ANTON DE KOM UNIVERSITEIT VAN SURINAME

Faculteit der Maatschappijwetenschappen

De opzet van de Interne Controle Unit voor de districten middels "Wide Area Network" (WAN) binnen het "Decentralization and Local Government Strengthening Program (DLGP)"

Thesis ter verkrijging van de graad van Bachelor of Science in de economie

Student : Autar Suresh
Begeleider : Drs. M. Pershad

Paramaribo, augustus 2010

Voorwoord

De voor u liggende thesis wordt gepresenteerd in het kader van het afronden van de studie economie aan de Anton de Kom Universiteit van Suriname.
Mijn streven is geweest om een thesis te schrijven die voldoet aan alle te stellen wetenschappelijke eisen en die tegelijkertijd toegankelijk blijft en toegevoegde waarde heeft voor de praktijk.

Sinds de opkomst van automatisering hebben organisaties een duidelijke ontwikkeling doorgemaakt. In de haast om van een mainframe netwerk over te stappen naar een cliënt/server netwerk, hebben veel organisaties echter nagelaten om een systeem van interne controlemaatregelen te ontwikkelen. Gelukkig zien steeds meer organisaties de problemen in en ondernemen positieve stappen om de controlemaatregelen en de beveiliging van computers te vergroten. Controlemaatregelen worden nu een deel van het proces bij de ontwikkeling van applicaties.

Als aankomend econoom zal je oplossingen moeten kunnen aandragen om de systemen te beveiligen tegen alle mogelijke bedreigingen. Ook zal je dan goed op de hoogte dienen te zijn van de ontwikkelingen binnen de informatie- en communicatietechnologie (ICT).

Hierbij wil ik een ieder bedanken die op enige wijze heeft bijgedragen aan de totstandkoming van deze thesis, in het bijzonder mijn begeleider drs. M. Pershad van de Project Implementation Unit van DLGP.
Een expliciete vermelding verdient de steun, verkregen van mijn richtingscoördinator drs. R. Dwarka, die bereid was mijn concept kritisch te lezen en van commentaar te voorzien.
Een speciaal woord van dank gaat uit naar drs. A. Sheoratan R.A. van SRA Accountants-kantoor.
Ook gaat een dankwoord uit naar (wijlen) drs. P. Khedoe voor zijn assistentie mijn concept kritisch te lezen en van commentaar te voorzien.

Mijn dank gaat ook uit naar R. Ahmadali, ICT specialist van de PIU van het DLGP, die bereid was zijn assistentie te verlenen bij het beantwoorden van eventuele onduidelijkheden met betrekking tot mijn thesis en overige personeelsleden van de DLGP-unit.

Paramaribo, augustus 2010

AUTAR, Suresh

Lijst van gebruikte afkortingen

BIC : Bevolkings Informatie Centrum

DLGP : Decentralization and Local Government Strengthening Program

DLGP II : Decentralization and Local Government Strengthening Program II

DFP : Districts Financiën en Planning

ICT : Informatie- en Communicatie Technologie

IDB : Inter-American Development Bank

LAN : Local Area Network

PIU : Project Implementation Unit

WAN : Wide Area Network

WRO : Wet Regionale Organen

VPN : Virtual Private Network

Inhoudsopgave

Inleiding

De maatschappij is op weg naar een tijd waarin de vaardigheden voor "management op afstand" erg in trek zijn. De invloed van de elektronische technologie, de wens om de algemene kosten terug te dringen en de noodzaak om de souplesse te verhogen en/of te bevorderen, zijn aspecten die modernisering opeisen in het beleid van organisaties, waaronder de overheid. Overheidsorganisaties behartigen het algemeen belang. Overheidsorganisaties zijn huishoudingen die zonder tussenkomst van de markt producten en diensten beschikbaar stellen aan burgers, bedrijven en overige belanghebbenden (Starreveld, 2007: 367). Bij wet wordt geregeld welke activiteiten de overheid hoort uit te voeren. De daartoe benodigde financiële middelen zijn daarbij een middel om de activiteiten uit te voeren. Vanuit dit oogpunt bekeken, zal de modernisering van de overheid vooral gezocht moeten worden in een wezenlijk andere rolverdeling tussen burgers en overheid. Maatschappelijke problemen in Suriname kunnen niet door de overheid alleen worden opgelost. Iedereen zal daaraan naar vermogen en draagkracht moeten bijdragen. Dit betekent dat burgers zelf meer verantwoordelijkheid moeten nemen. Volgens de Surinaamse grondwet is Suriname een gedecentraliseerde eenheidsstaat. Derhalve blijkt het noodzakelijk te zijn dat burgers en hun organisaties de vrijheid krijgen om zelf bepaalde ontwikkelingen op lokaal niveau ter hand te nemen (B. Ahmadali, 1999: 5). Dit gegeven is de directe aanleiding tot decentralisatie. Taken en bevoegdheden worden hierbij overgedragen aan "lokale overheden", wat neerkomt op spreiding van bestuur en wel zodanig dat alle niveaus middels een coördinatiesysteem op elkaar zijn afgestemd. Dit is aanleiding geweest om binnen het Decentralisatieprogramma een Informatie- en Communicatie Technologie (ICT) systeem op te zetten en te beheren ten behoeve van de districten.

Sinds de opkomst van automatisering hebben organisaties een duidelijke ontwikkeling doorgemaakt. Enerzijds heeft deze veranderde invloed te maken met de voortdurende groei van de mogelijkheden van automatisering, zowel op het gebied van hardware (snelheid, capaciteit van computers), software (toepassingen op steeds meer functionele gebieden met steeds betere functionaliteit) of verbindingen (internet) (Beek, 2003:136).
De technologie is dus zover voortgeschreden dat conventionele systemen vervangen worden door computers. Het verzamelen, vastleggen, verwerken en het verstrekken van betrouwbare informatie geschiedt door middel van computers (Oonicx, 1990:17). Daar mensen en computer-

systemen ook feilbaar zijn, kan worden gesteld dat een samenstel van controlemaatregelen in acht moet worden genomen om fouten tijdig te ontdekken en te voorkomen. De elementen bij dergelijke systemen zijn onder andere de apparatuur, de mensen, de programmatuur, de organisatie en de betrokken gegevens. Met de verstrekte informatie kan alleen dan doelmatig worden gewerkt als de juiste informatie op het juiste tijdstip, in de juiste vorm en volledig wordt ontvangen.

Inleiding tot probleemstelling

De regering van Suriname streeft naar een betere ontwikkeling van de districten middels het creëren van lokale overheden, oftewel decentralisatie. Dit streven vindt zijn oorsprong in de grondwet van 1987 en in de Wet Regionale Organen. Het **"DECENTRALIZATION AND LOCAL GOVERNMENT STRENGTHENING PROGRAM" (DLGP)** moet het mogelijk maken dat alle lagen van de lokale bevolking maximaal participeren in elementaire maatschappelijke vraagstukken en als zodanig zelf de eigen prioriteiten kunnen bepalen voor de verbetering van woon -, leef -, werk- en productieomstandigheden (B. Ahmadali, 2005: 6).

Gelet op zwakke institutionele capaciteiten bij de lokale overheid, alsmede de beperkte ervaring van de overheid op het gebied van decentralisatie, met name financiële decentralisatie, is door de Surinaamse overheid een verzoek ingediend bij de Inter-American Development Bank (IDB) voor het begeleiden van de districten bij het decentralisatieproces (B. Ahmadali, 1999: 6). Decentralisatie betekent meer bevoegdheden krijgen om beslissingen over hun district te nemen.

De levering van elementaire diensten (waaronder gezondheidszorg, veiligheid, onderwijs enzovoort) is ook in Suriname afhankelijk van een coördinatiepunt, namelijk de centrale overheidsstructuur.

Het DLGP moet ook worden geplaatst in het kader van het beleid van de regering op het gebied van de versterking van de democratie. Dit is niet alleen een trend in de wereld en een vereiste van vele donorlanden en –organisaties bij het verstrekken van financiële hulp, maar het is ook de eis van de grondwet, die voor Suriname een gedecentraliseerde eenheidsstaat voorschrijft (B. Ahmadali, 1999: 3).

Het DLGP vereist een mechanisme, om de districten in hun gezamenlijke interessegebieden tot nauwere samenwerking duurzaam te binden en zo de burger in hun districten van dienst te zijn. ***Om de samenwerking gestalte te geven en kostenbesparend op te treden zullen de districten onder andere middels een Wide Area Network (WAN)-systeem opereren***. ***Als belangrijk onderdeel van het geautomatiseerd informatiesysteem (WAN) moet een adequaat interne controle systeem worden ingebouwd.*** Dit is een vereiste voor effectieve beleidsvoering; resultaten worden sneller afgemeten en in geval van afwijkingen kan snel worden opgetreden.
Het districtsmanagement moet te allen tijde over informatie kunnen beschikken om tijdig en effectief beslissingen te kunnen nemen, alsook om relevante controles uit voeren. Het is daarom van belang dat ten behoeve van elk district een administratieve organisatie met een goed functionerend interne controle-mechanisme aanwezig is.

Probleemstelling:

Het onderzoek heeft zich gericht op het beantwoorden van de volgende probleemstelling:
"Welke zijn de criteria voor het selecteren van een systeem voor het verrichten van interne controle taken?"
Subvragen:

- Wat is interne controle?
- Wat is een Local Area Network (LAN)?
- Wat houdt het Wide Area Network (WAN)-systeem in?
- Wat is de relatie tussen een LAN en een WAN?
- Wat is de relatie tussen interne controle en een geautomatiseerd systeem als WAN?

Doel van het werkstuk

Allereerst dient dit werkstuk ter verkrijging van de graad 'Bachelor of Science in de Economie'. Ten tweede kan dit werkstuk als handleiding dienen voor het DLGP voor de opzet van de interne controle unit middels het WAN-systeem.

Maatschappelijke relevantie

Er wordt getracht om aan de lezer een eenvoudig en overzichtelijk beeld te verschaffen over de opzet van de interne controle-unit voor de districten middels het WAN. Tevens kan dit

werkstuk extra informatie toevoegen aan vakken als Bedrijfsinformatie Systemen en Administratieve Organisatie. Tenslotte ligt het in de bedoeling dat deze thesis als leidraad kan dienen voor het opzetten van een controle-unit.

Methodologie

Deze thesis is gebaseerd op:

- een literatuurstudie, waarmee de theoretische richtlijnen worden belicht, welke nodig zijn om een beter inzicht te krijgen in het begrip 'controle' en de hieraan gerelateerde onderwerpen. Hiermee wordt getracht te komen tot verantwoorde uitspraken over de opzet van de interne unit als onderdeel van het WAN-systeem binnen het DLGP.
- een empirisch onderzoek dat plaatsvond middels het afnemen van interviews van de medewerkers / functionarissen van het PIU-team van het DLGP, het Ministerie van Regionale Ontwikkeling en districtsfunctionarissen alsook middels het doen van observaties bij het WAN gebouw.

Opbouw van deze thesis

In hoofdstuk 1 worden de theoretische grondslagen van interne controle en Wide Area Network belicht.

In hoofdstuk 2 wordt er aandacht besteed aan het DLGP. De componenten die relevant zijn voor deze thesis worden in dit hoofdstuk beschreven.

In hoofdstuk 3 komen aan de orde de criteria en maatregelen voor het selecteren van een effectief automatiseringssysteem.

