*Naam 1e examinator:* **Ron van Loon** *Naam 2e examinator:* **Sabrina Jupijn**



**Naam:** Renzo Brinkhof

**Student-id:** 1581649

**Opleiding:** HBO-Bachelor Accountancy

**Instituut:** HU FEM

# Voorwoord

Voor u ligt mijn scriptie „IT Governance en de accountant‟. Mijn naam is Renzo Brinkhof en heb dit afstudeeronderzoek uitgevoerd ter afronding van mijn bachelor-opleiding HBO Accountancy aan de Hogeschool Utrecht. Ik heb mijn afstudeeronderzoek, in de periode van februari tot juni 2014, voor het accountantskantoor MTH Hoevelaken uitgevoerd.

Dit rapport is een uitwerking van mijn afstudeeronderzoek, waarbij de meest voorkomende problemen, met betrekking tot informatiebeveiliging, binnen het MKB, in kaart zijn gebracht. Het doel is om een beheermethodiek te ontwikkelen met algemene IT-beheersmaatregelen, die speciaal is gericht op MKB-bedrijven. Ik heb verschillende registeraccountants, die werkzaam zijn in de controlepraktijk bij MTH te Hoevelaken, geïnterviewd. Daarnaast heb ik verschillende controledossiers van MKB-bedrijven geraadpleegd, om de meest voorkomende problemen, met betrekking tot informatiebeveiliging, in kaart te brengen. De getroffen IT- beheersmaatregelen zijn tot stand gekomen door het afnemen van interviews en het verrichten van observaties, alsmede het doen van literatuuronderzoek, waarbij een aantal elementen uit de beheermethodieken en kwaliteitsnormen: ITIL, ISO 20.000 en COBIT, zijn gebruikt.

Het gebruik van deze zelf ontwikkelde beheermethodiek, levert zowel voordelen op voor MKB-bedrijven, als voor de accountant, die de jaarrekening moet controleren van een MKB-bedrijf. Enerzijds kunnen MKB-bedrijven door het toepassen van deze beheermethodiek een correct en fatsoenlijk IT beheer realiseren, dat voldoende is afgestemd met de businessbehoeften (Loon, 2013; Noë, 2006). Anderzijds kunnen accountants, waaronder de werkzame accountants bij MTH te Hoevelaken, deze zelf ontwikkelde beheermethodiek met algemene IT-beheersmaatregelen voorleggen aan klanten, om nu en in de toekomst minder aanvullende gegevensgerichte controlewerkzaamheden uit te hoeven voeren (Wildschut, 2013).

Ik ben van mening, dat MKB-bedrijven op dit moment te weinig aandacht schenken aan IT beheer en in het bijzonder informatiebeveiliging. Zeker als je ziet dat de IT systemen, van veel bedrijven, tegenwoordig in toenemende mate worden gehackt. Daarnaast heb ik veel affiniteit met IT en wil ik mijn kennis over dit onderwerp graag verbreden. Voor mij waren dit redenen, om dit onderzoek uit te voeren.

Mijn dank gaat uit naar alle medewerkers binnen MTH te Hoevelaken, die een bijdrage hebben geleverd aan dit onderzoek, alsmede mijn bedrijfsmentor en docentbegeleider, die mij gedurende het verrichten van mijn onderzoek hebben ondersteund.

Renzo Brinkhof

Utrecht, juni 2014

Inhoudsopgave

[Voorwoord 2](#_Toc392516901)

[Managementsamenvatting 5](#_Toc392516902)

[1 Inleiding 7](#_Toc392516903)

[1.1 Stageverlenende organisatie 7](#_Toc392516904)

[1.2 Aanleiding 9](#_Toc392516905)

[1.3 Probleemdefinitie 10](#_Toc392516906)

[1.4 Afbakening onderzoek 11](#_Toc392516907)

[1.5 Doelstelling 11](#_Toc392516908)

[1.6 Hoofdvraag 11](#_Toc392516909)

[1.7 Deelvragen 12](#_Toc392516910)

[2 Methodologie 12](#_Toc392516911)

[2.1 Desk research 12](#_Toc392516912)

[2.2 Field research 12](#_Toc392516913)

[2.3 Koppeling deelvragen 13](#_Toc392516914)

[2.4 Betrouwbaarheid en validiteit 15](#_Toc392516915)

[3 IT Governance 15](#_Toc392516916)

[4 Bronnen voor IT normen 17](#_Toc392516917)

[4.1 ITIL 18](#_Toc392516918)

[4.1.1 Service Lifecycle 19](#_Toc392516919)

[4.1.2 ITIL implementaties 20](#_Toc392516920)

[4.1.3 ITIL in de praktijk 21](#_Toc392516921)

[4.2 ISO 20.000 22](#_Toc392516922)

[4.2.1 ISO 20.000 implementaties 25](#_Toc392516923)

[4.2.2 ISO 20.000 in de praktijk 25](#_Toc392516924)

[4.3 COBIT 26](#_Toc392516925)

[4.3.1 COBIT-kubus 27](#_Toc392516926)

[4.3.2 COBIT implementaties 30](#_Toc392516927)

