Revisie van BS 7799 Part 1
Een vergelijking met de Code voor Informatiebeveiliging

Ernst J. Oud - Getronics Business Continuity BV

> And you all know, security
> Is mortals' chiefest enemy.
> Shakespeare - Macbeth Act III

Inleiding.

In november 1994 is de **'Code voor Informatiebeveiliging, een leidraad voor beleid en implementatie'** verschenen (hierna genoemd de Code). Dit document, uitgegeven door het Nederlands Normalisatie Instituut[1], is een vertaling van de British Standard 7799 Part 1 en is gedeeltelijk aangepast aan de Nederlandse situatie. BS 7799 is ontwikkeld door het Department of Trade and Industry en wordt uitgegeven door het British Standards Institute. Oorspronkelijk bestond BS 7799 uit slechts één document maar bij het beschikbaar komen van Part 2 werd het oorspronkelijke document bekend onder de naam BS 7799 Part 1.

BS 7799 Part 2 is niet verkrijgbaar in een Nederlandse versie. Dat deel beschrijft het certificatieschema - onder de naam c-cure - zoals in Engeland in 1998 ingevoerd is en geeft aan hoe een organisatie kan kiezen - op basis van risico analyse - welke van de in BS 7799 Part 1 genoemde maatregelen relevant zijn. In Nederland bestaat wel een certificatieschema (ontwikkeld door ICIT) maar dit vormt geen expliciet deel van de Code.

Revisie van BS 7799 Part 1.

In 1998 is een project gestart om BS 7799 Part 1 (de gevolgen voor Part 2 worden tevens onderzocht) aan te passen aan de huidige stand van zaken. Een *Draft for Public Comment* is in september 1998 vrijgegeven (kostprijs £ 14,-); de sluitingsdatum voor het opgeven van wijzigingen was gesteld op 30 november 1998. Voorzien is vrijgave van de gereviseerde versie voor de lente van 1999.

Een vergelijking van de Draft met de Code[2].

Hoewel BS 7799 goed bruikbaar is in Nederland, is in veel gevallen de Code te prevaleren. Zolang echter de Code nog niet geënt is op de nieuwe versie van BS 7799, kan het relevant zijn te analyseren welke verschillen (zullen) bestaan tussen deze twee documenten. Hieronder worden de meest belangrijke verschillen besproken.

In de tabellen op de volgende bladzijden refereert de nummering, indien niet anders aangegeven, aan de bestaande paragrafen in de Code. Syntactische veranderingen of wijzigingen in spelling en dergelijke worden niet genoemd. Is in de tabellen alleen een paragraafnummer opgenomen in de kolom 'Paragraaf in Draft' dan betreft het een volledig nieuwe paragraaf.

[1] Bestelnummer LOS 20003:1994

[2] Opgemerkt dient te worden dat op dit moment (december 1998) alleen een draft van de nieuwe versie voorhanden is; kleine verschillen tussen de uiteindelijke versie en de draft zijn dus mogelijk waardoor de vergelijking met de Code anders uit kan komen.

Samenvatting.

Samengevat (uitgewerkt vanaf blz. 4) zijn de volgende belangrijkste wijzigingen aangebracht:

- Twee sleutelmaatregelen zijn komen te vervallen; het totaal aantal maatregelen is nu **121**.
- Beveiliging richting derden, bij uitbesteding en bij telewerken krijgt extra aandacht.
- Het belang van risico management wordt meer expliciet vermeld.
- Het begrip ‘computersysteem’ wordt ruimer geïnterpreteerd.
- De maatregel ‘viruscontrole’ wordt uitgebreid naar alle kwaadaardige software.
- Electronic commerce wordt meegenomen inclusief relevante begrippen als non-repudiation.
- Publiek toegankelijke systemen (zoals websites) worden behandeld.
- Encryptie systemen en sleutelmanagement krijgen meer aandacht.
- Wijzigingsbeheer wordt meer expliciet vermeld.
- De tekst m.b.t. het onderwerp continuïteitsplanning, is vrijwel geheel herschreven.
- De problematiek rond het vergaren van bewijslast wordt toegelicht.

Aanpassingen aan de Code voor Informatiebeveiliging.

