in dit verband in het tweede deel van zijn verslag op te nemen. Een dergelijke vermelding zal vermeden worden wanneer de administratieve organisatie, met inbegrip van de interne controlemechanismen, als aangepast aan de aard en de omvang van het bedrijf wordt geacht." (Wijziging, IBR-Jaarverslag 1997, *p.* 363.)

Ook in een kleine of middelgrote onderneming kan de revisor de voorafgaande fase van zijn controleopdracht afronden met het besluit dat de controleomgeving en de organisatie van het boekhoudkundig systeem voldoende zijn om hem onder normale omstandigheden zijn opdracht te laten uitoefenen.

8. Het controleverslag

Paragraaf 3.3.7., eerste lid van de Algemene controlenormen stelt: "Indien de interne controle belangrijke tekortkomingen vertoont, en indien de revisor geen genoegen heeft kunnen nemen met alternatieve controleprocedures, zal hij in zijn verslag vermelden in welke onderdelen van de organisatie deze leemte voorkomen en welke rubrieken door deze leemtes een aanzienlijk risico lopen. Daaruit zal een voorbehoud (3.7.2.) of een onthoudende verklaring (3.8.1.) voortvloeien, naargelang het geval." (Wijziging, Jaarverslag 1997, *p.* 363.)

De verwijzing naar een betekenisvolle leemte in het systeem van de interne controle is niet verplicht indien de revisor bewijskrachtig controlemateriaal heeft verkregen langs een andere weg. Indien de zogenaamde *compliance tests* de revisor de nodige zekerheid verschaffen dat de informatie betrouwbaar is, is hij niet verplicht deze leemte te melden in het deel van het verslag dat de verklaring over de financiële staten betreft. De revisor kan het echter wel nuttig achten hiernaar te verwijzen als er een betekenisvol risico blijft bestaan dat de fraude en vergissingen niet aan het licht zouden komen.

2.3. Controle in een omgeving waarin gebruik wordt gemaakt van geautomatiseerde informatiesystemen (3 oktober 1997)[63]

1. Inleiding

*1.1.*Deze aanbeveling steunt op de algemene controlenormen van het IBR en past de IFAC-ISA 401 "Auditing in *a* Computer Information Systems Environment" toe. Verder houdt deze aanbeveling ook rekening met de principes die worden geformuleerd in de Controleaanbeveling 2.1. "Controlerisico" (3 december 1993).

Onderhavige aanbeveling geeft een aantal richtlijnen voor de revisorale controle in

[63] Advies Hoge Raad voor het Bedrijfsrevisoraat en de Accountancy d.d. 1 juli 1997, Jaarverslag HREB, 1997, p. 25-26.

een omgeving waar de cliënt gebruikmaakt van geautomatiseerde informatiesystemen (GIS).

In het kader van deze aanbeveling is sprake van een GIS-omgeving indien een computer van welke grootte dan ook, door de organisatie wordt gebruikt voor de verwerking van financiële informatie welke voor de controle van belang is, ongeacht het feit of de verwerking bij de onderneming zelf of bij derden plaatsvindt.

De hieronder uitgewerkte controlestrategie is erop gericht om in een GIS-omgeving de inherente risico's en de interne controlerisico's op te sporen die de interpretatie van de jaarrekening kunnen beïnvloeden.

*1.2.*De algemene doelstelling en de reikwijdte van een controle veranderen niet in een GIS-omgeving.

*1.3.*Het gebruik van een computer verandert wel de verwerking, de opslag en de communicatie van de financiële informatie en kan van invloed zijn op de administratieve organisatie en interne controle van de huishouding. Derhalve kan een GIS-omgeving van invloed zijn op:

- De te verrichten werkzaamheden van de bedrijfsrevisor bij het verkrijgen van voldoende inzicht in de administratieve organisatie en interne controle.
- De inschatting van het inherent risico en het interne controlerisico welke onderdeel vormen van de risicoanalyse.
- De opzet en de uitvoering van de systeemgerichte en gegevensgerichte werkzaamheden, die vereist zijn voor het bereiken van de controledoelstelling.

2. Vaardigheden en bekwaamheid

2.1.<*em*>De bedrijfsrevisor dient voldoende kennis te bezitten omtrent de GIS om de (te) verrichte(n) werkzaamheden te kunnen plannen, sturen, begeleiden en te beoordelen. De bedrijfsrevisor dient te overwegen of er ten behoeve van de controle behoefte is aan specialistische GIS-kennis. Deze kan nodig zijn voor:

- Het verkrijgen van voldoende inzicht in de administratieve organisatie en interne controle waarop de GIS-omgeving van invloed is.
- Het vaststellen van het effect van de GIS-omgeving op de inschatting van het risico op jaarrekeningniveau en op het risico op het niveau van de jaarrekeningposten en de soorten transacties.
- De opzet en de uitvoering van adequate systeemgerichte en gegevensgerichte werkzaamheden.

Indien er behoefte is aan specialistische kennis, roept de bedrijfsrevisor de hulp in van een deskundige die dergelijke kennis bezit. De deskundige kan van de eigen organisatie van de bedrijfsrevisor zijn of van daarbuiten. Als een dergelijke deskundige wordt ingeschakeld, dient de bedrijfsrevisor toereikende controle-

informatie te verkrijgen dat dergelijke werkzaamheden toereikend zijn voor zijn controledoelstellingen, met inachtneming van hetgeen hierover is opgenomen in de “Controleaanbeveling 3.4. inzake het gebruikmaken van de werkzaamheden van deskundigen”.