[4.3.3 COBIT in de praktijk 30](#_Toc392516928)

[4.4 Vergelijking ITIL, ISO 20.000 en COBIT 31](#_Toc392516929)

[5 Bronnen voor IT normen in relatie tot IT Governance 34](#_Toc392516930)

[6 Informatiebeveiliging 35](#_Toc392516931)

[7 Resultaten van het empirisch onderzoek 37](#_Toc392516932)

[7.1 IT versterkt de kwaliteit van de AO/IC bij MKB-bedrijven 38](#_Toc392516933)

[7.2 IT verzwakt de kwaliteit van de AO/IC bij MKB-bedrijven 38](#_Toc392516934)

[7.3 Betere IT-control bij MKB-bedrijven realiseren 39](#_Toc392516935)

[7.3.1 Aanknopingspunten van beheermethodieken en kwaliteitsnormen voor betere IT-control bij MKB-bedrijven 39](#_Toc392516936)

[7.3.2 IT-beheersmaatregelen bij MKB-bedrijven 42](#_Toc392516937)

[7.3.3 Toepasbaarheid van de beheermethodieken en kwaliteitsnormen in het MKB 50](#_Toc392516938)

[8 Conclusie en aanbevelingen 53](#_Toc392516939)

[9 Reflectie onderzoek 55](#_Toc392516940)

[Literatuur 57](#_Toc392516941)

[Bronnen 59](#_Toc392516942)

[Bijlage 1 ITIL 61](#_Toc392516943)

[Bijlage 2 ISO 20.000 66](#_Toc392516944)

[Bijlage 3 COBIT 67](#_Toc392516945)

[Bijlage 4 Interview 72](#_Toc392516946)

[Bijlage 5 Interview 76](#_Toc392516947)

# Managementsamenvatting

In deze managementsamenvatting wordt de inhoud van dit rapport beknopt weergegeven. Het onderwerp, alsmede de probleemstelling en het doel van dit onderzoek zullen nader worden toegelicht. Bovendien zullen de belangrijke bevindingen en conclusies, die uit dit onderzoek naar voren zijn gekomen, nader worden toegelicht. Ten slotte zullen de aanbevelingen, die uit dit onderzoek voortvloeien, worden besproken.

**Onderwerpsafbakening en probleemstelling**

De informatietechnologie (IT) speelt al een hele grote rol in ons dagelijks leven en die rol zal in de komende jaren alleen maar groter worden (Bolland, 2011; Fijneman, 2005). IT is echter kostbaar en zal naar alle waarschijnlijkheid in de toekomst alleen maar duurder worden (Bolland, 2011). Hierin schuilt het gevaar, dat veel MKB-bedrijven hierdoor geneigd zijn om te weinig aandacht te schenken aan IT beheer, met alle gevolgen van dien. Dit blijkt ook vaak het geval te zijn. De laatste jaren lukt het hackers namelijk regelmatig om IT systemen binnen te komen en allerlei gegevens te ontvreemden.Een adequate informatiebeveiliging is hier enorm van belang en dat zal in de komende jaren alleen maar groter worden.

Aan de hand van beheermethodieken en kwaliteitsnormen, als ITIL, ISO 20.000 en COBIT, kunnen bedrijven IT beheersbaar maken (Noë, 2006). In de praktijk, zijn deze bronnen voor IT normen echter voornamelijk geschikt voor grote bedrijven en in mindere mate voor MKB-bedrijven. De enorm hoge kosten voor de implementatie en het feit dat het implementeren hiervan een enorm complex proces is, zijn de redenen waarom het MKB hier weinig gebruik van maakt (Bolland, 2011). Daarnaast besteden ook accountants, waaronder de accountants die werkzaam zijn bij MTH te Hoevelaken, door gebrek aan kennis, vaak te weinig aandacht aan het IT beheer bij klanten.

**Doel**

Het doel van dit onderzoek, is om een beheermethodiek met algemene IT-beheersmaatregelen te ontwikkelen voor het inrichten, beheersen en verbeteren van IT-processen, met betrekking tot informatiebeveiliging, die speciaal is gericht op MKB-bedrijven. Hiervoor zullen allereerst de meest voorkomende zwakheden, met betrekking tot IT, bij MKB-bedrijven, in kaart moeten worden gebracht. Deze zwakheden hebben in dit onderzoek betrekking op informatiebeveiliging en verzwakken uiteindelijk de kwaliteit van de AO/IC. Het uiteindelijke resultaat is een top 10 lijst met IT-zwakheden bij MKB-bedrijven, met voor elke IT-zwakheid in ieder geval één passende IT-beheersmaatregel.

Met behulp van deze zelf ontwikkelde beheermethodiek, kunnen MKB-bedrijven een fatsoenlijk en correct IT beheer realiseren. Dit kan zowel voordelen opleveren voor het bedrijf zelf, als voor de accountant. Bedrijven kunnen aan de hand van deze beheermethodiek, eventueel adequate maatregelen nemen om een correct en fatsoenlijk IT beheer te realiseren, met als gevolg dat de bedrijfsdoelstellingen sneller en gemakkelijker kunnen worden gerealiseerd. Bovendien kunnen accountants, waaronder de werkzame accountants bij MTH te Hoevelaken, deze zelf ontwikkelde beheermethodiek met algemene IT-beheersmaatregelen voorleggen aan klanten, om nu en in de toekomst minder aanvullende gegevensgerichte controlewerkzaamheden uit te hoeven voeren (Wildschut, 2013).