Navraag bij het NNI leerde dat men voornemens is, na formalisering (lente 1999) van de revisie van BS 7799 Part 1, een vertaling/aanpassing voor Nederland uit te voeren hetgeen zal resulteren in een Versie 2 van de Code voor Informatiebeveiliging. Dit impliceert aanpassing van het ICIT certificatieschema, alsmede aanpassing van electronische vragenlijsten zoals SecurityPAC van CPA en de Riskette van Coseco. Ook blijft een vraagstuk open welke maatregelen te treffen zijn bij reeds gecertificeerde instanties of voor organisaties die met certificatie trajecten bezig zijn.

Openstaande punten.

Hoewel deze revisie van BS 7799 Part 1 het document aanpast aan de stand van zaken zijn toch nog duidelijke omissies aanwezig. Elke organisatie welke een beveiligingsbeleid wenst te formuleren wordt met dit document in de juiste richting gestuurd maar de desbetreffende paragraaf is nog steeds vrij beknopt. BS 7799 en de Code zijn beide documenten die de lezer vooral aangeven wat er moet gebeuren maar hoe blijft veelal in het duister. Ook wordt het proces van het selecteren van de juiste maatregelen slechts aangestipt en niet meer dan dat.

Gemist wordt vooral de integratie met een product zoals CRAMM of andere kwantitatieve of kwalitatieve risico-analyse methodes. De leesbaarheid van het document laat te wensen over; zo wordt informatieve tekst afgewisseld met te implementeren maatregelen, soms zelfs in dezelfde alinea. Checklists op basis van de Code (een door het NGI opgepakt project) kunnen dit laatste probleem wegnemen.

De inleiding (deel I van de Code)

Paragraaf in Code	Paragraaf in Draft	Wijziging
Deel 1	Introduction	In de inleiding van de Draft wordt op een aantal plaatsen gerefereerd aan een 'management framework' hetgeen duidelijk verwijst naar het nieuwe Part 2. Het 'management framework' wordt beschreven als zijnde het door het management gedragen beleidsdocument waarin richting, doelen en doelstellingen van informatiebeveiliging voor de organisatie beschreven staan, alsmede het proces van risico-analyse, selectie van maatregelen en audits.
Deel 1	Introduction	Meest belangrijke wijziging in de Draft is het vervallen van twee sleutelmaatregelen (welke als essentieel en fundamenteel gezien werden), te weten: **6.3.1 Viruscontrole** **10.2.1 De naleving van het beveiligingsbeleid** Hoogstwaarschijnlijk heeft aan deze wijziging ten grondslag gelegen dat als sleutelmaatregel het belang van het beleidsdocument voor informatiebeveiliging al onderkend wordt en dat naleving in dat geval verondersteld mag worden (benadrukt in 1.1.1). Dat viruscontrole noodzakelijk is wordt ook reeds genoemd in paragraaf 1.1.1. en het apart noemen van deze specifieke maatregel was altijd al enigszins opmerkelijk. Bovendien wordt elders in de Draft terecht opgemerkt dat steeds meer kwaadaardige software ontdekt wordt welke al dan niet onder de noemer 'virus' valt. Teveel nadruk op de maatregel viruscontrole werkt dan averechts.
Deel 1	Introduction	Als extra kritieke succesfactor wordt in de inleiding van de Draft opgemerkt het kunnen evalueren van de kwaliteit van de informatiebeveiliging door het voorhanden zijn van een uitgebreid meetsysteem; uiteraard als input voor verbeteringsprocessen. Ook dit vormt een indirecte verwijzing naar BS 7799 Part 2; deze beschrijft immers het certificatiesysteem.
Deel 1	Introduction	Paragraaf 0. in de Draft geeft definities van de gebruikte termen; in de Code ontbreekt deze lijst.

Hierna worden de categorieën uit Deel II van de Code met de Draft vergeleken.

Categorie 1 : Beveiligingsbeleid

Paragraaf in Code	Paragraaf in Draft	Wijziging
1.1.1		Toegevoegd is dat het beleidsdocument niet alleen aanwezig moet zijn maar dat alle medewerkers er op gewezen moeten worden. De consequenties van het overschrijden van de regels in het beleidsdocument moeten nadrukkelijk beschreven zijn.
1.1.1		De verantwoordelijkheid voor het beleidsdocument moet belegd zijn.
1.1.1		De gronden voor herzien van het beleidsdocument en meten van de effectiviteit worden nu expliciet genoemd.
1.1.1		Terecht wordt opgemerkt dat het beleidsdocument voor de doelgroep leesbaar moet zijn.

