Geautomatiseerde informatiesystemen en informatiebeveiliging in het MKB

"Goed huisvaderschap volgens de IT-auditor"

Afstudeerscriptie IT Postgraduate opleiding
aan de Vrije Universiteit te Amsterdam

Auteurs:
H. Verkuijlen
A. Folkers

31 oktober 2007

INHOUDSOPGAVE

Hoofdstuk 1 Inleiding

Voor u ligt als sluitstuk van de IT Postgraduate opleiding aan de Vrije Universiteit te Amsterdam onze scriptie "Geautomatiseerde informatiesystemen en informatiebeveiliging in het MKB, Goed huisvaderschap volgens de IT-auditor". In deze scriptie werken wij een onderwerp uit onze dagelijkse praktijk op een academisch verantwoorde wijze uit.

Wij geven een uitwerking van wat onder het begrip 'goed huisvaderschap' van geautomatiseerde informatiesystemen en informatiebeveiliging wordt verstaan en hoe deze in het midden- en kleinbedrijf - hierna te noemen het MKB - in de praktijk wordt toegepast.

De auteurs zijn als controlerend accountant werkzaam bij een top 10 accountantskantoor in Nederland. Onze cliënten bevinden zich voornamelijk in het bovensegment van het MKB.

De Europese Unie (en dus ook de Nederlandse overheid) deelt het bedrijfsleven in drie categorieën in: grootbedrijf, middenbedrijf en kleinbedrijf. Het MKB bestaat uit bedrijven met maximaal 250 medewerkers. Het kleinbedrijf heeft hooguit vijftig personeelsleden. Van alle Nederlandse ondernemingen heeft 1 procent meer dan 250 werknemers. Het MKB onderscheidt zich van grote ondernemingen door ondermeer: kleinschaliger in personele omvang, plattere structuur, dominante rol van de ondernemer en pragmatisme. Voorts beschikken MKB-ondernemingen in de regel over minder kennis en investeringsbudget. De kreten die je vaak van MKB-ondernemers hoort, is "hier moet gewerkt worden" en "aan teveel regels hebben wij geen boodschap".

Het MKB-segment heeft weliswaar zijn beperkingen qua omvang aan personeel, budget en kennis, maar het segment is bijzonder boeiend en belangrijk voor de Nederlandse economie. Het MKB wordt ook wel de motor van de Nederlandse economie genoemd omdat de groei van de werkgelegenheid en de bijdrage aan het bruto nationaal product in dit segment het grootst is. Het MKB investeert jaarlijks meer dan 2 miljard euro in informatietechnologie. De getallen in onderstaand tabel geven de belangrijkheid van het MKB in de Nederlandse economie weer.

Kerngegevens MKB in 2006

Aantal bedrijven:	743.000
Aandeel mkb:	99,7%
Werknemers totaal (excl. overheid):	7,2 miljoen
Werknemers in mkb:	4,2 miljoen
Omzet totaal bedrijfsleven:	€ 1.322,4 miljard
Omzet mkb:	€ 764,6 miljard

(bron: website MKB Nederland)

De ontwikkelingen in de informatietechnologie zijn ook aan de MKB-ondernemingen niet voorbijgegaan. Vrijwel elke MKB-ondernemer heeft zijn administratieve processen geautomatiseerd. Informatietechnologie wordt door MKB-ondernemingen ingezet voor een efficiënte en effectieve bedrijfsvoering gericht op het behalen van het ondernemingsdoel. Automatisering wordt door MKB-ondernemingen daarnaast ingezet voor het behoud van de concurrentiepositie, imago naar leveranciers, afnemers en personeel. Door bovenstaande ontwikkelingen neemt daardoor de noodzaak toe dat het geautomatiseerde informatiesysteem wordt beheerst door MKB-ondernemingen.

Informatiesystemen en informatiebeveiliging zijn onlosmakelijk met elkaar verbonden. Zonder beveiliging is het risico groot dat het informatiesysteem geen betrouwbare informatie verstrekt en/of niet beschikbaar is voor de gebruikers. Bovendien kan het gebrek aan informatiebeveiliging de continuïteit van de bedrijfsvoering in gevaar brengen. Door onvoldoende passende informatiebeveiligingsmaatregelen te nemen, loopt de organisatie het risico haar doelstellingen niet te behalen.

Dit hoofdstuk verduidelijkt de context van het scriptie onderzoek. Ten eerste wordt in paragraaf 1.1 de aanleiding en doelstelling van deze scriptie beschreven. De afbakening wordt beschreven in paragraaf 1.2. Paragraaf 1.3 gaat in op de centrale vraagstelling en de daarvan afgeleide deelvragen. De onderzoekaanpak van onze scriptie staat beschreven in paragraaf 1.4. De leeswijzer van de scriptie wordt vermeld in de laatste paragraaf van dit hoofdstuk in 1.5.

1.1 Aanleiding en doelstelling

In de praktijk van de (wettelijke) controle van de jaarrekening in het MKB-segment loopt de accountant vaak tegen een vergaande mate van automatisering bij zijn cliënten aan. Steeds meer bedrijven in het MKB gebruiken bijvoorbeeld ERP-software waarmee de primaire en logistieke processen worden beheerst.

In onze accountantspraktijk wordt de IT-auditor steeds meer ingezet bij (wettelijke) controleopdrachten in het MKB-segment. De accountant wenst voor zijn oordeelsvorming, op basis van een 'risk based audit approach', te steunen op hetzij geautomatiseerde controles, hetzij op gebruikerscontroles. In geval van geautomatiseerde controles dient de accountant over voldoende kennis te beschikken van ICT. Indien hij niet over voldoende ICT-kennis beschikt, kan hij een IT-auditor inschakelen. De accountant blijft echter eindverantwoordelijk voor de werkzaamheden die de IT-auditor voor hem uitvoert.

Gegeven het beperkte onderzoeksbudget, de gerichte onderzoekvraag en de ongedeelde verantwoordelijkheid voor de werkzaamheden van een IT-auditor is de volgende vraag van belang: Aan welke eisen dient de IT-omgeving minimaal te voldoen zodat nog sprake is van 'goed huisvaderschap' in het kader van interne beheersing voor de organisatie?

Wij vinden het interessant om te onderzoeken of het mogelijk is te komen tot een basisniveau aan maatregelen waar elke MKB-onderneming aan zou moeten voldoen, zodat nog sprake is van 'goed huisvaderschap'.

1.2 De afbakening

De uitdaging van de IT-auditor is te komen tot een set van maatregelen voor de beoordeling van het 'goed huisvaderschap'. Vanwege de pluriformiteit aan systemen in het MKB kan geen limitatieve opsomming voor het begrip 'goed huisvaderschap' worden gegeven. In deze scriptie willen wij daarom een subset van maatregelen beschrijven waaraan elke MKB-ondernemer zou moeten voldoen.

Voor het begrip 'goed huisvaderschap' hanteren wij de volgende definitie:
Het door de leiding van de huishouding opstellen en invoeren van basis beheersingsmaatregelen ten behoeve van geautomatiseerde informatiesystemen en informatiebeveiliging.

De basis beheersingsmaatregelen dienen te worden ingevoerd naast de specifieke beheersingsmaatregelen, die voor elke onderneming weer anders zullen zijn. Elke

onderneming loopt namelijk andere risico's in zijn bedrijfsvoering ondermeer door de verschillen in omvang, configuratie en ouderdom van systemen.

1.3 De onderzoeksvraag

De onderzoeksvraag luidt als volgt:
Wat omvat het begrip 'goed huisvaderschap' in het kader van geautomatiseerde informatiesystemen en informatiebeveiliging in het MKB?

Bij deze centrale vraagstelling hebben wij de volgende deelvragen afgeleid om het onderzoek te kunnen uitvoeren:

1. Aan welke eisen dient de beheersing van een geautomatiseerd informatiesysteem minimaal te voldoen?
2. Aan welke eisen dient de informatiebeveiliging minimaal te voldoen voor een MKB-ondernemer?
3. Hoe wordt 'goed huisvaderschap' in de praktijk toegepast?

1.4 De onderzoeksaanpak

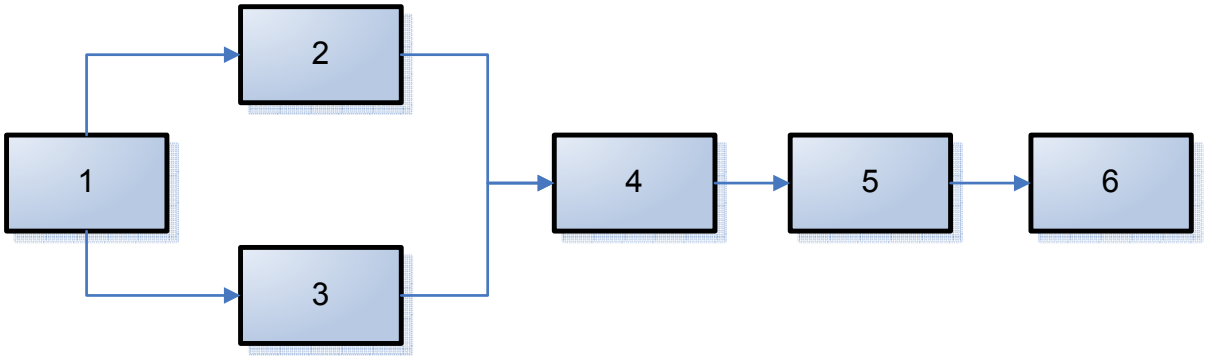
De onderzoeksaanpak kent de volgende elementen:

- Literatuuronderzoek;
    - Beheersing van geautomatiseerde informatiesystemen en informatiebeveiliging
    - Steunen op user-, application en general controls
    - Raadplegen van internetsites
- Interviews met accountants en IT-auditors;
    - Interviews met accountants over 'goed huisvaderschap'
    - Interviews met IT-auditors over 'goed huisvaderschap'

  Voor de interviews met accountants en IT-auditors hebben wij een enquête opgesteld.
- Het toepassen van praktijkkennis en houden van brainstormsessies;
- Vanuit de Code voor Informatiebeveiliging ISO 17999 een 'baseline' opstellen die een basis legt voor het 'goed huisvaderschap';
- Het verrichten van veldonderzoek onder 5 MKB-ondernemingen. Vraag hierbij is of deze voldoen aan het 'goed huisvaderschap'. Hiervoor hebben wij gebruik gemaakt van de genoemde, door ons opgestelde, enquête.

1.5 Leeswijzer

De scriptie is als volgt ingedeeld:



1. Inleiding
2. Interne beheersing van de geautomatiseerde informatiesystemen in het MKB
3. Het minimumniveau aan maatregelen om de informatiebeveiliging in het MKB te kunnen waarborgen
4. Toetsing in de praktijk (interviews, enquêtes en veldonderzoek)
5. Bevindingen en conclusie
6. Aanbevelingen

Hoofdstuk 2 Interne beheersing van de geautomatiseerde informatiesystemen in het MKB

Zoals in het vorige hoofdstuk beschreven, kent het MKB een aantal beperkingen qua schaalgrootte. Daardoor is het in veel gevallen niet mogelijk de beheersingsmaatregelen die in best practices (gebaseerd op grote ondernemingen) beschreven worden in volle omvang te implementeren voor MKB-ondernemingen.