3. Planning

*3.1.*De bedrijfsrevisor dient inzicht te verkrijgen in het belang en de complexiteit van de GIS-activiteiten en de beschikbaarheid van gegevens voor de controle ten behoeve van het plannen van de onderdelen van de controle waarop de GIS- omgeving van de huishouding van invloed kan zijn. Dit inzicht omvat onderwerpen zoals:

- Het belang en de complexiteit van de geautomatiseerde verwerking van elke belangrijke administratieve toepassing. De belangrijkheid is afhankelijk van het materieel belang van de beweringen in de jaarrekening waarop de geautomatiseerde gegevensverwerking van invloed is. Een toepassing wordt als complex aangemerkt als bijvoorbeeld:
    - Het aantal transacties zodanig is dat het voor de gebruikers moeilijk is om tijdens de gegevensverwerking fouten te identificeren en te corrigeren.
    - De computer automatisch transacties van materieel belang genereert of mutaties genereert in andere toepassingen.
    - De computer gecompliceerde bewerkingen van financiële informatie uitvoert en/of automatisch transacties van materieel belang of journaalposten genereert waarvoor geen afzonderlijke goedkeuring wordt gegeven.
    - Transacties op geautomatiseerde wijze met andere organisaties plaatsvinden (zoals in systemen waarmee gegevens op geautomatiseerde wijze met elkaar verbonden zijn (EDI)) zonder voorafgaande beoordeling van de juistheid of aanvaardbaarheid.
- De organisatiestructuur van de GIS-activiteiten van de opdrachtgever en de mate waarin de geautomatiseerde verwerking in de huishouding is gecentraliseerd of gedecentraliseerd, in het bijzonder als dit van invloed is op de functiescheidingen.
- De beschikbaarheid van gegevens. Basisdocumenten, bepaalde computerbestanden en ander bewijsmateriaal waarover de bedrijfsrevisor wil beschikken kan slechts tijdelijk of alleen maar in geautomatiseerde vorm beschikbaar zijn. Het GIS van de opdrachtgever kan interne rapportage opleveren die van nut kunnen zijn voor het verrichten van gegevensgerichte werkzaamheden (in het bijzonder cijferanalyse). De mogelijkheid voor het toepassen van door de computer ondersteunde controletechnieken kan leiden tot verhoogde efficiëntie in de uitvoering van de controlewerkzaamheden of kan de bedrijfsrevisor in staat stellen om op een economische wijze bepaalde werkzaamheden met betrekking tot een gehele populatie van posten of transacties uit te voeren.

*3.2.*Als de GIS van groot belang zijn, dient de bedrijfsrevisor ook inzicht te verkrijgen in de GIS-omgeving en in welke mate deze van invloed kan zijn op de beoordeling van het inherent risico en het interne controlerisico. De aard van de risico’s en de eigenschappen van de interne controlemaatregelen in een GIS-omgeving

omvatten onder meer:

- Het gemis aan vastleggingen van de transacties. Bepaalde GIS zijn zo opgezet dat een vastlegging van een volledige transactie welke voor controledoeleinden nuttig is slechts tijdelijk of alleen maar in geautomatiseerde leesbare vorm beschikbaar is. In de situatie dat een complex toepassingsprogramma een groot aantal stappen in de verwerking omvat kan het zijn dat er geen volledige controleerbare vastlegging beschikbaar is. Dienovereenkomstig kan het moeilijk zijn om met handmatige procedures tijdig fouten in de logische bewerkingen van het toepassingsprogramma te ontdekken.
- Uniforme verwerking van transacties. De geautomatiseerde verwerking behandelt gelijksoortige transacties met dezelfde verwerkingsinstructies. Aldus zijn rekenfouten welke in het algemeen voorkomen bij handmatige verwerking vrijwel uitgesloten. Omgekeerd zullen programmafouten (of andere systematische fouten in de hardware of software) in het algemeen leiden tot onjuiste verwerking van alle transacties.
- Het gemis aan functiescheidingen. Veel controlemaatregelen die in het algemeen in handmatige systemen door afzonderlijke personen worden uitgevoerd kunnen in het GIS geïntegreerd zijn. Zo kan een persoon die toegang heeft tot computerprogramma's, de verwerking of de bestanden in de gelegenheid zijn om onverenigbare functies te verrichten.
- Kans op fouten en onjuistheden. De kans op menselijke fouten bij de ontwikkeling, het onderhoud en de werking van het GIS kan groter zijn dan in handmatige systemen, in het bijzonder vanwege de gedetailleerdheid welke inherent is aan deze activiteiten. Derhalve is de kans dat personen ongeautoriseerd toegang verkrijgen tot bestanden of bestanden kunnen wijzigen zonder dat dit sporen nalaat in de GIS groter dan in handmatige systemen.
  Verder kan de afgenomen menselijke betrokkenheid bij het afhandelen van de door de GIS verwerkte transacties de aandacht voor fouten en onjuistheden verminderen. Fouten die tijdens het ontwerp of aanpassing van toepassingsprogramma's of systeemsoftware worden gemaakt kunnen voor lange tijd onontdekt blijven.
- Het initiëren of uitvoeren van transacties. De GIS kunnen in staat zijn om bepaalde transacties automatisch te initiëren of uit te voeren. De autorisatie van deze transacties of procedures hoeft niet op dezelfde wijze als bij handmatige systemen te zijn vastgelegd en de autorisatie door de leiding van de huishouding van deze transacties kan impliciet begrepen zijn in de acceptatie van het ontwerp van de GIS en de latere aanpassingen ervan.
- Afhankelijkheid van andere op de geautomatiseerde gegevensverwerking betrekking hebbende interne controlemaatregelen. Geautomatiseerde gegevensverwerking kan verslagen of andere vastleggingen voortbrengen die worden gebruikt voor de handmatige controlewerkzaamheden in de gebruikersomgeving. De effectiviteit van deze handmatige controlewerkzaamheden kan afhankelijk zijn van de effectiviteit van interne controlemaatregelen met betrekking tot de volledigheid en juistheid van de geautomatiseerde gegevensverwerking. Omgekeerd is de effectiviteit en de

consistente werking van de interne controlemaatregelen op de geautomatiseerde gegevensverwerking vaak afhankelijk van de effectiviteit van de algemene beheersingsprocedures van de GIS.