Tenslotte komen de conclusies en aanbevelingen aan de orde.

Hoofdstuk 1 Theoretische grondslagen van interne controle en het Wide Area Network

1.1 Algemeen

Een administratieve organisatie wordt omschreven als het gehele complex van organisatorische maatregelen dat direct of indirect betrekking heeft op de goede werking van de bestuurlijke informatievoorziening (Beek, 2003: 37). Het vakgebied "Bestuurlijke Informatievoorziening omvat de organisatie van het administratieve apparaat, de organisatie van de gegevensverwerking, de analyse van de informatiebehoeften, de bronnen van de gegevens, de distributie van de informatie en de regels waaraan het informatiesysteem moet voldoen (Beek, 2003: 18). Het ontbreken van een goede administratieve organisatie leidt vaak tot leemtes in de organisatie, waardoor het nemen van beslissingen, het plannen en beheersen van bedrijfsprocessen, het afleggen van verantwoording over het gevoerde beleid en beheer, evenals de controle op de verantwoording in gevaar kunnen komen.

Controle is het toetsen van de werkelijkheid aan een norm. De normen dienen daarbij vooraf en zo recent mogelijk te worden bepaald. Tot de interne controle worden gerekend zowel de maatregelen die in de organisatie door mensen worden genomen als de uitvoering hiervan binnen een geautomatiseerd systeem. Het Nederlandse begrip ‘interne’ controle vindt zijn oorsprong in de managementfunctie. Tot die functie behoren al van oudsher de aspecten plannen, organiseren, dirigeren en controleren. Interne controle omvat alle elementen van leiding, waarop de controle als complement kan worden gezien (Beek, 2003: 84).

Tot de *objecten van interne controle* worden gerekend (Beek, 2003: 84):

- *de niet- levende systemen* (computers, netwerken, randapparaten);
- *de levend geachte systemen* (organisaties, organisatie van systeemontwikkeling, gegevensverwerking);
- *de levende systemen* (mensen en groepen, bijvoorbeeld de bij de automatisering betrokkenen).

Het Amerikaanse begrip ‘internal control’ heeft in tegenstelling tot het Nederlandse begrip meer te maken met het beheersen van de organisatie. Het begrip omvat dan ook: de organisatie

en de planning daarvan inclusief de procedures en richtlijnen ter bescherming van (Beek, 2003: 84):

- de bezittingen;
- de controle op de accuratesse en van de betrouwbaarheid van de financiële gegevens;
- het bevorderen van de efficiëntie.

Deze thesis is gebaseerd op het opzetten van een intern controle-unit. Bij de verdere uitwerking van deze thesis zal slechts de Nederlandse visie in ogenschouw worden genomen. Zoals eerder aangegeven, vindt controle steeds plaatst door het toetsen van de werkelijkheid aan de gestelde norm. Iedere controle heeft te maken met drie elementen, te weten (Starreveld, 2002: 394):

- de grootheid (object) die moet worden gecontroleerd wordt aangeduid als de ist-positie;
- de grootheid die als controle maatstaf dient wordt als soll-positie aangeduid; de soll- positie is het hulpmiddel waarmee het resultaat van een gepleegde handeling en/of grootheid (ist-positie) kan worden beoordeeld;
- de eigenlijke toetsing vindt plaats door het constateren of onder de ist-positie aangeduide grootheden afwijken van de onder soll-positie vermelde grootheden (het verschil is al of niet nul).

Technisch geschiedt de eigenlijke controle door het constateren of de ist-positie afwijkt van de soll-positie. Indien een afwijking wordt geconstateerd, dient deze afwijking vervolgens te worden gesignaleerd – hier in de zin van waarschuwen – en wel in die gevallen dat de afwijking groter is dan de daarvoor gestelde tolerantie.

1.2 Soorten van controle

Het begrip controle omvat de volgende typen van controle (Starreveld, 2002: 251):

- zelfcontrole: is de controle die wordt uitgevoerd op eigen verrichte activiteiten. Deze controle wordt uitgeoefend door het resultaat van de verrichting te vergelijken met de daarvoor door hem of haar gestelde of aanvaarde norm. Degene die zelfcontrole verricht hoeft geen persoon te zijn, het kan ook een machine zijn, die zodanig is geprogrammeerd

dat na het verrichten van een handeling, deze direct wordt gecontroleerd aan de hand van een vooraf gestelde norm;

- interne controle: deze controle definiëren wij als de controle op de oordeelsvorming en de activiteiten van anderen, voor zover die controle ten behoeve van de leiding van de betrokken huishouding door of namens die leiding wordt uitgeoefend;
- externe controle: is de controle die door een derde wordt uitgeoefend ten behoeve van anderen dan de leiding van de betrokken huishouding;
- sociale controle: de controle die een groep van personen of een gemeenschap uitoefent op de oordeelsvorming, de activiteiten en het gedrag van een lid van die groep of die gemeenschap.

Gezien de omstandigheid dat iedere vorm van controle kosten met zich meebrengt, dient de vraag te worden gesteld waarom deze drie vormen van controle naast elkaar voorkomen en/of een van deze controles wel door een van de andere of door beide andere vormen kan worden vervangen. Het onderscheid in het begrip controle heeft te maken met de reikwijdte van de drie bovengenoemde vormen van controle. Onder *reikwijdte* van een controle verstaan wij de functionele afstand tussen degene voor wie de uitgevoerde controle van betekenis is enerzijds en de controleur anderzijds. Zo zal de reikwijdte van de externe controle groter zijn dan die van de interne controle en deze laatste is weer groter dan de reikwijdte van de zelfcontrole (Starreveld, 2002: 253).

1.3 Interne controle

1.3.1 De behoefte aan interne controle

De behoefte aan interne controle en beveiliging komt voor een groot deel voort uit de scheiding van leiding en eigendom van de organisatie. De delegatie van taken, bevoegdheden en verantwoordelijkheden aan een medewerker ontslaat de leider niet van zijn eigen verantwoordelijkheid jegens de eigenaren. Hij blijft verantwoordelijk voor de inzet en de uitvoering van de taken van de medewerker en moet daarom controle uitoefenen of de uitwerking voldoet aan de opdracht. Dit betekent ook dat de interne controle door of namens de leiding dient plaats te vinden (Beek, 2003:89).

1.3.2 Doel Interne Controle

Het doel van interne controle is het voorkomen, en het tijdig opsporen en corrigeren van onvolkomenheden in de uitoefening van bedrijfsactiviteiten (waaronder het vormen van een oordeel), alsmede het scheppen van de mogelijkheid om zo nodig nieuwe maatregelen te treffen teneinde te voorkomen dat de gesignaleerde onvolkomenheden in de toekomst weer optreden (Starreveld, 2002: 390).

1.3.3 Controle maatregelen

Voor de interne controle zijn met betrekking tot het informatiesysteem drie groepen van maatregelen van belang, te weten (Beek, 2003: 89):

- de preventieve maatregelen;
- de maatregelen ter waarneming of constatering van de betrouwbaarheid en de effectiviteit, ook wel genoemd repressieve maatregelen;
- de eventuele maatregelen van correctie.

Alvorens men overgaat tot het vaststellen van de preventieve maatregelen die ingevoerd dienen te worden, zullen de leiding van de organisatie en de werkzame controller de risico's die in de organisatie bestaan, moeten onderkennen. Risico is daarbij op te vatten als de kans op een bedreiging welke kan leiden tot een schade. Het weten welke risico's bestaan, alsmede hun onderlinge samenhang en mate van belangrijkheid, kan alleen worden vastgesteld door een goede risicoanalyse (Beek, 2003: 89). Risico's kunnen alleen worden opgelost als er voldoende controle- en beveiligingsmaatregelen worden toegepast en wel zodanig dat deze effectief werken. Om zeker te zijn dat de preventieve maatregelen werken zoals bedoeld, zullen deze moeten worden aangevuld met maatregelen ter waarneming of constatering van de betrouwbaarheid en de effectiviteit. Deze maatregelen worden repressieve maatregelen genoemd. Blijkt bij de constatering namelijk dat er iets fout is gegaan, dan dient doorgaans correctie plaats te vinden. We spreken dan in dit geval van corrigerende maatregelen (Beek, 2003:92).

1.3.4 Functiescheidingen, functievermenging en samenspanning

Functiescheidingen

Bij functiescheidingen is het de bedoeling om de taken zodanig op te delen en beperkingen in de bevoegdheden van de verschillende functionarissen aan te brengen dat onder andere (Starreveld, 2002:398):

- iedere functionaris slechts een beperkt aantal schakels van het totale omloopproces kan beïnvloeden. Deze beperking is namelijk noodzakelijk in verband met de mogelijkheid dat anders een functionaris in staat zou zijn een transactie uit te voeren zonder dat deze transactie op de een of andere wijze wordt verantwoord. Het aantal schakels per functionaris dient dan ook zover te worden ingekrompen dat hierdoor het gevaar een transactie 'buiten de boeken te houden' verdwenen is;
- beslissingen tot het beschikken over zaken alleen kunnen worden genomen door personen die niet zelf met de bewaring van die zaken belast zijn;
- personen die als uitvoerders verantwoordelijk zijn voor het rendement van bepaalde technische of commerciële omzettingsprocessen, niet tevens belast zijn met een relatief langdurige bewaring voor de aan te wenden verkregen goederen, respectievelijk gelden;
- mogelijkheden worden geschapen tot het verkrijgen van elkaar wederzijds controlerende verantwoordingsverslagen van personen met niet – identieke en zo mogelijk tegen- gestelde belangen;
- geen functionarissen die beschikkings- en/of uitvoeringsmacht uitoefenen, deelneemt aan enig deel van de registratie dat kritisch is ten aanzien van de op zijn of haar activiteit uit te oefenen controle;
- ten aanzien van die onderdelen van de administratie die praktisch mede een bewarings- karakter hebben, de controle in handen wordt gelegd van een ander dan degene door wie dat onderdeel van de administratie wordt gevoerd.

Functievermenging

Als iemand belast is met twee of meer naar hun aard verschillende functies, spreken we van functievermenging. De controle op de juistheid van de verantwoordingen is dan niet meer mogelijk (Beek, 2003: 96).

Samenspanning

Indien de functies beschikken, bewaren, registreren en controleren wel gescheiden zijn, maar twee of meer functionarissen zodanig zijn gaan samenwerken dat zij bewust een foutieve registratie van de bedrijfshandelingen bewerkstelligen, spreekt men van samenspanning. Samenspanning heeft altijd als doel te frauderen (Beek, 2003: 96).