Categorie 2 : Beveiligingsorganisatie

Paragraaf in Code	Paragraaf in Draft	Wijziging
2.1		Toegevoegd is de opmerking dat informatiebeveiliging een multidisciplinaire aanpak vereist.
2.1.2		Toegevoegd is dat de commissie ter coördinatie van informatiebeveiliging verantwoordelijk is dat beveiliging en audits bij nieuwe projecten meegenomen worden.
2.1.3		De verantwoordelijkheid voor beveiliging wordt nu neergelegd bij de informatie beveiligingsmanager daar waar in de Code alleen de eigenaar wordt genoemd.
2.2		In de doelstelling voor controle op toegang door derden wordt nu gewezen op het tevens toepasbaar zijn van BS 7799 bij uitbesteding.
2.2.1		Een aantal situaties bij toegang door derde partijen worden geschetst met de gevolgen voor de beveiliging. Veel nadruk wordt gelegd op het vastleggen van verplichtingen in een contract met derde partijen.
2.2.2		Aan de beveiligingsvoorwaarden op te nemen in een contract met een derde partij zijn er een aantal toegevoegd zoals beveiliging van kapitaalgoederen (‘assets’) en het betrekken van onderaannemers (‘subcontractors’). Duidelijk is (zie ook de toevoeging van 2.3) dat het toenemende belang van BS 7799 bij uitbesteding nu onderkend wordt.
	2.3	Een geheel nieuwe paragraaf m.b.t. outsourcing is toegevoegd. Doelstelling is het handhaven van informatiebeveiliging ondanks het uitbesteden van de verantwoordelijkheid voor de verwerking aan een andere organisatie.
	2.3.1	Een zestal punten ter opname in een uitbestedingscontract worden genoemd zoals het vastleggen van de beschikbaarheid bij calamiteiten en de eisen te stellen aan fysieke en logische beveiliging.

Categorie 3 : Classificatie en beheer van bedrijfsmiddelen

Paragraaf in Code	Paragraaf in Draft	Wijziging
3.1.1		Het belang van een overzicht van bedrijfsmiddelen wordt extra benadrukt met betrekking tot risico management. De waarde en belangrijkheid van bedrijfsmiddelen dient bekend te zijn om het vereiste beveiligingsniveau te kunnen bepalen.
3.2.1		Vertrouwelijkheid, integriteit en beschikbaarheid worden niet meer expliciet genoemd als aandachtspunten bij classificeren maar enkele algemene tips worden gegeven.
3.2.2		Bij deze paragraaf wordt nu gewezen op het feit dat een toegewezen label (classificatie) in de tijd kan wijzigen. Gewezen wordt dat te zwaar classificeren hoge kosten met zich meebrengt.

Categorie 4 : Beveiligingseisen ten aanzien van personeel

Paragraaf in Code	Paragraaf in Draft	Wijziging
4.1.2		Screening van sollicitanten wordt ook aangeraden bij uitbesteding en bij tijdelijke werknemers. Tevens wordt het belang onderkend van het regelmatig herhalen van dergelijke onderzoeken. Aangegeven wordt een aantal voorbeelden van wijzigingen in gedrag waar men alert op moet zijn.
4.1.3		Ook voor de geheimhoudingsverklaring wordt aangegeven dat wijzigingen in een arbeidscontract tot herziening kunnen leiden.
	4.1.4	De voorwaarden en condities met betrekking tot informatiebeveiliging op te nemen in een arbeidscontract worden genoemd. Nadrukkelijk wordt gewezen op het belang deze ook te laten gelden buiten kantoortijden en buiten het kantoor in het geval van thuiswerkers.
4.3.1		Het belang van terugkoppeling aan de rapporteur van een beveiligingsincident wordt aangegeven.
	4.3.4[3]	Het proces om te leren van incidenten en het belang daarvan wordt (rudimentair) geschetst.

