De Nederlandsche Bank

Directie

Westeinde 1
Postbus 98
1000 AB Amsterdam

Bestuur Nederlands
Instituut van Registeraccountants
Postbus 7984
1000 AD AMSTERDAM

Datum
20 september 1988

Betreft: Memorandum omtrent de betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking in het bankwezen

Mijne heren,

Hierbij doen wij u toekomen onze per heden gedateerde circulaire aan het bankwezen met het bijbehorende Memorandum inzake het in hoofde vermelde onderwerp.

Hoogachtend,

DE NEDERLANDSCHE BANK NV

Directeur

Bijlage: 1

De Nederlandsche Bank NV
Handelsregister Amsterdam 3396

4400

De Nederlandsche Bank

Westeinde 1
Postbus 98
1000 AB Amsterdam

Directie

Aan de instellingen ingeschreven in het Register als bedoeld in artikel 12, eerste lid van de Wet Toezicht kredietwezen

Datum
20 september 1988

Betreft: Memorandum omtrent de betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking in het bankwezen

Mijne heren,

Het snel toenemende belang van de geautomatiseerde gegevensverwerking leidt binnen het bankwezen tot een grotere afhankelijkheid en kwetsbaarheid. Naar het zich laat aanzien zal mede als gevolg van een verdergaande integratie van automatiseringsprocessen, waarbij - bijvoorbeeld - derden middels datacommunicatie rechtstreeks (betalings)transacties aanbieden de kwetsbaarheid verder kunnen toenemen.
De Bank heeft zich, gezien de geschetste ontwikkelingen, begin 1986 nader georiënteerd inzake de inspanningen van de banken op dit terrein. Zij heeft zich in haar oriëntatie, met inachtneming van de eigen verantwoordelijkheden van de onder toezicht staande instellingen, met name gericht op het waarborgen van de betrouwbaarheid en de continuïteit van de geautomatiseerde gegevensverwerking.
Daarbij bleek dat de onder toezicht staande instellingen in het algemeen reeds essentiële organisatorische maatregelen hadden getroffen. De opzet en uitwerking daarvan toonde echter verschillen in detaillering en tempo.
Voorts is daarbij vastgesteld dat algemeen aanvaarde normen ten aanzien van de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking zowel nationaal als internationaal nog in ontwikkeling zijn.
De betrokkenheid van de Bank bij deze problematiek is gebaseerd op het belang dat zij hecht aan een ongestoord en betrouwbaar verloop van de geautomatiseerde gegevensverwerking. Uitgangspunt daarbij is dat gebeurtenissen die de liquiditeits- en/of solvabiliteitspositie van een instelling wezenlijk kunnen aantasten voorkomen moeten worden. Mede om die reden heeft de Bank het nodig geoordeeld door het uitbrengen van een memorandum bij te dragen aan meer uniforme uitgangspunten voor een toereikend risicobeheer op het gebied van de geautomatiseerde gegevensverwerking.

De Nederlandsche Bank NV
Handelsregister Amsterdam 3396

4400

– Omtrent de inhoud van dit memorandum is, mede gezien de complexheid van de materie, uitvoerig overleg gepleegd met representatieve organisaties van het bankwezen, het Nederlands Instituut van Registeraccountants en met door deze organisaties aangewezen deskundigen.

In het memorandum wordt bevestigd dat de primaire verantwoordelijkheid voor maatregelen van beveiliging en interne controle gericht op de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking ligt bij het management van de instelling. Het memorandum omvat daartoe een aantal uitgangspunten.