- De mogelijkheid van toename van het toezicht door de leiding van de huishouding. De GIS kan de leiding van de huishouding een verscheidenheid aan analytische middelen verschaffen, die kunnen worden gebruikt om de activiteiten van de huishouding te beoordelen en het toezicht daarover te houden. De beschikbaarheid van deze aanvullende interne controlemaatregelen kan, indien ze worden gebruikt, de gehele interne controlestructuur versterken.
- De mogelijkheid tot het gebruik maken van door de computer ondersteunde controletechnieken. Het feit dat voor de verwerking en het analyseren van grote hoeveelheden gegevens gebruik kan worden gemaakt van een computer schept voor de bedrijfsrevisor de mogelijkheid om algemene of specifieke, door de computer ondersteunde controletechnieken toe te passen. De risico's en de interne controlemaatregelen die het gevolg zijn van deze eigenschappen van de GIS kunnen van invloed zijn op de inschattingen van de bedrijfsrevisor van de risico's en op de aard, het tijdstip van uitvoering en de omvang van de controlewerkzaamheden.

4. Risico-inschatting

*4.1.*Het inherente risico en het interne controlerisico in een GIS-omgeving kunnen zowel een algemeen effect als een post-specifiek effect hebben op de waarschijnlijkheid van onjuistheden van materieel belang en wel als volgt:

- De risico's kunnen het gevolg zijn van onvolkomenheden in essentiële GIS-activiteiten zoals de ontwikkeling en het onderhoud van de programma's, het gebruik van systeemsoftware, de verwerking, de fysieke beveiliging van de GIS en het gebruik van specifieke hulpprogramma's die de geautomatiseerde gegevensverwerking ondersteunen (utilities). Deze onvolkomenheden kunnen een algemeen effect hebben op alle gebruikte toepassingsprogrammatuur.
- De risico's kunnen de kans op fouten of frauduleuze handelingen in specifieke toepassingen, in bepaalde gegevensbestanden, of in specifieke verwerkingsactiviteiten vergroten. Fouten zijn bijvoorbeeld niet ongewoon bij systemen die complexe logische bewerkingen of berekeningen uitvoeren, of waarbij rekening moet worden gehouden met veel verschillende uitzonderingsbepalingen. Systemen die kasbetalingen of andere liquide middelen controleren zijn zeer gevoelig voor frauduleuze handelingen door gebruikers of GIS-personeel.

*4.2.*Als zich nieuwe ontwikkelingen in de GIS-technologie voordoen worden deze door de opdrachtgever vaak gebruikt om steeds complexere computersystemen te bouwen zoals bijvoorbeeld aansluitingen van microcomputers op mainframes, gedecentraliseerde gegevensbestanden, verwerking door eindgebruikers en bedrijfsondersteunende systemen die informatie direct in het administratieve systeem overbrengen. Deze systemen verhogen de algehele complexiteit van de specifieke

toepassingen waarop de GIS van invloed zijn. Als gevolg daarvan kunnen zij het risico verhogen en is verdere beoordeling vereist.

5. Controlestrategie voor GIS-omgevingen

*5.1.**Werkschema*

Het hierna volgende diagram geeft een overzicht van de stappen die men kan onderkennen bij het uitvoeren van de controlewerkzaamheden in GIS-omgevingen.<beeld_H:\verwerking\framemaker\frameExport\verwerking\figuren\fig2 [Converted].tif>

Bij de tenuitvoerlegging van zijn controlewerkzaamheden in een GIS-omgeving zal de revisor de volgende werkzaamheden uitvoeren:

Stap 1: het verzamelen van achtergrondinformatie en de planning van de controlewerkzaamheden.

Stap 2: het uitvoeren van een voorafgaandelijke analyse die de volgende werkzaamheden omvat:

- het uitvoeren van een algemene diagnostiek toegespitst op de sleutelcontroles die binnen de GIS-omgeving werden voorzien;
- het evalueren van de inherente- en de controlerisico's die door de geautomatiseerde gegevensverwerking worden geïnduceerd, waarbij de nadruk wordt gelegd op integriteit en continuïteit.

Stap 3: het nemen van een beslissing met betrekking tot de te volgen controlestrategie en dit op basis van de in dit stadium beschikbare informatie:

- ofwel beslist de revisor te steunen op de interne controle;
- ofwel zal de revisor deze vervangen door aangepaste substantiële controles en overgaan naar stap 7.

Indien de GIS-omgeving beheerd wordt door een andere entiteit van de groep, of een derde en de revisor niet in staat is om de nodige controlewerkzaamheden uit te voeren, zal ook tot een substantiële aanpak moeten worden besloten.

Stap 4: de uitvoering van een gedetailleerd onderzoek van de algemene informatie technologiecontroles (afgekort: IT-controles).

Stap 5: de beslissing om over te gaan tot het onderzoek van de toepassingscontroles: als de algemene IT-controles gebrekkig blijken, kan de revisor beslissen niet over te gaan tot het onderzoek van de toepassingscontroles en over te gaan naar stap 7.

Stap 6: het gedetailleerd onderzoek van de interne controlemechanismen die in en rond de diverse toepassingen geïmplementeerd werden.