[3] De bestaande paragraaf 4.3.4 wordt 4.3.5

Categorie 5 : Fysieke beveiliging en beveiliging van de omgeving

Paragraaf in Code	Paragraaf in Draft	Wijziging
5.1		In de doelstelling wordt de term ‘clear desk policy’ uitgebreid met de ‘clear screen policy’.
5.1.1		Een extra aantal richtlijnen voor fysieke beveiliging wordt genoemd zoals de aanwezigheid van een receptie, inbraakalarm en autorisatie van extern personeel. Ook wordt expliciet het omgaan met een bomalarm genoemd.
5.1.2		Een tweetal extra richtlijnen voor het beperken van toegangsrechten wordt gegeven; met name bij wijzigingen in de werkzaamheden van derde partijen.
5.1.3		Een scheiding wordt aangebracht in de richtlijnen die gelden voor de plaats waar de informatieverwerking plaatsvindt en het overige deel van de vestiging. Voor de laatste wordt een aantal extra richtlijnen gegeven zoals het in bewaring geven van sleutels bij politie of bewakingsinstantie en het reinigen van kruipruimtes vanwege het brandgevaar.
5.1.4		Opgenomen is de richtlijn dat inkomende goederen ingevoerd worden in het register van bedrijfsmiddelen.
5.1.5		De clear desk policy wordt uitgebreid met de tem clear screen policy en gewezen wordt op het leegruimen van printers zodra gevoelige informatie afgedrukt is.
5.1.6		Een aantal extra richtlijnen voor het verwijderen van bedrijfseigendommen wordt gegeven zoals het noteren van in- en uitgaande goederen en het uitvoeren van willekeurige controles.
5.2.2		Het belang van een back-up stroomgenerator (no-break) wordt genoemd naast de UPS. Ook wordt het belang van noodschakelaars en noodverlichting benadrukt.
5.2.3		Beveiliging van kabels wordt uitgebreid met aandacht voor het gebruik van optische bekabeling en het uitvoeren van controles (‘sweeps’) op ongeautoriseerde apparatuur gekoppeld aan de bekabeling.
5.2.4		Bij onderhoud van apparatuur wordt gewezen op de risico’s bij het verzenden van apparatuur buiten de vestiging. Gewezen wordt op de controle of in dergelijke gevallen dekking in verzekeringen aanwezig is.

Categorie 5 : Fysieke beveiliging en beveiliging van de omgeving (vervolg)

Paragraaf in Code	Paragraaf in Draft	Wijziging
5.2.5		Beveiliging van apparatuur buiten het bedrijf wordt niet alleen toepasbaar verklaard op IT-apparatuur maar geldt bijvoorbeeld ook voor organizers, mobiele telefoons en papieren. Gewezen wordt op het belang van goede verzekeringen. Voor de beveiliging van mobiele apparatuur wordt verwezen naar een nieuwe paragraaf (7.8.1); in de Code wordt bij 5.2.5 gewezen op de gevaren van draagbare computers; dit punt is hier komen te vervallen.
5.2.6		Bij het veilig afvoeren van apparatuur wordt met nadruk gewezen op het feit dat het mogelijk is normaal gewiste gegevens van schijven te herstellen. Fysieke vernietiging kan dus bij hoge vertrouwelijkheid noodzakelijk zijn.

Categorie 6 : Computer- en netwerkbeheer

Paragraaf in Code	Paragraaf in Draft	Wijziging
		Gewezen wordt op het feit dat informatieverwerking niet alleen computersystemen omvat maar ook netwerken, mobiele systemen, voicemail, multimedia etc. etc.
6.1.1		Met betrekking tot schriftelijke bedieningsprocedures wordt het regelmatig herzien aangegeven en het belang wordt genoemd van procedures aangezien deze beschrijven hoe werknemers zich kunnen houden aan het beveiligingsbeleid.
6.1.2		De ‘denial of service’ aanval is toegevoegd als voorbeeld van een incident.
6.1.3		Voor een kleine organisatie wordt geschetst dat functiescheiding mogelijk wordt door het signaleren van het veranderen van rol indien meerdere functies toch bij één persoon belegd zijn.
6.1.4		Voor de scheiding tussen de operationele- en ontwikkelingsprocessen worden een tweetal extra richtlijnen gegeven rond het besturen van wijzigingen en wachtwoordbeheer.
6.2.2		Gewezen wordt op het belang dat bij systeemacceptatie de zekerheid aanwezig is dat er geen implicaties zijn voor de beveiliging.