Uit het verlengde van deze doelstelling, is de volgende hoofdvraag geformuleerd: *‘’Op welke wijze kunnen organisaties in het MKB, veel voorkomende zwakheden met betrekking tot IT, die tot gevolg hebben dat de accountant tijdens de controle niet kan steunen op de AO/IB, beheersen?’’*

Om een antwoord te krijgen op deze hoofdvraag, zijn een viertal theoretische deelvragen en een tweetal empirische deelvragen opgesteld. De antwoorden op deze deelvragen zijn verkregen door het afnemen van een aantal interviews, het verrichten van observaties in een aantal controledossiers en het doen van literatuuronderzoek, waarbij de beheermethodieken en kwaliteitsnormen: ITIL, ISO 20.000 en COBIT, zijn beschreven en onderling met elkaar zijn vergeleken. Hieronder worden de belangrijke bevindingen en conclusies uit dit onderzoek nader toegelicht.

**Belangrijkste bevindingen en conclusies**

Uit dit onderzoek, blijkt dat IT zowel de kwaliteit van de AO/IC bij MKB-bedrijven versterkt, als de kwaliteit van de AO/IC verzwakt. Bij de controle van MKB-bedrijven, treffen accountants veelal de volgende problemen aan, die de kwaliteit van de AO/IC verzwakken:

1. Ontbreken van een formeel opgesteld IT beleid: binnen het MKB wordt IT te vaak als bijzaak gezien en de normen en inrichting worden vaak bepaald op basis van gebruikersgemak;
2. Softwarematige fouten in de IT-infrastructuur;
3. Beperkt gebruik van proces- en/of systeemdocumentatie bij de invoering van nieuwe systemen/pakketten: binnen het MKB gebeurt het regelmatig dat wijzigingen in systemen/pakketten ongecontroleerd tot stand komen, met verwarring bij gebruikers en IT medewerkers als gevolg;
4. Onvoldoende periodieke monitoring van de kwaliteit van systemen;
5. Onvoldoende back-uppen van gegevensdragers met behulp van een data back-up systeem;
6. Niet goed ingeregelde competenties (autorisatie): gebruikers/medewerkers hebben vaak te veel bevoegdheden, doordat veel MKB-bedrijven ‘’gebruikersgemak’’ als uitgangspunt hanteren bij het bepalen van de normen en inrichting met betrekking tot IT. IT systemen moeten immers een inrichting hebben die praktisch is;
7. Tekortkomingen in de authenticatie: regelmatig komt het bij MKB-bedrijven voor dat er gebreken zijn in het versleutelen/coderen tegen bedreigingen, waarbij het regelmatig voorkomt dat meerdere gebruikers/medewerkers hetzelfde wachtwoord gebruiken, met ongeautoriseerde toegang tot informatiesystemen of bepaalde vertrouwelijke informatie als gevolg;
8. Beperkt gebruik van proces- en/of systeemdocumentatie met betrekking tot informatiebeveiliging: binnen het MKB gebeurt het regelmatig dat gebruikers/medewerkers niet weten welke acties zij moeten verrichten, op het moment dat er zich ernstige incidenten of storingen voordoen met betrekking tot de IT systemen;
9. Gebreken in de inrichting van de logische toegangsbeveiliging;
10. Gebreken in de inrichting van de fysieke beveiliging en beveiliging van de omgeving: het gebeurt regelmatig dat er onverwachte/illegale componenten op een netwerk zijn aangesloten. Tevens komt het regelmatig voor dat een server in de bezemkast onvoldoende wordt gekoeld, met brandgevaar of elektriciteitsonderbreking als gevolg.

De in dit rapport besproken bronnen voor IT normen: ITIL, ISO 20.000 en COBIT, kunnen worden gebruikt om voor deze in kaart gebrachte problemen, met betrekking tot informatiebeveiliging, passende IT-beheermaatregelen te treffen. Hoewel deze bronnen voor IT normen in de praktijk weinig worden gebruikt door MKB-bedrijven, zijn deze beheermethodieken en kwaliteitsnormen toch zeker interessant voor het MKB. Het gebruik van deze beheermethodieken en kwaliteitsnormen draagt immers bij aan het realiseren van een correct en fatsoenlijk IT beheer en zorgt ervoor dat MKB-bedrijven in ieder geval bezig zijn met ‘’IT Governance’’ en hier dus voldoende aandacht aan schenken.

Zowel ITIL, als ISO 20.000 en COBIT, geven in de processen invulling aan informatiebeveiliging, waarbij de algemene informatiebeveiligingsmaatregelen veelal zijn gebaseerd op ISO 27.002: Code voor Informatiebeveiliging (Elsinga, 2014). Echter, blijkt dat de invulling aan informatiebeveiliging, bij deze beheermethodieken en kwaliteitsnormen, beperkt is. ITIL, ISO 20.000 en COBIT zijn voor een groot deel gericht op IT beheer. Informatiebeveiliging gaat echter veel verder dan alleen IT beheer.

