses daarvan te verseker, naamlik:

- Vinniger responstyd word verwag.
- Kleiner hoeveelhede, meer gereelde aankope.
- Aftyd kan nie aanvaar word nie, aangesien vervaardigings-kontinuïteit belangrik is.
- Betalingsvoorwaardes word afgedwing.
- Toegang tot databasis en aldus sekuriteit daar rondom is wesentlik.
- Gemeenskaplike standaarde en koppelvlakke ('interface') is van toepassing.
- Sekere handkontroles sal gerekenariseerd word.
- Papiergedrewe stelsels en informasie sal deur rekenaars vervang en beheer word.
- Ongemagtigde toegang mag lei tot manipulasie, korrupsie, spioenasie en finansiële verlies.
- Onderskeid moet getref kan word tussen gemagtigde en ongemagtigde boodskappe deur die rekenaar.
- Regsaanspreeklikheid moet aangespreek word en dit mag verskil betreffende die bestaande en die gerekenariseerde metode van besigheid doen.

4.2.2.2 Verandering in risiko

Die verandering in risiko met die oorskakeling na EDU, mag insluit:

- onderbreking van prosesseringsvermoë,
- verskille rakende regsaanspreeklikheid,
- onakkurate en ontoepaslike aanteken van finansiële inligting,
- verhoogde bedrogsvlakke,
- verkeerde besigheidsbesluite word geneem as gevolg van foutiewe inligting,
- foute in rekenaarstelsels wat ongesiens mag plaasvind,
- 'n tekort aan rekenaarpersoneel,
- verlies van vertroulikheid,
- verlies van handkontroles,
- tekort aan en verlies van transaksiespoor en
- 'n toenemende vertroue op datakommunikasie en derdepartye-betrokkenheid.

4.2.2.3 Kontroleriglyne

Die oogmerke en die nodigheid vir interne kontroles verander nie as gevolg van die instelling van EDU nie. Dit is dus nog steeds nodig om verskeie gesonde besigheidsbeginsels te oorweeg.

- Strategiese beplanning en die daarstel van kriteria wat die entiteit die beste sal pas, moet plaasvind.
- 'n Risiko-analise moet toegangsbeheer van derde partye tot data, regsaanspreeklikheid en die kontinuïteit van dataprosessering insluit.

- Spesifieke standaarde vir EDU moet ingestel word. Hier word verwys na die "UN/EDI FACT STANDARDS" (United Nations Electronic Data Interchange for Administration, Commerce and Transport"). Dié standaarde sluit applikasie, implementering en boodskapontwerpreëls in.

- Beleid en prosedures moet voorsiening maak vir 'n elektroniese manier van besigheid doen.

- Ooreenkomste moet boodskap inhoud, formaat, boodskap erkenning, sekuriteitsverantwoording, aanspreeklikheid en toetsingskriteria aanspreek.

- Standaard-aanwending en sagtewarevoldoening moet van toepassing wees.

- Bestuur moet betrokke en verbind wees tot EDU.

- Rekeningkundige kontroles moet toegepas word.

- Omgewingsbeheermaatreëls moet toegepas word.

- Fisiese toegangsbeheer in programmatuur en data, programveranderinge, rugsteunprosedure en gebeurlikheidsbeplanning moet gevolg word.

- Voorkomende beheermaatreëls om die risiko van ongemagtigde, foutiewe en onwettige transaksies te verminder en te verhoed, moet ingestel word.

- Transaksies moet na al die toepaslike apparatuur gestuur word en slegs daarheen.

- Verslaggewing moet geskik en tydig wees.

- Tydelike datalêers moet verskans word teen ongemagtigde toegang.

- Korrekte boodskapopskrif, naskrif en identifikasie-inligting moet toegepas word.

- Formele en effektiewe beleid en prosedures om besigheidsvennote te verifieer, moet ingestel word.

- Die bron van EDU-transaksies moet gestaaf word.

- Kriptiese tegnieke moet aangewend word.
- 'n Data-sekuriteitsbeleidsdokument moet voorgelê word.
- Logiese en fisiese toegangsbeheer moet neergelê word.
- 'n Beleid vir kommunikasiesekuriteit moet verseker dat slegs gemagtigde boodskappe gestuur en ontvang word. Geen boodskappe moet foutief gekanaliseer of omgestuur word nie en boodskappe moet nie verlore gaan, gewysig of gedupliseer word nie.
- Die kommunikasienetwerk moet veilig bly en nie faal nie.
- Sekuriteit oor waarde-toegevoegde netwerke moet skriftelik neergelê word en hulle verantwoordelikhede en pligte moet volledig uiteengesit word, wat insluit fisiese toegangsbeheermaatreëls, datastoring, rugsteunprosedure, gebeurlikheidsplanne, die aanteken van transaksies en die algehele akkuraatheid van sagteware, asook kontroles om die akkuraatheid en volledigheid van data te verseker.

4.2.3 Debat oor elektroniese handel

4.2.3.1 Inleiding

In Julie 1999 is 'n besprekingsdokument oor e-handel uit die kantoor van die Minister van Kommunikasie vrygestel. Vroeër het e-handel privaat deur EDU tussen organisasies plaasgevind.

E-handel verwys dan na handeldryf oor die internet, soos beskryf deur Davies (vergelyk paragraaf 4.2.1).

4.2.3.2 Areas vir bespreking

Die besprekingsdokument verwys na verskeie areas vir oorweging en sluit in:

- Uitreiking van wetgewing teen 2001.

- Die daarstelling van 'n nasionale e-handelsbeleid wat ag slaan op die situasie in Suid-Afrika.
- Opbou van geloofwaardigheid.
- Vertroulikheid van data gedurende transaksies.
- Sekuriteit ten opsigte van die betaling en ontvangs van goedere.
- Implikasies van verskeie wette, soos byvoorbeeld die Maatskappyewet, kontraktereg en Belastingwet.
- Daarstel van grondbeginsels vir aankope en verkope oor die internet.
- Daarstel van kriptografie en beleid rakende digitale handtekeninge en die stawing van partye.
- Daarstel van 'n hoë graad van kredietwaardigheid en sekerheid rakende regeringsbeleid en regulasies.
- Ooreenstemming ten opsigte van aangeleenthede rakende belasting, doeane, wisselkoers en die handel dryf in beperkte goedere.
- Die reg op intellektuele kopiereg.
- Voorkoming van bedrog.
- Promosie van e-handel, die verryking van inligtingstegnologie, telekommunikasie en finansiële dienste.
- Neerlê van beginsels in die ontwikkeling van e-handel en spesifiek:

  uitwissing van armoede,

  opheffing van histories mindergegoede groepe,

  ekonomiese groei,

globale kompeterentheid en

promosie van 'n "post industrial society".

Daar word aanvaar dat groter klem gelê sal word op die uitwissing van armoede en die opheffing van histories agtergeblewe groepe, wat 'n spesifieke nadruk sal hê in vergelyking met die Amerikaanse regulasies.

- Verskille tussen die tradisionele manier van handel dryf en e-handel, met verwysing na die onpersoonlikheid, outomatisasie en alleenstaande begrip van e-handel.

- Vertroue dat die beginsels in e-handel ten opsigte van aankope, betaling, kwaliteit, diens, regsbeskerming en verantwoording, soortgelyk sal wees as dié in die tradisionele bedryf.

- Dat gebruikers beskerm sal wees en alle inligting veilig is. Die beginsels sluit onder andere sekuriteit, privaatheid, oorspronklikheid en die nakoming van beloftes in.

- Die erkenning van intellektuele eienaarskap, met klem op die "Trade Related Aspects of Intellectual Property Rights", 1995 (TRIPS).

- Die beheer en gebruik van internetname en -adresse.

4.2.4 Groenskrif oor e-handel

Die groenskrif oor e-handel het in November 2000 verskyn. Hoofstukke 1, 5, 9, 11, 12 en 13 van die groenskrif word hier geklassifiseer as dit wat met e-handel in die algemeen te make het, en sal in hierdie afdeling in oënskou geneem word.

Die ander dissiplines wat behandel word, is die wetlike aspekte in hoofstukke 2, 3, 6 en 10 van die groenskrif, en hier word dit bespreek in Hoofstuk 6; die belastingaspekte in hoofstuk 4 van die groenskrif, word hier bespreek in Hoofstuk 7, en die sekuriteitsaspekte in hoofstukke 7 en 8 van die groenskrif word hier in Hoofstuk 5 bespreek.

Hoofstuk 1 van die groenskrif bespreek globalisering en die inligtings- gemeenskap. Die transformasie van die globale ekonomie van 'n industriële na dié gebaseer op kennis en inligting, skep verskeie geleenthede en uitdagings. Dit word moontlik gemaak deur die gebruik van inligtings- en kommunikasie-tegnologie ("Information and Communications Technologies" – ICT's). Die gebrek aan infrastruktuur, hoë koste, swak kwaliteit infrastruktuur, 'n tekort aan toepaslike vaardigheid, lae vlak van lees-en-skryf-kennis en onvoldoende kapitale investering, is areas wat die ontwikkeling van ICT's in ontwikkelende lande kan verhinder.

ICT's word onderskraag deur digitalisasie wat die konvergensie van telekommunikasie, verspreiding, inligtingstegnologie en publikasie moontlik maak.

Die internet fasiliteer 'n grenslose omgewing vir kommunikasie en die lewering van sekere elektroniese dienste. Konvergensie van tegnologieë is 'n groot dryfkrag wat tot die eksponensiële groei van elektroniese handel bydra, binne 'n omgewing wat bevorderlik is om met vertroue handel te dryf en inligting uit te ruil.

Elektroniese handel word hier gedefinieer as die gebruik van elektroniese netwerke om inligting, produkte en dienste van betalings uit te ruil, vir kommersiële en kommunikasiedoeleindes, tussen individue (gebruikers) en besighede, tussen besighede, tussen individue, binne die regering, tussen die publiek en die regering, en tussen besighede en die regering.

Die hoofvoordele van e-handel is die verbeterde reaksietyd, verbeterde mededingende posisionering, die gemak om transaksies te sluit, vergrote markpenetrasie en aldus verhoogde omset, verhoogde gebruikersgerief en -keuse, verlaagde pryse en verhoogde gebruikersdienste.

Kwaliteit van lewe, internasionale riglyne, 'n raadplegende proses, veranderlikheid, tegnologies neutraal, tegnologies gebaseerde oplossings, 'n publieke private samehorigheid en die ondersteuning van klein, medium en mikro-ondernemings (SMME's), omarm die beginsels vir 'n e-handels- beleid vir Suid-Afrika. Die groenskrif is 'n raadplegende dokument met die regering se rol om hindernisse wat die ontwikkeling vir die groei van e-handel inhibeer, te voorkom en te verwyder.

E-handel word op verskeie forums gedebatteer, onder andere die "Organisation for Economic Co-operation and Development" (OECD), "United Nations Commission of International Trade Law" (UNCITRAL), "World Bank" en die "World Trade Organisation" (WTO).

Hoofstuk 5 van die groenskrif verwys na die multilaterale handelstelsel (MTS) wat deel vorm van die WTO en e-handel. Om e-handelgroei te stimuleer, is die daarstel van handelsooreenkomste en regsbeginsels om dit te implementeer, tegnologiese neutraliteit en die aanwending van gelykmatige reëls vir ekonomiese transaksies nodig. Die rade op goedere, dienste en die Raad van Intellektuele Eiendom (TRIPS) vorm deel van die WTO en ondersoek sake rondom globale elektroniese handel.

Hoofstuk 9 van die groenskrif bespreek die toegang tot infrastruktuur, kompetisie in telekommunikasie en konvergensie. E-handelgroei word ook onder andere geraak deur die bekostigbaarheid van toegang tot infrastrukture en genoegsame bandwydte. Die e-handel-infrastruktuur moet voldoende kapasiteit hê en dus vinnig en betroubaar wees. Toegang tot infrastrukture en dienste teen bekostigbare tariewe, is in Suid-Afrika vir baie gebruikers en klein besighede 'n hindernis en kan e-handelgroei demp. E-handel benodig 'n standaardplatform vir operasionele standaarde, wetlike standaarde en inligtingsekuriteitstandaarde.

Hoofstuk 11 van die groenskrif behandel e-handelstransaksiebetalings. Elektroniese betalings kan geskied deur die gebruik van tradisionele krediet- en debietkaarte en allerlei nuwe tipe krediet-instrumente. Die sekuriteit rondom hierdie vorms van betaling is van die bekommernisse in die opbou van vertroue in internet gebaseerde transaksies. Virtuele banke, slimkaarte, betaling per sellulêre telefone en geïntegreerde ontvangerdekodeerders ("set-top box"), vorm deel van die nuwe betalings- instrumente.

Die Suid-Afrikaanse Reserwebank het in April 1999 'n situasieskrif oor elektroniese geld gepubliseer, waarin voorgestel word dat ondersoek ingestel moet word na digitale tjeks, die voorkoming van die vervalsing van elektroniese geld en 'n definisie van die uitreiking van elektroniese geld.

Hoofstuk 12 van die groenskrif verwys na die voordele van e-handel en die nodigheid daarvan om dit na alle gemeenskappe en voorheen benadeelde individue uit te brei. E-handel bied 'n geleentheid vir minder ontwikkelde lande om hulle markte intern sowel as ekstern te vergroot. Dit kan geografiese grense hervorm en daartoe bydra om gemeenskappe in opvoeding, gesondheid en regeringsdienste te transformeer. Hoë fokus word geplaas op die kondisies om SMME's by te staan in die gebruik van e-handel. Dit sluit toegang tot bekostigbare telekommunikasie- infrastruktuur en internetkoppeling, bekwaamheid, asook kennis en vertroue in die elektroniese omgewing in. Vennootskappe is die sleutel tot die skep van 'n omgewing wat groei in elektroniese handel kan skep.

Hoofstuk 13 van die groenskrif bespreek die raamwerk vir 'n e-regering en die rede daarvoor. Dit is nie net van toepassing op die Suid-Afrikaanse regering nie, maar die beginsels is op alle organisasies van toepassing.

4.2.5 E-handel in werking

Sedert 1997 word die vordering van e-handel deur verskeie persone met verskillende vlakke van sukses en toekomsverwagtinge waargeneem. Hierna volg sekere van die opmerkings wat al in die verband gemaak is:

- "The Internet will change everything, every company, every country. There will be no company except an e-business company 10 years from now" (Chambers, 2001:46).

  Kan hierdie stelling sonder meer aanvaar word, of sal dit oor tyd bewys word?

- E-handel se sukses lê in 'n samesmelting van ou vaardighede en nuwe direksie. Wins, rekenskap, verantwoordelikheid en kliënt verhoudings is die sleutel tot e-handelsukses. Die koste van die verkryging van gebruikers, infrastruktuur, ondersteuning en sekuriteit is hoog en daarom is herhalende besigheid noodsaaklik (Koen, 1999:42).

Hierdie opmerking is in teenstelling met die positiewe standpunt van Chambers (vergelyk paragraaf (1)).

- In "Computing SA" van 2 November 1998 word verwag dat e-handel teen 2002 R87 biljoen sal bereik.

- Daar word verwag dat e-handel sal blom in Suid-Afrika, maar dat vertroue 'n belangrike rol speel in die besluit om aankope elektronies te maak (Van Zyl, 1998:13).

- Teen 2003 sal 5% van wêreldverkope elektronies geskied (Bidoli, 1999:54).

- In 'n artikel met die opskrif, "FNB forges ahead with e-trading", in "NETMASTER AFRICA", Vol. 3 No. 10 van Oktober 1998, word Eerste Nasionale Bank voorgehou dat hulle aanwendings-pakkette gaan installeer om aankope aanlyn oor die internet volledig beskikbaar te stel.

  Terselfdertyd word verklaar dat e-handel nie slegs 'n gegons is nie, maar alreeds 'n noodsaaklikheid is, met e-besigheid as die nuwe generasie van handel dryf oor die internet (Williams, 1998:46).

- Daar word aangevoer dat maatskappye se e-handel deur webtuistes in staat gestel word om volle, of gedeeltes van transaksies, aanlyn te voltooi (Gordon, 1999:18).

- Afsette aanlyn oor die internet is 'n realiteit en voorsien 'n effektiewe alternatiewe distribusiekanaal (Webster, 1998:20).

- Een van die hoofoorwegings vir suksesvolle verkope oor die internet, is die integrasie van die agterkant-infrastruktuur en die kontroles rondom voorraadstelsels. Spoed, gemak van gebruik, aanpasbaarheid, die veiligheid van transaksies en virtuele persepsie is die primêre faktore vir die sukses van aanlyn-verkope (Gibson, 1998:6-7).

- Terselfdertyd word gewaarsku dat sekuriteit 'n groot faktor is vir die sukses van e-handel oor die internet (Olsson *et al.*, 1998:8,14).

- Berman (2002:2-6) sê die volgende:

  "Realities of E-commerce teach costly but valuable lessons." Die realiteit van e-handel is dat e-handel van besigheid-tot-gebruiker nie aan die verwagtinge voldoen het nie. Oponthoude in die aflaai van inligting, onvermoë om pryse en dienste te vergelyk en die frustrasie om goedere wat aanlyn gekoop is, af te haal by die poskantoor, jaag gebruikers terug na winkelsentrums.

- Die sukses van e-handel lê daarin dat dit ordentlik gedoen moet word. Die integrasie van die Web met die bestaande stelsels, voor en agter, is deurslaggewend. Versoenbaarheid van stelsels, die internet as deel van die sake-strategie en die slotsom dat die uitvoerende hoof en nie die inligtingstegnoloog nie, in beheer bly, is belangrik vir die sukses van e-handel (Lawrence, 2000:40).

- Daar word sewe wette vir 'n e-handelstrategie voorgestel, wat soos volg opgesom word:

  Eerstens is dit aaneenlopende beplanning en reaksie van 'n bewegende teiken om sukses. Tweedens kan daar geen geheime wees nie en inligting moet voordelig aangewend word.

  Derdens moet globaal gedink word. Daar moet 'n wisselwerking tussen gebruikers en maatskappye wees.

  Spoed en innovasie is verder belangriker as grootte, en stelsels moet vinnig en geredelik verander kan word. Aanpasbaarheid moet veranderinge kan in ag neem en laastens moet die besigheid rondom die gebruiker gebou word (Oliver:10-12).

- In die "Harvard Business Review" van November/Desember 2000, bevraagteken Richard Wise en David Morrison die toekoms van e-handel in besigheid-tot-besigheid-transaksies.

- E-handel impliseer 'n verskeidenheid sake vir verskillende mense, maar almal stem daarmee saam dat dit tans een van die grootste groeigebiede is. Voorts dat meer

maatskappye as ooit nou besef dat hulle deel van die beweging moet word, anders kan hulle ondergaan (Gibson, 1999:4).

Die wêreld het skielik die "e" ontdek. E-handel, e-sake, e-diens, e-verbruikers, e-enigiets! Maar in Suid-Afrika gaan dit egter nie so goed met e-handel nie. Groei is hoofsaaklik belemmer deur bekommernisse oor die tegnologie en deur verbruikers wat hulle bekommer oor die veiligheid van die internet en die geldigheid van transaksies (Williams, 1999:12).

- Aandag behoort nou gegee te word aan die moontlikhede van e-handel binne en buite die organisasie. Oorweging moet geskenk word aan gekoppelde verkope en bemarking, asook die gekoppelde bestuur van ingewikkelde prosesse, of dit nou tussen ondernemings, of tussen 'n onderneming en 'n klant is.

  Die sleutel tot sukses is volgens Ling (1999:34) om die prosesse te kies wat die meeste voordeel sal trek uit die drastiese herontwerp om aan te pas by die moontlikhede wat die elektroniese omgewing bied. Die internet onderstreep en ondersteun goeie sakebenaderings en behels ook 'n ondersoek na kritieke gebiede en hoe die aanpassing van kernsake-prosesse om by die elektronika aan te pas, werklik 'n verskil kan maak.

- E-handel benodig 'n raadgewende liggaam om gebruikers te beskerm teen oneerlike e-handelstransaksies oor die internet.

  'n Verslag uitgereik deur "Consumers International", 'n federasie van 245 internasionale gebruikersorganisasies, waar ondersoek gedoen is oor aankope aanlyn onderstreep die nodigheid van so 'n liggaam. Hulle bevinding het ingesluit dat baie goedere hulle bestemming laat bereik of glad nie, geen melding gemaak word van afleweringskoste nie, slegs 53% van die maatskappye 'n beleid gehad het oor die terugstuur van goedere, slegs 13% van die terreine aangedui het dat persoonlike inligting nie aan derde partye verkoop sal word nie en dat in twee gevalle, kliënte na vier maande nog steeds op die terugontvangs van geld gewag het na die goedere teruggestuur is. Visa het ook aangedui dat 47% van dispute en bedrog, internet gebaseer was (Firth, 1999:32).

4.2.6 E-besigheid

E-besigheid omsluit e-handel en word soos volg aan die leserspubliek voorgestel:

- Die konsep *e-besigheid* word deur e-handel bevorder. Williams (1998:17) sê e-besigheid sluit die integrasie van alle besigheidsgebeure binne die besigheidsiklus in, van kliëntnavrae tot produkaflewering.

- E-besigheid word soos volg deur Anderson (2000:4) gedefinieer: "For consumers, e-business is about going out, electronically and getting access to the services and products they want. For corporations it's about managing relationships with clients, vendors and customers in the right light of internet."

- Maatskappye beweeg deur die hieropvolgende vier stadiums na e-besigheid:

  Eerstens word 'n webterrein geskep. Daarna ontwikkel 'n groter begrip vir die potensiaal van e-handel. Die derde fase is die investeringsfase en die funksionaliteit van webterreine om e-handel te ondersteun, sodat die integrasie met derde partye vir betaling en sertifisering moontlik gemaak word.

  Terreine word geïntegreer met die maatskappy se hoofstelsels, beide voor en agter. Laastens word daar op die verkryging en die koppel met verskafferkettings gefokus. Broers (:78-84) beklemtoon die volgende nege stappe om vir e-besigheid voor te berei:

  Eerstens moet behoorlike vooraf beplanning plaasvind om te bepaal wat bereik wil word. Daar moet in ag geneem word dat die beginsels van konvensionele besigheid ook ten opsigte van e-besigheid geld.

  Tweedens moet oorweeg word of die besigheidsproposisie lewensvatbaar is. Derdens of dit 'n aanvaarbare alternatief vir die bestaande proses is.

  Bestellingsvervulling en logistieke moet waarde toevoeg vir jou kliënt om koste-effektief te wees. Verseker verder dat die hele maatskappy inkoop in e-besigheid en

dat dit 'n strategiese besluit is. Sesdens, bly realisties in jou verwagtinge. Ondersoek en vind die geskikste tegnologie en kies die beste gebruiklike vennoot en stelsel vir jou onderneming.

Laastens moet die proses voortdurend hersien word en aanpassings gemaak word om aan die voorpunt te bly.

4.2.7 E-onderneming

Die konvergensie van tegnologieë en konvensionele manier van besigheid doen met e-handel en e-besigheid, lei handel na 'n volgende fase, naamlik die era van e-ondernemings.

'n E-onderneming is 'n stelsel wat 'n waardeketting behels, van die verkryging van rou materiaal in die verskaffingsiklus, tot kleinhandelgebruikers en gebruikersbestuur aan die vraagkant. Die volledige stelsel vind plaas deur die tradisionele baksteen-en-sementbates met die effektiwiteit van kuberbemiddeling te kombineer.

Die era van e-besigheid word gekarakteriseer deur inisiatiewe wat fokus op die kernvaardighede van 'n onderneming, waar die besigheidsmodel georiënteer word tot die prosessamevoeging.

Die oorgang van e-handel na e-besigheid en dan na 'n e-onderneming, sluit in die begrip en voorsiening vir die veranderinge wat moet plaasvind in die onderneming ten opsigte van kultuur, mense, besigheidsmodelle, organisatoriese modelle, aanwendingsmodelle, bestuursprosesse en tegnologie (Hoque:28-30).

Bylaag 1 vervat die evolusieproses na 'n e-onderneming.

4.2.8 E-betaling

E-betaling vorm die laaste skakel om die lus van die proses van e-handel en e-besigheid te voltooi. Die e-betalingsrevolusie is die proses van papiertjeks na kredietkaarte, na debietkaarte, na slimkaarte, na elektroniese beurs, na e-tjeks, na mikro-betalings, na elektroniese wissel-aanbieding (Koprewski:22-23).

Suid-Afrikaanse banke het hulle vertroue in die internet behou en poog nog steeds om kliënte na elektroniese kanale, soos die internet en die telefoon oor te skakel, en om daardeur koste te verminder en 'n beter diens te lewer.

Suid-Afrika se klein populasie internetgebruikers en hoë telefoonkoste, verleen hom nie daartoe dat ambisieuse aanlynwaaghalsighede beproef word nie. Terselfdertyd is gebruikers teensinnig om hulle bankgebruike te verander.

Plaaslike banke in byvoorbeeld in die Verenigde State en Europa, volg twee benaderings om in die internet te investeer. Eerstens deur die skep van 'n afsonderlike internethandelsmerk, en tweedens om telefone en takdienste met die internet aan te vul. Hierdeur word gepoog om meer gebruikers te trek, aanlynbankgebruik te stimuleer en transaksiekoste te verlaag (Harris, 2001:92).

4.2.9 Samevatting

Die internet is nie oorspronklik ontwikkel of ontwerp om handel te bedryf nie. Dit het later as 'n natuurlike proses gevolg.

Baie van die voordele van e-handel, die risiko's en kontroles, is reeds tydens EDU aangespreek.

Die debat rondom e-handel is formeel in 1999 begin, gevolg deur 'n groenskrif in 2000 en bekragtiging deur die Wet op Elektroniese Kommunikasie en Transaksies, Wet No. 25 van 2002.

Die sukses van e-handel is nie 'n outomatiese proses nie en die grootste struikelblok is dié van wantroue. Vertroue in die bestel-, ontvangs- en betalingsproses ontbreek nog in 'n groot mate.

In 'n opname onder universiteite en besigheidskole is bepaal dat alhoewel die term e-handel nie uitgedien is nie, dit vervang is deur 'n meer resultaat gedrewe proses, naamlik e-besigheid (Tobin, 2001:24). Hierdie stelling word beaam deurdat 'n nuwe koers ingeslaan word en dat e-handel nou oor sake gaan (e-besigheid) (Horn, 2002:21).

Wat is die beste oorkoepelende term? E-handel, e-besigheid of e-onderneming? E-handel spoel oor in e-besigheid en dan na 'n e-onderneming. Bylaag 1 som hierdie ontwikkelingsproses op.

Die doel van e-handel in 'n onderneming, of dit slegs 'n nuwe verkoopskanaal is of watter groter rol dit ookal speel, sal bepaal hoeveel kapitaal geïnvesteer sal word op 'n webwerf en onderliggende infrastrukture. Om handel elektronies suksesvol te bedryf, moet dit vir enige onderneming deel vorm van hulle strategiese beplanningsproses en die besigheidsplan. Normale sakebeginsels moet nog steeds beoefen word.

HOOFSTUK 5

SEKURITEIT IN ELEKTRONIESE HANDEL

5.1 INLEIDING

Thomas Jefferson het in 1810 gesê: "Money, not morality, is the principal commerce of a civilized nation."

Dit wil dus voorkom dat geld, en nie moraliteit nie, die internet sal dryf. As daar nie behoorlike sekuriteit bestaan nie, sal kriminele dit as 'n geleentheid benut en uitbuit (Ghosh, 1998:preface).

Maatskappye moet dus optree op die gebied van sekuriteit, om e-handel te laat oorleef (De Jong:58).

In "Business IT Africa", Maart 2002, bladsy 4, word die bestaande onderskryf in 'n artikel met die opskrif: "Security concerns hinder e-commerce adoption", en dus bestaan daar geen twyfel nie, dat een van die grootste inhibeerders vir die aanvaarding van e-handel, die vrees rondom sekuriteit is.

Nie net moet die totale konsep van e-handel veilig wees nie, maar tensy die veiligheid van kredietkaarte as 'n betalingsmeganisme oor die internet beveilig is en witboordjie-misdaad verhoed word, sal kliënte ook e-handel teëstaan en die toekoms daarvan benadeel (Ghosh, 1998:2,13,16).

Die begin van die sukses van e-handel, lê dus in die sukses waarmee sekuriteit in e-handel toegepas word om diefstal en bedrog te verhoed.

5.2 AREAS VAN KOMMER

5.2.1 Inleiding

Konvensionele metodes om inligting te beskerm en te beveilig word gekenmerk deur alleenstaande instrumente wat apart werk om 'n sekere deel van die netwerk te beveilig.

Hoe meer maatskappye lewensnoodsaaklike rekenaars intern en aan die internet koppel, hoe meer kwesbaar word die betrokkenes.

Daar is vier kritiese areas waar sagteware by e-handelstransaksies betrokke is en waar sekuriteit van uiterste belang is, naamlik kliënt-sagteware, datatransaksieprotokol, webbedienersagteware en die netwerk-bediener se operasionele sagteware (Ghosh, 1998:3).

Dreigemente en aanslae met betrekking tot die sekuriteit van rekenaarstelsels en konvensionele transaksies kan intern of ekstern van aard wees. Die aanslae kan geklassifiseer word as vandalisme en sabotasie, verbreking van privaatheid en konfidensialiteit, diefstal en bedrog, die oortreding van data-integriteit en die weerhouding van diens (Ghosh, 1998:9,11-21).

Die vier areas van kommer word nou verder bespreek.

5.2.2 Kliëntsekuriteit

5.2.2.1 Die probleem

Die kwesbaarheid van webkliënte-sagteware wat gebruik word om webterreine te snuffel of om kommersiële transaksies uit te voer, kan 'n impak hê op die sekuriteit van 'n organisasie se stelsels. Deurblaaiersagteware en die risiko van lewendige of aktiewe data op die web, is die twee hoofareas van risiko (Ghosh, 1998:22).

Wat eers net 'n statiese uitstalling van inligting op 'n web was, is nou 'n interaksie van uitvoerbare inhoud. Die eens statiese "Hyper Text Markup Language" (HTML)-sagteware, word nou vervang met sagteware wat aktiewe inhoud oorplaas na die gebruiker se rekenaar Sulke programmeringstale is Java, Active X, VB Script, en andere.

Tegnologie bekend as "push" en "pull" word nou in deurblaaiers geïntegreer. Intekenare vir "Microsoft Internet Explorer" en "Netscape Communicator" moet bewus wees van die sekuriteitsrisiko's wat hulle loop.

5.2.2.2 Die oplossing

5.2.2.2.1 Sertifisering

Hierdie risiko kan oorbrug word deur die gebruik van stawingskodes. Dit behels, om aansoek te doen vir 'n sagtewarepublikasiesertifikaat (SPC – "Software Publisher Certificate") van 'n sertifiseringsoutoriteit. Die sagtewarepubliseerder reik 'n publieke en 'n privaat sleutel uit om sagteware te onderteken.

Die privaat sleutel bly geheim vir die publiseerder en die publieke sleutel word met elke sertifikaat uitgereik. Deur gebruik te maak van die publieke en private sleutels, kan 'n digitale handtekening geskep word om die identiteit van 'n ondertekenaar en die integriteit van data te verifieer. Die privaat sleutel word gebruik om wiskundig 'n publieke sleutel te skep.

Die publieke sleutel word bekend gestel met die uitreiking van die sagtewarepublikasiesertifikaat aangesien die privaat sleutel nie ontdek kan word met die publieke sleutel alleen nie.

5.2.2.2.2 Ander kontroles

Addisioneel tot paragraaf 5.2.2.2.1, is sekuriteit ontwikkel deur Java en wat aanvaarbaar in web-aanwendings is.

Java maak gebruik van 'n sekuriteitsmodel, "sandbox". Dié model verhoed dat sagteware buite 'n sekere gebied opereer. 'n Tegniek om sekuriteit mee na te gaan, doen dinamiese toetse terwyl die programme funksies uitvoer om te verhoed dat ongemagtigde take uitgevoer word.

Voorts is dit volgens Ghosh (1998:31-92) noodsaaklik om 'n anti-virusprogram te installeer. Dit sal korrupte lêeraanhegsels wat sonder meer uitgestuur word, neutraliseer.

5.2.3 Datatransaksiesekuriteit

5.2.3.1 Die probleem

'n Protokol is 'n stel formele reëls wat beskryf hoe om data oor 'n netwerk te stuur (vergelyk Hoofstuk 3). Hulle is noodsaaklik vir apparate om inkomende inligting te interpreteer. Daar bestaan verskeie veilige datatransaksieprotokolle. Elke organisasie moet kies watter protokol die beste vir 'n spesifieke behoefte is.

In die besluitnemingsproses moet onder andere die enkodering van data, stawing van kliënte en bedieners, asook die hantering van betaling oorweeg word.

Veilige web gebaseerde kommersiële datatransaksie kan plaasvind deur gebruik te maak van protokolle soos "Secure Sockets Layer" (SSL) en "Secure Hypertext Transfer Protocol" (S-HTTP).

Alhoewel beide hierdie protokolle stawing van beide partye en privaatheid bied tydens transaksies, voorsien dit nie protokolle vir betaling nie.

5.2.3.2 Die oplossing

5.2.3.2.1 Veilige kanale

Die internet protokol (IP) is inherent 'n onveilige kanaal om inligting oor te stuur. Inligting kan onderskep, gelees, vernietig of verander word in die proses.

Die internet is oorspronklik ontwikkel om heterogene platforms te hanteer sodat mense met verskillende rekenaars en operasionele stelsels kan kommunikeer.

Om dit te oorkom, is veiliger protokolle ontwerp wat bo-op die internet sit, soos byvoorbeeld die "Transport Control Protocol" (TCP).

Veilige kanale tussen webkliënte en webbedieners kan verkry word deur die gebruik van SSL en S-HTTP bo-op die TCP/IP.

5.2.3.2.1.1 SSL

SSL is 'n protokol om 'n veilige kanaal te voorsien en is addisioneel tot die IP en TCP. Dit bied veilige kommunikasie, stawing van die bediener en data-integriteit van die boodskappakket of inligting.

SSL voorsien enkodering van die data-oorplasing tussen die webkliënt en die webbediener.

Dit verseker dat die bediener gesertifiseer is deur 'n sertifiseringsoutoriteit en die ooreenstemming van die publieke sleutel met die getekende sertifikaat (vergelyk paragraaf 5.2.2.2.1).

Die stawing van die identiteit van die webbediener kan en moet geverifieer word, deur die sertifikaattoekenning na te gaan op die webbladsy onder die inhoudsopgawe. Let daarop dat SSL nie die sekuriteit van die data wat op die kliënte en bediener sit, beskerm nie. Dit word in paragraaf 5.2.5 van hierdie hoofstuk bespreek.

5.2.3.2.1.2 S-HTTP

S-HTTP volg 'n soortgelyke kanaal as SSL om sekuriteit tydens kommunikasie te voorsien, stawing van die bediener en data-integriteit van die boodskap of pakket-inligting. Dit maak gebruik van enkodering en die gebruik van 'n publieke en privaat sleutel digitale handtekeninge om boodskappe of inligting te enkodeer. Waar SSL die hele internetsessie enkodeer, forseer S-HTTP die beveiligingsprosedure wat ooreengekom is tussen die kliënt en die bediener.

Alhoewel S-HTTP meer buigsaam as SSL is, is dit moeiliker om te konfigureer.

Aangesien SSL vooraf gekonfigureer is, is dit makliker om te gebruik in die meer dominante tegnologie van tans (Ghosh, 1998:101-124).

- Die veilige kanale wat in paragraaf 5.2.3.2.1 bespreek is, voorsien nie kanale vir die oordra van betaling tussen partye vir goedere of dienste gelewer nie. Betalingstelstelkanale gaan verder as om net die kanaal te beskerm.

Waar SSL en S-HTTP bo-op TCP en IP sit, sit die betalingstelselkanale bo-op SSL en S-HTTP.

Die betalingstelselkanale kan ingedeel word onder opgaarrekening-betalingstelsels en opgaarwaarde-betalingstelsels.

5.2.3.2.1.3 Opgaarrekening-betalingstelsels

Elektroniese betalingsmetodes is reeds in Oktober 1994 gevestig toe die eerste internet kommersiële betalingstelsel, "First Virtual Internet Payment System" (FV) geïmplementeer en in gebruik geneem is.

Hierna het ander gevolg. Die drie algemene betalingskanale is FV, "CyberCash's Secure Internet Payment System" (CyberCash) en "Secure Electronic Transaction" (SET).

5.2.3.2.1.3.1 FV

FV maak nie gebruik van kriptologie of 'n beveiligde manier van kommunikasie nie. Dit is gebaseer op e-pos- boodskappe en die eerlikheid van gebruiker, en dien verder as 'n makelaar vir kredietkaarttransaksies tussen gebruikers en handelaars.

5.2.3.2.1.3.2 CyberCash

In teenstelling met FV, maak CyberCash wel van kriptologie gebruik.

Dit voorsien 'n kanaal om kredietkaart-betalingstransaksies oor die internet te fasiliteer en te beskerm.

Vanuit die gebruiker se oogpunt is die voordeel van die CyberCash-kanaal, dat die kredietkaartnommer beskerm is deurdat die nommer geënkodeer word deur CyberCash se publieke sleutel. Dit verhoed dat die handelaar selfs die gebruiker se kredietkaartnommer kan waarneem.

Die magtigingsproses word op die tradisionele manier met die deelnemende bank voltrek.

5.2.3.2.1.3.3 SET

"Secure Electronic Transaction" (SET) is die standaard vir kredietkaartbetalings oor die internet.

Hierdie elektroniese betalingsmetode kan in 'n reële tydsomgewing, of in 'n stoor-en-stuur-aan-manier, soos elektroniese pos, aangewend word.

SET word deur Mastercard en Visa onderskryf en is deur vooraangeskrewe sagtewarehuise ontwikkel, naamlik IBM, Microsoft, Netscape, Verisign, en so meer.

Verder verseker SET sekuriteit ten opsigte van konfidensialiteit, data- integriteit, kliëntestawing en handelaar-stawing.

5.2.3.2.1.4 Opgaarwaarde-betalingstelsels

Elektroniese kontant verwys na 'n opwindende toekoms in die aanvaarding van betaling en word tans met 'n digitale ekwivalent vervang.

Elektroniese kontant word in 'n elektroniese eenheid gestoor. Die eenheid word met kontant gelaai (e-kontant), oorgedra van 'n tradisionele rekening. Transaksies word aflyn of aanlyn gedoen. Aanlyn sal deur 'n bank geskied en is minder privaat as af-lyn.

Om bedrog te voorkom deur ongemagtig toe te voeg tot die gestoorde waarde van die e-kontant, word gebruik gemaak van simmetriese sleutels, publieke-sleutel-enkripsie (PKE) en asimmetriese enkripsie.

'n Bekende vorm van e-kontant is vandag "e-bucks" van FNB (Ghosh, 1998:124-147).

5.2.3.2.2 Slimkaarte

Daar word vandag al meer voorspel dat die toekoms van elektroniese transaksiebetalings deur middel van slimkaarte ("Smart Cards") sal geskied. Slimkaarte word tans aangewend in onder andere vooraf betaalde telefoonkaarte en dobbelhuise.

Soos beskryf in paragraaf 5.2.3.2.1.4, kan die eenheid vir die stoor van e-kontant, slimkaarte wees (Ghosh, 1998:147-154).

5.2.4 Webbedienersekuriteit

5.2.4.1 Die probleem

Waarom bekommerd wees oor die sekuriteit van die webbediener? Die sekuriteit van 'n stelsel is net so sterk as die swakste skakel daarvan.

Die webbediener het drie hoofkomponente wat die handelsbediener van die internet opmaak, naamlik voorkantbedienersagteware, die agterkantdatabasis en die integrasie-sagteware.

Data kan beskadig of vernietig word. Die bediener kan tot stilstand gebring word, wat verantwoordelik sal wees vir die tot stilstand kom van dienslewering. Die installering en uitleg van die verdedigingstelsel deur onder andere brandmure, toegangsbeheer deur gebruik te maak van wagwoorde en stawingsmeganismes, is van uiterste belang.

5.2.4.2 Die oplossing

5.2.4.2.1 Webbedienersekuriteit

Die voorkantbedienersagteware het verskeie funksies. 'n Balans tussen sekuriteit en funksionaliteit moet bereik word. Dit word gedoen in 'n sekuriteitsbeleidsdokument wat die besigheids-, sowel as die sekuriteitsvereistes neerlê.

5.2.4.2.1.1 Installasie

Die stelseladministrateur is verantwoordelik vir die installasie van die web-bediener en word die eienaar van die lêers en die toegangsvlakke. Lêer-toegang moet spesifiek verhoed word met die konfigurasie.

5.2.4.2.1.2 Lêertoegang

Toestemming tot lêertoegang spesifiseer wie 'n lêer kan lees, skryf of voltrek.

Dit is een vorm van voorbehoud dat ongemagtigde interne gebruikers toegang verkry tot bedienerkonfigurasie-lêers, dokumentasielêers en konfidensiële kliëntelêers.

Gebruikers buite die webbedieners behoort nie lees- of skryftoegang te hê tot enige ondersteunende lêers nie, maar slegs tot web geaktiveerde lêers.

5.2.4.2.1.3 Vlakke van kliëntprivilege

Foutiewe konfigurasie kan tot gevolg hê dat vlakke van privilege geënkodeer kan word. Dit sal tot gevolg hê dat ongemagtigde gebruikers van spesifieke vlakke, op hoër vlakke lêers kan skep, verander of vernietig.

Die konfigurasie van toegangsvlakke moet noukeurig en met versigtigheid bewerkstellig word.

5.2.4.2.1.4 Konfigurasie

Die konfigurasie van die bediener moet volgens 'n nougesette sekuriteitsbeleid geskied om 'n veilige webterrein daar te stel.

5.2.4.2.1.5 Toegangsbeheer

Normaalweg vind toegangsbeheer deur drie beheermeganismes plaas.

5.2.4.2.1.5.1 Kliëntgasheernaam en internetprotokoladresbeperkings

Een van die mees basiese beheermeganismes is om die toegang tot die webbladsye te beperk, baseer op die kliëntgasheernaam of internetprotokoladres. Slegs gemagtigde kliënte mag webblaaie of die totale web besoek, indien hulle vooraf gemagtig is en die gasheernaam en die internetprotokoladres ooreenstem.

5.2.4.2.1.5.2 Gebruiker- en wagwoordstawing

Dit behels dat 'n kliënt 'n gebruikersidentiteit en wagwoord besit wat op 'n toegangsbeheerlys (ACL – "Access Control List") geplaas word, en nagegaan word alvorens toegang verleen word.

Wagwoorde word gewoonlik geënkodeer en kan óf sentraal óf op 'n distribusiebasis beheer word.

5.2.4.2.1.5.3 Stawing deur middel van digitale sertifikate

Ten einde veiliger vlakke van toegang daar te stel, kan digitale sertifikate en simmetriese enkodering gebruik word om beide partye te verifieer.

Hierdie begrip is reeds in paragraaf 5.2.3.2 bespreek.

5.2.4.2.2 Algemenepoort-koppelvlakskrif

Algemenepoort-koppelvlakskrif ("Common Gate-way Interface Script") behels daardie koppelvlaksagteware wat op die webbediener ingevoer word in reaksie op webaansoeke. Dit word soms ook gebruik om agterkantdatabasisse aan te vul.

Aangesien hierdie koppelvlaksagteware maklik binnegedring kan word, is die oorspronklike opstel daarvan met goed ontwerpte sekuriteitsbeginsels belangrik.

Voorts moet behoorlike gekonfigureerde gidse, vanwaar algemenepoort-koppelvlakskrif-programme uitgevoer kan word, daargestel word.

5.2.4.2.3 Databasis-aantasbaarheid

Databasisse is noodsaaklik vir webhandelsaanwending en om gebruikers te staaf alvorens toegang tot webbladsye gegee word.

Databasisse word gewoonlik deur skermmure geplaas vir die sekuriteit daarvan, en toegang daartoe moet behoorlik beheer word. Wagwoorde behoort gekripteer te word. Indien behoorlik aangewend, sal dit langtermynsekuriteit verleen. Weereens is die sukses hiervan geleë in die toegangsbeheerlyste en wagwoorde.

5.2.4.2.4 Ontwerp van veiliger sagteware

Die ontwerp en implementering van tegnieke in sagteware om sekuriteitsdeurbrake te verhoed of minimaliseer, is addisioneel tot voldoende sekuriteit.

Verder moet analitiese metodes toegepas word om die bestaan van gevaarlike strukture en gedrag te bespeur.

5.2.4.2.5 Analisering van sekuriteitsagteware

Die meeste sagtewareprogrammeerders, programmeer volgens spesifikasies van wat verwag word dat 'n program sal doen, in plaas daarvan om te konsentreer op wat die sagteware nie moet doen of toelaat nie.

Sagteware behoort dus getoets te word om seker te maak dat dit voldoen aan funksionaliteit en tweedens om seker te maak dat dit nie onreëlmatig op onverwagte insette sal reageer nie (Ghosh, 1998:157-202).

5.2.5 Operasionelestelselsekuriteit

5.2.5.1 Die probleem

Tot so onlangs as 1990 is tafelbladrekenaars as alleenstaande eenhede gesien.

Netwerke het hierdie situasie egter verander en groter kollektiewe krag en inhoud geskep.