De Bank wenst in haar positie als toezichthoudster periodiek meer expliciet geïnformeerd te worden over de wijze waarop aan de zorg voor betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking inhoud wordt gegeven. Daarbij ziet zij een taak weggelegd voor de bij de instelling fungerende externe accountant, die de opzet en het daadwerkelijk bestaan van het voor de automatiseringsorganisatie geldende stelsel van maatregelen en procedures voor zover gericht op de aspecten betrouwbaarheid en continuïteit beoordeelt.
In de jaarlijks uit te brengen management letter dient verslag te worden gedaan van diens bevindingen.
Een en ander brengt met zich mede dat in de controle-opdracht aan de externe accountant een daarop afgestemde passage dient te worden opgenomen, ingevolge welke de externe accountant zich als aanvulling op de werkzaamheden van de interne accountant een oordeel dient te vormen over eerdergenoemde continuïteits- en betrouwbaarheidsaspecten. Indien en voor zover er geen interne accountantsdienst werkzaam is of deze accountantsdienst de vereiste deskundigheid daartoe ontbeert zal verdergaande eigen actie van de externe accountant nodig kunnen zijn.

De modaliteiten van dit memorandum zijn op de instelling van toepassing met ingang van het boekjaar dat eindigt op of na 31 december 1988.

Wij verzoeken u deze brief alsmede het memorandum aan uw Raad van Commissarissen en uw externe accountant ter kennis te brengen.

De Bank is voornemens het memorandum te publiceren in haar kwartaalbericht van december 1988.

Hoogachtend,

DE NEDERLANDSCHE BANK NV

Directeur

MEMORANDUM OMTRENT DE BETROUWBAARHEID EN CONTINUITEIT VAN GEAUTOMATISEERDE GEGEVENSVERWERKING IN HET BANKWEZEN

1 INLEIDING

De voortschrijdende integratie van de automatisering in de bedrijfsprocessen en de toenemende complexiteit en verwevenheid van geautomatiseerde systemen leiden binnen het bankwezen tot een grotere afhankelijkheid en kwetsbaarheid. De risico's, die hiermede samenhangen, kunnen zeer aanzienlijk zijn. In dit verband wordt gedoeld op de risico's, die de betrouwbaarheid en continuïteit van de gegevensverwerking en daarmede de continuïteit van de instelling zelve bedreigen. In het navolgende worden onder het begrip betrouwbaarheid tevens die maatregelen begrepen, die frauduleus gebruik van de geautomatiseerde (betalingsverkeer)systemen en het zich onrechtmatig toeëigenen van vertrouwelijke informatie tegengaan. Onder het begrip continuïteit wordt in dit kader de ongestoorde voortgang van de gegevensverwerking verstaan. Inbreuken op de betrouwbaarheid en continuïteit zullen ernstige repercussies kunnen hebben voor de liquiditeits- en/of solvabiliteitspositie van de instelling(en) en het vertrouwen in de betrokken instelling(en) kunnen schaden. Voorts kan ook de ongestoorde verwerking van het betalingsverkeer in het geding zijn. Naar het zich laat aanzien zal mede als gevolg van een verdergaande integratie van automatiseringsprocessen, waarbij derden middels datacommunicatie rechtstreeks (betalings)transacties aanbieden de kwetsbaarheid sterk kunnen toenemen.
Om deze redenen wenst de Bank in haar rol van toezichthoudster te bevorderen, dat binnen het bankwezen door de onder toezicht staande instellingen gerede aandacht wordt gegeven aan maatregelen tot beveiliging en interne controle gericht op de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking. Daarbij ziet de Bank zich geconfronteerd met het probleem, dat nationaal en internationaal nog geen algemeen aanvaard normenstelsel ter zake van deze beveiliging en interne controle bestaat. Dit in aanmerking nemend wordt in het onderhavige memorandum uiteengezet op welke wijze de Bank hieraan nadere uitwerking wil geven.

2 UITGANGSPUNTEN VOOR DE BANK ALS TOEZICHTHOUDSTER

De betrokkenheid van de Bank is gebaseerd op het belang, dat zij hecht aan een ongestoord, betrouwbaar verloop van de geautomatiseerde gegevensverwerking. Het algemene uitgangspunt daarbij is, dat door de instelling gerede aandacht wordt besteed aan de risico's, die de liquiditeit en/of solvabiliteit van de betrokken instelling wezenlijk kunnen aantasten.
De primaire verantwoordelijkheid in deze berust bij het management van de instelling. Het management zal mitsdien een beleid moeten formuleren en (doen) uitwerken, dat aan deze als randvoorwaarden aan te merken desiderata van de Bank tegemoet komt.