Categorie 6 : Computer- en netwerkbeheer (vervolg)

Paragraaf in Code	Paragraaf in Draft	Wijziging
6.3.1		De term ‘viruscontrole’ wordt algemener gemaakt en is gewijzigd in kwaadaardige software (‘malicious software’). De term diskette is vervangen door ‘electronic media’. De richtlijnen zijn gemoderniseerd en beschrijven nu ook email attachments, de gevaren bij het verkrijgen van bestanden uit externe netwerken en het op de hoogte zijn (door vakbladen e.d. te raadplegen) van de verschillen tussen virussen en de zogenaamde ‘hoaxes’ (nep-virussen). Het ongewenst propageren van valse informatie (rond nep-virussen) wordt genoemd.
6.4.1		Het belang van controle dat back-ups hersteld kunnen worden (‘restore’) wordt onderstreept. Tevens is toegevoegd de opmerking dat eigenaars aan dienen te geven wanneer data gearchiveerd en verwijderd moet worden.
6.4.4		Aangegeven wordt dat ook bij kleinere systemen klimaatbeheersing van belang kan zijn.
6.6.2		De procedures voor behandeling van gegevens worden ook toepasbaar verklaard voor bijvoorbeeld mobiele computers en fax machines.
6.6.3		De beveiliging van systeemdocumentatie in openbare netwerken wordt als speciaal aandachtspunt genoemd.
6.6.4		De afvoer van spraakopnamen is toegevoegd.
6.7		De term ‘electronic commerce’ wordt genoemd.
6.7.1		Bij uitwisseling van gegevens worden classificatielabels genoemd als aandachtspunt in overeenkomsten tussen partijen.
6.7.3		De term EDI is vervangen door de meer generieke term ‘electronic commerce’.
6.7.5		De term elektronische kantoorsystemen wordt uitgebreid met mobiele systemen, voice-mail, en fax apparatuur. Ook wordt gewezen op het belang van beleid en richtlijnen voor de gevaren van opnamen van spraakverbindingen, het opslaan van faxen en de distributie van post.
	6.7.6	Ten aanzien van publiekelijk toegankelijke systemen (als voorbeeld wordt een website genoemd) worden richtlijnen gegeven m.b.t. het handhaven van verplichtingen in wetgeving en het schaden van het belang van de organisatie. Het belang van digitale handtekeningen wordt aangegeven en een drietal punten met betrekking tot de verwerking van invoer vanuit publieke netwerken worden gegeven (compleetheid, snelheid, beveiliging tijdens transport en het beveiligen van toegang van het publieke systeem naar daaraan gekoppelde systemen).

Categorie 7 : Toegangsbeveiliging van systemen

Paragraaf in Code	Paragraaf in Draft	Wijziging
7.1.1		Voor het beleid ten aanzien van toegangscontrole wordt een groter aantal richtlijnen gegeven; zo wordt het 'need to know' principe vermeld en wordt het documenteren van het beleid rond 'vertrouwen' en de propagatie daarvan in netwerken toegelicht. Tevens wordt een vijftal aandachtspunten m.b.t. toegangsregels genoemd zoals het verschil tussen verplichte en optionele rechten en het verschil tussen automatisch gegenereerde rechten en die aangebracht door administrators.
7.2.1		Sanctiebeleid voor ongeautoriseerde toegang door werknemers en derde partijen wordt als nieuw aandachtspunt genoemd.
7.2.2		Het toewijzen van privileges voor speciale doeleinden dient te geschieden op andere user ID's dan met welke de normale activiteiten plaatsvinden.
7.2.3		Gewezen wordt op beschikbare technologie voor encryptie van wachtwoorden en voor biometrie zoals vingerafdruk detectie.
7.4.8		Met betrekking tot het beheer van netwerk-routing wordt opgemerkt dat men kennis dient te hebben van de sterkte van de gebruikte mechanismes.
7.5		Toegevoegd is de richtlijn dat gelukte en mislukte aanlog pogingen opgeslagen dienen te worden. Tevens wordt het challenge-response mechanisme genoemd.
7.5.3		Voor gebruikersidentificatie worden een aantal mogelijke mechanismes opgesomd zoals biometrie, tokens en smart-cards.
7.6		Met betrekking tot toegangsbeveiliging voor toepassingen wordt opgemerkt dat deze toegang alleen dient te bestaan voor de eigenaar, andere geautoriseerde personen of gedefinieerde groepen gebruikers.
7.6.2		Opgemerkt wordt het belang van het verwijderen van onnodige software gereedschappen en systeemsoftware.
7.7.1		Voor het vastleggen van bijzondere gebeurtenissen ('events') worden voorbeelden gegeven van de gegevens welke vastgelegd moeten worden (user ID's, datum, tijd etc.).
7.7.2		Ook voor de bewaking van systeemgebruik worden voorbeelden zoals in 7.7.1 gegeven.