Die internet is nooit ontwerp om betroubaar of veilig te wees nie, maar sekuriteit het later essensieel geword met die koms van kommersiële transaksies en die oordra van vertroulike inligting. Kriptografiese protokolle is ontwerp om bo-op TCP/IP-protokolle te sit, om sodoende veilige kommunikasie te bewerkstellig. Dit beveilig egter nie rekenaars wat aan die internet gekoppel word nie.

Die operasionele stelsel is die fondament van enige sagteware wat op 'n masjien werk. Breuke in die operasionelestelselsagteware, kan die sekuriteit verswak. Die konfigurasie van die operasionelestelselsagteware en brandmure is van kardinale belang.

5.2.5.2 Die oplossing

Indien die onveilige en kwesbare areas bekend is, kan verbeterde en addisionele maatstawwe geïmplementeer word om 'n veilige omgewing te skep.

5.2.5.2.1 Brandmure

Brandmure is die eerste linie van verdediging teen ongemagtigde en soms kwaadwillige gebruikers. Dit word geplaas tussen die rekenaarnetwerk wat beskerm moet word, en die netwerk wat onder sekuriteitsbedreiging is. Dit kan egter ook gebruik word tussen interne netwerke vir afskermings-, afsonderings- en toegangsbeheerdoeleindes.

Indien dit behoorlik gekonfigureer is, kan brandmure die meeste ongemagtigde en kwaadwillige aanvalle voorkom.

Brandmure is 'n kombinasie van roteerders en rekenaars wat programme uitvoer om netwerkaansoeke te stoor en aan te stuur volgens die evaluering van 'n stel reëls.

Weereens is dit belangrik dat 'n beveiligheidsbeleid ontwikkel en gedokumenteer word om uitvoering te gee aan die behoorlike konfigurasie van brandmure.

5.2.5.2.2 Netwerkbedieners

Daar is sewe kategorieë waar netwerkbedieners kwesbaar mag wees. Hierdie kategorieë word vervolgens bespreek.

5.2.5.2.2.1 Fatale gebreke ("Deadly Defaults")

Dit verwys na daardie opstel van sagteware of stelselkonfigurasies wat onveilig is en die stelsel oop laat vir binnedringing.

Dit is nodig dat behoorlike konfigurasie van sagteware en stelsels plaasvind, toegangsbeheer volledig gedokumenteer en toegepas word, asook die stawing van gebruikers ten alle tye uitgevoer word.

5.2.5.2.2.2 Foute in die webbediener

Die webbediener is die voorkantsagteware en alhoewel dit met brandmure beskerm kan word, kan dit aangeval word aangesien toegang as gevolg van geldige dienste verkry word.

Weereens kan dit verhoed word deur behoorlike gekonfigureerde dienste en die laai van die nuutste sagtewareweergawe.

5.2.5.2.2.3 Foute in CGI-skrif

Algemenepoort-koppelvlakskrif voorsien die sagteware wat op die webbediener uitgevoer word in reaksie op webaansoeke.

Aangesien hierdie aanwendings uitgevoer word op die bediener en insette van gemagtigde of kwaadwillige gebruikers kry, kan dit ernstige sekuriteitsrisiko's veroorsaak, tensy dit noukeurig geïnstalleer is.

Dit is belangrik om die CGI-skrif te oudit en beheer oor die inhoud van die CGI uitvoerbare voorskrifte uit te oefen.

Sagteware soos Tripwire kan ook aangewend word om kontroletotale te skep van die uitvoerbare beelde van elke CGI-program. Hierdie kontroletotale moet periodiek nagegaan word om te verseker dat CGI-skrif nie mee gepeuter is nie.

5.2.5.2.2.4 Netwerksagteware-onveiligheid

Netwerksagteware ondersteun netwerkdienste wat naby verwant is aan die operasionele stelsels van die masjiene wat onderling verbind is en word soms netwerkoperasionelestelsels genoem.

Die veiligheid van dié stelsels word onder meer vervat in die gehalte van wagwoordtoepassing, die stawingsproses, die gebruik van identifikasienommers en korrekte internetadresse.

Die korrekte implementering en gebruik van sagteware en sekuriteitstelsels is van kardinale belang.

5.2.5.2.2.5 Weiering van diens

Aanvalle waarin diens geweier word, is 'n tipiese poging om netwerkbedieners tot stilstand te bring en toegang tot die internet te stop. Dit is belangrik om die verskillende

maniere en metodes van hierdie aanvalle te ken, om sodoende toenemend die sekuriteitstelsel te verbeter en aan te pas.

5.2.5.2.2.6 Onvoldoende stawing

Een van die swak skakels in enige rekenaarsekuriteitstelsel, is die stawing van gebruikers. Stawing word gebruik om te verifieer dat gebruikers toegang mag hê tot rekenaarbronne. Die aanbieding van beide identifikasie en wagwoorde, verhoog die sekuriteit.

Die databasis hiervan moet streng bewaar word en periodiek geoudit word om ongemagtigde toegang na te gaan en die toegangsreëls te toets vir die beskerming wat dit bied.

Om stawing veiliger of doeltreffender te maak, sal die uitreik van publieke/privaatsleutelpare deur gebruikers toegepas moet word.

Voorts sal biometriese toestelle in die toekoms, persone aan unieke eienskappe kan eien, byvoorbeeld duimafdrukke, en daardeur stawing verder beveilig.

5.2.5.2.2.7 Operasionelestelselgebreke

'n Reeks sagteware, stelselsagteware, voorsien dienste aan die operasionele stelsel. Ongemagtigde gebruikers kan die operasionele stelsel binnedring deur swak beveiligde areas aan te val. Behoorlike gekonfigureerde brandmure kan dit egter verhoed. Daar is egter twee tipe aanvalle waaraan aandag gegee moet word.

Eerstens verwys bufferoorvloei na foute wat ontstaan as die hoeveelheid datatoevoer nie nagegaan word, alvorens dit geskryf word op 'n vaste hoeveelheid (lengte) buffer nie. As die geheue te klein is, spoel data oor, wat korrup mag word deur ongemagtigde persone, ("Hackers") wat skade wil aanbring.

Dit is noodsaaklik dat sekuriteit om bufferoorvloei te verhoed, voortdurend nagegaan en vernuwe moet word.

Tweedens moet stelselregistrasie, naamlik dit wat die stelselkonfigurasie-inligting vir die uitvoerbaarheid van programme hou, beskerm word. Indien nie, kan dit tot ongemagtigde toegang, korrupsie en die faling van die totale stelsel lei.

Sekuriteit vir die aflaai en die uitvoering van programme moet versigtig en volgens veilige metodes plaasvind.

Die beveiliging van die netwerk se operasionelestelselsagteware is krities in die beveiliging en sekuriteit van e-handel. 'n Sekuriteitsprogram om gereeld stelselregisters en die brandmuurregister te monitor, is kardinaal daartoe (Ghosh, 1998:205-249).

5.3 INFORMASIESEKURITEITSBELEID

'n Beleidsdokument rondom die sekuriteit van informasie (inligting) is noodsaaklik om 'n organisasie se belegging in rekenaarinligtingstelsels en netwerke te beskerm, die inligting wat daarin vervat is te beskerm, om besigheids- en wetlike risiko's te beskerm en te verhoed, en laastens, om die reputasie en goeie naam van die organisasie te beskerm.

Enige afwykings van so 'n beleidsdokument behoort tot dissiplinêre aksie te lei met swaar strawwe. Hoe moet so 'n dokument daaruit sien?

5.3.1 Inligtingsekuriteitsbeleid

Die dokument wat die inligtingsekuriteitsbeleid vervat, behoort aan die volgende aspekte aandag te gee:

- Administratiewe verantwoordelikheid van die beleid.
- Inhoudsopgawe van areas waaraan aandag gegee moet word, is:
- Verklaring van verantwoordelikheid:
- Bestuurders en oorsieners se verantwoordelikheid.
- Inligtingsbestuurder se verantwoordelikheid.

- Die internet en e-pos:
- Beleid ten opsigte van internet- en e-posbenutting.
- Aanvaarbare gebruikskodes.
- Onaanvaarbare gebruike.
- Aflaai van lêers.
- Werknemersverantwoordelikheid.
- Kopieregte.
- Monitering van inligting.
- Rekenaarvirusse:
- Voorkoming en verdediging.
- Inligtingsbestuurder se verantwoordelikheid.
- Werknemer se verantwoordelikheid.
- Toegangskodes en wagwoorde:
- Inligtingsbestuurder se verantwoordelikheid.
- Werknemer se verantwoordelikheid.
- Oorsiener se verantwoordelikheid.
- Mensebronne-afdeling se verantwoordelikheid.
- Fisiese sekuriteit:
- Werknemer se verantwoordelikheid.
- Inligtingsafdeling se verantwoordelikheid.

- Kopieregte en lisensie-ooreenkomste:
- Organisasie- en werknemersverbintenisse.
- Eienaarskap.
- Inligtingsafdeling se verantwoordelikheid.
- Werknemers se verantwoordelikheid.
- Siviele optrede.
- Kriminele optrede.

5.3.2 Aanvaarding

'n Vorm vir ondertekening deur elke werknemer vir die erkenning en aanvaarding van die inligtingsekuriteitsbeleidsdokument behoort uitgereik te word. So 'n handeling sal die erns waarmee die werkgewer sekuriteit bejeën, benadruk en die werknemer bedag maak op die gevolge van die nievoldoening aan so 'n beleid (Dumas, 1998:1-8).

5.4 ONTWIKKELING IN E-HANDELSEKURITEIT

Die voorafgaande deel van hierdie hoofstuk het klem gelê op die gebiede van sekuriteit binne die e-handelmilieu. Ghosh het sy boek, "E-Commerce Security weak links, best defenses", oor sekuriteit in e-handel in 1998 vrygestel. Met hoe 'n groot mate van erns is sekuriteit in e-handel aanvaar?

Hierna volg verskeie uittreksels van artikels en skrywes wat sedert 1998 tot 2001 in hierdie verband verskyn het. In 2002 en 2003 het geen nuwe e-sekuriteit beginsels verskyn nie en bestaandes is aangepas of versterk.

5.4.1 1998

- Smith (1997:1) skryf dat daar beweer word dat kriptologie die enigste alternatief is om internetdata te beveilig en dat data wat van een rekenaar na 'n ander beweeg, die versekering van 'n beveiligde fisiese omgewing verlaat. Kriptologie herformeer

en transformeer data om dit veiliger te maak tydens die vloei daarvan. Dit verseker die konfidensialiteit, asook die stawing en integriteit van data.

- Inligtingsekuriteit moet geïnkorporeer word in 'n organisasie se prosedures en beleid, en formeel gedokumenteer en na omgesien word (Harcourt-Cooke *et al.*, 1998:4-5).

  In netwerksekuriteit sal organisasies in ag moet neem dat hoë standaarde van sekuriteit gehandhaaf moet word om immuun, voorbereid en beskermd te wees.

  Indiepte-verdediging, rondom-verdediging, datavloei-verdediging deur onder meer gebruik te maak van brandmure en enkodering, is noodsaaklik.

  Dit is belangrik dat aandag gegee moet word aan integriteit, kontinuïteit, konfidensialiteit en die identifikasie van inligting (Germishuys, 1998:7).

- Wêreldwyd koppel organisasies hulle netwerke aan die internet, skep intranette en ekstranette om inligting heen en weer te stuur en stel hulle bloot aan gevare soos krakers, virusse, ongemagtigde toegang, verbreking van konfidensialiteit, asook die steel en sabotasie van inligting.

  Om beskerming te verleen en veiligheid daar te stel, is toegangsbeheer tot inligting noodsaaklik, konfidensialiteit moet verseker word, identifikasie moet gevra word en inligting moet beskerm word. Dit kan gedoen word deur die instel van onder meer anti-virusse, enkripsie, privaat netwerke, wagwoorde, digitale sertifikate en slimkaarte (Katz, 1998:6).

- In die "Computerweek" van 28 September 1998, bladsy 3, word verwys na SET, en dat die SET-protokolle vier pilare het, naamlik konfidensialiteit van inligting, integriteit van inligting, stawing van partye en geldigheid van transaksies.

  Die bevordering van SET deur banke sal die vertroue by gebruikers skep dat transaksies veilig sal kan plaasvind. Enkripsie, digitale handtekeninge, fisiese sleutels, kriptologie, SSL, en so meer, bied voldoende sekuriteit en skep daardeur vertroue by gebruikers (Apteker,1998:27).

SET bied sekuriteit ten koste van eenvoud, deurdat dit kompleks en duur is, maar dat dit goed werk (Essilk, 1998:8-9).

- In 'n spesiale bylae van die "Finansies en Tegniek" van 9 Oktober 1998, in 'n opskrif: "Veiligheid moet voorrang geniet", sonder deelnemers aan 'n opname oor e-handel dit uit, dat sekuriteit een van die grootste bekommernisse is.

  Brandmure, digitale sertifikate en veilige koppelvlakke word algemeen gebruik om sekuriteit te bevorder.

- Slimkaarte bied 'n geweldige veilige en gerieflike oplossing vir gebruikers wat wil gebruik maak van wêreldwye handel in 'n virtuele mark oor die internet. Dit vervat persoonlike identifikasie, digitale sertifikate, kriptografie en kan ook by SSL of SET gevoeg word om die hoogste moontlike vlak van gekoppelde veiligheid tydens transaksies te verskaf (Venter, 1998:14).

- Digitale sertifikate mag enkripsie vervang, maar daar is nog steeds vyf hoofareas van sekuriteit, naamlik privaatheid, magtigingsproses, deursigtigheid, integriteit en beskikbaarheid, waaraan aandag gegee moet word (Davis, 1998:54).

- Daar is vier elemente van sekuriteit waaraan aandag gegee moet word, naamlik die stawing van masjiene en gebruikers, magtiging van toegangsbeheer deur middel van brandmure, privaatheid van inligting (data) deur enkripsie, en data-integriteit. Die volgende stelling van Hembrough (1997:15) is egter belangrik: "Security is a living, breathing thing and needs to be treated as such."

- Sekuriteit is volgens Lopez (1998:18) seker die grootste en mees komplekse area waarmee organisasies voorkom in die ontplooiing en ontwikkeling van netwerke en uitwaartse kommunikasie te doen kry. Die ontwikkeling van 'n sekuriteitsbeleid is daarom noodsaaklik en moet onder meer die fisiese sekuriteit van die netwerk, toegangsbeheer, inligtingsbeskerming en transaksiesekuriteit bevat.

- Tagtig persent van alle sekuriteitsbreuke vind intern plaas. Dit is dus noodsaaklik dat organisasies addisioneel tot brandmure, die jongste opsporingsmeganismes installeer om netwerke teen interne aanvalle te beskerm (Azbel, 1998:22).

- Elke e-handel-inisiatief is uniek en benodig eiesoortige vlakke van sekuriteit. Behoorlike beveiliging benodig volgens Quartero (1998:26) meer as net die installasie van brandmure en virusbeveiligingsagteware.

- Die beheer van inligting is nog altyd van kardinale belang in besighede. Datasekuriteit en enkripsie gaan oor die beheer van inligting, wie dit mag lees, verander, waar en van wie dit kom, en waar en hoe dit verander is. MacGregor (1998:27) wys daarop dat meer nadruk op die grootdatastoorstelsel geplaas moet word en gemagtigde toegang slegs deur digitale handtekeninge (digitale sertifikate) behoort te geskied. Spesialiste moet sekuriteitstelsels implementeer en dokumenteer.

- Digitale identifikasie of digitale sertifikate bepaal volgens Venter (1998:28) die graad van vertroue wat nodig is om e-handel te laat slaag. Die moontlikheid om konfidensialiteit en die stawing van gebruikersidentiteit te waarborg, is fundamenteel in veilige elektroniese kommunikasie en elektroniese handel.

5.4.2 1999

"Koop veilig op die Internet", 'n artikel wat in die "Huisgenoot" van 25 Februarie 1999 verskyn, verwys na digitale sertifikate en stel voor dat 'n gebruiker op die volgende let:

- Gebruik 'n veilige blaaier en webterrein.
- Wees versigtig met wie jy sake doen.
- Stel vas of die terrein betroubaar is.
- Vind uit of daar 'n verklaring is van privaatheid.
- Gee slegs die nodigste besonderhede.
- Verander wagwoorde van tyd tot tyd.
- Vind uit hoe lank aflewering sal neem.
- Dring aan op jou regte asof dit 'n gewone transaksie is.

- Vee jou spore dood.

Die toename in rekenaar aangewese geweld oor die afgelope twee jaar, vestig die aandag daarop dat alle persone wat in e-handel bedrywig is, al hoe meer effektiewe maniere moet vind om hulle informasietegnologie-infrastrukture veiliger te maak (Levenstein, 1999:36).

Alhoewel gebruikers dit gerieflik mag vind om besigheid oor die internet te doen (e-handel), is die veiligheid van transaksies en die privaatheid van persoonlike inligting 'n groot bekommernis. 'n Gebrek aan sekuriteit is 'n groot struikelblok vir die internet (Venter, 1999:36).

Parkes (1999:58) wys daarop dat brandmure (skutmure) voorgestel word as 'n allesomvattende beskermingsmeganisme wat aanvalle op wye-area-netwerke opspoor, dit verhinder en rapporteer. Dit het drie primêre funksies, naamlik dat dit data-pakkette filtreer op grond van die netwerkadresinligting, dit dien as die gevolmagtigde om interne adviesskemas te versluier en dit bied toepassings-intelligensie.

Enkripsie, stawing gegrond op wagwoorde, brandmure en digitale sertifikate is belangrik in die proses om 'n beskermende stelsel te hê.

Risiko's bestaan rondom die sekuriteit van netwerke en verskillende menings word gehandhaaf oor die beste vorm van sekuriteit. Volgens Herdan (1998:5) is daar egter tien tipes sekuriteit wat toegepas behoort te word naamlik:

- Wagwoordstawing.
- Brandmure.
- Data-enkripsie.
- Veilige e-pos.
- Veilige soklaagbedieners (SSL).
- Digitale sertifikate.

- Digitale handtekeninge.
- Veilige elektroniese transaksies (SET).
- Veilige boodskap.
- Slimkaartstawing.

Verskeie struikelblokke bestaan vir e-handel. Brewer (1998:9) noem tien sodanige struikelblokke, naamlik:

- Aanspreeklikheid.
- Verskille in internasionale regsaspekte en regulasies.
- Vrees vir die internet.
- 'n Tekort aan bestuursondersteuning.
- 'n Tekort aan operasionele samewerking tussen gebruikers.
- Koste/Voordeel-analise.
- 'n Tekort aan vertroue in e-handel.
- 'n Tekort aan onderhoudingsteun.
- Tegnologiese agterstand.
- Sekuriteitsbekommernisse.

'n Totale besigheidsoplossing is dus nodig, die integrasie van besigheidsprosesse en 'n inligtingstegnologie-infrastruktuur.

Baie organisasies neem nie sekuriteitsdreigemente ernstig op nie. Dit is voordelig dat verskillende sekuriteitspakkette getoets moet word om die regte kombinasie vir 'n bepaalde organisasie te vind. 'n Ander alternatief is om die sekuriteitsaspekte aan 'n bron buite die organisasie toe te vertrou (Bennett *et al.*, 1999:16).

Korporatiewe spioenasie, kwaadwillige kerwery en kredietkaart-bedrog kan volgens Venter (1999:28) opgelos word deur gebruik te maak van digitale sekuriteit vir die internet en e-handel.

5.4.3 2000

Coelho (2000:2-3) sê dat daar twee hoofareas is waarteen gewaak moet word ten opsigte van aanspreeklikheid, naamlik:

Aanspreeklikheid teenoor kliënte en derde partye:

- As jy nie langer diens kan lewer oor die internet nie.
- As jy foutiewe sagteware ontwikkel en aanbied.
- As jy foutiewe produkte lewer.
- As daar foutiewe inligting op jou webterrein is.
- As jy die oorsaak daarvan is om 'n virus uit te stuur.
- As 'n kraker jou kliënt se inligting binnedring.
- As jy intellektuele eiendom benadeel.
- As jou webterrein besmet word met afbrekende inligting.

Aanspreeklikheid deur jouself gely:

- Onvermoë om handel te doen as gevolg van 'n stelselstilstand.
- As jy foutiewe sagteware ontwikkel en lewer.
- Produkaanspreeklikheid. Leweransier kan nie lewer nie.
- Valse inligting deur voornemende kliënte. Verlies van kontantvloei.
- Kraker manipuleer stelsels.

- Herstel van jou publieke aansien.

Du Toit (2000:1) verwys na verskeie risiko-areas wat in e-handel en risikobestuur bestaan, naamlik:

- Virusse.
- Diefstal.
- Aftakeling van data.
- Ongemagtigde gebruik van data.
- Afbrekende inligting (laster).
- Inligtingstegnologie-oorspoeling (skending).
- Privaatheidskendings.
- Stawing.
- Reputasieskending.
- Kliëntprivaatheid.
- Kopiereg- en handelsmerkskendings.
- Onafhanklikheidsrisiko.
- Toepaslikheid van data (ouderdomsanalise).
- Diskriminasie.
- Handel met die buiteland:

  Hier word spesifiek na belasting, regsaanspreeklikheid, omgewingsake en lisensie-ooreenkomste verwys.

- Besigheidsonderbreking (24/7/365).

- Veiligheidsmaatreëls om jou teen kredietkaartdiefstal te beskerm, sluit volgens Venter (2000:36) in om jou rekenaar met 'n wagwoord te beskerm, die wagwoord geheim te hou, om nie roofprogrammatuur te gebruik nie, om nie jou e-posadres te gebruik om vorms op die internet in te vul nie, om 'n veilige snuffelaar te gebruik en om ten minste SSL-beskerming te hê.

- Internetsekuriteit is 'n besigheidsprobleem. Dit is net nog 'n koöperatiewe bedreiging en moet hanteer word binne die besigheidsrisiko-model.

- Schneier (2000:1-6) wys in hierdie verband daarop dat eerstens aanvaar moet word dat dit 'n risiko is wat aanvaar word as 'n koste om besigheid te doen. Tweedens, dat sommige risiko's wel deur tegniese en/of prosedurele metodes verminder kan word, en laastens dat sekere risiko's deur kontrakte of versekering oorgedra kan word.

- Al manier om voor te bly, is deur opsporing en reaksie op kwesbaarheid. Die versigte aanwending van tegnologie om koste-effektief die risiko te verminder, is die regte bestuurstegnologie. Sekuriteit is 'n proses, nie 'n produk nie.

- In die "F & T NET", Vol. 5 No. 5, word poorte ("portals") voorgestel as 'n beter middel vanuit 'n sekuriteitsoogpunt, aangesien dit sterk bemagtigingsmetodes, 'n standvastige beleid, toegangsbeheer, monitering en ouditering moontlik maak.

- E-handel sal slegs oorleef as organisasies optree op die gebied van sekuriteit en anti-virusbeskerming.

- Dit sluit intellektuele eiendom, korrupte data, verlies aan produktiwiteit en regsaanspreeklikheid in.

- 'n Sekuriteitstrategie behels volgens (De Jong:58) 'n gesentraliseerde benadering.

- Sekuriteit is 'n integrale deel van 'n e-besigheidstrategie en verwys na beide die makro- sowel as mikro-markte. Hierby is die breë gemeenskap en infrastruktuurvoorsieners, sowel as individuele organisasies betrokke (Higgins, 2000).

5.4.4 2001

Fabro (2001:3) skryf dat vertrouelinge, werknemers, kliënte en besigheidsvennote soms meer sekuriteitsbreuke veroorsaak, as buitepersone. E-sekuriteit behoort as die ekstensie van 'n bestaande bestuurstrategie betreffende besigheidsrisiko te dien.

Sekuriteit is 'n dinamiese proses, 'n aanhoudende tog wat gedurig verander soos die omgewing verander.

E-sekuriteit help 'n besigheid om sy risiko te bestuur. Dit benodig e-sekuriteitsbeleid, onderrig en tegnologiese kennis. Om effektief te wees, moet sekuriteit 'n platform skep wat uitstrek na alle bedieners, kliënte, netwerke, gebruikers, aanwendings en toegangspoorte. Dit moet ten volle geïntegreerd wees en sentraal beheer word.

In die "Fortune" se spesiale advertensieafdeling oor e-sekuriteit, 9 Julie 2001, No. 15, word e-besigheidsaanwendings gesien as 'n manier om onbekende gebruikers op korporatiewe webterreine toe te laat.

Krakers en kuberkriminele val al hoe meer stelsels aan oor motiewe soos eie gewin, asook politieke redes of vir gewone pret.

E-sekuriteit moet 'n balans handhaaf tussen die koste en die verontriefting van sterk sekuriteitsprosedures, in vergelyking met die hoeveelheid beskerming wat gebied word.

'n Addisionele manier om die internet veilig en beheerbaar te maak, is deur virtuele privaat netwerk (VPN's).

Alle kommunikasie word deur 'n "tonnel" gelei en geïntegreer met die organisasie se netwerksekuriteit, waar VPN's bydra om 'n koste-doeltreffende internet te skep. Dit is egter belangrik dat 'n behoorlik geïntegreerde sekuriteit-infrastruktuur daargestel word.

'n Allesomvattende e-sekuriteitstrategie moet onder andere identiteit, bewyslas, toegang, transaksiekonfidensialiteit en boodskap integriteit aanspreek.

Slimkaarte bied privaat beskermde oplossings, met sekuriteits-sagteware vir e-vertroue wat help om 'n besigheid te verdedig teen aanvalle van buite.

Sekuriteit strek verder as 'n brandmuur. Green (2001:8) beskou sekuriteit as 'n strategiese besluit en sê dit moet in alle e-besigheidstelsels en aanwendings geïntegreer word. Die besigheid, nie die netwerk nie, moet beveilig word.

In die "Business IT Africa" van Maart 2001, Vol. 1 No. 1, word in 'n artikel "Security and Resources", daarna verwys dat die openheid van die internet vra na gedurige aandag rondom die sekuriteit van gekoppelde netwerke.

Die koste van virusse, elektroniese diefstal en die weerhouding van diens is te ernstig om te ignoreer. Hoe meer die internet groei, ontwikkel ongemagtigde aanvalle. Sekuriteitsmiddele soos onder meer brandmure, stawing, toegangsbeheer, aanspreeklikheidsooreenkomste met derde partye en data-enkripsie op sigself is nie voldoende nie, alhoewel dit die risiko's verminder.

Korporatiewe beleidsbepaling en die dokumentasie en toepassing daarvan, is net so belangrik. Daar moet gedurig nagegaan word wát beveilig moet word en hóé. Die Gartner-groep beveel aan dat organisasies vier stappe moet oorweeg om netwerksekuriteit te versterk, naamlik om die sekuriteitstelsel gedurig na te gaan, te sorg dat die konfigurasie van die brandmure behoorlik funksioneer, om gedurig inkomende e-pos te skandeer vir virusse en om gebruik te maak van streng stawingsprosedures.

'n Geïntegreerde sekuriteit-infrastruktuur en sentrale beheer word deur Hurley (2001:56) as noodsaaklik beskou om hedendaags doeltreffende sekuriteit in elektroniese handel (e-handel) te bied.

Volgens Burgers (2001:52) word sekuriteit verhoog met die aanvaarding van data-enkripsie en die gebruik van wagwoorde. Dit beteken egter nie dat stawing en magtiging, konfidensialiteit en enkripsie asook verantwoordelikheid en ouditering gevolglik geskend moet word nie.

Daar bestaan 'n onvermoë om die stawing van die identiteit van partye wat betrokke is by besigheid-tot-besigheid (B2B) te laat geskied in hoëwaardetransaksies. Die risiko lê daarin dat metodes by laewaardetransaksies, naamlik besigheid-tot-gebruiker (B2C),

gebruik word in hoëwaardetransaksies. Sekuriteit moet hier versterk word (Green, 2001:20).

Green (2001:21) skryf in sy artikel, "Hoe versterk ons die sekuriteit?", dat die stawing van die deelnemers in 'n B2B-transaksie moet plaasvind by die punt van ingang, in teenstelling met dié van B2C, wat by die betalingspunt plaasvind.

Slimkaarte is kaarte wat magnetiese streepkaarte vervang, met 'n klein rekenaarskyfie daarop ("chip"), wat dit self teen aanvalle kan beskerm en inligting self kan prosesseer. Dit maak gebruik van enkripsie en versteekte sleutels op die skyfie en op die terminaal. Die kaart staaf die terminaal en die terminaal die kaart.

Slimkaarte gebruik data-enkripsiestandaarde (DES) en opereer privaat en publieke sleutels (Sion:12-14).

Volgens Crook (:28) is daar tien goue reëls vir netwerksekuriteit, naamlik:

- Organisasies moet 'n volledige sekuriteitsbeleid ontwikkel en implementeer.
- Instel van sekuriteitsdienste, soos byvoorbeeld stawing, enkripsie, brandmuur, skanderingsmiddele, veilige inskakel-toestelle en virus-opspoorders.
- Skep van wagwoorde en die stawing wat maklike toegang sal elimineer.
- Implementering van die opsporing van reële-tyd-indringing.
- Monitering en evaluasie van logregisters.
- Data-berging en -storing in buiteplekke.
- Plan van optrede sou aanvalle plaasvind en sekuriteit binnegedring word.
- Sekuriteitoudits uitvoer en swak areas regstel.
- Gereelde opgradering van sekuriteitstelseluitvoer.
- Opleiding van IT-personeel in sekuriteitstegnieke.

5.4.5 Opsomming

Dit is duidelik dat die aantal handboeke en artikels oor e-sekuriteit erkenning gee aan die noodsaaklikheid daarvan in e-handel. Nie net beskerm dit besighede en gebruikers nie, maar dit skep ook vertroue by gebruikers om e-handel suksesvol te maak.

Daar is geen twyfel dat die kommer wat in die bogenoemde artikels uitgespreek word, relevant is en aangespreek moet word om e-handel se toekomstige aanvaarding en sukses te verseker nie.

5.5 GROENSKRIF OOR E-HANDEL

Die groenskrif oor e-handel het in November 2000 verskyn. Hoofstukke 7 en 8 van die groenskrif word hier geklassifiseer as dit wat met sekuriteit te make het.

Hoofstuk 7 verwys na die toekomstige groei van e-handel en dat die bou van vertroue tussen die gebruiker, besigheid en die regering primêr is.

Die kontroles rondom sekuriteit in konvensionele handel mag dalk nie voldoende wees om vertroue in e-handel te stel nie en om e-handelsekuriteit te verseker, moet stawing, konfidensialiteit, integriteit en ontkenning aanwesig wees. Terselfdertyd is wetlike, prosedurele en tegniese toepassings om die sekuriteit van data te verseker belangrik, om sodoende die volle potensiaal van e-handel te bereik. Kriptografie, digitale handtekeninge, 'n publieke-sleutel-infrastruktuur, 'n sertifiserings-outoriteit en die behoud van privaatheid om te kommunikeer moet insgelyks aanwesig wees.

Seksie 14(d) van die Konstitusie voorsien die beskerming van die privaatheid van individue ten opsigte van kommunikasie, maar beperk dit op sy beurt ingevolge seksie 36.

Kubermisdaad word beskou as onwetlike optrede en sluit die gebruik van elektroniese stelsels, netwerke, tegnologie en eenhede soos telefone, mikrogolwe, satelliete en rekenaars in.

Hoofstuk 8 behandel die beveiliging van gebruikers. Gebruikers moet beskerm word teen ongevraagde goedere en kommunikasie, onwettige en skadelike goedere, dienste

en inhoud, die gevare om te maklik aanlyn te koop, onvoldoende inligting, die gevare van inbreuk maak op privaatheid, die risiko om van beskerming ontneem te word deur onbekende, onvoldoende of konflikterende regsbeginsels van ander lande, asook teen kuberbedrog.

Gebruikerskonfidensialiteit behels ook dat gebruikers die voorreg om skade te verhaal kan hê teen ongewenste transaksies.

Die internasionale toepassing van reëls vir kontrakte oor 'n afstand moet in ag geneem word. Vooraf inligting, geskrewe bekragtiging, die reg om te onttrek, vrywaring, onwettige verkope, nakoming, kommunikasiemetodes, jurisdiksie en bindende regte, moet alles deel vorm van 'n stelsel van sekuriteit.

Privaat en persoonlike inligting moet beskerm word en hier kan die riglyne soos neergelê deur die "Organisation for Economic Co-operation and Development" (OECD), oorweeg word.

Dit sluit die volgende in, naamlik die beperking op die hoeveelheid privaat inligting wat verkry mag word, die relevansie van persoonlike data aangevra, die rede hoekom spesifieke persoonlike data verkry word, die beperkte gebruik van persoonlike data, die beskerming van sulke persoonlike data, openlikheid ten opsigte van die gebruik van hierdie data, die openbaarmaking van die spesifieke data wat oor 'n persoon gehou word, aan dié persoon, en die aanvaarding van rekenskap gegee deur 'n datahouer, om aan hierdie beginsels gehoor te gee.

5.6 SAMEVATTING

5.6.1 Wat is e-sekuriteit?

Sean Reuben definieer e-sekuriteit in die "BMI-Techknowledge New Economy Builders Handbook 2000" soos volg: "e-Security can be defined as enabling a trusted means of communicating and transacting over private and public networks, multiple computer environments, system infrastructures, and communication protocols."

5.6.2 Wat is e-risiko?

In die "Computerweek" van 7 Mei 2001, som Melissa Powell e-risiko op as:

- risiko om e-besigheid te bedryf,
- blootstelling aan internasionale aanspreeklikheid,
- professionele skadeloosstelling,
- besigheidsonderbreking,
- laster,
- verbreking van intellektuele eiendomsregte,
- verbreking van privaatheid en
- beskerming van data/inligting.

Hierdie vervat die hoofareas van e-risiko om aangespreek te word.

5.6.3 Amp K. Ghosh publiseer sy boek "E-Commerce Security", in 1998

Wat het sedertdien gebeur of is ontwikkel om sekuriteit rondom e-handel te verseker? Vanuit artikels wat verskyn het gedurende 1998 en daarna, het geen nuwe begrippe na vore gekom nie. Slegs VPN's word in 2001, verwys na in paragraaf 5.4.4, aangebied as 'n addisionele manier om die internet veiliger te maak.

5.6.4 Opsomming

E-sekuriteit is 'n allesomvattende begrip en moet gedurig aangepas word om ten alle tye die sekuriteit te bied om die aanvalle van die dag die hoof te bied. Die vinnige verspreiding van nuwe virusse en maklike toegang tot kraker-instrumente bedreig die e-ekonomie (Pieterse, 2000:35).

Dit noop dat netwerke beskerm moet word teen indringers ("The Economist", 2002:28-30) en volgens Els (2000:40) bly veiligheid die sleutel in e-sake.

E-sekuriteit moet gedokumenteer word in 'n beleidsdokument en eienaarskap daarvan moet deur werkgewers sowel as werknemers aanvaar word. Cobit ("Control Objectives for Information and Related Technology") moet 'n integrale deel vorm van so 'n beleidsdokument.

Patrick Ryan som in Andersen se nuusbrief van Oktober/November 2001, inligtingsekuriteit skematies op. Dit word in Bylaag 2 weergegee en vervat die totale sekuriteitsdissipline.

HOOFSTUK 6

DIE WET EN ELEKTRONIESE HANDEL

6.1 INLEIDING

'n Nuwe bedreiging en verhoogde risiko staar volgens Taylor (1999:7) e-handel in die gesig deur vervolging in lande se jurisdiksie waar daar besigheid bedryf word.

Wat sal die uitslag wees van sulke regsaanspreeklikhede? Wanneer is 'n kontrak aangegaan? Watter land se wette sal geld? Watter partye is betrokke? Hierdie vrae en nog baie ander word gevra rondom e-handel en die wetlike aspekte daarby betrokke.

Om hierdie en ander vrae te beantwoord, is dit belangrik om aandag te skenk aan die wetlike aspekte om handel oor die internet te doen. Die sukses van e-handel sal onder andere afhang van die beskerming wat gebruikers vanuit 'n regsoogpunt sal geniet. Die regsgeldigheid van e-transaksies en die vervolging van kubermisdaad moet nasionaal en internasionaal afdwingbaar wees, om sodoende gebruikersvertroue te skep in e-handel.

Hierdie hoofstuk ondersoek die voorgenoemde en ander aspekte van e-reg.

6.2 KUBERREG

6.2.1 Inleiding

Een van die belangrikste aspekte wat e-handel moet verwerk, is die veilige oordra van inligting en veral waar dit gaan oor die maak van betalings vir goedere en dienste wat oor die internet verkry is.

Regsdeskundiges sal die verskil in gaping tussen die tradisionele manier van besigheid doen en dié oor die internet, sensitief moet hanteer.

Die gewone reg het volgens Hoffman *et al.* (1997:voorwoord) oor die afgelope 2000 jaar ontstaan en is nie toegerus om die snel groeiende e-handelsontwikkeling na te volg nie. Daar is ook min regsake wat as riglyne kan dien by regsgevalle betreffende e-handel.

Die kuberreg moet voorsiening maak vir die fasilitering en regulering van elektroniese kommunikasie en transaksies. Dit moet onder andere regsekerheid en vertroue met betrekking tot e-transaksies by gebruikers skep, asook 'n veilige en effektiewe omgewing vir e-handel daarstel.

6.2.2 Nuwe reëls

Dit is die oop aard van die internet wat die regsprobleme veroorsaak.

Huidige wetskrywers en uitslae van regsake is meer verklarend van aard, eerder as die vernuwing van die huidige wette. Die internet is revolusionêr van aard en die reg is nie goed ingestem om met revolusionêre idees te handel nie.

Besighede sien volgens Hoffman *et al.* (1997:14-15) aan die een kant op na die reg vir stabiliteit en konsekwentheid van voorspelbaarheid, en aan die ander kant vir effektiwiteit, buigsaamheid en reaksie.

6.2.3 Digitale tegnologie

Die kuberruimte is die plek waar kontrakte gemaak word, produkte van dienste gekoop en verkoop word en geld van hande sal wissel. In die kuberruimte is alle inligting in 'n digitale (stringe van l'e en O'e) formaat.

Die internet is 'n stel standaarde met die telefoon, vastelyn of mobiel, wat daarmee koppel.

Die internet is 'n hoofweg met 'n poort van ingang deur 'n internet diensverskaffer (ISP – "Internet Service Provider"), modem en rekenaar om via die telefoon toegang te bewerkstellig. E-pos, Wêreldwye web (www) en ander protokolle word as voertuie op die hoofweg (internet) gebruik.

Om 'n teenwoordigheid in die kuberruimte te skep, is dit die maklikste om deur 'n ISP te werk, 'n e-posadres en/of 'n webbladsy op te stel met elektroniese data-interaksie wat óf deur 'n geslote óf oop (internet) netwerk kan plaasvind.

Intranette, dit is geslote interne rekenaarnetwerke, kan van die internet gebruik maak (Hoffman *et al.*, 1997:16-27).

6.2.4 Besigheidstransformasie

Lawrence Livermore som elektroniese handel in 1989 op as die konsolidasie van tegnologie, materiaal, mense en prosesse op 'n elektroniese netwerk vir kommersiële transaksies.

Dit is die wegbeweeg van papier, na 'n papierlose omgewing. Geskrewe kontrakte en fakture word elektroniese dokumente. Huidige metodes om geld te verwissel, word elektronies gedoen.

Besigheidstransformasie behels ook die gebruik van buitebronne om dit te doen wat gewoonlik intern gedoen sou word. Daar is hoofvoordele vir besighede om hierdie roete te gaan. Eerstens verminder dit die investering in kapitaal en ontwikkelingskoste vir tegnologie en vervaardigingsprosesse. Dit voorsien organisasies met 'n groter mate van beweeglikheid in nuwe ontwikkelde markte en derdens kan buitebronne makliker vervang of verander word in veranderde markte.

Die digitale ekonomie is 'n kennis-ekonomie, globaal en geoutomatiseer. Die nuwe ekonomie se hoofbate is intellektueel van aard en werknemers is nie meer net 'n koste nie. Handel kan nou oor die rekenaar (internet), televisie of deur roepsentrums gedoen word (Hoffman *et al.*, 1997:30-42).

6.2.5 Elektroniese privaatheid

In 'n globale, digitale ekonomie word privaatheid 'n ernstige bekommernis vir "Netizens" (inwoners van die internet). 'n Digitale ekonomie is 'n ekonomie van netwerke en koppel verskeie gebruikers. Dit is ook 'n vinnig bewegende inligtingsekonomie.

Die privaatheid van inligting in die werkplek en kliëntdata is belangrik om onder meer gebruikersvertroue en werknemersatisfaksie te verseker (Hoffman *et al.*, 1997:43-49).

6.2.5.1 Die Wet en privaatheid

Die hart van Suid-Afrika se wetgewing is vervat in die Konstitusie (Wet 108 van 1996).

In artikel 14 van die Wet word daarna verwys dat 'n persoon, huis, eiendom nie ondersoek mag word nie, dat besittings nie gekonfiskeer mag word nie en dat daar nie inbreuk op die privaatheid van kommunikasie mag plaasvind nie.

In artikel 32 word die reg aan persone gegee tot toegang van enige inligting deur die staat gehou en tot inligting deur 'n persoon gehou wat nodig is om regte te beskerm of uit te oefen. Nie een van hierdie artikels handel egter met die vrae rondom inligting in die kuberruimte nie.

In artikel 50 en 50A van die "Verklaring van Regte", word daar egter bepaal dat die gebruik en/of openbaarmaking van inligting van die Staat en privaat organisasies slegs mag geskied indien toestemming deur die betrokke partye verleen is.

Die Suid-Afrikaanse reg ten opsigte van privaatheid is gebaseer op die Romeinse reg, wat meer beskerming as die Engelse reg bied.

Behalwe vir hofuitsprake in die Verenigde Koninkryk van Amerika (VKA), Talley v. California en Gibson v. FLIC en die "Electronic Communication Privacy Act" (ECPA) en "Privacy Protection Act" van VKA, wat 'n mate van beskerming gegee het en bied, is die proses op sigself regulasie aangewese.

Die algemene reg ("common law") of spesifieke wetgewing sal toegepas moet word, maar dit sal voordelig wees as besighede self standpunt sal inneem om die privaatheid van individue, kliënte en werknemers te beskerm.

Die Kanadese het byvoorbeeld 'n model, die "Canadian Standards Association Model Code" ontwikkel om persoonlike inligting te beskerm. Hierdie tien beginsels kan help dat besighede die bekommernisse oor die skending van privaatheid kan hanteer (Hoffman *et al.*, 1997:50-60).

Die tien beginsels word vervat en weergegee in Bylaag 3.

6.2.6 Inligtingsekuriteit

Die sekuriteit rondom e-handel en inligting is reeds in meer besonderhede in Hoofstuk 5 bespreek.

Kommunikasie van inligting moet eerstens onleesbaar wees vir derde partye. Dit kan moontlik gemaak word deur die gebruik van enkripsie, simmetries of asimmetries. Hierdie proses moet egter beheer word. Die Suid-Afrikaanse Wet van Verbod op Onderskepping en Monitering, beskerm kommunikasie deur middel van telefone en telekommunikasielyne hierteen, maar is swyend oor e-pos.

Tweedens moet inligting nie veranderbaar wees nie. Kontrole-totale en wagwoorde kan hiervoor aangewend word.

Laastens moet die ontvanger van die inligting seker wees dat die oorsprong (stuurder) se identiteit waar is. Dit word gedoen deur 'n stawingsproses van digitale handtekeninge. Ook hier moet kontrole uitgeoefen word en die gewone reg oor kontrakte en verbreking van pligte, sal toegepas kan word.

Die Verenigde Nasies se kommissie oor Internasionale Handelswetgewing (UNITRAL), het 'n model uitgereik oor elektroniese handel. Dit inkorporeer publieke-sleutel-infrastruktuur (PKI) -stelsels en die sertifiseringsoutoriteit (CA) om sleutelhouer-sertifikate te staaf (Hoffman *et al.*, 1997:63-80).

6.2.7 Intellektuele eiendom

Intellektuele eiendom – IE ("Intellectual Property") verwys na skeppings soos boeke, kuns, uitvindsels, rekenaarprogramme, handelsmerke, en so meer.

Beskerming van IE is nie wydverspreid nie en daar is beperkings, soos byvoorbeeld die Wet op Handelsmerke, Wet No. 194 van 1993, Wet op Patente, Wet No. 57 van 1978 en die Wet op Kopieregte, Wet No. 98 van 1978.

"Netizens" het IE altyd as gemeenskaplike eiendom behandel. Handelsmerke en kopieregte skep veral probleme in die kuberruimte (Hoffman *et al.*, 1997:83,84).

6.2.7.1 Handelsmerke

Handelsmerke dien die doel om te kan onderskei tussen goedere of dienste in die mark wat afkomstig is van 'n spesifieke organisasie. Dit mag 'n naam en/of 'n teken wees.

Die Maatskappyewet, Wet No. 61 van 1973 en die Wet op Beslote Korporasies, Wet No. 69 van 1984, verleen ook beskerming waar name geregistreer is (Hoffman *et al.*, 1997:94).

6.2.7.2 Kopieregte

Kopieregte verwys na 'n stel reëls om eksklusief regte uit te oefen om 'n stuk werk te beheer en vir wins te eksploiteer.

Die regsreëls is basies dieselfde wêreldwyd, aangesien die meeste lande die Berne Konvensie (1886) soos aangepas, onderskryf het.

Lande wat lede is van die Wêreldhandelsorganisasie (WTO) word ook verbind aan die TRIPS-ooreenkoms van 1994 en gee daardeur eenvormigheid.