Ook de Raad van Commissarissen dient het beleid ter zake en de regelmatige bijstelling daarvan in haar verantwoordelijkheid te betrekken, hierbij gebruikmakend van de bevindingen van de, mede te hunnen behoeve fungerende, externe accountant. De Bank wenst periodiek geïnformeerd te worden over de vraag of hieraan naar behoren inhoud wordt gegeven. Een dergelijke toetsing kan naar de mening van de Bank het meest doelmatig worden uitgevoerd door de bij de instelling fungerende externe accountant.
Van diens bevindingen wenst de Bank alsdan kennis te nemen (voor de concrete uitwerking wordt verwezen naar het gestelde in paragraaf 5).

3 BELEIDSVERANTWOORDELIJKHEID VOOR BETROUWBAARHEID EN CONTINUITEIT VAN DE GEAUTOMATISEERDE GEGEVENSVERWERKING

De stelling, dat de beleidsverantwoordelijkheid voor de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking berust bij het management van de instelling is niet omstreden.
Een toereikend beleid hiertoe inzake beveiliging en interne controle is van een dusdanig gewicht, dat een systematische benadering geboden is.
Op basis van een periodiek bij te stellen risico-afweging zal het management een beleid moeten uitstippelen, dat erop is gericht de risico's uit dien hoofde zover mogelijk terug te dringen.
De Bank is zich er wel van bewust, dat eventualiteiten, die tot een doorbreking van het stelsel van de te implementeren maatregelen en procedures leiden, nimmer ten volle zijn uit te sluiten. In haar optiek moet het bestaande stelsel van maatregelen en procedures voldoen aan redelijkerwijs te stellen eisen.
In eerste aanleg zal door de instelling moeten worden tegengegaan, dat de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking in het geding komen.
Hiertoe zijn maatregelen vereist, gericht op preventie, tijdige detectie, correctie en schadebeperking.
Gegeven haar eindverantwoordelijkheid zal het management à tempo middels een terugrapportage op de hoogte gesteld dienen te worden omtrent de voortgang van de te implementeren maatregelen en de naleving van de bestaande voorschriften.
Regelmatig moet worden bezien of gewijzigde omstandigheden aanleiding geven het beleid ter zake bij te stellen.

4 AANDACHTSPUNTEN VOOR BETROUWBAARHEID EN CONTINUITEIT VAN DE GEAUTOMATISEERDE GEGEVENSVERWERKING

Gesteld kan worden, dat de bancaire activiteiten, de automatiseringsgraad en de feitelijke automatiseringsopzet van de onder toezicht staande instellingen zeer uiteenlopend zijn. Tevens kan worden geconstateerd, dat de technologische ontwikkelingen zowel ten aanzien van de systemen, van de methoden van inbreken daarin, als ten aanzien van het beveiligingsinstrumentarium bijzonder snel gaan.

Concrete algemeen aanvaarde normen ten aanzien van de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking zijn zowel nationaal als internationaal in ontwikkeling.
In Nederland heeft dit binnen het NIVRA geleid tot een opdracht aan de werkgroep EDP van de Commissie Automatiseringsvraagstukken om uitgangspunten voor de beveiliging en controle van geautomatiseerde gegevensverwerking te ontwikkelen.
Daarop vooruitlopend wil de Bank voorshands volstaan met het aangeven van de onderstaande minimale uitgangspunten:
- de primaire verantwoordelijkheid voor de betrouwbaarheid en de continuïteit van de geautomatiseerde gegevensverwerking berust bij het management van de instelling. Deze verantwoordelijkheid houdt in, dat het beleid dienaangaand expliciet moet zijn geformuleerd en gebaseerd moet zijn op een regelmatig bij te stellen risico-inventarisatie
- bij de afweging van concrete maatregelen gericht op de betrouwbaarheid en continuïteit dient, gegeven de technische mogelijkheden, voorrang te worden gegeven aan het beperken van risico's, die direct of indirect door een gestagneerde dienstverlening de solvabiliteits- en/of de liquiditeitspositie van de instelling in gevaar kunnen brengen
- de uitwerking van het instellingsbeleid dient maatregelen te bevatten voor de wijze waarop uitvoering aan het beleid wordt gegeven, in technische, organisatorische en personele zin
- in aanmerking nemend de omvang van de instelling en de aard van de automatiseringsorganisatie dient te zijn voorzien in een adequaat opgezette interne controle.
In de aan dit memorandum toegevoegde bijlage is meer diepgaand aangegeven op welke wijze inhoud gegeven kan worden aan het proces van risicobeheersing.