1.4 Controlemiddelen

Controlemiddelen vormen het gereedschap van de controleur-administrateur. De controle-middelen kunnen op verschillende wijze worden toegepast. Het te kiezen controlemiddel hangt derhalve geheel af van de doelstelling van de controle. Enkele controlemiddelen zijn (Beek,2003: 118):

- verbandscontrole: bij verbandscontrole wordt gebruikgemaakt van het feit dat er tussen verschillende grootheden een onderling verband aanwezig is. Dit houdt in dat als de juistheid van een van de grootheden reeds is vastgesteld, daaruit de grootte van het bedrag van de daarmee verband houdende grootheid kan worden afgeleid;
- cijferbeoordeling: bij cijferbeoordeling worden cijfers vergeleken met een norm en wel:
  - in onderling verband over een bepaalde periode en
  - gezien tegenover de ontwikkeling van een aantal jaren;
- aanwezigheidscontrole: bij aanwezigheidscontrole wordt het bestaan van waarden op een bepaald tijdstip vastgesteld, bijvoorbeeld door middel van inventarisatie van voorraden, kasgelden en aangeschafte inventaris;
- ontstaanscontrole: er is sprake van ontstaanscontrole als van registraties de rechtmatigheid van het ontstaan van de posten wordt nagegaan. Bijvoorbeeld vaste activa;
- afloopcontrole: er is sprake van afloopcontrole als de aanwezigheid van bezittingen en/of schulden per een reeds verschenen datum vastgesteld wordt door de afwikkeling van de posten na te gaan. De controle geschiedt dus achteraf;
- controle met behulp van opgaven van derden: van deze methode kan gebruik worden gemaakt om meer zekerheid te verkrijgen en ter besparing van controlearbeid. Van belang is hierbij is dat bijzonder gelet moet worden op de betrouwbaarheid van de opgaven. De

controle vindt plaatst middels vergelijking van de opgaven met bijvoorbeeld de geregistreerde ontvangen aantallen. Bijvoorbeeld opgaven van grondstoffen- leveranciers van de in een bepaalde periode afgeleverde aantallen en soorten grond- stoffen;

- controlemiddelen en automatisering: bij geavanceerde geautomatiseerde toepassingen blijven de functies van de controlemiddelen onaangetast. Hierbij is het wel van belang dat de zekerheid bestaat dat de gegevens worden bewaard.

1.5 Controletechnieken

Bij controletechnieken gaat het om de vraag hoe het gereedschap wordt gehanteerd. De techniek van de controle omvat het geheel van de verrichtingen (werkzaamheden en gedetailleerde werkinstructies) om de controledoelstellingen te bereiken. Men onderscheidt hierbij de volgende begrippenparen (Starreveld, 2002:404):

- directe en indirecte controle: directe controle is controle die zich door waarneming richt op de te controleren activiteiten zelf. Het doel van deze controle is dan om na te gaan of de activiteiten worden uitgevoerd volgens de taakopdracht, die daartoe gedetailleerd moet worden opgemaakt. Indirecte controle is de controle die zich richt op het product of het resultaat van de te controleren activiteit. Men controleert daarbij of het product of het resultaat ten grondslag liggende activiteiten controleert;
- formele en materiële controle: formele controle is de controle waarbij wordt nagegaan of aan de gestelde voorschriften is voldaan. Materiële controle is de controle waarbij wordt nagegaan of:
  - de verantwoorde handeling of toestand inderdaad heeft plaatsgevonden, respectievelijk bestaat en
  - bovendien bedrijfseconomisch toelaatbaar is of aanvaardbaar is;
- positieve en negatieve controle: positieve controle is de controle die zich op de juistheid van de te controleren gegevens richt. Het gaat erom of het gegeven juist (dus ook niet te vroeg) is verantwoord of geregistreerd, en/of de handeling die aan de verantwoording of registratie ten grondslag lag, wel terecht en door de bevoegde persoon is geschied (de rechtmatigheid). Negatieve controle is de controle die zich richt op de vraag of alles wat

verantwoord of geregistreerd zou moeten worden, ook wel verantwoord of geregistreerd is. Uiteraard valt hieronder ook de controle op het te laat verantwoorden of registreren;

- detail- en totaalcontrole: detailcontrole is de controle waarbij iedere post afzonderlijk wordt gecontroleerd, terwijl bij totaalcontrole groepen gelijksoortige posten op de een of andere wijze worden samengevoegd tot totalen, die worden vergeleken met controle totalen die langs andere weg uit hetzelfde grond materiaal of uit andere daarmee inhoudelijk samenhangende gegevens zijn verkregen of afgeleid.

1.6 Geautomatiseerde informatiesystemen

Een systeem is een verzameling componenten die op een bepaalde wijze zijn gerelateerd en geordend en die samen het gestelde doel willen bereiken. Een informatiesysteem is 'het geheel van mensen, machines en activiteiten, gericht op het verzamelen en verwerken van gegevens op zodanige wijze dat kan worden voorzien in de informatiebehoeften van een organisatie alsmede in die van externe belanghebbenden of belangstellenden' (Jans,1999:81). Bij geautomatiseerde informatiesystemen geschiedt het verzamelen, vastleggen, verwerken en het verstrekken van betrouwbare informatie door middel van computers.

Geautomatiseerde systemen zijn binnen moderne organisaties een niet weg te denken fenomeen. Het ontwikkelen van dergelijke systemen is een complex en moeilijk beheersbaar proces. Tezamen met de snelle technologische ontwikkelingen vormt het een belangrijk aandachtspunt voor elke organisatie.

Een geautomatiseerd systeem bestaat uit de volgende elementen (Starreveld, 2002: 612):

- de apparatuur, niet alleen bevattende de centrale verwerkingseenheid en geheugens, maar ook de perifere apparatuur in al haar verschijningsvormen;
- de programmatuur, die zowel de systeem- als de toepassings- of applicatie program- matuur bevat;
- de mensen, die direct of indirect met de apparatuur en programmatuur te maken hebben. Men dient hierbij niet alleen te denken aan hen die in een toepassingscentrum of -afdeling werken, maar ook aan al die functionarissen die de toepassingen gebruiken;

- de organisatie, zowel wat haar structuur als haar werking betreft. De werking van de organisatie komt onder meer tot uiting in de gevolgde procedures en de daarbij van toepassing zijnde voorschriften;
- de betrokken gegevens, dat wil zeggen de te verwerken gegevens, de als informatie te verstrekken gegevens en de bij de verwerking benodigde gegevensverzamelingen.

Om een geautomatiseerd informatiesysteem (in het bijzonder de programmatuur) binnen een organisatie op een betrouwbare en bedrijfszekere wijze te kunnen gebruiken, zijn vele elementen noodzakelijk. De belangrijkste zijn (Starreveld, 2002: 573):

- een applicatie met eventuele koppelingen naar andere applicaties;
- de bijbehorende handmatige procedures met opgeleide gegevensleveranciers;
- de geconverteerde gegevens;
- een technische infrastructuur (computers, netwerken, enzovoorts.);
- opgeleide gebruikers;
- een (functionele) organisatie, gericht op het in bedrijf houden van de technische infrastructuur (productieorganisatie, ook wel aangeduid als computer- of rekencentrum);
- een (functionele) organisatie om het onderhoud van het systeem te ondersteunen;
- documentatie voor de gebruikers, de onderhoudsorganisatie en de productie- organisatie.

Criteria voor beoordeling inzake informatiesystemen (Starreveld, 2002: 499-500)**:**

- effectiviteit: hiermee wordt bedoeld in hoeverre de doelstellingen van de systemen in de praktijk worden verwezenlijkt;
- tijdigheid/vorm van de informatie: hiermee wordt bedoeld in hoeverre voor de uitvoering en/of sturing van de processen benodigde informatie tijdig en in de juiste vorm aan de systemen kunnen worden ontleend;
- gebruikersvriendelijkheid: hiermee wordt bedoeld in hoeverre de systemen door de gebruikers als toegankelijk en gebruikersvriendelijk worden ervaren;
- beveiliging: hiermee wordt bedoeld hoe het is gesteld met de beveiliging en de integriteit van de vastgelegde gegevens;
- betrouwbaarheid: hiermee wordt bedoeld hoe het met de betrouwbaarheid van de systemen is gesteld;

- kosten/baten: hiermee wordt bedoeld in hoeverre de kosten van de systemen tegen de baten opwegen.

1.7 Beveiliging van de programmatuur en gegevensbestanden

Beveiliging is een heel belangrijk aspect binnen informatiesysteem. Zonder goede beveiligingsmaatregelen werkt het informatiesysteem in technische zin correct. Bij het beveiligen van het systeem, in het bijzonder de beveiliging van de programmatuur en de gegevensbestanden, dient aandacht te worden besteed aan de beveiliging tegen de buitenwereld. Met beveiliging tegen de buitenwereld wordt in dit geval bedoeld, beveiliging tegen:

- computervirussen: een computervirus is een programma dat in staat is zichzelf in andere programma's te nestelen en op diverse manieren schade aan te richten (Beek, 2003: 188);
- wormen: een worm is een bijzondere vorm van een virus. Het kenmerk is het vertragen van de systeemprogrammatuur. Wormen verplaatsen zich zonder gebruik te maken van een ander programma. Ze verspreiden zich vooral via netwerken (Beek, 2003: 189);
- gemengde bedreigingen: combineren de verspreidingskenmerken van virussen en wormen (Panko, 2005: 362). Hieronder vallen:
  - trojaanse paarden: een trojaanse paard is een schadelijk programma dat een gebruiker onopgemerkt op zijn computer installeert. Het wordt opgenomen in een bepaalde programma en wordt actief na een bepaalde gebeurtenis (Beek, 2003: 189);
  - hackers: een gebruiker die voor de grap of uit financieel gewin op andere computersystemen binnendringt (Casad, 2001: 340).

Beveiliging tegen computervirussen, wormen en trojaanse paarden kan plaatsvinden door een antivirussoftware. Antivirussoftware beschermt een organisatie echter alleen tegen kwaadaardige programma's. Om virussen te stoppen, moet een organisatie zijn computers beschermen met antivirusprogramma's die elk inkomend e-mailbericht of diskette kunnen scannen op signaturen waaraan virussen worden herkend. Deze antivirusprogramma's scannen ook de andere typen malware (kwaadwillende software), zoals wormen en trojaanse paarden (Panko, 2005: 361-362).

Beveiliging tegen hackers kan geschieden middels firewalls. Firewalls zijn toegangscontrole-apparaten voor het netwerk van een organisatie tegen aanvallen van buitenaf. Firewalls zijn in principe randbeveiligingsproducten, wat betekent dat ze zich bevinden in een randgebied tussen het interne en externe netwerk. Goed geconfigureerde firewalls zijn een noodzakelijke beveiliging geworden. Een firewall voorkomt echter niet dat een aanvaller een systeem benadert via een erkende verbinding (Maiwald, 2001: 11).