**Aanbevelingen**

Zoals hierboven al is gemeld, maken MKB-bedrijven relatief weinig gebruik van bronnen voor IT normen. De redenen hiervoor zijn reeds besproken. MKB-bedrijven hebben echter zeker wel wat aan deze beheermethodieken en kwaliteitsnormen en zouden deze bronnen voor IT normen kunnen gebruiken, door niet alle processen integraal over te nemen maar een selectie te maken van de processen, die van belang zijn voor het bedrijf. Doordat ITIL, ISO 20.000 en COBIT, met betrekking tot de verschillende processen, waaronder informatiebeveiliging, elkaar aanvullen, is het tevens aan te raden, om als MKB-bedrijf, deze bronnen voor IT normen naast elkaar te gebruiken. Het volledig toepassen van één van deze beheermethodieken en kwaliteitsnormen zal niet voldoende zijn.

Voor de in kaart gebrachte problemen, met betrekking tot informatiebeveiliging, bij MKB-bedrijven, kunnen een aantal IT-beheersmaatregelen worden getroffen. De volgende IT-beheersmaatregelen kunnen worden getroffen, om de in kaart gebrachte problemen, met betrekking tot informatiebeveiliging, bij MKB-bedrijven, op te lossen dan wel in de toekomst te voorkomen:

1. Opstellen van een lange termijn IT beleid;
2. Toepassing van de ITIL-processen ‘’Request Management’’ en ‘’Problem Management’’;
3. Gebruik van proces- en/of systeemdocumentatie bij de invoering van nieuwe systemen/pakketten;
4. Periodieke monitoring van de kwaliteit van systemen;
5. Periodiek back-uppen van gegevensdragers met behulp van een data back-up systeem;
6. Ingeregelde competenties (autorisatie);
7. Ingeregelde authenticatie;
8. Gebruik van proces- en/of systeemdocumentatie met betrekking tot informatiebeveiliging;
9. Geregelde logische toegangsbeveiliging;
10. Geregelde fysieke beveiliging en beveiliging van de omgeving.

Deze IT-beheersmaatregelen, zijn tezamen met de meest voorkomende problemen, met betrekking tot informatiebeveiliging, bij MKB-bedrijven, ondergebracht in een zelf ontwikkelde beheermethodiek, die in dit rapport is opgenomen.

# 1 Inleiding

In dit hoofdstuk zal de stageverlenende organisatie, die de opdrachtgever is van dit onderzoek, nader worden beschreven. Tevens zal de aanleiding, probleemstelling, doelstelling, hoofdvraag en deelvragen van dit onderzoek worden beschreven.

## 1.1 Stageverlenende organisatie

MTH, voorheen Meeuwsen Ten Hoopen Accountant en Belastingadviseurs, is dé regionale full service dienstverlener (overige dienstverlening > beschikbaar stellen van personeel) van Nederland, op het gebied van accountancy, belastingadvies, corporate finance, werkgeversdiensten, ondernemersadvies en persoonlijk financieel advies (MTH, n.d.).

Creatief in de advisering en efficiënt in de uitvoering. MTH heeft op dit moment 18 verschillende vestigingen in Nederland. De vestiging waar ik stage heb gelopen, is vestiging Hoevelaken. Bij de vestiging in Hoevelaken zijn zo’n 60 mensen werkzaam.

MTH ziet zichzelf als een geheel eigen adviseur voor bedrijven en instellingen en heeft een aantal pijlers waarop men bouwt, deze zijn:

* direct en persoonlijk contact met de klant;
* advies op maat en dus geheel eigen;
* creëren van toegevoegde waarde voor de klant met een eigen adviseur als sparringpartner en verlengstuk van de organisatie.

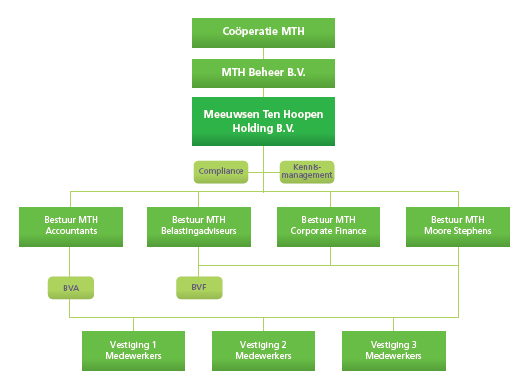
Naast de hierboven genoemde pijlers, heeft MTH ook een aantal kernwaarden geformuleerd die ervoor moeten zorgen dat men zowel intern als extern met relaties, scherp en alert blijft. De kernwaarden zijn:

* vertrouwen: vertrouwen is volgens MTH de basis voor elke relatie;
* verantwoordelijkheid: verantwoordelijkheid moet zowel worden gegeven als worden genomen;
* openheid: streven naar openheid in het contact met relaties en collega’s;
* respect: respecteren van de natuur, de medewerkers en elkaars visie en kijk op de wereld;
* een goed gevoel: zelfstandig denkende professionals die op doeltreffende en eerlijke wijze met plezier samenwerken.