5 DE ROL VAN DE EXTERNE ACCOUNTANT

De Bank is van mening, dat in de opdracht die de onder toezicht staande instelling verstrekt aan de externe accountant begrepen moet zijn, dat deze zich periodiek een oordeel vormt omtrent de betrouwbaarheid en continuïteit van voor de bedrijfsprocessen essentiële geautomatiseerde gegevensverwerking.
In de opvatting van de Bank betreft dit geautomatiseerde gegevensverwerking waarvan het niet of niet voldoende beveiligd functioneren een wezenlijke aantasting kan opleveren van de liquiditeits- en/of solvabiliteitspositie van de instelling.
De externe accountant zal zich daartoe een oordeel moeten vormen over de opzet en het daadwerkelijk bestaan (ten tijde van de waarneming) van het voor de automatiseringsorganisatie geldende stelsel van maatregelen en procedures, voor zover dat is gericht op de aspecten betrouwbaarheid en continuïteit, zoals omschreven in paragraaf 1 van dit memorandum.
Omtrent diens bevindingen maakt de externe accountant melding in de jaarlijks uit te brengen management letter, waarbij nader wordt ingegaan op eventuele gesignaleerde tekortkomingen en onvolkomenheden.

- Door het management van de instelling zal in reactie daarop moeten worden aangegeven langs welke weg hierin voorzien gaat worden.
  Een en ander dient te worden geconcretiseerd door een afzonderlijk op te nemen passage in de door de instelling aan de externe accountant verstrekte opdracht. De hiervoor te kiezen bewoordingen kunnen als volgt luiden:
  'De externe accountant vormt zich in het kader van de controle op de jaarrekening, als aanvulling op de werkzaamheden van de interne accountant, mede een oordeel over de continuïteits- en betrouwbaarheidsaspecten van de geautomatiseerde gegevensverwerking, voor zover van wezenlijk belang voor de instelling'.
  Deze werkzaamheden kunnen worden uitgevoerd met een andere periodiciteit dan de werkzaamheden in het kader van de jaarrekeningcontrole.

AANDACHTSPUNTEN VOOR EEN TOEREIKENDE BETROUWBAARHEID EN CONTINUITEIT VAN DE GEAUTOMATISEERDE GEGEVENSVERWERKING

1 ALGEMEEN

Het belang, dat gehecht moet worden aan een adequate beheersing en beveiliging van de infrastructuur ten aanzien van geautomatiseerde gegevensverwerking bij de onder toezicht staande instellingen, laat zich voorshands niet kwantificeren. Daarvoor is de verscheidenheid naar aard, omvang en automatiseringsgraad van de instellingen te groot. Zelfs bij instellingen, die gemeten naar deze criteria als gelijkwaardig aan te merken zijn, zullen op grond van de feitelijk gekozen automatiseringsstructuur essentiële verschillen bestaan.
De Bank is van mening, dat de beleidsverantwoordelijkheid voor de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking een zaak is, die primair het management van de instelling regardeert.
Daarom volstaat zij met het beschrijven van aandachtspunten. Achtereenvolgens komen het beleid, de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking aan de orde. Onder punt 5 is voorts een richtinggevend overzicht van aandachtspunten ter zake opgenomen.