1.8 Controlemaatregelen en beveiliging bij geautomatiseerde systemen

Maatregelen en procedures die aanwezig moeten zijn om een juiste, volledige en continue gegevensverwerking te waarborgen, zijn:

- functionele organisatie: plaats van de automatiseringsafdeling en functiescheiding tussen systeemontwikkeling en systeembeheer, en tussen de automatiserings- functie en de gebruikersomgeving. Valt direct onder de verantwoordelijkheid van de directie (Westra, 2002:208);
- change management: change management heeft betrekking op de maatregelen en procedures bij het implementeren van nieuwe automatiseringssystemen of het aanbrengen van wijzigingen op de bestaande. Belangrijk hier is dat de ontwikkeling van het nieuwe systeem volledig gescheiden plaatsvindt van de verwerking, of wel dat er functiescheiding bestaat tussen de ontwikkel- en testomgeving en de operationele verwerking (Westra, 2002:208);
- logische toegangsbeveiliging: de logische toegangsbeveiliging dient te worden gezien als het doortrekken van de traditionele functiescheiding binnen een organisatie in het geautomatiseerde systeem. Binnen de huidige computersystemen is een aantal softwarecomponenten aanwezig dat het mogelijk maakt om een geheel van op elkaar sluitende maatregelen te treffen, zodat slechts geautoriseerde functionarissen toegang krijgen tot de gegevens waarvan zij eigenaar dan wel gebruiker zijn (Beek, 2003:194). De noodzakelijke controle-technische functiescheidingen zijn opgenomen in de raad-, pleeg- en vooral de mutatiebevoegdheden per gebruiker zoals vast- gelegd in de competentietabel. Handelingen die worden verricht met het geautomatiseerd systeem worden geregistreerd

(logging). Pogingen tot ongeautoriseerde toegang worden via signaleringslijsten onder de aandacht gebracht van bevoegde functionarissen. Het is van belang dat inbreuken (of pogingen daartoe) nader worden onderzocht om herstellende werkzaamheden te kunnen verrichten, maar ook om herhaling te voorkomen (Westra, 2002:208);

- fysieke toegangsbeveiliging: de fysieke beveiliging richt zich op de toegangs- beveiliging tot de computerruimte en op de beveiliging van de opslag tegen brand, inbraak en dergelijke (Westra, 2002:208);
- back up-, recovery- en uitwijkprocedures: bij een back-upsysteem gaat het om een reservesysteem dat is bedoeld om de taken die worden uitgevoerd over te nemen als zich daarin storingen voordoen. In de praktijk wordt hieronder verstaan dat van de programmatuur en de opgeslagen gegevens een kopie of reserve-exemplaar aanwezig is. Van belang hierbij is dat tenminste één kopie op een externe locatie wordt bewaard. De herstel/recovery-procedures moeten regelmatig worden getest. Verder dienen er contractuele bepalingen met de leveranciers over service en vervangende apparatuur te zijn als ook toereikende verzekeringen ingeval van calamiteiten (Westra, 2002:208);
- documentatie: een andere belangrijke controlemaatregel is dat er documentatie- procedures bestaan. Het is van belang dat de gebruikers en dat de systeemdocumentatie up-to-date zijn. Tot de systeemdocumentatie behoren onder meer een beschrijving van het systeem of subsysteem, schema's van het functioneel en technisch ontwerp, een overzicht van controlemaatregelen, de testprocedures en testresultaten. De gebruikersdocumentatie bevat procedure- beschrijvingen, voorschriften, instructies, formulieren en schermindelingen. Deze behoren door de gebruikers te worden getest (Jans, 1999: 186);
- systeemcontroles (geprogrammeerde controle): het geautomatiseerd systeem moet voorzien in ingebouwde systeemcontroles, zoals bestaanbaarheidscontroles, redelijk- heidscontroles en controles op de doorlopende nummering. Deze controles kunnen zijn opgenomen in de hardware, de systeemsoftware en/of in de applicaties (toepassingen) zelf. Geprogram-meerde controles kunnen de verdere verwerking blokkeren of slechts signaleren. Bij blokkering van het systeem is uiteraard ook relevant wie bevoegd is deze blokkeringen te 'overrulen' om het systeem weer operationeel te krijgen en welke procedures hierbij worden gehanteerd. Uitgaande van de documentatie worden testgevallen ontworpen, bijvoorbeeld door invoer van niet-bestaande belastingbetalers, en pogingen tot manipulatie achteraf. Per

testgeval wordt de werkelijke uitkomst vergeleken met de voorspelde. De testgevallen vormen in feite de confrontatie tussen enerzijds de opzet van de interne controlemaatregelen (zoals opgenomen in de documentatie) en anderzijds het bestaan (de feitelijke aanwezigheid) hiervan. Of deze maatregelen vervolgens daadwerkelijk gedurende gehele controleperiode naar behoren hebben gefunctioneerd - de adequate werking - is overigens niet alleen afhankelijk van de opzet en het bestaan van de maatregelen, maar ook van de eventuele inbreuken hierop. Het onderzoek van het logbestand is dus onmisbaar bij de controle op de werking van de geprogrammeerde controles. Het bestand moet zodanig zijn beveiligd dat manipulatie onmogelijk is, zelfs niet door de systeembeheerder (Westra, 2002: 211);

- gebruikerscontroles: gebruikerscontroles (usercontrols) zijn handmatige controles, die specifiek zijn ontworpen om de volledigheid, juistheid en geldigheid van transacties te bewaken. Gebruikerscontroles zijn te onderscheiden in:
  juistheid en volledigheid van de gegevensverwerking:

(a) variabele (stand- of stroom-) gegevens:

- totaalcontrole aan de hand van voortellingen;
- bestandscontroletotalen (batchtotals): beginstand + invoerstand = eindstand;

(b) vaste (stam-)gegevens:
integrale, functioneel gescheiden, detailcontrole van de output met brongegevens, zoals geautoriseerde prijs- en kortingslijsten (Westra, 2002: 213).

1.9 Computernetwerken

Een netwerk wordt gedefinieerd als twee of meer computers die met elkaar verbonden zijn met als doel te communiceren en informatie en andere bronnen met elkaar te delen. Netwerken zijn er in allerlei soorten en maten. We onderkennen in het algemeen twee hoofdcategorieën: Local Area Network (LAN) en Wide Area Network (WAN). Afgeleid van het LAN en WAN zijn er ook nog Personal Area Network (PAN), Metropolian Area Network (MAN) en Campus Area Network (CAN) (Scrimger, 2002: 11).

De meeste netwerken zijn gebouwd rond een kabelverbinding die de computers met elkaar verbindt. Deze verbinding biedt de computers de mogelijkheid via een draad "te praten" en "te luisteren". Naast kabelverbindingen zijn er ook draadloze verbindingen mogelijk, zoals wifi, infraroodpoorten, bluetooth-radioverbindingen en andere protocollen. Deze bieden de mogelijkheid een verscheidenheid aan apparaten draadloos aan computers te koppelen.
Wil een netwerk functioneren, dan moet het aan drie basiseisen voldoen, het netwerk moet namelijk (Microsoft Corporation, 2001: 332):

- verbindingen verschaffen: hieronder valt de hardware die nodig is om een computer aan het netwerk te koppelen, namelijk;
  - het netwerkmedium: de netwerkhardware die de computers fysiek aan elkaar koppelt. Dit is de kabel tussen de computers of een draadloze verbinding;
  - de netwerkinterface: de hardware die een computer aan het netwerkmedium koppelt en dienst doet als tolk tussen de computer en het netwerk. Om een computer aan het netwerk te koppelen, is een uitbreidingsbord nodig dat we een netwerkinterfacekaart (nic) noemen;
- communicatie verschaffen: omvat de regels ten aanzien van de manier waarop computers (communiceren en elkaar begrijpen);
- service verschaffen: bestaat uit alles wat een computer deelt met de rest van het netwerk. Een computer kan bijvoorbeeld een printer, bepaalde directory's of bestanden delen.

Typen netwerken

Er zijn in feite twee typen netwerken die onderling verschillen in hoe ze informatie opslaan, hoe ze de beveiliging afhandelen en hoe ze computers op het netwerk laten samenwerken. Deze twee typen zijn (Microsoft Corporation, 2001: 334):

- peer-to-peer-netwerk: in dit netwerk doen alle computers dienst als server (die zijn gegevens of services met andere computers deelt) of als cliënt (die gegevens of services van een andere computer gebruikt), afhankelijk van de behoefte van de gebruiker;
- servernetwerk: dit netwerk vereist een centrale server (dedicated computer) die de toegang tot alle gedeelde bestanden en randapparaten beheert. Dit is een veilige omgeving en geschikt voor de meeste organisaties. In dit geval beheert de servercomputer waarop het

netwerkbesturingssysteem draait, de beveiliging en de toegang tot bronnen. De cliëntcomputer maakt verbinding met het netwerk en gebruikt de beschikbare bronnen.

Netwerkbesturingssysteem

Het netwerkbesturingssysteem of Network Operating System (NOS) bestaat uit een familie van programma's die in netwerkcomputers draaien. Sommige programma's bieden de mogelijkheid bestanden, printers en andere apparaten over het netwerk te delen. Computers die hun bronnen delen worden servers genoemd en computers die bronnen van andere computers gebruiken, staan bekend als 'clients". Het is gebruikelijk cliënt- en serversoftware op dezelfde computer te draaien. Zo hebt u toegang tot bronnen op een andere computer terwijl, collega's gebruikmaken van bronnen op uw computer (Microsoft Corporation, 2001: 338). Bij pc's zijn er drie populaire Network Operating Systems: Linux, Novell netware en server-versies van microsoft windows.

Local Area Networks

Een Local Area Network ofwel LAN is een netwerk dat een beperkte afstand overbrugt (meestal een locatie of een gebouw) en het delen van informatie en bronnen mogelijk maakt. Een LAN kan zo eenvoudig zijn als twee met elkaar verbonden computers of zo gecompliceerd als een grote locatie waarin vele computers met elkaar verbonden zijn. Een LAN is populair omdat het de aparte computers de mogelijkheid biedt hun eigen verwerkingsmogelijkheden en geheugen te gebruiken, terwijl programma's en gegevens op elke computer in het netwerk kunnen worden opgeslagen. Het voornaamste voordeel van een LAN is om zijn vermogen te delen. Tabel 1 geeft een overzicht van enkele voordelen van het delen van de meest voorkomende bronnen in een LAN (Microsoft Corporation, 2001: 333).

Tabel 1 voordelen in een LAN van het delen van de meest voorkomende bronnen

Bron	**Voordeel**
Gegevens	Het delen van gegevensbestanden die in een gemeenschappelijke locatie staan, maakt toegankelijkheid voor meerdere gebruikers eenvoudiger. Het is ook eenvoudiger om de gegevensintegriteit te bewaren wanneer er één centrale database is. Grote

	klantendatabases en boekhoudgegevens zijn ideaal voor een LAN-systeem.
Randapparaten	Dankzij het delen van bijvoorbeeld printers kunnen meer gebruikers taken naar één printer verzenden. Dit is handig wanneer er maar één hoge-kwaliteitsprinter in een kantoor staat met die het hele kantoor moet gebruiken, wat kostenbesparingen oplevert in de hardware en overbodige bronnen als één apparaat niet werkt.
Software	Het delen van één exemplaar van een toepassing kan rendabel zijn (veel softwarefabrikanten geven locatielicenties uit; dat zijn licenties voor meerdere gebruikers op één server). Het maakt onderhoud en upgraden ook eenvoudiger.
Opslagruimte	Grotere, snellere schijfsystemen kunnen rendabel worden gebruikt voor eenvoudige back-ups.

(Bron: Microsoft Corporation; A+ Certificering Training Kit; derde editie; blz.334)

Naast het vermogen bronnen te delen, bieden LAN's nog vele andere voordelen, waaronder (Microsoft Corporation, 2001: 334):

- veerkracht: regelmatige back-ups van het gehele systeem verminderen sterk het gevaar van gegevensverlies. Door gegevens naar back-up servers te kopiëren, kunnen netwerken blijven functioneren als een primaire server faalt;
- communicatiegateways: goedkope toegang tot fax- en internetverbindingen;
- e-mail: rendabele en gemakkelijke communicatie over het hele netwerk.