Dit is nie nodig om 'n kopiereg te registreer nie. Solank dit voldoen aan die vereistes van die Wet op Kopieregte, geniet dit outomaties beskerming. Volgens hierdie Wet moet werke neergeskryf wees, genoteer word, aangebied word in digitale data of seine, of verwerk wees na 'n materiaalvorm. Aangesien die Wet aangepas is om digitale inligting as 'n materiaalvorm te klassifiseer, sal werke op die internet voldoen aan die vereistes van publikasie in 'n materiaalvorm.

Wanneer sal kopiereg op die internet verbreek word? Eerstens, slegs as kopiereg oorspronklik bestaan het. Tweedens, slegs as die groter gedeelte van 'n werk of die hele werk afgelaai word. Derdens, daar sal geen verbreking van kopiereg plaasvind as daar onder die beginsel van regverdige optrede opgetree word nie. Dit gee veral aan navorsers, akademici, kommentators en verslaggewers wye regte om inligting af te laai en te gebruik.

Laastens kan daar geen verbreking wees as 'n lisensie vir die gebruik van 'n stuk werk toegeken is nie. Dit verander op sigself nie eienaarskap nie, maar gee 'n belofte dat daar geen regsoptrede sal plaasvind vir die gebruik van die inligting nie. Daar kan geargumenteer word dat weens die feit dat 'n persoon sy werk op die internet "oopstel", 'n lisensie vir die gebruik daarvan geïmpliseer word.

Ongemagtigde toegang en gebruik, dit is die verbreking van sekuriteitsprotokolle, kan tot regsoptrede lei (Hoffman *et al.*, 1997:84-90).

6.2.7.3 Domeinname

Een van die grootste regsgeskille, is dié tussen die houers van domeinname en die houers van handelsmerke of geregistreerde name. Domeinname word geregistreer deur 'n internet-diensverskaffer (IDV of ISP) by die domeinnaamstelsel.

Hierdie registrasie is nie beperk deur grense nie. Om nie 'n domeinnaam te registreer nie, is soortgelyk aan 'n handelsnaam, vandag amper nalatig (Hoffman *et al.*, 1997:97-99).

6.2.8 Kontrakte oor die internet

'n Kontrak verwys na 'n ooreenkoms tussen twee of meer partye om sekere handelinge uit te voer. Daar is geen spesiale voorwaardes nie en formaliteite maak 'n kontrak slegs makliker om as bewys te lewer van wat ooreengekom is.

'n Aanbod, daarenteen, is 'n uitnodiging om tot 'n bindende ooreenkoms toe te tree.

'n Aanbod mondelings, skriftelik, per faks of e-pos, het dieselfde resultaat. Die aanbod moet liefs spesifiek wees waar dit gaan oor die beskikbaarheid van 'n produk en prys. Dit moet aanvaar of verwerp word, en swye sal nie as aanvaarding dien nie.

Waar 'n aanbod bestaan om sagteware gratis af te laai en vir 'n spesifieke aantal dae te gebruik en dié aantal dae te oorskry, sal betaling geëis kan word aangesien die gratis tydperk oorskry is en die aanbod om te betaal daardeur aanvaar is.

Kontrakte oor die internet verskil geensins van die tradisionele metode nie. Om egter beter beskerming te verleen, sal formele optredes vereis word met 'n gepaste digitale handtekening.

Huidige wette sal aangepas moet word om die elektroniese manier van besigheid doen, te inkorporeer (Hoffman *et al.*, 1997:103-118).

6.2.9 Aanspreeklikheid

6.2.9.1 Onregmatige dade

Aanspreeklikheid vir verkeerde optrede kan óf teen die persoon óf teen reputasie wees ("injuria"), óf ten opsigte van finansiële verlies ("aquilian").

Onregmatige dade verskil van die verbreking van 'n kontrak daarin dat 'n kontrak vooraf opgestelde verpligtinge het, dat dit by die verbreking van 'n kontrak vir die reg oor die regmaak van die verbreking gaan en laastens oor 'n spesifieke aanspreeklikheid ten opsigte van kosteverhaling.

In elektroniese handel vind oortreding meer gereeld plaas as gevolg van die gereeldheid daarvan dat interaksie meer voorkom, dat daar 'n skuif is van 'n fisiese na 'n virtuele persepsie en dat gemeenskapstandaarde meer betrokke kan wees (byvoorbeeld: pornografie) (Hoffman *et al.*, 1997:121-126).

6.2.9.2 Laster

Laster kan slegs plaasvind as dit gepubliseer word. Op die internet moet bepaal word wie die publiseerder is, byvoorbeeld die diensverskaffer of die gebruiker wat die publikasie maak. Verder moet bepaal word watter land se wette toegepas moet word (Hoffman *et al.*, 1997:127-129).

6.2.9.3 Ander vorme van aanspreeklikheid

- Nalatigheid.
- Ekonomiese verlies.

- Foutiewe uitsprake.
- Produkte.
- Bedrog.
- Krakers. (Hoffman *et al.*, 1997:131-140).

6.2.10 Buitelandse transaksies

Die koms van die internet het globalisering versnel. Elektroniese handel het kommersiële onderhandeling tussen mense van verskillende agtergronde, lande en regstelsels makliker gemaak.

Daar is gewone of substantiewe reg, en dit is die regsbeginsels tussen 'n spesifieke gemeenskap en privaat internasionale reg, wat bepaal watter reg toegepas sal word as daar 'n geskil tussen twee of meer verskillende regsbeginsels is.

Daar is basies drie fundamentele konflikte wat aandag geniet:

Eerstens gaan dit oor jurisdiksie. Wie gaan 'n saak aanhoor? In Suid- Afrika word dit bepaal aan hand van die vraag of 'n regverdige uitspraak moontlik is en of die verdedigende party eiendom in Suid-Afrika het. Dit is belangrik om hierdie aspek in gedagte te hou vir besighede wat sake oor die internet doen.

Tweedens kan die partye self besluit oor die keuse van watter land se regstelsel toegepas moet word. Indien nie, sal 'n hof besluit. Indien twee lande in konflik mag kom, sal die land waar die saak aanhangig gemaak is, se regstelsel gevolg word.

Laastens sal die afdwingbaarheid van 'n regsbesluit in ag geneem word. 'n Suid-Afrikaanse hof sal nie sonder meer 'n vreemde land se hofuitspraak afdwing nie, tensy daar 'n afdwingbaarheidsooreenkoms met die vreemde land bestaan. Om die uitdagings van elektroniese handel te hanteer, moet ooreenkomste tussen lande bereik word om voorsiening te maak vir elektroniese nuwighede, partye moet vooraf besluit oor watter regstelsel van toepassing sal wees en moontlik sal daar 'n kuberhof ingestel moet word (Hoffman *et al.*, 1997:144-153).

6.3 E-WET

In die aanloop tot die uitreiking van 'n wet om e-handel te beheer, het veskeie artikels daaroor verskyn. Voorbeelde hiervan is:

Daar is tien fundamentele regsfaktore vir e-handel. Die ou fundamentele faktore van sake doen is egter nog steeds van toepassing, maar die volgende riglyne is volgens Mostert (2000:40) nodig om beskermingsmeganismes te ontwikkel en in te stel sonder om handelsversperring te skep:

- Vermy die 1/10-reël

Verkry 'n wetlik korrekte versoek om 'n kwotasie, alvorens 'n e-handelsoplossing sonder meer aanvaar en geïmplementeer word. Dit sal verhoed dat kopers R10 sal spandeer aan die implementering, integrasie en bedryf vir elke R1 wat vervaardigers vir e-handelstegnologie kwoteer.

- Evalueer huidige sakeverhoudinge

Maak seker dat daar geen kontraktuele verpligting bestaan om in 'n huidige verskaffingsketting te bly nie.

- Arbeidsreg

Suksesvolle e-handel mag meebring dat sekere personeellede oortollig raak. Herontplooi of pleeg oorleg met personeel om die beste oplossing te kry.

- Evalueer die reguleringsomgewing

Raadpleeg 'n e-sake-prokureur om te verseker dat vereistes van die Suid-Afrikaanse Inkomstediens oor die behoud van oorspronklike dokumente, rekenaardrukstukke, fakture vir e-verkryging en so meer aan voldoen word.

- Belasting

Beplan en handel die e-belastingsbeplanning af, alvorens e-handel plaasvind.

- Korporatiewe strukturering

Handel alle ooreenkomste met derde partye af, alvorens e-handelfiliale in werking gestel word.

- Verkryging, ontwikkeling en instandhouding van IT

Maak seker dat ooreenkomste in plek is vir koppeling en diensvlakke, lisensies vir apparatuur en programmatuur, ontwikkelings- en ondersteuningsdiens, webwerfontwikkeling en met die webgasheer.

- Diensverskaffers met waardetoevoeging

Sien om na ooreenkomste met lewerings- of versendingsagente, deurgangverskaffers, betalingsoplossing, bankinstellings, digitale sertifikaat en sertifiseringsowerhede, telekommunikasie-wisselwerking en privaat virtuele netwerkgebruikers.

- Internetbepalings en voorwaardes

Bepaal die wetlike aspekte van die webwerf, die reguleringsvereistes, kontraksluiting, risiko's en verpligtinge, betaling en lewering, belastings, doeaneregte, jurisdiksie, intellektuele eiendom, geskilbeslegging, privaatheid, veiligheid, waarborge en aanpasbaarheid by nuwe omstandighede.

- Veiligheid en privaatheid

Tref voldoende maatreëls vir die nakoming van die grondwetlike en gemeenregtelike reg op privaatheid en om aan die vereistes te voldoen om aanspreeklikheid te vermy.

Volgens Grunning (2001:4) is die e-handelswet 'n erns by die staat, en gebruikers en handelaars moet beskerm word, terwyl wette ten opsigte van intellektuele eiendom, nasionale betaalstelsels, telekommunikasie en sekuriteit aangepas sal moet word.

Die meeste regsfirmas het spesiale afdelings wat spesifiek konsentreer op e-wet.

Mallinicks-prokureurs adverteer byvoorbeeld dat hulle e-wetafdeling bestaan uit, IT-wet, Internet-wet, en e-Besigheidswet, waar ooreenkomste gekonstruktureer word vir die

inhoudsontwikkeling, portale, netwerkdienslewering, sagteware-ontwikkeling, internetbetaling en bankonderhoudsvoorsiening, B2B, B2C, e-posbeleid, domeinname, jurisdiksie, elektroniese handtekeninge, kopieregte, handelsmerke, IP- adresse, en so meer.

Die reg om privaatheid is in die Konstitusie vervat en die internet bring nuwe areas ten opsigte van privaatheid na vore. Privaatheid is die hart van 'n verhouding tussen besigheid en gebruikers, en behels kritieke sake rondom mag en waarde, asook die gebruik en misbruik van kommersiële inligting.

Indringing en die misbruik van inligting, asook die hoër vlak van kommer oor privaatheid by die gebruik van die internet, is van belang vir gebruikers.

Dit is egter nodig om in ag te neem dat daar 'n verskil is tussen gemeenskappe, oor die vlak van kommer wat oor privaatheid bestaan. Spanje, Suid-Afrika en die Verenigde Koninkryk is sprekend van lande met die meeste kommer oor hierdie saak. Internet-diensverskaffers word die minste vertrou in lande soos Europa, die Middel-Ooste en Afrika, maar in Suid-Afrika is 34% van die respondente tevrede daarmee om hulle persoonlike inligting aan diensverskaffers toe te vertrou.

'n Ondersoek het ook getoon dat die verbreking van privaatheid eerder aan die polisie as 'n ander instansie aangegee sal word. Bylaag 4 toon 'n tabelgrafiek van die vertroue wat op instansies geplaas word. Besighede sal moet verseker dat die interaksie tussen hulself en die gebruiker, privaat-vriendelik op die internet sal wees (Maritz:166-168).

Die internet is volgens MacIntosh (1998:12) 'n globale markplek, minus globale wetgewing.

Die staat sal volgens McLeod (1998:92) ondersoek instel oor belasting, kopiereg, patentverbreking, sekuriteit, kommer oor privaatheid, elektroniese betaalstelsels, die nodigheid vir 'n kommersiële kode vir die internet, en wetgewing sal ook enkripsie en die multimedia-oorvleueling insluit. Teen 2000 sal 'n groenskrif uit wees.

Dekker (1999:1) wys daarop dat krakers onder die Suid-Afrikaanse regstelsels aangekla kan word vir diefstal en wetgewing hiervoor sal moontlik teen 2001 ingestel word.

Korporatiewe prokureurs volgens Stones (1999:1) wil huidige wetgewing toepas op kuberruimte, maar onsekerheid bestaan oor watter land jurisdiksie sal hê, hoe 'n uitspraak toegepas sal word in 'n ander land. Verskeie wetgewing kan verbreek word deur die internet, asook die verbreking van wisselkoersreëls met die gebruik van kredietkaarte vir betaling.

Die Internet is volgens Bhagattjee (2000:17) een van die vinnigste en effektiefste maniere om besigheid te doen, maar dit is een van die swakste om deur die wet beskerm te word. Daar is geen regulasies in Suid-Afrika in plek nie, en kontrakte moet deur die internet afdwingbaar wees. Aanvaarding van voorwaardes moet duidelik weerspieël word, asook die metode van aanvaarding, watter regstelsel voorkeur sal geniet, hoe gebruikers geïdentifiseer en geverifieer word en wie die risiko neem vir beskadigde en gesteelde goedere.

'n Kliënt of gebruiker kan 'n webterreineienaar aankla en die klaer of gebruiker se regstelsel moet dan toegepas word (Hargreaves *et al.*, 2000:8).

Volgens die Suid-Afrikaanse kriminele wetgewing kan slegs iets wat tasbaar is, gesteel word. Wat dan van elektroniese data? Vincente (2000:22) sê dat volgens die Anton Pillar Orde kopieë van hardeskywe aangevra kan word as getuiemateriaal, maar voorkoming is beter as regsoptrede.

Die Verenigde Koninkryk van Amerika stel volgens Du Toit (2000:6) elektroniese handtekeninge vanaf Oktober 2000 in werking, gee erkenning daaraan en kontrakte mag daarmee onderteken word, wat as bindend en afdwingbaar aanvaar sal word.

Stones (2001:2) wys daarop dat afgevaardigdes verskil oor die regulering van e-handel. Sakemanne, vakbondverteenwoordigers, prokureurs, regeringsafgevaardigdes en akademici verskil oor basies elke aspek en leiding van ander lande wat reeds regulasies het, sal geneem moet word.

Wetgewing in Suid-Afrika sal volgens Bidoli *et al.* (2001:6) teen die einde van 2001 plaasvind, en internasionale beste praktyke sal toegepas moet word. Suid-Afrika sal sy vernaamste handelsvennote moet volg, dit is die OECD ("Organisation for Economic Co-operation and Development")-beginsels en e-wet sal moet inval met huidige

handelsooreenkomste, soos "General Agreement on Trade Services", "S.A. Development Community" en die "World Trade Organisation" (WTO).

In Webber Wentzel Bowens se "Brief" No. 6 van Januarie 2002, word verwys na die Verenigde Koninkryk se beskerming van gebruikersregulasies en die databeskermingswet. ("UK Consumer Protection (Distance Selling) Regulations (Statutory Instrument 2000 No. 2334") en "The Data Protection Action 1998"). Hierdie regulasies verwys na 'n afkoelperiode (7 dae), alvorens 'n e-handeltransaksie afdwingbaar word en op watter manier inligting oor individue verkry en openbaar mag word.

Beide regulasies sal vir Suid-Afrikaanse besighede geld wat kantore, takke of agentskappe in die Verenigde Koninkryk hou en sal in ag geneem moet word tesame met ons eie wetgewing.

6.3.1 Groenskrif oor e-handel

Die groenskrif oor e-handel het in November 2000 verskyn. Hoofstukke 2, 3, 6 en 10 van die groenskrif word hier geklassifiseer as dit wat met wetgewing en regulasie te make het.

Hoofstuk 2 verwys daarna dat die huidige wetgewing gerig is op papier gebaseerde kommersiële transaksies. Dit is dus nodig om nuwe formules daar te stel wat elektroniese transaksies sal insluit.

'n Stabiele omgewing om besigheid te doen, moet geskep word, waar gebruikersbeskerming krities is. Daar word ook aanvaar dat e-handel nie in 'n wetlike vakuum plaasvind nie, waarvoor 'n nuwe regstelsel geskep moet word nie, maar dat die huidige wetgewing en regulasies aangepas moet word om e-handel te akkommodeer. Edward Nathan & Friedland prokureursfirma is aangestel om hierna te kyk.

Die beginsels wat in aanmerking geneem moet word, is die nodigheid vir wetgewing om die nasionale implementering van elektroniese handelstransaksies in die raamwerk van internasionale standaarde te ondersteun; om te verseker dat kommersiële transaksies deur papier of elektroniese metodes kan geskied; om wetgewing in te stel en te beperk,

wat die algemene effektiwiteit van kommersiële transaksies sal verseker; om te verseker dat wetgewing sal toelaat dat kontrakte ook tegnologies neutraal kan plaasvind en dat internasionale standaarde en reëls, soos die van UNCITRAL, in ag geneem word.

Hoofstuk 3 verwys daarna dat elke land 'n regstelsel het wat sy inwoners verseker van wettige tradisionele papier gebaseerde kommersiële transaksies.

Suid-Afrika sal moet besluit watter regsbasisse as gevolg van elektroniese handel verander moet word. Dit behoort nie nodig te wees om alles nuut uit te vind nie en internasionale standaarde behoort in ag geneem te word. Regsbeginsels moet gelyke status vir beide elektroniese en tradisionele handel hê en daar moet kontraktuele veiligheid en selfregulasie bestaan. Klarigheid oor wat 'n elektroniese dokument opmaak, wat beteken op skrif en in 'n oorspronklike vorm, en vir hoe lank elektroniese inligting van dokumente gehou moet word, asook die stawing van dokumente, moet aangespreek word.

Daar moet verder duidelike riglyne neergelê word oor die aanvaarbaarheid van elektroniese rekords en die gewig wat dit in 'n hof sal dra, asook wanneer elektroniese kommunikasie 'n kontrak is en afdwingbaar word.

Terselfdertyd sal besluit moet word wanneer 'n elektroniese dokument as 'n feit of die waarheid aanvaar sal word, en oor die tyd en plek van afstuur of ontvangs van elektroniese kommunikasie en die aanvaarding van elektroniese en digitale handtekeninge.

Hoofstuk 6 verwys na die plaaslike en/of internasionale inhoud van intellektuele eiendom, kopiereg, patente en handelsmerke. Dit lig die ondoeltreffendheid van plaaslike en internasionale beskerming van intellektuele eiendom in die elektroniese omgewing uit.

Dit verwys na die wet op kopiereg, handelsmerke, die TRIPS- ooreenkoms en die regulasies van die WTO.

Hoofstuk 10 bespreek die hantering van domeinname, plaaslik en internasionaal, en waar die bestuur en verantwoordelikheid daarvoor geplaas moet word. Dit stel ook vrae rondom die teenstrydighede tussen domein- en handelsname. 'n Maatskappy, Uniforum, 'n Artikel 21-maatskappy bestuur die naamadres in Suid-Afrika (co.za). Die versoek is dat 'n onafhanklike Domeinnaam Outoriteit ("Domain Name Authority" - DNA), die proses bestuur.

Die groenskrif oor elektroniese handel wat deur die Departement van Kommunikasie vrygestel is, skep meer vrae as wat antwoorde gegee word

Dit is nodig dat die Suid-Afrikaanse regulasies, ook die internasionale regulasies in ag moet neem (Thompson *et al.*, 2001:125-126).

6.4 WET NO. 25, 2002

6.4.1 Inleiding

Die Wet op Elektroniese Kommunikasie en Transaksies, 2002, Wet No. 25, 2002 is op Dinsdag 25 Junie 2002 deur die Nasionale Raad van Provinsies goedgekeur en die Engelse teks is deur die President deur middel van 'n digitale handtekening op 31 Julie 2002 onderteken. Die volledige Wet word as Bylaag 5 ingebind.

Die Wet word in veertien hoofstukke verdeel en is van toepassing ten opsigte van enige elektroniese transaksie of databoodskap.

Dit verleen egter nie sonder meer geldigheid aan enige transaksie wat in Bylae 2 van die Wet genoem word nie (art. 4 (4)).

Bylae 2 van die Wet verwys na die Wet op Vervreemding van Grond (Wet No. 68 van 1981) en spesifiek na 'n ooreenkoms vir die vervreemding van onroerende eiendom en 'n ooreenkoms vir die langtermynhuur van onroerende eiendom vir langer as 20 jaar. Verder verwys dit na die Wet op Testamente (Wet No. 7 van 1953) en die Wet op Verhandelbare Instrumente (Wet No. 34 van 1964).

Sekere artikels van die Wet, aangedui in Kolom B van Bylae 1 van die Wet, is ook nie van toepassing op die voorafgenoemde Wette, asook die Wet op Seëlregte (Wet No. 77 van 1968) nie (art. 4 (3)).

'n Persoon, ook gedefinieer as 'n openbare liggaam, mag addisionele vereistes stel, alvorens databoodskappe aanvaar word (art. 4 (2)(6)).

6.4.2 Oogmerke

Die oogmerke van die Wet word in artikel 2 weergegee.

Artikel 2(c), 2(e) en 2(i), verwys na die bevordering van elektroniese transaksies en kommunikasie en die aanmoediging vir belegging en innovering van elektroniese transaksies. Artikel 2(l) en 2(p) verwys na die behoeftes van besondere gemeenskappe, ook gestremdes en die bevordering van KMMO's.

Artikel 2(o) verwys na die ontwikkeling van menslike hulpbronne. Daar kan geen twyfel wees dat die regering ernstig is met die uitbou van elektroniese kommunikasie en transaksies nie. Om die vordering en sukses te meet, kan verwag word dat statistiese inligting aangevra sal word van organisasies.

Sal die Sentrale Statistiekdiens betrek word? Sal regstellende aksie en swart bemagtiging soos omvat in die basiese kondisies van indiensneming (Wet No. 11, 2002) en Wet No. 97, 1998 ten opsigte van die ontwikkeling van vaardighede en die verwagtinge van die BEE-Kommissie se verslag ("BEE" – Swart Ekonomiese Bemagtiging), ook hier ten volle toepasbaar wees? Watter praktiese implikasies sal die Wet tot gevolg hê?

Artikel 7,8 en 9 van die Wet deel spesifiek respektiewelik met voorheen benadeelde persone en gemeenskappe, ontwikkeling van menslike hulpbronne en KMMO's en die inskakel van hierdie sake binne 'n e-strategie.

6.4.3 E-strategie

Artikel 5 van die Wet vereis dat 'n nasionale e-strategie vir drie jaar binne 24 maande vir die Republiek ontwikkel moet word.

Die e-strategie moet in die staatskoerant gepubliseer word, jaarliks hersien word, indien nodig, en 'n vorderingsverslag moet jaarliks ter tafel gelê word. Terselfdertyd moet die Minister beleid ten opsigte van elektroniese transaksies formuleer.

Voorheen benadeelde persone en gemeenskappe (art. 7), ontwikkeling van menslike hulpbronne (art. 8) en KMMO's (art. 9) moet ingesluit word in die ontwikkeling van die nasionale e-strategie.

Die Wet maak geen voorsiening vir straf of skuldigbevinding indien die Minister die vereistes van Hoofstuk 2 nie nagekom het nie.

Sal die Minister die Wet gehoorsaam en die dokument binne twee jaar voltooi?

Dit is dus ook nie nou duidelik hoe die nasionale e-strategie die e-strategieë van organisasies sal raak nie.

6.4.4 Regserkenning

'n Databoodskap word in artikel 1 van die Wet gedefinieer as data wat op elektroniese wyse voortgebring, gestuur, ontvang of geberg word en sluit in 'n stem en 'n rekord wat geberg word.

Die Wet erken dat databoodskappe regskrag en regswerking het.

Dit voldoen aan die regsvereiste van "op skrif wees" (art. 12) solank dit toeganklik is op 'n wyse wat vir latere verwysing beskikbaar is. So ook kan 'n databoodskap aan die vereiste van oorspronklike vorm voldoen, indien dit volledig en onveranderd gebly het, behalwe vir byvoeging van endossemente (art. 14).

Dit mag ook as getuienis toelaatbaar wees (art. 15), voldoen aan die behoud van inligting (art. 16) en aan die vereistes van veelvoudige afskrifte (art. 19(1)) en vir die voorlê as 'n dokument of inligting (art. 17(1)).

Hoofstuk 3 van die Wet handel ook met geregistreerde of gesertifiseerde pos (art. 19(14), elektroniese agente (art. 20) en in Deel 2 van die hoofstuk, met kommunikering van databoodskappe.

6.4.5 Elektroniese handtekeninge

Artikel 13, 18 en 19(3) gee regskrag en regswerking aan elektroniese handtekeninge en gevorderde elektroniese handtekeninge. Die Wet definieer elektroniese handtekening (art. 1) as data wat aangeheg of geïnkorporeer word by, of logies geassosieer word met ander data en wat deur die gebruiker bedoel is om as 'n handtekening te dien, en 'n gevorderde elektroniese handtekening as 'n elektroniese handtekening wat ontstaan uit 'n proses wat deur die Owerheid geakkrediteer is.

Die Direkteur-generaal tree as die Akkreditasie-owerheid op (art. 34(1)) en administreer die akkreditasieproses soos vervat in Hoofstuk 6 en mag 'n onafhanklike ouditeursfirma aanstel om periodiek oudits van waarmerkingsdiensverskaffer te doen (art. 36(1)(c)).

Waarmerkingsdiensverskaffer (art. 1) is persone wie se waarmerkingsprodukte of -dienste, dit is produkte of dienste wat ontwerp is om die houer van 'n elektroniese handtekening aan ander persone te identifiseer (art. 1), deur die Akkreditasie-owerheid geakkrediteer is (art. 37) of erken word (art. 40).

6.4.6 Kriptografie

Benewens die akkreditasieproses, moet die Direkteur-generaal ook 'n register van kriptografieverskaffers instel en byhou (art. 29(1)) en geen persoon mag kriptografiedienste of -produkte in die Republiek verskaf voordat daardie persoon in die register aangeteken is nie.

Inligting vervat in die register is geheim van aard, tensy dit benodig word ingevolge artikel 31(2).

6.4.7 Beskerming van verbruikers, persoonlike inligting en kritieke databasisse

Hoofstukke 7, 8 en 9 behandel respektiewelik die beskerming van verbruikers, persoonlike inligting en kritieke databasisse.

Behalwe dat 'n leweransier sekere inligting ingevolge artikel 43(1) op die webwerf beskikbaar moet stel, word daar in artikel 43(5) spesifiek daarna verwys dat die leweransier 'n voldoende veilige betaalstelsel moet gebruik en indien nie, aanspreeklik gehou sal word ingevolge art. 43(6) vir enige skade gely deur 'n verbruiker as gevolg van die versuim van die leweransier om hieraan te voldoen.

'n Afkoeltydperk (art. 44) word daargestel en die uitsluiting van enige regte ingevolge Hoofstuk 7, is ongeldig.

Artikel 51(6) verbied 'n datakontroleur om enige persoonlike inligting wat gehou word aan 'n derde party te openbaar.

Persoonlike inligting, is inligting aangaande 'n herkenbare individu, wat nie reeds meer as 20 jaar oorlede is nie (art. 1).

Die Minister kan sekere klasse inligting tot kritieke data verklaar, indien dit in die belang van nasionale veiligheid van die Republiek of die ekonomiese en maatskaplike welsyn van sy burgers is (art. 53(a)).

Sulke kritieke databasisse sal in 'n register aangeteken word (art. 54(2) en kan van tyd tot tyd deur kuberinspekteurs of 'n onafhanklike ouditeur, (art. 57) geoudit word.

Dit is noodsaaklik dat e-handelaars die bepalings van art. 43 en 51 noukeurig bestudeer om enige negatiewe impak wat die nienakoming op die onderneming se winste mag hê, te elimineer.

Ouditeure sal ook as deel van die statutêre oudit, webwerwe moet toets dat dit aan die vereistes van art. 43 voldoen en dat data wat as kritiek geklassifiseer is, voldoende beskerm is teen ongemagtigde toegang en gebruik.

6.4.8 Kuberinspekteurs

Die Wet maak voorsiening dat die Direkteur-generaal, kuberinspekteurs mag aanstel (art. 80).

Kuberinspekteurs het wye magte en bevoegdhede (art. 82) ten opsigte van die inspeksie van webwerwe (art. 81(1)(a)), kriptografiediensver-skaffers (art. 81(1)(b)), waarmerkingsdiensverskaffers (art. 81(1)(c)), kritieke databasisse (art. 81(1)(d)) en die bystandsverlening aan die Suid- Afrikaanse Polisiediens (art. 81(2)).

Artikel 57(2) voorsien dat 'n oudit op kritieke databasisse deur kuberinspekteurs of 'n afhanklike ouditeur gedoen word.

Ouditeursfirmas sal die aanstelling en bevoegdhede en ouditverslae van kuberinspekteurs in ag moet neem in die uitvoering van hulle pligte.

6.4.9 Kubermisdaad

Kubermisdaad word omskryf in hoofstuk 8 van die Wet en verwys na die ongemagtigde of opsetlike toegang, inmenging, onderskepping, vernietiging of verandering van data, die peuter met enige toestel, wagwoorde of toegangskodes of om wederregtelik enige veiligheidsmaat-reëls te oorkom. Straf met 'n boete of gevangenisstraf tot vyf jaar mag uitgereik word. Is vyf jaar straf voorkomend genoeg om voornemende kubermisdadigers af te skrik?

6.4.10 Domeinnaam-owerheid

Hoofstuk 10 van die Wet behandel die oprigting van die Owerheid as 'n maatskappy, beoog in artikel 21(1) van die Maatskappyewet 1973 (Wet No. 61) deur die Minister, om ingevolge artikel 65 die .za-domeinnaam- ruimte te administreer en te bestuur, met inagneming van internasionale beste praktyk.

Die Raad moet uit nege persone bestaan (art. 62(2)(d)) en artikel 62(3)(a) verwys spesifiek na verteenwoordigend uit geslag en gestremdheid.

Die maatskappy moet teen Julie 2003 ingelyf wees en artikel 61(4) sit uiteen sekere voorsienings wat onder andere in die Akte van die oprigting van statute opgeneem moet word. Artikel 66 en 67 handel met die finansies en verslagdoening van die owerheid en alternatiewe geskilbeslegting ten opsigte van die .za-domeinnaamruimte, word in artikel 69 aangegee.

6.4.11 Diensverskaffer

Die Minister kan ingevolge artikel 71 op aansoek deur 'n bedryfsverteenwoordigende liggaam, 'n diensverskafferliggaam erken. Die beperkings op aanspreeklikheid ingestel op diensverskaffers in Hoofstuk 11, is slegs van toepassing indien die diensverskaffer 'n lid van die liggaam is (art. 72(a)).

Die bepalinge vervat in Hoofstuk 11 ter beskerming van diensverskaffers moet sorgvuldig bestudeer word deur gebruikers van diensverskaffers, om te kan bepaal watter regsaanspreeklikheidsbeperkinge bestaan.

Gebruikers moet kennis neem van artikel 79(a) waar hierdie Hoofstuk nie enige verpligting raak wat op 'n ooreenkoms gebaseer is nie.

6.4.12 E-regeringsdienste en ander bepalings

Artikel 27 erken dat dokumente, permitte, lisensie, uitreik van goedkeurings en betaling, in die vorm van databoodskappe aanvaar mag word en betaling in elektroniese wyse mag geskied.

Ingevolge artikel 28(2), is die Suid-Afrikaanse Poskantoor Beperk 'n voorkeurwaarmerkingsdiensverskaffer.

Artikel 90 behandel die jurisdiksie van howe. Dit verhoed egter nie dat die jurisdiksie kontraktueel vir 'n spesifieke transaksie bepaal mag word nie.

Artikel 92 herroep die Wet op Rekenaargetuienis (Wet No. 57, 1983).

6.5 SAMEVATTING

Die vinnige ontstaan en ontwikkeling van die internet en die vermoë wat geskep is om handel daaroor te doen, het baie dissiplines agterweë gelaat. Een daarvan, is dié van regsbeginsels en wetgewing vir 'n grenslose, nasionaliteitslose entiteit.

Alhoewel vrae rondom wat 'n e-kontrak is, waar e-jurisdiksie lê, wie die e-partye is, hoe e-privaatheid verseker word, sal onregmatige dade aangespreek word, wat die reg op

domeinname is, die regskrag en regswerking van e-handtekeninge, deur die Wet op Elektroniese Kommunikasie en Transaksies aangespreek word, sal die werking van die Wet en die toepassing daarvan in die praktyk getoets en verklaar moet word deur toekomstige regsuitsprake.

Alhoewel die Wet op Elektroniese Kommunikasie en Transaksies, sekere internasionale tendense soos die erkenning van die regskrag en regswerking van elektroniese handtekeninge (vergelyk paragraaf 6.3.7), die aanvaarding van 'n afkoelperiode (vergelyk paragraaf 6.3.8) en andere in ag neem, is daar verseker nog baie grys areas wat vorentoe aandag sal moet geniet. So byvoorbeeld, sal die regsafdwingbaarheid rondom die beskerming van persoonlike inligting (Hoofstuk 8 van die Wet), die vervolging van kubermisdadigers (Hoofstuk 13) en andere, internasionaal ooreengekom moet word.

Nou, meer as ooit tevore sal gebruikers voorkomend moet optree en grys areas kontraktueel moet vasmaak.

HOOFSTUK 7

BELASTING VAN ELEKTRONIESE HANDEL

7.1 INLEIDING

Die e-handel het benewens op ander gebiede van dié nuwe manier van sake doen, ook vrae gelaat oor die hantering van die belasting op elektroniese transaksies, nie net plaaslik nie, maar veral op globale gebiede.

Die basis van die Suid-Afrikaanse inkomstebelastingstelsel was gebaseer op die beginsel van "bron" van verdienste. Hierdie basis is verander vanaf 1 Januarie 2001 na die beginsel van "inwoner". Die meeste eerstewêreldlande volg die beginsel om belasting te hef op inwoners se wêreldwye inkomste en op inkomste verdien in daardie land deur nie-inwoners. Hierdie nuwe basis is 'n groot belastingbeleidsverandering vir Suid-Afrika en kan die voorloper wees vir belastingbeginsels van toepassing op e-handel.

Onder die huidige internasionale belastingreg kan belasting slegs gehef word deur 'n land as 'n entiteit 'n permanente onderneming in die land het. Hierdie hoofstuk ondersoek hoe e-handel hierdie reël verander al dan nie, watter ander bekommernisse bestaan en hoe dit oorbrug kan word.

7.2 DIE PROBLEEM

Die huidige belastingwette is voor die era van die internet opgestel en lande het reeds op daardie stadium reuse bedrae aan belastinginkomste verloor op transaksies wat oor die internet bedryf is.

Verskeie sake, wat insluit die gebrek aan geografiese grense, onvoldoende rekords, die beginsel van bron van verdienste en die beginsel van permanente residensie/vestiging word deur Tafelberg (1998:2-4) bespreek en dubbel-belastingooreenkomste en die nodigheid vir globale samewerking op hierdie gebied in die toekoms moet ondersoek word.

Belasting van e-handel word volgens Lascelles (1999: 20) 'n al groter vraagstuk vir regerings. Die "Accountancy International", Januarie 1999, Volume 123 No. 1265, verwys na belasting en e-handel, en voorsien dat dit nog 'n geruime tyd sal neem, alvorens die belastingoutoriteite en besigheid die belastingimplikasies van e-handel sal bemeester.

Daar is vier sake wat aandag moet kry in die belasting van e-handel, naamlik die karaktereienskappe van die inkomste, die belangrikheid van die beginsel van *domicilium* en bron van inkomste, permanente vestiging en ook oordragspryse.

Die belastingstelsel moet dieselfde basis gebruik om belasting te hef op ekonomies gelyke inkomstes, of dit dan nou tradisioneel of elektronies verdien is.

Marshall (1999:19) beveel aan dat die huidige belastingbeginsels eerder aangepas moet word, in plaas daarvan om nuwes te ontwikkel.

E-handel bied volgens Nunes (1999:48) aan belastingbetalers 'n fasiliteit om transaksies buite Suid-Afrika te doen en daardeur belasting te vermy.

7.3 WAT IS DIE OPLOSSING?

Daar moet liefs gekonsentreer word op die uitbreiding van e-handel, as om te veel bekommerd te wees oor verlore belasting.

Die redenasie is eerstens, dat die bedrae te klein is om te belas en dit slegs nog moeiliker raak as die handel in verskillende jurisdiksies val. Tweedens, dat haastige, geforseerde oplossings miskien die verkeerdes sal wees.

Daar moet oorweeg word of dit nodig is vir internasionale ooreenkomste en die internet moet liefs toelaat dat belastingkompetisie plaasvind. Verder dat die belastingverliese klein is en dat e-transaksies gesien moet word as doeanevrye winkels.

Derdens stel Lascelles (1999:20) die vraag na waarom baie tyd en geld spandeer moet word in 'n poging om belasting op e-handel te beheer, as e-handel so veranderlik is.

Wet 31 van 1998 en 'n nuwe belasting op e-aandeletransaksies verwys daarna dat die makelaar verantwoordelik is vir die belasting op transaksies wat dit weer van die oordragnemerkliënt kan verhaal (Friedland, 1999:23).

Die Suid-Afrikaanse Inkomstediens berei volgens Ludski (2000:3) voor vir die belasting van e-handel deur 'n nuwe resident gebaseerde belasting op wêreldwye inkomste in te stel. Hierdie proses is op 1 Januarie 2001 ingestel.

Die Inkomstediens versoek dat die opgawevorms inligting moet gee oor e-handeltransaksies; dat verkope en aankope oor die internet, verskaf moet word; dat die name en webadresse van die vernaamste internetkliënte gelys moet word; dat residensie in plaas van bron in 2001 as beginsel toegepas sal word. Dit beteken dat wêreldwye verdienste verklaar moet word en krediete daarteen vir belasting in vreemde lande betaal, geëis kan word (Leib, 2000:1).

In Oktober 2000 se "Business Day Professional" word in die artikel "Taxman casts net for e-merchants", ook daarna verwys dat 'n bediener nie 'n permanente adres skep nie en dat die meeste lande residensie as 'n beginsel gebruik om e-handel te belas. Die terme, "look through" en CFE (Beheerde vreemde entiteite – "Controlled Foreign Entities") word voorgehou.

Kemp (2001:7) sê dat die beginsels van CFE deur Inkomstedienste toegepas kan word en waar oordragspryse nie markverwant is nie, kan hulle 'n netto-inkomste toeken wat gelykstaande is aan 'n bedrag verdien deur die uiteindelike beheerdes.

Die Verenigde State van Amerika is dit eens dat bestaande wetgewing in plaas van die daarstel van nuwes, eerder toegepas moet word.

Die OECD ("Organisation for Economic Co-operation and Development") voorsien ook dat die bestaande, eerder as nuwe wetgewing op e-handel toegepas word en dat 'n bediener nie 'n permanente adres daarstel nie. Die Verenigde Koninkryke volg ook die voorgaande standpunt. Dit wil verder voorkom dat Suid-Afrika ook dié rigting sal volg.

Daar is basies drie areas waar e-handel op die globale belasting 'n impak kan hê.

7.3.1.1 Bron van residensie

Suid-Afrika het oorgeskakel na die beginsel van residensie- belasting vir jare van aanslag op of na 1 Januarie 2001. Dit voorsien 'n meer effektiewe basis om die impak van e-handel mee te hanteer.

7.3.1.2 Permanente vestiging

Die beginsel in paragraaf 7.3.7.1, tesame met "permanente establishment" versterk die belastinghantering van e-handel.

Om vas te stel of 'n bediener 'n belasbare teenwoordigheid skep, moet in ag geneem word of die bediener van 'n "permanente" aard is, of die entiteit geheel of gedeeltelik sy besigheid deur die bediener bedryf, die verhouding met die internetdiensverskaffer en die aard van die aktiwiteit wat deur die bediener plaasvind.

7.3.1.3 Karakterisering van inkomste

Onder e-handel is die karakterisering van inkomste belangrik, aangesien onder dubbelbelastingooreenkomste verskillende artikels van toepassing is.

Daar is byvoorbeeld 'n verskil in die hantering van belasting op die verkoop van goedere of die ontvang van tantieme en die hantering van dienslewerings inkomste en kundigheid, wat as tantieme geklassifiseer word.

Behalwe dat Suid-Afrika reeds oorgeskakel het na residensie in plaas van bron as beginselbasis vir belasting, het die Inkomstediens ook reeds aangedui dat voorlopige belastingopgawes en elektroniese betalings vir BTW en LBS beskikbaar is (Du Plessis, 2001:15).

7.4 GROENSKRIF OOR E-HANDEL

Die groenskrif oor e-handel het in November 2000 verskyn. Hoofstuk 4 van die groenskrif handel oor e-handel en Suid-Afrikaanse belasting.

Produkte kan elektronies of fisies, dit is volgens die ou tradisionele manier, gelewer word. Onder dubbelbelastingooreenkomste, is die karakterisering van inkomste belangrik. Is betaling ontvang vir produkverkope of as tantieme inkomste?

Internasionaal lei die OECD, die VSA-regering van die WTO, die beginsels rondom e-handel en belasting. Die OECD verwys na vier aanvaarde algemene belastingbeginsels. Eerstens, neutraliteit. E-handel en konvensionele handel behoort neutraal te wees ten opsigte van belasting. Die ekonomiese oorwegings behoort besigheidsbesluite te motiveer.

Tweedens, daar moet effektiwiteit wees in die nakomingskoste wat minimaal behoort te wees.

Derdens, die belastingreëls behoort beslis en eenvoudig toepasbaar te wees en laastens, die regte belastingsbedrag moet op die regte tyd, verhaalbaar wees. As sodanig word effektiwiteit en redelikheid gehandhaaf.

Die VSA se Tesourie Departement identifiseer ook neutraliteit en verwys dan verder na die belangrikheid van residensie as basis van belasting en die klassifisering van inkomste.

Die debat rondom residensie of bron as basis, is slegs 'n punt vir bespreking voor 1 Januarie 2001, waarna residensie as beginsel in Suid-Afrika ook aanvaar is.

Indirekte belasting sal ook aangespreek moet word. Waar die klassifisering belangrik is by dubbelbelastingooreenkomste en doeane-belasting uitgesluit mag word, is BTW steeds betaalbaar, tensy dit vrygestel is volgens die wet.

Die akkurate identifikasie van die party verantwoordelik om 'n spesifieke belasting te betaal, is fundamenteel tot enige belastingstelsel. Dit is dus nodig dat die minimum reëls in hierdie verband neergelê word. Minimum inligting behoort voorsien te word, waar webterreine gebruik word. Bewyslas in e-handel behoort soortgelyk as dié van tradisionele metodes te wees. Ten opsigte van die kollektering van belastings behoort daar groter internasionale samewerking te wees.

7.5 SAMEVATTING

Die ontwikkeling en uitbreiding van die internet en e-handel mag die effek hê dat die belastingbasisse van lande mag krimp en daardeur fiskale inkomste negatief raak.

Twee hoofredes hiervoor, is die kommer wat bestaan rondom die definisie van jurisdiksie en die administrasie en afdwingbaarheid van reëls, regulasie en wetgewing.

Suid-Afrika het ook sedert Januarie 2001 oorgeskakel na die beginsel van residensie in plaas van bron.

Residensie ten opsigte van 'n natuurlike persoon, verwys gewoonlik na 'n inwoner van die Republiek, waar dié van Maatskappye en Beslote Korporasies na registrasie verwys, maar spesifiek in artikel 1 van die Wet op Inkomstebelasting, Wet no. 58 van 1962, na bestuur en beheer in die Republiek. Trusts en vennootskappe word gedefinieer as natuurlike persone.

Die klassifisering van inkomste verdien is ook belangrik in die toepassing van dubbelbelastingooreenkomste.

Permanente vestiging sal verder die belastinghantering van e-handel versterk.

Neutraliteit, effektiwiteit, sekerheid en eenvoudigheid, tesame met geregtigheid en buigsaamheid is van die algemene beginsels wat op die belasting van e-handel toegepas moet word.

In die ontwikkeling van 'n belastingraamwerk vir e-handel, is dit noodsaaklik dat die belastingstelsel regverdig sal wees. Nie net vir die belastingbetaler nie, maar ook teenoor lande. Dit behoort voorspelbaar te wees en nie die doen van besigheid te versteur nie.

Die navorsing en riglyne wat reeds deur organisasies soos die OECD, die VSA se Tesourie Departement en die WTO gedoen en neergelê is, behoort in ag geneem te word. Dit sal verhoed dat Suid-Afrika nie 'n belastingbeleid sal ontwikkel wat geïsoleer is van ander e-handelsvennote nie.

HOOFSTUK 8

REKENINGKUNDIGE BEHEER IN ELEKTRONIESE HANDEL

8.1 INLEIDING

Dieselfde beginsels wat tradisioneel op baksteen-en-beton-ondernemings van toepassing is, is volgens Ruthven (2000:40) eweneens van toepassing op e-handel. Nie net geld hierdie stelling vir die bestuur van 'n maatskappy en onderliggende sake-beginsels nie, maar sekerlik ook vir die rekeningkundige beheer van e-handelstransaksies.

Rekeningkundige beheer is reeds omskryf in Hoofstuk 2 en behels die werksaamhede van beide die rekenmeester en die ouditeur.