MTH beschikt over een breed klantenbestand, van particulieren en MKB tot grootbedrijf. De organisatie is niet alleen op lokaal, regionaal en nationaal niveau actief, maar ook op internationaal niveau. MTH heeft een partnerschap met het wereldwijde netwerk van zelfstandige kantoren van Moore Stephens. Om bedrijven en instellingen zo goed mogelijk van dienst te kunnen zijn, heeft MTH de specifieke branchekennis gebundeld in kennisgroepen, zoals voor de detailhandel en de bouw en vastgoed. Op deze manier kan MTH voor haar cliënten de juiste sparringpartner zijn. Teams houden de kennis van de desbetreffende sector continu up-to-date en ondersteunen elkaar. Ook de medewerkers van MTH kunnen bij complexe vraagstukken terecht bij deze teams.

MTH streeft ernaar om haar cliënten een goed gevoel te kunnen geven. Men hanteert daarbij een bepaalde aanpak. Iedere adviseur binnen MTH krijgt de verantwoordelijkheid en men verwacht dan ook dat de desbetreffende adviseur deze verantwoordelijkheid neemt die bij zijn of haar kennis- en ervaringsniveau past. Op deze manier wordt er ruimte gerealiseerd om zelfstandig te kunnen beslissen, te groeien en te ondernemen. De adviseurs van MTH krijgen van kwaliteitssystemen en ervaren collega’s en specialisten maximale rugdekking. Op deze manier kan iedere medewerker van MTH, cliënten voorzien van advies op maat.

De aanpak van MTH, waar cliënten een eigen vaste sparringpartner hebben, heeft als voordeel dat de desbetreffende adviseur van MTH op de hoogte is van het bedrijf of de instelling. Daarnaast weet de adviseur de weg naar nieuwe kansen of oplossingen van problemen. Het kan voorkomen dat die weg binnen MTH gaat lopen naar collega’s met meer specifieke kennis of vaardigheden, waar de cliënt van profiteert. De desbetreffende adviseur kan binnen MTH eventueel specialisten inschakelen, waarna samen het bedrijf versterkt kan worden.



\* **Figuur 1:** Organisatiestructuur MTH (Rijken, Riedstra & Hoek, 2012)

De laatste jaren laat MTH een omzetdaling zien (Rijken, Riedstra & Hoek, 2012). In het jaar 2010 had MTH een omzet van 41,2 miljoen euro, waarna de omzet in het jaar 2011 daalde naar 41,1 miljoen euro en in het jaar 2012 naar 39,4 miljoen euro.

## 1.2 Aanleiding

De informatietechnologie (IT) speelt al een hele grote rol in ons dagelijks leven en die rol zal in de komende jaren alleen maar groter worden (Bolland, 2011; Fijneman, 2005). Veel bedrijven hebben IT ondersteuning bij het uitvoeren van de bedrijfsprocessen. Met behulp van IT kunnen bedrijfsprocessen effectiever en efficiënter verlopen. Er zitten dus enorm veel voordelen aan het gebruik van IT, echter ook de nadelen vereisen de nodige aandacht. IT is kostbaar en zal naar alle waarschijnlijkheid in de toekomst alleen maar duurder worden (Bolland, 2011). Door de kostbaarheid van IT, zijn veel bedrijven geneigd om te weinig aandacht te schenken aan IT beheer. Dit heeft weer enorm veel negatieve gevolgen, denk hierbij aan het feit dat er in de laatste jaren steeds meer bedreigingen en kritische toepassingen zijn als het gaat om IT (Romney, 2012). Bedrijven moeten zich hier tegen weren en naar oplossingen zoeken om deze bedreigingen uit te bannen. Een adequate beveiliging is al enorm van belang en dat zal in de komende jaren alleen maar groter worden.

Hieruit kan dus geconcludeerd worden, dat onze wereld steeds meer afhankelijker is geworden van de informatietechnologie (IT) en dat geldt dus ook voor bedrijven (Bolland, 2011; Fijneman, 2005). De vraag is echter hoe bedrijven in de praktijk omgaan met IT beheer. Uiteindelijk gaat het erom dat er binnen bedrijven voldoende aandacht wordt geschonken aan de primaire kwaliteitsaspecten voor de bedrijfsgegevens, namelijk vertrouwelijkheid, integriteit, beschikbaarheid en controleerbaarheid (Romney, 2012). Op deze manier kunnen bedrijven de continuïteit versterken. De laatste jaren hebben echter uitgewezen, dat niet altijd voldoende aandacht wordt geschonken aan deze primaire kwaliteitsaspecten. Zo lukt het hackers immers nog regelmatig om IT systemen binnen te komen en allerlei gegevens te ontvreemden.

## 1.3 Probleemdefinitie

Steeds meer bedrijven hebben een IT beheer, dat onvoldoende is afgestemd met de businessbehoeften (Noë, 2006). Uit de laatste jaren blijkt immers dat er steeds meer bedreigingen en kritische toepassingen zijn als het gaat om IT (Romney, 2012). Dit kan negatieve effecten hebben op het behalen van de bedrijfsdoelstellingen en dus uiteindelijk de bedrijfscontinuïteit.