Dit hoofdstuk gaat over het minimum IT-beheersingsniveau van informatiesystemen (general IT, application and user controls) in het MKB. De volgende onderwerpen zullen worden besproken: geautomatiseerde informatiesystemen in het MKB (paragraaf 2.1), kleinschalige automatisering (paragraaf 2.2), genereren van betrouwbare informatie in het MKB (2.3), beheersingsmaatregelen (paragraaf 2.4) en functiescheiding en controleerbaarheid (paragraaf 2.5).

2.1 Geautomatiseerde informatiesystemen in het MKB

Het begrip geautomatiseerde informatiesystemen (hierna afgekort als GIS) kan als volgt worden omschreven: een samenhangend en georganiseerd geheel aan hardware, software, documenten en de daarbij betrokken partijen, dat tot doel heeft het verzamelen, verwerken, produceren, opslaan en uitwisselen van informatie ten behoeve van specifieke bedrijfsprocessen en gebruikers. (bron: grondslagen IT-auditing; Fijneman, Roos Lingreen, Veltman, 2005). Deze omschrijving is universeel toepasbaar, ook in het MKB. Er wordt namelijk geen onderscheid gemaakt in de omvang van de onderneming en de complexiteit van het systeem.

Accountantskantoor Deloitte gebruikt de volgende classificatie om aan te geven of automatisering hoofd- of bijzaak is bij de ondersteuning van bedrijfsprocessen:

- Extent to which the entity use computers in the business
- Complexity of the computer processing environments
- Importance of computer systems to the entity's principal activities

Bovenstaande classificatie leidt tot de volgende onderverdeling:

1. **Dominant**
   If computers are used in all significant aspects of the business and the entity's ability to operate is highly dependent on computers of management is dependent on the use of computergenerated information to control the business. Most financial institutions and highly automated manufacturing or distribution entities are computer dominant.

2. **Significant**
   If entities have one or two complex systems that are used extensively and are important to the entity's principal business activities but, on the whole, the entity's use of computers is not dominant.

3. **Minor**
   If the extent of computer use is confined to relatively simple tasks that are of limited importance to the entity's principal business activities. Entities fall into this category if they have only one ore two computer applications that are relatively simple (e.g. payroll and general ledger).

Uit presentatie van de heer Drs. J. de Groot RA MPA van Deloitte " Symposium De accountant van morgen IT hoofdzaak of bijzaak" d.d. 21 september 2006 Tias.

Op basis van de classificatie van Deloitte valt het MKB onder de noemers 'significant' en 'minor'. De primaire bedrijfsproccessen van de meeste MKB-ondernemingen worden veelal in mindere mate of minder significante wijze ondersteund door automatisering. Ook is de complexiteit van de automatiseringsomgeving minder in vergelijking met die van grote ondernemingen.

2.2 Kleinschalige automatisering in het MKB

Typisch voor het MKB is de kleinschaligheid van de bedrijfsvoering. Dat geldt ook voor de automatisering. Het kenmerkende van kleinschalige automatisering is dat sprake is van een kleinschalige organisatie rondom de automatisering. Het heeft dus niets met de technische mogelijkheden van hard- en software te maken, maar alles met de organisatorische mogelijkheden.

NIVRA studierapport 17 noemt de volgende kenmerken van kleinschalige automatisering (bron: Kleinschalige automatisering en Accountant, NIVRA, 1984):

- De computer wordt gebruikt voor de gegevensverwerking van meerdere afdelingen (gebruikers) van de organisatie;
- De computer is als regel geplaatst bij gebruikersafdelingen en niet in een afzonderlijk rekencentrum;
- Weinig personen zijn fulltime belast met automatiseringswerkzaamheden;
- Het kenmerkende van kleinschalige automatisering is de omvang van de organisatie van de automatisering.

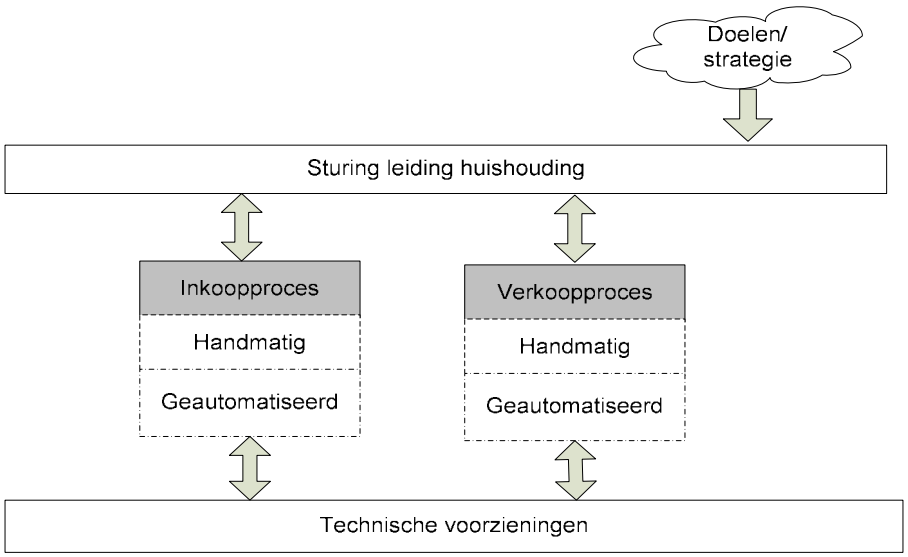
Dit heeft een aantal consequenties voor de kwaliteitsaspecten van de informatievoorziening die verderop in dit hoofdstuk aan bod zullen komen.

2.3. Genereren van betrouwbare informatie in het MKB

De leiding, de gebruikers en de auditor van een huishouding wensen te steunen op betrouwbare informatie uit het geautomatiseerd informatiesysteem. Iedere partij heeft met deze informatie zijn eigen doel. De organisatie wenst zijn organisatiedoelstelling te halen en daarover geïnformeerd te worden. De auditor wenst te steunen op betrouwbare informatie voor het controleren van het informatiesysteem.

Onder betrouwbaarheid verstaan wij in deze scriptie de controleerbaarheid van het GIS en de juiste, volledige en tijdige verwerking van de gegevens, gerealiseerd door geautoriseerde gebruikers.

In het MKB komt informatie binnen een bedrijfsproces met name tot stand door een combinatie van handmatige en geautomatiseerde handelingen. In de figuur hieronder geven we schematisch de mix weer van geautomatiseerde en handmatige handelingen voor een handelsonderneming.



(Oorspronkelijke weergave bewerkt uit de AA in een (kleinschalig) geautomatiseerde omgeving, 2002)

Een onderdeel van het inkoopproces dat handmatig uitgevoerd zou kunnen worden is bijvoorbeeld de bestellingenadministratie. Een geautomatiseerd onderdeel van het inkoopproces is bijvoorbeeld de crediteurenadministratie. Het geautomatiseerde onderdeel kan alleen worden uitgevoerd door inzet van technische voorzieningen zoals software, hardware en datacommunicatie.

Stelsel van interne beheersingsmaatregelen
Voor een betrouwbare verwerking van gegevens, zowel handmatig als geautomatiseerd, moet de onderneming een stelstel van interne beheersingsmaatregelen (controls) invoeren (al dan niet op basis van een risicoanalyse). Deze controls kunnen betrekking hebben op de gehele organisatie of op een specifiek bedrijfsproces. De controls voor de gehele organisatie zijn randvoorwaardelijk van aard en kunnen eveneens worden onderverdeeld in een handmatig en geautomatiseerd aspect. Voorbeelden van handmatige controls zijn de inrichting van de functiescheidingen en het opstellen van beleidsrichtlijnen. Voorbeelden van geautomatiseerde controls zijn change management en toegangsbeveiligingsmaatregelen.

2.4 Beheersingsmaatregelen

Aan een informatiesysteem dienen kwaliteitseisen te worden gesteld. De belangrijkste eisen zijn volgens ons: beschikbaarheid, integriteit, exclusiviteit en controleerbaarheid. Deze eisen gelden in essentie zowel voor grote ondernemingen als voor het MKB.

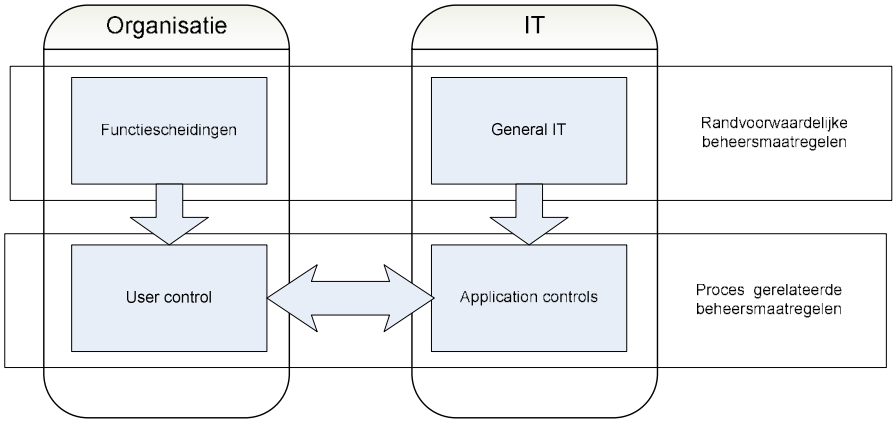
NIVRA-geschrift 53 (1989) vertaalt deze kwaliteiseisen als volgt:

- **Beschikbaarheid**
  De ongestoorde voortgang van de informatieverwerking.
- **Integriteit**
  De informatie is in overeenstemming met het afgebeelde deel van de realiteit en niets is achtergehouden of verdwenen.
- **Exclusiviteit**
  De beperking van de bevoegdheid en mogelijkheid tot muteren, uitlezen, kopiëren of kennisnemen (van informatie en van andere systeemcomponenten) tot een gedefinieerde groep van gerechtigden.
- **Controleerbaarheid**
  Hierbij gaat het primair om de mogelijkheid voor de mens om vast te stellen hoe het informatiesysteem en zijn componenten zijn gestructureerd.

Om aan deze kwaliteitseisen te voldoen, dient de organisatie beheersingsmaatregelen te treffen. We maken voor deze beheersingsmaatregelen onderscheid in general IT controls, application controls en user controls.

2.4.1 General IT controls

General IT controls zijn het fundament voor de applications controls en User controls. Ter illustratie hiervan is in onderstaand schema de samenhang tussen general IT controls, application controls en user controls opgenomen.