Wide Area Network

Een Wide Area Network (ofwel WAN) overbrugt relatief grote geografische gebieden (Microsoft Corporation, 2001: 334). Een WAN-verbinding is gebaseerd op een verbindingsmedium dat geen onderdeel van een LAN is. WAN-verbindingen zijn vaak serieel en worden aangeboden door telecommunicatiebedrijven. Er kan gekozen worden uit verschillende soorten WAN-verbindingen. Kleine bedrijven huren bijvoorbeeld een verbinding met een kleine bandbreedte. De bandbreedte is per definitie de hoeveelheid gegevens die de verbinding per tijdseenheid kan verwerken. Vergelijk de bandbreedte met de waterstroom door

een pijp. De hoeveelheid water die de pijp per tijdseenheid kan passeren, is aan een maximum gebonden. Als de wateraanvoer toeneemt, moet een pijp met een grotere diameter worden geïnstalleerd. Bandbreedte werkt precies hetzelfde. Een normale WAN-verbinding heeft een bandbreedte die een veelvoud is van 64 kbps (kilobits per seconde). Gebruikelijke WAN-verbindingen zijn 128 kbps, 256 kbps, 512 kbps en t1. T1 heeft een bandbreedte van 1,54 Mbs (megabits per seconde).

Een belangrijk onderscheid tussen LAN en WAN-verbindingen is dat WAN-verbindingen niet permanent zijn. Als het telecommunicatiebedrijf per ongeluk de verkeerde schakelaar omzet, wordt de WAN-verbinding verbroken en kan de gebruiker alleen lokaal communiceren. In een LAN, met permanente verbindingen, wordt een verbinding verbroken als een kabel breekt of de stroom uitvalt.

Stel dat een bedrijf (bedrijf B) besluit een WAN-verbinding te kopen. Telecommunicatiebedrijf Z verhuurt bedrijf B een T1 voor € 800 per maand. Bedrijf B heeft twee locaties die onafhankelijk van elkaar zijn, maar wel gegevens delen via een WAN-verbinding. Als bedrijf B vergeet de rekening van het telecommunicatiebedrijf te betalen, is de WAN-verbinding niet langer beschikbaar en kunnen de beide locaties van bedrijf B niet langer met elkaar communiceren, maar nog wel binnen elke locatie.

De verbinding in een LAN zijn permanent en worden niet beheerd door een telecommunicatiebedrijf. WAN-verbindingen zijn gebaseerd op kabelsystemen die een telecommunicatiebedrijf beheert en exploiteert (Scrimger, 2002: 11).

Aanleidingen om een WAN te bouwen

WAN's hebben drie belangrijke doelen, namelijk (Panko, 2005:274):

- het eerste doel is het bieden van externe toegang aan klanten of aan individuele medewerkers die thuis werken of verplaatsbaar zijn;
- het tweede is het verbinden van twee of meer locaties binnen hetzelfde bedrijf;
- het derde is toegang bieden tot internet.

WAN-technologieën (Panko, 2005:274)[1]:

- **virtual private networks (VPN`s):** internet is echter een onveilige omgeving, dus moet bedrijfstransmissie via internet cryptografisch beveiligd worden. Virtual Private Networks (VPN`s) maken voor datatransmissie gebruik van internet met extra beveiliging. Typen VPN's:
  - externe VPN`s: deze VPN`s worden gebruikt voor externe toegang: het verbinden van een individuele gebruiker met een bedrijfslocatie;
  - site-to-site VPN`s: deze VPN`s worden gebruikt voor site-to-site- transmissie. Deze verbinden LAN`s op verschillende locaties en ze transporteren het verkeer van meerdere gebruikers. Dientengevolge zullen site-to-site VPN`s op den duur het VPN-gebruik gaan domineren;
  - Host-to-host VPN`s: VPN`s kunnen ook rechtstreeks tussen twee hosts worden aangelegd. Hierdoor kunnen twee medewerkers op een veilige manier met elkaar communiceren.

[1] Binnen het kader van dit werkstuk is het niet toereikend om een gedetailleerd overzicht te geven over de WAN-technologieën. Voor de geïnteresseerde lezer wordt een uitgebreid aanbevolen: R. Panko; 2005; Datanetwerken en telecommunicatie; Pearson Education; vijfde editie; blz. 274.

Hoofdstuk 2 “Decentralization and Local Government Strengthening Program”

2.1 Algemeen

Zoals in de inleiding is aangegeven kunnen maatschappelijke problemen in Suriname niet worden opgelost door de overheid alleen. Iedereen zal daarom naar vermogen en draagkracht hiertoe moeten bijdragen. Dit is de directe aanleiding tot decentralisatie. Het Decentralisatieprogramma (DLGP), uitgevoerd binnen het ministerie van Regionale Ontwikkeling met ondersteuning van de IDB, heeft tot doel financiële zelfstandigheid te verlenen aan de districten in Suriname. Het decentralisatieprogramma (DLGP) bestaat uit twee fasen, namelijk (B. Ahmadali, 2005: 8):

- DLGP-1; in het DLGP-1 ging het erom de districten Wanica, Para, Nickerie, Commewijne en Marowijne te certificeren. Deze districten zijn reeds gedecentraliseerd;
- DLGP-2: het DLGP-2 dat logisch aansluit op DLGP-1, is in maart 2009 aangevangen voor de duur van 5 jaar. Met behulp van het DLGP-2 programma worden de districtsoverheden van de districten Paramaribo, Sipaliwini, Coronie, Saramacca en Brokopondo evenals voorgaande districten versterkt om zodoende een zelfstandig begrotings- en financieel beheer te voeren.

Om het doel op zo goed mogelijke wijze te bereiken, is het programma onderverdeeld in de volgende componenten, namelijk (B. Ahmadali, 2005: 9):

- wettelijke hervormingen;
- budget en financieel management;
- inkomstengenerering;
- bevolkingsparticipatie;
- civiele werken.

Alhoewel DLGP uit de bovengenoemde componenten bestaat, zal ik met name component budget en financieel management belichten, omdat deze het meest relevant is voor mijn probleemstelling. Het doel van component budget en financieel management is een kern van stelsels in de districten te ontwikkelen, zodat deze hun eigen budget en financieel systeem

beheren. De kern van stelsels die ingericht zal worden in de districten omvat: 1. administratie en planning, 2. begroting en financieel beheer, 3. districtsinkomsten genereren.
Het programma biedt ondersteuning aan de districten op de volgende gebieden (B. Ahmadali, 2007: 25):

- opbouwen van capaciteit voor betrouwbare administratie en audit-mogelijkheden gericht op het versterken van de financiële positie van het district;
- installatie van een ICT-netwerk dat de districten moet verbinden met zowel het Ministerie van Financiën als het Ministerie van Regionale Ontwikkeling ter bevordering van de onderlinge communicatie tussen diverse overheidsinstellingen onderling en overheid en burger, overheid en particulieren sector;
- training, aanschaf van apparatuur en meubilair, herstructureren van het strategisch plan van het Ministerie, het treffen van communicatie en mediafaciliteiten voor het hoofdkantoor, de rehabilitatie van het hoofdkantoor.

2.2 Local Area Network (LAN) binnen DLGP

Een belangrijk doel van het DLGP-1-programma is geweest om bepaalde financiële bevoegdheden van de centrale overheid over te dragen aan de districten. Om deze bevoegdheden correct te kunnen uitvoeren, was het noodzakelijk een bepaalde mate van automatisering door te voeren in de districten, zoals:

- *toegang tot email:* bij de start van de implementatie in 2003 had geen van de pilot districten toegang tot internet. De Project Implementation Unit (PIU) heeft op elke locatie een interne mailserver geïnstalleerd, waardoor de interne communicatie een heel stuk werd verbeterd. De Districts-Administrateurs hadden (en hebben) via een inbelnummer van Telesur toegang tot hun e-mails. In Wanica, Paramaribo en Sipaliwini is er een ADSL-aansluiting; daar hebben meerdere personeelsleden van de Afdeling Districts Financiën en Planning (DFP) en het Bevolkings Informatie Centrum (BIC) internettoegang. DFP, zorgt voor planning, districtsinkomsten en uitgaven. De afdeling BIC is belast met de uitwisseling van informatie tussen burger en bestuur;
- *een LAN-netwerk per district:* hierop staan per locatie minimaal 4 computers aangesloten, namelijk de pc’s van de kassier, de "Budget and Financial Management (BFM)-unit", de

BIC-unit en de Districts-Administrateur. Per eind juni 2010 zullen de commissariaten van Wanica, Para, Nickerie, Commewijne en Marowijne via een WAN worden gekoppeld aan het hoofdkantoor te Combé. Vermeld dient te worden dat er in de districten (met uitzondering van Wanica) geen personeel met afdoende kennis van ICT aanwezig is;

- *financiële software:* voor de DFP units is AccountView aangeschaft en geleverd door Integrated Computer Service. Bij het leveren is ook een training verzorgd voor de gebruikers. AccountView financiële software draait lokaal in de vijf gecertificeerde districten. De bedoeling is dat op de hoofdlocatie ook AccountView draait; op dagbasis wordt dan via het WAN gesynchroniseerd vanuit de districten naar de hoofdlocatie, onder andere zodat zaken als interne controle makkelijk op de hoofdlocatie kunnen plaatsvinden. Het Alfresco Document Management Systeem zal lokaal op alle locaties draaien en niet centraal. Het Alfresco Document Management Systeem is een open source document management systeem waarmee eenvoudig documenten kunnen worden opgeslagen, gevonden en gedeeld; en
- *een database*: Business & Data Solutions heeft een database ontwikkeld waarin de BIC-units van de districten informatie kunnen verwerken (winkels, scholen, enzovoorts). Het is de bedoeling dat deze database op korte termijn via het op te zetten DLGP WAN netwerk wordt verbonden aan een centrale database, zodat de informatie via het internet kan worden opgevraagd. De database is door Business & Data Solutions ook omgezet van Microsoft SQL naar MySQL vanwege het open source-beleid van DLGP. MySQL is een database programma waarmee grote hoeveelheden data op de webserver kunnen worden bewaard en gemanipuleerd.

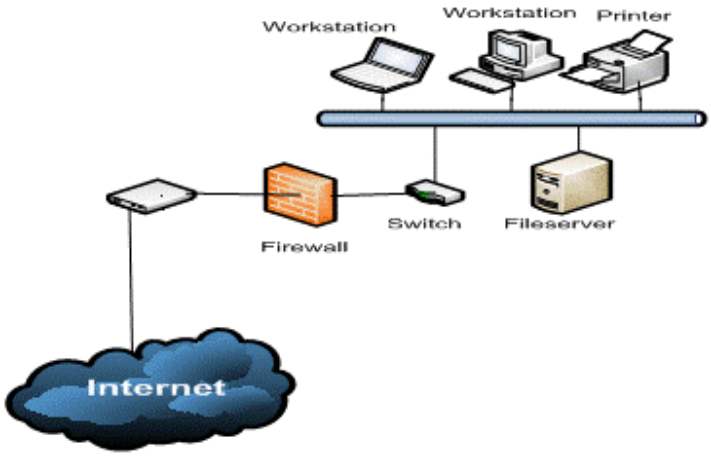
Eisen voor de technische infrastructuur (LAN) binnen DLGP:

- een plaatselijk netwerk met minimaal 4 computers;
- verbinding tot het centrale DLGP-netwerk door gebruik te maken van een stabiele internetverbinding;
- een gateway om een snelle toegang tot een ander netwerk te garanderen;
- een firewall om bescherming van het netwerk tegen bijvoorbeeld hackers vanuit het internet te garanderen;

- een plaatselijke server voor: het delen en opslaan van gegevens, het samendelen van de printer;
- user accounts voor de plaatselijke netwerkgebruikers, back-up;
- randapparatuur (zoals modem, switch enzovoorts).