2 BELEID MET BETREKKING TOT BEVEILIGING EN INTERNE CONTROLE

Binnen de instelling zal de leiding zich geregeld terdege en expliciet rekenschap moeten geven van de risico's, die aan de geautomatiseerde gegevensverwerking zijn verbonden. Bij de uit dien hoofde voorgestane interne controle- en beveiligingsmaatregelen zal een afweging van nut en kosten worden gemaakt. Bij de afweging van concrete maatregelen, gericht op continuïteit en betrouwbaarheid dient voorrang te worden gegeven aan het beperken van risico's, die direct of indirect door een gestagneerde dienstverlening, de solvabiliteits- en/of liquiditeitsposities in gevaar kunnen brengen.
In dit beleid zullen de hoofddoelstellingen tot uitdrukking moeten komen:
- bescherming van de geautomatiseerde gegevensverwerking tegen voorvallen die de continuïteit van dit proces kunnen verstoren
- bescherming van gegevensbestanden en computerprogramma's tegen al dan niet opzettelijke verminking en onbevoegd gebruik, zowel intern als extern
- beperking van de schade in geval discontinuïteit, verminking of onbevoegd gebruik zich voordoet.

Een risico-afweging, waarin de bedreigingen voor een betrouwbare en in continuïteit functionerende gegevensverwerking zijn uitgewerkt, kan dienen als startpunt voor het op te stellen beveiligingsbeleid en de eisen van interne controle.

De leiding zal het aldus geformuleerde beleid moeten uitdragen over alle geledingen binnen de instelling, vanuit een algehele prioriteitsafweging de benodigde budgetten (qua personele inzet en financiële middelen) beschikbaar moeten stellen en toezien op een tijdige implementatie van de in dit kader uit te voeren maatregelen.

Met de nodige regelmaat zal aan de leiding terug gerapporteerd moeten worden hoe de feitelijke stand van zaken met betrekking tot de beveiliging en de interne controle is en of de toepasselijke voorschriften worden nageleefd. Eveneens regelmatig moet beoordeeld worden of het beleid op grond van gewijzigde omstandigheden bijstelling behoeft.

3 BETROUWBAARHEID VAN DE GEAUTOMATISEERDE GEGEVENSVERWERKING

Met de vorming van een goed gestructureerde gebruikers- en automatiseringsorganisatie wordt de grondslag gelegd voor geautomatiseerde systemen die een volledige, juiste, tijdige en geoorloofde verwerking van gegevens waarborgen.
Er moet naar worden gestreefd functiescheidingen aan te brengen tussen systeemontwikkeling en -onderhoud, verwerking en gebruik.
Bij het ontwikkelen van geautomatiseerde (deel)systemen is het gebruik van standaardmethoden en technieken sterk aan te bevelen. Ook het opzetten van de documentatie volgens een vaste systematiek heeft de voorkeur.
Het testen, accepteren en overdragen van aldus ontwikkelde systemen dient volgens een vaste procedure te geschieden. Teneinde te voorkomen dat systeemontwikkeling bij haar testwerkzaamheden toegang heeft tot onderdelen van operationele systemen is een adequate scheiding vereist tussen de produktie-omgeving en de testomgeving. Hetzelfde geldt voor het reguliere onderhoud van de reeds operationeel zijnde systemen.

In dit kader moet worden bedacht, dat beheersing en controle van geautomatiseerde systemen eerst daadwerkelijk effect krijgen door de mensen die met deze systemen werken dan wel daarvan gebruik maken. Derhalve zal bij de vormgeving van de organisatie aandacht moeten worden gegeven aan een kwalitatief en kwantitatief goede personeelsbezetting.

Bij majeure wijzigingen en onderhoud van operationele systemen kan het aanbeveling verdienen het totale ontwikkelingstraject opnieuw te doorlopen om volledig recht te kunnen doen aan alle voornoemde aspecten.
In de operationele sfeer zullen gegevensverwerkende systemen toereikende vastleggingen moeten opleveren, die de mogelijkheid bieden om de goede werking en uitkomsten van het systeem te controleren (bijvoorbeeld met behulp van 'logging-faciliteiten').