Bron: college sheets IT-audit opleiding VU,2007)

Onder general IT controls wordt verstaan .
Controls that relate to all or many computerized accounting activities, such as those relating to the plan or organization of data procecessing activities and the separation of incompatible functions. (Bron: Accounting Information Systems, 2006)

General IT controls bestaat volgens de gebruikelijke literatuur uit de volgende onderdelen:

- IT-beleid en -management (informatie, automatisering en beveiligingsbeleid)
- Change management
- Fysieke maatregelen
- Logische toegangsbeveiliging
- Continuïteit en operationeel beheer

Hieronder zullen we een aantal onderdelen kort toelichten. In hoofdstuk 4 worden alle onderdelen nader toegelicht.

Change management
Change management is een van de belangrijkste onderdelen van de general IT controls. Dit proces legt namelijk de basis voor de voortdurende werking van de application controls in het geautomatiseerd systeem. Gebruikers dienen de wijzigingen aan het geautomatiseerd informatiesysteem te testen en accepteren. Indien MKB-organisaties zelf software ontwikkelen, is het van belang dat functiescheiding bestaat tussen het ontwikkelen, testen en accepteren. In het MKB wordt echter voornamelijk gebruikgemaakt van standaardprogrammatuur.

Bij aankoop van standaardprogrammatuur verschuift de aandacht van het ontwikkelen naar het selecteren van een betrouwbare leverancier (die beproefde software biedt).

Een punt van aandacht is dat veel standaardsoftware de mogelijkheid heeft instellingen (parameters) zodanig te veranderen dat deze invloed heeft op de werking van het

toepassingprogramma. Het wijzigen van parameters dient daarom op dezelfde procedurele wijze te worden behandeld als de (eigen) systeemontwikkelingsactiviteiten.

Logische toegangsbeveiliging
Logische toegangsbeveiliging bestaat uit de organisatorisch en softwarematig getroffen beveiligingsmaatregelen om ongeautoriseerde toegang tot het besturingsysteem en netwerk te voorkomen.

In het MKB zijn verschillende besturingsystemen in gebruik die ieder weer hun eigen kenmerken hebben. Het komt daarbij regelmatig voor dat het beheer van het besturingsysteem en netwerk is uitbesteed aan derden. Dit betekent dat de onderneming hiervoor procedures opgesteld moet hebben aan welke taken en verantwoordelijkheden de beheerder van dit systeem zich dient te houden. De afspraken zullen in een service level agreement (SLA) moeten worden vastgelegd. De algemene eisen waaraan de logische toegangsbeveiliging dient te voldoen zijn:

- Identificatie: het GIS moet kunnen vaststellen wie de gebruiker is.
- Authenticatie: de gebruiker dient aan te tonen dat hij ook degene is die hij beweert te zijn via zijn identificatie.
- Autorisatie: het GIS dient te beschikken over de mogelijkheid om bevoegdheden te geven aan de gebruiker die hij voor zijn functie nodig heeft.
- Rapportering: het systeem moet over faciliteiten beschikken om het gebruik daarvan te kunnen controleren.

Het GIS dient inzicht te geven in het gebruik van de toegangsbeveiliging waardoor deze maatregel controleerbaar wordt. De wijzigingen in de identificatie en autorisatiegegevens moeten worden vastgelegd. Dit geldt eveneens voor de activiteiten van de gebruikers met betrekking tot het gebruik van de gegevens en programma's. Het systeem dient te beschikken over loggingsfaciliteiten die automatisch een vastlegging maakt van aangebrachte wijzigingen. Hierdoor is het mogelijk de volledigheid van aangebrachte wijzigingen achteraf vast te vaststellen.

2.4.2 Application controls

Onder application controls wordt verstaan:
Controls that relate to the data input, files, programs, and output of a specific computer application. (Bron: Accounting Information Systems, 2006)

Invoercontroles zijn ontworpen voor een betrouwbare input van gegevens.
Voorbeelden hiervan zijn:

- Bestaanbaarheidscontroles;
  Bestaat het artikelnummer en debiteurennummer?
- Volledigheidscontroles;
  Zijn alle velden ingevoerd?
- Juistheidsontroles;
  Controle op invoer autorisatie en/of unieke factuurnummers.

Overige geprogrammeerde controles zijn ondermeer:

- Stuurparameters;
  Instellingen en parameters die bepalend zijn voor het bedrijfsproces binnen de applicatie. Een voorbeeld hiervan is de signaleringlijst van het overschrijden van ingestelde tolerantiegrenzen.
- Stambestanden;
  Dit betreft de toegang en beheer van de stamgegevens binnen de applicatie.
- Overrulen van het systeem;

Dit zijn handelingen waarvoor speciale bevoegdheid nodig is om voorgeprogrammeerde controls te omzeilen. Een voorbeeld hiervan is het accepteren van het overschrijden van een kredietlimiet bij transacties.
- Competentietabel;
  De controletechnische functiescheiding uit de bedrijfsprocessen dient doorgevoerd te zijn in de functies in de applicatie. Deze wordt verder uitgewerkt in het onderdeel functiescheiding binnen het geautomatiseerd systeem.
- Interfaces;
  Dit zijn verbindingen die datastromen mogelijk maken uit verschillende applicaties. Een voorbeeld hiervan is het inlezen van informatie uit een kassasysteem in het grootboek.
- Doorlopende nummering controles.
  Verwerkingverslagen, bijvoorbeeld in het grootboek, dienen te zijn voorzien van een doorlopende nummering voor het vaststellen van de volledigheid hiervan.

Logische toegangsbeveiliging in relatie tot de applicatie behoort tot de onvervangbare maatregelen van interne controle. In feite is dit een van de belangrijkste maatregelen. Immers indien dit niet adequaat is geregeld in de applicatie, resteert voor de MKB-onderneming alleen nog de functiescheiding buiten de applicatie om alsnog betrouwbare informatie te verkrijgen. Met een voorbeeld uit de MKB-praktijk zullen wij dit verduidelijken. Het hoofd administratie heeft binnen de applicatie zowel registrerende als autoriserende rechten binnen de inkoopfunctie. Hierbij is sprake van functievermenging. De directeur van de onderneming betaalt via telebanking de inkoopfacturen. De directeur neemt voordat hij het betaalbestand autoriseert de bijbehorende fysieke inkoopfacturen door met de onderliggende stukken. Door deze beheersmaatregel kunnen leemtes in de logische toegangsbeveiliging alsnog worden gecompenseerd.

Deze aspecten worden verder uitgewerkt in paragraaf 2.5 functiescheiding en controleerbaarheid van het systeem.

2.4.3 User controls

De betrouwbaarheid van de uitkomsten van de gegevensverwerking wordt vastgesteld op basis van de informatiecontroles gebaseerd op een fundament van geprogrammeerde controles en internal controles binnen de automatiseringsorganisatie. De geprogrammeerde controles en general ICT controles zijn de voorwaarde om informatiecontroles te kunnen uitvoeren (Bron: J.C. Boer, compact 1999). Deze informatiecontroles worden uitgevoerd door de gebruikers**.**

Onder user controls wordt verstaan: handmatig door de gebruiker van het systeem uitgevoerde handelingen. Deze maatregelen zijn specifiek ontworpen om de volledigheid, juistheid en geldigheid van de transacties te bewaken, zoals het op elkaar aansluiten van lijsten uit het systeem. Voor de controleerbaarheid van deze maatregelen is het van belang dat ze zichtbaar worden vastgelegd. In het MKB komt het regelmatig voor dat aan gebruikers van het GIS meer rechten zijn toegekend dan noodzakelijk is. Hierdoor is het risico aanwezig van doorbreking van functiescheiding binnen de organisatie, waardoor extra handmatige controles nodig zijn om deze leemte te compenseren.

2.5 Functiescheiding en controleerbaarheid

In deze paragraaf komt de door de organisatie te treffen functiescheiding en controleerbaarheid van het geautomatiseerd systeem aan de orde. Dit is voor de auditor van belang of de organisatie wel controleerbaar is.

Aan de orde komt automatisering en gebruikersorganisatie, competentietabel, accounting en audittrail en netwerk van controletotalen.

2.5.1 Automatisering en gebruikersorganisatie

Er dient primaire functiescheiding te zijn tussen de automatiserings- en gebruikersorganisatie. (Bron: leerboek accountantscontrole Frielink, de Heer, 1993).
De automatiseringsorganisatie heeft de mogelijkheid(doch niet de bevoegdheid) om wijzigingen in de gegevens aan te brengen. (Bron: leerboek accountantscontrole Frielink, de Heer, 1993).
De automatiseringsorganisatie draagt zorg voor de integriteit van de opslag en de verwerking, transport en toegankelijkheid van de gegevens. Ook moet de technische infrastructuur gewaarborgd worden. De verantwoordelijkheden van de automatiseringsfunctie voor een betrouwbare informatievoorziening zijn:

- Ongeautoriseerden mogen geen toegang hebben tot de gegevens van de gebruikers.
- De technische infrastructuur, systeem en applicatieprogrammatuur mogen niet ongeautoriseerd kunnen worden veranderd.

In het MKB heeft de automatiseringsorganisatie een beperkte omvang, veelal bestaande uit een systeembeheerder. (Bron: de AA in een (kleinschalig) geautomatiseerde omgeving, 2002). Deze systeembeheerder beschikt veelal over vergaande bevoegdheden tot het systeem, terwijl het niet altijd nodig is dat hij hier continue over beschikt ('het need to know'-principe). Dit kan worden voorkomen door een kluisprocedure in te voeren. Voorts kan aan de directie van de onderneming periodiek een opgave worden verstrekt van de bevoegdheden waarover de systeembeheerder beschikt. De systeembeheerder geniet overigens een vertrouwensfunctie binnen de onderneming net als bijvoorbeeld de procuratiehouder.

De leiding van de huishouding zou een afweging moeten maken welk belang de systeembeheerder in het MKB zou kunnen hebben bij het veranderen van de gegevens. Wijzigingen die de systeembeheerder aanbrengt dienen te worden gelogd. Achteraf kunnen hierop dan nog detectieve controlemaatregelen uitgevoerd worden.

De gebruikersorganisatie heeft betrekking op de toegang van de gebruikers tot de gegevens. Zij zijn de eigenaar van de applicatie en gegevens. De gebruikers hebben gebruikerscontroles ontworpen om de betrouwbaarheid van de informatievoorziening te bewaken. (Bron: Compendium van de Accountantscontrole deel 1, Westra en Mooijekind, 1995)
De controles kunnen worden onderscheiden in:

- Het vaststellen van de juistheid en volledigheid van de gegevensverwerking.
- De integriteit van de opslag van de gegevens.

Beide controles zijn vervolgens onder te verdelen in vaste en variabele gegevens.

2.5.2 Competentietabel

Het GIS dient te beschikken over de mogelijkheid om die bevoegdheden toe te kennen aan een gebruiker die hij uit hoofde van zijn functie nodig heeft. Deze worden vastgelegd in een competentietabel (ook wel autorisatietabel genoemd). De competentietabel moet worden 'vertaald' naar rechten binnen het GIS. De wijze van realisatie verschilt per (type) applicatie. Per (groep van) gebruiker(s) worden de raadpleeg-, invoer-, en mutatiebevoegdheden vermeld.