Zie figuur 1 voor het LAN per district.

Figuur 1 LAN van een district



(Bron: R. Ahmadali; 2009; Het DLGP ICT component terugblik & toekomstvisie; blz. 26)

2.3 Huidige DLGP Wide Area Network

Een nieuwe fase binnen het DLGP is het verbinden van al deze lokale netwerken met elkaar, dus het opzetten van een WAN-netwerk. De technologie die hiermee gepaard gaat, is in Suriname slechts binnen enkele bedrijven geïmplementeerd en zeker binnen de Overheid is het aanleggen van een WAN-netwerk een nieuwe ontwikkeling. Vandaar dat er diverse studies zijn uitgevoerd binnen het DLGP, alvorens daadwerkelijk het WAN-netwerk op te zetten (R. Ahmadali; 2009:3).

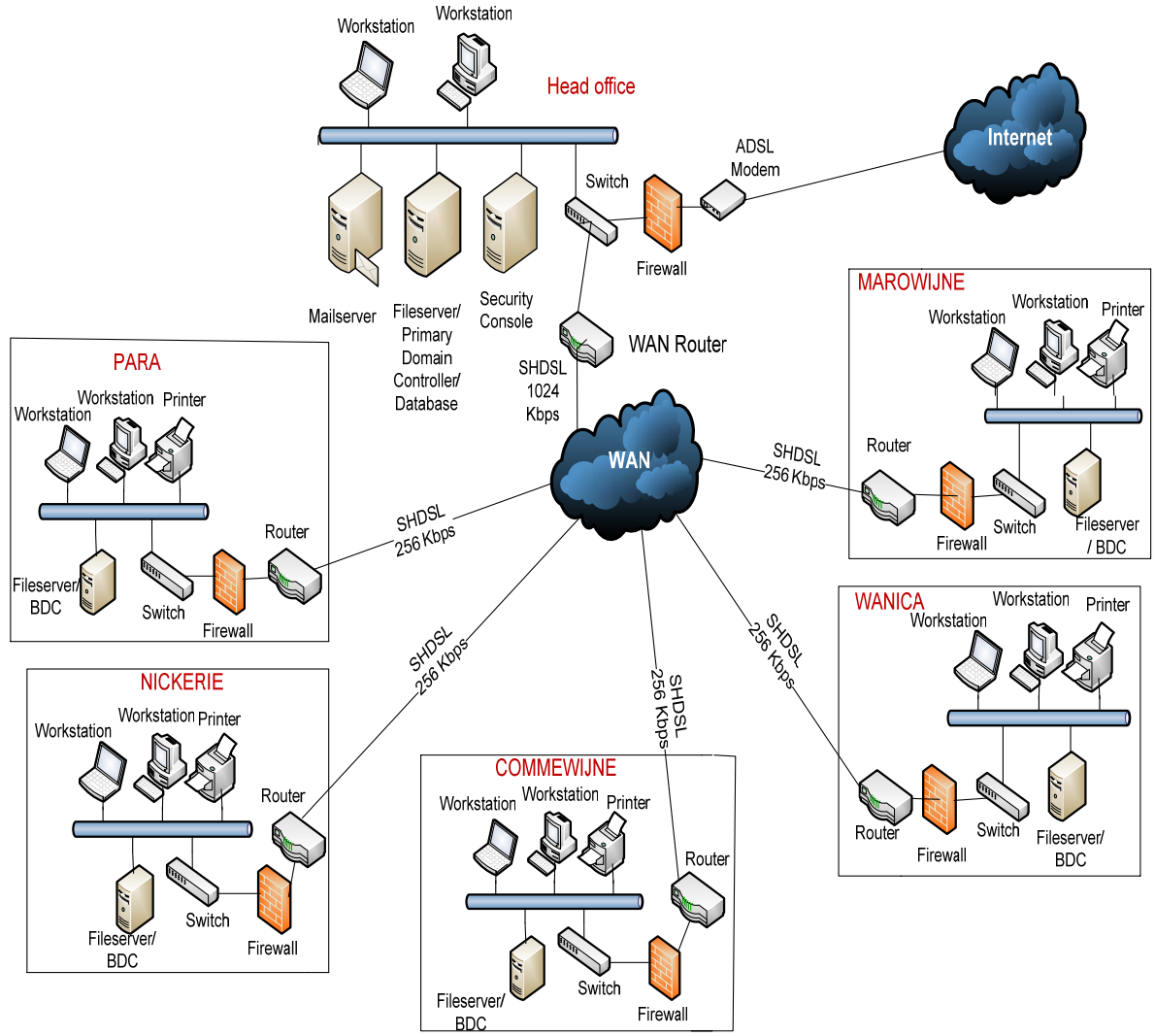
Deze studies zijn (R. Ahmadali; 2009:3):

- voorstudie door ITEE N.V.: in deze studie is de hele opzet van het WAN netwerk beschreven voor de vijf pilot districten. Benodigde leaselines, hardware en software overzicht, netwerk configuratie, licenties, enzovoorts;
- electrical assessment: deze studie, uitgevoerd door Advanced Management of Power Systems (AMPS), had tot doel de kwaliteit van de elektriciteitsvoorziening op de commissariaten van de vijf-pilot districten te beoordelen en aanbevelingen te doen tot verbetering. Dit was noodzakelijk, zodat op een duurzame wijze de WAN-apparatuur kan worden geplaatst in de districten;
- platformstudie: het doel van deze studie, uitgevoerd door ir. Achmed Neijhorst, was om na te gaan of het kostentechnisch voordeliger is om onder het welbekende Windows platform het WAN-netwerk op te zetten, ofwel over te schakelen naar het Linux platform, dat bekend staat om zijn stabiliteit en lage licentiekosten. Op grond van deze studie is besloten om het gebruik van open source software te stimuleren;
- upgrading netwerk ministerie van Regionale Ontwikkeling: vooruitlopend op de aansluiting naar de WAN-centrale, heeft een ICT-consultant binnen het ministerie van Regionale Ontwikkeling het lokale netwerk grondig gereviseerd en personeel getraind hoe met de vernieuwingen om te gaan.

Het Wide Area Network dat is opgezet in de districtskantoren van Wanica, Para, Nickerie, Marowijne en Commewijne is noodzakelijk om uitvoering te geven aan de nieuwe vorm van overheidsbeleid, namelijk e-government. Het WAN zal gebruikt worden voor:

- voor een centrale emailserver voor alle sites;
- voor een document management en routing systeem op alle locaties;
- bestaande lokale databases waarbij district-informatie zal worden gehost op de centrale server, zodat het toegankelijk zal zijn vanuit het internet;
- de financiële controle van de districten, die zal worden gedaan vanuit het centrale kantoor via het WAN;
- voor centraal en beveiligde internet voor alle locaties.

Figuur 2 huidige WAN-systeem



(Bron: R. Ahmadali; 2009; de DLGP ICT component terugblik & toekomstvisie; blz. 21)

Met de inzet van het WAN streeft het ministerie van Regionale Ontwikkeling ernaar om effectiviteit en efficiëntie te bereiken door het delen van applicaties, informatie systemen en uitwisselen gegevens tussen het DLGP-hoofdkantoor in Paramaribo en de pilot-districten Wanica, Para, Nickerie, Commewijne en Marowijne, en in een later stadium ook de overige districten (Itee NV; 2008: 3).

Centraal draait er:

- MySQL-database op centrale server te Combe; locaties (de districten) werken rechtstreeks daarop via een web-interface;

- zimbra mailserver centraal op Combe; alle locaties hebben toegang daartoe via Thunderbird email cliënt of webinterface.

Toekomstige situatie: belastingsoftware is nu in de fase van voorstudie; er zal een web interface worden gebouwd, zodat vanuit de districten belastingen kunnen worden geïnd ten behoeve van de Belastingdienst, en de betaling kan op elke gewenste locatie plaatsvinden, ongeacht voor welk district wordt betaald.

De Domain Controller, Mail Server, Security Management Console en Firewall server zal worden geïnstalleerd bij de DLGP Head Office. Wij stellen daarom voor de installatie van 4 servers, elk met de volgende doeleinden (Itee NV; 2008: 15):

- server 1: Domain Controller / file server / Print server / database server. De Domein Controller bedient alle DLGP-gebruikers, terwijl de andere functionaliteiten vooral zijn voorbehouden voor de gebruikers op het hoofdkantoor;
- server 2: mail server. De mailserver bedient alle DLGP-gebruikers.
- server 3: firewall & Security Console. Deze server regelt internettoegang voor alle DLGP-gebruikers en is ook de centrale coördinatie die oplossing moet bieden in alle probleem die worden gesignaleerd in de DLGP locaties;
- server 4: deze server is een reserve server die snel kan worden ingezet in het geval dat een van de andere servers uitvalt. Deze strategie biedt een kosteneffectieve minimalisering van de downtime.

Alle servers zijn identiek, zorgen voor uniformiteit en voor hardware en software-compatibiliteit.

Zoals eerder gezegd zal de interne controle van de districten gedaan worden vanuit het centrale kantoor van het WAN. Voor het uitoefen van adequaat interne controle moeten de eisen van interne controle in relatie gebracht worden met het WAN-systeem. Het is daarom noodzakelijk om vast te stellen aan welke criteria het WAN moet voldoen. In het volgende hoofdstuk zal worden ingegaan welke de criteria zijn en waaraan het WAN systeem moet voldoen om een gedegen interne controle uit te voeren.

Hoofdstuk 3 De interne controle criteria en voorstellen toe te passen maatregelen met betrekking tot een effectieve WAN systeem

3.1 Algemeen

Na het afwegen van de kosten en baten heeft het DLGP gemeend om een afdeling interne controle ten behoeve van alle districten op te zetten met dien verstaande dat elk district afzonderlijk zal worden gecontroleerd en de informatie daarvan ook afzonderlijk zal worden gepresenteerd aan het desbetreffende district. Deze interne controle unit zal rechtstreeks onder de District Administrateurs en de Districts-Commissarissen ressorteren. De Districts-Commissarissen hebben informatie over het algemeen management nodig ten behoeve van het districtsbeleid, terwijl de District Administrateurs specifieke financiële informatie nodig hebben. Gegevens per district moeten alleen voor het desbetreffende district op confidentiële en geautoriseerde basis geproduceerd worden door de geautomatiseerde unit van interne controle.

Voordelen van de centraal geautomatiseerde afdeling interne controle binnen het DLGP zijn:

- minder personeel nodig voor het verrichten van interne controle taken;
- de medewerkers hoeven zich niet dagelijks te verplaatsen naar de districten;
- automatisering van het administratieproces gaat gepaard met verregaande standaardisatie van berichten; er is dus landelijk sprake van een uniforme werkwijze;
- het is eenvoudig om de uitgaven en inkomsten na te trekken;
- door lagere "handlingkosten" en lagere verzendkosten (netwerkkosten in plaats van portokosten) zullen de kosten voor het berichtenverkeer aanzienlijk lager en sneller zijn;
- het binnenkomende elektronische berichtenverkeer biedt de mogelijkheid om in de toekomst de binnenkomende berichten elektronisch te verwerken (het "paperless office");
- tijd die de postverzorging en -bezorging nu in beslag neemt, wordt weggenomen. Dit zal voordelen hebben vooral bij spoedeisende zaken.