Bij eerdere gelegenheden heeft de Bank bij het begrip betrouwbaarheid het accent gelegd op het frauderisico. Dat zulks gebeurt, is niet zonder reden; de gegevensstromen binnen het bankwezen hebben immers frequent het karakter van geldstromen.
Misbruik van deze gevoelige gegevensstromen impliceert een directe (financiële) schade voor de instelling. In geval een succesvolle fraude in de publiciteit komt, zal deze afbreuk doen aan het vertrouwen in de betrokken instelling in het bijzonder en in het bankwezen in het algemeen. Met name bij sterk geautomatiseerde betalingsverkeersystemen is verhoogde aandacht voor strikte naleving van de procedures in het invoertraject noodzakelijk.

Thans dienen zich nieuwe vormen van betalingsverkeer aan waarbij, via elektronische weg, betalingen geïnitieerd kunnen worden door derden. Het behoeft geen betoog, dat door de deelnemende instellingen grote zorg besteed moet zijn aan de authenticatie van de opdrachtgever. Bovendien zullen de instellingen geëigende maatregelen dienen te treffen teneinde te verhinderen, dat derden onbevoegd kunnen binnendringen in de communicatienetwerken, die hiertoe gebruikt worden (bijvoorbeeld met behulp van encryptie).

4 CONTINUITEIT VAN DE GEAUTOMATISEERDE GEGEVENSVERWERKING

Naar mate de geautomatiseerde processen van gegevensverwerking meer en meer ineengrijpen en menselijke tussenkomst steeds zeldzamer wordt, is het ongestoord functioneren afhankelijk van de beschikbaarheid van computerapparatuur, programmatuur, actuele bestanden en documentatie, alsmede van een verantwoord omgaan met de geautomatiseerde systemen. De gevaren, die het ongestoord functioneren en daarmee de continuïteit in de gegevensverwerking bedreigen, zullen geïnventariseerd moeten worden. Zo mogelijk zullen de maatregelen een preventief karakter moeten dragen.

Ingeval apparatuur, programmatuur, bestanden en/of documentatie verloren gaan of in het ongerede raken, zal de instelling binnen de daarvoor in het beleid vastgelegde tijd de kritisch geachte gegevensverwerkende processen en bestanden moeten kunnen herstellen.
Daarvoor zijn back-up- en recovery-procedures, alsmede noodvoorzieningen noodzakelijk.
Voorgaande procedures en maatregelen dienen te zijn vastgelegd in een noodvoorzieningenplan. Met enige regelmaat moet het noodvoorzieningenplan getoetst worden (bijvoorbeeld sloepenrol).
Het noodvoorzieningenplan zal bij wijzigende omstandigheden aanpassing behoeven.

5 RICHTINGGEVEND OVERZICHT VAN AANDACHTSPUNTEN VOOR BEVEILIGING EN INTERNE CONTROLE

A) Beleid met betrekking tot beveiliging en eisen van interne controle

1. Definiëring, concretisering en beheersing van het beleid met betrekking tot beveiliging en interne controle, onder eindverantwoordelijkheid van het hoogste management.

2. Aanpassen van dat beleid aan veranderde omstandigheden.

3. De inhoud van het beleid dient mede gericht te zijn op:
- minimalisering van de risico's door preventieve maatregelen
- het tijdig ontdekken van onregelmatigheden
- het beperken van schade; en
- het tijdig terugbrengen in de oorspronkelijke situatie.

4. Het dient duidelijk te zijn welke functionaris(sen) in de organisatie is (zijn) belast met de beleidsvoorbereiding, coördinatie en het toezicht op de uitvoering van het beveiligingsbeleid en de interne controle.

5. In de organisatie dient met voldoende frequentie te worden gerapporteerd over de opzet en werking van het geconcretiseerde beveiligingsbeleid en de interne controle.