Tevens is ook voor de accountant in deze tijd een adequaat IT beheer binnen een bedrijf enorm van belang, voornamelijk bij de controle van de jaarrekening. Veel bedrijven zijn immers in toenemende mate geautomatiseerd. Op het moment dat de accountant kan steunen op de IT systemen en dus ook op de AO/IB, zijn aanvullende gegevensgerichte controlewerkzaamheden meestal niet noodzakelijk (Wildschut, 2013).

Hieruit kan dus geconcludeerd worden, dat een correct en fatsoenlijk IT beheer, zowel voordelen kan opleveren voor het bedrijf zelf als voor de accountant. Op het moment dat er een correct en fatsoenlijk IT beheer is, zal het bedrijf immers de bedrijfsdoelstellingen sneller en gemakkelijker realiseren. Bovendien hoeft de accountant bij de controle van de jaarrekening minder aanvullende gegevensgerichte controlewerkzaamheden uit te voeren.

Veel bedrijven, voornamelijk grote bedrijven, proberen IT beheersbaar te maken. Hiervoor wordt veelvuldig gebruik gemaakt van beheermethodieken en kwaliteitsnormen, als ITIL, ISO 20.000 en COBIT (Noë, 2006). Met behulp van deze beheermethodieken en kwaliteitsnormen kunnen bedrijven IT-processen inrichten, beheersen en verbeteren. Het implementeren van deze beheermethodieken en kwaliteitsnormen brengen echter in de praktijk enorm hoge kosten met zich mee (Bolland, 2011). Bovendien is het implementeren van deze beheermethodieken en kwaliteitsnormen over het algemeen een enorm complex proces. Dat is dan ook de reden dat bij MKB-bedrijven vaak weinig aandacht wordt geschonken aan deze beheermethodieken en kwaliteitsnormen en dus het inrichten, beheersen en verbeteren van IT-processen. Tevens schenken ook accountants, waaronder de accountants die werkzaam zijn bij MTH te Hoevelaken, vaak weinig aandacht aan het inrichten, beheersen en verbeteren van IT-processen bij klanten.

In dit onderzoek, zal als het gaat om IT beheer, de zwakheden bij MKB-bedrijven in kaart worden gebracht, waarna een beheermethodiek zal worden ontwikkeld met algemene IT-beheersmaatregelen, die gericht is op MKB-bedrijven. MKB-bedrijven kunnen aan de hand van deze beheermethodiek, eventueel adequate maatregelen nemen om een correct en fatsoenlijk IT beheer te realiseren dat aansluit met de businessbehoeften (Noë, 2006). Bedrijfsdoelstellingen kunnen op deze manier sneller en gemakkelijker worden gerealiseerd.

Daarentegen kunnen accountants, waaronder de werkzame accountants bij MTH te Hoevelaken, deze zelf ontwikkelde beheermethodiek met algemene IT-beheersmaatregelen voorleggen aan klanten, om nu en in de toekomst minder aanvullende gegevensgerichte controlewerkzaamheden uit te hoeven voeren (Wildschut, 2013). Er kan in dit geval dus gesteund worden op de AO/IB. Dit onderzoek zal voornamelijk betrekking hebben op het belang van de accountant bij een correct en fatsoenlijk IT beheer binnen een bedrijf.

## 1.4 Afbakening onderzoek

Aan de hand van dit onderzoek, zal een beheermethodiek worden ontwikkeld voor het inrichten, beheersen en verbeteren van IT-processen, die speciaal is gericht op MKB-bedrijven. Om dit te kunnen realiseren zijn allereerst de meest voorkomende zwakheden, met betrekking tot IT, bij MKB-bedrijven, in kaart gebracht. Deze zwakheden hebben in dit onderzoek betrekking op informatiebeveiliging en verzwakken uiteindelijk de kwaliteit van de AO/IC. Het in kaart brengen van de meest voorkomende zwakheden, met betrekking tot informatiebeveiliging, is bewerkstelligd door het afnemen van interviews, het verrichten van observaties en het doen van literatuuronderzoek. De aandacht met betrekking tot literatuuronderzoek is uitgegaan, naar ITIL, ISO 20.000 en COBIT (Noë, 2006; Looijen, 2011). Deze beheermethodieken en kwaliteitsnormen worden immers in de praktijk veelvuldig toegepast en zijn op dit moment actueel. Het uiteindelijke resultaat is een top 10 lijst met IT-zwakheden bij MKB-bedrijven, met voor elke IT-zwakheid in ieder geval één passende IT-beheersmaatregel.