Is daar 'n verskil in die rekeningkundige beheer van transaksies ontstaan deur elektroniese handel teenoor transaksies voortspruitend uit die tradisionele manier van besigheid doen?

Die risiko in e-besigheid is volgens Mitchell (2000:44) dieselfde as die van die konvensionele wêreld. Dit is net groter en meer openbaar en moet dus met groter omsigtigheid hanteer word.

Tegniese sake word gou-gou finansiële sake, en daarom behoort die finansiële departement gedurig advies te gee en ook die departement van inligtings-tegnologie daaraan te herinner om risiko te minimaliseer. Aanhoudende toetsing en monitering is baie belangrik in die identifisering en voorkoming van probleme.

Sou e-handel 'n verandering teweeg bring in rekeningkundige beheer teenoor dit wat reeds ontwikkel is vir die beheer van tradisionele rekeningkundige prosedures? Is die algemeen aanvaarde rekeningkundige en ouditstandaarde ook van toepassing op e-handelstransaksies of moet dit bygewerk word om hierdie transaksies te kan akkommodeer?

Watter effek het e-handel op finansiële verslaggewing en die oudit van finansiële state? Watter nuwe risiko's en prosedures wag op die rekenmeester en die ouditeur?

Om antwoorde op hierdie vrae en ander te kry, is dit nodig om die impak wat inligtingstegnologie op die rekeningkunde mag hê, te ondersoek.

8.2 DIE IMPAK

In die jare voor 1988 het die gebruik van rekenaars min aandag in die rekeningkunde gekry.

In die "Journal of Accountancy" tussen 1950-1988 het oor die 2000 artikels verskyn wat oor die rekeningkunde handel en net in 60 daarvan, word na rekenaar gebaseerde aspekte verwys. Ook in die "Accounting and Business Research" het vir die periode 1970-1988, meer as 600 artikels verskyn oor rekeningkundige aspekte, met net 9 daarvan wat handel oor rekenaar gebaseerde aspekte van die rekeningkunde en die ouditkunde.

Sedertdien het rekeningkundige stelsels al hoe meer rekenaargebaseerd geraak. Opvoedkundige inrigtings het sedertdien begin om die gebruik van rekenaars in die rekeningkunde te doseer.

Die rekeningkundige stelsel verteenwoordig 'n belangrike deel van enige organisasie se inligtingstelsel en is vandag rekenaargebaseerd. Rekenaars is dus 'n integrale deel van die rekeningkunde en met die integrasie van rekenaars en stelsels is die beheer rondom sulke integrasies van uiterste belang. Rekeningkundige stelsels gaan wyer as die finansiële rekeningkunde en sluit verskeie ekonomiese aspekte in, byvoorbeeld die suksesvolle invordering van geld by kredietverkope en die gevolg daarvan op die kontantvloei en groeimoontlikhede van 'n onderneming, vooruitskattings van winsgewendheid, batevlakke, strategiese beplanning en begrotingsbepalings met spoed, akkuraatheid en "wat-as"-scenario's, wat deur middel van geïntegreerde rekenaarstelsels bepaal word.

Die voortbringing van inligting word ook aangewend in regsaspekte, prysberekeninge, belastingbepaling en toekomstige beleidsbepaling. Rekenaaroudits, sekuriteit en

bedrog is van die nuwe uitdagings waaraan bestuur, rekenmeesters en ouditeure aandag moet gee (Williams *et al.*, 1991:1-14).

8.2.1 Inligtingstegnologie (IT) en die ekonomie

Inligtingstegnologie is die samewerking van rekenaars en telekommunikasie. Dit is die tegnologie van geoutomatiseerde inligtingsprosessering en kommunikasie. IT kom voor in persoonlike rekenaars, telefone, faksmasjiene, fotokopieerders, satelliete en so meer.

Die ontwikkeling van IT het vervaardigers daartoe in staat gestel om inligtingstelsels binne produksie baie te verbeter. Dit het verbeterde en verhoogde produkontwikkeling en ontwerp tot gevolg gehad, vernuwing en ook meer produktiewe fabriek- en produkuitleg daargestel, wat bygedra het tot 'n verlaging in produkkoste.

Operasionele inligting is 'n tipe neweproduk van die aktiwiteit van produksie en sluit ekonomiese data vir die rekeningkunde en tegniese data in, byvoorbeeld die hoeveelhede en koste van invoermateriaal.

Hierdie inligting vorm deel van bestuursinligtingstelsels (MIS), waar rekeningkundige inligting 'n groot rol speel, en dit strategiese inligting voorsien as die basis om ekonomiese besluite op 'n medium en 'n langtermyn-basis te neem. Die akkuraatheid van inligting is belangrik vir die sukses in die besluitnemingsproses.

IT het ook 'n vraag na die noodsaaklikheid van 'n nuwe soort kennis en vaardigheid in mense laat ontstaan. Sedert 1962 (Machlup) het die produksie van inligting en kennis meer aandag, as die produksie van goedere begin kry. Hierdie stelling is later in 1977 deur Porot verder ondersoek. Finansiële en tegniese transaksies behels die kommunikasie van inligting tussen ekonomiese agente (Monk, 1991:21-30).

IT sal daarom 'n direkte uitwerking op die rekeningkundige praktyk hê. Die aanvraag en aanbied van rekeningkundige inligting lê in die keuse van individue. Dit is 'n wetenskaplike benadering tot die rekeningkunde, aangesien die primêre objektief daarvan is om rekeningkundige praktyke en prosedures te verstaan.

Korporatiewe verslagdoening het ten doel om publieke inligting te voorsien aan persone soos beleggers wat ekonomiese besluite neem, wat op sy beurt 'n uitwerking op die welvaart van individue en gemeenskappe as geheel het. Volgens Pareto (1896) se kriteria sal 'n inligtingstelsel spesiale waarde hê as dit moontlik is om 'n individu se verwagte gebruikswaarde te verhoog, sonder om die verwagte gebruikswaarde van 'n ander individu te verlaag, binne die verwagte gebruikswaardes wat die individue sou gehad het in die ekonomie sonder so 'n inligtingstelsel.

Die akkuraatheid van inligting is dus belangrik, aangesien inligting en finansiële verslagdoening 'n uitwerking op die markpryse van aandele mag hê, en as sodanig ook op die ekonomiese kragte. Terselfdertyd kan privaat inligting, dit is inligting wat nie aan die publiek beskikbaar is nie, ook 'n positiewe of 'n negatiewe uitwerking op die markpryse hê.

Die vyf hoofbronne van sosiale voordeel van publieke inligting behels die volgende: om die reeks handelsgeleenthede te vergroot en daardeur die risiko te versprei; om die reële produksie en beleggingsbesluite te verbeter; om die uitgawes in die produksie van privaat inligting te verlaag; om beheer oor bestuursbesluite te verhoog en laastens om die koste van binne-inligtingseine te verlaag.

Die rekeningkunde voorsien verskeie state (inligting) aan beleggers, soos byvoorbeeld onder andere verdienstestate, balansstate en kontantvloeistate, maar dit is nie duidelik of enige van hierdie state 'n inligtingstelsel verteenwoordig nie.

Vroeër jare het die sensitiwiteit ten opsigte van die openbaarmaking van sekere kommersiële inligting 'n rol gespeel, waar vandag word al hoe meer regulasies en wette uitgereik om die openbaarmaking van inligting so wyd as moontlik te maak (Walker, 1991:32-54).

8.2.2 Inligtingstegnologie (IT) en finansiële rekeningkunde

8.2.2.1 Inleiding

Williams *et al.* (1991:123) maak die volgende stellings: "In many ways the study and professing of accountancy derive from shortcomings in the data recording process."

Hiermee word bedoel dat daar 'n onvermoë is om 'n volledige en absolute beskrywing van gebeure, waardes en konteks in alle dimensies op te neem.

Die dubbelinskrywings boekhoudingstelsel om rekeningkundige data op te neem, is die eerste keer deur Pacioli gedokumenteer en is vandag nog 'n universele metode. Hierdie dubbelinskrywings boekhoudingstelsel het egter tekortkominge deurdat dit nie volledige inligting opneem nie. Hier word verwys na inligting wat gestoor kan word en later opgeroep word om gebruik te word in onder andere die verslagdoeningsproses, begrotings, finansiële modellering en koste-allokasies. Dit sluit ook gedetailleerde rekords van verskaffers, kliënte en ander interne en eksterne data in. Hierdie datavaslegging is soms onprakties in 'n handstelsel, maar word gefasiliteer met die ontwikkeling van inligtings-tegnologie. Die voordeel van die vermoë van die moderne rekenaar en rekenaar gebaseerde stelsels om data in groter hoeveelhede te stoor, te manipuleer en op te roep, moet gebruik word. Dit behoort meer koste-effektief as handgeskrewe stelsels te wees en behoort meer nuttige inligting beskikbaar te stel.

8.2.2.2 Matriksgebaseerde rekeningkunde

Die oorskakeling van tradisionele opname en prosessering van rekeningkundige transaksies na nuwe raamwerke van aanbieding, sluit meestal die gebruik van matrikse in. Oorspronklik het die oorskakeling gewentel rondom wetenskaplike en wiskundige redes en dat rekenaars meer gemaklik getalle kon manipuleer as dit in 'n matriks- of tabelvorm gestoor word.

Matriks gebaseerde sagteware soos Multiplan, Lotus en Excel, getuig hiervan. Die ontwikkeling van die relasiemetode vir databasistelsels was 'n belangrike deurbraak in die ontwikkeling en ontwerp van rekeningkundige stelsels.

Die voordele van die dubbelinskrywings handstelsel, naamlik dat rekords omvattend en ordelik is, 'n volledigheidstoets voorsien en maklik opsommende finansiële state voorsien, moet deel uitmaak van 'n rekenaarstelsel. Die beginsel van T-rekeninge en 'n twee-dimensionele matriks moet behoue bly.

Die tweeledige effek van 'n transaksie moet in 'n matriks gebaseerde rekeningkundige stelsel gefasiliteer word. Dit is 'n transaksiematriks (T-matriks) van gelyke rye en kolomme, waar 'n ry die debiet hou en 'n kolom die krediet.

'n Rekeningkundige inligtingstelsel mag in substelsels verdeel word om data te aanvaar wat weer in transaksieleêers gestoor word en gebruik word om die T-matriks op te dateer. Die organisasie van die data in die substelsels en die uitvoer-verwagtinge mag heelwat verskil. *Substelsel* verwys na byvoorbeeld aankope en verkope, kontant-ontvangstes en betalings, algemene joernaal, finansiële verslaggewing en begrotings.

Die aanwendingsprogramme onderliggend tot substelsels, bevat gedetailleerde inligting en rekords van byvoorbeeld kliënte en verskaffers. Voldoende inligting word in die T-matriks gestoor vanwaar aanwendingsprogramme in die substelsel dit onttrek.

Sluitingsinskrywings kan outomaties deur 'n aanwendingsprogram uitgevoer word, sonder dat dit deur die algemene joernaal ingevoer hoef te word.

Balanse van rekeninge word in 'n spesiale kolom (Vector) gehou en word deur die aanwendingsprogramme in die substelsel vir finansiële verslaggewing as 'n proefbalans onttrek.

Die konvensionele manier van rekeningkundige stelsels ten opsigte van die gestandaardiseerde toevoer is deur navorsers soos Sorter (1969) gekritiseer. Hy argumenteer dat dit onmoontlik is om toevoer-inligting te spesifiseer vir wyd-eenlopende gebruike en stel 'n gebeurtenis rekeningkundige stelsel voor.

Navorsers soos Colantoni (1971), Lieberman en Whinston (1975), asook Haseman en Whinston (1976) het 'n databasis-benadering voorgestel. 'n Relasiedatabasistelsel sal nie slegs historiese transaksies hou nie, maar ook toekomstige gebeurtenisse sal ingesluit kan word. In so 'n stelsel sal die integriteit en volledigheid van rekeningkundige data beskerm moet word en 'n transaksiematriks kan hiervoor gebruik word.

Die redes om matrikse in rekenaar gebaseerde stelsels in die rekeningkunde te inkorporeer, is eerstens dat 'n matriks waarin balanse gestoor word, 'n totale prentjie van 'n organisasie se toestand op enige stadium gee. In 'n aanlyn-stelsel kan inligting vinnig

en effektief geproduseer word. Tweedens, periodieke verslaggewing kan onderneem word deur die gebruik van matrikse. Derdens, transaksierekords word slegs eenmalig gestoor, naamlik in toepaslike transaksielêers. Vierdens, rekeningbalanse word gestoor om aanpasbaar met finansiële modelleringstaal en spreiblad-pakkette vir begrotings en beplanning te wees. Vyfdens, die gebruik van matrikse is aanpasbaar met en behoort relasie-databasisbestuurstelsels in die rekeningkunde te bevorder. Laastens, 'n matriksraamwerk is 'n bruikbare basis om 'n nuwe leerreëlmodel in die rekeningkunde te ontwikkel (Leech *et al.*, 1991:127-148).

8.2.2.3 Databasis gebaseerde rekeningkundige stelsels

Dit is belangrik dat die verskil tussen stelsels en tegnologie verstaan moet word. Veranderinge in tegnologie wat 'n verbeterde spoed van dataprosessering en outomatiese beheer teweeg mag bring, mag die uitwerking hê dat daar verandering in rekeningkundige stelsels moet plaasvind om die voordele van die tegnologiese verandering te benut.

Dit is nie noodwendig so dat tegnologiese veranderinge in die rekeningkunde ook 'n verandering van rekeningkundige stelsels *meebring* nie.

Hoofraam-rekeningkundige sagteware sowel as persoonlike rekenaar gebaseerde rekeningkundige pakkette behels slegs gerekenariseerde weergawes van joernalisering en pos-roetines wat dubbelinskrywingsbeginsels gebruik om prosedures te definieer, en rekeningtabelle om ekonomiese gebeurtenisse te klassifiseer.

Die tabelle van rekeninge en die dubbelinskrywingsprosedure is 'n skema om finansiële data te organiseer, te klassifiseer en te versamel (Geerts, 1991:159-181).

Finansiële data, tesame met ander inligting wat in substelsels gehou word, naamlik onder andere rekords van kompeteerders, produkte en kostestrukture vorm integrale inligting wat kan bydra tot die besluitnemingsproses asook prosesse soos probleemoplossing, beplanning, beheer en verrigting-evaluasie (Gregory, 1991:187-1999).

Hierdie databasis vorm dan ook die platform vir kundige stelsels (ES). ES is 'n rekenaarstelsel wat die kennisbasis van 'n kundige hou in 'n vorm wat dit moontlik maak dat die rekenaar intelligente advies kan gee of intelligente besluite kan neem (Collier, 1991:216-230).

ES word veral aangewend in die ouditkunde en in belasting-aangeleenthede (Connell, 1991:406-408).

Dit is hierdie databasis wat beskerm moet word teen ongewenste en ongemagtigde toegang.

8.2.2.4 Ouditering en rekenaars

Die ouditering van 'n rekenaaromgewing het sedert die ontstaan in die sestigerjare, die gebruik van programme ingesluit om ouditeure by te staan in die analisering en bevestiging van die akkuraatheid van data. Dit verwys na 'n voorbeeld van 'n substantiewe (stawing) ouditprosedure.

Daar benewens is toetsdata gebruik om die akkuraatheid van programme te bevestig, asook vraelyste en ander prosedures om ouditeure by te staan om interne kontroles te evalueer. Hierdie sake verwys dan na beheermaatreëltoetse.

Die omvang van ouditering in die rekenaaromgewing sluit ook onder andere die onderhoud van ouditrekords oor rekenaar-lêers, die aanwending van geprogrammeerde kwaliteit kontroleprosedure en die gebruik van geoutomatiseerde vraelyste en ES in, om verskeie aspekte van 'n ouditeur se kennisbasis te omvat. Dit sluit verder ook die gebruik van 'n ouditeur se eie rekenaarstelsels en programme in die ouditprosedure in. Voorts behels dit die evaluering van interne kontroleprosedures rondom die aanwending van rekenaars.

Dit is dan noodsaaklik dat ouditeure in die ouditering van die rekenaaromgewing, oor die nodige vaardigheid en kennis moet beskik om met gevorderde inligtingsprosesseringstelsels te handel. Hierby ingeslote ook die evaluering van die geldigheid en akkuraatheid van verslaggewing van inligting.

Soos die gebruik van byvoorbeeld robotika toeneem in die vervaardigingsproses, die toename van ES, die integrasie van stelsels, toename van die gebruik van slimkaarte as alternatief tot toegangswagwoorde en digitale handtekening as kontrole-prosedures en virtuele realiteit, plaas dit groter druk op rekenmeesters en ouditeure om funksionele kundigheid te ontwikkel. Die voorgaande omvat ook begrip van kontroleteorie, analise van risiko, evaluasie van voorkomende maatreëls, netwerksekuriteit, ongemagtigde toegang, geheimhouding en stawing deur gebruik te maak van enkripsie en stawingsprogramme (Court *et al.*, 1991:429-443).

8.2.2.5 Kontrolering van papierlose besigheidstransaksies

Die subkomitee van die Komitee vir Inligtingstegnologie van die Suid-Afrikaanse Instituut van Geoktrooieerde Rekenmeesters het in Desember 1996 'n riglyn oor papierlose besigheidstransaksies uitgereik om die bestuur, inligtingstelselpersoneel en ouditeure by te staan met die risiko en kontroles wat met hierdie soort transaksies gepaardgaan. Alhoewel die riglyn spesifiek verwys na die interskakeling van elektroniese data (EDI), is dit ook van toepassing op e-handel oor die internet.

Suksesvolle e-handel behels eerstens, die aktiewe bystand van al die geaffekteerde afdelings in 'n organisasie, tweedens, die daarstel en byhou van 'n volledige risiko-analise en laastens, die steun van alle partye, insluitende topbestuur. 'n Verhoogde risiko ontstaan as gevolg daarvan dat in 'n groter mate op rekenaars staatgemaak word vir die daaglikse operasies. Hierdie tendens sal tot 'n groter katastrofe lei indien daar byvoorbeeld aftyd in rekenaartyd ontstaan, stelsels korrup raak, virusse data vernietig, ongemagtigde toegang tot data ontstaan, vertroulike inligting bekend raak en onbehoorlike ouditspore bestaan.

Kontroles oor bestaande stelsels sowel as nuwe stelsels moet foute tydens die prosesseringstadium vroegtydig identifiseer en voorkom. Waar besigheid-tot-besigheidtransaksies (B2B) plaasvind, kan toegangsbeheer tot die stelsel doeltreffend toegepas word om sodoende ongewenste toegang te verhoed en 'n verlies van konfidensiële inligting te vermy.

Sorg moet gedra word dat foute tydens 'n transaksie beperk en sover moontlik uitgeskakel word. Transmissie moet slegs binne 'n veilige kommunikasieproses geskied, wat onder andere wagwoorde, enkripsie en digitale handtekening insluit.

Dit is noodsaaklik dat harde- en sagteware gedurig getoets en bygewerk word met die nuutste tegnologie om ongewenste toegang te verhoed. Terselfdertyd moet hernuwingsplanne vir rampe bygewerk word om stelsels vinnig op te kry indien harde- en sagteware sou faal. Dit sluit ook in, die bywerk van beleids- en prosedurehandleidings om e-handel te omvat.

Die fisiese kontrole behoort die beskerming teen vuur, stof en water in te sluit, asook herwinning na kragonderbrekings, datastoring en duplikaatdataberging van die perseel af, lugverkoeling en versekering. Organisasies behoort e-handel as deel van hulle besigheidsplanne en strategiese planne in te sluit.

Rekeningkundige kontroles en rekonsiliasies moet voorsiening maak daarvoor om daagliks e-handelstransaksies te monitor vir die volledigheid van transaksies, toepassing van sekuriteitsmaatreëls en die uitdruk van ouditspore.

Net soos by die tradisionele rekeningkunde, moet pligte binne die transaksie- en kontrolesiklusse geskei word, om sodoende interne kontroles te versterk.

8.3 E-HANDEL – OUDIT-IMPLIKASIES

Die Australiese Rekeningkundige Navorsingstigting (AARF) het namens die gesertifiseerde Publieke Rekenmeesters (CPA's) van Australië en die Instituut van Geoktrooieerde Rekenmeesters in Australië, 'n "Auditing and Assurance Guidance Statement, AGS1056" in Mei 2002 uitgereik, met die title, "Electronic Commerce – Effect on the Audit of a Financial Report".

Dié standpunt, vervang 'n vorige standpunt met dieselfde nommer, uitgereik in Augustus 2000 en vervat die volgende riglyne aan ouditeure om hulle by te staan waar entiteite meedoen in kommersiële aktiwiteite waar gekonnekteerde rekenaars oor 'n publieke netwerk soos die internet gebruik word.

Die mate waarin e-handel deel uitmaak van 'n entiteit se besigheids-aktiwiteite en die toename daarvan, sal die toename van nuwe elemente van risiko bepaal, wat deur die ouditeur in die beplanning en uitvoering van sy oudit, in ag geneem moet word.

Die vlak van vaardigheid en kennis wat benodig word om die effek van e-handel op die oudit te bepaal en vas te stel, sal bepaal of die personeel toegewys om die oudit uit te voer, oor voldoende kennis van inligtingstegnologie en internetbesigheid beskik.

Die entiteit se e-handelstrategie en aktiwiteite, gebruike van tegnologie en die personeel se kennis van inligtingstegnologie, asook kennis van hoe om risiko's wat e-handel daarstel binne die raamwerk van interne kontrolestelsels en sekuriteitsinfrastruktuur te beheer, sal 'n rol speel in die toewysing van oudit-personeel.

Die ouditeur mag besluit om van die werk van 'n kundige gebruik te maak. Dit is egter noodsaaklik dat die ouditeur kennis van die entiteit moet bekom. Hierdie kennis sal hom daartoe in staat stel om die gebeure, transaksies en praktyke wat 'n aansienlike uitwerking op die finansiële verslag of ouditverslag mag hê, te kan identifiseer.

Sodanige kennis is belangrik om die aansienlike uitwerking wat e-handel op die entiteit en op die ouditrisiko mag hê, te kan evalueer. Die aanvaarding van verskeie vlakke van risiko mag die sekuriteit van finansiële rekords en die volledigheid en vertroue van die voorsiene finansiële inligting affekteer.

Dit is dan nodig dat die ouditeur die aktiwiteit van e-handel binne die totale besigheidstrategie in ag neem: Is dit 'n nuwe aktiwiteit of beoog dit om huidige aktiwiteite meer effektief te maak? Hoe wesentlik is e-handel tot die totale inkomste? Wat is die bestuur se benadering tot risiko en hoe raak dit die risikoprofiel van die entiteit? Watter belangrikheid wys die bestuur aan e-handel geleenthede en risiko's toe?

Waar aktiwiteite van e-handel bestuur en beheer word deur van buitebronne gebruik te maak, moet die ouditeur aandag gee aan sulke ooreenkomste en hoe die entiteit reageer op risiko's wat daarmee gepaardgaan. Besigheidsrisiko's sluit in die verlies van integriteit van transaksies, onvoldoende ouditspore, deurlopende sekuriteitsrisiko's (virusaanvalle, bedrog, ongemagtigde toegang), onvoldoende rekeningkundige beleid

ten opsigte van byvoorbeeld kapitalisasie of die afskryf van webtuistekoste, omskakeling van vreemde valuta, voorsiening gemaak vir die terugsending van goedere, die nienakoming van belasting, regs- en statutêre regulasies, onvoldoende aandag aan bindende faktore in e-handelskontrakte, vertroue op e-handel, en die moontlikheid van stelsel- en infrastruktuurfaling.

Deur 'n infrastruktuur wat voldoende sekuriteit voorsien, moet besigheidsrisiko's soos die verifikasie van kliënte en verskaffers by e-handel, die integriteit van transaksies, die nakoming van handelsterme en die ooreenkoms van betaling, die totstandkoming van privaatheid, asook inligtingsbeskermingsprotokolle beperk word.

Om te verseker dat die integriteit van inligting (-data) en die sekuriteit in en rondom rekenaars en rekenaarstelsels behoorlik ingestel is en funksioneer, is dit verkieslik dat die ouditeur en kundiges reeds tydens die beplannings- en ontwikkelingsfase teenwoordig is. Dit sluit in waar rekenaars slegs gebruik word vir die transformasie van handgeskrewe stelsels na 'n geoutomatiseerde stelsel, of 'n volle geïntegreerde stelsel.

Hierdie koppeling van stelsels veroorsaak unieke kontroleprobleme soos byvoorbeeld die transaksiekontroles, datavolledigheid, akkuraatheid, eienaarskap, tydigheid, toegang en ouditering, wat alles geëvalueer moet word. Virusse, die seleksie van rekenaarhardeware en die opstel daarvan, asook die keuse van sagteware moet noukeurig oorweeg word.

Kontroles sluit in die vereistes wat gebruikers stel, segregasie van pligte, toevoer en prosesseringskontroles en die distribusie van inligting (verslae). Die gebruik van toetsdata, parallelle simulasie, reprosessering van data op die toetser se stelsel, en so meer, is van die metodes om die operasionaliteit van rekenaarstelsels te toets (Ratliff *et al.*, 1996:793-841).

Rekenaarondersteunde ouditteqnieke ("Computer Assisted Audit Techniques" – CAAT's), is programme wat ontwikkel is om die ouditeur by te staan in die ouditproses. Hierdie programme sal opgegradeer moet word in die evaluering van kontroles in e-handelstelsels. (Lay *et al.*, 1987:103-119.)

Waar regs- en statutêre sake nagegaan word, mag dit nodig wees om van 'n kundige gebruik te maak (prokureur).

Die bepaling van die risikovlak word beïnvloed deur die kontrole-omgewing en die kontroleprosedures wat toegepas word deur die entiteit. In e-handel word die behoud van die integriteit van kontrole-prosedures en toegang tot rekords, spesifiek relevant.

Die sekuriteit van inligting is 'n belangrike aspek, waar toegang deur 'n publieke netwerk daartoe verkry kan word. Magtiging, stawing, konfidensialiteit, integriteit en die beskikbaarheid van inligting moet beskerm word en die gebruik van brandmure, sagteware vir virus-beskerming, enkripsie, beheer oor die ontwikkeling en implementering van stelsels en die voortdurende opgradering van stelsels en sagteware, is noodsaaklik. Die ouditprosedures ten opsigte van die integriteit van inligting in die rekeningkundige stelsel van e-handelstransaksies, behels die evaluering van die betroubaarheid van die stelsels in gebruik, om inligting te kan in neem en prosesseer. Dit behels 'n in diepte ouditttoets van die stelsel en fokus spesifiek op die verifiëring van invoerdata, voorkoming van duplikasies, die vooraf aanvaarding van handelsterme, geldigheid van 'n transaksie, volledigheid van 'n transaksie, die distribusie van transaksie-inligting oor die hele netwerk en of die rekords behoorlik bygehou, gekopieer en beveilig is.

Waar stelsels geïntegreer is en effektief as een stelsel opereer, moet die ouditeur die kontroles oorweeg wat die integrasie beheer, en spesifiek aandag gee aan sake wat die volledigheid en akkuraatheid van transaksieprosessering en -storing affekteer, en wat die tyd van aanvaarding van inkomste, aankope, ander transaksies, asook die identifikasie en opneem van betwiste transaksies raak.

Die ouditeur moet ook die inligtingsbeleid en sekuriteitskontroles van die entiteit nagaan, om te kan bevestig dat geen ongemagtigde veranderinge aan die rekeningkundige stelsels, rekords of stelsels wat data aan die rekeningkundige stelsel verskaf, gemaak is nie.

Die Raad van Openbare Rekenmeesters en Ouditeure het 'n praktyk-standpunt, SAAPS 1013 (vergelyk paragraaf 8.5.11 van hierdie hoofstuk), in Julie 2002 uitgereik. Die effek

van e-handel op die oudit van finansiële state is in ooreenstemming met die voorgenoemde in paragraaf 8.3.1 bespreek, behalwe dat daar verwys word na Suid-Afrikaanse standpunte, naamlik die standpunte oor kennis van die besigheid (OU310), risiko-beoordeling en interne beheer (OU401), gebruik van die werk van 'n kundige (OU620), en andere. Hierdie standpunt is slegs in Engels beskikbaar.

Beide AGS 1056 (8.3.1) en SAAPS 1013 is gebaseer op die Internasionale Ouditpraktykstandpunt (IAPS) 1013, "Electronic Commerce – Effect on the Audit of Financial Statements".

8.4 E-HANDEL EN DIE ALGEMEEN AANVAARDE REKENINGKUNDIGE PRAKTYK (AARP)

8.4.1 Inleiding

Standpunte oor AARP word opgestel en geopenbaar deur die Suid-Afrikaanse Instituut van Geoktrooieerde Rekenmeesters (SAIGR) en word deur die Rekeningkundige Praktykeraad (RPR) goedgekeur.

Die RPR is in 1973 gestig met die hoofdoelstelling om dit wat die Raad beskou as algemeen aanvaarde rekeningkundige praktyk, te vestig en te bewerkstellig. Die Maatskappyewet verwys in Artikel 286(3) na algemeen aanvaarde rekeningkundige praktyk en dat finansiële jaarstate ooreenkomstig daarmee opgestel moet word. Die doel is om rekeningkundige standaarde voort te bring wat die mees algemene rekeningkundige toepassing het, maar wat ongewenste alternatiewe uitskakel.

Om hulp te verleen in die toepassing van standpunte oor AARP, moet oorweging gegee word aan twee sake, naamlik (a) wese-bo-vorm en (b) wesenlikheid.

Wese-bo-vorm beteken dat transaksies en ander gebeure ooreenkomstig hul wese en finansiële werklikheid verantwoord en aangebied word en nie slegs in ooreenstemming met hul regsvorm nie.

Alle items wat wesentlik genoeg is om evaluerings of besluite te beïnvloed, behoort ingevolge RE100 geopenbaar te word in finansiële state. 'n Volledige lys van

standpunte oor AARP, rekeningkundige riglyne, menings en 'n vertolking van standpunte oor AARP, word in Bylaag 6 weergegee. Hierdie standpunte is dan ook van toepassing op e-handelstransaksies. Standpunte wat veral in ag geneem moet word tydens e-handel, word hierna uitgelig.

8.4.2 Raamwerk (RE 000)

Hierdie raamwerk sit uiteen watter begrippe grondliggend is aan die opstel en aanbieding van finansiële state vir eksterne gebruikers.

Om dit te bereik is dit noodsaaklik dat rekeningkundige stelsels en rekords slegs inligting bevat wat betroubaar en bruikbaar is, vry van wesentlike foute en onewewigtigheid. Hieruit vloei dan ook voort die proses van sekuriteit in en rondom stelsels en inligting soos bespreek in Hoofstuk 5.

8.4.3 Aanbieding van finansiële state (RE 101)

Die doel van hierdie standpunt is om die grondslag vir die aanbieding van veeldoelige finansiële state voor te skryf en geld vir alle tipes ondernemings, ook dus e-handelsondernemings.

Dit stel dat finansiële state 'n redelike weergawe behoort te wees van die finansiële stand, finansiële posisie en kontantvloei van 'n onderneming en dat onvanpaste rekeningkundige behandeling nie reggestel word deur die openbaarmaking van rekeningkundige beleid wat toegepas is nie en ook nie deur aantekeninge of verduidelikende materiaal nie.

Dit verwag voorts dat rekeningkundige beleid, dit is die spesifieke beginsels, grondslae, konvensies, reëls en praktyke wat deur 'n onderneming in die opstel en aanbieding van finansiële state aanvaar word, só gekies en toegepas behoort te word dat finansiële state aan al die vereistes van elke toepaslike standpunt oor AARP en elke toepaslike goedgekeurde vertolking voldoen.

Rekeningkundige beleid sluit onder andere in beleid ten opsigte van die erkenning van inkomste, belastings, omrekening van buitelandse valuta en verskansing, omskrywing

van sake en geografiese segmente en die grondslag vir die toewysing van koste tussen segmente.

Openbaarmaking sluit ook in die domisilie en regsvorm van die onderneming, land van inkorporasie, 'n beskrywing van die aard van die onderneming se bedrywighede en die uiteindelike moederonderneming.

8.4.4 Inkomstebelasting (RE 102)

Die doel van hierdie standpunt is om die rekeningkundige verantwoording vir inkomstebelasting voor te skryf. Dit vereis dat 'n onderneming verantwoording doen van die belastinggevolge van transaksies en sluit alle binnelandse en buitelandse inkomstebelasting in, ook belastings soos terughoubelasting.

8.4.5 Voorraad (RE 108)

In paragraaf .05 van hierdie standpunt, word omskryf wat voorraad behels. Hierdie omskrywing moet ook virtuele voorraad insluit. Dit is byvoorbeeld waar lugtyd elektronies gelewer word vanaf 'n operateur aan 'n diensverskaffer en dan deur die diensverskaffer aan die gebruikers verkoop word en kan elektroniese betaling insluit.

8.4.6 Inkomste (RE 111)

Die doelstelling van die standpunt is om die rekeningkundige hantering van inkomste wat uit sekere tipes transaksies en gebeure ontstaan, voor te skryf.

Dit sluit in die meting van inkomste, identifisering van 'n transaksie en die openbaarmaking daarvan, en hierby ingeslote is ook die toepassing daarvan op e-handelstransaksies.

8.4.7 Die uitwerking van veranderings in wisselkoerse (RE 112)

'n Entiteit kan transaksies in buitelandse valuta doen of hy kan buitelandse bedrywighede hê.

Met die grenslose reikwydte van e-handel, is die toepassing van hierdie standpunt vir die verantwoording van transaksies in buitelandse valuta veral van belang, waar 'n onderneming nou as gevolg van e-handel vir die eerste keer daarmee te doen kry.

8.4.8 Segmentverslagdoening (RE 115)

Hierdie standpunt handel oor die beginsels vir verslagdoening oor finansiële inligting volgens segmentinligting en sluit in die verskillende grafiese gebiede waarin 'n onderneming bedrywig is. Baie ondernemings sal as gevolg van hulle e-handelsbedrywighede nou aandag aan hierdie standpunt moet gee.

8.4.9 Kontantvloei (RE 118)

Die standpunt oor kontantvloei verwys spesifiek na kontantvloei uit buitelandse valuta en die verslaggewing daarvan (paragraaf .30 en .32). Waar ondernemings as gevolg van e-handelstransaksies meer en meer inkomste uit die buiteland verdien, moet aandag aan hierdie standpunt gegee word.

8.4.10 Hiperinflasionêre ekonomieë (RE 124)

Hierdie standpunt verwys na waar 'n onderneming sake doen in die geldeenheid van 'n hiperinflasionêre ekonomie.

Ondernemings wat aktief deur middel van e-handel besigheid bedryf, moet die effek van hierdie standpunt op hulle bedryfsresultate oorweeg.

8.4.11 Onaantasbare bates (RE 129)

Die doel van hierdie standpunt is om die rekeningkundige behandeling vir onaantasbare bates voor te skryf.

'n Onaantasbare bate is 'n identifiseerbare nie-monetêre bate sonder fisiese substansie wat gehou word vir gebruik in die produksie of verskaffing van goedere of dienste, en dit sluit vir administratiewe doeleindes in.

Hierdie standpunt bespreek dan ook spesifiek navorsings- en ontwikkelingsuitgawes. Hierdie standpunt is veral van belang vir die hantering van sulke uitgawes vir webtuistes en rekeningkundige stelsels om e-handel te dryf en die erkenning en behandeling van latere uitgawes. Dit behandel dan verder ook die amortisasieproses van sulke onaantasbare bates.

8.5 E-HANDEL EN OUDITSTANDAARDE

8.5.1 Inleiding

Die Suid-Afrikaanse Instituut van Geoktrooieerde Rekenmeesters (SAIGR) is 'n lid van die "International Federation of Accountants" (IFAC) en onderneem onder andere daardeur om die werk van die IFAC te ondersteun; spesifiek by die inkorporasie van die beginsels waarop die internasionale ouditstandaarde (ISA), soos ontwikkel deur die Komitee vir Internasionale Ouditpraktyke (IAPC) van die IFAC berus, in die nasionale (Suid-Afrika) ouditstandaarde.

Die SAIGR het in 1994 goedgekeur dat die standpunte van die Suid-Afrikaanse Ouditstandaarde (SAOS) gebaseer sal word op dié van die internasionale standaarde. Die Openbare Rekenmeesters en Ouditeursraad is die statutêre liggaam wat hierdie proses beheer.

Hierdie standpunte word in Bylaag 7 weergegee en moet as 'n geheel deur 'n ouditeur oorweeg en toegepas word tydens 'n oudit en dek ook dus e-handelstransaksies. Spesifieke standpunte vir toepassing by e-handel word hierna uitgelig.

8.5.2 Woordelys van terme (SAOS 110)

Die aanhegsel tot SAOS 110 verwys spesifiek na die IT-woordelys. Dit erken die beginsels van enkripsie (kriptografie) van brandmure, wat belangrike rolle speel in die veiligheid en beheer by e-handel.

8.5.3 Die doelwit van en algemene beginsels wat 'n oudit van finansiële state reël (SAOS 200)

Die doel van 'n oudit van finansiële state is om die ouditeur in staat te stel om 'n mening uit te spreek of die finansiële state, in alle wesentlike opsigte, die finansiële toestand van die entiteit op 'n spesifieke datum, en die resultate van sy bedrywighede en kontantvloei-inligting vir die tydperk geëindig op daardie datum, redelik weergee, in ooreenstemming met 'n geïdentifiseerde verslagdoeningsraamwerk en/of statutêre vereistes (paragraaf .02).

Die ouditeur moet veral die ouditprosedures wat in ag geneem moet word by die nagaan van e-handel, sorgvuldig oorweeg.

8.5.4 Gehalte van ouditwerk (SAOS 220)

Tesame met SAOS 200, moet SAOS 220 in ag geneem word, veral ten opsigte van die vaardighede en bevoegdheid van personeel met betrekking tot e-handel en die rol van IT daarin.

8.5.5 Oorweging van Wette en Regulasies in 'n oudit van finansiële state (SAOS 250)

Wanneer ouditprosedures beplan en uitgevoer word, en wanneer die resultate daarvan geëvalueer en gerapporteer word, behoort die ouditeur daarvan bewus te wees dat die entiteit se nienakoming van wette en regulasies die finansiële state wesentlik kan beïnvloed (paragraaf .02).

Waar e-handel dit vergemaklik om wêreldwyd sake te doen, verkope sowel as aankope, is dit noodsaaklik dat die impak van wette en regulasie van sulke lande waarin sake gedoen word, ook tydens die beplanningstadium oorweeg word.

8.5.6 Beplanning (SAOS 300)

Spesifieke aandag sal in die beplanningstadium geskenk moet word aan e-handel en die effek daarvan op die rekeningkundige beleid en interne beheerstelsel van die entiteit, die risiko, asook die wesentlikheidsvlakke en veiligheid van inligting.

8.5.7 Risikobeoordeling en interne beheer (SAOS 400)

Spesiale aandag moet gegee word aan die effek wat e-handel op die risikobeoordeling en interne beheer van 'n entiteit het. Dit is veral van belang in die bepaling van die inherente risiko en die kontrole-risiko.

Hierdie risiko-elemente sal die aanvaarbaarheidsvlak van ontwikkelings-risiko bepaal.

8.5.8 Ouditwerk in 'n rekenaarinligtingstelselomgewing (SAOS 401)

Die doel van hierdie standpunt is om standaarde daar te stel en leiding te gee oor prosedures wat gevolg moet word wanneer 'n oudit in 'n rekenaar-inligtingstelselomgewing (RIS-omgewing) uitgevoer word.

Onder andere moet die uitwerking daarvan op beheermaatreëls en risiko in 'n e-handelsomgewing noukeurig bepaal word.

Die risiko's en die interne beheerkenmerke sluit onder meer in die gebrek aan transaksiespore, gebrek aan skeiding van funksies, die moontlikheid van foute en onreëlmatighede, die outomatiese uitvoering van transaksies en rekenaar-verwerkingsbeheer.

8.5.9 Risikobeoordeling en interne beheer – Rekenaarinligtingstelsel-kenmerke en -oorwegings (SAOS 4011)

Wanneer 'n entiteit 'n rekenaar van enige tipe of grootte gebruik in die verwerking van finansiële inligting, bestaan daar 'n rekenaarinligtingstelomgewing (RIS-omgewing). Kyk ook paragraaf .01 van SAOS 401 in hierdie verband.

Kenmerke soos die konsentrasie van funksies en kennis, konsentrasie van programme en data, afwesigheid van invoerdokumente, gebrek aan sigbare transaksiespoor, gebrek aan sigbare afvoer en maklike toegang tot data en rekenaarprogramme, moet sorgvuldig in ag geneem word, veral waar e-handel bedryf word. Beheermaatreëls vir toepassing-stelselontwikkeling en instandhoudingsbeheer, rekenaarwerkingsbeheer, stelselprogrammatuurbeheer, logiese toegangsbeheer, invoer- en afvoerbeheer, asook verwerking en beheer oor rekenaardatalêers, moet beoordeel en getoets word.

8.5.10 Gebruik van die werk van 'n kundige (SAOS 620)

'n Kundige kan deur die entiteit of ouditeur aangestel word, of in diens van hierdie partye wees.

Met die gebruik van e-handel moet die nodigheid en gebruik van kundiges in die RIS-omgewing en in die vertolking van ooreenkomste, wetgewing en regulasies, oorweeg word.

8.5.11 Suid-Afrikaanse Ouditpraktykstandpunte (SAOPS)

Die SAOPS (SAAPS) vorm nie deel van die standpunte van SAOS nie en beoog nie om die gesag van 'n standpunt van SAOS te hê nie.

Dit voorsien egter riglyne by die aanwending van standpunte van SAOS en behoort in ag geneem te word by die toepassing van standpunte van SAOS.

Aangesien e-handel elektronies geskied, óf as 'n besigheid, óf as 'n bemarkings- of aanskaffingskanaal, is dit van pas om tesame met SAOS 401 en SAOS 4011, ook die volgende SAOPS in ag te neem:

"IT Environments – Stand Alone Personal Computers" (SAOPS 1001)

"IT Environments – Online Computer Systems" (SAOPS 1002)

"IT Environments – Database Systems" (SAOPS 1003)

"Electronic Commerce – Effect on the Audit of Financial Statements" (SAOPS 1013)

Hierdie praktykstandpunt is volledig in paragraaf 8.3 van hierdie hoofstuk bespreek.

8.5.12 Die Kingverslag oor korporatiewe bestuur

Korporatiewe beheer is in 1994 in Suid-Afrika geïnstitusionaliseer deur middel van die Kingverslag.

Die Kingkomitee is in 1992 deur die Instituut van Direkteure gestig om korporatiewe beheer in Suid-Afrika te oorweeg.

Baie van die konsepte vervat in dié verslag is in wetgewing opgeneem. Dit sluit in arbeidsverhoudings (Wet 66 van 1995), basiese kondisies van indiensneming (Wet 76 van 1997), omgewingsbestuursake (Wet 107 van 1998), maatskappyereg (Wet 61 van 1973, soos gewysig), en ander sake.

Die Kingkomitee het in 2002 'n bygewerkte verslag uitgereik wat die een van 1994 vervang en dit sluit areas van ondersoek in wat die rekeningkunde en die ouditkunde oorweeg, asook op die gebied van interne oudit, beheer en risikobestuur.

Die nuwe verslag is saamgevat in Die Kode van Korporatiewe Praktyke en Gedrag ("The Code of Corporate Practices and Conduct") ("Kode").

Die Kode is eerstens van toepassing op alle maatskappye genoteer op die Johannesburgse Effektebeurs ("JSE Securities Exchange South Africa"), tweedens op banke, finansiële instellings en entiteite onder die Wet op Publieke Finansiebestuur (PFMA). Alle ander maatskappye behoort ook aandag te gee aan die aanwending van die Kode.

Paragraaf 3.1.4 van die Kode verwys spesifiek na risikobestuur en die beveiliging van inligting, asook die onderhou van wette en regulasies.

Paragraaf 3.1.5 verwys na verskeie areas van risiko's en sluit dié van operasionele en tegniese risiko in en dit word meer breedvoerig in Deel 2 van die Kode behandel.

Paragraaf 3.2.3 handel met risiko en interne beheer wat aansluit by paragraaf 4, naamlik Interne Ouditkunde. Hier word na die funksie en bestek daarvan verwys en die

standaarde deur die Instituut van Interne Ouditeure neergelê met spesifieke vermelding van die rekeningkunde en die ouditkunde in paragraaf 6.

Waar Deel 2 risikobestuur breedvoerig behandel, word interne oudit in Deel 3 behandel en verwys terug na risikobeheer en die identifisering, evaluering en bepaling van die omvang daarvan.

Deel 5 handel met die rol van rekeningkundige en ouditfunksies. Dit erken AARP en die daarstelling van ouditkomitees, en in hoofstuk 4 van die Kode word inligtingstegnologie breedvoerig bespreek. Elektroniese formasie van kontrakte, stawing en integriteit, verbruikersbeskerming, belasting en die regswerking word aangehaal met verwysing na die groenskrif oor e-handel.

Dit is belangrik dat die beheer rondom e-handel hierdie regulasies sal erken en insluit in beleidsdokumente wat inligtingstegnologie binne 'n onderneming reël.

Die Kode is tans slegs in Engels beskikbaar.