Categorie 7 : Toegangsbeveiliging van systemen (vervolg)

Paragraaf in Code	Paragraaf in Draft	Wijziging
	7.8	Een geheel nieuwe paragraaf wordt gewijd aan mobiele computers en telewerkers. De risico's van dergelijke apparatuur door het gebruik in openbare ruimtes en met betrekking tot ontvreemding worden geschetst. Gewezen wordt op de noodzaak tot het creëren van bewustzijn van deze risico's bij de gebruikers van dit soort apparatuur. Tevens wordt de koppeling tussen de externe systemen en de kantoorsystemen besproken. Als beleid dient neergelegd te worden de regels met betrekking tot zenden/ontvangen van gegevens en het maken van back-ups.

Categorie 8 : Ontwikkeling en onderhoud van systemen

Paragraaf in Code	Paragraaf in Draft	Wijziging
8.1		Onderstreept wordt dat het ontwerp en implementatie van een bedrijfsproces ondersteund door applicaties en diensten qua beveiliging minstens zo belangrijk is dan die van losse componenten.
8.1.1		Het belang van garanties omtrent de integriteit van software wordt onderstreept, alsmede het feit dat nieuwe systemen de bestaande beveiliging niet mogen beïnvloeden.
8.2.2		Met betrekking tot de controle op interne verwerking wordt een aantal extra voorbeelden genoemd zoals controleren op de volgorde van uitvoering en uitvoering op de juiste tijd.
	8.2.3[4]	Het valideren van de uitvoer van systemen wordt beschreven en een vijftal richtlijnen worden gegeven zoals controles of gegevens plausibel, accuraat en compleet zijn.
8.2.4		De paragraaf rond gegevens-encryptie is uitgebreid met enige informatie rond de gangbare 'geheime sleutel' en 'publieke sleutel' technieken. Enkele voor- en nadelen worden opgesomd.
	8.2.5	Een extra paragraaf omtrent digitale handtekeningen is toegevoegd. Toegelicht wordt de werking en de rol van een gecertificeerde autoriteit ('CA').

[4] De bestaande paragraaf 8.2.3 wordt 8.2.4

Categorie 8 : Ontwikkeling en onderhoud van systemen (vervolg)

Paragraaf in Code	Paragraaf in Draft	Wijziging
	8.2.7	Een extra paragraaf is toegevoegd met betrekking tot het niet kunnen betwisten van een transactie ('non-repudiation'). De werking wordt toegelicht en een aantal voorbeelden van mogelijke diensten die gebruik kunnen maken van deze techniek (zoals het niet kunnen betwisten van de levering van goederen) wordt genoemd.
	8.2.8	Een extra paragraaf rond sleutelbeheer is toegevoegd. De componenten welke een rol spelen in een sleutelbeheerssysteem worden opgesomd en de risico's worden geschetst alsmede de maatregelen die getroffen kunnen worden zoals cryptografie, hiërarchie en fysieke beveiliging. Ook de rol van de certificerende autoriteit wordt toegelicht.
8.4.1		Wijzigingsbeheer wordt ook van toepassing verklaard voor instructies en gebruikersprocedures en opgemerkt wordt dat wijzigingen de bedrijfsprocessen niet mogen verstoren. Het belang van een separate testomgeving wordt aangegeven.
8.4.2		Wijzigingen in het besturingssysteem zullen ook tot wijzigingen in het continuïteitsplan kunnen en/of moeten leiden.
	8.4.4	Een extra paragraaf is toegevoegd met betrekking tot de zogenaamde Trojan code en heimelijke toegang ('covert channels'). Een zestal tips wordt gegeven welke het risico verkleinen zoals het aanschaffen van software bij een gereputeerde bron en het regelen van toegang tot broncode.

Categorie 9 : Continuïteitsplanning

Paragraaf in Code	Paragraaf in Draft	Wijziging
9.1		Het proces van continuïteitsplanning wordt gedetailleerder geschetst. Zo is nu aangegeven dat het onderkennen van de risico's de eerste stap is en dat continuïteitsplanning niet alleen herstel omvat maar ook minimalisering van de gevolgen.
9.1.1		Het belang van risico-analyses wordt onderstreept. Het rangschikken van processen naar prioriteit en de dan noodzakelijke maatregelen m.b.t. de continuïteit wordt meer expliciet genoemd.
9.1.1		Onderkend wordt het belang van inbedding van continuïteitsplanning in de bedrijfsprocessen. De verantwoordelijkheid dient op het juiste niveau belegd te zijn.