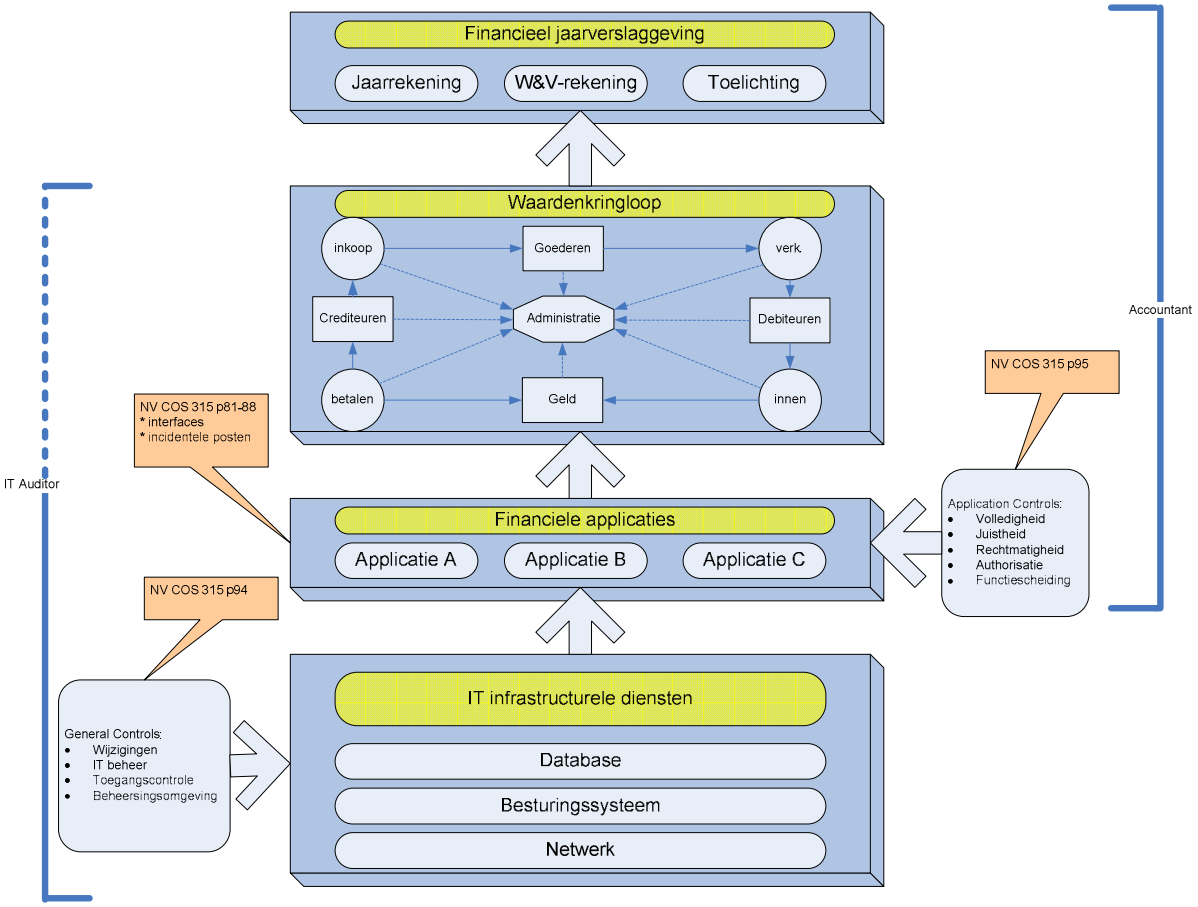
2.5.3 Accounting en audit trail

Transacties binnen een geautomatiseerd systeem dient men administratief te kunnen volgen en ze dienen te zijn voorzien van controleerbare vastleggingen. (Bron: Compendium van de Accountantscontrole deel 1, Westra en Mooijekind, 1995). Het administratief kunnen volgen

van transacties wordt het 'accounting trail' genoemd. Een voorbeeld hiervan is het volgen vanaf een verkooporder (het brondocument) tot en met de betaling van een verkoopfactuur in het geautomatiseerd systeem. De audit trail heeft betrekking op de mogelijkheid om transacties in het geautomatiseerd systeem te kunnen controleren.

2.5.4 Netwerk van controletotalen

De applicatie dient bij voorkeur te zijn voorzien van een totaal aan verbandscontroles. Deze controles worden ook wel een netwerk van controletotalen genoemd. Hiermee kan de gebruiker de juiste en volledige gegevensverwerking vaststellen. Verbandscontoles komen in verschillende verschijningsvormen voor. Onderstaand schema geeft specifiek de relatie van de IT-beheersingsmaatregelen in het kader van de jaarrekening (controle) weer. Hierbij hebben wij eveneens de scope van de werkzaamheden van de IT-auditor en de accountant weergeven alsmede de referentie naar de relevante standaarden.



In het volgende hoofdstuk zullen de hier behandelde theoretische kaders voor de inrichting van de minimale beheersingsmaatregelen worden vertaald naar praktische eisen op het gebied van informatiebeveiliging in het MKB.

Hoofdstuk 3 Het minimumniveau aan maatregelen om de informatiebeveiliging in het MKB te waarborgen

In dit hoofdstuk zal ingegaan worden op de vraag waarom MKB-ondernemingen aandacht aan informatiebeveiliging dienen te besteden. In paragraaf 3.1. wordt de informatiebeveiliging in het MKB behandeld. In paragraaf 3.2 zullen wij de code voor informatiebeveiliging behandelen. Deze paragraaf legt de basis voor belangrijke beveiligingsmaatregelen die de MKB-onderneming volgens ons in zou kunnen voeren. In hoofdstuk 4 wordt een selectie van het minimum aan beveiligingsmaatregelen geselecteerd vanuit de code voor informatiebeveiliging en hoofdstuk 2. Deze beveiligingsmaatregelen vormen de basis voor het 'goed huisvaderschap'.

3.1 Informatiebeveiliging in het MKB

Het MKB onderscheidt zich van grote ondernemingen door ondermeer: kleinschalig in personele omvang, plattere structuur, dominante rol van de ondernemer, pragmatisch, informeel en direct resultaat gericht. Veel informatiesystemen zijn niet ontworpen met het oog op veiligheid (code voor informatiebeveiliging 2005). Het treffen van veiligheidsmaatregelen kost voor een MKB-ondernemer geld en heeft daarom geen prominente plaats in de bedrijfsvoering. De ondernemer in het MKB die direct resultaat wil zien zal zich afvragen 'waarom moet ik in informatiebeveiliging investeren?'.

Naast het feit dat het MKB fors investeert in ICT zullen de volgende voorbeelden laten zien waarom informatiebeveiliging ook in het MKB noodzakelijk is.

Informatiebeveiliging is noodzakelijk in het MKB (1)
Uit onderzoek in opdracht van het Digibewust programma van het ministerie van EZ is het volgende naar voren gekomen. Tweederde van de ondernemers denkt dat de databeveiliging in hun bedrijf goed tot zeer goed is geregeld. Uit nieuw onderzoek blijkt dat ze hierbij toch vaak een onjuist beeld hebben. Zo erkent 82 procent van de ondernemers dat ze geen formele afspraken over digitale beveiliging hebben. Niet meer dan 22 procent traint hun medewerkers in het veilig beheren van data. Ze laten dit dan vaak over aan het persoonlijke inzicht en de goede wil van de medewerkers. Bovendien heeft een op de vijf bedrijven geen enkel back-up beleid, waardoor het risico van dataverlies op de loer ligt. 22 procent van de ondervraagde MKB'ers heeft een of meerdere keren te maken gehad met digitale incidenten. Veelvoorkomende gevallen zijn diefstal van pc of laptop (56 procent), virusinfectie (54 procent), een defect in de infrastructuur (31 procent) of een spywareprobleem (30 procent). Juist de ondernemers die zeggen goed op de hoogte te zijn van beveiliging, blijken vaker een incident te hebben meegemaakt.
(bron: Computable 04-07-2007)

Informatiebeveiliging is noodzakelijk in het MKB (2)
Beveiliging is bij het midden- en kleinbedrijf rampzalig slecht geregeld. De ICT-sector moet zich dat aantrekken. De server is weggezet onder de trap. De wachtwoorden staan op gele velletjes aan de zijkant van de kast. Bovenop ligt een back-uptape die dateert van maanden her. De virusscanner wordt nooit geüpdatet. Beveiliging van ICT-systemen is geen issue bij het mkb, zo blijkt op het eNederland Congres.
(bron: Automatisering Gids, 16-11-2006)

Informatiebeveiliging is noodzakelijk in het MKB (3)
Uit onderzoek van Syntens in 2006 onder vijftig MKB-ondernemingen in Flevoland blijkt dat de ondernemingen unaniem aangeven in hoge mate afhankelijk te zijn van ICT en van internet. Indien wij deze lijn landelijk doortrekken betekent dit dat ICT van essentieel belang is voor de continuïteit van de bedrijfsvoering van MKB-ondernemingen.

Doordat MKB-ondernemingen afhankelijker van ICT zijn geworden, zijn zij hierdoor kwetsbaarder voor bedreigingen van de informatiebeveiliging. Deze bedreigingen kunnen bestaan uit allerlei bronnen, zoals computerfraude, spionage, sabotage, vandalisme en technische oorzaken.

De vraag is of MKB-ondernemers zich van deze bedreigingen bewust zijn. Bewustwording van de noodzaak tot beveiliging bij het management is onontbeerlijk, maar ontbreekt nog vaak. (bron: Publicatie wie maakt u management bewust, KWINT 2004)

Om de schade door de bedreigingen te minimaliseren dient de MKB zijn informatie te beveiligen. Informatiebeveiliging is het inrichten en onderhouden van een stelsel van maatregelen om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie en informatiesystemen te waarborgen (bron: grondslagen IT-auditing; Fijneman, Roos Lingreen, Veltman, 2005)

Voor elke MKB-onderneming kan de nadruk van de kwaliteitsbegrippen beschikbaarheid, integriteit en continuïteit op een ander niveau liggen. Voor de ene MKB-onderneming is beschikbaarheid belangrijk en voor de andere vertrouwelijkheid. MKB-ondernemingen dienen naast betrouwbaarheid en beschikbaarheid voor de eigen bedrijfsuitvoering ook aandacht te besteden aan wettelijke eisen van beveiliging. Wet beveiliging van persoonsgegevens (WBP) is hier een voorbeeld van.