8.5.13 Maatskappyewet, Wet 61 van 1973 gewysig na Wet 35 van 2001

Die Maatskappyewet vervat in hoofstuk 11, artikel 284 tot artikel 309 daarvan, behels die rekeningkunde en openbaarmakingsvereistes.

Artikel 284 (1) (c) en (d) verwys na die dag-tot-dag-inligting wat rekeningkundig bygehou moet word. Dit sluit in alle kontant ontvang en betalings gemaak, die byhou van goedere gekoop en verkoop en die besonderhede van die verkopers en kopers.

Artikel 284 (2) bepaal dat rekeningkundige rekords per hand in gebinde vorm of enige ander vorm (elektronies), gehou mag word.

Die Maatskappyewet bepaal in artikel 300 (i) dat die ouditeur van 'n maatskappy sorg moet dra dat die beginsels van die algemeen aanvaarde rekeningkundige praktyk konsekwent toegepas is.

Skedule 4 van die Maatskappyewet sit die spesifieke vereistes vir die jaarliks- en interim finansiële state uiteen, asook vir voorlopige finansiële state en dit sluit dus ook e-handelstransaksies in.

E-handel vorm deel van dit wat nagekom moet word volgens die Maatskappyewet en kan nie uitgesluit word daarvan nie.

8.5.14 Internet rekeningkundige en ouditkundesake

Ernst & Young LLP, het gedurende Januarie 2000 'n interne riglyn uitgereik waarin rekeningkundige en ouditsake met betrekking tot die internet uitgelig is.

Die groei in die hoeveelheid ondernemings wat goedere en/of dienste oor die internet lewer, het veroorsaak dat daar 'n toename ontstaan het in sake rakende rekeningkundige hantering en gebruike.

Alhoewel baie van hierdie sake ooreenstem met dié wat nie-kuber-ondernemings raak, is dit die gereeldheid van die sake in 'n kuber-wêreld, wat dit meer prominent maak. Die sake is veral van toepassing op die internetondernemings wat geklassifiseer kan word as Internet-diensverskaffers (byvoorbeeld telefoon en TV-media), Internetpoort-ondernemings (byvoorbeeld die lewering van uitgebreide inligting op webtuistes, met gewoonlik 'n eie soekenjin), internethandels-ondernemings (doen besigheid slegs oor die internet) en ander verwante internetondernemings (is afhanklik van die sukses van internet om eie besigheid te groei).

Spesifieke transaksies wat na vore kom, is onder andere advertensie-ruilhandelstransaksies. Advertensie-ruilhandelstransaksies is daardie transaksies waar ondernemings op mekaar se webwerwe adverteer, nie teen vergoeding nie, maar om reikwydte te vergroot. Behoort daar 'n waarde op die gebruik as advertensiekoste geplaas te word en op die inkomste vir die uitverhuur van sulke spasie? Die konsensus is dat 'n redelike waarde op sulke inkomste en uitgawe geplaas moet word, indien dit bepaal kan word gebaseer op 'n onderneming se historiese praktyk vir die ontvangs van sulke inkomste of vergoeding van sulke uitgawes.

Indien sodanige praktyk nie bestaan nie, is die redelike waarde waarskynlik, zero. RE 000 en RE 111 behoort in ag geneem te word in die finale besluit by die hantering van hierdie spesifieke transaksie.

'n Tweede spesifieke transaksie is die ontwikkelingskoste van webwerwe. Dit sluit in die ontwikkeling van die sagteware om die webwerf te dryf, die populasie daarvan met inligting en hardeware-aankope.

Die koste aangegaan in die beplanningsfase behoort as 'n uitgawe hanteer te word. Koste vir webwerfsteun, byvoorbeeld lisensiegeld, behoort ook as 'n uitgawe hanteer te word oor die periode van die voordeel (RE 129).

Hardewarekoste behoort gekapitaliseer te word as 'n vaste bate en daarvolgens behandel te word (RE 129). Dit sal ook sodanige sagtewarekoste insluit. Die registrasie van die domeinnaam behoort gekapitaliseer te word en voldoen aan RE 128. Ook hier moet RE 000, RE 123, RE 128, RE 129 en die vertolking van standpunte 423 in ag geneem word in die rekeningkundige hantering van die transaksies.

Waar 'n ekwiteitsinstrument aangewend word vir die betaling van dienste of om ekwiteit in 'n verskafferondememing te verkry, moet RE 000 en die vertolking van standpunt 417 en RE 125 en RE 128 nagekom word.

Dit is duidelik, dat wat ookal spesifiek en uniek mag wees as gevolg van die rekeningkundige hantering van e-handelstransaksies, sulke transaksies noukeurig getoets moet word aan die hand van AARP met inagneming van SAOS.

8.5.15 Finansiële verslaggewing deur internetondernemings

Die AARP lê nie spesifiek riglyne neer vir internetondernemings nie.

Die definiëring van inkomste, die hantering van ruilhandel, die allokasie van waardes binne 'n kontrak vir die komponente daarvan, die behandeling van webwerfontwikkeling en implementeringskoste, die afskrif van ontasbare bates en klandisiewaarde, moet spesifiek geadresseer word.

Binne die raamwerk van AARP en SAOS is dit egter moontlik om aanbieding en hantering van die transaksies binne 'n internetonderneming te bepaal en dat spesifieke standpunte nie nodig is binne die AARP-verband om riglyne te verskaf nie (Coppin, 2001:17).

8.6 SAMEVATTING

Rekeningkundige beheer omvat die gebiede van die rekeningkunde en die ouditkunde. Die boekhouding en beheer van handgeskrewe transaksies en/of rekenaartransaksies behoort nie in wese te verskil nie.

Die uiteindelike sukses van handgeskrewe en/of rekenaarstelsels, lê in die beheermaatreëls wat ingestel is en toegepas word.

Dit is egter so dat rekenaarstelsels en veral geïntegreerde stelsels, 'n groter risiko teweeg bring en meer kundigheid nodig is om die effek van die vloei van transaksies te monitor en verstaan.

Hierin ontstaan die sukses van die verantwoording van e-handels-transaksies verantwoording alreeds by die opstel van strategieë vir die instel en aanvaarding van e-handel as deel van die besigheidstrategie.

Die koste spesifiek tot die beplanning, ontwikkeling en implementering van e-handel oor die internet, stel nuwe denke en uitdagings daar, maar val binne die raamwerk van gesonde rekeningkundige beheer soos neergelê in onder andere die AARP, SAOS en die JSB-reëls.

Die netwerkinfrastruktuur en die sekuriteit daar rondom, tesame met die beveiliging van inligting teen ongewenste toegang en korrupsie, staan nie afsonderlik van beheerreëlmaatreëls rondom rekeningkundige rekenaarstelsels nie. Hierdie saak is volledig in Hoofstuk 5 bespreek.

Rekenaarstelsels om rekeningkundige transaksies te verantwoord is nie nuut tot die e-handel nie, maar die laasgenoemde verhoog egter die moontlikheid van 'n groter toenemende aantal gebruikers van sulke stelsels en die moontlikheid van verhoogde

volumes van transaksies. Die integrasie van rekeningkundige stelsels met ander dissiplines binne die organisasie verhoog die risikovlakke vir korrupsie, bedrog en die akkuraatheid van inligting (databasis). Dit is hierdie spesifieke areas wat meer aandag en 'n hoër mate van interne beheer moet geniet.

'n Verhoogde risiko, verandering in die gebiede en vlakke van risiko, integriteit, stawing van inligting, integrasie van transaksies, betroubaarheid van inligting en stelsels, is insgelyks deel van veranderde besigheidsrisiko teweeg gebring deur e-handel. Beveiligde infrastrukture is fundamenteel om effektiewe sekuriteitsbeheermaatreëls daar te stel. Die sagteware wat die transaksies vir e-handel beheer en integreer met 'n onderneming se infrastruktuur staan in hierdie verband sentraal. Jeremy Waterman skryf in die "Sunday Times Business Times" van 2 November 1998 dat kundige sagteware gebruik moet word om hierdie unieke rekeningkundige uitdaging op te los. Vyf jaar later, bly hierdie stelling nog waar.

Daar moet gedurig aandag geskenk word aan die rekeningkundige en interne beheermaatreëls, die akkurate prosessering van transaksies, belasting, regswerking en regulasies, rekeningkundige beleid en of 'n onderneming nog voldoen aan die lopende saak begrip.

Dit is veral die feit dat e-handel oor die internet 'n globale netwerk is, wat aanleiding tot verhoogde risiko gee.

Verhoogde opleiding van rekenmeesters in inligtingstegnologie en die gebruik maak van deskundiges op hierdie gebied kan nie agterweë gelaat word nie.

HOOFSTUK 9

SLOT EN AANBEVELINGS

9.1 INLEIDING

Tradisioneel doen 'n gebruiker sake deur fisies 'n besigheid te besoek en per tjek, kontant of met 'n kredietkaart vir dienste of goedere te betaal, en verder geskied rekeningkundige inligting in sulke gevalle handgeskrewe of aflyn op rekenaars. Met die ontwikkeling van 'n beheer-en-kontrole-stelsel in 1964, genaamd RAND, word die weg gebaan vir die ontstaan van die internet en e-handel. Die "e" word 'n voorvoegsel vir baie nuwe maniere om handel, sake of besigheid oor die internet te doen.

Maar ongelukkig bring hierdie nuwe manier van handel doen ook sy eiesoortige probleme. Kliëntsagteware, datatransaksieprotokol, webbedienersagteware en die netwerkbediener se operasionele sagteware word kwesbaar teen aanslae van binne en buite, en hierin speel e-sekuriteit 'n belangrike rol om op 'n vertrouenswaardige manier kommunikasie en transaksies oor publieke en private netwerke te doen.

Aangesien e-handel geen grense het nie en handel nou internasionaal oor die internet kan plaasvind, word die jurisdiksie van waar handel plaasvind en die heffing van belasting, beide beginsels wat internasionaal oorweeg moet word. Hierdie en ander sake word in die groenskrif oor elektroniese handel bespreek, waarvan sommige sake in die Wet op Elektroniese Kommunikasie en Transaksies (Wet No. 25, 2002) vervat is.

Kennis van e-handel en die ontstaan van die internet, die daarstel van sekuriteit om veilige e-handelsgeleentheid te skep, die erkenning van internasionale regswerking en belasting, is alles van primêre belang om die rekeningkundige beheer in e-handel te verstaan en te evalueer.

Hierdie proefskrif behandel dan hierdie gebiede afsonderlik, aangesien dit deel vorm van suksesvolle rekeningkundige beheer al dan nie.

9.2 SAMEVATTENDE OORSIG

Die primêre doel van die navorsing was om die rekeningkundige beheer in elektroniese handel te kwantifiseer en riglyne daar te stel om deur middel van voldoende rekeningkundige beheer die risiko om elektronies handel te dryf, te minimaliseer.

Verdere doelstellings was om die begrip *rekeningkundige beheer* voor te stel nie net as die ten boek stel van transaksies deur middel van dubbelinskrywings-boekhouding nie, maar as 'n meer omvattende begrip.

Beide die primêre en verdere doelstellings van hierdie navorsing is vervul.

Die teorie van die rekeningkunde leer ons die ontwikkeling van die rekeningkunde nie 'n willekeurige prôses is nie, maar eerder 'n langsame proses behels om die regte benadering te kry wat 'n rekeningkundige oplossing vir 'n rekeningkundige probleem sal bied.

Die ontwikkeling van rekeningkundige beheer het oor eeue heen geskied en is vandag nog steeds toepaslik en geldig. Die ontstaan van e-handel verander nie die wese van rekeningkundige beheer nie, maar laat die ontwikkeling van spesifieke kontroles vir e-handel toe. Die sukses van e-handel sal afhang van die doeltreffendheid van hierdie rekeningkundige beheer en die mate van die integriteit en vertroue wat dit aan alle gebruikers wêreldwyd bied.

Elektroniese handel word omskryf as die gebruik van elektroniese netwerke om inligting uit te ruil in die verkoop van produkte en dienste, en vir die betaling daarvan. Dit is hierdie netwerke van prosesse wat rekeningkundig beheer moet word en waar nuwe kontroles ontwikkel, ingestel en toegepas moet word.

Sekuriteit in elektroniese handel is van kardinale belang en maak 'n wesentlike deel uit van die rekeningkundige beheer. Nie net moet dit besighede en gebruikers beskerm nie, maar ook vertroue by gebruikers skep sodat elektroniese handel suksesvol sal wees. Die risiko's en spesifieke sensitiewe areas wat beskerm moet word, is in Hoofstuk 5 bespreek.

Net soos e-handel deel vorm van 'n organisasie se toekomstige strategie en die sukses daarvan gedryf word deur die betrokkenheid van topbestuur, is die betrokkenheid van regerings belangrik om stabiliteit aan e-handel te gee. Dit is die grenslose openheid van die internet wat regsprobleme veroorsaak en besighede sien op na die reg om aan die een kant stabiliteit en konsekwentheid van voorspelbaarheid te skep en aan die ander kant effektiwiteit, buigsaamheid en reaksie. Privaatheid van inligting, eienaarskap, regsgeldigheid en aanspreeklikheid is 'n paar van die areas wat internasionaal aandag moet geniet en gesinkroniseer moet word. Wat veral bevraagteken word, is die afdwingbaarheid van jurisdiksie tussen partye.

Alhoewel daar ver gevorder is met die erkenning van databoodskappe, e-kontrakte en e-handtekeninge, is die Wet op Elektroniese Kommunikasie en Transaksies (Wet No. 25, 2002) nie rigied nie. Artikel 5 van die Wet vereis 'n nasionale e-strategie van drie jaar wat binne twee jaar voltooi moet word, en daar sal sekerlik gedurende hierdie proses sake na vore kom wat wysigings tot die Wet mag bring.

Seker een van die grootste uitdagings van e-handel is op die gebied van belasting. Die huidige belastingwette en dubbelbelastingsooreenkomste is opgestel voor die inwerkingtreding van e-handel en dit is moontlik 'n bedekte seën dat e-handel nog nie sy volle potensiaal bereik het nie en dat die volume van e-handel klein is, vergeleke met die totale internasionale handelsyfers. Alhoewel die groenskrif oor e-handel wel belasting bespreek, is dit nie vervat in Wet No. 25 van 2002 nie. Daar is dus nog tyd vir regerings om internasionale beginsels vir e-belasting daar te stel.

Met die inagneming van nuwe kontroles rondom die sekuriteit in e-handel, is dieselfde beginsels wat tradisioneel op baksteen-en-beton-ondernemings van toepassing is, eweneens van toepassing op e-handel. Rekenaars is 'n integrale deel van die rekeningkunde en met die koms van die internet is meer databasisse toeganklik vir gemagtigde gebruikers. Inligting moet beskerm word sodat akkurate inligting voorsien kan word in die verslagdoeningsproses en persoonlike inligting veilig is teen ongemagtigde toegang. In die evaluering van die totale risiko van 'n organisasie, is dit duidelik dat rekeningkundige beheer onder andere getoets word deur middel van tegnieke soos die CAAT's-program. Dit is dan noodsaaklik dat in die ouditering van die

rekenaaromgewing en in die e-handel-scenario, persone die nodige kennis en vaardigheid sal hê en gebruik sal maak van kundiges.

Deur te bly by die beginsels van gesonde rekeningkundige beheer, die nakoming van AARP, SAOS, die Maatskappyewet, die reëls van die Johannesburgse Effektebeurs, die Kode van Korporatiewe Praktyke en die nuwe Wet op Elektroniese Kommunikasie en Transaksies, kan die risikovlakke vir korrupsie en bedrog, asook die akkuraatheid van inligting verlaag word. Daar moet gedurig aandag geskenk word aan die rekeningkundige en interne beheermaatreëls, die akkurate prosessering van transaksies, belasting, regswerking en regulasies, rekeningkundige beleid en strategie, sodat nuwe uitdagings vroegtydig die hoof gebied kan word.

9.3 AANBEVELINGS

9.3.1 Regsgeldigheid

Alhoewel die Wet op Elektroniese Kommunikasie en Transaksies, Wet No. 25, 2002 sekere internasionale tendense soos die erkenning van die regskrag en regswerking van elektroniese handtekeninge en afkoelperiodes in ag neem, is daar ander aangeleenthede waaroor navorsing gedoen moet word en riglyne neergelê kan word.

Hierdie aangeleenthede verwys na onder andere die vraag rondom die regsafdwingbaarheid by die beskerming van persoonlike inligting en die internasionale vervolging van kubermisdadigers.

'n Ontleding en vergelyking van debatte gevoer in organisasies soos die OECD, die WTO en UNCITRAL, met die van wette wat internasionaal deur lande afgekondig word, kan bydra om 'n internasionale aanvaarbaarheid oor die aangeleentheid te bereik. Dit sou kon lei tot 'n internasionale e-hof!

9.3.2 Belasting in e-handel

Belasting in e-handel is tans seker dié area wat die minste aandag geniet in die uitbou van e-handel.

Navorsing op die gebied van belasting, met inagneming van dit wat reeds gedoen is deur die OECD, die WTO en die Tesourie Departement van die VSA, sal bydra tot die ontwikkeling van 'n belastingraamwerk wat regverdig is; nie net op individue nie, maar ook teenoor organisasies en teenoor lande. Só 'n raamwerk sal die verlies aan inkomste van regerings verhoed en belastingontduiking teenwerk.

9.3.3 Kennis en vaardigheid

Soos inligtingstegnologie die hoofmedia van besigheidstransaksies en inligting wêreldwyd word, is dit noodsaaklik dat organisasies 'n verhoogde bewustheid van die sensitiwiteit van inligting wat in hulle inligtingstegnologiestelsels gestoor is, ervaar en stappe doen om dit te beveilig teen diefstal, verlies, misbruik en spioenasie. Met die koms van rekenaars en inligtingstegnologie wat e-handel dryf, is dit belangrik dat die hulpmiddele wat beskikbaar is om 'n veilige milieu te skep, toegepas word.

Om dit te kan doen en om die toegepaste rekeningkundige beheer te kan evalueer, moet individue die nodige kennis en vaardigheid hê. Hierdie kennis en vaardigheid strek van topbestuur tot by die spesialiste in 'n organisasie. Voortdurende navorsing oor die mate waarin rekeningkundige beheer deel uitmaak van studierigtings sal bydra tot die sukses van organisasies en e-handel, asook vir die hele toekoms van e-handel.

BIBLIOGRAFIE

ANDERSON, B. 2000. The reality of e-Business. *Netmaster Africa*, 5(9):4.

APTEKER, R. 1998. Come on Banks, SET us up for real virtual buying. *Sunday times Business times*, July, 5.

AZBEL, I. 1998. Beware the back door security threat. *Netmaster Africa*, 3(11):22.

BENNETT, R. & LUBER, P. 1999. Securing the perimeter. *Computing SA*, 19(24):16.

BERMAN, M. 2002. Realities of E-Commerce teach costly but valuable lessons. *Business IT Africa*:2, March.

BHAGATTJEE, P. 2000. Law lags for Web-trade. *Sunday times business times,* Aug. 13.

BIDOLI, M. 1999. The switch to e-commerce. *Financial mail*, Jan. 15.

BIDOLI, M., McLEOD, D., MOKODITOA, T. & PLANTING, S. 2001. Laying down the Law. *Future company*, May, 11.

BREWER, G. 1998. Secure commerce. *Computer week*, 2nd Annual Global Information Security Survey, Nov. 9.

BROERS, R. The rules of business still apply. *Convergence*,1(1):78.

BRUCE, S. bruce@well.sf.ca.us. 2001. Short history of the Internet. *The magazine of fantasy and science fiction*, Feb. 1993. [E-pos aan:] Poggenpoel. A. (e-adres) Jul. 30.

BURGERS, P. 2001. Secure and Trusted environment. The Panacea for e-Business success. *Business IT Africa*, August 2001.

CHAMBERS, J. 2001. The 2nd Industrial Revolution: why the Internet changes everything. *Convergence*, 2(1).

COELHO, R. 2000. Insuring against risky (e) business. Webber Wentzel Bowens. *Brief No. 4.*

COLLIER, P. 1991. Using computers as management tools. (*In* WILLIAMS, B.C. & SPAUL, B.J. IT and Accounting. London : Chapman & Hall.)

CONNELL, N.A.D 1991. Artificial intelligence and Accounting. (*In* WILLIAMS, B.C. & SPAUL, B.J. IT and Accounting. London : Chapman & Hall.)

COPPIN, G. 2001. Financial reporting by Internet firms. *Accountancy S.A.*, 17, April.

CORREIA, C., FLYNN, D., ULIANA, E. & WORMALD, M. 1990. *Finansiële bestuur.* Kaapstad : Juta & Kie.

COURT, J.M. & MUGGRIDGE, N.J. 1991. Auditing and computers. (*In* WILLIAMS, B.C. & SPAUL, B.J. IT and Accounting. London : Chapman & Hall.

CROOK, B. The 10 golden rules of network security. *Secure IT*, 1(1):28.

DAVIES, G. 1998. E-Commerce is here to stay. *F & T Net*, 2(5):14, Sept.

DAVIS, B. 1998. In the certificates we trust. *Information week S.A.*, May 1998.

DE JONG, K. Sekuriteit is die grootste struikelblok. *F & T Net*, 4(5):58.

DEKKER, L.D. 1999. Hackers beware. *Computer week* 22(2):1, Jan. 25.

DROMS, W.G. 1990. Finance and accounting for non financial managers. Reading Mass : Addison-Wesley.

DU PLESSIS, B. 2001. E-commerce adds a new dimension. *Accountancy S.A.*, 15, Aug.

DU TOIT, G. (Prof) 2000. E-commerce and risk management. *The innovator*, May.

DU TOIT, J. 2000. Elektroniese handtekeninge kry groen lig in Amerika. *Sake Beeld,* Okt. 3.

DUMAS, H. 1998. Information security policy. Tech Republic, [Web:] www.techrepublic.com. [Date of access: 2001].

EDWARDS, J.R. 1989. A history of financial accounting. Wiltshire : Antony Rowe.

ELS, F. 2000. Internet: veiligheid die sleutel in e-Sake. *Finansies & tegniek*, 40, Jul. 7.

ESSILK, K., TORSTEN, B. & GUTH, R. 1998. Global e-Commerce waits for SET. *Computing S.A.*, 8, June 15.

FABRO, M. 2001. E-Security. *Fortune*, 143(2):3, Jan. 22.

FAUL, M.A., EVERINGHAM, G.K., REDELINGHUYS, H.F. & VAN VUUREN, L.M. 1989. Finansiële rekeningkunde. Durban : Butterworths.

FIRTH, D. 1999. E-Commerce needs a monitoring body. *Computing S.A.*, 19(24):32.

FRIEDLAND, R. 1999. Belasting op e-aandele transaksies. *Finansies en tegniek,* Junie, 4.

GEERTS, G. & McCARTHY, W.E. 1991. Database accounting systems. (*In*: WILLIAMS, B.C. & SPAUL, B.J. IT and Accounting. London : Chapman & Hall.)

GERMISHUYS, L.M. 1998. Network security: is your organization immune, prepared or protected? *Accounting SA*, Febr.

GHOSH, A.K. 1998. E-Commerce security: weak links, best defenses. New York : John Wiley & Sons.

GIBSON, K. 1998. Commerce takes to the Internet. *F & T Net*, 2(5):6, Sept.

GIBSON, K. 1999. SA maatskappye moet e-handelgolf ry. *F & T Net*, 3(4):4, Julie.

GORDON, G. 1998. E-Commerce eyes the consumer. *Sunday Times Metro*, July, 19.

GREEN, J. 2001. Overcoming the e-payment hurdle in B2B Commerce. *Network Times*, July 2001.

GREEN, J. 2001. Security goes beyond the firewall. *Business IT Africa*, March.

GREEN, J. 2001. Security still a major hurdle. *Business IT Africa*, August.

GREGORY, A. 1991. Management accounting and information technology. (*In*: WILLIAMS, B.C. & SPAUL, B.J. IT & Accounting. London : Chapman & Hall.)

GUNNING, E. 2001. E-Handel-wet staat se erns. *Rapport*, April, 29.

HANNAY, B. 2003. How it all began. *Accountancy*. Febr.

HARCOURT-COOKE, S. & FRYER, V. 1998. Computer fraud: risks and implications. *Accountancy S.A.*, May.

HARGREAVES, D. & EAGLESHAM, J. 2000. E-Commerce rule to be passed. *Business Day*, Nov, 15.

HARRIS, L. 2001. A threat and an opportunity. *Financial mail*, Nov. 30.

HEMBROUGH, J. 1997. Building a security policy is vital to protect assets. *F & T Net*, Bylae van Junie 1997.

HERDAN, D. 1998. Beyond the firewall. *Computer Week*, 2nd Annual Global Information Security Survey, Nov. 9

HIGGINS, M. 2000. Wake up call. *Fortune*, 142(2), Jul. 10. Special Advertising Section.

HOFFMAN, J., JOHNSTON, D., HANDA, S. & MORGAN, C. 1997. Cyberlaw. Cape Town : Ampersand Press.

HOQUE, F. Building the e-Enterprise: creating new business and technology Architectures. *Convergence*, 1(1):28.

HORN, A. 2002. Nuwe koers word ingeslaan: nou gaan e-handel oor sake. *Sake-Beeld*, Maart, 28.

HURLEY, J. 2001. Securing the e-Business. *Business IT Africa*, 56, Aug.

KATZ, C. 1998. Securing the stable door. *Foresight*, 1(3):6, Nov.

KEMP, R. 2001. The taxation of global electronic commerce under the new South African residence based tax system. *Leading,* Arthur Anderson newsletter. February/March 2001.

KOEN, P.G.W. 1999. The secret to e-commerce. *Computing SA.*, 19(24):42.

KOJIMA, O. 1995. Accounting history. Osaka : A.N. Offset Co.

KOPREWSKI, G. The electronic wallet. *Intelligence*, 5(2):22.

LAMBRECHTS, I.J. 1990. Finansiële Bestuur. Pretoria : Van Schaik.

LAMPERTI, F.A. & THURSTON, J.B. 1953. Internal auditing for management. New York : Prentice-Hall.

LASCELLES, D. 1999. So what if holes in the net let tax leak through. *Financial mail*, 29 January 1999, 152(3):20.

LAWRENCE, G. 2000. Doen dit ordentlik. *Finansies en tegniek*, 40, Sept. 29.

LAY, P. & STILL, R. 1987. Control and auditing of accounting information systems. Cape Town : Juta & Co.

LEECH, S.A. & MEPHAM, M.J. 1991. The Development of Matrix-based Accounting. (*In*: WILLIAMS, B.C. & SPAUL, B.J. IT and Accounting. London : Chapman & Hall.)

LEIB, J. 2000. SARS closes e-commerce loopholes. *Business day*, 1, Sept. 28.

LEVENSTEIN, E. 1999. When security fails. *Computing SA*, 19(24):36, Jun. 28.

LING, A. 1999. E-Handel bied geleenthede aan almal. *F & T Net*, 3(4):34, Jul. 4.

LOPEZ, R. 1998. Security in the connected enterprise. *Netmaster Africa*, 3(11):18, Nov.

LUDSKI, H. 2000. SARS gears up to tax income from e-commerce. *Sunday times business times*, Nov. 19.

MACGREGOR, K. (Prof). 1998. How secure is a secure system? *Netmaster Africa*, 3(11):27, Nov.

MACINTOSH, C. 1998. The Internet is a global marketplace minus global legislation. *Intelligence*, 12, Special Edition, 1998.

MARITZ, E. Mind your own e-business. *Convergence*, 2(2):166.

MARSHALL, B. 1999. Surfing the Problems? *Accountancy S.A.*, March 1999.

MATHEWS, M.R. & PERERA, M.H.B. 1996. Accounting theory & development. Melbourne : Nelson, a Thomson Publishing Co.

MAUTZ, R.K. & SHARAF, H.A. 1961. The philosophy of auditing. Florida : American Accounting Association.

MCLEOD, D. 1998. State's Cyberlaw plans unveiled. *Financial Mail*, Vol. 150 No. 7, 28 August 1998.

MITCHELL, M. 2000. IT's a Risk. *Accountancy*, 126(1288):44, Dec.

MONK, P. 1991. The Impact of IT on the economy. (*In*: WILLIAMS, B.C. & SPAUL, B.J. IT and Accounting. London : Chapman & Hall.)

MOSTERT, W. 2000. Tien fundamentele regsfaktore vir e-handel. *Finansies & Tegniek*, Okt. 6

NUNES, T. 1999. Tax holes in the webbing of the Net. *Financial mail*, 153(12):48, Jun. 15.

OLIVER, R.W. The seven laws of e-Commerce strategy. *The e-Strategist*, 1(111):10, Decision Processes International.

OLSSON, J. & DAVIES, G. 1998. E-Commerce in the Business World. *F & T Net*, Vol 2. No. 5, September 1998.

PARKES, W. 1999. Metodes om inligting te beskerm. *F & T Net*, 3(1), Januarie/Februarie 1999.

PIETERSE, G. 2000. Kuberkrakers: elektroniese handel loop kwaai deur. *Finansies & Tegniek*, Jul. 14.

PUTTICK, G. & VAN ESCH, S. 1998. The principles and practice of auditing. Kaapstad : Juta & Co.

QUARTERO, E. 1998. Tackling the e-Commerce security issues. *Netmaster Africa*, 3(11):26, Nov.

RATLIFF, R.L., WALLACE, W.A., SUMMERS, G.E., MCFARLAND, W.G. & LOEBBECKE, J.K. 1996. Internal auditing. Principles and Tecniques. Altamonte Springs : Institute of Internal Auditors.

RUTHVEN, J. 2000. 'n Losse benadering is moeilikheid soek. *Finansies en Tegniek*, Nov, 24.

SCHNEINER, B. 2000. Closing the windows of exposure. Counterpane internet security, Inc. 2000. [Web:] http://www.counterpane.com/window.html. [Date of access: 2000].

SION, J. Smartcards. *Secure IT*, Vol. 1 No. 1.

SMITH, R.E. 1997. Internet cryptography. USA : Addison Wesley Longman.

STONES, L. 1999. Beware the coming of the e-police. *Business day*. After Hours. 9-11 July 1999.

STONES, L. 2001. Delegates disagree about regulation of laws. *Business day*, April, 23.

TALBERG, J. 1998. Tax and the internet. *Brief No.* 1, August 1998 (Webber Wentzel Bowens).

TAYLOR, R. 1999. New threat to e-commerce. *Business day*, July, 28. (bladsy)

THE ECONOMIST. 2002. Inoculating the network. *The economist technology quarterly report*, 22nd June 2002.

THOMPSON, C. & HAYSON INC ATTORNEYS. 2001. *Internet Law* – The legal stuff.

TOBIN, P. 2001. The new face of online commerce. *Sunday times business times*, Nov. 15.

VAN ZYL, T. 1998. E-Commerce set to boom in S.A. *Business day survey*, Nov. 18.

VENTER, G. 1998. Certificates close security loopholes. *Netmaster Africa*, 3(11):28, Nov.

VENTER, G. 1998. Slimkaarte maak hulle buiging op die Internet. *F & T Net*, November 1998.

VENTER, G. 1999. Better security fundamental for increased e-commerce. *Computing S.A.*,19(24):36, Jun. 28.

VENTER, G. 1999. Sekuriteit verlig vrese vir e-handel. *F & T Net* Vol. 3 No. 4, Julie 1999.

VENTER, G. 2000. Hoe veilig is jy op die Internet? *F & T Net*, Desember 2000.

VICENTE, A. 2000. Don't get a lawyer, get a firewall. *Computer Week*, 23 October 2000.

VORSTER, Q., KOORNHOF, C., KOEN, M., OBERHOLSTER, J. & KOPPESCHOOR, Z. 2002. Beskrywende rekeningkunde. Durban : Butterworths.

WALKER, M. 1991. The information economics approach to financial reporting. (*In*: WILLIAMS, B.C. & SPAUL, B.J. IT and Accounting. London : Chapman & Hall.)

WEBSTER, E. 1998. Retail Technology. *Business Day Survey*, 5 October 1998.

WILLIAMS, B.C. & SPAUL, B.J. 1991. The impact of information technology. (*In* : IT and Accounting. London : Chapman & Hall.)

WILLIAMS, G. 1999. SA maatskappye moet e-handelgolf ry. *F & T Net*, 3(4):4, Jul. 4.

WILLIAMS, N. 1998. Integrating business with the supply chain. *Netmaster Africa,* 3(10), Oct.

WILLIAMS, N. 1998. Moving beyond e-commerce to e-business. *Accountancy SA,* May.

WILLIAMSON, D. 2003. Objectives of Accounting. [Web:] http//www.duncanwil.co.uk/objacc.html. [Date of access: 2003].

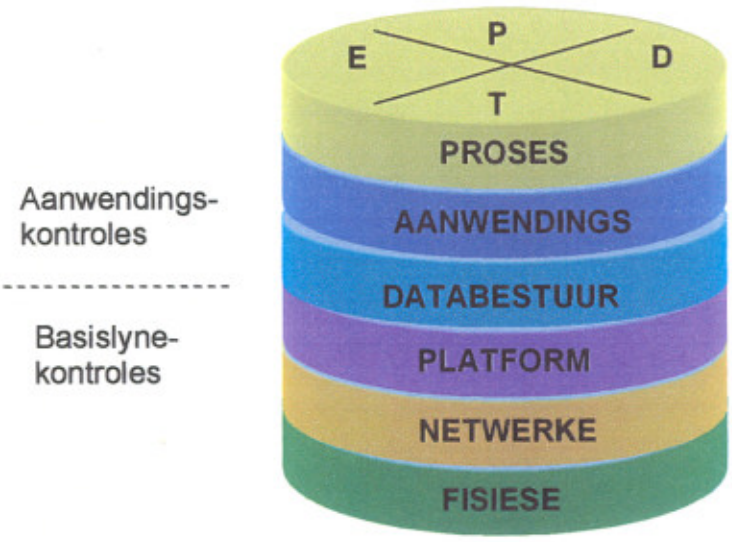
YAMEY, B.S. 1978. Essays on the history of accounting. New York : Arno Press.

BYLAAG 1

ELEKTRONIESE HANDEL: ONTWIKKELINGSPROSES

	1.1 Brosjure Ware	E-handel	E-besigheid	E-onderneming
Kultuur	Visioenêr, korporatief, tradisioneel	Chaos, .com mania, reaktiewe, individualistiese beheer, buitensporig	Besigheidsmodel gefokus, proaktief, proses ontwerp, samewerking, merknaam	Onderneming gefokus, interaktief, geïntegreerd, bemagtiging, kritieke doel
Mense	Tegnologiese fokus	Tegnologie en implementasie gefokus, hoë bekwaamheid	Proses/Ontwerp gefokus, kerngeskik	Analities/opbrengs gefokus, strategie georiënteer, kennis gebaseer
Besigheidsmodel	Inhoud vertoon	Inhoud aggregasie, waagkapitaal, oorspronklike publieke aanbod	Proses aggregasie, Hibride, konsolidasie	Mense aggregasie, integrasie, koöperatief, virtuele korporasies
Organisatoriese model	Konvensioneel	Funksie gefokus, geïsoleerd, uitvinder gedryf, binnenshuis	Kruis organisasie gefokus, gedesentraliseerd, e-besigheid gedryf, buitebronne	Uitgebreide onderneming gefokus, meewerkend, van bo aangespoor, buitebronnevennootskappe
Aanwendingsmodel	Webwerf gebaseer	Besigheid-tot-gebruiker (B2C) gefokus aanlyn vir tasbare goedere	Besigheid-tot-Besigheid (B2B) aankoop, B2B-gemeenskappe, intellektuele goedere, B2C-vendusies	Kritieke doelaanwendings vir unieke besigheidsprosesse
Bestuursproses	Produk, verkope aangedrewe	Situasie gedryf, projek georiënteerd, ongebonde	Proses gedryf, program georiënteerd, verbonde	Metode/Model/ opbrengs aangedryf, onderneming oplossing georiënteerd, geïntegreerd en uitgebrei
Tegnologie	Staties	Katalisator, kliënt gedryf, uniek	Dryfkrag, rekenaarbediener aangedryf, aanvaarbaar	Helpende, netwerk gedrewe en gedistribueerde kommoditeit

INLIGTINGSSEKURITEITRAAMWERK



P – Strategie en Beleid
D – Beheerde Ontplooiing
E – Monitor Voorvalle
T – Tegnologiese Argitektuur

Die Inligtingsekuriteitraamwerk beskryf die verhouding en risiko tussen die verskeie besigheidskomponente wat enige besigheidsproses ondersteun.

Die afwesigheid van, of onvoldoende sekuriteit mag die totale teenwoordigheid van sekuriteit ongeldig maak.

FISIESE Hierdie laag verwys na die manier waarop fisiese toegang beperk is.

NETWERKE Dit is die stappe wat gedoen is om ongemagtigde toegang daartoe te beperk en verwys na die konfigurasie van netwerk-sekuriteitskomponente, soos byvoorbeel brandmure.

PLATFORM Dit verwys na die veiligheidskonfigurasie van die operasionele stelsel.

DATABESTUUR Hierdie laag hou verband met die implementering van toegangskontroles oor dataléers of databasisse, asook na interne datastoring en transmissie.

AANWENDINGS Dit hou verband met die konfigurasie en funksionaliteit van enige spesifieke aanwendingspakket. Dit bevat onder andere gebruikersname en wagwoorde.

PROSESSE Dit verwys na die besigheidsprosesse en sekuriteit daar rondom.

BYLAAG 3

MODEL VAN DIE ASSOSIASIE VIR KANADESE STANDAARDE OOR DIE BEVEILIGING VAN PERSOONLIKE INLIGTING

Die Assosiasie vir Kanadese Standaarde, het 'n model ontwikkel om persoonlike inligting te beskerm. Die tien beginsels om besighede te help om die skending van privaatheid te beheer, is:

VERANTWOORDELIKHEID

'n Organisasie is verantwoordelik vir die persoonlike inligting onder sy beheer en moet 'n individu aanwys wat verantwoordelik is vir die nakoming van die volgende beginsels.

IDENTIFISERINGSDOEL

Die doel waarvoor persoonlike inligting versamel word, sal deur die organisasie geïdentifiseer word tydens of voordat die inligting bekom word.

TOESTEMMING

Die wete en toestemming van die individu is nodig vir die insameling, gebruik of openbaarmaking van persoonlike inligting, behalwe waar dit onvanpas is.

BEPERKTE VERSAMELING

Die versameling van persoonlike inligting sal beperk word tot dit wat benodig word vir die doel geïdentifiseer deur die organisasie. Inligting sal deur regverdige en wettige metodes versamel word.

BEPERKINGE, GEBRUIK, OPENBAARMAKING EN RETENSIE

Persoonlike inligting sal beperk word tot wat nodig is vir die doel deur die organisasie geïdentifiseer.

AKKURAATHEID

Persoonlike inligting sal so akkuraat, volledig en op datum wees, as wat nodig is vir die doel waarvoor dit gebruik word.

BEVEILIGING

Persoonlike inligting sal beskerm word deur veiligheidsmaatreëls, toepaslik volgens die sensitiwiteit van die inligting.

OPENHEID

'n Organisasie sal geredelik spesifieke inligting aan individue bekendmaak ten opsigte van sy beleid en praktyke met betrekking tot die bestuur van persoonlike inligting.

INDIVIDUELE TOEGANG

Indien versoek, sal 'n individu ingelig word van die bestaan, gebruik en openbaarmaking van sy of haar persoonlike inligting en toegang daartoe verkry.

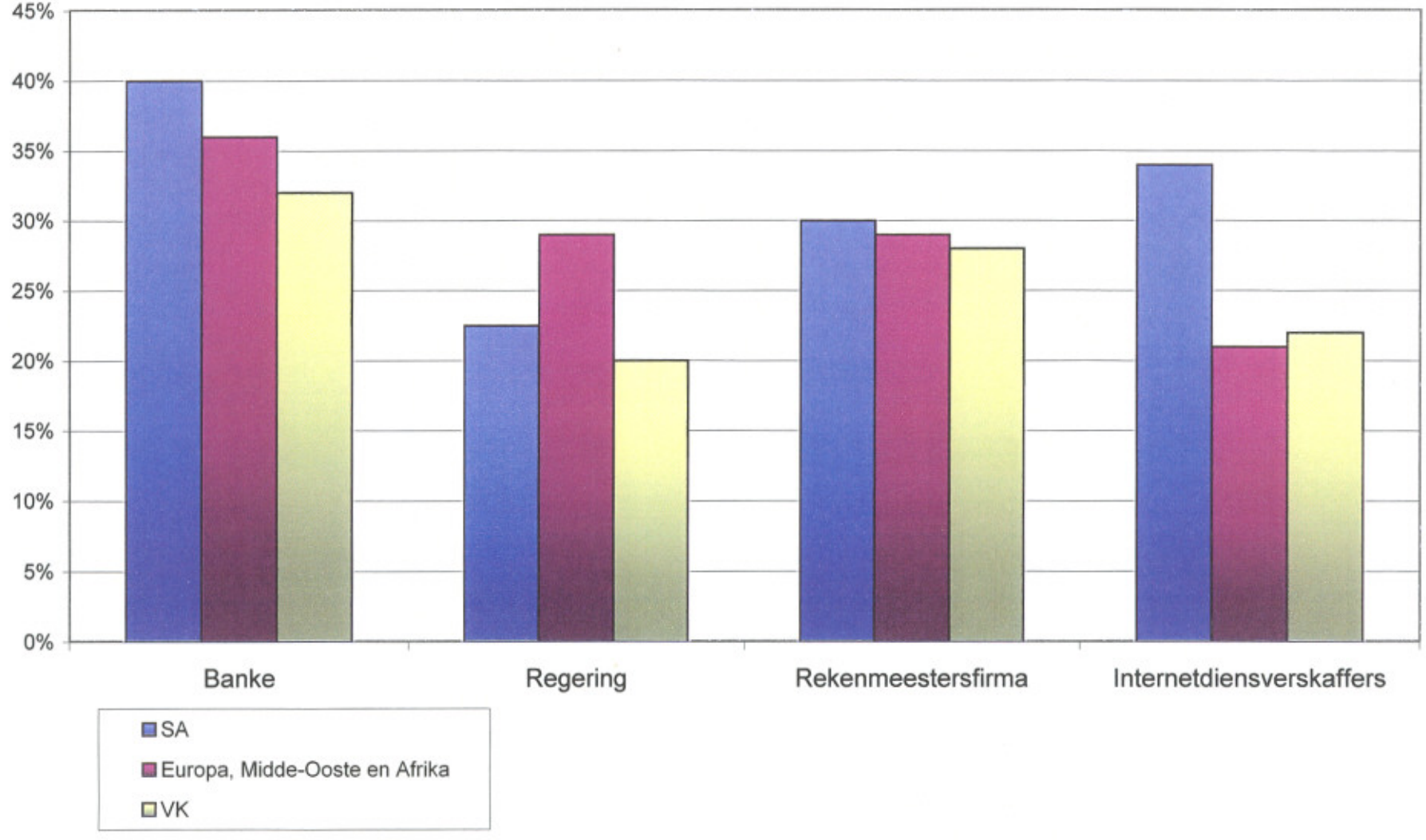
'n Individu mag die akkuraatheid en volledigheid van die inligting betwis en dit paslik wysig.

UITDAGING TEN OPSIGTE VAN NAKOMING

'n Individu mag 'n uitdaging rig ten opsigte van die nakoming van bogenoemde beginsels.

(Hoffman *et al.*, 1997: 50-60.)

VERTROUE IN ORGANISASIES



Bylaag 4

WET OP ELEKTRONIESE KOMMUNIKASIE EN TRANSAKSIES 25 VAN 2002

[GOEDGEKEUR OP 31 JULIE 2002] [DATUM VAN INWERKINGTREDING: 30 AUGUSTUS 2002]

(Engelse teks deur die President geteken)

WET

Om voorsiening te maak vir die vergemakliking en regulering van elektroniese kommunikasies en transaksies; om voorsiening te maak vir die ontwikkeling van 'n nasionale e-strategie vir die Republiek; om universele toegang tot elektroniese kommunikasies en transaksies en die gebruik van elektroniese transaksies deur KMMO's te bevorder; om voorsiening te maak vir mensehulpbronontwikkeling met betrekking tot elektroniese transaksies; om misbruik van inligtingstelsels te verhinder; om die gebruik van e-regeringsdienste aan te moedig; en om voorsiening te maak vir verwante aangeleenthede.