Stap 7: de aanpassing van de controlestrategie voor wat betreft het analytisch onderzoek en de substantiële testen.

Elk van deze stappen wordt hierna verder uitgewerkt.

5.2. Het verzamelen van de achtergrondinformatie en de planning van de controlewerkzaamheden (stap 1)

De revisor moet basisinformatie inwinnen aangaande de GIS-omgeving en met name t.a.v.:

a) de IT-strategie en -planning die de onderneming uitwerkte, de werkmethodes binnen het departement informatica, de IT-beveiligingspolitiek en het bestaan van interne procedures binnen de informatica;
b) de technologieën die de entiteit aanwendt, met inbegrip van de telecommunicatienetwerken, de daarop betrekking hebbende procedures, met name wat de communicatie met derden betreft, o.m. banken, leveranciers, klanten,...;
c) de toepassingsarchitectuur en voor elke toepassing: oorsprong, aard van de verwerking en onderlinge interacties;
d) de methodes die werden gehanteerd bij het ontwerpen, het ontwikkelen en het onderhouden van toepassingen;
e) de betekenisvolle wijzigingen, die zich in de loop van de controleperiode hebben voorgedaan, de historiek van de belangrijke problemen die zich hebben gesteld en de in dit verband aangereikte oplossingen.

Deze informatie stelt de revisor in staat het belang van de GIS-omgeving voor de onderneming in te schatten en schetst het kader voor de verdere werkzaamheden.

5.3. Voorafgaandelijke analyse (stap 2)

Met het oog op de uitwerking van zijn controlestrategie zal de revisor:

a) bepalen welke bijkomende inherente risico's verbonden zijn aan de GIS-omgeving;
b) een voorafgaandelijke analyse maken van de algemene IT-controles en van de controles die betrekking hebben op de individuele toepassingsprogramma's. Het betreft hier enkel de controles waarop hij oordeelt nuttig en efficiënt te kunnen steunen. Deze analyse stelt hem in staat het interne controlerisico in te schatten daar de zwakheden binnen de controlestructuur en de GIS-omgeving worden gedocumenteerd;
c) in voorkomend geval, het gebruik van geïnformatiseerde controletechnieken voorzien.

5.4. Het bepalen van de controlestrategie (stap 3)

De algemene IT-controles kunnen de kwaliteit en de betrouwbaarheid van de verwerkingen door de toepassingsprogramma's beïnvloeden. Het ontbreken van gepaste controles kan bovendien de integriteit van de verwerkte gegevens in het gedrang brengen.

Bij het bepalen van zijn controlestrategie beschikt de revisor over twee mogelijkheden:

a) indien hij beslist op de interne controle te steunen, moet hij de controles die gelden voor de ganse GIS-omgeving ("algemene IT-controles") onderzoeken, alsook deze die vervat zijn in of georganiseerd zijn rond elke individuele toepassing ("toepassingscontroles"). Indien deze controles onvoldoende blijken, kan de revisor besluiten terug te vallen op voor handen zijnde compenserende manuele procedures;
b) indien hij beslist om niet te steunen op het systeem van interne controle, moet hij overgaan tot uitgebreide substantiële controles.

De weerhouden optie wordt in belangrijke mate beïnvloed door efficiëntieoverwegingen en zal met name gebaseerd zijn op de resultaten van de voorafgaandelijke analyse.

5.5. Gedetailleerd onderzoek van de algemene IT-controles (stap 4)

De algemene IT-controles zijn gericht op het geheel van de geautomatiseerde activiteiten. Zij laten toe een redelijke zekerheid te verwerven dat binnen de GIS-omgeving de algemene doelstellingen van interne controle worden bereikt. Deze algemene IT-controles kunnen in volgende categorieën worden ondergebracht:

- controles die betrekking hebben op het beheer en de organisatie van de informatica-afdeling;
- controles die betrekking hebben op de implementatie van de toepassingen;
- uitbatingscontroles;
- logische toegangscontroles;
- controles m.b.t. de fysische beveiliging en m.b.t. het rampenplan.

Voor meer details in dit verband verwijzen wij naar bijlage A.

De revisor moet rekening houden met de impact van deze controles op de geautomatiseerde toepassingen, wanneer deze toepassingen informatie voortbrengen die verwerkt wordt in de jaarrekening.

5.6. Beslissing m.b.t. het onderzoek van de toepassingscontroles (stap 5)

Indien de algemene IT-controles voldoening schenken zal de revisor overgaan tot het

onderzoek van de toepassingscontroles (stap 6).

Komt de revisor tot het besluit dat de toepassingscontroles belangrijke gebreken vertonen, dan zal hij niet op deze controles kunnen steunen voor het verder verloop van zijn opdracht. Hij zal dit vastleggen in zijn werkdocumenten en nagaan in welke mate het zinvol is om de interne controle verder te onderzoeken. Indien het onderzoek van de interne controle wordt afgebroken, zal hij nagaan in welke mate hij alternatieve controleprocedures kan uitvoeren, die toelaten het getrouw beeld van de jaarrekening te bevestigen overeenkomstig de aanbeveling betreffende de impact van de interne controle op de controlewerkzaamheden.

5.7. Onderzoek van de toepassingscontroles (stap 6)

Onder "toepassingscontroles" verstaat men enerzijds, de geautomatiseerde controleprocedures die binnen de toepassing werden voorzien, en anderzijds, de manuele verificatieprocedures waarop een organisatie steunt om de verwerking van gegevens te controleren.

Deze twee types van controles zullen door de revisor beoordeeld worden en dit zowel individueel als in hun onderling verband. Het geheel van deze controles garandeert immers de volledigheid, de juistheid, het geautoriseerd karakter en de validiteit van de financiële en operationele informatie vervat in het systeem.