Bij informatiebeveiliging in het MKB wordt vaak gedacht aan de financiële informatie in de database van een financieel pakket. In het MKB dient ook aandacht te worden besteed aan bewerkte informatie vanuit de financiële software tot management rapportages. Deze vertrouwelijke informatie, veelal in excel- of wordformaat, staat in directories die onbedoeld voor veel medewerkers toegankelijk zijn. Dit geldt eveneens voor platte tekst bestanden die bij de overdracht van gegevens van de ene applicatie naar de andere applicatie worden ingelezen. De leiding van de huishouding dient zich van dit risico bewust te zijn. Informatie kan in ongerede raken door de mens, techniek en door externe oorzaken. De MKB-ondernemer die zijn informatie wil beveiligen dient te analyseren welke risico's de informatie kunnen bedreigen. De MKB-ondernemer kan een risico immers accepteren, verminderen, vermijden, of delen. Indien deze bekend zijn, kunnen beveiligingsmaatregelen genomen worden. Welke maatregelen hangt onder meer af van de waarde die de informatie heeft voor deze organisatie en de kosten en baten overweging die met deze maatregelen gemoeid zijn. In de praktijk zal elke onderneming in het MKB andere beveiligingsmaatregelen treffen. De te treffen beveiligingsmaatregelen zijn ondermeer afhankelijk van de cultuur en omvang van de organisatie, de branche etc.

Overbeek e.a. (Informatiebeveiliging 1999) vragen zich ook af wat informatie voor 'u' waard is. Risico's dienen bewust te worden genomen. Beveiligingsmaatregelen kunnen worden ingedeeld naar de middelen die ze gebruiken organisatorisch, procedureel, fysiek en technisch. Per maatregel wordt een effect nagestreefd. Deze kunnen worden ingedeeld in de dreiging waarin ze opereren: preventief, defectief, repressief, correctief en evaluatie.

3.2 De code voor informatiebeveiliging

In deze paragraaf zullen wij nader ingaan welke beveiligingsmaatregelen de MKB-onderneming zou moeten treffen in het kader van goed huisvaderschap.

Beveiligingsmaatregelen kunnen worden ingedeeld in basismaatregelen en specifieke maatregelen. Basismaatregelen zijn van toepassing op vrijwel elke onderneming. Specifieke beveiligingsmaatregelen zijn op maat gemaakt voor de organisatie en uitgevoerd door of namens de leiding van de huishouding door middel van risicobeoordeling.
De basismaatregelen zijn te beschouwen als een subset van uitgangspunten die de leiding van de onderneming minimaal zou moeten treffen om te kunnen voldoen aan informatiebeveiliging.

Om structuur aan te brengen in het basisniveau van beveiligingsmaatregelen hebben wij gekozen voor 'de code voor informatiebeveiliging' (ISO/IEC 17799:2005).

De code bestaat uit vijftien hoofdstukken, elf hoofdcategorieën en behelst ruim 130 beveiligingsbeheersmaatregelen. Vanuit deze beheersmaatregelen zullen wij per hoofdstuk belangrijke maatregelen voor MKB-ondernemingen bespreken.

De elf hoofdcategorieën zijn:

1. Beveiligingsbeleid (paragraaf 3.2.1)
2. Organisatie van informatiebeveiliging (paragraaf 3.2.2)
3. Beheer van bedrijfsmiddelen (paragraaf 3.2.3)
4. Beveiliging van personeel (paragraaf 3.2.4)
5. Fysieke beveiliging en beveiliging van de omgeving (paragraaf 3.2.5)
6. Beheer van communicatie- en bedieningsprocessen (paragraaf 3.2.6)
7. Toegangsbeveiliging (paragraaf 3.2.7)
8. Verwerving, ontwikkeling en onderhoud van informatiesystemen (paragraaf 3.2.8)
9. Beheer van informatiebeveiligingsincidenten (paragraaf 3.2.9)
10. Bedrijfscontinuïteitsbeheer (paragraaf 3.2.10)
11. Naleving (paragraaf 3.2.11)

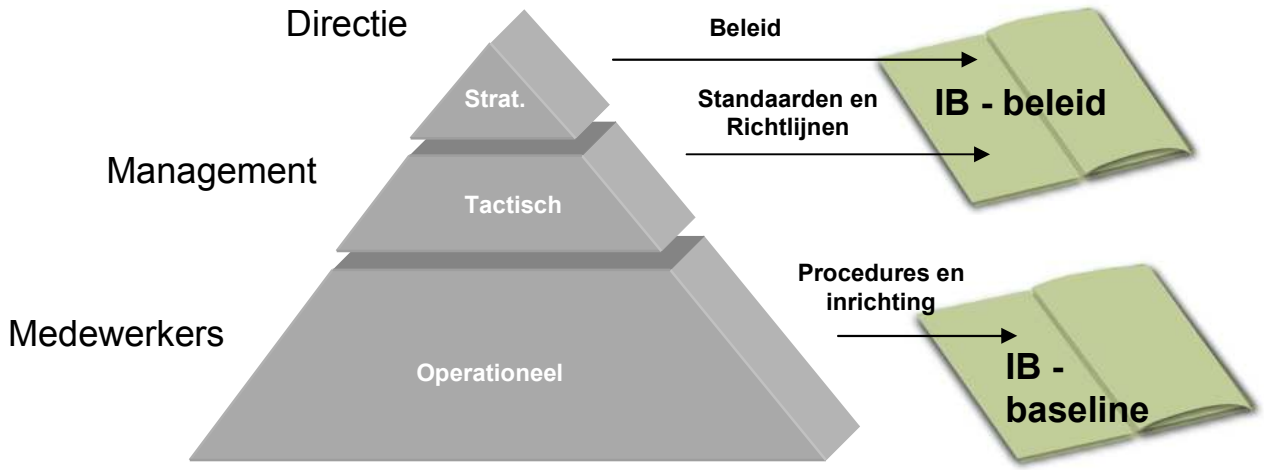
3.2.1 Beveiligingsbeleid

De ondernemingsleiding dient door middel van het opstellen van het informatiebeveiligingsbeleid in hoofdlijnen aan te geven op welke wijze zij automatisering in haar organisatie wil toepassen. Dit beleid dient in lijn te zijn met de bedrijfsdoelstellingen. Het beveiligingsbeleid dient op alle niveau's in de organisatie te worden doorgevoerd om zo de bedrijfsdoelstellingen te realiseren.

Doelstelling
De leiding van de huishouding sturing en ondersteuning geven ten behoeve van informatiebeveiliging.

De minimale eisen en onderwerpen van het beveiligingsbeleid zijn:
- Welke bedrijfsprocessen ondersteund worden met automatisering;
- Het gewenste niveau van beveiliging en welke beheersmaatregelen genomen dient te worden;
- Het beleid en het belang daarvan op een geschikte wijze kenbaar te maken aan alle werknemers en overige personen die toegang hebben tot het informatiesysteem;
- Algemene verantwoordelijkheid van de managers en medewerkers ten behoeve van informatiebeveiliging;
- Een exemplaar van eisen en voorschriften met betrekking tot de beveiliging dient beschikbaar te zijn voor zowel werknemers als derden die toegang hebben tot het informatiesysteem;
- De ter beschikking staande middelen voor het adequaat uit kunnen voeren van de taken van de medewerkers;

- Inrichting van een beveiligingsorganisatie;
- Hoe het beleid wordt nageleefd.



De code raakt elk niveau van de organisatie.
(bewerkte afbeelding van presentatie GVIB, 2005 Kelvin Rorive)

3.2.2 Organisatie van informatiebeveiliging

Nu de leiding een beleidsdocument in hoofdlijnen heeft opgesteld is het noodzakelijk dat er een organisatie wordt samengesteld die zorgt voor de verdere inrichting en handhaving van het beveiligingsbeleid.

Doelstelling
Het beheren van de informatiebeveiliging binnen de organisatie. Deze organisatie dient te zorgen voor een duidelijke koers van de informatiebeveiliging. De beveiligingsorganisatie dient te worden gevormd uit leden van het managementteam van de onderneming. Alle leden van dit team zijn namelijk verantwoordelijk voor de beveiliging van de informatie.

De structuur van de beveiligingsorganisatie in het MKB zou bij voorkeur moeten bestaan uit een vertegenwoordiger van de gebruikersorganisatie, automatiseringsorganisatie en de directie. Een manager uit de gebruikersorganisatie zou een functionaris uit het primaire proces kunnen zijn, bijvoorbeeld verkoop. De systeembeheerder zou de automatiseringsorganisatie kunnen vertegenwoordigen. Door de gebruikersorganisatie als eigenaar van de gegevens en de systeembeheerder als technische functionaris in de organisatie te betrekken ontstaat hierdoor een evenwichtig stuurorgaan.

De aan de beveiligingsorganisatie gestelde taken en eisen zijn:
- Het toewijzen van verantwoordelijkheden voor de beveiliging van gegevens en het geautomatiseerde systeem aan functionarissen.
- Het instellen van initiërende, sturende en controlerende beveiligingstaken binnen de diverse afdelingen in de onderneming.
- Het opstellen en definiëren van beveiligingsprocedures waar werknemers en overige gebruikers van het geautomatiseerde systeem aan moeten voldoen.
- De coördinatie, het uitvoeren en eventuele bijstelling van het beveiligingsbeleid en maatregelen.
- Goedkeuren van nieuwe informatievoorzieningen.
- De beveiligingsvoorwaarden van de organisatie op laten nemen in contracten met derden.

3.2.3 Beheer van bedrijfsmiddelen

De onderneming dient een duidelijk beeld te hebben van welke belangrijke informatie en bedrijfsmiddelen zij tot haar beschikking heeft. Deze informatie en middelen dienen op een passende wijze beschermd te worden.

Doelstelling
Een adequate bescherming en beheer van bedrijfsmiddelen.

De te stellen eisen aan het beheer van bedrijfsmiddelen zijn:

- Informatie-bedrijfsmiddelen dienen te worden verantwoord en toegewezen aan een eigenaar zodat deze hiervoor verantwoordelijk kan worden gesteld.
- Er dient een inventarisatieoverzicht aanwezig te zijn welke informatie-bedrijfsmiddelen de organisatie heeft.
- De onderneming dient de belangrijkheid van haar bedrijfsmiddelen te classificeren.
- Er dienen duidelijke richtlijnen te zijn hoe de bescherming van deze bedrijfsmiddelen uitgevoerd moet worden en wie hiervoor verantwoordelijk is. Hierdoor kan het juiste niveau van beveiligingsmaatregelen genomen worden.

3.2.4 Beveiliging van personeel

Het personeel en derden die toegang hebben tot de gegevens en ICT-infrastructuur zijn een belangrijke schakel in het informatiebeveiligingsbeleid. Aandacht voor het personeel en derden is noodzakelijk omdat zij tenslotte hiermee werken.

Doelstelling
Personeel en externe gebruikers bewust maken zodat zij hun verantwoordelijkheden voor informatiebeveiliging begrijpen. Deze gebruikers in staat stellen hun kennis en ervaring te benutten om beveiligingstaken naar behoren uit te voeren teneinde de beveiligingsrisico’s te verminderen.