INDELING VAN ARTIKELS

Artikels

Deel 1
Regsvereistes vir databoodskappe

Deel 2
Kommunikering van databoodskappe

HOOFSTUK IV
E-REGERINGSDIENSTE

HOOFSTUK V
KRIPTOGRAFIEVERSKAFFERS

HOOFSTUK VI
WAARMERKINGSDIENSVERSKAFFERS

Deel 1
Akkreditasie-owerheid

Deel 2
Akkreditasie

HOOFSTUK VII
VERBRUIKERSBESKERMING

HOOFSTUK VIII
BESKERMING VAN PERSOONLIKE INLIGTING

HOOFSTUK IX
BESKERMING VAN KRITIEKE DATABASISSE

HOOFSTUK X
DOMEINNAAMOWERHEID EN ADMINISTRASIE

Deel 1
Instelling en inlywing van .za-Domeinnaamowerheid

Deel 2
Bestuur en personeel van Owerheid

HOOFSTUK XIII
KUBERMISDAAD

HOOFSTUK XIV
ALGEMENE BEPALINGS

HOOFSTUK I
UITLEG, OOGMERKE EN TOEPASSING (aa 1-4)

1 Woordomskrywing

In hierdie Wet, tensy uit die samehang anders blyk, beteken-

'administrateur van kritieke databasis' die persoon verantwoordelik vir die bestuur en beheer van 'n kritieke databasis;

'bewaarplek' die primêre register van die inligting wat deur 'n registrasiekantoor bygehou word;

'data' elektroniese voorstellings van inligting in enige formaat;

'databoodskap' data wat op elektroniese wyse voortgebring, gestuur, ontvang of geberg word, en sluit in-

(a) stem, waar die stem in 'n geoutomatiseerde transaksie gebruik word; en

(b) 'n rekord wat geberg word;

'datakontroleur' 'n persoon wat persoonlike inligting vanaf of ten opsigte van 'n datasubjek versoek, versamel, vergelyk, prosesseer of berg;

'datasubjek' 'n natuurlike persoon van wie of ten opsigte van wie persoonlike

inligting na die inwerkingtreding van hierdie Wet versoek, ingesamel, vergelyk, geprosesseer of geberg word;

'Departement' die Departement van Kommunikasiewese;

'derde party' met betrekking tot 'n diensverskaffer, 'n intekenaar op die diensverskaffer se dienste of enige ander gebruiker van die diensverskaffer se dienste of 'n gebruiker van inligtingstelsels;

'deurblaaiprogram' ('browser') 'n rekenaarprogram wat 'n persoon in staat stel om databoodskappe met hiperskakels te lees;

'Direkteur-generaal' die Direkteur-generaal van die Departement;

'domeinnaam' 'n alfa-numeriese benaming wat geregistreer of toegewys is ten opsigte van 'n elektroniese adres op die Internet;

'domeinnaamstelsel' 'n stelsel om domeinname na IP-adresse of ander inligting om te skakel;

'DTP' ('WAP') draadlose toepassingsprotokol, 'n oop internasionale standaard wat deur die 'Wireless Application Protocol Forum Limited', 'n maatskappy wat ingevolge die wette van die Verenigde Koninkryk ingelyf is, ontwikkel is vir toepassings wat draadlose kommunikasie gebruik, en sluit Internettoegang vanaf 'n mobiele telefoon in;

'elektroniese agent' 'n rekenaarprogram of 'n elektroniese of ander ge-outomatiseerde middel wat onafhanklik gebruik word om 'n handeling te begin of om in die geheel of gedeeltelik op databoodskappe of prestasies in 'n geoutomatiseerde transaksie te reageer;

'elektroniese kommunikasie' 'n kommunikasie deur middel van databoodskappe;

'elektroniese handtekening' data wat aangeheg of geïnkorporeer word by, of logies geassosieer word met ander data en wat deur die gebruiker bedoel is om as 'n handtekening te dien;

'e-pos' elektroniese pos, 'n databoodskap wat in 'n elektroniese kommunikasie gebruik word, of bedoel is om gebruik te word, as 'n posboodskap tussen die opsteller en die geadresseerde;

'e-regeringsdienste' enige openbare diens wat op elektroniese wyse deur enige openbare liggaam in die Republiek gelewer word;

'geadresseerde', ten opsigte van 'n databoodskap, 'n persoon wat deur die opsteller bedoel is om die databoodskap te ontvang, maar nie 'n persoon wat as tussenganger ten opsigte van daardie databoodskap optree nie;

'geoutomatiseerde transaksie' 'n elektroniese transaksie wat in geheel of gedeeltelik aangegaan of verrig is deur middel van databoodskappe waarin die gedrag of databoodskappe van een party of beide partye nie deur 'n natuurlike persoon hersien word in die gewone loop van sodanige natuurlike persoon se besigheid of werk nie;

'geregistreerde' 'n aansoeker om of houer van 'n domeinnaam;

'gevorderde elektroniese handtekening' 'n elektroniese handtekening wat ontstaan uit 'n proses wat deur die Owerheid geakkrediteer is, soos bepaal in artikel 37;

'hiperskakel' 'n verwysing of skakel vanaf 'n punt in een databoodskap wat 'n deurblaaiprogram of ander tegnologie of funksionaliteit verwys na 'n ander databoodskap of punt daarin, of na 'n ander plek in dieselfde databoodskap;

'IKTNN' ('ICANN') die Internet-korporasie vir Toegewese Name en Nommers, 'n Kalifornies openbarebelangvereniging sonder winsbejag wat ingevolge die wette van die staat van Kalifornië in die Verenigde State van Amerika in die lewe geroep is;

'inligtingstelsel' 'n stelsel om databoodskappe voort te bring, te stuur, te ontvang, te berg, te vertoon of andersins te prosesseer, en sluit die Internet in;

'inligtingstelseldienste' ook die verskaffing van verbindings, die bedryf van fasiliteite vir inligtingstelsels, die verskaffing van toegang tot inligtingstelsels, die uitsending of roetering van databoodskappe tussen punte wat deur 'n gebruiker gespesifiseer word, en die prosessering en berging van data op die individuele versoek van die ontvanger van die diens;

'Internet' die onderling verbinde stelsel van netwerke wat rekenaars oor die wêreld deur gebruikmaking van die OBP/IP verbind en sluit toekomstige weergawes daarvan in;

'IP-adres' beteken die nommer wat die koppelingspunt van 'n rekenaar of ander toestel met die Internet aanwys;

'kasgeheue' hoë-spoedgeheue wat data vir relatief kort tydperke, onder rekenaarbeheer, berg ten einde versending en prosessering van data te versnel;

'KMMO's' ('SMMEs') Klein, Medium en Mikro Ondernemings soos beoog in die Bylaes by die Kleinsake Ontwikkelingswet, 1996 (Wet 102 van 1996);

'kriptografiediens' 'n diens wat gelewer word aan 'n afsender of 'n ontvanger van 'n databoodskap of aan enigeen wat 'n databoodskap berg, en wat ontwerp is om die gebruik van kriptografiese tegnieke te vergemaklik ten einde-

(a) te verseker dat slegs sekere persone toegang tot sodanige data of

databoodskap kan verkry of dit in 'n verstaanbare vorm kan plaas;

(b) te verseker dat die egtheid of integriteit van die data of databoodskap vasgestel kan word;

(c) die integriteit van die data of databoodskap te verseker; of

(d) te verseker dat die oorsprong van die data of databoodskap korrek vasgestel kan word;

'kriptografieproduk' 'n produk wat gebruik maak van kriptografiese tegnieke en deur 'n afsender of ontvanger van databoodskappe gebruik word ten einde-

(a) te verseker dat slegs relevante persone toegang tot sodanige data kan verkry;

(b) die egtheid van die data te verseker;

(c) die integriteit van die data te verseker; of

(d) te verseker dat die oorsprong van die data korrek vasgestel kan word;

'kriptografieverskaffer' 'n persoon wat kriptografiese dienste of produkte in die Republiek verskaf of voornemens is om dit te verskaf;

'kritieke data' data wat ingevolge artikel 53 deur die Minister verklaar word van belang vir die beskerming van die nasionale veiligheid van die Republiek of die ekonomiese en maatskaplike welsyn van sy burgers te wees;

'kritieke databasis' 'n versameling kritieke data in elektroniese vorm, waar toegang daartoe verkry kan word, of vanwaar dit gereproduseer of onttrek kan word;

'kuberinspekteur' 'n inspekteur in Hoofstuk XII bedoel;

'lkTVD' ('ccTLD') landskode-topvlakdomein van die Internet se domeinnaamstelsel wat ooreenkomstig die tweeletterkodes in die Internasionale Standaard ISO 3166-1 (Kodes vir Naamvoorstellings van Lande en hul Onderverdeling), toegewys is;

'Minister' die Minister van Kommunikasie;

'OBP/IP' ('TCP/IP') die Oorsendingsbeheerprotokol/Internetprotokol wat deur 'n inligtingstelsel gebruik word om met die Internet te verbind;

'openbare liggaam'-

(a) enige staatsdepartement of administrasie in die nasionale of provinsiale sfeer van regering of enige munisipaliteit in die plaaslike sfeer van regering; of

(b) enige ander funksionaris of instelling wanneer dit-

(i) 'n bevoegdheid uitoefen of plig uitvoer ingevolge die Grondwet, of 'n provinsiale grondwet;

(ii) 'n bevoegdheid uitoefen of 'n werksaamheid verrig ingevolge enige wetgewing;

'opsteller' 'n persoon deur wie, of ten behoewe van wie, 'n databoodskap voorgee om gestuur of voortgebring te wees voor berging, indien wel, maar sluit nie 'n persoon in wat as 'n tussenganger ten opsigte van daardie databoodskap optree nie;

'Owerheid' beteken die .za-Domeinnaamowerheid;

'persoon' ook 'n openbare liggaam;

'persoonlike inligting' inligting aangaande 'n herkenbare individu, met inbegrip van, maar nie beperk nie tot-

(a) inligting wat verband hou met die ras, geslagtelikheid, geslag, swangerskap, huwelikstaat, nasionale, etniese of sosiale herkoms, kleur, seksuele georiënteerdheid, ouderdom, fisiese of geestesgesondheid, welsyn, gestremdheid, godsdiens, gewete, oortuiging, kultuur, taal en geboorte van die individu;

(b) inligting wat verband hou met die opvoeding of die mediese, kriminele of werksgeskiedenis van die individu of inligting in verband met finansiële transaksies waarby die individu betrokke was;

(c) enige identifiserende nommer, simbool, of ander besonderheid wat aan die individu toegeken is;

(d) die adres, vingerafdrukke of bloedgroep van die individu;

(e) die persoonlike menings, beskouings of voorkeure van die individu, behalwe waar dit gaan om 'n ander individu of aangaande 'n voorstel vir 'n toewysing, 'n toekenning of 'n prys wat aan 'n ander individu toegeken staan te word;

(f) korrespondensie wat deur die individu gestuur is wat implisiet of eksplisiet van 'n private en vertroulike aard is of verdere korrespondensie wat die inhoud van die oorspronklike korrespondensie sou openbaar;

(g) die beskouinge of menings van 'n ander individu aangaande die individu;

(h) die beskouinge of menings van 'n ander individu aangaande 'n voorstel vir 'n toewysing, 'n toekenning of 'n prys wat aan die individu gedoen staan te word, maar met uitsluiting van die naam van die ander individu waar dit saam met die beskouinge of menings van die ander individu verskyn; en

(i) die naam van die individu waar dit verskyn tesame met ander persoonlike inligting wat betrekking het op die individu of waar die openbaarmaking van die naam self inligting aangaande die individu sal ontbloot,

maar sluit inligting aangaande 'n individu wat reeds meer as 20 jaar gelede oorlede is, uit;

'private liggaam'-

(a) 'n natuurlike persoon wat enige nering, besigheid of professie bedryf of bedryf het, maar slegs in daardie hoedanigheid;

(b) 'n vennnootskap wat enige nering, besigheid of professie bedryf, of dit bedryf het; of

(c) enige voormalige of bestaande regspersoon,

maar nie 'n openbare liggaam nie.

'registrasiekantoor' 'n entiteit wat deur die Owerheid gelisensieer is om 'n spesifieke subdomein te bestuur en te administreer;

'registrateur' 'n entiteit wat deur die Owerheid gelisensieer is om 'n bewaarplek by te hou;

'sertifiseringsdiensverskaffer' 'n persoon wat 'n waarmerkingsproduk of -diens verskaf in die vorm van 'n digitale sertifikaat geheg aan, ingelyf by of logies geassosieer met 'n databoodskap;

'subdomein' enige onderafdeling van die .za-domeinnaamruimte wat op die tweedevlakdomein begin;

'transaksie' 'n transaksie van hetsy 'n kommersiële of nie-kommersiële aard, wat die verskaffing van inligting en e-regeringsdienste insluit;

'tuisblad' die primêre toegangspunt-webbladsy van 'n webwerf;

'tussenganger' 'n persoon wat ten behoewe van 'n ander persoon, hetsy as agent al dan nie, 'n bepaalde databoodskap stuur, ontvang of berg of ander dienste ten opsigte

van daardie databoodskap lewer;

'TVD' ('TLD') in topvlakdomein van die domeinnaamstelsel;

'tweedevlakdomein' die subdomein of wat onmiddellik volg onder die lkTVD;

'universele toegang' toegang tot Internetverbinding en elektroniese transaksies deur alle burgers van die Republiek;

'verbruiker' 'n natuurlike persoon wat 'n elektroniese transaksie met 'n verskaffer aangaan of wil aangaan as eindgebruiker van die goedere of dienste wat deur daardie verskaffer aangebied word;

'Verbruikersakekomitee' die Verbruikersakekomitee ingestel deur artikel 2 van die Wet op Verbruikersake (Onbillike Sakepraktyke), 1988 (Wet 71 van 1988);

'voorskryf' by regulasie kragtens hierdie Wet voorskryf;

'waarmerkingsprodukte of -dienste' produkte of dienste wat ontwerp is om die houer van 'n elektroniese handtekening aan ander persone te identifiseer;

'waarmerkingsdiensverskaffer' 'n persoon wie se waarmerkingsprodukte of -dienste deur die Akkreditasie-owerheid geakkrediteer is kragtens artikel 37 of erken word kragtens artikel 40;

'webbladsy' 'n databoodskap op die Wêreldwye Web;

'webwerf' enige plek op die Internet wat 'n tuisblad of webbladsy bevat;

'Wêreldwye Web' beteken 'n raamwerk om inligting te lees wat 'n gebruiker toelaat om inligting wat op 'n veraf rekenaar gebêre word op te spoor en toegang daartoe te verkry en om verwysings vanaf een rekenaar te volg na verwante inligting op 'n ander rekenaar;

'.za-domeinnaamruimte' die .za-lkTVD wat aan die Republiek toegewys is ooreenkomstig die tweeletterkodes in die Internasionale Standaard ISO 3166-1.

2 Oogmerke van Wet

Die oogmerke van hierdie Wet is om in die openbare belang elektroniese kommunikasie en transaksies moontlik te maak en te vergemaklik, en om vir daardie doel-

(a) die belang van die inligtingsekonomie vir die ekonomiese en maatskaplike voorspoed van die Republiek te erken;

(b) universele toegang te bevorder veral in gebiede wat ondervoorsien is;

(c) begrip vir, aanvaarding van en groei in die getal elektroniese transaksies in die Republiek te bevorder;

(d) versperrings tot elektroniese kommunikasies en transaksies in die Republiek te verwyder en te voorkom;

(e) regsekerheid en vertroue ten opsigte van elektroniese kommunikasies en transaksies te bevorder;

(f) tegnologiese neutraliteit by die toepassing van wetgewing op elektroniese transaksies te bevorder;

(g) e-regeringsdienste en elektroniese kommunikasies en transaksies met openbare en private liggame, instellings en burgers te bevorder;

(h) te verseker dat elektroniese transaksies in die Republiek aan die hoogste internasionale standaarde voldoen;

(i) belegging en innovering ten opsigte van elektroniese transaksies in die Republiek aan te moedig;

(j) 'n veilige, geborge en effektiewe omgewing vir die verbruiker, sakewêreld en die Regering te ontwikkel om elektroniese transaksies te bedryf en te gebruik;

(k) die ontwikkeling van elektroniesetransaksiedienste te bevorder wat gehoor gee aan die behoeftes van gebruikers en verbruikers;

(l) te verseker dat, met betrekking tot die verskaffing van elektroniese-transaksiedienste, die spesiale behoeftes van besondere gemeenskappe en gebiede en van gestremdes behoorlik in ag geneem word;

(m) nakoming van aanvaarde internasionale tegniese standaarde by die verskaffing en ontwikkeling van elektroniese kommunikasies en transaksies te verseker;

(n) die stabiliteit van elektroniese transaksies in die Republiek te bevorder;

(o) die ontwikkeling van menslike hulpbronne in die omgewing van elektroniese transaksies te bevorder;

(p) KMMO's binne die omgewing van elektroniese transaksies te bevorder;

(q) effektiewe gebruik en bestuur van die .za-domeinnaamruimte te verseker;

en

(r) te verseker dat die nasionale belang van die Republiek nie deur die gebruik van elektroniese kommunikasies in gevaar gestel word nie.

3 Uitleg

Hierdie Wet mag nie so uitgelê word dat dit enige statutêre reg of die gemenereg daarvan uitsluit om toegepas te word op, of om erkenning of akkommodasie te verleen aan elektroniese transaksies, databoodskappe of enige ander aangeleentheid waarvoor in hierdie Wet voorsiening gemaak word nie.

4 Toepassingsfeer

(1) Behoudens enige bepaling tot die teendeel in hierdie artikel, is hierdie Wet van toepassing ten opsigte van enige elektroniese transaksie of databoodskap.

(2) Niks in hierdie Wet word so uitgelê-

(a) dat dit van 'n persoon vereis om enige inligting, dokument of handtekening deur of in elektroniese formaat voort te bring, te kommunikeer, te toon, te prosesseer, te stuur, te ontvang, aan te teken, te behou, te berg of te vertoon nie; of

(b) dat dit 'n persoon verbied om vereistes te stel ten opsigte van die wyse waarop daardie persoon databoodskappe sal aanvaar nie.

(3) Die artikels van hierdie Wet wat in Kolom B van Bylae 1 genoem word, is nie van toepassing op die wette wat in Kolom A van daardie Bylae genoem word nie.

(4) Hierdie Wet moet nie uitgelê word asof dit geldigheid verleen aan enige transaksie wat in Bylae 2 genoem word nie.

(5) Hierdie Wet beperk nie die werking van enige wet wat uitdruklik die gebruik van databoodskappe magtig, verbied of reël nie, met inbegrip van enige vereiste van of ingevolge 'n wet, dat inligting op 'n besondere manier geplaas of vertoon moet word, of dat enige inligting of dokument op 'n besondere wyse versend moet word.

HOOFSTUK II
MAKSIMERING VAN VOORDELE EN BELEIDSRAAMWERK (aa 5-10)

Deel 1
Nasionale e-strategie (aa 5-9)

5 Nasionale e-strategie

(1) Die Minister moet binne 24 maande na die promulgering van hierdie Wet 'n driejaar- nasionale e-strategie vir die Republiek ontwikkel, wat aan die Kabinet vir goedkeuring voorgelê moet word.

(2) Die Kabinet moet, by aanvaarding van die nasionale e-strategie, die implementering van die nasionale e-strategie tot 'n nasionale prioriteit verklaar.

(3) Die Minister, by die ontwikkeling van die nasionale e-strategie soos beoog in subartikel (1)-

(a) moet alle sake in verband met e-regeringsdienste bepaal in oorleg met die Minister vir die Staatsdiens en Administrasie;

(b) moet die rolle van elke persoon, entiteit of sektor by die implementering van die nasionale e-strategie bepaal;

(c) moet as die verantwoordelike Minister optree om die implementering van die nasionale e-strategie te koördineer en te moniteer;

(d) kan die ondersoeke onderneem wat hy of sy nodig mag ag;

(e) kan navorsing onderneem en op hoogte bly met ontwikkelinge wat verband hou met elektroniese kommunikasies en transaksies in die Republiek en internasionaal;

(f) moet deurentyd die mate waarin die oogmerke van die nasionale e-strategie bereik is, beskou en evalueer;

(g) kan skakel, oorleg pleeg en saamwerk met openbare liggame, die privaatsektor of enige ander persoon; en

(h) kan, in oorleg met die Minister van Finansies, deskundiges en ander konsultante aanstel op die voorwaardes wat die Minister bepaal.

(4) *(a)* Die Minister moet, in oorleg met ander lede van die Kabinet, onderwerpe wat in die nasionale e-strategie behandel moet word, en die beginsels wat die implementering van so 'n onderwerp moet beheer, bepaal;

(b) Voordat enige onderwerp en beginsels waarvoor in paragraaf *(a)* voorsiening gemaak word, voorgeskryf word, moet die Minister by kennisgewing in die *Staatskoerant* kommentaar van alle belanghebbende partye versoek en enige kommentaar wat ontvang word, oorweeg.

(c) Die nasionale e-strategie moet, onder andere, uiteensit-

(i) die elektroniesetransaksiestrategie van die Republiek, met onderskeiding

tussen regionale, nasionale, kontinentale en internasionale strategieë;

(ii) programme en middele om universele toegang, mensehulpbronontwikkeling en ontwikkeling van KMMO's waarvoor in hierdie Deel voorsiening gemaak word, te bereik;

(iii) programme en middele om die algehele gereedheid van die Republiek ten opsigte van elektroniese transaksies te bevorder;

(iv) wyses om die Republiek as 'n voorkeurverskaffer en -gebruiker van elektroniese transaksies in die internasionale mark te bevorder;

(v) bestaande regeringsinisiatiewe wat regstreeks of onregstreeks relevant is tot, of 'n invloed het op, die nasionale e-strategie en, indien toepaslik, hoe sulke inisiatiewe gebruik staan te word om die oogmerke van die nasionale e-strategie te bereik;

(vi) die rol wat na verwagting deur die privaatsektor gespeel sal word by die implementering van die nasionale e-strategie, en hoe die regering die deelname van die privaatsektor om sodanige rol te speel, kan versoek;

(vii) die omskrewe doelwitte, met inbegrip van tydsraamwerke waarbinne die oogmerke bereik moet word; en

(viii) die hulpmiddels wat vereis word om die oogmerke te bereik waarvoor in die nasionale e-strategie voorsiening gemaak word.

(5) Na goedkeuring deur die Kabinet moet die Minister die nasionale e-strategie in die *Staatskoerant* publiseer.

(6) Ten einde die oogmerke van die nasionale e-strategie te bereik, kan die Minister, in oorleg met die Minister van Finansies-

(a) finansiering verkry van bronne buiten die staat;

(b) fondse vir die implementering van die nasionale e-strategie toewys aan die instellings en persone wat ingevolge die nasionale e-strategie vir lewering verantwoordelik is, en toesig hou oor die uitvoering van hul mandate; en

(c) die stappe doen wat nodig is om alle betrokke partye in staat te stel om hul onderskeie verpligtinge na te kom;

(7) Die Minister moet jaarliks aan die Kabinet verslag doen oor vordering gemaak en oogmerke bereik of uitstaande en kan hierby insluit enige ander aangeleentheid wat die Minister tersaaklik ag.

(8) Die Minister moet die nasionale e-strategie jaarliks hersien en in oorleg met alle betrokke Kabinetslede, die nodige wysigings aanbring.

(9) Geen wysiging of aanpassing van die nasionale e-strategie is effektief nie, tensy dit deur die Kabinet goedgekeur is.

(10) Die Minister moet enige wesenlike hersiening van die nasionale e-strategie in die *Staatskoerant* publiseer.

(11) Die Minister moet 'n jaarlikse verslag in die Parlement ter tafel lê aangaande die vordering wat met die inwerkingstelling van die nasionale e-strategie gemaak is.

6 Universele toegang

Ten opsigte van universele toegang moet die nasionale e-strategie strategieë en programme uiteensit om-

(a) Internetverbinding aan benadeelde gemeenskappe te verskaf;

(b) die privaatsektor aan te moedig om skemas te begin om universele toegang te verskaf;

(c) die aanneming en gebruik van nuwe tegnologieë vir die bereiking van universele toegang te kweek; en

(d) openbare bewustheid, begrip en aanvaarding van die voordele van Internet-verbinding en elektroniese sake doen te stimuleer.

7 Voorheen benadeelde persone en gemeenskappe

By die ontwikkeling van die nasionale e-strategie moet die Minister voorsiening maak vir wyses om die voordele van elektroniese transaksies vir histories benadeelde persone en gemeenskappe te maksimeer, met inbegrip van, maar nie beperk nie tot die-

(a) beskikbaarstelling of toeganklik maak van fasiliteite en infrastruktuur aan sodanige persone en gemeenskappe, om die bemarking en verkoop van hul goedere of dienste deur middel van elektroniese transaksies moontlik te maak;

(b) verskaffing of verkryging van ondersteuningsdienste vir sulke fasiliteite en infrastruktuur om met die effektiewe uitvoering van elektroniese transaksies behulpsaam te wees; en

(c) verlening van bystand en advies aan sulke persone en gemeenskappe oor wyses om elektroniese transaksies effektief aan te neem en te gebruik.

8 Ontwikkeling van menslike hulpbronne

(1) By die ontwikkeling van die nasionale e-strategie moet die Minister voorsiening maak vir wyses om die ontwikkeling van menslike hulpbronne te bevorder, soos in hierdie artikel uiteengesit, binne die raamwerk van die regering se geïntegreerde strategieë vir die ontwikkeling van menslike hulpbronne, met inagneming van strukture en programme wat tot stand gekom het kragtens bestaande wetgewing.

(2) Die Minister moet oorleg pleeg met die Ministers van Arbeid en Onderwys oor bestaande fasiliteite, programme en strukture vir onderwys, opleiding en mensehulpbronontwikkeling in die inligtingstegnologiesektor wat toepaslik is op die oogmerke van hierdie Wet.

(3) Behoudens subartikels (1) en (2) moet die Minister vaardigheidsontwikkeling bevorder op die gebiede van-

(a) inligtingstegnologieprodukte en -dienste ter ondersteuning van elektroniese transaksies;

(b) sakestrategieë vir KMMO's en ander besighede om elektroniese transaksies te gebruik;

(c) sektorale, regionale, nasionale, kontinentale en internasionale beleidsformulering vir elektroniese transaksies;

(d) projekbestuur oor die implementering van elektroniese transaksies deur die openbare en privaatsektor;

(e) bestuur van die .za-domeinnaamruimte;

(f) bestuur van die IP-adresstelsel vir die Afrika-vasteland, in oorleg met ander Afrikastate;

(g) sameloping tussen kommunikasietegnologieë wat elektroniese transaksies raak;

(h) tegnologie en sakestandaarde vir elektroniese transaksies;

(i) onderwys oor die aard, omvang, invloed, bedryf, gebruik en voordele van elektroniese transaksies; en

(j) enige ander aangeleentheid wat elektroniese transaksies raak.

9 KMMO's

Die Minister moet, in oorleg met die Minister van Handel en Nywerheid, die

toereikendheid van enige bestaande prosesse, programme en infrastruktuur wat voorsiening maak vir die gebruik van elektroniese transaksies deur KMMO's evalueer, en, na aanleiding van sodanige evaluering, kan-

(a) elektroniese kommunikasiesentrums vir KMMO's instel of die instelling daarvan vergemaklik;

(b) die ontwikkeling van webwerwe of webwerfpoorte vergemaklik wat KMMO's in staat sal stel om elektronies sake te doen en inligting oor markte, produkte en tegniese bystand te verkry; en

(c) die verskaffing vergemaklik van sodanige professionele en deskundige bystand en advies aan KMMO's oor wyses om die doen van elektroniese sake effektief vir hul ontwikkeling te gebruik.

Deel 2
Beleid oor elektroniese transaksies (a 10)

10 Beleid oor elektroniese transaksies

(1) Die Minister moet, behoudens hierdie Wet, beleid ten opsigte van elektroniese transaksies formuleer.

(2) By die formulering van die beleid in subartikel (1) beoog, moet die Minister-

(a) optree in oorleg met die Kabinetslede wat regstreeks deur sodanige beleidsformulering of die gevolge daarvan geraak word;

(b) behoorlik ag slaan op-

(i) die oogmerke van hierdie Wet;

(ii) die aard, omvang en invloed van elektroniese transaksies;

(iii) internasionale beste praktyk en ooreenstemming met die reg en riglyne van ander jurisdiksies en internasionale liggame; en

(iv) bestaande wetgewing en hul administrasie in die Republiek.

(3) Die Minister moet beleidsriglyne in die *Staatskoerant* publiseer oor vraagstukke wat op elektroniese transaksies in die Republiek van toepassing is.

(4) Met die inwerkingstelling van hierdie Hoofstuk moet die Minister die ontwikkeling van innoverende inligtingstelsels en die groei van aanverwante nywerhede aanmoedig.

HOOFSTUK III
VERGEMAKLIKING VAN ELEKTRONIESE TRANSAKSIES (aa 11-26)

Deel 1
Regsvereistes vir databoodskappe (aa 11-20)

11 Regserkenning van databoodskappe

(1) Inligting is nie sonder regskrag of regswerking bloot op grond daarvan dat dit geheel of gedeeltelik in die vorm van 'n databoodskap is nie.

(2) Inligting is nie sonder regskrag of regswerking bloot op grond daarvan dat dit nie vervat is in die databoodskap wat voorgee dat dit aanleiding gee tot die regskrag en regswerking nie, maar slegs na verwys word in sodanige databoodskap.

(3) Inligting wat by 'n ooreenkoms ingelyf is en wat nie in die openbare domein is nie word geag ingelyf te gewees het by 'n databoodskap indien daardie inligting-

(a) na verwys word op 'n wyse waarin 'n redelike persoon die verwysing daarna en inlywing daarvan sou opgemerk het; en

(b) toeganklik is in 'n vorm waarin dit deur die ander party gelees, geberg en herwin kan word, hetsy elektronies of in die vorm van 'n rekenaardrukstuk solank dit vir die party wat dit inlyf redelik moontlik is om die inligting te reduseer tot elektroniese formaat.

12 Skrif

'n Regsvereiste dat 'n dokument of inligting op skrif moet wees, word nagekom indien die dokument of inligting-

(a) in die vorm van 'n databoodskap is; en

(b) toeganklik is op 'n wyse wat vir latere verwysing bruikbaar is.

13 Handtekening

(1) Waar die handtekening van 'n persoon regtens vereis word en die regsreël spesifiseer nie die tipe handtekening nie, word aan daardie vereiste met betrekking tot 'n databoodskap voldoen slegs indien 'n gevorderde elektroniese handtekening gebruik word.

(2) Behoudens subartikel (1), is 'n elektroniese handtekening nie sonder regskrag en regswerking bloot op grond daarvan dat dit in elektroniese vorm is nie.

(3) Waar 'n elektroniese handtekening vereis word deur die partye tot 'n

elektroniese transaksie en die partye nie ooreengekom het op die tipe elektroniese handtekening wat gebruik moet word nie, word aan hierdie vereiste voldoen ten opsigte van 'n databoodskap indien-

(a) 'n metode gebruik word om die persoon te identifiseer en die persoon se goedkeuring aan te dui van die inligting wat gekommunikeer is; en

(b) in die lig van al die toepaslike omstandighede ten tyde van die gebruik van die metode, die metode so betroubaar was as wat geskik was vir die doeleindes waarvoor die inligting gekommunikeer is.

(4) Waar 'n gevorderde elektroniese handtekening gebruik is, word sodanige handtekening geag 'n geldige elektroniese handtekening te wees en behoorlik toegepas te gewees het, tensy die teendeel bewys word.

(5) Waar 'n elektroniese handtekening nie deur die partye by 'n elektroniese transaksie vereis word nie, is 'n wilsuitdrukking of ander verklaring nie sonder regskrag en regswerking nie bloot op grond daarvan dat-

(a) dit in die vorm van 'n databoodskap is; of

(b) dit nie bewys word deur 'n elektroniese handtekening nie, maar bewys word op 'n ander wyse waarvan so 'n persoon se bedoeling of ander verklaring afgelei kan word.

14 Oorspronklike

(1) Waar 'n wet vereis dat inligting in sy oorspronklike vorm aangebied of behou moet word, voldoen 'n databoodskap aan daardie vereiste indien-

(a) die integriteit van die inligting die toets ingevolge subartikel (2) geslaag het, vanaf die tyd waarop dit vir die eerste keer in sy finale vorm as 'n databoodskap of andersins voortgebring is; en

(b) daardie inligting in staat is om vertoon of voorgelê te word aan die persoon aan wie dit aangebied moet word.

(2) By die toepassing van subartikel (1) *(a)* moet die integriteit beoordeel word-

(a) deur te oorweeg of die inligting volledig en onveranderd gebly het, behalwe vir die byvoeging van enige endossement en enige verandering wat in die normale verloop van kommunikasie, berging en vertoon ontstaan;

(b) in die lig van die doel waarvoor die inligting voortgebring is; en

(c) met inagneming van alle ander toepaslike omstandighede.

15 Toelaatbaarheid en bewyswaarde van databoodskappe

(1) In enige regsgeding mag die reëls van bewysreg nie so aangewend word dat die toelaatbaarheid van 'n databoodskap as getuienis ontken word-

(a) bloot op grond daarvan dat dit 'n databoodskap uitmaak nie; of

(b) indien dit die beste getuienis is wat redelikerwys van die persoon wat dit aanbied verwag kan word om te verkry, op grond daarvan dat dit nie in sy oorspronklike vorm is nie.

(2) Inligting in die vorm van 'n databoodskap moet behoorlike bewyswaarde verleen word.

(3) By die beoordeling van die bewyswaarde van 'n databoodskap, moet oorweging geskenk word aan-

(a) die betroubaarheid van die wyse waarop die databoodskap voortgebring, geberg of gekommunikeer is;

(b) die betroubaarheid van die wyse waarop die integriteit van die databoodskap gehandhaaf is;

(c) die wyse waarop die opsteller daarvan geïdentifiseer is; en

(d) enige ander toepaslike faktor.

(4) 'n Databoodskap wat deur 'n persoon in die normale loop van sake gemaak is, of 'n afskrif of drukstuk daarvan, of 'n uittreksel vanuit so 'n databoodskap wat deur 'n ampsdraer in diens van so 'n persoon as korrek gesertifiseer is, is by administratiewe of dissiplinêre verrigtinge ingevolge enige regsreël, die reëls van 'n selfregulerende organisasie, of enige ander wet, of gemenereg, toelaatbaar as getuienis teen enige persoon, en kom neer op weerlegbare bewys van die feite vervat in so 'n rekord, afskrif, drukskrif of uittreksel.

16 Behoud

(1) Waar 'n wet vereis dat inligting behou moet word, word aan daardie vereiste voldoen deur sodanige inligting in die vorm van 'n databoodskap te behou, indien-

(a) die inligting in die databoodskap vervat, toeganklik is sodat dit bruikbaar is vir latere verwysing;

(b) die databoodskap in die formaat is waarin dit voortgebring, gestuur of

ontvang is, of in 'n formaat wat bewys kan word die inligting wat voortgebring, gestuur of ontvang is, akkuraat voor te stel; en

(c) die oorsprong en bestemming van daardie databoodskap en die datum en tyd waarop dit gestuur of ontvang is, vasgestel kan word.

(2) Die verpligting om inligting te behou soos beoog in subartikel (1) slaan nie op enige inligting waarvan die uitsluitlike doel is om dit moontlik te maak om die boodskap te stuur of te ontvang nie.

17 Voorlegging van dokument of inligting

(1) Waar 'n wet vereis dat 'n persoon 'n dokument of inligting moet voorlê, word daar behoudens artikel 28 voldoen aan daardie vereiste indien die persoon, deur middel van 'n databoodskap, 'n elektroniese weergawe van daardie dokument of inligting voorlê, en indien-

(a) met inagneming van al die toepaslike omstandighede ten tyde van die afstuur van die databoodskap, die metode van voortbringing van die elektroniese vorm van daardie dokument 'n betroubare wyse gebied het om die behoud van die integriteit van die inligting vervat in daardie dokument te verseker; en

(b) dit ten tyde van die versending van die databoodskap redelik was om te verwag dat die inligting daarin vervat geredelik toeganklik sou wees, sodat dit bruikbaar sou wees vir daaropvolgende verwysing.

(2) By die toepassing van subartikel (1) word die integriteit van die inligting vervat in 'n dokument gehandhaaf indien die inligting volledig en onveranderd gebly het, behalwe vir-

(a) die byvoeging van enige endossement; of

(b) enige onwesenlike verandering wat in die normale verloop van kommunikasie, berging of vertoon ontstaan.

18 Notarisering, erkenning en sertifisering

(1) Waar 'n wet vereis dat 'n handtekening, verklaring of dokument notarieel verly, erken, bewys of onder eed afgelê moet word, word aan daardie vereiste voldoen indien die gevorderde elektroniese handtekening van die persoon wat gemagtig is om daardie handelinge te verrig, aangeheg of ingelyf word by of logies geassosieer word met die elektroniese handtekening of databoodskap.

(2) Waar 'n wet vereis of toelaat dat 'n persoon 'n gesertifiseerde afskrif van 'n dokument of inligting verskaf, en die dokument bestaan in elektroniese vorm, word aan

daardie vereiste voldoen indien die persoon 'n drukstuk verskaf wat gesertifiseer is as 'n ware afskrif van die dokument of inligting.

(3) Waar die reg dit vereis of toelaat dat 'n persoon 'n gesertifiseerde afskrif van 'n dokument moet of kan voorsien en die dokument bestaan uit 'n papier- of ander fisiese formaat, word daar aan die vereiste voldoen indien 'n elektroniese afskrif van die dokument gesertifiseer word as 'n ware afskrif en die sertifisering bevestig word deur die gebruik van 'n gevorderde elektroniese handtekening.

19 Ander vereistes

(1) Daar word aan 'n vereiste in 'n wet dat veelvoudige afskrifte van 'n dokument gelyktydig by 'n enkele ontvanger voorgelê moet word, voldoen deur die voorlegging van 'n enkele databoodskap wat deur daardie ontvanger gereproduseer kan word.

(2) 'n Uitdrukking in 'n wet, hetsy as selfstandige naamwoord of werkwoord gebruik, met inbegrip van die uitdrukkings 'dokument', 'rekord', 'aanteken', 'indien', 'voorlê', 'inlewer', 'aflewer', 'uitreik', 'publiseer', 'skryf in', 'druk' of woorde of uitdrukkings met soortgelyke effek moet uitgelê word sodat dit sodanige vorm, formaat of handeling met betrekking tot 'n databoodskap insluit, tensy andersins daarvoor voorsiening gemaak word in hierdie Wet.

(3) Waar dit regtens vereis word dat 'n seël op 'n dokument aangebring moet word en die regsreël nie die metode of formaat voorskryf waardeur so 'n dokument elektronies verseël moet word nie, word daar aan hierdie vereiste voldoen indien die dokument die vereiste dat dit verseël moet word, aandui en die dokument die gevorderde elektroniese handtekening vervat van die persoon deur wie dit vereis word om verseël te word.

(4) Waar enige regsreël dit vereis of toelaat dat 'n persoon 'n dokument of inligting deur geregistreerde of gesertifiseerde pos of 'n soortgelyke diens, moet of kan stuur, word daar aan hierdie vereiste voldoen indien 'n elektroniese afskrif van die dokument of inligting gestuur word aan die Suid-Afrikaanse Poskantoor Beperk, dit geregistreer word deur genoemde Poskantoor en deur daardie Poskantoor gestuur word aan die elektroniese adres wat deur die afstuurder voorsien word.

20 Geoutomatiseerde transaksies

In 'n geoutomatiseerde transaksie-

(a) kan 'n ooreenkoms gesluit word waar 'n elektroniese agent 'n handeling uitvoer wat regtens vir sluiting van 'n ooreenkoms vereis word;

(b) kan 'n ooreenkoms gesluit word waar al die partye tot 'n transaksie, of enige van hulle, 'n elektroniese agent gebruik;

(c) word 'n party wat 'n elektroniese agent gebruik om 'n ooreenkoms te sluit,

behoudens paragraaf *(d)* geag om gebonde te wees aan die bedinge van daardie ooreenkoms, ongeag of daardie persoon die handelinge van die elektroniese agent of die bedinge van die ooreenkoms hersien het;

(d) 'n party wat deur wisselwerking met 'n elektroniese agent 'n ooreenkoms wil sluit, word nie deur die bepalings van die ooreenkoms verbind nie, tensy voor die totstandkoming van die kontrak, daardie bepalings hersien kon word deur 'n natuurlike persoon wat daardie party verteenwoordig.

(e) word geen ooreenkoms gesluit waar 'n natuurlike persoon regstreeks met die elektroniese agent van 'n ander persoon onderhandel en 'n wesenlike fout tydens die skepping van 'n databoodskap gemaak het en-

(i) die elektroniese agent nie aan daardie persoon 'n geleentheid gegee het om die fout te voorkom of reg te stel nie;

(ii) daardie persoon, so gou doenlik nadat daardie persoon dit te wete gekom het, die ander persoon van die fout in kennis stel;

(iii) daardie persoon redelike stappe doen, met inbegrip van stappe wat ooreenstem met die ander persoon se opdragte om enige prestasie wat ontvang is, terug te besorg of daardie prestasie te vernietig, indien aldus gelas; en

(iv) daardie persoon nie enige wesenlike voordeel of waarde gebruik of ontvang het uit enige prestasie wat van die ander persoon ontvang is nie.

Deel 2
Kommunikering van databoodskappe (aa 21-26)

21 Wysiging by ooreenkoms tussen partye

Hierdie Deel is slegs van toepassing indien die partye wat by die skepping, stuur, ontvangs, berging of andersins by die prosessering van databoodskappe betrokke is nie ooreenkoms bereik het aangaande die kwessies waarvoor daarin voorsiening gemaak word nie.

22 Sluiting en geldigheid van ooreenkomste

(1) 'n Ooreenkoms is nie sonder regskrag en regswerking bloot omdat dit gedeeltelik of in die geheel deur middel van databoodskappe gesluit is nie.

(2) 'n Ooreenkoms wat deur middel van databoodskappe tussen partye gesluit word, word gesluit op die tyd wanneer en plek waar die aanvaarding van die aanbod deur die aanbieder ontvang word.

23 Tyd en plek van kommunikasies, versending en ontvangs

(1) 'n Databoodskap-

(a) wat by die sluiting van of prestasie ingevolge 'n ooreenkoms gebruik is, moet geag word deur die opsteller gestuur te wees wanneer dit 'n inligtingstelsel buite die beheer van die opsteller binnegaan of, indien die opsteller en geadresseerde in dieselfde inligtingstelsel is, wanneer dit in staat is om deur die geadresseerde herwin te word;

(b) moet geag word deur die geadresseerde ontvang te gewees het wanneer die volledige databoodskap 'n inligtingstelsel binnegaan wat deur die geadresseerde vir daardie doel aangewys of gebruik word en in staat is om deur die geadresseerde herwin of geprosesseer te word; en

(c) moet geag word vanaf die opsteller se gewone besigheidsplek of woning gestuur te gewees het en by die geadresseerde se gewone besigheidsplek of woning ontvang te gewees het.

24 Betuiging van voorneme of ander verklaring

Tussen die opsteller en die geadresseerde van 'n databoodskap is 'n betuiging van voorneme of ander verklaring nie sonder regskrag en regswerking bloot op grond daarvan dat-

(a) dit in die vorm van 'n databoodskap is nie; of

(b) dit nie deur 'n elektroniese handtekening gestaaf word nie maar op ander maniere waaruit die persoon se voorneme of ander verklaring afgelei kan word.

25 Toeskrywing van databoodskappe aan opsteller

'n Databoodskap word geag dié van die opsteller te wees indien dit-

(a) persoonlik deur die opsteller gestuur is;

(b) gestuur is deur 'n persoon wat magtiging gehad het om ten opsigte van daardie databoodskap namens die opsteller op te tree; of

(c) gestuur is deur 'n inligtingstelsel wat deur of namens die opsteller geprogrammeer is om outomaties te werk tensy dit bewys word dat die inligtingstelsel hierdie programmering nie behoorlik uitgevoer het nie.

26 Erkenning van ontvangs van databoodskap

(1) Geen erkenning van ontvangs van 'n databoodskap is nodig om regswerking aan daardie boodskap te gee nie.

(2) 'n Ontvangserkenning kan gegee word deur middel van-

(a) enige kommunikasie deur die geadresseerde, hetsy outomaties of andersins; of

(b) enige gedrag van die geadresseerde wat voldoende is om aan die opsteller aan te dui dat die databoodskap ontvang is.

HOOFSTUK IV
E-REGERINGSDIENSTE (aa 27-28)

27 Aanvaarding van elektroniese indiening en uitreiking van dokumente

Enige openbare liggaam wat ooreenkomstig enige wet-

(a) die indiening van dokumente aanvaar of vereis dat dokumente geskep of behou word;

(b) 'n permit, lisensie of goedkeuring uitreik; of

(c) vir 'n wyse van betaling voorsiening maak,

kan, ondanks andersluidende bepalings van sodanige wet-

(i) die indiening van sodanige dokumente, of die skepping of behoud van sodanige dokumente in die vorm van databoodskappe aanvaar;

(ii) sodanige permit, lisensie of goedkeuring in die vorm van 'n databoodskap uitreik; of

(iii) betaling in elektroniese formaat of op elektroniese wyse doen of ontvang.

28 Vereistes kan vermeld word

(1) In enige geval waar 'n openbare liggaam enige van die werksaamhede bedoel in artikel 27 verrig, kan sodanige liggaam by kennisgewing in die *Staatskoerant* die volgende vermeld:

(a) Die wyse waarop en formaat waarin die databoodskappe ingedien, geskep, behou of uitgereik moet word;

(b) in gevalle waar die databoodskap onderteken moet word, die tipe

elektroniese handtekening wat vereis word;

(c) die wyse waarop en formaat waarin die elektroniese handtekening aan die databoodskap geheg moet word, daarby ingelyf moet word of andersins daarmee geassosieer moet word;

(d) die identiteit van of kriteria waaraan voldoen moet word deur enige waarmerkingsdiensverskaffer wat gebruik word deur die persoon wat die databoodskap indien of dat so 'n waarmerkingsdiensverskaffer 'n voorkeurdiensverskaffer is;

(e) die toepaslike beheerprosesse en prosedures om voldoende integriteit, veiligheid en vertroulikheid van databoodskappe of betalings te verseker; en

(f) enige ander vereistes vir databoodskappe of betalings.