## 1.5 Doelstelling

De doelstelling van dit onderzoek voor de opdrachtgever luidt als volgt:

*“Dit onderzoek heeft als doel om een beheermethodiek te ontwikkelen voor het inrichten, beheersen en verbeteren van IT-processen, met betrekking tot informatiebeveiliging, die speciaal is gericht op MKB-bedrijven. Het uiteindelijk op te leveren eindproduct bestaat hierbij uit een rapportage van bevindingen, met een top 10 lijst van meest voorkomende informatiebeveiligingsproblemen, bij MKB-bedrijven, en voor elk informatiebeveiligingsprobleem in ieder geval één passende IT-beheersmaatregel.’’*

De doelstelling van dit onderzoek voor mij als student luidt als volgt:

*‘’Dit onderzoek heeft als doel om mijn kennis te vergroten voor wat betreft de geautomatiseerde gegevensverwerking binnen MKB-bedrijven, wat met de komende jaren in het vooruitzicht, van enorme waarde kan zijn bij mijn functioneren in de praktijk. Ten slotte geeft dit onderzoek mij de mogelijkheid om mij te verbeteren op de domeincompetenties: ontwerpen, inrichten en onderhouden van (geautomatiseerde) informatiesystemen voor het besturen van organisaties en het vormgeven, inrichten en toetsen van de administratieve organisatie.’’*

## 1.6 Hoofdvraag

Uit het verlengde van de doelstelling van dit onderzoek, is de volgende hoofdvraag geformuleerd:

*‘’Op welke wijze kunnen organisaties in het MKB, veel voorkomende zwakheden met betrekking tot IT, die tot gevolg hebben dat de accountant tijdens de controle niet kan steunen op de AO/IB, beheersen?’’*

## 1.7 Deelvragen

Voor dit onderzoek zijn zes deelvragen geformuleerd, die uiteindelijk samen de hoofdvraag beantwoorden. Er zijn in totaal vier theoretische en twee empirische deelvragen geformuleerd.

**Theoretische deelvragen:**

1. *‘‘Wat is het belang van IT Governance voor organisaties?’’*
2. *‘’Welke bronnen voor IT normen worden in de praktijk veelal toegepast?’’*
3. *‘‘Op welke wijze geven de veel gebruikte bronnen voor IT normen invulling aan IT Governance?’’*
4. *‘‘Op welke wijze zijn de veel gebruikte bronnen voor IT normen in de praktijk te implementeren?’’*

**Empirische deelvragen:**

1. *“Welke versterkingen en verzwakkingen van de interne controle met betrekking tot IT, komen accountants bij de controle van MKB-bedrijven veelal tegen?‘’*
2. *“Welke IT-beheersmaatregelen, waaronder general en application IT controls, zijn bij de controle van MKB-bedrijven voor de accountant van belang om te kunnen steunen op de AO/IB?’’*

# 2 Methodologie

Dit onderzoek bestaat zowel uit een theoretisch als een empirisch (praktisch) deel. Hiervoor zijn verschillende methoden van onderzoek toegepast, die in dit hoofdstuk nader zullen worden beschreven. Het uiteindelijke doel van het gehele onderzoek, is het ontwikkelen van een beheermethodiek met algemene IT-beheersmaatregelen, die speciaal is gericht op MKB-bedrijven. Om dit te kunnen bewerkstelligen zijn allereerst de meest voorkomende zwakheden, met betrekking tot IT, bij MKB-bedrijven, in kaart gebracht.

## 2.1 Desk research

De voor dit onderzoek geformuleerde theoretische deelvragen, zijn beantwoord met behulp van literatuuronderzoek.

Er is voor deze methode van onderzoek gekozen, omdat deze methode het meest effectief en efficiënt is om een antwoord te krijgen op de geformuleerde theoretische deelvragen. Tevens is deze methode van onderzoek uitvoerbaar. Er is meer dan genoeg literatuur beschikbaar met betrekking tot IT; zie hiervoor de bijgevoegde literatuur en bronnen.

## 2.2 Field research

Voor beantwoording van de empirische deelvragen in dit onderzoek, is gebruik gemaakt van de onderzoeksmethoden: interviews en observaties.

Registeraccountants, die werkzaam zijn in de controlepraktijk bij MTH te Hoevelaken, stonden open om kennis en ervaringen uit de praktijk te delen. Verschillende registeraccountants, die werkzaam zijn in de controlepraktijk bij MTH te Hoevelaken, zijn geïnterviewd. Deze registeraccountants zijn geselecteerd op basis van ervaring en kennis. Tijdens de interviews zijn de registeraccountants ondervraagd omtrent de werking van de geautomatiseerde omgeving bij MKB-bedrijven.

Ten slotte zijn voor de beantwoording van de empirische deelvragen in dit onderzoek, een aantal controledossiers geraadpleegd om informatie te verkrijgen omtrent de bevindingen over de geautomatiseerde omgeving bij verschillende MKB-bedrijven. De geobserveerde controledossiers zijn geheel willekeurig geselecteerd of door een registeraccountant voorgesteld. Er is hierbij een checklist gebruikt, die is gekoppeld aan de theorie; in dit geval ISO 27.002: Code voor Informatiebeveiliging. De bevindingen, die uit deze checklists naar voren zijn gekomen, hebben uiteindelijk geresulteerd in een top 10 lijst met meest voorkomende IT-zwakheden bij MKB-bedrijven.