3.2 Criteria voor de Interne Controle en maatregelen met betrekking tot een effectief WAN-systeem

In de voorgaande hoofdstukken is reeds verwoord dat het WAN-systeem als medium zal dienen voor en tussen de districten en het ministerie van Regionale Ontwikkeling. Een systeem van interne controle onder beheer van een daarvoor bestemde unit zal worden aangesloten op het WAN vanwaaruit de belangrijke geautomatiseerde functies gecontroleerd zullen worden. Voor het opzetten van de unit voor de interne controle in het kader van het DLGP zijn er heel wat criteria die in relatie gebracht moeten worden met een geautomatiseerd systeem zoals het WAN.

Zoals in hoofdstuk 1 vermeld, is een geautomatiseerd systeem opgebouwd uit vele elementen, waarvan de belangrijkste zijn:

- een applicatie met eventuele koppelingen naar andere applicaties;
- de bijbehorende handmatige procedures met opgeleide gegevensleveranciers;
- de geconverteerde gegevens;
- een technische infrastructuur (computers, netwerken, enzovoorts);
- opgeleide gebruikers;
- een (functionele) organisatie gericht op het in bedrijf houden van de technische infrastructuur (productieorganisatie, ook wel aangeduid als computer- of rekencentrum);
- een (functionele) organisatie om het onderhoud van het systeem te ondersteunen;
- documentatie voor de gebruikers, de onderhoudsorganisatie en de productie- organisatie.

Van de in hoofdstuk 1 genoemde beoordelingscriteria inzake de integratie van de taken van de interne controle in een informatie systeem zijn de belangrijkste als volgt:

- management;
- beveiliging;
- onderhoud en beheer;
- effectiviteit;
- tijdigheid en vorm van de informatie;
- betrouwbaarheid;

- autoriteit;
- procedures.

-

Tabel 1 Deze criteria zijn hieronder in de tabel in relatie gebracht met de interne controle en de daarbij te treffen maatregel.

Criteria	**Maatregelen**
Criterium: management. Het WAN systeem moet onder het beheer zijn van de leiding van de districten. Toelichting: De unit van interne controle moet rechtstreeks vallen onder de Districts Administrateurs en Districts-Commissarissen (leiding). *Relatie met de interne controle*: interne controle is controle op de oordeelsvorming en de activiteiten van anderen, voorzover de controle ten behoeve van de betrokken huishouding door of namens die leiding wordt uitgeoefend; daarom moet worden voldaan aan dit criterium.	Functionele organisatie (Zie uitleg paragraaf 1.8)
Criterium: autoriteit en verantwoordelijkheid. Deze dienen duidelijk gescheiden te zijn van de tussen de verschillende overige functies. Toelichting: Er moet duidelijk een functiescheiding zijn tussen systeemontwikkeling en systeembeheer en tussen de automatiseringsfunctie en de gebruikersomgeving. *Relatie met interne controle:* als iemand belast is met twee of meer naar hun aard verschillende functies is de controle op de juistheid van de verantwoordingen is dan niet meer mogelijk. Bijvoorbeeld: elke persoon die onbelemmerde toegang heeft tot de computer, heeft de mogelijkheid heeft om fraude te plegen die niet (zo vlug) aan het licht zal komen.	Functionele organisatie (Zie uitleg paragraaf 1.8)
Criterium: onderhoud en beheerafdeling. Er moet een afdeling onderhoud en beheer zijn, die ervoor moet zorgen dat continuïteit, performance en beschikbaarheid van de ICT-infrastructuur gegarandeerd zijn. Toelichting: Onderhoud van een applicatie houdt in het oplossen van fouten en het	Change management (Zie uitleg paragraaf 1.8)

implementeren van gewenste wijzigingen in het programma. *Relatie met interne controle*: Dit criterium is noodzakelijk omdat de interne controle niet kan steunen op een software-pakket waarmee de administratie werkt, als dat pakket fouten heeft.	
Criterium: de fysieke bekwaamheid om computerapparatuur te gebruiken, moet beperkt zijn. Toelichting: De afdeling interne controle moet weten waar elke computers staan en dient te zien dat de computerapparatuur in afgesloten ruimten opgeborgen wordt. Alleen personeel dat gemachtigd is, moet toegang verkrijgen. *Relatie met interne controle:* door de computers in een afgesloten ruimte te plaatsen; bevordert de interne controle ten eerste de functiescheiding en ten tweede ook de bescherming van de informatie tegen diefstal, brand enzovoorts.	Fysieke beveiliging (Zie uitleg paragraaf 1.8)
Criterium: functiescheiding middels programmatuur. Toelichting: Het moet mogelijk zijn om autorisaties te configureren voor een gebruiker of gebruikersgroep, waarbij deze rechten heeft om een bepaalde functionaliteit binnen het systeem (invoeren, raadplegen, wijzigen, verwerking, rapportages maken) op te roepen. Toegangsbeveiliging moet geregeld worden tot op het niveau van menu en record. Toegangsbeveiliging wordt normaliter geregeld in een competentietabel. Beperkte logische toegang tot het systeem betekent dat een systeem een mogelijkheid heeft om een onderscheid te maken tussen gemachtigde en niet-gemachtigde gebruikers. Autorisatie dient op documentniveau geregeld te zijn. *Relatie met interne controle:* de functiescheidingen komen in het WAN door middel hiervan tot stand.	Logische toegang beveiliging (Zie uitleg paragraaf 1.8)
Criterium: beveiligen van het WAN-systeem. Een ander belangrijk criterium dat binnen het DLGP onmisbaar is, is het beveiligen van het WAN. Toelichting: De ontwikkeling van een strategie met betrekking tot de interne controle voor pc's begint bij het inventariseren van alle pc's en het in kaart brengen waarvoor zij gebruikt worden. Elke pc zal geclassificeerd dienen te worden, afhankelijk	Netwerk beveiliging (Zie uitleg paragraaf 1.9)

van de risico's verbonden met de applicaties. Bijvoorbeeld: een pc die gebruikt wordt voor het bijhouden van de ontvangsten en het voorbereiden van betalingen, staat bloot aan meer risico's dan een pc die gebruikt wordt voor tekstverwerking. *Relatie met interne controle:* de informatie is een strategisch middel. Het is dus een absolute noodzaak om deze informatie goed te beveiligen. Op de informatie gaat interne controle worden uitgeoefend, daarom moet het netwerk goed beveiligd worden, zodat onbevoegden er niet in kunnen komen.	
Criteruim: beveiliging van gegevensbestanden en programmatuur. Toelichting: Ter ondersteuning van standaardapplicaties is altijd ondersteunende software aanwezig. De belangrijkste functie hiervan is om de informatiesystemen te beheersen en verder te beveiligen. *Relatie met interne controle:* dit criterium is niet weg te denken binnen het DLGP, omdat er geen interne controle zal kunnen plaatsvinden als er schade wordt aangericht aan de programmatuur en gegevensbestanden.	Antivirus en firewall (Ondersteunende applicaties) (Zie uitleg paragraaf 1.7)
Criteruim: continuïteit van gegevensbestanden. Toelichting: Op het gebied van de beveiliging tegen calamiteiten (back-up en recovery) dienen maatregelen te worden getroffen, zodanig dat, in het geval van vernietiging of beschadiging van gegevens en/of programmatuur, de gegevensverwerking op aanvaardbare wijze kan worden voortgezet. Met betrekking tot uitwijkregelingen dienen maatregelen te worden getroffen zodanig dat, in het geval van vernietiging of beschadiging van apparatuur en/of gebouwen, de gegevensverwerking op aanvaardbare wijze kan worden voortgezet. De data die met behulp van de applicatie wordt beheerd, moet via het back- up en recovery mechanisme worden beheerd. Mocht er verlies van data optreden, dan moet dit via het restore-mechanisme worden hersteld. Het programma dient overweg te kunnen met de herstelde data. Er moeten dagelijks back-ups gemaakt worden. Back-ups mogen niet bewaard worden bij de mainframe (daar waar data wordt ingevoerd en verwerkt). Ook moeten back-ups moeten beveiligd worden tegen brand en waterschade. Verder dient de regelmatig recovery (herstel) regelmatig te worden getest om te kijken of die	Back-up, recovery en uitwijkprocedures (Zie uitleg paragraaf 1.8)

werkt. *Relatie met interne controle:* in geval van schade moet er interne controle verricht worden met de data die als back-up is vastgelegd.	
Criterium: het bestaan van documentatie-procedures en normen. Toelichting: Documentatie moet actueel gehouden worden. Goed geplande en duidelijk voorgeschreven documentatienormen bieden de volgende voordelen: - het vergemakkelijken van de communicatie; - het gebruik als een verwijzing en trainingsmiddel voor systeemgebruikers en voor nieuwe werknemers die in dienst komen; - het vergemakkelijken van onderhoud van de programma's; - het reduceren van problemen indien onverhoopt een werknemer van baan verandert. Bijvoorbeeld: als een werknemer halverwege een belangrijk project met ontslag gaat, kan veel tijd verspild worden met pogingen om het werk te continueren indien geactualiseerde documentatie niet voorhanden is. *Relatie met interne controle:* documentatie beschrijft de normen en procedures hoe gegevens verwerkt dienen te worden. Controle is het toetsen van de werkelijkheid aan de vastgestelde norm; daarom moet dit criterium ook geïmplementeerd worden.	Documentatie (Zie uitleg paragraaf 1.8)
Criterium: diverse controles uitvoeren met programmatuur. Toelichting: Het geautomatiseerde systeem moet voorzien in ingebouwde systeemcontroles, zoals bestaanbaarheidscontroles, redelijkheidscontroles en controles op de doorlopende nummering. Logbestanden: de applicatie moet in staat zijn om logbestanden te genereren, waardoor eventuele problemen meer specialistisch kunnen worden geanalyseerd. De autorisatie van de log-gegevens moeten zodanig zijn, dat deze nooit kunnen worden gewijzigd. Ten behoeve van de traceerbaarheid moet elke mutatie van gegevens (administratie) worden opgebouwd in de programma-historie. Hierbij moet de vermelding van de persoon die de wijziging aangebracht heeft, bewaard worden. *Relatie met interne controle:* deze controle-middelen en controle-technieken	Systeemcontroles (Zie uitleg paragraaf 1.8)

zijn opgenomen in hardware en software pakketten.	
Criterium: de applicatie moet in staat zijn management-rapportages te genereren. Toelichting: De applicatie dient de mogelijkheden te bieden om op een eenvoudige wijze management-informatie te genereren in de vorm van rapportages, en rapport-gegevens te exporteren naar diverse standaardformaten.	
Criterium: handmatige controles uitoefenen. Toelichting: Deze handmatige controles zullen uitgeoefend moeten worden (buiten automatisering om ter controle van input - output), bijvoorbeeld: - aansluitingen; - cijferanalyse; - controlerende tussenrekeningen; - controle met documenten; - vergelijken van interne gegevens met externe informatie; - kasopnames. *Relatie met interne controle:* de handmatige controles vinden plaats zowel in een manueel als in een geautomatiseerd systeem plaats. Interne controle steunt sterk op handmatige controles, Bijvoorbeeld bij cijferanalyse als blijkt dat er een groot verschil is met de vorige periode.	Gebruikers-controle (Zie uitleg paragraaf 1.8)
Criterium: minimaliseren van de tijd dat het systeem plat ligt. Toelichting: Storingen in de hardware of software kunnen ervoor zorgen dat het WAN systeem uitvalt. De primaire activiteiten binnen het DLGP kunnen dan niet worden ondersteund.	Fysieke beveiliging (Zie uitleg paragraaf 1.8)
Criterium: er dient gekwalificeerd personeel aangetrokken te worden. Het WAN-systeem biedt de mogelijkheden om controle effectiever en efficiënter uit te voeren. Om met zo'n geautomatiseerd systeem te werken moet er personeel aangetrokken worden dat is opgeleid en verder ook nog aanvullende kennis en ervaring heeft. Relatie met interne controle: interne controle geschiedt door	Opgeleid personeel

medewerkers van de eigen organisatie.	