(2) Vir die doeleindes van subartikel (1) *(d)* is die Suid-Afrikaanse Poskantoor Beperk 'n voorkeurwaarmerkingsdiensverskaffer en kan die Minister enige ander waarmerkingsdiensverskaffer as 'n voorkeurwaarmerkingsdiensverskaffer aanwys, gebaseer op so 'n waarmerkingsdiens se verbintenisse met betrekking tot die verskaffing van universele toegang.

HOOFSTUK V
KRIPTOGRAFIEVERSKAFFERS (aa 29-32)

29 Register van kriptografieverskaffers

(1) Die Direkteur-generaal moet 'n register van kriptografieverskaffers instel en byhou.

(2) Die Direkteur-generaal moet die volgende besonderhede ten opsigte van 'n kriptografieverskaffer in daardie register aanteken:

(a) Die naam en adres van die kriptografieverskaffer;

(b) 'n beskrywing van die tipe kriptografiediens of kriptografieproduk wat verskaf word; en

(c) die ander besonderhede wat voorgeskryf word om die kriptografieverskaffer of sy of haar produkte of dienste voldoende te identifiseer en op te spoor.

(3) Daar word nie van 'n kriptografieverskaffer verwag om vertroulike inligting of handelsgeheime ten opsigte van sy of haar kriptografieprodukte of -dienste te verskaf nie.

30 Registrasie by Departement

(1) Niemand mag kriptografiedienste of kriptografieprodukte in die Republiek verskaf voordat die besonderhede in artikel 29 (2) bedoel ten opsigte van daardie persoon in die register in artikel 29 (1) beoog, aangeteken is nie.

(2) 'n Kriptografieverskaffer moet die Direkteur-generaal op die voorgeskrewe wyse voorsien van die inligting wat vereis word en die voorgeskrewe administratiewe gelde betaal.

(3) Daar word geag dat 'n kriptografiediens of kriptografieproduk in die Republiek verskaf word indien dit verskaf word-

(a) vanaf persele in die Republiek;

(b) aan 'n persoon wat in die Republiek aanwesig is wanneer daardie persoon van die diens of produk gebruik maak; of

(c) aan 'n persoon wat die diens of produk gebruik vir die doeleindes van 'n besigheid wat in die Republiek of vanaf persele in die Republiek bedryf word.

31 Beperkings op openbaarmaking van inligting

(1) Inligting wat vervat is in die register waarvoor in artikel 29 voorsiening gemaak word, mag nie openbaargemaak word aan enige ander persoon as werknemers van die Departement wat verantwoordelik is vir die byhou van die register nie.

(2) Subartikel (1) is nie van toepassing nie ten opsigte van inligting wat openbaargemaak word-

(a) aan 'n toepaslike owerheid wat 'n kriminele misdryf ondersoek of vir die doeleindes van enige strafregtelike verrigtinge;

(b) aan regeringsagentskappe wat verantwoordelik is vir veiligheid en sekuriteit in die Republiek, ooreenkomstig 'n amptelike versoek;

(c) aan 'n kuberinspekteur;

(d) ooreenkomstig artikel 11 of 30 van die Wet op Bevordering van Toegang tot Inligting (Wet 2 van 2000); of

(e) vir doeleindes van enige siviele verrigtinge wat verband hou met die verskaffing van kriptografiedienste of kriptografieprodukte en waarby 'n kriptografieverskaffer 'n party is.

32 Toepassing van Hoofstuk en misdrywe

(1) Die bepalings van hierdie Hoofstuk is nie van toepassing op die Nasionale Intelligensie-agentskap wat ingestel is ingevolge artikel 3 van die Wet op Intelligensiedienste, 1994 (Wet 38 van 1994), nie.

(2) 'n Persoon wat 'n bepaling van hierdie Hoofstuk oortree of versuim om daaraan te voldoen, is skuldig aan 'n misdryf en is by skuldigbevinding strafbaar met 'n boete of met gevangenisstraf vir 'n tydperk wat nie twee jaar oorskry nie.

HOOFSTUK VI
WAARMERKINGSDIENSVERSKAFFERS (aa 33-41)

Deel 1
Akkreditasie-owerheid (aa 33-36)

33 Woordomskrywing

In hierdie Hoofstuk, tensy die samehang anders aandui, beteken-

'akkreditasie' 'n erkenning van 'n waarmerkingsproduk of -diens deur die Akkreditasie-owerheid.

34 Aanstelling van Akkreditasie-owerheid en ander beamptes

(1) By die toepassing van hierdie Hoofstuk moet die Direkteur-generaal as die Akkreditasie-owerheid optree.

(2) Die Akkreditasie-owerheid kan, na oorleg met die Minister, werknemers van die Departement as Adjunk Akkreditasie-owerhede en beamptes aanstel.

35 Akkreditasie vrywillig te wees

(1) Behoudens artikel 30 kan 'n persoon sonder die voorafgaande magtiging van enige ander persoon waarmerkingsprodukte of -dienste in die Republiek verkoop of verskaf.

36 Bevoegdhede en pligte van Akkreditasie-owerheid

(1) Die Akkreditasie-owerheid kan-

(a) die optrede, stelsels en werking van 'n waarmerkingsdiensverskaffer moniteer om te verseker dat dit aan artikel 38 en die ander verpligtinge van waarmerkingsdiensverskaffers ingevolge hierdie Wet voldoen;

(b) die akkreditasie van 'n waarmerkingsproduk of -diens tydelik opskort of

intrek; en

(c) 'n onafhanklike ouditeursfirma aanstel om periodieke oudits van die waarmerkingsdiensverskaffer te doen om te verseker dat dit aan artikel 38 en die ander verpligtinge van waarmerkingsdiensverskaffers ingevolge hierdie Wet voldoen;

(2) Die Akkreditasie-owerheid moet 'n databasis wat vir die publiek toeganklik is, byhou ten opsigte van-

(a) waarmerkingsprodukte of -dienste wat ingevolge artikel 37 geakkrediteer is;

(b) waarmerkingsprodukte en -dienste wat ingevolge artikel 40 erken word;

(c) akkreditasies of erkennings wat ingetrek is; en

(d) die ander inligting wat voorgeskryf word.

Deel 2
Akkreditasie (aa 37–41)

37 Akkreditasie van waarmerkingsprodukte en -dienste

(1) Die Akkreditasie-owerheid kan waarmerkingsprodukte of -dienste ter ondersteuning van gevorderde elektroniese handtekeninge akkrediteer.

(2) 'n Aansoek om akkreditasie moet-

(a) op die voorgeskrewe wyse by die Akkreditasie-owerheid gedoen word en gestaaf word deur die voorgeskrewe inligting; en

(b) vergesel gaan van die voorgeskrewe geld, wat nie terugbetaalbaar is nie.

(3) 'n Persoon wat valslik voorgee dat sy of haar produkte of dienste by die Akkreditasie-owerheid geakkrediteer is, is skuldig aan 'n misdryf.

38 Kriteria vir akkreditasie

(1) Die Akkreditasie-owerheid mag nie waarmerkingsprodukte of -dienste akkrediteer nie tensy die Akkreditasie-owerheid oortuig is dat 'n elektroniese handtekening waarop die waarmerkingsprodukte of -dienste betrekking het-

(a) uniek aan die gebruiker gekoppel is;

(b) in staat is om daardie gebruiker te identifiseer;

(c) geskep is deur die gebruik van middele wat onder die uitsluitlike beheer van daardie gebruiker onderhou kan word;

(d) op so 'n wyse aan die data of databoodskap waarop dit betrekking het, gekoppel sal wees dat enige latere verandering van die data of databoodskap opspoorbaar is; en

(e) word gebaseer op die van-aangesig-tot-aangesig identifikasie van die gebruiker.

(2) By die toepassing van subartikel (1) moet die Akkreditasie-owerheid die volgende faktore ten opsigte van 'n waarmerkingsdiensverskaffer in ag neem voor die akkreditering van waarmerkingsprodukte of -dienste:

(a) Die verskaffer se finansiële en menslike hulpbronne, met inbegrip van die bates;

(b) die kwaliteit van die verskaffer se hardeware- en sagtewarestelsels;

(c) die verskaffer se prosedures om produkte of dienste te prosesseer;

(d) die beskikbaarheid van inligting aan derde partye wat op die waarmerkingsproduk of -diens staatmaak;

(e) die gereeldheid en omvang van oudits deur 'n onafhanklike liggaam;

(f) die faktore bedoel in subartikel (4) waar die produkte en dienste deur 'n sertifiseringsdiensverskaffer gelewer word; en

(g) enige ander toepaslike faktor wat voorgeskryf word.

(3) By die toepassing van subartikel (2) *(b)* en *(c)* moet die hardeware- en sagtewarestelsels en prosedures minstens-

(a) redelik beveilig wees teen inmenging en misbruik;

(b) 'n redelike vlak van beskikbaarheid, betroubaarheid en korrekte werking verskaf;

(c) redelik geskik wees om hul bedoelde funksies te verrig; en

(d) voldoen aan algemeen aanvaarde sekerheidsprosedures.

(4) By die toepassing van subartikel (1), waar die produkte of dienste deur 'n sertifiseringsdiensverskaffer voorsien word, kan die Akkreditasie-owerheid voor die

akkreditering van waarmerkingsprodukte of -dienste bepalings maak oor-

(a) die tegniese en ander vereistes waaraan sertifikate moet voldoen;

(b) die vereistes vir die uitreiking van sertifikate;

(c) die vereistes vir sertifiseringspraktykstate;

(d) die verantwoordelikhede van die sertifiseringsdiensverskaffer;

(e) die aanspreeklikheid van die sertifiseringsdiensverskaffer;

(f) die rekords wat gehou moet word en die wyse waarop en die tydperk waarvoor dit gehou moet word;

(g) vereistes vir voldoende prosedures vir die opskorting en intrekking van sertifikate; en

(h) vereistes oor voldoende kennisgewingsprosedures met betrekking tot die opskorting en intrekking van sertifikate.

(5) Die Akkreditasie-owerheid kan enige nodige voorwaardes of beperkings oplê wanneer 'n waarmerkingsproduk of -diens geakkrediteer word.

39 Intrekking of beëindiging van akkreditasie

(1) Indien die Akkreditasie-owerheid oortuig is dat 'n waarmerkingsdiensverskaffer versuim het of ophou om te voldoen aan enige van die vereistes, voorwaardes of beperkings onderworpe waaraan akkreditasie kragtens artikel 38 verleen is of erkenning ingevolge artikel 40 gegee is, kan die Akkreditasie-owerheid die akkreditasie opskort of intrek.

(2) Behoudens die bepalings van subartikel (3) mag die Akkreditasie-owerheid nie die akkreditasie beoog in subartikel (1) opskort of intrek nie, tensy die Akkreditasie-owerheid-

(a) die waarmerkingsdiensverskaffer skriftelik in kennis gestel het van die voorneme om dit te doen;

(b) 'n beskrywing gegee het van die beweerde skending van enige van die vereistes, voorwaardes of beperkings onderworpe waaraan akkreditasie kragtens artikel 38 verleen is of erkenning ingevolge artikel 40 gegee is;

(c) aan die waarmerkingdiensverskaffer die geleentheid gegee het om-

(i) skriftelik op die bewerings te reageer; en

(ii) die beweerde skending binne 'n redelike tyd reg te stel.

(3) Die Akkreditasie-owerheid kan akkreditasie kragtens artikel 38 verleen of erkenning ingevolge artikel 40 gegee, opskort met onmiddellike werking vir 'n tydperk wat nie 90 dae oorskry nie, hangende implementering van die prosedures wat vereis word deur subartikel (2), indien die volgehoue akkreditasie of erkenning van die waarmerkingdiensverskaffer redelik waarskynlik onherstelbare skade aan verbruikers of aan enige persoon wat by 'n elektroniese transaksie in die Republiek betrokke is, sal veroorsaak.

(4) 'n Waarmerkingsdiensverskaffer wie se produkte of dienste ingevolge hierdie Hoofstuk geakkrediteer is, kan sodanige akkreditasie te eniger tyd beëindig, behoudens die voorwaardes waarop ten tyde van die akkreditasie of daarna ooreengekom word.

40 Akkreditasie van buitelandse produkte en dienste

(1) Die Minister kan, by kennisgewing in die *Staatskoerant* en behoudens die voorwaardes wat deur hom of haar bepaal word, die akkreditasie of soortgelyke erkenning wat aan enige waarmerkingsdiensverskaffer of sy of haar waarmerkingsprodukte of -dienste in 'n buitelandse jurisdiksie verleen is, erken.

(2) 'n Waarmerkingsdiensverskaffer wat valslik voorgee dat sy of haar waarmerkingsprodukte of -dienste deur die Minister ingevolge subartikel (1) erken is, is skuldig aan 'n misdryf.

41 Regulasies betreffende akkreditasie

Die Minister kan regulasies uitvaardig ten opsigte van-

(a) die regte en verpligtinge van persone met betrekking tot die voorsiening van geakkrediteerde produkte en dienste;

(b) die wyse waarop die Owerheid nakoming van daardie verpligtinge moet administreer en kontroleer;

(c) die prosedure wat pas by die verlening, opskorting en intrekking van akkreditasie;

(d) gelde wat betaal moet word;

(e) inligtingsekerheidsvereistes of -riglyne; en

(f) enige ander toepaslike aangeleentheid wat nodig en dienstig is om voor te skryf vir die behoorlike implementering van hierdie Hoofstuk.

HOOFSTUK VII
VERBRUIKERSBESKERMING (aa 42-49)

42 Bestek van toepassing

(1) Hierdie Hoofstuk is slegs op elektroniese transaksies van toepassing.

(2) Artikel 44 is nie van toepassing nie op 'n elektroniese transaksie-

(a) vir finansiële dienste, met inbegrip van maar nie beperk nie tot, beleggingsdienste, versekerings- en herversekeringsbedrywighede, bankdienste en bedrywighede met betrekking tot handel in effekte;

(b) by wyse van 'n veiling;

(c) vir die lewering van voedsel, drank of ander goedere bedoel vir alledaagse verbruik wat by die huis, verblyfplek of werkplek van die verbruiker gelewer word;

(d) vir dienste wat begin is met die verbruiker se toestemming voor die einde van die tydperk van sewe dae bedoel in artikel 44 (1);

(e) waar die prys vir die voorsiening van goedere of dienste afhanklik is van skommelinge in die finansiële markte wat nie deur die voorsiener beheer kan word nie;

(f) waar die goedere-

(i) vervaardig word volgens die verbruiker se spesifikasies;

(ii) duidelik op die persoon afgestem is;

(iii) weens die aard van die goedere nie teruggegee kan word nie;

(iv) geneig is om vinnig te bederf of te verstryk;

(g) waar die verseëling om oudio- of video-opnames of rekenaarsagteware deur die verbruiker gebreek is;

(h) vir die verkoop van koerante, weekblaaie, tydskrifte en boeke;

(i) vir die voorsiening van dobbel- en loterydienste; of

(j) vir die voorsiening van akkommodasie, vervoer, spyseniers- of ontspanningsdienste en waar die leweransier, wanneer die transaksie beklink word, onderneem om hierdie dienste op 'n spesifieke datum of

binne 'n spesifieke tydperk te lewer.

(3) Hierdie Hoofstuk is nie van toepassing op 'n regulerende owerheid wat ingevolge 'n regsreël tot stand gebring is nie indien daardie regsreël maatreëls vir verbruikersbeskerming met betrekking tot elektroniese transaksies voorskryf.

43 Inligting wat verskaf moet word

(1) 'n Leweransier wat enige goedere of dienste te koop, te huur of te ruil aanbied by wyse van 'n elektroniese transaksie moet die volgende inligting aan verbruikers beskikbaar stel op die webwerf waar sodanige goedere of dienste aangebied word:

(a) Sy of haar volle naam en regstatus;

(b) sy of haar fisiese adres en telefoonnommer;

(c) sy of haar webwerfadres en e-posadres;

(d) lidmaatskap van enige selfregulerende of akkrediteringsliggame waaraan daardie leweransier behoort of by aangesluit is en die kontakbesonderhede van daardie liggaam;

(e) enige gedragskode wat daardie leweransier onderskryf en hoe die verbruiker elektronies toegang tot daardie gedragskode kan verkry;

(f) in die geval van 'n regspersoon, sy registrasienommer, die name van sy ampsdraers en sy plek van registrasie;

(g) die fisiese adres waar daardie leweransier regsbetekening van dokumente sal ontvang;

(h) 'n voldoende beskrywing van die hoofkenmerke van die goedere of dienste wat deur daardie leweransier aangebied word om 'n verbruiker in staat te stel om 'n ingeligte besluit oor die voorgestelde elektroniese transaksie te neem;

(i) die volle prys wat vir die goedere of dienste betaal moet word, met inbegrip van vervoerkostes, belastings en enige ander gelde of kostes;

(j) die wyse van betaling;

(k) enige bedinge van ooreenkoms, met inbegrip van waarborge, wat op die transaksie van toepassing sal wees, en hoe verbruikers elektronies tot daardie bedinge toegang kan verkry of dit kan berg of reproduseer;

(l) die tydperk waarbinne die goedere versend of afgelewer sal word of

waarbinne die dienste gelewer sal word;

(m) die wyse waarop en tydperk waarbinne verbruikers toegang kan verkry tot 'n volledige rekord van die transaksie en dit kan byhou;

(n) die beleid van daardie leweransier oor teruggawe, vervanging en terugbetaling;

(o) enige alternatiewe geskilbeslegtingskode wat daardie leweransier onderskryf en hoe die verbruiker elektronies toegang tot die bewoording van daardie kode kan verkry;

(p) die veiligheidsprosedures en privaatheidsbeleid van daardie leweransier met betrekking tot betaling, betalingsinligting en persoonlike inligting;

(q) waar van toepassing, die minimum duur van die ooreenkoms in die geval van ooreenkomste vir die lewering van produkte of dienste wat op 'n deurlopende grondslag of herhaaldelik uitgevoer moet word; en

(r) die regte van verbruikers ingevolge artikel 44, waar van toepassing.

(2) Die leweransier moet 'n verbruiker 'n geleentheid gee-

(a) om die hele elektroniese transaksie te hersien;

(b) om enige foute reg te stel; en

(c) om aan die transaksie te onttrek, voordat enige bestelling finaal geplaas word.

(3) Indien 'n leweransier versuim om aan die bepalings van subartikel (1) of (2) te voldoen, kan die verbruiker die ooreenkoms kanselleer binne 14 dae na ontvangs van die goedere of dienste kragtens die transaksie.

(4) Indien 'n transaksie gekanselleer word ingevolge subartikel (3)-

(a) moet die verbruiker die prestasie van die leweransier teruggee, of waar van toepassing, ophou om die gelewerde dienste te gebruik; en

(b) moet die leweransier alle betalings wat deur die verbruiker gedoen is, teruggee minus die regstreekse koste om die goedere terug te besorg.

(5) Die leweransier moet 'n betalingstelsel gebruik wat voldoende veilig is met verwysing na aanvaarde tegnologiese standaarde ten tyde van die transaksie en na die tipe transaksie wat betrokke is.

(6) Die leweransier is aanspreeklik vir enige skade wat deur 'n verbruiker gely word as gevolg van 'n versuim deur die leweransier om aan subartikel (5) te voldoen.

44 Afkoeltydperk

(1) 'n Verbruiker is geregtig om sonder rede en sonder strafbeding enige transaksie en enige verwante kredietooreenkoms vir die lewering-

(a) van goedere te kanselleer binne sewe dae na die datum van die ontvangs van die goedere; of

(b) van dienste te kanselleer binne sewe dae na die datum van die sluiting van die ooreenkoms.

(2) Die enigste vordering wat die verbruiker opgelê kan word, is die regstreekse koste om die goedere terug te stuur.

(3) Indien betaling vir die goedere of dienste geskied het voordat 'n verbruiker 'n reg in subartikel (1) bedoel, uitoefen, is die verbruiker geregtig op 'n volledige terugbetaling van sodanige betaling, en die terugbetaling moet geskied binne 30 dae na die datum van kansellasie.

(4) Hierdie artikel mag nie uitgelê word asof dit die regte van 'n verbruiker waarvoor in enige ander wet voorsiening gemaak word, benadeel nie.

45 Ongevraagde goedere, dienste of kommunikasies

(1) Enige persoon wat ongevraagde handelskommunikasies aan verbruikers stuur, moet die verbruiker voorsien-

(a) van die opsie om sy of haar intekening op die poslys van daardie persoon te kanselleer; en

(b) op versoek van die verbruiker, van die identifiseringsbesonderhede van die bron waarvandaan daardie persoon die verbruiker se persoonlike inligting gekry het.

(2) Geen ooreenkoms word bereik waar 'n verbruiker versuim het om op 'n ongevraagde kommunikasie te antwoord nie.

(3) Enige persoon wat versuim om te voldoen aan subartikel (1) of dit oortree, is skuldig aan 'n misdryf en is, na skuldigbevinding, strafbaar met die strafmaatreëls wat in artikel 89 (1) voorgeskryf word.

(4) Enige persoon wat ongevraagde handelskommunikasies stuur aan 'n persoon wat die afsender in kennis gestel het dat sulke kommunikasies onwelkom is, is skuldig

aan 'n misdryf en, na skuldigbevinding, strafbaar met die strafmaatreëls wat in artikel 89 (1) voorgeskryf word.

46 Prestasie

(1) Tensy die partye anders ooreengekom het, moet die leweransier die bestelling uitvoer binne 30 dae na die dag waarop die leweransier die bestelling ontvang het.

(2) Wanneer 'n leweransier versuim om die bestelling binne 30 dae of binne die ooreengekome tydperk uit te voer, kan die verbruiker die ooreenkoms met sewe dae geskrewe kennis beëindig.

(3) Indien 'n leweransier nie ingevolge die ooreenkoms uitvoering kan gee nie, op grond daarvan dat die bestelde goedere of dienste nie beskikbaar is nie, moet die leweransier die verbruiker onmiddellik van hierdie feit in kennis stel en enige betalings binne 30 dae na die datum van sodanige kennisgewing terugbetaal.

47 Toepaslikheid van buitelandse reg

Die beskerming wat in hierdie Hoofstuk aan verbruikers verleen word, is van toepassing ongeag die regstelsel wat op die betrokke ooreenkoms van toepassing is.

48 Nie-uitsluiting

Enige bepaling in 'n ooreenkoms wat die regte waarvoor in hierdie Hoofstuk voorsiening gemaak word, uitsluit, is ongeldig.

49 Klagtes aan Verbruikersakekomitee

'n Verbruiker kan 'n klagte by die Verbruikersakekomitee indien ten opsigte van enige nie-nakoming van die bepalings van hierdie Hoofstuk deur 'n leweransier.

HOOFSTUK VIII
BESKERMING VAN PERSOONLIKE INLIGTING (aa 50-51)

50 Omvang van beskerming van persoonlike inligting

(1) Hierdie Hoofstuk is slegs van toepassing op persoonlike inligting wat deur middel van elektroniese transaksies verkry is.

(2) 'n Datakontroleur kan vrywilliglik die beginsels in artikel 51 vermeld, onderskryf deur sodanige feit in enige ooreenkoms met 'n datasubjek in te skryf.

(3) 'n Datakontroleur moet al die beginsels in artikel 51 vermeld, onderskryf en nie slegs dele daarvan nie.

(4) Die regte en verpligtinge van die partye met betrekking tot die skending van die beginsels in artikel 51 vermeld, word beheers deur die bedinge van enige ooreenkoms tussen hulle.

51 Beginsels vir elektroniese insameling van persoonlike inligting

(1) 'n Datakontroleur moet die uitdruklike geskrewe toestemming van die datasubjek hê vir die insameling, vergelyking, prosessering of openbaring van enige inligting oor daardie datasubjek, tensy hy of sy regtens toegelaat word of vereis word om dit te doen.

(2) 'n Datakontroleur mag nie persoonlike inligting oor 'n datasubjek wat nie nodig is vir die wettige doel waarvoor die persoonlike inligting vereis word elektronies versoek, insamel, vergelyk, prosesseer of berg nie.

(3) Die datakontroleur moet die spesifieke doel waarvoor enige persoonlike inligting versoek, ingesamel, vergelyk, geprosesseer of geberg word, skriftelik aan die datasubjek openbaar.

(4) Die datakontroleur mag nie sonder die uitdruklike geskrewe toestemming van die datasubjek persoonlike inligting vir 'n ander doel as die geopenbaarde doel gebruik nie, tensy hy of sy regtens toegelaat of vereis word om dit te doen.

(5) Die datakontroleur moet, solank die persoonlike inligting gebruik word en vir 'n tydperk van minstens een jaar daarna, 'n aantekening hou van die persoonlike inligting en die spesifieke doel waarvoor die persoonlike inligting ingesamel is.

(6) 'n Datakontroleur mag nie enige persoonlike inligting wat gehou word aan 'n derde party openbaar, tensy regtens vereis of toegelaat of spesifiek skriftelik deur die datasubjek daartoe gemagtig nie.

(7) Die datakontroleur moet, solank die persoonlike inligting gebruik word en vir 'n tydperk van minstens een jaar daarna, 'n rekord hou van enige derde party aan wie die persoonlike inligting geopenbaar is en van die datum waarop en die doel waarvoor dit geopenbaar is.

(8) Die datakontroleur moet alle persoonlike inligting wat verouderd geraak het, skrap of vernietig.

(9) 'n Party wat beskik oor persoonlike inligting kan daardie persoonlike inligting gebruik om profiele vir statistiese doeleindes saam te stel en kan vrylik handel dryf met sodanige profiele en statistiese data, solank die profiele of statistiese data nie deur 'n derde party gekoppel kan word aan enige spesifieke datasubjek nie.

HOOFSTUK IX
BESKERMING VAN KRITIEKE DATABASISSE (aa 52-58)

52 Bestek van beskerming van kritieke databasisse

Die bepalings van hierdie Hoofstuk is slegs van toepassing op 'n kritieke-databasisadministrateur en kritieke databasisse of dele daarvan.

53 Identifisering van kritieke data en kritieke databasisse

Die Minister kan by kennisgewing in die *Staatskoerant*-

(a) sekere klasse inligting wat van belang is vir die beskerming van die nasionale veiligheid van die Republiek of die ekonomiese en maatskaplike welsyn van sy burgers tot kritieke data vir die doeleindes van hierdie Hoofstuk verklaar; en

(b) prosedures instel wat by die identifisering van kritieke databasisse vir die doeleindes van hierdie Hoofstuk gevolg moet word.

54 Registrasie van kritieke databasisse

(1) Die Minister kan by kennisgewing in die *Staatskoerant*-

(a) vereistes bepaal vir die registrasie van kritieke databasisse by die Departement of die ander liggaam wat die Minister aanwys;

(b) prosedures bepaal wat vir registrasie gevolg moet word; en

(c) enige ander aangeleentheid met betrekking tot registrasie bepaal.

(2) By die toepassing van hierdie Hoofstuk beteken registrasie van 'n kritieke databasis die aanteken van die volgende inligting in 'n register wat deur die Departement of die ander liggaam wat die Minister aanwys, bygehou word:

(a) Die volle naam, adres en kontakbesonderhede van die administrateur van die kritieke databasis;

(b) die ligging van die kritieke databasis, met inbegrip van die ligging van konstituerende dele daarvan waar 'n kritieke databasis nie op 'n enkele plek geberg word nie;

(c) 'n algemene beskrywing van die kategorieë of tipes inligting wat in die kritieke databasis geberg word, met uitsluiting van die inhoud van so 'n kritieke databasis.

55 Bestuur van kritieke databasisse

(1) Die Minister kan sekere minimum standaarde of verbiedinge voorskryf ten opsigte van-

(a) die algemene bestuur van kritieke databasisse;

(b) toegang tot, oordrag en beheer van kritieke databasisse;

(c) infrastrukturele of prosedurele reëls en vereistes om die integriteit en egtheid van kritieke data te verseker;

(d) prosedures en tegnologiese metodes wat gebruik moet word by die berging of bewaring van kritieke databasisse;

(e) rampherstelplanne in die geval van verlies van kritieke databasisse of dele daarvan; en

(f) enige ander aangeleentheid wat vereis word vir die voldoende beskerming, bestuur en beheer van kritieke databasisse.

(2) Ten opsigte van kritieke databasisse wat deur openbare liggame geadministreer word, moet alle regulasies wat in subartikel (1) beoog word, uitgevaardig word in oorleg met alle Kabinetslede wat deur die bepalings van hierdie Hoofstuk geraak word: Met dien verstande dat die Minister nie inligting in artikel 54 (2) beoog moet aanteken nie indien daardie inligting redelikerwys-

(a) die sekerheid van sodanige databasisse kan aantas; of

(b) die fisiese veiligheid van 'n persoon in beheer van die kritieke databasis kan aantas.

(3) Hierdie Hoofstuk mag nie so uitgelê word dat dit die reg van 'n openbare liggaam aantas om enige werksaamheid te verrig wat ingevolge enige ander wetgewing gemagtig is nie.

56 Beperkings op openbaarmaking van inligting

(1) Inligting vervat in die register waarvoor in artikel 54 voorsiening gemaak word, mag nie aan enige persoon openbaargemaak word anders as aan werknemers van die Departement wat verantwoordelik is vir die hou van die register nie.

(2) Subartikel (1) is nie van toepassing nie ten opsigte van inligting wat openbaargemaak word-

(a) aan 'n toepaslike owerheid wat 'n kriminele oortreding ondersoek of vir die doeleindes van enige strafverrigtinge;

(b) aan regeringsinstansies wat verantwoordelik is vir veiligheid en sekuriteit in die Republiek na aanleiding van 'n amptelike versoek;

(c) aan 'n kuberinspekteur vir doeleindes van artikel 57;

(d) na aanleiding van artikels 11 en 30 van die Wet op Bevordering van Toegang tot Inligting, 2000; of

(e) vir doeleindes van enige siviele verrigtinge wat betrekking het op die kritieke data of dele daarvan.

57 Reg op inspeksie

(1) Die Direkteur-generaal kan, van tyd tot tyd, oudits laat uitvoer by 'n administrateur van 'n kritieke databasis om nakoming van die bepalings van hierdie Hoofstuk te evalueer.

(2) Die oudit kan deur kuberinspekteurs of 'n onafhanklike ouditeur uitgevoer word.

58 Nie-nakoming van Hoofstuk

(1) Indien die oudit wat in artikel 57 beoog word, nie-nakoming van hierdie Hoofstuk deur die administrateur van 'n kritieke databasis aantoon, moet die Direkteur-generaal die administrateur van die kritieke databasis skriftelik daarvan verwittig en-

(a) die bevindinge van die ouditverslag uiteensit;

(b) die handeling uiteensit wat vereis word om die nie-nakoming reg te stel; en

(c) die tyd uiteensit waarbinne die regstellingsaksie uitgevoer moet word.

(2) Die administrateur van 'n kritieke databasis wat nalaat om die regstellingsaksie uit te voer binne die tydperk wat in die kennisgewing aangegee word, is skuldig aan 'n misdryf.

HOOFSTUK X
DOMEINNAAMOWERHEID EN ADMINISTRASIE (aa 59-69)

Deel 1
Instelling en inlywing van .za-Domeinnaamowerheid (aa 59-61)

59 Instelling van Owerheid

'n Regspersoon word hierby ingestel wat bekend moet staan as die .za-

Domeinnaamowerheid, met die doel om verantwoordelikheid te aanvaar vir die .za-domeinnaamruimte vanaf 'n datum bepaal deur die Minister by kennisgewing in die *Staatskoerant* en by kennisgewing aan alle relevante owerhede.

60 Inlywing van Owerheid

(1) Die Minister moet 12 maande vanaf die datum van inwerkingtreding van hierdie Wet, alle stappe doen wat nodig is vir die inlywing van die Owerheid as 'n maatskappy beoog in artikel 21 (1) van die Maatskappywet, 1973 (Wet 61 van 1973).

(2) Alle burgers en permanente inwoners van die Republiek is benoembaar vir lidmaatskap van die Owerheid en moet op aansoek geregistreer word as lede, teen betaling van 'n nominale bedrag om die koste van registrasie van lidmaatskap te dek, en sonder dat aan enige formaliteit voldoen hoef te word.

(3) Met die oog op die inlywing van die Owerheid moet 'n persoon wat die Minister verteenwoordig en die lede van Namespace ZA soos op die datum van die aansoek vir inlywing, geag word lede van die Owerheid te wees.

61 Owerheid se akte van oprigting en statute

(1) Die akte van oprigting en statute van die Owerheid moet met hierdie Hoofstuk en, behalwe waar hierdie Hoofstuk anders bepaal, ook met die Maatskappywet, 1973 (Wet 61 van 1973), bestaanbaar wees.

(2) Ondanks die Maatskappywet, 1973, het 'n wysiging van die akte van oprigting en statute wat 'n uitwerking het op enige reëling deur enige bepaling van hierdie Hoofstuk getref, geen regskrag en regswerking nie tensy die Minister skriftelik tot sodanige wysiging ingestem het, welke instemming nie onredelik weerhou mag word nie.

(3) Geen geld is betaalbaar ingevolge die Maatskappywet, 1973, ten opsigte van die reservering van die naam van die maatskappy, die registrasie van die vermelde akte van oprigting en statute en die uitreiking van die sertifikaat om met besigheid te begin nie.

(4) Die akte van oprigting en statute van die Owerheid moet, onder andere, voorsiening maak vir-

(a) die reëls vir die belê en hou van vergaderings van die Raad, met inbegrip van die kworum vereis vir en die notule wat gehou moet word van daardie vergaderings;

(b) die wyse waarop besluite geneem moet word;

(c) die instelling van enige afdeling van die Owerheid om gespesialiseerde werksaamhede te verrig;

(d) die instelling en werking van komitees, met inbegrip van 'n bestuurskomitee;

(e) die koöptering deur die Raad of 'n komitee van enige persoon om die Owerheid of komitee met die oorweging van enige besondere aangeleentheid by te staan;

(f) die voorbereiding deur die Raad van 'n jaarlikse besigheidsplan ingevolge waarvan die bedrywighede van die Owerheid jaarliks beplan word;

(g) die bank en belegging van fondse deur die Raad;

(h) bepalings ter reëling van die wyse waarop, en die prosedures waarvolgens, kundigheid van enige persoon verkry kan word om die oogmerke van die Owerheid te bevorder;

(i) die beslegting deur arbitrasie van enige geskil aangaande die uitleg van die akte van oprigting en statute van die Owerheid;

(j) die delegering van bevoegdhede en opdra van pligte aan direkteure, komitees en werknemers: Met dien verstande dat die Raad-

(i) nie van enige bevoegdheid of plig uit hoofde van die delegasie of opdrag ontneem mag word nie; en

(ii) enige besluit geneem kragtens enige delegering of ingevolge enige opdrag kan verander of ter syde kan stel;

(k) die prosedures en kriteria vir die oprigting en opsegging van tweedevlakdomeine aan sulke domeine;

(l) appèlmeganismes;

(m) die ampstermyn van direkteure;

(n) die omstandighede waaronder en die wyses waarop 'n direkteurskap beëindig word;

(o) kriteria vir die diskwalifikasie van direkteure;

(p) die wyse waarop toelaes vasgestel word wat aan direkteure betaal moet word vir bywoon van vergaderings; en

(q) die bevoegdhede en pligte van direkteure.

Deel 2
Bestuur en personeelvoorsiening van Owerheid (aa 62-63)

62 Raad van direkteure van Owerheid

(1) Die Owerheid word bestuur en beheer deur 'n Raad van direkteure wat bestaan uit nege direkteure, van wie een die voorsitter is.

(2) Die aanstellingsproses is soos volg:

(a) Die Minister moet 'n onafhanklike kiespaneel aanstel wat bestaan uit vyf persone wat openbare respek afdwing vir hulle regverdigheidsin, wysheid en begrip van kwessies rakende die Internet, kultuur, taal, die akademie en die sakewêreld, wie se name in 'n kennisgewing in die *Staatskoerant* gepubliseer moet word;

(b) die Minister moet 'n uitnodiging rig aan die publiek vir nominasies vir lede van die Raad deur middel van koerante wat algemene sirkulasie deur die hele Republiek het, gekoppelde nuusdienste, radio en by kennisgewing in die *Staatskoerant*;

(c) nominasies moet gedoen word aan die paneel wat ingevolge paragraaf *(a)* saamgestel is;

(d) die paneel moet by die Minister aanbeveel die name van nege persone om in die Raad aangestel te word met inagnememing van die sektore van belanghebbendes wat in subartikel 3 *(b)* vermeld word;

(e) indien die Minister nie oortuig is dat die aanbeveling van die paneel aan subartikel (3) voldoen nie, kan die Minister die paneel vra om die aanbeveling te hersien en nuwe aanbevelings te maak;

(f) die Minister moet die lede van die Raad aanstel, en die name van diegene wat aangestel is in die *Staatskoerant* publiseer;

(g) die Minister moet die Voorsitter van die Raad aanstel vanuit die name wat deur die paneel aanbeveel is.

(3) *(a)* Die Raad, in sy geheel gesien, moet breedweg verteenwoordigend wees van die demografie van die land, ook met verwysing na geslag en gestremdheid.

(b) Sektore van belanghebbendes soos in subartikel 2 *(d)* bedoel, is-

(i) Die bestaande Domeinnaamgemeenskap;

(ii) Akademiese en regsektore;

(iii) Wetenskap-, tegnologie- en ingenieursektore;

(iv) Arbeid;

(v) Sake en die privaatsektor;

(vi) Kultuur en taal;

(vii) Openbare sektor;

(viii) Internetgebruikersgemeenskap.

(4) Direkteure moet persone wees wat verbind is tot regverdigheid, openheid en verantwoordbaarheid en aan die oogmerke van hierdie Wet.

(5) Alle direkteure dien in 'n deeltydse en nie-uitvoerende hoedanigheid.

(6) Enige vakature in die Raad moet gevul word ingevolge subartikels (2) en (3).

63 Personeel van Owerheid

(1) Die hoof- uitvoerende beampte van die Owerheid wat deur die Raad aangestel word, moet alle werk verbonde aan die werksaamhede van die Owerheid uitvoer.

(2) Die hoof- uitvoerende beampte moet bygestaan word deur personeel wat deur die Raad aangestel word.

(3) Die Raad moet die diensvoorwaardes, vergoeding en diensvoordele van die hoof- uitvoerende beampte en die personeel bepaal.

(4) Indien die hoof- uitvoerende beampte om enige rede nie in staat is om sy of haar werksaamhede te verrig nie, kan die Raad 'n persoon in diens van die Owerheid aanwys om as waarnemende hoof- uitvoerende beampte op te tree totdat die hoof- uitvoerende beampte in staat is om diens te hervat.

Deel 3
Werksaamhede van Owerheid (aa 64-65)

64 Lisensiëring van registrateurs en registrasiekantore

(1) Geen persoon mag 'n bewaarplek op datum bring of 'n tweedevlakdomein administreer tensy sodanige persoon deur die Owerheid gelisensieër is om dit te doen nie.

(2) 'n Aansoek om as 'n registrateur of registrasiekantoor gelisensieër te word, moet op die voorgeskrewe wyse en behoudens die voorgeskrewe gelde gedoen word.

(3) Die Owerheid moet die voorgeskrewe voorwaardes en kriteria toepas wanneer 'n aansoek in subartikel (2) bedoel, geëvalueer word.

65 Werksaamhede van Owerheid

(1) Die Owerheid moet-

(a) die .za-domeinnaamruimte administreer en bestuur;

(b) voldoen aan die internasionale beste praktyk in die administrasie van die .za-domeinnaamruimte;

(c) registrasiekantore lisensieer en reël;

(d) registrateurs vir die onderskeie registrasiekantore lisensieer en reël; en

(e) riglyne publiseer oor-

(i) die algemene administrasie en bestuur van die .za-domeinnaamruimte;

(ii) die vereistes en prosedures vir domeinnaamregistrasie; en

(iii) die onderhou van en openbare toegang tot 'n bewaarplek,

met behoorlike inagneming van die beleidslasgewings wat die Minister van tyd tot tyd by kennisgewing in die *Staatskoerant* kan uitvaardig.

(2) Die Owerheid moet openbare bewustheid aangaande die ekonomiese en kommersiële voordele van domeinnaamregistrasie bevorder.

(3) Die Owerheid-

(a) kan dié ondersoeke loods wat hy nodig ag;

(b) moet navorsing doen oor en op die hoogte bly van ontwikkelings in die Republiek en elders oor die domeinnaamstelsel;

(c) moet voortdurend die mate waarin die .za-domeinnaamruimte voldoen aan die behoeftes van die burgers van die Republiek besigtig en evalueer; en

(d) kan, van tyd tot tyd, inligting uitreik oor die registrasie van domeinname in die Republiek.

(4) Die Owerheid kan, en moet wanneer deur die Minister daartoe versoek,

aanbevelings aan die Minister doen met betrekking tot beleid aangaande enige aangeleentheid wat op die .za-domeinnaamruimte betrekking het.

(5) Die Owerheid moet voortdurend die doeltreffendheid van hierdie Wet evalueer en dinge wat ingevolge daarvan insake die bestuur van die .za-domeinnaamruimte gedoen word.

(6) Die Owerheid kan-

(a) met enige persoon of ander owerheid skakel, oorleg pleeg en saamwerk; en

(b) deskundiges en ander konsultante aanstel op die voorwaardes as wat die Owerheid bepaal.

(7) Die Owerheid moet die gevestigde regte en belange respekteer en ondersteun van partye wat aktief met die bestuur en administrasie van die .za-domeinnaamruimte gemoeid was ten tyde van sy instelling: Met dien verstande dat-

(a) sodanige partye 'n tydperk van ses maande verleen moet word waartydens hulle kan voortgaan om ten opsigte van hul bestaande gedelegeerde subdomeine op te tree; en

(b) na die verstryking van die tydperk van ses maande, sodanige partye behoorlik aansoek moet doen om gelisensieerde registrateurs en registrasiekantore te wees soos waarvoor in hierdie Deel voorsiening gemaak word.

Deel 4
Finansies en verslagdoening (aa 66-67)

66 Finansies van Owerheid

(1) Alle gelde wat deur die Owerheid ontvang word, moet gedeponeer word in 'n bankrekening in die naam van die Owerheid by 'n bank wat kragtens die Bankwet, 1990 (Wet 94 van 1990), of by 'n onderlinge bank wat kragtens die Wet op Onderlinge Banke, 1993 (Wet 124 van 1993), opgerig is.

(2) Die hoof- uitvoerende beampte is die rekenpligtige beampte van die Owerheid, en moet verseker dat-

(a) behoorlik rekord gehou word van al die finansiële transaksies, bates en laste van die Owerheid; en

(b) so gou as moontlik, maar nie later nie as drie maande na die einde van 'n boekjaar, rekeningstate wat die inkomste en uitgawes van die Owerheid

weergee en 'n balansstaat van die bates en laste van die Owerheid soos aan die einde van die boekjaar, opgestel word en aan die Raad en Minister voorgelê word.

(3) Die Owerheid word gefinansier vanuit-

(a) die kapitaal wat in die Owerheid belê of daaraan geleen is;

(b) geld wat deur die Parlement vir daardie doel bewillig is;

(c) inkomste verkry uit die verkoop of ander kommersiële benutting van sy lisensies, goedkeurings, produkte, tegnologie, dienste of kundigheid ingevolge hierdie Wet;

(d) lenings wat deur die Owerheid aangegaan is;

(e) die opbrengste van enige verkoop van bates;

(f) inkomste of rente verdien op die Owerheid se kontantbalanse, of op geld daardeur belê; en

(g) geld wat ontvang is by wyse van toewysing, bydrae, donasie of erfenis van enige bron, binne of buite die Republiek.

(4) Die fondse van die Owerheid moet gebruik word om uitgawes te dek wat deur die Owerheid aangegaan is in verband met sy funksionering, besigheid en bedrywighede ingevolg hierdie Wet.

(5) *(a)* Die gelde mag so gebruik word slegs soos daarvoor voorsiening gemaak is in 'n staat van die Owerheid se geraamde inkomste en uitgawes wat deur die Minister goedgekeur is.

(b) Geld wat by wyse van toewysing, bydrae, donasie of erfenis ingevolge subartikel (3) *(g)* ontvang is, moet aangewend word ooreenkomstig enige voorwaardes wat deur die betrokke toekenner, bydraer, donateur of erflater opgelê is.

(6) *(a)* Die Raad moet in elke boekjaar, op 'n tyd deur die Minister vasgestel, aan die Minister vir goedkeuring 'n staat van die Owerheid se geraamde inkomste en uitgawes vir die volgende boekjaar voorlê.

(b) Die Raad kan te eniger tyd in die loop van 'n boekjaar, 'n bykomende staat van geraamde inkomste en uitgawes van die Owerheid vir daardie boekjaar voor die Minister vir goedkeuring voorlê.

(c) Die Minister kan goedkeuring verleen aan die staat in paragraaf *(a)* bedoel, met die goedkeuring van die Minister van Finansies.

(d) Die Owerheid mag nie enige uitgawes aangaan wat die totale bedrag wat kragtens paragraaf *(c)* goedgekeur is, oorskry nie.

(7) Die Raad kan 'n reserwefonds stig vir enige doel wat met die Owerheid se werksaamhede kragtens hierdie Wet verband hou en wat deur die Minister goedgekeur is, en kan aan die reserwefonds toewys die geld wat vir die doeleindes beskikbaar gestel word in die staat van geraamde inkomste en uitgawes of bykomende staat in subartikel (6) beoog.