Meer en meer wordt vastgesteld, dat de nieuwe technologieën aanleiding geven tot de vervanging van manuele controles door geautomatiseerde controles.

Voor meer details aangaande de toepassingscontroles verwijzen wij naar bijlage B.

5.8. Aanpassing van de controlestrategie (stap 7)

Op basis van zijn gedetailleerd onderzoek van de algemene IT-controles en van de interne controlemaatregelen ingebouwd in of uitgevoerd rond, de verschillende toepassingen, zal de revisor nagaan of de interne controle in haar geheel beschouwd voldoening schenkt.

Indien de revisor op basis van zijn onderzoek vaststelt dat het systeem van interne controle belangrijke leemtes vertoont, zal hij zijn substantiële controles uitbreiden. Indien de interne controleprocedures voldoening geven, zal hij op beduidende wijze zijn substantiële controles kunnen beperken.

* * *

Bijlage A: Algemene IT-controles

Definitie

De algemene IT-controles omvatten controlemechanismen die gelden voor de gehele GIS-omgeving. Zij laten toe een redelijke zekerheid te verwerven dat de algemene doelstellingen van de interne controle worden bereikt. Deze controles kunnen in vijf categorieën worden ingedeeld:

- controles die betrekking hebben op het beheer en de organisatie van de informatica-afdeling;
- controles die betrekking hebben op de implementatie van de toepassingen;
- uitbatingscontroles;
- logische toegangscontroles;
- fysische beveiliging en rampenplan.

1. Controles die betrekking hebben op het beheer en de organisatie van de informatica-afdeling

In dit kader worden o.m. volgende aspecten geëvalueerd:

- de plaats van de informatica-afdeling binnen het algemene organogram van het bedrijf;
- de kwaliteit van de IT-strategie, van het IT-plan en het voorhanden zijn van een informaticabudget;
- de samenstelling, de rol, de verantwoordelijkheden en de wijze waarop de stuurgroep informatica werkt;
- de wijze waarop de directie de diverse informaticaprojecten opvolgt en de mate waarin zij tussenkomt bij het toewijzen van informaticamiddelen;
- de betrokkenheid en rol van de interne auditafdeling m.b.t. de geautomatiseerde informatieverwerking;
- het bestaan van een evenwicht tussen de informaticamiddelen die beschikbaar zijn en de noden die voortvloeien uit het informaticaplan;
- de relaties tussen de eindgebruikers en de informatica-afdeling;
- de structuur van de informatica-afdeling, het bestaan van functiebeschrijvingen en de realisatie van een functiescheiding tussen ontwikkeling, gegevensbeheer en uitbating;
- de inhoud en de kwaliteit van de personeelspolitiek voor de informatica-afdeling (aanwerving, ontslag, evaluatie, promotie, opleiding);
- de inhoud, de kwaliteit en de naleving van de beveiligingspolitiek;
- de naleving van specifieke wetgeving m.b.t. GIS-omgevingen (wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, wet ter bescherming van de auteursrechten op

computerprogramma's,...)[64].

2. Controles met betrekking tot de implementatie van toepassingen

Deze controles hebben betrekking op de wijze waarop informaticatoepassingen worden ontwikkeld, aangeschaft en onderhouden. Zij dragen in belangrijke mate bij tot de kwaliteit van de toepassingen die worden geïmplementeerd. Binnen deze categorie kan een onderscheid worden gemaakt tussen:

- maatwerk door eigen personeel of door een toeleverancier;
- de aanschaffing, het parametreren, de eventuele aanpassing en de implementatie van pakketten;
- onderhoud van de toepassingen.

2.1. Maatwerk door eigen personeel of door een toeleverancier

Het succes van belangrijke ontwikkelingsprojecten is in hoge mate afhankelijk van de kwaliteit van het projectmanagement. Een gedegen projectsturing veronderstelt onder meer:

- een duidelijk engagement en actieve tussenkomst van de directie;
- de medewerking van ervaren projectleiders;
- een aangepaste ontwikkelingsmethodologie, aangevuld met duidelijke ontwikkelingsprocedures en -standaarden;
- het bestaan van gedegen kwaliteitscontroles;
- uitgewerkte budgetten;
- een gedetailleerde omschrijving van de uit te voeren taken;
- een duidelijke omschrijving van de verantwoordelijkheden;
- systematische opvolging door geschreven rapportering gericht aan alle partijen en de ondernemingsleiding.

Daarnaast zijn vanuit een revisoraal standpunt volgende factoren belangrijk:

- het bestaan van gescheiden technische omgevingen voor de ontwikkeling, voor het testen en voor het productief gebruik;
- formele verantwoording van het ontwikkelingsproject op basis van een haalbaarheidsstudie en de formele specificaties van de behoeften van de gebruikers;
- het in acht nemen van beveiligings- en controlevereisten in elk stadium van het ontwikkelingstraject;
- een correcte integratie van de toepassing in de toepassingsarchitectuur;
- de uitvoering van tests van individuele modules, van systeemtests, van integratietests en van acceptatietests waarbij wordt nagegaan of de programmatuur

[64] Indien deze wetgeving door de cliënt niet wordt gerespecteerd, dient de revisor te overwegen dit in de "management letter" te rapporteren.

technisch correct werkt en tegemoetkomt aan de behoeften van de gebruikers;
- projecten moeten formeel worden geaccepteerd door de gebruikers vóór het in productie nemen;
- er moet worden nagegaan of de toepassingen werden ontwikkeld en gedocumenteerd volgens de geldende regels;
- het bestaan van een gecontroleerde procedure voor overdracht van de ontwikkelingsomgeving naar de productieve omgeving; parallel aan de technische implementatie moeten de organisatorische en procedurele aspecten van de administratieve organisatie worden herzien;
- de gebruikers moeten behoorlijk worden opgeleid; bijkomende documentatie moet waar nodig worden opgesteld met het oog op de integratie van de toepassing in de administratieve omgeving.