De volgende eisen en maatregelen kunnen aan het personeel worden gesteld:

- In arbeidscontracten dient te worden opgenomen wat de functies en taken zijn voor het personeel en dat zij moeten instemmen met een geheimhoudingsverklaring. Voorts dient hierin te worden opgenomen dat zij verantwoordelijk zijn voor het uitvoeren van beveiligingsrichtlijnen die door of namens de directie zijn opgesteld. Het niet nakomen van deze richtlijnen zal disciplinair bestraft moeten worden.
- Regelmatig bewustwording van informatiebeveiliging te krijgen door dit bijvoorbeeld in periodieke beoordelingsgesprekken en of personeelsmedelingen te behandelen.
- Het laten screenen van nieuwe personeelsleden die toegang krijgen tot gevoelige informatie. In het MKB kan dit bijvoorbeeld eenvoudig door enkele referenties te raadplegen en of een verklaring van goed gedrag te eisen.
- Gebruikers dienen getraind te worden in het bewust zijn van de bedreigingen en van belang van de informatiebeveiliging.
- Gebruikers dienen te worden aangemoedigd risico’s met betrekking tot de beveiliging te melden.

3.2.5 Fysieke beveiliging en beveiliging van de omgeving

Als onbevoegde personen zich zo maar, zonder beperking, op plaatsen in de organisatie kunnen begeven, is de kans groot dat de informatie in gevaar komt of dat informatiesystemen worden verstoord. Daarom dient de organisatie voor belangrijke ICT-voorzieningen en informatie hiervoor, gepaste fysieke maatregelen te treffen om dit risico te verminderen.

Doelstelling
Het voorkomen van fysieke toegang van onbevoegden tot ruimtes die kunnen leiden tot schade en of verstoring van de informatievoorziening.

De eisen en maatregelen die de organisatie in dit kader moeten treffen zijn:

- Het terrein en of gebouw van de onderneming dient fysiek beveiligd te zijn.
- Ruimten in de organisatie waar kritische informatie en informatiesystemen bevinden dienen te worden afgesloten voor onbevoegden.
- De onderneming dient voorzieningen te treffen zodat zij weet wie de bezoekers zijn en waar zij zich bevinden.
- Gevoelige en kritische informatie dient na werktijd in afgesloten ruimten te worden opgeborgen.

3.2.6 Beheer van communicatie- en bedieningsprocessen

De informatie binnen het geautomatiseerde systeem komt tot stand door middel van de inzet van hardware- en softwarecomponenten. Deze componenten dienen op een geschikte wijze te worden bediend en beheerd door de gebruikers van het systeem. In het MKB heeft de afdeling systeembeheer, die veelal een bescheiden omvang heeft, hier een belangrijke taak in.

Doelstelling
Het waarborgen van een correcte en veilige bediening van de IT-middelen.

De eisen en maatregelen die de organisatie in dit kader moet treffen zijn:

- Er dienen schriftelijke procedures te worden opgesteld wie verantwoordelijk is voor het operationele beheer van de IT-middelen en hoe deze bediend moeten worden om een veilige en correcte bediening te verzekeren.
- Er dient functiescheiding te zijn tussen het beheer en de uitvoering van risicovolle taken die de informatie in het gevaar kunnen brengen.
- Voor de functiescheiding tussen de automatiserings- en gebruikersorganisatie verwijzen wij u naar paragraaf 5 van hoofdstuk 2.
- In het MKB zou in verband met de beperkte omvang in ieder geval een audit trail en of supervisie door of namens de directie van de activiteiten mogelijk moeten zijn.
- Indien het beheer van de IT-middelen aan derden is uitbesteed, dienen de gevolgen van de informatiebeveiliging beoordeeld te worden, omdat er gegevens kunnen worden beschadigd, verloren of ongeautoriseerd openbaar gemaakt kunnen worden.
- Procedures dienen te worden opgesteld en geïmplementeerd voor het ontwikkelen, testen en onderhouden van het systeem.
- Wijzigingen aan het systeem dienen te worden geregistreerd en goedgekeurd door bevoegden om de wijzigingen in dit systeem te beheersen.
- De onderneming dient een virusscanner te installeren en te onderhouden in verband met de bescherming tegen kwaadaardige programmatuur die de gegevens aan zouden kunnen tasten.
- Externe verbinding met derden dient beschermd te zijn (bijvoorbeeld met VPN).

- Informatiedragers behoren adequaat beveiligd te zijn.

3.2.7 Toegangsbeveiliging

De logische toegang tot de gegevens en IT-voorzieningen is de belangrijkste interne controlemaatregel voor de betrouwbaarheid van informatie, voor zowel de auditor als de onderneming. Door het niet goed nadenken over het verlenen van rechten kan de informatie ongewild worden benaderd door ongeautoriseerde gebruikers.

Doelstelling
Beheersen van de toegang tot informatie.

De eisen en maatregelen die de onderneming in dit kader dient te treffen zijn:

- Het toegangsbeleid dient te worden vastgesteld en gedocumenteerd op basis van de uitgangspunten 'wie mag wat benaderen' en 'wie autoriseert dit'.
- Het is hierbij van belang dat alleen die personen toegang krijgen tot informatie die zij voor hun functie nodig hebben ('need to know'-principe). Regels met betrekking tot toegangsbeveiliging dienen te worden ondersteund door duidelijke verantwoordelijkheden.
- De gebruikers van het systeem dienen geregistreerd en afgemeld te worden.
- De functiescheidingen in de organisatie dienen in lijn te zijn met de functiescheiding in het geautomatiseerd systeem. Zie hiervoor ook paragraaf 4 van hoofdstuk 2.
- Er dienen procedures en richtlijnen te zijn voor wie de bevoegdheden van de gebruikers met betrekking tot de benadering van het systeem beheert.
- Het systeem dient te zijn voorzien van toegangsbeveiligingsoftware met identificatie, authenticatie- en autorisatiefaciliteiten.
- In een toegangsapplicatie dient functiescheiding ingericht te zijn tussen de invoer en autorisatie van een transactie. Een nadere uiteenzetting van de logische toegangsbeveiliging is beschreven in hoofdstuk 2.

3.2.8 Verwerving, ontwikkeling en onderhoud van informatiesystemen

Reeds bij de ontwikkeling of bij de verwerving van een geautomatiseerd informatiesysteem zal al met de eisen van beveiliging van de organisatie rekening gehouden moeten worden.

Doelstelling
Beveiligingseisen opstellen voor nieuwe informatiesystemen.

De maatregelen en eisen die de onderneming in deze categorie minimaal zou moeten treffen zijn:

- Voor nieuwe informatiesystemen dient al voor de ontwikkeling en/of verwerving van informatiesystemen rekening te worden gehouden met de beveiligingseisen.
- Gegevens die ingevoerd worden in toepassingsystemen dienen te zijn voorzien van invoer, verwerking en uitvoercontroles om te bewerkstelligen dat deze gegevens juist en volledig zijn**.**
- Gevoelige gegevens dienen te worden beveiligd door middel van encryptie.
- Indien wijzigingen worden doorgevoerd aan het besturingsysteem, als gevolg van bijvoorbeeld patches, dienen de gevolgen van deze wijziging voor de beveiliging bekend te zijn. Deze wijzigingen aan het systeem dienen te worden bijgehouden in een wijzigingsregister.

3.2.9 Beheer van informatiebeveiligingsincidenten

Indien er zwakke plekken in de beveiligingsorganisatie zijn en/of beveiligingsincidenten door de gebruikers worden geconstateerd, is het van belang dat zij dit op een geschikte wijze melden aan de verantwoordelijken.

Doelstelling
Het zorg dragen voor een systeem voor het melden van gebeurtenissen op het gebied van informatiebeveiliging en zwakheden in informatiesystemen, zodat tijdig corrigerende maatregelen genomen kunnen worden.

De maatregel die in dit kader minimaal genomen dient te worden is:

- Zowel aan werknemers als aan derden dient op een geschikte wijze kenbaar te worden gemaakt dat al hetgeen de informatiebeveiliging van de organisatie in gevaar kan brengen direct wordt gemeld aan de juiste leidinggevende.

3.2.10 Bedrijfscontinuïteitsbeheer

Als door een calamiteit de gegevens, programmatuur of apparatuur uitvallen is het nodig dat de bedrijfsprocessen toch voortgezet kunnen worden. Deze categorie behandeld welke maatregelen minimaal hiervoor genomen dienen te worden.

Doelstelling
Onderbreken van bedrijfsactiviteiten tegengaan en kritische bedrijfsprocessen beschermen tegen de gevolgen van omvangrijke storingen in informatiesystemen om tijdig herstel te bewerkstelligen.

De maatregelen die minimaal genomen dienen te worden zijn:

- Er dienen procedures opgesteld te zijn over de back-up strategie en wie hier verantwoordelijk voor is. Het dient altijd mogelijk te zijn om gegevens die verloren zijn gegaan te herstellen met een back-up.
- Van de back-ups behoren meerdere generaties bewaard te worden.
- Back-ups dienen op een veilige plaats te worden bewaard.
- Periodiek dienen de back-ups getest te worden.

3.2.11 Naleving

Het opzetten en invoeren van een beveiligingsysteem heeft geen waarde als deze niet wordt gecontroleerd. Regelmatig zal moeten worden gecontroleerd of aan het beveiligingsbeleid en de geldende beveiligingsnormen wordt voldaan.

Doelstelling
Het voorkomen van schendingen van contractuele, wettelijke en beveiligingseisen.

De eisen die hieraan gesteld worden zijn:

- Er behoren procedures te zijn ingevoerd waarbij het niet toegestaan is onrechtmatig auteursrechtelijk materiaal te kopiëren of te gebruiken voor niet zakelijke doeleinden.
- Belangrijke bedrijfsdocumenten dienen te worden beschermd tegen diefstal, vernietiging of verlies overeenkomstig de wettelijke en eisen van het bedrijf.
- De onderneming dient privacygevoelige informatie te beschermen.
- Regelmatig dient er controle te zijn op de naleving van de uitvoering van het informatiebeveilingsbeleid en -normen.
- Er dienen richtlijnen te zijn aan de gebruikers van het ICT-systeem dat zij deze voorzieningen niet mogen misbruiken voor niet-zakelijke doeleinden.

Hoofdstuk 4 Selectie van het minimum aan beveiligingsmaatregelen voor het MKB

In hoofdstuk 3 zijn belangrijke beveiligingsmaatregelen voor MKB-ondernemingen behandeld volgens de code voor informatiebeveiliging. Het MKB dient een balans te vinden in de juiste invoering van beveiligingsmaatregelen. De invoering van teveel beveiligingsmaatregelen kost immers geld en kan de bedrijfsvoering verstoren. Voor het MKB is het volgens ons beter om een gering aantal basismaatregelen te implementeren die daadwerkelijk werken, dan een groot aantal maatregelen die niet of nauwelijks effect hebben. Bovendien werkt een beperkt aantal basismaatregelen laagdrempelig, waardoor deze eerder geaccepteerd zouden worden door MKB-ondernemingen.