B) Betrouwbaarheid van de geautomatiseerde gegevensverwerking

1. Ontwikkeling van informatiesystemen

1.1 Structurering van communicatie en stellen van verantwoordelijkheden tussen de betrokken gebruikers, automatiseringsdeskundigen en controle- en beveiligingsdeskundigen (bijvoorbeeld projectorganisatie).

1.2 Ontwikkeling met behulp van gestandaardiseerde ontwikkelings- en programmeringsmethoden.

1.3 Risico-afweging als onderdeel van het ontwikkelingstraject die leidt tot het vaststellen van beheersbare risico's en past binnen het door het management gedefinieerde beleid.

1.4 Het ontwikkelen van goed op elkaar afgestemde voorschriften en procedures voor de verwerkingsomgeving en gebruikersomgeving tijdens de systeemontwikkeling.

1.5 Gestandaardiseerde test, acceptatie en overdrachtprocedure voor in eigen beheer en door derden ontwikkelde systemen (duidelijke fiatteringsprocedures).

1.6 Autorisatie van wijzigingen in het kader van het onderhoud.

1.7 Voor majeure wijzigingen in bestaande systemen moet een soortgelijke procedure gevolgd worden als voor nieuw te ontwikkelen systemen.

2. Gegevensverwerking

2.1 Aandacht voor risico's bij operationele systemen, bijvoorbeeld als gevolg van veranderde omstandigheden.

2.2 Scheiding tussen de produktie- en testomgeving.

2.3 Functiescheiding tussen systeemontwikkeling en -onderhoud, verwerkingsorganisatie en gebruikersorganisatie.

2.4 Beschikbaarheid van alle organisatorische, technische en programmadocumentatie die nodig is om het systeem operationeel te houden en te onderhouden, ontwikkeld volgens een gestandaardiseerde methode.

2.5 Geautomatiseerde systemen dienen zodanig te zijn opgezet, dat de juistheid, volledigheid, tijdigheid en geoorloofdheid van de ingevoerde en uitgevoerde gegevens en de verwerking kan worden vastgesteld.

2.6 Organisatorische, technische en/of programmatische bescherming tegen bewuste of onbewuste ongeautoriseerde toegang tot programmatuur en bestanden.

2.7 Een passend beheer van gegevensbestanden en programmabibliotheken, aan de hand van nauw omschreven procedures ter waarborging van het gebruik van geautoriseerde versies.

2.8 Standaards voor de bevoegdheidsregeling en identificatie bij gegevens- en programmagebruik.

2.9 Beveiligingen van gevoelige informatie tijdens transport tegen ongeautoriseerd raadplegen of veranderen.
(Datatransmissie met behulp van communicatienetwerken, tape-transport, transport van PC-gegevensdragers enz.)

C) Continuïteit van de geautomatiseerde gegevensverwerking

1. Door het management dient een risico-afweging met betrekking tot continuïteit van de gegevensverwerking plaats te vinden. Als risico's kunnen onder andere worden onderkend:
- technische risico's en calamiteiten, waaronder: brand, technische storingen, onderbreking energievoorziening, stormschade, blikseminslag

- criminaliteitsrisico's, waaronder: geweld, vandalisme, sabotage, terrorisme, diefstal van gegevens, afluisteren, bedrijfsspionage, fraude, gegevensmanipulatie
- onverhoopte slordigheden, waaronder: wissen/verminken van gegevens, inbreuk op privacy, menselijke fouten
- overige risico's, waaronder: arbeidsonrust, staking.

2. Herstel, na incidentele verstoring, van de continuiteit van kritisch geachte gegevensverwerkende systemen, al of niet met behulp van uitwijk, binnen de daarvoor door het beleid bepaalde tijd.
In samenhang hiermee het aanmaken en juist bewaren van de hiervoor noodzakelijke back-up-kopieën van programma's en gegevensbestanden. Met enige regelmaat beproeven van de juiste werking van het noodvoorzieningenplan (bijvoorbeeld sloepenrol).