In het geval dat maatwerk door een derde wordt ontwikkeld, dient aandacht te worden besteed aan de bepalingen van het aannemingscontract (en dit o.m. met betrekking tot de eigendom van de programmatuur en de toekomstige bijwerking).

2.2. Aanschaffing, parametrering en implementatie van pakketten

De aankoop en de implementatie van pakketten moet zoals elk ander project beheerd worden. Daarenboven moet met de volgende aspecten rekening worden gehouden:

- pakketten dienen te worden geselecteerd op basis van een formele behoeftedefinitie, waarbij in voorkomend geval de huidige werkmethodes en procedures in vraag worden gesteld en de doelstellingen indien nodig worden geherdefinieerd;
- het aankoopcontract dient duidelijke specificaties te omvatten m.b.t. de verwachte performantie, de functionaliteiten, de door de leverancier te leveren documentatie, de eigendom of neerlegging van de broncode, technische ondersteuning bij de implementatie, toekomstig onderhoud en opleiding van de gebruikers. Daarnaast dient duidelijk te worden gerefereerd aan de werkdocumenten en briefwisseling die aan de selectie van het pakket vooraf gingen;
- bij de selectie van pakketten dient o.m. rekening te worden gehouden met:
  - de betrouwbaarheid en reputatie van de leverancier;
  - de functionele kenmerken, de controle- en beveiligingskarakteristieken van het pakket;
  - de kwaliteit van de door de leverancier geleverde ondersteuning;
  - de kwaliteit van de documentatie voor de eindgebruikers;
  - de beschikbaarheid van een technische basisdocumentatie;
  - de contractuele garanties die de leverancier kan voorleggen inzake de ondersteuning van het pakket in de tijd;
- elk pakket dient te worden getest vooraleer het in productie wordt genomen;
- het pakket moet geïntegreerd worden in de bestaande toepassingsarchitectuur, en deze integratie moet worden gedocumenteerd;
- na de aankoop van een pakket moeten upgrades op een systematische manier worden opgevolgd.

Ten slotte dient opgemerkt dat alle belangrijke aanpassingen dienen te verlopen volgens de hierboven aangehaalde regels voor eigen ontwikkeling (2.1.).

2.3. Onderhoud

Voor belangrijke aanpassingen aan bestaande programmatuur gelden uiteraard dezelfde regels als voor nieuwe ontwikkelingen. Alhoewel voor courant onderhoud normalerwijze niet op een projectbasis wordt gewerkt, blijven de basisprincipes van toepassing. Hierbij is het vooral van belang om over een duidelijk systeem te beschikken voor het registreren, beoordelen, uitvoeren en toewijzen van prioriteiten van de gevraagde aanpassingen. Het is essentieel om bij het uitvoeren van wijzigingen de documentatie aan te passen.

3. Uitbatingscontroles

Uitbatingscontroles waarborgen dat de dagdagelijkse informatieverwerking op een correcte en een betrouwbare wijze verloopt en laten de onderneming toe doelmatig in te spelen op eventuele incidenten. In dit verband zullen volgende aspecten worden onderzocht:

3.1. Technisch-operationeel beheer

De activiteiten die onder deze hoofding worden gegroepeerd, hebben enerzijds betrekking op het behoud van de performantie van het systeem en anderzijds, op de coördinatie en de planning van de evolutie van de IT-infrastructuur.

3.2. Het beheer van de vooropgestelde dienstverlening

Deze activiteiten zullen uitmonden in overeenkomsten tussen de diverse partijen die bij de geautomatiseerde informatieverwerking betrokken zijn (de eindgebruiker, de systeemontwikkelaar, de uitbating,...) en dragen bij tot een kwaliteitsvolle dienstverlening.

3.3. Beheer van de technische evolutie van de infrastructuur

Het betreft de procedures, die geïmplementeerd werden om de wijzigingen te coerdineren en op te volgen die aan de GIS-omgeving worden aangebracht (materieel, systeem, netwerk, enz.).

3.4. Beheer van de informaticaconfiguratie

Deze activiteiten hebben betrekking op de identificatie en het beheer van het materieel en de basisprogrammatuur.

3.5. Beheer van incidenten

Deze procedures beschrijven de wijze waarop problemen waarmee de informatica-afdeling te kampen heeft worden behandeld (vastlegging van de problemen en abnormale situaties, verwijzing naar de oorsprong van het incident, opvolging en bijsturing, interactie tussen de systeemontwikkelaars en de gebruikers,...).

3.6. Uitbatingsprocedures

Naast algemene procedures betreffende de dagdagelijkse uitbating van het systeem (het nemen van veiligheidskopieën, restore-procedures, richtlijnen voor het opstarten en stoppen van het systeem) zijn specifieke uitbatingsprocedures voor de toepassingen noodzakelijk.

3.7. Backup en restoreprocedures

Zowel van de gegevens als van de programma's en de systeemomgeving moeten veiligheidskopieën genomen worden. Deze kopieën moeten op een beveiligde locatie worden bewaard. Voldoende recente veiligheidskopieën moeten extern worden bewaard.

3.8. Archiverings- en desarchiveringsprocedures

Er moeten formele procedures bestaan m.b.t. de archivering van gegevens en programmatuur. De genomen maatregelen moeten rekening houden met de wettelijke bewaringstermijnen en met de operationele behoeften terzake.