Wij hebben tien maatregelen geselecteerd vanuit de code waaraan elke ondernemer in het MKB zou moeten voldoen zodat nog sprake is van goed huisvaderschap. Door middel van een enquête zijn deze maatregelen voorgelegd aan 25 gekwalificeerde professionals die in het MKB-veld werkzaam zijn. In de enquête is de mening over de ons opgestelde maatregelen gevraagd. Daarnaast is de lijst gehanteerd voor het praktische veldonderzoek onder 5 MKB-ondernemingen.

Het volgende minimum aan beveiligingsmaatregelen dient een MKB-ondernemer volgens ons op te stellen en te implementeren:

1. Classificeer de belangrijkste informatie en neem hiervoor passende maatregelen. Stel voorwaarden aan de continue beschikbaarheid.
2. Opstellen en implementeren van beveiligingshuisregels door/namens de directie waar elke gebruiker van het geautomatiseerde systeem aan dient te voldoen door middel van het tekenen van een verklaring.
3. Medewerkers en (directie) bewust maken van beveiliging.
4. Het toewijzen van verantwoordelijkheid voor beveiliging.
5. Installeren en actueel houden van antivirussoftware en firewall (indien de onderneming een verbinding heeft met het internet)
6. Het dagelijks maken en testen van back-ups en deze bewaren op een beveiligde plaats.
7. Het geautomatiseerde systeem dient te zijn voorzien van toegangsbeveiliging met identificatie-, authenticatie- en autorisatiefaciliteiten die aansluiten op de functiescheiding binnen de organisatie.
8. Het zorgen voor fysieke beveiliging voor de bedrijfsmiddelen.
9. Het registreren van aanpassingen aan het systeem op basis van autorisatie van de proceseigenaren (change management).
10. Het controleren of de beveiligingshuisregels worden nageleefd (monitoring).

De enquêtevraagstelling luidt als volgt:

Indien u tien basisbeveiligingsmaatregelen voor een geautomatiseerd systeem en informatiebeveiliging dient op te stellen voor een MKB-ondernemer, bent u het dan eens met bovenstaande maatregelen? Zo niet, kunt u dan aan deze lijst maatregelen toevoegen of weglaten, dit mogen er maximaal tien zijn.

4.1 Enquête- en veldonderzoek van de lijst met maatregelen

Uitgangspunten bij de invoering van basismaatregelen voor de MKB-ondernemingen dient te zijn:
(1) een zo een efficiënt mogelijk resultaat tegen de geringste inspanning, (2) deze dienen de bedrijfsvoering zo min mogelijk te verstoren en (3) de basismaatregelen zouden zonder risicoanalyse ingevoerd moeten worden, omdat de risico's in elke onderneming aanwezig zijn.

In dit hoofdstuk worden de uitkomsten van de enquête onder auditors en het veld onderzoek naar de praktische toepasbaarheid onder MKB-ondernemingen behandeld. De lijst van voorgestelde maatregelen hebben wij besproken in hoofdstuk 4. In paragraaf 4.2 worden de uitkomsten van de enquête besproken en in paragraaf 4.5 zal het onderzoek onder MKB-ondernemingen worden behandeld. Beide onderzoeken zijn gering van omvang aangezien dit anders niet realistisch was uit te voeren binnen de beschikbare tijd zoals deze binnen de opleiding is vastgesteld.

4.2 Het enquêteonderzoek onder auditors

Wij hebben vijfentwintig accountants en tien IT-auditors) uitgenodigd hun mening te geven over de voorgestelde lijst met tien beheersingsmaatregelen. Elf accountants en zes IT-auditors hebben gereageerd op onze uitnodiging. Het enquêteonderzoek is uitgevoerd in oktober 2007.

Alle auditors waren van mening dat de door ons voorgestelde lijst van maatregelen in opzet praktisch toepasbaar is voor MKB-ondernemingen. Drie accountants kunnen zich volledig in de lijst vinden en hadden geen opmerking. Wel vroegen zij zich af of er geen hiërarchie in de maatregelen aangebracht dient te worden.

Wij zullen de door ons voorgestelde lijst aanpassen indien de resultaten van de enquête hiertoe aanleiding geeft.

4.3 Respons op de voorgestelde maatregelen

Voorstel 1:
Classificeer de belangrijkste informatie en neem hiervoor passende maatregelen. Stel voorwaarden aan de continue beschikbaarheid.

- *Alle respondenten zijn het eens met deze maatregel.*

Voorstel 2:
Opstellen en implementeren van beveiligingshuisregels door/namens de directie waar elke gebruiker van het geautomatiseerde systeem aan dient te voldoen door middel van het tekenen van een verklaring.

- *Dit punt wordt gedragen door de meeste respondenten. Enkele zijn van mening dat deze maatregel gecombineerd kan worden met het volgende punt: het bewust maken van beveiliging.*

Voorstel 3:
Medewerkers en (directie) bewust maken van beveiliging.

- *Zie hiervoor de opmerking bij punt 2*.

Voorstel 4:
Het toewijzen van verantwoordelijkheid voor beveiliging.

- *Deze maatregel zou bij de directie belegd moeten worden, en zou dus als afzonderlijk punt kunnen vervallen**.***

Voorstel 5:
Installeren en actueel houden van antivirussoftware en firewall (indien de onderneming een verbinding heeft met het internet).

- *Naast het updaten van virus en firewall ook securitys-updates van het besturingsysteem*.

Voorstel 6:
Het dagelijks maken en testen van back-ups en deze bewaren op een beveiligde plaats.

- *Het periodiek testen in plaats van dagelijks van de back-up. Daarnaast dient de back-up op een externe plaats beveiligd te worden**.***

Voorstel 7:
Het geautomatiseerde systeem dient te zijn voorzien van toegangsbeveiliging met identificatie-, authenticatie- en autorisatiefaciliteiten die aansluiten op de functiescheiding binnen de organisatie

- *Op netwerk,applicatie en databaseniveau. Is de functiescheiding niet het probleem in het MKB ?*

Voorstel 8:
Het zorgen voor fysieke beveiliging voor de bedrijfsmiddelen (apparatuur)

- *Alle respondenten zijn het hiermee eens.*

Voorstel 9:
Het registreren van aanpassingen aan het systeem op basis van autorisatie van de proceseigenaren (change management).

- *Alle respondenten zijn het hiermee eens.*

Voorstel 10:
Het controleren of de beveiligingshuisregels worden nageleefd (monitoring).

- *Alle respondenten zijn het hiermee eens.*

4.4 Nieuw aangedragen punten uit het enquêteonderzoek

- Stel een informatie, ICT en beveiligingsbeleid op waarin deze tien maatregelen de basis vormen. Wijs hiervoor een verantwoordelijke in de organisatie aan.
- Informatie op een laptop dient te worden encrypt. Medewerkers op kantoor bewaren hun data alleen op de centrale server en niet lokaal op hun PC.
- Scheiding aanbrengen tussen ontwikkel-, test- en productieomgeving.
- Het goed vastleggen en bewaken van afspraken met externe dienstverleners en leveranciers (Service Level Management). Het MKB maakt veel gebruik van externe ondersteuning. Het is daarbij van groot belang dat de zaken (genoemd onder de voorgaande bullets) die zijn uitbesteed ook voldoende worden beheerst.
- Zorg dat de werknemers middels scholing op een juiste en verantwoorde manier kunnen omgaan met de programmatuur en beveiliging.
- Het regelen van de escrow overeenkomst.

- Melden van incidenten bij de systeembeheerder of leverancier.
- Het registreren van programmatuur en software.

4.5 Het veldonderzoek van de lijst met maatregelen onder MKB-ondernemingen

Deze paragraaf heeft tot doel na te gaan of de voorgestelde lijst met basismaatregelen praktisch toepasbaar is voor MKB-ondernemingen. De geselecteerde cliënten wilde wel meewerken aan het onderzoek maar gaven er nadrukkelijk de voorkeur aan dat zij anoniem wilde blijven. De lijst hebben wij ter plaatse besproken met de directie en/of systeembeheerder. De cliënten zijn: een uitzendbureau, een bouwbedrijf, een transportonderneming, een enveloppenfabriek en een uitgeverij.

Hieronder zullen wij de uitkomsten van dit onderzoek bespreken in de vorm van zwakke en sterke punten.

4.5.1 Zwakke punten uit het onderzoek

Voorstel 1b:
Eén bedrijf heeft maatregelen genomen voor uitwijk. De overige bedrijven hebben hiervoor nog geen maatregelen getroffen.

Voorstel 2:
Eén onderneming heeft formele beleidsregels opgesteld en laten ondertekenen door de gebruikers. Daarnaast waren er twee bedrijven die wel bepaalde internet en laptopregels hadden opgesteld, maar deze waren niet ondertekend. Twee ondernemingen hadden helemaal geen formele beveiligingsregels opgesteld.

Voorstel 3:
Twee ondernemingen vermeldden dat de systeembeheerder en of leverancier de medewerkers/directie informeert over de beveiligingsaangelegenheden. Bij één onderneming komt het bewustzijn van de beveiliging wel eens in het stafoverleg aan de orde.

Voorstel 4:
Zit impliciet in de taak van de verantwoordelijke medewerkers en of leverancier. Er is veel vertrouwen dat zij hun taken naar behoren uitvoeren.
Drie ondernemingen vermeldden dat de kennis ontbreekt om de systeembeheerder en leverancier te kunnen controleren.

Voorstel 6:
De back-up wordt bij vier bedrijven niet integraal getest. Wel wordt wel eens een bestandje teruggezet.

Voorstel 9:
Eén onderneming maakt registratie van aanpassing aan het systeem door de systeembeheerder in verband met zijn verantwoordelijkheid. Eén bedrijf registreert alleen wijzigingen aan de applicatie.
Drie bedrijven houden helemaal geen registratie bij. De proceseigenaren hebben nauwelijks invloed op de operationele wijzigingen (prijzen, kortingen e.d.) worden veelal door de directie en of stafoverleg bepaald. De wijzigingen aan het systeem worden niet in overleg met de proceseigenaar bepaald.

Voorstel 10:
Controle of regels worden nageleefd zijn er niet expliciet. Er is veel oogtoezicht.

4.5.2 Sterke punten uit het onderzoek

Voorstel 1:
De ondernemingen zijn bewust van wat en waar hun belangrijkste informatie bevindt. De ondernemingen onderkennen dat dit een fundamentele maatregel is. Zij moesten hier wel even over nadenken. Veel belangrijke informatie zit in de hoofden van de medewerkers, en beperkt in het systeem.

Voorstel 5:
Alle ondernemingen hebben een virusscanner en firewall, deze worden regelmatig voorzien van updates. De meeste ondernemingen hebben ook een spamfilter geïnstalleerd.

Voorstel 7:
De ondernemingen hebben een vorm van identificatie, authenticatie en autorisatie mechanisme in hun systeem. Wel is het zo dat deze rechten veelal per afdeling zijn toegekend.

Voorstel 8:
Bij alle ondernemingen is er afdoende fysieke beveiliging. De server bevindt zich in een afgesloten ruimte.