(**Bron**: eigen onderzoek)

Deze zijn de belangrijkste criteria voor de opzet van de WAN interne controle-unit

Conclusies en Aanbevelingen

Conclusies

Op basis van de geformuleerde probleemstelling kan de conclusie worden getrokken dat het kiezen van een geautomatiseerd systeem als WAN ten behoeve van de interne controle afhankelijk is van de criteria management, autorisatie, onderhoud en beheer, fysieke bekwaamheid, functiescheiding, beveiliging, applicatie, efficiëntie, documentatie- processen en kwalificaties.
Een multi-toepasbaar pakket aan criteria en maatregelen met betrekking tot het WAN ten behoeve van interne controletaken wordt aangeraden. In ons huidig informatie tijdperk kan de rol van de interne controle vergemakkelijkt worden door het WAN, wat voor efficiëntie en tijdige bijsturing kan zorgen.

Aanbevelingen

Op basis van de geformuleerde probleemstelling, de realisaties van het DLGP en in het bijzonder de doelstelling van het DLGP blijkt dat het aspect interne controle nader uitgewerkt c.q. toegepast dient te worden. De samenwerking tussen de districten dient onder andere middels de interne controle-unit middels het WAN-systeem gestalte te krijgen en kostenbesparend en efficiëntie- verhogend op te treden. Hierbij is als belangrijk onderdeel van het geautomatiseerd informatiesysteem (WAN) een adequaat interne controle-systeem onmisbaar. Als onderzoeksresultaat zijn uit dit onderzoek de criteria die geselecteerd zijn voor de opzet van de interne controle-unit middels WAN voortgevloeid. Dit is opgenomen in hoofdstuk 3 van deze thesis. In dit hoofdstuk is breedvoerig ingegaan op de criteria die in relatie met interne controle moeten worden aan- gebracht. De in dit hoofdstuk genoemde te treffen criteria en maatregelen worden daarom ook als een aanbeveling aan de PIU van het DLGP beschouwd.

Samenvatting

Sinds de opkomst van de automatisering hebben organisaties een duidelijke ontwikkeling doorgemaakt. Enerzijds heeft deze ontwikkeling te maken met de voortdurende groei van de mogelijkheden van automatisering, zowel op het gebied van hardware (snelheid, capaciteit van computers), software (toepassingen op steeds meer functionele gebieden met steeds betere functionaliteit) of verbindingen (internet). Maatschappelijke problemen in Suriname kunnen niet door de overheid alleen worden opgelost. Iedereen zal daaraan naar vermogen en draagkracht moeten bijdragen. Dit betekent dat burgers meer zelf de verantwoordelijkheid moeten nemen Dit gegeven is de directe aanleiding tot decentralisatie. In hoofdstuk 1 worden de theoretische grondslagen van interne controle en Wide Area Network (WAN) belicht.
In hoofdstuk 2 wordt er aandacht besteed aan het DLGP. De component die relevant is voor deze thesis wordt in dit hoofdstuk beschreven.
In hoofdstuk 3 komen aan de orde de criteria en maatregelen voor het selecteren van een effectief automatiseringssysteem.
Tenslotte komen de conclusies en aanbevelingen aan de orde
Het onderzoek heeft zich gericht op het beantwoorden van de volgende probleemstelling:
"Welke zijn de criteria voor het selecteren van een systeem voor het verrichten van interne controle taken?". Om antwoord te kunnen geven op de probleemstelling zijn de criteria die nodig zijn voor het verrichten van interne controle taken in relatie gebracht met het WAN.

Het WAN-systeem zal als medium dienen voor en tussen de districten en het ministerie van Regionale Ontwikkeling. Een intern controle-systeem onder beheer van een interne controle unit zal worden aangesloten op het WAN van waaruit de belangrijke geautomatiseerde functies gecontroleerd zullen worden. Het kiezen van een geautomatiseerd systeem als het WAN ten behoeve van de interne controle is afhankelijk van de criteria management, autorisatie, onderhouden en beheer, fysieke bekwaamheid, functiescheiding, beveiliging, applicatie, efficiëntie, documentatie-processen en kwalificaties. Een multi-toepasbaar pakket aan criteria en maatregelen met betrekking tot het WAN ten behoeve van interne controle taken is aangeraden. In dit informatietijdperk kan de rol van de interne controle vergemakkelijkt worden door het WAN, wat voor efficiëntie en tijdige bijsturing kan zorgen.

Hiertoe is als belangrijk onderdeel van het geautomatiseerd informatiesysteem (WAN) een adequaat interne controlesysteem onmisbaar. Als onderzoeksresultaat zijn uit dit onderzoek de criteria die geselecteerd zijn voor de opzet van de interne controle unit middels WAN, voortgevloeid.

Begrippenlijst

Browser	Software die wordt gebruikt om over het Word Wide Web te surfen.
Cliënt	Een computer die is aangesloten op een netwerk en gebruik maakt van de beschikbare bronnen op de server.
Communicatie	Omvat de regels ten aanzien van de manier waarop computers praten en elkaar begrijpen. Omdat computers vaak verschillende software hebben draaien, moeten ze om met elkaar te communiceren dezelfde taal spreken. Zonder gedeelde communicatie kunnen computers geen informatie uitwisselen en blijven ze geïsoleerd.
Domeincontroller	Een domeincontroller is een server in een computernetwerk van Microsoft Windows die centraal beheert wie er toegang tot welke stukken van het domein mag hebben.
Gateway	Een gateway is een toegangspoort, een koppeling tussen verschillende computernetwerken. Het is meestal een computer die fungeert als vertaler tussen twee totaal verschillende systemen.
Gegeven	Een gegeven is een voorstelling van een feit of idee in een in een zodanige vorm- namelijk in de vorm van signalen -dat deze door een proces kan worden bewaard, verplaatst of bewerkt.
Informatie	Informatie is datgene wat het bewustzijn van de mens bereikt en bijdraagt tot zijn kennisbeeld.
Mailserver	Een mailserver is een server die verantwoordelijk is voor het verwerken van e-mails.
Services:	Een service bestaat uit alles wat een computer deelt met de rest van het netwerk. Een computer kan bijvoorbeeld een printer of bepaalde directory's of bestanden delen.

Internet	Een systeem dat computernetwerken over de hele wereld koppelt.
Internet Protocol	Het protocol dat wordt gebruikt om te definiëren hoe gegevens over het internet worden getransporteerd.
LAN	Een LAN is een netwerk dat een korte, beperkte afstand overbrugt (zoals een gebouw) en waarin computers informatie en bronnen kunnen delen.
Netwerk	Een groep computers die aan elkaar is gekoppeld zodat deze gegevens en bronnen kunnen delen.
Netwerkkaart	Een netwerkkaart is uitbreidingskaart die een computer koppelt aan een stel andere computers, zodat ze toegang hebben tot informatie en programma's.
Protocol	Een set regels die het gegevensverkeer regelen. Het formaat dat wordt gebruikt om bestanden te uploaden of downloaden, zodat twee verschillende computers in een standaardformaat kunnen communiceren.
Randapparatuur	Een extern apparaat dat aan een computer is gekoppeld, zoals een printer, een scanner of een modem.
Router	Een apparaat dat werkt als een brug, maar in staat is de beste route tussen netwerken te selecteren op basis van de verkeersdrukte. Een router kan ook twee verschillende netwerken koppelen.
Server	De computer waarop het netwerkbesturingssysteem draait, dat de beveiliging regelt en de toegang tot bronnen beheert. Strikt genomen is het elke computer die informatie opslaat en andere gebruikers toestaat kopieën op te halen van die informatie.
Software	Elk programma (of elke set opdrachten) dat ervoor zorgt dat de computer een taak of een functie uitvoert.
WAN	Een netwerk dat een groot geografisch gebied beslaat. Het netwerk is gekoppeld via telefoonlijnen, ISDN-lijnen (Integrated

Services Digital Network), DSL, kabel, radiogolven of satellieten.

Bronvermelding

Primaire bronnen:

1. Beek A., Meuwissen R.H.G. en Vaassen E.H.J, 2003, Hoofdlijnen Bestuurlijke informatievoorziening, Wolters-Noordhoff b.v, Groningen/Houten, vierde druk.
2. Casad J., 2001, TCP/IP in 24 uur, Pearson Education, tweede druk.
3. Gupta M., Lasalle M., Leitzke C., Parihar M. en Scrimger, R., 2002; TCP/IP het complete handboek, Academic Service.
4. Jans E.O.J., 1999, Grondslagen administratieve organisatie, Samson, 17 druk.
5. Maiwald E., 2001, Netwerk beveiliging, Academic Service, eerste druk.
6. Microsoft Corporation, 2001, A+ certificering training kit, Academic Service, derde editie.
7. Oonincx J.A.M. en Pruijn R.A.M., 1990, Interne Controle bij systemen voor automatische informatieverzorging, Samsom, eerste druk.
8. Panko R., 2005, Datanetwerken en telecommunicatie, Pearson Education, vijfde editie.
9. Starreveld R. W., van Leeuwen O.C. en van Nimwegen H., 2002, Bestuurlijke informatieverzorging deel 1: Algemene Grondslagen, Stenfert Kroese, Groningen/ Houten, vijfde druk.
10. Starreveld R.W., van Leeuwen O.C. en van Nimwegen H., 2007, "Bestuurlijke informatieverzorging deel 2B, toepassingen: Typologie van de bedrijfshuishoudingen, Wolters-Noordhoff, Groningen/ Houten, vijfde druk.
11. Westra B. A. J. en Mooijekind M. J. Th, 2002, Compendium van de Accountantscontrole deel 1, Pentagan BV, Ede, derde druk.

Secundaire bronnen

1. Ahmadali B., 1999, Financiële decentralisatie en versterking van het districtsbestuur in Suriname.
2. Ahmadali B., 1999; Leidraad Decentralisatie 2003-2006.
3. Ahmadali B.; 2007; " DLGP Eindrapport 2007".
4. Ahmadali R.; 2009; "Het DLGP ICT component terugblik & toekomstvisie".

5. Itee NV; 2008; "Implementing a Wide Area Network within the framework of the Decentralization and Local Government Strengthening Program".

Interviews

1. De heer drs. Pershad Mahender, taskmanager Districtsinkomsten en Uitgaven binnen het DLGP;
2. De heer Ahmadali Riaz, DLGP ICT manager binnen het DLGP.