3.9. Procedures voor het beheer van gegevensdragers

Er moeten duidelijke richtlijnen bestaan ten aanzien van het beheer van gegevensdragers (inventaris, hergebruik, identificatie).

3.10. Planning van de uitbating

De batchverwerking moet worden gepland, geparametreerd en uitgevoerd op basis van vooraf vastgestelde richtlijnen.

3.11. "Logging" – Controlespoor

Er moet een controlespoor bestaan betreffende de uitvoering van alle belangrijke geautomatiseerde processen.

4. Logische toegangscontroles

Logische toegangscontroles laten toe de toegang tot het systeem te beperken tot geautoriseerde gebruikers. Meestal maakt men gebruik van een combinatie van gebruikersidentificaties (user ID's) en paswoorden om deze doelstellingen te realiseren.

Om de doelmatigheid van dit systeem te garanderen, moet aan de volgende voorwaarden voldaan worden:

- individuele identificatie van de verschillende gebruikers;
- duidelijke procedures voor het beheren van de gebruikersprofielen (definiëren van nieuwe gebruikers, verwijderen van personeelsleden die de organisatie verlaten, aanpassing van het profiel wanneer iemand van functie verandert, enz.);
- richtlijnen en controlemaatregelen met betrekking tot de confidentialiteit, de structuur en het beheer van de paswoorden (lengte van de geheime code, periodieke wijziging,...);

- controle over gebruikersprofielen met belangrijke privileges (systeemploeg, security officer,...);
- integriteit van het beveiligingspakket en het besturingssysteem zelf.

Bovendien moeten maatregelen worden genomen om de toegang van de gebruikers te beperken tot die programma's, transacties, bestanden, gegevens en "utilities" die rechtstreeks verband houden met hun functie in de entiteit. Een controlespoor van alle verwerkingen dient voor handen te zijn.

Daarnaast moeten detectieve controles worden opgezet om de effectieve werking van het beveiligingssysteem te bevestigen en, in voorkomend geval, inbreuken te rapporteren en op te volgen.

Tenslotte moet ook de toegang tot het netwerk op een specifieke wijze worden gecontroleerd. Bijkomende controles op dit vlak zijn van belang indien externe partijen via het netwerk toegang kunnen hebben tot het systeem (b.v. via dial-up verbindingen).

5. De fysieke beveiliging en het rampenplan

5.1. De fysieke beveiliging

Er moeten preventieve en detectiemaatregelen genomen worden om het systeem te beveiligen tegen gevaren zoals brand, waterschade, stroomonderbreking, inbraak,...
Een gedegen fysieke beveiliging is gebaseerd op volgende principes:

Situering van het rekencentrum
Bij het uitbouwen van een computerzaal dient rekening te worden gehouden met de aanwezige externe bedreigingen zoals industriële activiteit, watervoorraden, voorraden van brandbaar materiaal, enz.

Toegangscontrole
De toegang tot het materieel (computers en telecommunicatieapparatuur, enz.) dient te worden beperkt.

Brandbeveiliging
Er moeten specifieke maatregelen voor branddetectie en -bestrijding genomen worden.

Stroomvoorziening
De continuïteit van de elektrische stroomvoorziening dient te worden verzekerd. Typische maatregelen in dit verband zijn: het plaatsen van apparatuur die de netspanning nivelleert, back-upbatterijen, noodaggregaten, enz.

Werkomgeving
Er moeten aangepaste maatregelen worden getroffen voor het conditioneren van de informaticazaal (temperatuur, vochtigheidsgraad, enz.).

Netwerken
Maatregelen dienen te worden genomen om de beschikbaarheid van het netwerk te verzekeren (triangulatie, alternatieve communicatieverbindingen,...).

5.2. Rampenplan

Een effectief rampenplan wordt uitgewerkt op basis van een methodologie waarin volgende aspecten aan bod komen:

- identificatie van essentiële bedrijfsfuncties op basis van een risicoanalyse;
- vaststelling van het verband en de afhankelijkheden tussen deze functies;
- bepaling van de uitwijk/herstelstrategie;
- analyse van de potentiële bedreigingen;
- beschrijving van mogelijke oplossingen en de ermee gepaard gaande kosten;
- documentatie van het herstelplan en de procedures;
- ontwikkeling en documentatie van alternatieve procedures voor de gebruikers;
- testen van het herstelplan;
- toewijzen van de verantwoordelijkheden voor onderhoud van het plan; en training van de betrokken personeelsleden.

6. End user computing

Onder de term “end user computing” wordt het gebruik verstaan, van IT-middelen door eindgebruikers in de onderneming. Deze middelen kunnen zowel centraal als gedecentraliseerd ter beschikking worden gesteld (microcomputers).

Sommige controles en veiligheidsmaatregelen die toepasselijk (of essentieel) zijn voor grote systemen, zijn praktisch niet haalbaar in dit soort omgeving. In de praktijk zal dit aanleiding geven tot accentverschuivingen binnen de controleomgeving.

Door de lage toegangsdrempel en enkel omwille van het feit dat de gegevens worden verwerkt door “een” computer, bestaat bovendien het gevaar dat de eindgebruikers een onvoorwaardelijk vertrouwen stellen in de financiële informatie die door dergelijke systemen wordt opgeslagen en gegenereerd. Gezien end user computer tools eerder gericht zijn op de individuele eindgebruikers, wordt de graad van accuratesse en betrouwbaarheid van informatie in belangrijke mate mee bepaald door de interne controlemaatregelen, die door het management worden opgelegd en worden toegepast door de gebruikers.