4.5.3 Overige punten die tijdens het veldonderzoek naar voren zijn gekomen.

Uit het onderzoek bleek nergens dat gebruikers hun wachtwoorden op hun beeldscherm hebben geplakt. Ook staat de server niet onbeveiligd in een ruimte en is de back-up niet van ‘maanden’ geleden gemaakt. Dit beeld wordt wel eens geschetst van MKB-ondernemingen. De regels zijn niet overal formeel. De onderneming leert ook van zijn tekortkomingen en past op basis daarvan zijn maatregelen aan. De onderzochte MKB-ondernemingen vinden het zinvol dat er een lijst van maatregelen zou zijn waar zij minimaal aan zouden moeten voldoen in het kader van goed huisvaderschap. In dit onderzoek ontstond een prettige discussie met cliënten. Eén onderneming was op de hoogte van het bestaan van de code voor informatiebeveiliging. Eén bouwbedrijf vermeldde dat excel-sheets met gevoelige informatie goed waren beveiligd. Twee bedrijven vermeldden dat de rechten van vertrokken medewerkers niet worden gewijzigd.

Hoofdstuk 5 Conclusie

De onderzoekvraag van deze scriptie luidt: '*Wat omvat het begrip 'goed huisvaderschap' in het kader van geautomatiseerde informatiesystemen en informatiebeveiliging in het MKB?'.* Onderstaand geven wij onze bevindingen en conclusies naar aanleiding van de gestelde deelvragen:

1. Aan welke eisen dient de beheersing van een geautomatiseerd informatiesysteem minimaal te voldoen?

   Bevindingen naar aanleiding van ons onderzoek

   Beheersingsmaatregelen in het GIS bestaan uit: general IT, application en user controls.
   De beheersingsmaatregelen in het MKB zijn in essentie dezelfde als in grote bedrijven. Alleen is de impact van deze maatregelen vanwege de kenmerken van het MKB anders. Indien de organisatorische maatregelen binnen de GIS zwak zijn geregeld, is het afhankelijk van de getroffen organisatorische maatregelen (buiten het GIS om) om alsnog betrouwbare informatie te verkrijgen. Tijdens literatuur onderzoek is gebleken dat er weinig over specifieke beheersingsmaatregelen in het MKB is beschreven. Deze dienen afgeleid te worden van de bestaande literatuur voor grote ondernemingen.

   Conclusie
   Er is minimaal functiescheiding gewenst tussen de automatisering en gebruikersorganistie om de betrouwbare informatieverwerking te waarborgen. Ter compensatie van de in de regel zwakke general IT controls binnen de MKB ondernemingen, zal de onderneming vooral steunen op de user controls. Gebruikers kunnen deze controles alleen maar uitvoeren als het GIS minimaal is voorzien van een accounting trail.

2. Aan welke eisen dient de informatiebeveiliging minimaal te voldoen voor een MKB-ondernemer?

   Bevindingen naar aanleiding van ons onderzoek
   Wij hebben gekozen voor de Code voor informatiebeveiliging als leidraad voor de inrichting van informatiebeveiliging. Het MKB is vanwege zijn kenmerken te klein om de code integraal in te voeren en heeft behoefte aan een set van minimale maatregelen. Over het algemeen geldt dat alle geënquêteerde auditors van mening zijn dat de door ons voorgestelde lijst van maatregelen in opzet praktisch toepasbaar is voor MKB-ondernemingen. Naar aanleiding van het onderzoek onder deze professionals hebben wij van de oorspronkelijke enquêtelijst drie voorstellen samengevoegd (2, 3 en 4). Daarnaast hebben wij twee nieuwe maatregelen (8 en 9) toegevoegd.

   Conclusie
   De volgende lijst met basisbeveiligingsmaatregelen dient bij een MKB-onderneming te worden ingevoerd zodat sprake is van 'goed huisvaderschap':

   Maatregel 1
   Classificeer de belangrijkste informatie en neem hiervoor passende beveiligingsmaatregelen. Stel voorwaarden aan de continue beschikbaarheid.

   Maatregel 2
   Opstellen en implementeren van beveiligingshuisregels door/namens de directie waar elke gebruiker van het geautomatiseerde systeem aan dient te voldoen door

middel van het tekenen van een (instemmings) IT-verklaring. Confronteer gebruikers regelmatig met deze verklaring.

Maatregel 3
Installeren en up-to-date houden van anti-virussoftware, security patches van het besturingsysteem en firewall (indien de onderneming een verbinding heeft met het internet).

Maatregel 4
Het dagelijks maken van back-ups en deze periodiek testen. Bewaar deze op een externe plaats.

Maatregel 5
Het geautomatiseerde systeem dient te zijn voorzien van toegangsbeveiliging met identificatie- , authenticatie- en autorisatiefaciliteiten die aansluiten op de functiescheiding binnen de organisatie.

Maatregel 6
Het zorgen voor fysieke beveiliging voor de bedrijfsmiddelen.

Maatregel 7
Het registreren van aanpassingen aan het systeem op basis van autorisatie van de proceseigenaren (change management).

Maatregel 8
Zorg dat de werknemers door scholing op een juiste en verantwoorde manier kunnen omgaan met programmatuur en beveiliging.

Maatregel 9
Melden van incidenten bij de verantwoordelijke(n).

Maatregel 10
Het controleren of de beveiligingshuisregels worden nageleefd (monitoring).

3. Hoe wordt ‘goed huisvaderschap’ in de praktijk toegepast?

Bevindingen naar aanleiding van ons onderzoek
De door ons opgestelde lijst met minimale maatregelen wordt door veel MKB-ondernemers die betrokken waren bij ons veldonderzoek in de kern gedragen. De onderzochte ondernemingen vonden het zinvol dat zij een handzame, pragmatische lijst met maatregelen gepresenteerd kregen waaraan zij zich konden spiegelen. In dit onderzoek ontstond een prettige discussie met cliënten en auditors.

Conclusie
Onderstaand worden de conclusies teruggekoppeld naar de oorspronkelijke lijst met voorstellen opgenomen in het begin van hoofdstuk 4. Ten aanzien van maatregel 1 tot en met 4 blijkt in de MKB-praktijk dat deze veelal wel onderkend worden maar niet geformaliseerd zijn. De maatregelen 5 tot en met 8 worden door MKB-ondernemingen in de basis toegepast. De diepgang hiervan varieert en kan in de praktijk niet worden teruggekoppeld aan maatregel 1 tot en met 4. Maatregel 9 en 10 komen in de MKB-praktijk niet vaak voor.

Eindconclusie
Goed huisvaderschap in het kader van geautomatiseerde informatiesystemen en informatiebeveiliging in het MKB omvat enerzijds functiescheiding tussen de automatisering en gebruikersorganistie, een stelsel van user controls en een accounting trail. Anderzijds vergt goed huisvaderschap een set van minimale, op het MKB gerichte maatregelen. De door ons opgestelde lijst met minimale maatregelen wordt door veel auditors en MKB-ondernemers die betrokken waren bij ons onderzoek als praktisch en uitvoerbaar gezien.

Hoofdstuk 6 Aanbevelingen

Op basis van de centrale vraagstelling (‘Wat omvat goed huisvaderschap in het kader van geautomatiseerde informatiesystemen en informatiebeveiliging in het MKB?’) en de eindconclusie doen wij de volgende aanbevelingen:

- Wij adviseren MKB-ondernemingen de definitieve lijst met beveiligingsmaatregelen in te voeren. Omdat het hier de minimum maatregelen betreft dient de MKB-ondernemer specifiek beveiligingsmaatregelen door middel van risicoanalyse vast te stellen.

- Wij zouden graag meer aandacht zien van IT-auditors, de (IT-audit) opleidingen en de (IT) vakbladen voor de specifieke MKB-situatie. Gezien de economische betekenis en het onontgonnen terrein van informatiebeveiliging in het MKB ligt hier een dankbare/uitdagende taak voor IT-auditors.

Geraadpleegde literatuur

Code voor informatiebeveiliging (ISO/IEC 17799:2005)

NIVRA studierapport 34: Normatieve maatregelen voor de geautomatiseerde gegevensverwerking in het kader van de jaarrekeningcontrole, 1995

NIVRA geschrift 53: Kwaliteitsoordelen over informatievoorziening,1989
Kluwer

Concept handreiking samenwerking NIVRA-NOREA

NOvAA leidraad 12 De AA in een (kleinschalig) geautomatiseerde omgeving, 2002

Bommel en Van Goor.
IT-auditing afbakenen in het kader van jaarrekeningcontrole MAB juni 2005.

Westra en Mooijekind
Compendium van de Accountantscontrole deel 1. Westra en Mooijekind, 1995
Pentagan Publishing

Meeuwissen , Vaassen CS
Interformatie & Control Interne Beheersing , 2006
Uitgeverij Wolters Noordhoff

J.C.Boer
Compact jubileumuitgave ICT-aspecten bij de accountantscontrole van de routinematige transactieverwerking, Compact,1999
KPMG/Ten Hagen Stam uitgevers

Hartjes
EDP-audit in het kader van de jaarrekeningcontrole. Handboek EDP-auditing, deel C Kwaliteitsbeoordeling van de informatievoorziening.

Koopmans en Bollen
Vertrouwde AO/IC in een nieuw wereld in, artikel in TBA , 104e druk jaargang 2000.

Fijneman,Roos Lindgreen, Kai Hang Ho
IT-auditing en de praktijk, 2006
Academic service

Fijneman,Roos Lindgreen, Piet Veltman
Grondslagen IT-auditing, 2005
Academic service

Poel en waardenburg
Jaarrekeningcontrole en EDP audit, Artikel MAB, 1989

Artikel:
Security: geen maatregelen maar risicoreductie
ZBC Consultants bv, versie 2, 2004

Artikel:
Mag een auditor nog wel normatief denken ?
ZBC Consultants bv, 2007

Croesz, Nieuwendijk
Informatievoorziening en automatisering, 1996
Kluwer Bedrijfswetenschappen

Overbeek, Sipman
Informatie beveiliging 2e druk, 1999.
Tutein Nolthenius

Informatiebeveiliging in bedrijf, VNO NCW 2002
VNO NCW

Artikel:
Publicatie wie maakt u management bewust, KWINT 2004

IT Service Management, een introductie op basis van ITIL,2004
Van haren Publishing

SBV Forensics B.V
De gunst.
Financiële software en informatiebeveiliging.
Artikel in publicatie van SBV Forensics

Romney, Steinbart
Accounting Information Systems, tenth edion,2006
Pearson Education International

Starreveld CS
Bestuurlijke informatieverzorging Deel 1, algemene grondslagen,2002
Wolters-Noordhoff B.V

Bommel, Van Goor
IT-auditing afbakenen in het kader van de jaarrekeningcontrole
Artikel uit MAB, juni 2005

J.C. Boer
ICT-aspecten bij de accountantscontrole van de routinematige transactieverwerking
Artikel in jubileum uitgave Compact,1999

Frielink, De heer
Leerboek Accountantscontrole deel 3B
Steinfert Kroese Uitgevers