Categorie 9 : Continuïteitsplanning (vervolg)

Paragraaf in Code	Paragraaf in Draft	Wijziging
		Paragraaf 9.1.2 t/m 9.1.4 uit de Code zijn grotendeels vervangen door een viertal nieuwe paragrafen. De 'oude' informatie is gehergroepeerd en sterk uitgebreid.
	9.1.2	'Business Continuity and impact analysis'. De BIA (Business Impact Analysis) wordt beschreven. Het belang van onderkennen van de juiste risico's vergt deelname van alle betrokken partijen. Aangegeven wordt dat bedrijfscontinuïteit breder is dan continuïteit van IT voorzieningen.
	9.1.3	'Writing and implementing the continuity plan'. Het bepalen van de juiste tijdschalen wordt onderkend. Een vijftal stappen in het proces wordt genoemd, te weten het vaststellen van verantwoordelijkheden, selectie en implementatie van de juiste maatregelen, het ontwikkelen van documentatie, het opleiden van de betrokken partijen en het testen en bijwerken van het plan. Doelstelling is het herstel van de dienstverlening binnen een acceptabele tijd waarvoor alle daarvoor benodigde componenten noodzakelijk zijn.
	9.1.4	'Business continuity planning framework'. Continuïteitsplannen moeten voldoen aan een standaard opbouw. Een zevental onderdelen van een continuïteitsplan worden beschreven, zoals activeringscondities, noodprocedures, onderhoud van het plan en het creëren van bewustzijn. Het belang van het toewijzen van beheerders van de componenten wordt onderschreven.
	9.1.5	'Testing, maintaining and re-assessing business continuity plans'. Het systematisch testen van een continuïteitsplan wordt beschreven. Een zestal mogelijkheden wordt geschetst zoals simulaties en volledige oefeningen. De koppeling met wijzigingsbeheer wordt besproken vanwege de snelheid van verouderen van continuïteitsplannen. De voorbeelden welke worden genoemd welke leiden tot wijzigingen zijn vrijwel gelijk als in 9.1.4 van de Code.

Categorie 10 : Toezicht

Paragraaf in Code	Paragraaf in Draft	Wijziging
10.1.1		Een extra vijftal regels tegen onrechtmatig kopiëren van programmatuur wordt gegeven zoals het kunnen bewijzen van eigenaarschap van licenties, handboeken e.d. en het tijdig reageren op tekortkomingen.
10.1.2		Het voldoen aan de wettelijke verplichtingen ten aanzien van bewaartermijnen wordt meer expliciet omschreven. Ook wordt aangegeven het belang van juist sleutelbeheer zodat archieven vrijgegeven kunnen worden inclusief (electronische) sleutels.
	10.1.5	Een extra paragraaf met betrekking tot vergaring van bewijslast is toegevoegd. Het belang wordt aangegeven alsmede de aandachtspunten zoals het juist vastleggen hoe bewijs tot stand is gekomen. Onderscheid wordt gemaakt tussen papieren en electronische gegevens. De rol van advocaten en politie wordt aangegeven.
10.2.1		Het naleven van het beveiligingsbeleid richt zich niet alleen op informatiesystemen. Ook worden genoemd de eigenaren van de gegevens en andere bronnen, de gebruikers en het management. De verantwoordelijkheid wordt bij de lijnmanagers belegd.

Websites van in het artikel genoemde organisaties:	
British Standards Institute	http://www.bsi.org.uk/
Certificatie volgens BS 7999	http://www.c-cure.org/
Nederlands Normalisatie Instituut	http://www.nni.nl/

Ernst J. Oud is senior consultant bij Getronics Business Continuity BV[5]. Op basis van de Code voor Informatiebeveiliging implementeert hij bij organisaties een integraal informatie-beveiligingsplan gebruikmakend van de in de praktijk beproefde projectmethode Integrated Security Methodology (ISM). Dhr. Oud is te bereiken via : ernstoud@euronet.nl

Datum:	29 december 1998
Versie:	1.0
Bestandsnaam:	[c:\data\word\Revisie van BS 7799 Part 1.doc]

[5] Voorheen bekend onder de naam CUC - Computer Uitwijk Centrum BV