Hieronder volgen een aantal punten die mede bepalend zijn voor de controlebenadering in dergelijke omgevingen en erop gericht zijn de beschikbaarheid, confidentialiteit en integriteit van informatiesystemen gebaseerd op “end user computing faciliteiten” te garanderen:

- het bestaan van formele voorschriften van de leiding inzake het gebruik en de controle van microcomputers in de onderneming;
- maatregelen inzake fysieke veiligheid: verminderen van het risico op diefstal, op accidentele schade en op oneigenlijk gebruik;
- controle op het gebruik van de programma’s (licentieverplichtingen, toegangscontrole, opleidingsvereisten, enz.);
- controle op de toegang tot door de eindgebruiker ontwikkelde toepassingen en gegevens, maatregelen die erop gericht zijn niet geautoriseerde wijzigingen te verhinderen;
- instructies m.b.t. de beveiliging en het gebruik van externe opslagmedia (diskettes, tapes, removable harddisks,...);
- controle op de betrouwbaarheid van de door de eindgebruiker ontwikkelde toepassingen;
- controle op de uitvoering van back-ups van software, ontwikkelde applicaties en gegevens;
- maatregelen ter voorkoming van infecties door computervirussen;
- controlemaatregelen en instructies m.b.t. verbindingsmogelijkheden rond netwerken.

* * *

Bijlage B: Toepassingscontroles

Definitie

Onder "toepassingscontroles" verstaat men enerzijds, de geautomatiseerde controleprocedures die binnen de toepassing werden voorzien, en anderzijds, de manuele verificatieprocedures waarop een organisatie steunt om de verwerking van gegevens te controleren.

Het geheel van deze controles garandeert de volledigheid, de juistheid, het geautoriseerd karakter en de validiteit van de financiële en operationele informatie vervat in het systeem.

1. Geautomatiseerde controleprocedures

Hieronder volgt een niet-limitatieve lijst van geautomatiseerde controleprocedures:

- echocontroles (edit checks): deze categorie omvat de controles op het formaat, de juistheid, het bestaan en de redelijkheid van gegevens die voor verwerking worden aangeboden. Zij verhinderen dat foutieve gegevens worden verwerkt;
- verificatie van de numerische sequentie: een controle van deze aard stelt een organisatie in staat na te gaan of alle gegevens werden ingevoerd, het betreft hier dus een volledigheidscontrole;
- geautomatiseerde afstemming (matching): indien nieuw ingebrachte gegevens kunnen worden vergeleken met gegevens die reeds op het systeem beschikbaar zijn kunnen ze op hun redelijkheid worden getoetst;
- autorisatiesystemen: in heel wat toepassingen worden transacties zonder meer goedgekeurd op basis van de gegevens in het autorisatieprofiel van de gebruiker. Dit laat de scheiding van functies toe.

2. Manuele controleprocedures

Onder deze categorie vallen alle controles die handmatig door de gebruikers worden uitgevoerd. Het gaat onder meer om:

- de analyse van bestuurlijke informatie;
- de opvolging op uitzonderingsrapporten;
- de uitvoering van reconciliaties;
- het vergelijken van gegevens, die door het informatiesysteem worden toegeleverd, met de realiteit (voorraadopnames, afstemming met rekeninguittreksels van klanten of leveranciers, enz.);
- de formele goedkeuring van transacties.

3. Interactie tussen toepassingscontroles en algemene IT-controles

Toepassingscontroles en algemene IT-controles zijn sterk met elkaar verbonden. De algemene IT-controles zijn noodzakelijk om de betrouwbaarheid te waarborgen van de toepassingscontroles, die gebaseerd zijn op geautomatiseerde verwerking.

De volgende voorbeelden verduidelijken dit:

- indien de controles m.b.t. de implementatie, de ontwikkeling en de aanpassing van toepassingen zwak werden uitgebouwd, bestaat de mogelijkheid dat de informatie van de leiding onbetrouwbaar is, dat "edit checks" niet op een correcte manier werken, dat controlelijsten verkeerd of onvolledig zijn. Wanneer de manueel uitgevoerde controles steunen op weinig betrouwbare rapporten, wordt afbreuk gedaan aan de doelmatigheid van het interne controlesysteem;
- indien de logische toegangscontrole over het systeem belangrijke leemten vertoont, kan de binnen de onderneming uitgebouwde functiescheiding in het gedrang komen.

2.4. Doelstelling van de controle van de jaarrekening (5 januari 1987)[65]

1. Inleiding

"De controle van de jaarrekening heeft" overeenkomstig paragraaf 1.3.1. van de Algemene controlenormen, "tot doel vast te stellen dat:

- de boekhouding en de jaarrekening opgemaakt en voorgesteld worden overeenkomstig de van toepassing zijnde wettelijke en reglementaire bepalingen;
- de jaarrekening (balans, resultatenrekening en de toelichting) een getrouw beeld geeft van het vermogen, de financiële toestand en de resultaten van de onderneming, rekening houdend met de wettelijke en reglementaire beschikkingen terzake, en dat de in de toelichting gegeven verantwoording relevant is."

Meer bepaald zal de controle van de jaarrekening de revisor in staat moeten stellen te verklaren dat:

- in de balans: alle bezittingen, tegoeden en verhaalrechten onder de activa voorkomen; deze op correcte wijze werden gerubriceerd en dat hun waardering met de nodige voorzichtigheid en consistentie werd verricht; alle schulden en verbintenissen onder de passiva voorkomen voor hun werkelijk nog verschuldigd bedrag en dat de nodige voorzieningen werden geboekt tot dekking van de

[65] Advies van de Hoge Raad voor het Bedrijfsrevisoraat d.d. 18 december 1986, Jaarverslag HREB, 1986-1987, niet genummerd.