(8) In die mate wat die Owerheid van wegspringkapitaal deur die Staat voorsien word, kan die Owerheid, ten keuse van die Minister van Finansies, onderworpe gestel word aan die Wet op Openbare Finansiële Bestuur, (Wet 1 van 1999), tot tyd en wyl die Owerheid, na die bevrediging van die Minister van Finansies, selfonderhoudend word deur die alternatiewe inkomstebronne waarvoor daar in subartikel (3) voorsiening gemaak word.

67 Verslae

So gou doenlik na die einde van elke boekjaar, moet die Raad 'n verslag oor sy bedrywighede gedurende daardie jaar voorlê aan die Minister wat dan daardie verslag in die Parlement ter tafel moet lê.

Deel 5
Regulasies (a 68)

68 Regulasies aangaande Owerheid

(1) Die Owerheid kan, met die goedkeuring van die Minister, regulasies uitvaardig aangaande-

(a) die vereistes waaraan registrasiekantore en registrateurs moet voldoen ten einde gelisensieer te word, met inbegrip van objektiewe standaarde met betrekking tot operasionele akkuraatheid, stabiliteit, kragdadigheid en effektiwiteit;

(b) die omstandighede waaronder en die wyse waarop registrasies opgedra, geregistreer, hernu, geweier of herroep kan word deur die registrasiekantore, met die behoorlike inagneming van die uitdruklike erkenning van die reg van groepe en lede van groepe binne die Republiek om hulle te identifiseer met kultuur-, taal-, geografiese, inheemse of ander uitdrukkings van erfenis, met inbegrip van enige sigbare of hoorbare elemente of kenmerke daarvan, of om dit te gebruik of te kommunikeer;

(c) prysvasstellingsbeleid;

(d) bepalings vir die herstel van 'n domeinnaamregistrasie en strawwe vir laat betalings;

(e) die bedinge van die ooreenkoms vir die domeinnaamregistrasie wat registrasiekantore en registrateurs moet aanneem en gebruik by die registrasie van domeinname, met inbegrip van kwessies ten opsigte van privaatheid, verbruikersbeskerming en alternatiewe geskilbeslegting;

(f) prosesse en prosedures om onregverdige en nie-mededingende praktyke te vermy, met inbegrip van vooroordeel teenoor, of voorkeurbehandeling van, werklike of voornemende geregistreerdes, registrasiekantore of registrateurs, protokolle of produkte;

(g) vereistes om te verseker dat elke domeinnaam 'n administratiewe en tegniese kontak bevat;

(h) die skepping van nuwe subdomeine;

(i) prosedures om die monitering van nakoming van die bepalings van hierdie Wet en die regulasies waarvoor in hierdie Hoofstuk voorsiening gemaak word, met inbegrip van gereelde tegniese oudits van die .za-domeinnaamruimte, te verseker;

(j) sodanige ander aangeleenthede met betrekking tot die .za-domeinnaamruimte wat nodig is om voor te skryf om die oogmerke van hierdie Hoofstuk te bereik; en

(k) beleid wat deur die Owerheid toegepas moet word.

Deel 6
Alternatiewe geskilbeslegting (a 69)

69 Alternatiewe geskilbeslegting

(1) Die Minister, in oorleg met die Minister van Handel en Nywerheid, moet regulasies uitvaardig vir 'n alternatiewe meganisme vir die beslegting van geskille ten opsigte van die .za-domeinnaamruimte.

(2) Die regulasies moet uitgevaardig word met behoorlike inagneming van internasionale presedent.

(3) Die regulasies kan-

(a) geskilbeslegtingsprosedures voorskryf in die geval van sekere tipes geskille wat in die regulasies bepaal word en wat op 'n domeinnaamregistrasie betrekking het;

(b) die rol voorskryf wat die Owerheid moet vervul by die administrasie van die geskilbeslegtingsprosedure;

(c) die aanstelling, rol en werksaamheid van geskilbeslegtingsberegters voorskryf;

(d) die prosedure en reëls wat by die beregting van geskille gevolg moet word, voorskryf;

(e) onwettige optrede of handelinge ten opsigte van domeinname voorskryf, terwyl tussen strafregtelike en siviele aanspreeklikheid onderskei word;

(f) maatreëls voorskryf om onwettige optrede of handelinge ten opsigte van domeinname te verhinder;

(g) die wyse waarop koste van en tyd waarbinne 'n vasstelling gemaak moet word, voorskryf;

(h) die implementering voorskryf van vasstellings wat ingevolge die geskilbeslegtingsprosedures gemaak is;

(i) die beperking van aanspreeklikheid van registrateurs en registrasiekantore vir die implementering van 'n vasstelling voorskryf; en

(j) die afdwinging en publikasie van vasstellings voorskryf.

HOOFSTUK XI
BEPERKING VAN AANSPREEKLIKHEID VAN DIENSVERSKAFFERS (aa 70-79)

70 Woordomskrywing

In hierdie Hoofstuk beteken 'diensverskaffer' enige persoon wat inligtingstelseldienste verskaf.

71 Erkenning van verteenwoordigende liggaam

(1) Die Minister kan, op aansoek deur 'n bedryfsverteenwoordigende liggaam vir diensverskaffers, sodanige liggaam by kennisgewing in die *Staatskoerant* erken vir die doeleindes van artikel 72.

(2) Die Minister kan slegs 'n verteenwoordigende liggaam in subartikel (1) bedoel, erken indien die Minister tevrede is dat-

(a) sy lede aan 'n gedragskode onderworpe is;

(b) lidmaatskap aan voldoende kriteria onderworpe is;

(c) die gedragskode voortdurende ondersteuning van voldoende standaarde van gedrag vereis; en

(d) die verteenwoordigende liggaam in staat is om sy gedragskode voldoende te moniteer en af te dwing.

72 Voorwaardes van toepaslikheid

Die beperkings op aanspreeklikheid by hierdie Hoofstuk ingestel, is slegs op 'n diensverskaffer van toepassing indien-

(a) die diensverskaffer 'n lid is van die verteenwoordigende liggaam bedoel in artikel 71; en

(b) die diensverskaffer die amptelike gedragskode van daardie verteenwoordigende liggaam aangeneem en geïmplementeer het.

73 Blote geleibuis

(1) 'n Diensverskaffer is nie aanspreeklik vir verskaffing van toegangsverbindings tot, of vir die bedryf van fasiliteite vir inligtingstelsels, of versending, roetering of berging van databoodskappe via 'n inligtingstelsel onder sy of haar beheer nie, mits die diensverskaffer-

(a) nie die versending begin nie;

(b) nie die geadresseerde kies nie;

(c) die werksaamhede op 'n outomatiese, tegniese wyse verrig sonder selektering van die data; en

(d) nie die data vervat in die versending verander nie.

(2) Die handelinge van versending, roetering en van verskaffing van toegang bedoel in subartikel (1) sluit in die outomatiese, tussentydse en kortstondige berging van die versende inligting, vir sover dit plaasvind-

(a) vir die uitsluitlike doel om die versending in die inligtingstelsel uit te voer;

(b) op 'n wyse wat dit gewoonweg ontoeganklik maak vir enigeen anders as verwagte ontvangers; en

(c) vir 'n tydperk wat nie langer is as wat redelikerwys vir die versending

nodig is nie.

(3) Ondanks hierdie artikel kan 'n bevoegde hof 'n diensverskaffer beveel om onwettige bedrywigheid ingevolge enige ander wet te staak of te verhinder.

74 Berging in kasgeheue

(1) 'n Diensverskaffer wat data versend wat deur 'n ontvanger van die diens verskaf word via 'n inligtingstelsel onder sy of haar beheer is nie aanspreeklik nie vir die outomatiese, tussentydse en tydelike berging van daardie data, waar die doel van die berging van sodanige data is om die verdere versending van die data na ander ontvangers van die diens op hul versoek meer effektief te maak, solank die diensverskaffer-

(a) nie die data verander nie;

(b) voldoen aan die voorwaardes van toegang tot die data;

(c) voldoen aan reëls met betrekking tot die opdatering van die data, uiteengesit op 'n wyse wat wyd erken en gebruik word deur die bedryf;

(d) nie inmeng met die wettige gebruik van tegnologie, wat wyd erken en gebruik word deur die bedryf, om inligting oor die gebruik van die data te verkry nie; en

(e) toegang tot data wat geberg is, verwyder of ongeskik maak by ontvangs van 'n afhaalkennisgewing bedoel in artikel 77.

(2) Ondanks hierdie artikel kan 'n bevoegde hof 'n diensverskaffer gebied om onwettige bedrywigheid ingevolge enige ander wet te staak of te verhinder.

75 Gasheer wees

(1) 'n Diensverskaffer wat 'n diens verskaf wat bestaan uit die berging van data wat deur 'n ontvanger van die diens verskaf word, is nie aanspreeklik vir skade wat ontstaan weens data wat op die versoek van die ontvanger van die diens geberg word nie, solank die diensverskaffer-

(a) nie werklike kennis het dat die databoodskap of 'n bedrywigheid in verband met die databoodskap die regte van 'n derde party skend nie; of

(b) nie bewus is van feite of omstandighede waaruit die skendende bedrywigheid of die skendende aard van die databoodskap blyk nie; en

(c) by ontvangs van 'n afhaalkennisgewing bedoel in artikel 77, spoedig optree om toegang tot die data te verwyder of ongeskik te maak.

(2) Die beperkings op aanspreeklikheid by hierdie artikel ingestel, is nie van toepassing op 'n diensverskaffer nie tensy hy of sy 'n agent aangestel het om kennisgewings van skendings te ontvang en deur sy of haar dienste, ook op sy of haar webwerwe op plekke wat vir die publiek toeganklik is, die naam, adres, telefoonnommer en e-posadres van die agent voorsien het.

(3) Ondanks hierdie artikel kan 'n bevoegde hof 'n diensverskaffer beveel om onwettige bedrywigheid ingevolge enige ander wet te staak of verhinder.

(4) Subartikel (1) is nie van toepassing wanneer die ontvanger van die diens onder die gesag of die beheer van die diensverskaffer optree nie.

76 Inligtingsopsporingsgereedskap

'n Diensverskaffer is nie aanspreeklik nie vir skade deur 'n persoon gely indien die diensverskaffer gebruikers verwys na of koppel aan 'n webbladsy wat 'n skendende databoodskap of skenkende bedrywigheid bevat, deur inligtingopsporingsgereedskap te gebruik, met inbegrip van 'n adresboek, indeks, verwysing, wyser of hiperskakel, indien die diensverskaffer-

(a) nie werklik kennis het dat die databoodskap of 'n bedrywigheid in verband met die databoodskap die regte van daardie persoon skend nie;

(b) nie bewus is van feite of omstandighede waaruit die skendende bedrywigheid of die skendende aard van die databoodskap blyk nie;

(c) nie 'n finansiële voordeel ontvang wat regstreeks aan die skendende bedrywigheid toegeskryf kan word nie; en

(d) die verwysing na of koppeling aan die databoodskap of bedrywigheid verwyder of toegang daartoe ongeskik maak binne 'n redelike tyd nadat hy of sy ingelig is dat die databoodskap of die bedrywigheid wat met die databoodskap verband hou, die regte van 'n persoon skend.

77 Afhaalkennisgewing

(1) By die toepassing van hierdie Hoofstuk moet 'n kennisgewing van onwettige bedrywigheid op skrif wees, moet dit deur die klaer aan die diensverskaffer of sy of haar aangewese agent gerig wees, en moet dit insluit-

(a) die volle name en adres van die klaer;

(b) die skriftelike of elektroniese handtekening van die klaer;

(c) identifisering van die reg wat na bewering geskend is;

(d) identifisering van die materiaal of bedrywigheid wat na bewering die onderwerp van onwettige bedrywigheid is;

(e) die vereiste regstellende optrede wat deur die diensverskaffer ingestel moet word ten opsigte van die klagte;

(f) telefoniese en elektroniese kontakbesonderhede, as daar is, van die klaer;

(g) 'n verklaring dat die klaer te goeder trou optree; en

(h) 'n verklaring deur die klaer dat na sy of haar wete die inligting in die afhaalkennisgewing waar en korrek is.

(2) Enige persoon wat by 'n diensverskaffer kennis gee van onwettige aktiwiteite met die wete dat dit 'n wesenlike wanvoorstelling van die feite is, sal vir skadevergoeding vir die onregmatige verwydering aanspreeklik wees.

(3) 'n Diensverskaffer is nie aanspreeklik vir onregmatige verwydering as gevolg van 'n kennisgewing nie.

78 Geen algemene verpligting om te moniteer

(1) Wanneer die dienste in hierdie Hoofstuk beoog verskaf word, is daar geen algemene verpligting op 'n diensverskaffer om-

(a) die data wat hy of sy versend of berg, te moniteer nie; of

(b) aktief feite of omstandighede te soek wat op 'n onwettige bedrywigheid dui nie.

(2) Die Minister kan, behoudens artikel 14 van die Grondwet, prosedures vir diensverskaffers voorskryf om-

(a) die bevoegde openbare owerhede stiptelik in kennis te stel van beweerde onwettige bedrywighede onderneem of inligting voorsien deur ontvangers van hul dienste; of

(b) inligting wat die identifisering van ontvangers van hul diens moontlik maak, op versoek van die bevoegde owerhede, aan die owerhede te kommunikeer.

79 Voorbehoudsbepaling

Hierdie Hoofstuk raak nie-

(a) enige verpligting wat op 'n ooreenkoms gebaseer is nie;

(b) die verpligting van 'n diensverskaffer wat as sodanig optree onder 'n lisensiërings- of ander reguleringsbestel wat by of kragtens 'n wet ingestel is nie;

(c) enige verpligting wat by wet of deur 'n hof opgelê is om toegang tot enige databoodskap te verwyder, te blokkeer of te ontsê nie; of

(d) enige reg tot beperking van aanspreeklikheid gebaseer op die gemene reg of die Grondwet.

HOOFSTUK XII
KUBERINSPEKTEURS (aa 80-84)

80 Aanstelling van kuberinspekteurs

(1) Die Direkteur-generaal kan enige werknemer van die Departement aanstel as kuberinspekteur wat gemagtig is om die werksaamhede waarvoor in hierdie Hoofstuk voorsiening gemaak word, te verrig.

(2) 'n Kuberinspekteur moet voorsien word van 'n sertifikaat van aanstelling, onderteken deur of namens die Direkteur-generaal, waarin verklaar word dat hy of sy as 'n kuberinspekteur aangestel is.

(3) 'n Sertifikaat waarvoor in subartikel (2) voorsiening gemaak word, kan in die vorm van 'n gevorderde elektroniese handtekening wees.

(4) Wanneer 'n kuberinspekteur enige werksaamheid ingevolge hierdie Wet verrig, moet hy of sy-

(a) in besit wees van 'n sertifikaat van aanstelling in subartikel (2) bedoel; en

(b) daardie sertifikaat toon aan enige persoon wat-

(i) aan 'n ondersoek onderworpe is of 'n werknemer van daardie persoon is; of

(ii) versoek om die sertifikaat te sien.

(5) Iemand wat-

(a) 'n kuberinspekteur by die verrigting van sy of haar werksaamhede ingevolge hierdie Hoofstuk hinder of belemmer; of

(b) homself of haarself valslik voordoen as 'n kuberinspekteur,

is skuldig aan 'n misdryf.

81 Bevoegdhede van kuberinspekteurs

(1) 'n Kuberinspekteur kan-

(a) enige webwerf of bedrywigheid op 'n inligtingstelsel in die openbare domein moniteer en inspekteer en enige onwettige optrede by die toepaslike owerheid aanmeld;

(b) ten opsigte van 'n kriptografiediensverskaffer-

(i) die bedrywighede van 'n kriptografiediensverskaffer ondersoek met betrekking tot sy of haar nakoming of nie-nakoming van die bepalings van hierdie Wet; en

(ii) 'n bevel op skrif aan 'n kriptografiediensverskaffer uitreik om die bepalings van hierdie Wet na te kom;

(c) ten opsigte van 'n waarmerkingsdiensverskaffer-

(i) die bedrywighede van 'n waarmerkingsdiensverskaffer ondersoek met betrekking tot sy of haar nakoming of nie-nakoming van die bepalings van hierdie Wet;

(ii) die bedrywighede ondersoek van 'n waarmerkingsdiensverskaffer wat homself of haarself, of sy of haar produkte of dienste valslik voordoen as geakkrediteer te wees deur die Owerheid of erken te wees deur die Minister soos in Hoofstuk VI bepaal; en

(iii) 'n bevel op skrif aan die waarmerkingsdiensverskaffer uitreik om die bepalings van hierdie Wet na te kom; en

(d) ten opsigte van 'n administrateur van 'n kritieke databasis, 'n oudit doen waarvoor in artikel 57 voorsiening gemaak word.

(2) Enige statutêre liggaam, met inbegrip van die Suid-Afrikaanse Polisiediens, met magte van inspeksie of deursoeking en inbeslagneming ingevolge enige wet kan aansoek doen om bystand van 'n kuberinspekteur om te help met 'n ondersoek: Met dien verstande dat-

(a) die versoekende liggaam by die Departement moet aansoek doen om bystand op die voorgeskrewe wyse; en

(b) die Departement dergelike bystand kan magtig op sekere voorwaardes.

82 Bevoegdheid om te inspekteer, te deursoek en in beslag te neem

(1) 'n Kuberinspekteur kan, by die verrigting van sy of haar werksaamhede, te eniger redelike tyd, sonder vooraf kennisgewing en op gesag van 'n lasbrief wat ingevolge artikel 83 (1) uitgereik is enige perseel betree of toegang verkry tot 'n inligtingstelsel wat betrekking het op 'n ondersoek en-

(a) daardie perseel of inligtingstelsel deursoek;

(b) enige persoon op daardie perseel deursoek indien daar redelike gronde bestaan om te glo dat die persoon persoonlike besit het van 'n artikel, dokument of rekord wat op die ondersoek betrekking het;

(c) uittreksels neem uit, of afskrifte maak van enige boek, dokument of rekord wat op of in die perseel of in die inligtingstelsel is en wat op die ondersoek betrekking het;

(d) die lewering van toepaslike lisensies en registrasiesertifikate eis en dit inspekteer soos waarvoor in enige wet voorsiening gemaak word;

(e) enige fasiliteite op die perseel wat gekoppel is aan of geassosieer is met die inligtingstelsel en wat op die ondersoek betrekking het, inspekteer;

(f) toegang verkry tot die werking van enige rekenaar of toerusting wat deel vorm van die inligtingstelsel, en enige geassosieerde apparaat of materiaal wat die kuberinspekteur redelike gronde het om te vermoed in verband met enige misdryf gebruik word of gebruik is, en sodanige werking, apparaat of materiaal inspekteer;

(g) enige inligtingstelsel of deel daarvan gebruik of laat gebruik om enige data te soek wat in sodanige inligtingstelsel vervat is of daartoe beskikbaar is;

(h) van die persoon deur wie of ten behoewe van wie die kuberinspekteur redelike gronde het om te vermoed die rekenaar of inligtingstelsel gebruik word of is, of van enige persoon wat in beheer is van, of andersins betrokke is by die werking van die rekenaar of inligtingstelsel vereis om hom of haar te voorsien van die redelike tegniese en ander hulp wat hy of sy vir die doeleindes van hierdie Hoofstuk vereis; of

(i) die navrae doen wat nodig is om vas te stel of die bepalings van hierdie Wet of enige ander wet waarop die ondersoek gebaseer is, nagekom is.

(2) 'n Persoon wat weier om samewerking te verleen of 'n persoon hinder wat besig is met 'n wettige deursoeking en inbeslagneming ingevolge hierdie artikel is skuldig aan 'n misdryf.

(3) Die Strafproseswet, 1977 (Wet 51 van 1977), is met die nodige wysigings van toepassing op deursoekings en inbeslagnemings ingevolge hierdie Wet.

(4) By die toepassing van hierdie Wet sluit enige verwysing in die Strafproseswet, 1977, na 'perseel' en 'artikel' 'n inligtingstelsel sowel as databoodskappe in.

83 Verkryging van lasbrief

(1) 'n Landdros of regter kan, op versoek van 'n kuberinspekteur maar behoudens die bepalings van artikel 25 van die Strafproseswet, 1977 (Wet 51 van 1977), 'n lasbrief uitreik wat ingevolge hierdie Hoofstuk deur 'n kuberinspekteur vereis word.

(2) By die toepassing van subartikel (1) kan 'n landdros of regter 'n lasbrief uitreik waar-

(a) 'n misdryf in die Republiek gepleeg is;

(b) die onderwerp van 'n ondersoek-

(i) 'n Suid-Afrikaanse burger is of gewoonlik in die Republiek woonagtig is; of

(ii) in die Republiek aanwesig is op die tydstip dat aansoek om die lasbrief gedoen word; of

(c) inligting ter sake by die ondersoek toeganklik is vanaf die jurisdiksiegebied van die hof.

(3) 'n Lasbrief om te betree, te deursoek en in beslag te neem, kan te eniger tyd uitgereik word en moet-

(a) die perseel of inligtingstelsel wat betree en deursoek kan word, identifiseer; en

(b) vermeld watter handelinge daarkragtens uitgevoer kan word deur die kuberinspekteur aan wie die lasbrief uitgereik is.

(4) 'n Lasbrief om te betree en te deursoek, is geldig totdat-

(a) die lasbrief uitgevoer is;

(b) die lasbrief gekanselleer word deur die persoon wat dit uitgereik het of, in die afwesigheid van daardie persoon, deur 'n persoon met soortgelyke gesag;

(c) die doel waarvoor dit uitgereik is, verval het; of

(d) een maand na die datum waarop dit uitgereik is, verstryk het.

(5) 'n Lasbrief om 'n perseel binne te gaan en te deursoek, kan slegs gedurende die dag uitgevoer word, tensy die regter of landdros wat dit uitgereik het, magtig dat dit op enige ander tyd uitgevoer kan word.

84 Handhawing van vertroulikheid

(1) Behalwe by die toepassing van hierdie Wet of vir die vervolging van 'n misdryf of na aanleiding van 'n hofbevel, mag 'n persoon wat na aanleiding van enige bevoegdhede kragtens hierdie Hoofstuk verleen, toegang tot enige inligting verkry het nie sodanige inligting aan enige ander persoon openbaar nie.

(2) Enige persoon wat subartikel (1) oortree, is skuldig aan 'n misdryf en by skuldigbevinding strafbaar met 'n boete of met gevangenisstraf vir 'n tydperk wat nie ses maande oorskry nie.

HOOFSTUK XIII
KUBERMISDAAD (aa 85-89)

85 Woordomskrywing

In hierdie Hoofstuk, tensy die samehang anders aandui, beteken-

'toegang' ook die handelinge van 'n persoon wat, nadat hy of sy kennis geneem het van enige data, bewus word van die feit dat hy of sy nie gemagtig is om toegang tot daardie data te hê nie en nogtans voortgaan met toegang tot daardie data.

86 Ongemagtigde toegang tot, onderskepping van of inmenging met data

(1) Behoudens die Wet op die Verbod op Onderskepping en Meeluistering, 1992 (Wet 127 van 1992), is 'n persoon wat opsetlik toegang verkry tot enige data, of dit onderskep, sonder magtiging of toestemming om dit te doen, skuldig aan 'n misdryf.

(2) 'n Persoon wat opsetlik en sonder magtiging om dit te doen, inmeng met data op 'n wyse wat veroorsaak dat sodanige data verander, vernietig of andersins oneffektief gemaak word, is skuldig aan 'n misdryf.

(3) 'n Persoon wat enige toestel, met inbegrip van 'n rekenaarprogram of komponent, wat primêr ontwerp is om veiligheidsmaatreëls vir die beskerming van data te oorkom, wederregtelik vervaardig, verkoop, te koop aanbied, vir gebruik verkry, ontwerp, vir gebruik aanpas, versprei of besit, of enige van daardie handelinge verrig met betrekking tot 'n wagwoord, toegangskode of enige ander soortgelyke data, met die opset om sodanige item wederregtelik te gebruik om hierdie artikel te oortree, is skuldig aan 'n misdryf.

(4) 'n Persoon wat enige toestel of rekenaarprogram in subartikel (3) vermeld gebruik om wederregtelik veiligheidsmaatreëls te oorkom wat ontwerp is om sodanige data of toegang daartoe te beskerm, is skuldig aan 'n misdryf.

(5) 'n Persoon wat 'n handeling wat in hierdie artikel beskryf word, verrig met die opset om in te meng met toegang tot 'n inligtingstelsel wat neerkom op 'n ontsegging, met inbegrip van gedeeltelike ontsegging, van diens aan regmatige gebruikers, is skuldig aan 'n misdryf.

87 Rekenaarverwante afpersing, bedrog en vervalsing

(1) 'n Persoon wat enige van die handelinge in artikel 86 beskryf, verrig of dreig om te verrig met die doel om enige onwettige handelsvoordeel te verkry deur te onderneem om sodanige optrede te staak of daarmee op te hou, of deur te onderneem om enige skade aangerig as gevolg van daardie handeling te herstel, is skuldig aan 'n misdryf.

(2) 'n Persoon wat enige van die handelinge in artikel 86 beskryf, verrig met die doel om enige onwettige voordeel te verkry deur te veroorsaak dat vervalste data vervaardig word met die bedoeling dat dit beskou word of dat daar op gehandel word asof dit eg is, is skuldig aan 'n misdryf.

88 Poging, en hulpverlening

(1) 'n Persoon wat probeer om enige van die misdrywe in artikels 86 en 87 bedoel te pleeg, is skuldig aan 'n misdryf en is by skuldigbevinding strafbaar met die strawwe uiteengesit in artikel 89 (1) of (2), na gelang van die geval.

(2) Enige persoon wat aan iemand hulp verleen om enige van die misdrywe in artikels 86 en 87 bedoel te pleeg, is skuldig aan 'n misdryf en is by skuldigbevinding strafbaar met die strawwe uiteengesit in artikel 89 (1) of (2), na gelang van die geval.

89 Strawwe

(1) 'n Persoon wat skuldig bevind is aan 'n misdryf bedoel in artikels 37 (3), 40 (2), 58 (2), 80 (5), 82 (2) of 86 (1), (2) of (3) is strafbaar met 'n boete of gevangenisstraf vir 'n tydperk wat nie 12 maande oorskry nie.

(2) 'n Persoon wat skuldig bevind is aan 'n misdryf bedoel in artikel 86 (4) of (5) of artikel 87 is strafbaar met 'n boete of gevangenisstraf vir 'n tydperk wat nie vyf jaar oorskry nie.

HOOFSTUK XIV
ALGEMENE BEPALINGS (aa 90-95)

90 Jurisdiksie van howe

'n Hof in die Republiek wat 'n misdryf ingevolge hierdie Wet verhoor, het jurisdiksie waar-

(a) die misdryf in die Republiek gepleeg is;

(b) 'n voorbereidingshandeling vir die misdryf of enige deel van die misdryf in die Republiek gepleeg is, of waar enige gevolg van die misdryf 'n uitwerking in die Republiek gehad het;

(c) die misdryf deur 'n Suid-Afrikaanse burger of 'n persoon met permanente verblyf in die Republiek of deur 'n persoon wat in die Republiek sake doen, gepleeg is; of

(d) die misdryf gepleeg is aan boord van 'n skip of vliegtuig wat in die Republiek geregistreer is of op 'n reis of vlug na of vanaf die Republiek was op die tydstip toe die misdryf gepleeg is.

91 Voorbehoud van gemenereg

Hierdie Hoofstuk raak nie strafregtelike of sivielregtelike aanspreeklikheid ingevolge die gemenereg nie.

92 Herroeping van Wet 57 van 1983

Die Wet op Rekenaargetuienis, 1983, word hiermee herroep.

93 Beperking van aanspreeklikheid

Nóg die Staat, nóg die Minister, of enige werknemer van die Staat is aanspreeklik ten opsigte van enige handeling of late te goeder trou en sonder growwe nalatigheid in die verrigting van 'n werksaamheid ingevolge hierdie Wet nie.

94 Regulasies

Die Minister kan regulasies uitvaardig betreffende enige saak wat ingevolge hierdie Wet voorgeskryf kan of moet word of enige saak wat dit nodig of dienstig is om voor te skryf vir die behoorlike implementering of administrasie van hierdie Wet.

95 Kort titel en inwerkingtreding

Hierdie wet heet die Wet op Elektroniese Kommunikasies en Transaksies, 2002, en tree in werking op 'n datum wat die President by proklamasie in die *Staatskoerant* bepaal.

Bylae 1

(kyk artikel 4 (3))

Item	Kolom A	Kolom B
1.	Wet op Testamente, 1953 (Wet 7 van 1953)	11, 12, 13, 14, 15, 16, 18, 19 en 21
2.	Wet op die Vervreemding van Grond, 1981 (Wet 68 van 1981)	12 en 13
3.	Wet op Verhandelbare Instrumente, 1964 (Wet 34 van 1964)	12 en 13
4.	Wet op Seëlregte, 1968 (Wet 77 van 1968)	11, 12, 14

Bylae 2

(kyk artikel 4 (4))

1.	'n Ooreenkoms vir die vervreemding van onroerende eiendom soos bepaal in die Wet op Vervreemding van Grond, 1981 (Wet 68 van 1981).
2.	'n Ooreenkoms vir die langtermyn huur van onroerende eiendom vir langer as 20 jaar soos bepaal in die Wet op Vervreemding van Grond, 1981 (Wet 68 van 1981).
3.	Die verlyding, retensie en voorlegging van 'n testament of kodisil soos omskryf in die Wet op Testamente, 1953 (Wet 7 van 1953).
4.	Die verlyding van 'n verhandelbare instrument soos omskryf in die Wet op Verhandelbare Instrumente, 1964 (Wet 34 van 1964).

BYLAAG 6 (A)

RE REKENINGKUNDE

ALGEMEEN AANVAARDE REKENINGKUNDIGE PRAKTYK

RE TITEL

Rekeningkundige Raamwerk

000 Raamwerk vir die opstel en aanbieding van finansiële state

Standpunte oor Algemeen Aanvaarde Rekeningkundige Praktyk

100 Voorwoord by standpunte oor Algemeen Aanvaarde Rekeningkundige Praktyk
(Paragraaf .03 hersien)

101 Aanbieding van finansiële state

102 Inkomstebelasting

103 Netto wins of verlies vir die tydperk, fundamentele foute en veranderinge in rekeningkundige beleid

104 Verdienste per aandeel

105 Hure

107 Gebeure na die balansstaatdatum

108 Voorraad

109 Konstruksiekontrakte

110 Verantwoording vir beleggings in geassosieerdes

111 Inkomste

112 Die uitwerking van veranderings in wisselkoerse

114 Leenkoste

115 Segmentverslagdoening

116 Employee benefits *(Slegs in Engels uitgereik)*

117 Eindigende bedrywighede

118 Kontantvloeistate
119 Finansiële verslagdoening van belange in gesamentlike ondernemings
120 Openbaarmaking in die finansiële state van banke
121 Openbaarmaking in die finansiële state van langtermynversekeraars
123 Eiendom, aanleg en toerusting
124 Finansiële verslagdoening in hiperinflasionêre ekonomieë
125 Finansiële instrumente: openbaarmaking en aanbieding
126 Openbaarmaking deur verwante partye
127 Tussentydse finansiële verslagdoening
128 Waardedaling van bates
129 Ontasbare bates
130 Voorsienings, voorwaardelike aanspreeklikheid en voorwaardelike bates
131 Besigheidsamevoegings
132 Gekonsolideerde finansiële state en rekeningkundige verantwoording vir beleggings in filiale
133 Financial instruments: recognition and measurement *(Slegs in Engels uitgereik)*
134 Rekeningkundige verantwoording vir staatstoekennings en openbaarmaking van staatshulp
135 Beleggingseiendom
136 Accounting and reporting by retirement benefit plans *(Slegs in Engels uitgereik)*
137 Agriculture *(Slegs in Engels uitgereik)*

Rekeningkundige Riglyne

201 Openbaarmaking van die gevolge van prysveranderings op finansiële resultate

Rekeningkundige Menings

300 Voorwoord by menings deur die Taakmag vir Rekeningkundige Vraagpunte uitgespreek

303 Rekeningkundige verantwoording vir sekondêre belasting op maatskappye

306 Wesensverdienste – Uitwerking van die uitreiking van RE 103 (Hersien) op die berekening en openbaarmaking van verdienste per aandeel

Vertolkings van Standpunte oor Algemeen Aanvaarde Rekeningkundige Praktyk

400 Voorwoord by vertolkings van standpunte oor Algemeen Aanvaarde Rekeningkundige Praktyk

401 Konsekwentheid – verskillende kosteformules vir voorraad

402 Konsekwentheid – kapitalisering van leenkoste

403 Uitskakeling van ongerealiseerde winste en verliese op transaksies met geassosieerdes

405 Kwalifikasie van finansiële instrumente – voorwoordelike vereffeningsvoorsienings

406 Koste van die modifikasie van bestaande programmatuur

407 Ingebruikneming van die Euro

408 Eerste toepassing van standpunte oor Algemeen Aanvaarde Rekeningkundige Praktyk as die primêre rekeningkundige grondslag

409 Besigheidsamevoegings – klassifisering as óf verkrygings óf verenigings van belange

410 Staatshulp – geen spesifieke verband met bedryfsaktiwiteite nie

411 Buitelandse valuta – kapitalisering van verliese voortspruitend uit drastiese geldeenheidevaluasies

412 Konsolidasie – spesialedoel-entiteite

413 Gesamentlik beheerde entiteite – niemonetêre bydraes deur ondernemers

414 Eiendom, aanleg en toerusting – vergoeding vir die waardedaling in of verlies aan items

415 Bedryfshure – aansporings

416 Aandelekapitaal – herverkrygde eie ekwiteitsinstrument (tesourie-aandele)

417 Ekwiteit – koste van 'n ekwiteitstransaksie

418 Konsekwentheid – alternatiewe metodes

419 Verslagdoeningsgeldeenheid – meting en aanbieding van finansiële state ingevolge die standpunt oor die uitwerking van veranderings in wisselkoerse en die standpunt oor finansiële verslagdoening in hiperinflasionêre ekonomieë

420 Die ekwiteitsmetode vir rekeningkundige verantwoording – erkenning van verliese

421 Inkomstebelasting – verhaling van herwaardeerde nie-afskryfbare bates

422 Besigheidsamevoegings – latere aansuiwerings van billike waardes en klandisiewaarde waaroor aanvanklik verslag gedoen is

423 Eiendom, aanleg en toerusting – groot inspeksie- of opknappingskoste

424 Verdienste per aandeel – finansiële instrumente en ander kontrakte wat in aandele vereffen kan word

425 Inkomstebelasting – veranderinge in belastingstatus van 'n ondernemer of sy aandeelhouers *(Slegs in Engels uitgereik)*

427 Evaluating the substance of transactions involving the legal form of a lease *(Slegs in Engels uitgereik)*

428 Business combinations – "date of exchange" and fair value of equity instruments (*Slegs in Engels uitgereik)*

429 Disclosure – service concession arrangements (*Slegs in Engels uitgereik)*

430 Reporting currency – translation from measurement currency to presentation currency *(Slegs in Engels uitgereik)*

431 Revenue – barter transactions involving advertising services *(Slegs in Engels uitgereik)*

433 Consolidation an equity method – potential voting rights and allocation of ownership interests *(Slegs in Engels uitgereik)*

ANDER PUBLIKASIES

Auditing and Accounting Guides

	Datum Uitgereik
Profit forecasts	Jul 1989
Audit guide on short term insurance	Okt 1992
Audit and accounting guide on pension funds	Jun 1995
The auditor's relationship with the statutory actuary in the long-term insurance industry	Sep 1998
Audit guide on long-term insurance	Des 1998
Trading while factually insolvent	Jul 1999
Guide on performance audit in the public sector	Jul 1999
Guide on DTI programmes for auditors and other accredited persons	Jun 2000
#Audit and accounting guide on medical funds	Feb 2001
#Accounting guide on short-term insurance	Feb 2001
Audit and accounting guide on close corporations	Des 2001

Corporate Governance Series

Stakeholder Communication in the Annual Report	Jan 1997
Guidance for Directors: Reporting on Internal Control	Jan 1997
Guidance for Directors: Going Concern and Financial Reporting	Mrt 1997
Guidance for Directors: The Role of Internal Audit	Mei 1998

Information Technology Series

Paperless Business Transactions – an introduction to the risks and controls	Jan 1995
Controlling Paperless Business Transactions (Are the risks controlled?)	Des 1996
#Guide on data warehousing	Mei 2000

Other

Accountancy SA (monthly journal)	
Audit committees (published jointly with the Institute of Internal Auditors and the Institute of Directors in Southern Africa)	Okt 1991
Accounting and reporting practices in the mining industry	Feb 1995
Derivatives: management principles	Sep 1995
The value of an audit	Mrt 1999

SAOS/OU OUDITKUNDE

SUID-AFRIKAANSE OUDITSTANDAARDE

SAOS	TITEL
000	Preface to South African Standards on auditing and related services
OU	
Inleidende aangeleenthede (100-199)	
100	Gerusstellingsaanstellings
*110	Glossary of terms
120	Raamwerk van Suid-Afrikaanse standaarde vir oudit- en verwante dienste
Verantwoordelikhede (200-299)	
200	Die doelwit van en algemene beginsels wat 'n oudit van finansiële state reël
210	Voorwaardes van ouditaanstellings
220	Gehaltebeheer vir ouditwerk
230	Dokumentasie
240	Die ouditeur se verantwoordelikheid om bedrog en foute in 'n oudit van finansiële state te oorweeg
250	Oorweging van wette en regulasies in 'n oudit van finansiële state
2501	Die oorweging van omgewingsaangeleenthede in die oudit van finansiële state
Beplanning (300-399)	
300	Beplanning
310	Kennis van die besigheid

320 Ouditwesenlikheid

Interne beheer (400-499)

400 Risikobeoordeling en interne beheer

401 Ouditwerk in 'n rekenaarinligtingstelselomgewing

4011 Risikobeoordeling en interne beheer – Rekenaarinligtingstelsel kenmerke en –oorwegings

Ouditbewyse (500-599)

500 Ouditbewyse

505 Eksterne bevestigings

510 Aanvanklike aanstellings – beginsaldo's

520 Analitiese prosedures

530 Ouditsteekproewe en ander selektiewe toetsingsprosedures

540 Oudit van rekeningkundige ramings

550 Verwante partye

560 Gebeure na die balansstaatdatum

570 Lopende saak

580 Bestuursverklarings

Gebruik van ander se werk (600-699)

600 Gebruikmaking van die werk van 'n ander ouditeur

610 Oorweging van die werk van interne oudit

620 Gebruik van die werk van 'n kundige

Ouditgevolgtrekkings en verslagdoening (700-799)

700 Die ouditeursverslag oor finansiële jaarstate (Aanhangsel hersien)

710 Vergelykende syfers

720 Ander inligting in dokumente wat geouditeerde finansiële jaarstate bevat

730	Mededeling van ouditaangeleenthede aan diegene wat met beheer belas is

Gespesialiseerde gebiede (800-899)

800	Die ouditeursverslag oor ouditaanstellings vir 'n spesifieke doel

Verwante dienste (900-999)

*910	Engagements to review financial statements
920	Aanstellings vir die uitvoering van ooreengekome prosedures ten opsigte van finansiële inligting
930	Aanstellings om finansiële inligting te kompileer

Standpunte oor Ouditstandaarde

OU	Titel

Standpunte oor veldwerk

257	Navrae by prokureurs

Suid-Afrikaanse ouditpraktykstandpunte

SAOPS	
	Titel
*1000	Inter-bank confirmation procedures
*1001	IT environments – stand-alone personal computers
*1002	IT environments – on-line computer systems
*1003	IT environments – database systems
*1005	The special considerations in the audit of small entities
*1009	Computer assisted audit techniques
*1012	Auditing derivative financial instruments

*1013	Electronic commerce – effect on the audit of financial statements
1100	Bankbevestigings

**Slegs op die oomblik in Engels uitgereik.*

SV SPESIALE VERSLAE

SV	TITEL
1	Die agent, Artikel 20 bis (2)(b) van die Versekeringswet, 1943
2	Die Lloyds agent, Artikel 60 (1)(p) van die Versekeringswet, 1943
4	Rekonsiliasie – behuisingseise
5	Die Raad vir Balju's
6	Buspendelaar Subsidie-eise
9	Die Wet op Landbouprodukte-Agente, 1992
10	Verslag van die onafhanklike ouditeurs van .... (naam van beleggingsbestuurder) aan die uitvoerende komitee van die Suid-Afrikaanse Termynbeurs kragtens regulasie 8 (2)(b) uitgevaardig kragtens artikel 37 van die Wet op Beheer van Finansiële Markte, 1989

UITSTAANDE BLOOTSTELLINGSKONSEPTE

ED	TITEL	Date Issued	Comment Date
139	Reporting accountant's report on the report of historical financial information to be included in a prospectus or JSE circular	Jun 2000	Aug 2000
140	Report of historical financial information to be included in a prospectus or JSE circular	Jun 2000	Aug 2000
*145	The audit of international commercial banks	Nov 2000	30 Jan 2001
*146	The relationship between banking supervisors and banks' external auditors	Feb 2001	31 May 2001
*149	Auditing fair value measurements and disclosure	Nov 2001	30 Nov 2001
*150	Electronic commerce using the internet or other public networks – effect on the audit of financial statements	Nov 2001	15 Dec 2001

**Issued by the International Auditing and Assurance Standards Board and released for public comment in South Africa by the Auditing Standards Committee of the Public Accountants' and Auditors' Board*

151	Headline earnings	Feb 2002	15 Mar 2002

152	Preface to the AC500-series of Statements of Generally Accepted Accounting Practice	Feb 2002	30 Apr 2002
153	Accounting for secondary tax on companies	Feb 2002	30 Apr 2002
*154	Amendment to AC 116, employee benefits: asset ceiling	Feb 2002	25 Mar 2002
*155	Improvements	May 2002	1 Sep 2002

**Issued by the International Accounting Standards Board and released for public comment in South Africa by the Accounting Practices Committee.*

	Batch 6 of draft Interpretation of Statements of Generally Accepted Accounting Practice	Apr 2001	30 Jun 2001
*ED-AC 426	Property, plant and equipment incidental and start-up operations		

HO HUIDIGE OMSENDBRIEWE

HO	TITEL
02/84	Ouditverslae met betrekking tot aktebesorgingstransaksies
07/89	Die verkoop van rekenaar-apparatuur en –programmatuur aan hul kliënte deur lede in openbare praktyk
07/90	Prosedures vir geringe strafbare misdrywe
04/91	Versuim om boeke vir oudit te lewer
05/91	Die Instituut se adviesdienste
09/91	Riglyne vir finansiële jaarstate van primêre landbou-koöperasies
10/91	Aansoek om vrystelling van openbaarmaking van inligting in die finansiële jaarstate ingevolge Artikel 15A(1)(b) van die Maatskappyewet, 1973
08/92	Algemene uitvoeraansporingskema (AUAS)
09/92	Die ouditeur se betrokkenheid by die droogte-noodleningskema van die Departement van Landbou
04/93	Skoolbestuurskomitees
05/93	Dissiplinêre prosedures
06/93	Sekwestrasie van die boedel van 'n lid
03/94	Verhaling van professionele gelde
09/94	In- en uitvoertransaksies van omvangryke maatskappyonder-nemings -deviesebeheertoegewing
11/94	Die ouditeur se aanspreeklikheid teenoor 'n derde party
02/95	Gebruik van die titels GR (SA) en Geregistreerde Rekenmeesteer en Ouditeur
01/96	Hantering van die professionele aanspreeklikheid van reken-meesters
*01/97	Guidance for auditors: Regulation 37(5) to the Banks Act
*03/97	Maintenance of Standards

*04/97	Guidance for auditors: The motor industry development programme
*05/97	Reporting on entities listed under the Reporting by Public Entities Act
05/98	Reg van die Suid-Afrikaanse Inkomstediens (SAID) om ouditlêers aan te vra
06/98	Die behoud van rekords en ouditwerkspapiere
01/99	Buitelandse portefeuljebeleggings deur Suid-Afrikaanse institusionele beleggings
02/99	Aansoek om die remittering van dividend-inkomste van ongenoteerde maatskappye: deviesebeheervereistes
03/99	Inkomste-oordragte uit trusts: deviesebeheervereistes
*05/99	Auditor's report on the annual financial statements of private higher education institutions
07/99	Belasting en professionele etiek
08/99	Nakoming van Artikel 286(3) en paragraaf 5 van Bylae 4 van die Maatskappyewet, 61 van 1973 en Standpunte oor Algemeen Aanvaarde Rekeningkundige Praktyk
*01/100	Monitored compulsory continuing professional education
*02/00	Guidance for auditors: auditor's report to be submitted to SASRIA Limited (SASRIA) *(Slegs beskikbaar op die webblad)*
*03/00	Guidance for auditors: the audit of lines 68 to 72 of the DI 400 regulatory return submitted to the Registrar of Banks *(Slegs beskikbaar op die webblad)*
05/00	Status van professionele verklarings
06/00	Bedrae wat kragtens die verordeninge deur die Raad bepaal word
*01/01	Continuing professional education: competence self-appraisal
*03/01	Professional fees

*05/01	Material irregularities in terms of section 20(5) of the Public Accountants' and Auditors' Act, 1991
*01/02	Guidance for auditors: productive asset allowance of the motor industry development programme
*04/02	Guideline on fees for audits done on behalf of the Auditor-General

**Slegs in Engels uitgereik.*