Er is voor deze methoden van onderzoek gekozen, omdat deze methoden ook in dit geval het meest effectief en efficiënt zijn om een antwoord te krijgen op deze deelvragen. Tevens zijn deze methoden van onderzoek uitvoerbaar. Accountants hebben tegenwoordig bij de controle van MKB-bedrijven bijna altijd te maken met (complexe) geautomatiseerde omgevingen. Bevindingen over de werking van de geautomatiseerde omgeving bij MKB-bedrijven, die zijn vastgelegd in de controledossiers en kennis en ervaringen die accountants in de praktijk hebben opgedaan, hebben een bijdrage geleverd aan de beantwoording van de empirische deelvragen.

## 2.3 Koppeling deelvragen

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Deelvraag | Doel | Onderzoeksmethode(n) | Bron(nen) |
| 1 | *Wat is het belang van IT Governance voor organisaties?* | MKB-bedrijven er bewust van maken dat zonder een correct en fatsoenlijk IT beheer, bedrijfsdoelstellingen niet behaald kunnen worden en de bedrijfscontinuïteit niet gewaarborgd is. | **Desk research:** boeken, internet searches en (wetenschappelijke) artikelen | **Desk research:**  - (Bolland, 2011);  - (Fijneman, 2006);  - (Fijneman, 2009);  - (Loon, 2013). |
| 2 | *Welke bronnen voor IT normen worden in de praktijk veelal toegepast?* | MKB-bedrijven een inzicht geven in de veel gebruikte beheermethodieken en kwaliteitsnormen om een correct en fatsoenlijk IT beheer te realiseren, dat voldoende is afgestemd met de businessbehoeften. | **Desk research:** boeken, internet searches en (wetenschappelijke) artikelen | **Desk research:**  - (APM Group, n.d.);  - (APM Group Limited, 2010);  - (Bloemendal, n.d.);  - (Bolland, 2011);  - (Bouker, n.d.);  - (Croon, 2008);  - (Fijneman, 2005);  - (Fijneman, 2009);  - (ISACA, n.d.);  - (ISACA, 2012);  - (IT Management Group, n.d.);  - (Lindgreen, 2005);  - (Looijen, 2011);  - (Mulder, 2012);  - (Noë, 2006);  - (Polter, n.d.);  - (Romney, 2012);  - (Stevens, 2008);  - (Ten Hagen, 2013);  - (Van Bon, 2007);  - (Van Gils, 2005);  - (Van ‘t Hoff, 2008);  - (Whizpr, 2007). |
| 3 | *Op welke wijze geven de veel gebruikte bronnen voor IT normen invulling aan IT Governance?* | MKB-bedrijven er bewust van maken dat beheermethodieken en kwaliteitsnormen kunnen bijdragen aan het realiseren van een correct en fatsoenlijk IT beheer,  dat voldoende is afgestemd met de businessbehoeften. | **Desk research:** boeken, internet searches en (wetenschappelijke) artikelen | **Desk research:**  - (Croon, 2008);  -(Fijneman, 2006);  - (Noë, 2006). |
| 4 | *Op welke wijze zijn de veel gebruikte bronnen voor IT normen in de praktijk te implementeren?* | MKB-bedrijven een inkijk geven hoe zij de veel gebruikte beheermethodieken en kwaliteitsnormen kunnen gebruiken om IT-processen in te richten, te beheersen en te verbeteren. | **Desk research:** boeken, internet searches en (wetenschappelijke) artikelen | **Desk research:**  -(Bouker, n.d.);  - (BSI Group, n.d.);  - (ITSMF, n.d.);  - (Jerphanion, n.d.);  - (Van Beem, n.d.);  - (Van Veen, n.d.). |
| 5 | *Welke verzwakkingen en versterkingen van de interne controle met betrekking tot IT, komen accountants bij de controle van MKB-bedrijven veelal tegen?* | MKB-bedrijven een inzicht geven in de meest voorkomende versterkingen en verzwakkingen van de interne controle, met betrekking tot IT, om de beheersing hiervan te kunnen verbeteren. | **Desk research:** boeken, internet searches en (wetenschappelijke) artikelen  +  **Field research:** interviews en observaties | **Desk research:**  - (Accountancy Nieuws, 2010);  - ( Crooij, 2013);  - (Fijneman, 2006);  - (Fijneman, 2009);  - (Looijen, 2011);  - (Romney, 2012).  **Field research:**  - Interview: Dhr. Wiebrand Cnossen RA, die als controleleider werkzaam is in de controlepraktijk bij MTH te Hoevelaken;  - Interview: Dhr. Chris Steenbeek RA, die werkzaam is in de controlepraktijk bij MTH te Hoevelaken;  - Observatie: Raadplegen van een aantal controledossiers. |
| 6 | *Welke IT-beheersmaatregelen, waaronder general en application IT controls, zijn bij de controle van MKB-bedrijven voor de accountant van belang om te kunnen steunen op de AO/IB?* | MKB-bedrijven een inzicht geven in toepasbare IT-beheersmaatregelen voor het realiseren van een correct en fatsoenlijk IT beheer, dat aansluit met de businessbehoeften. Bedrijfsdoelstellingen kunnen op deze manier sneller en gemakkelijk worden gerealiseerd. De accountant hoeft daarentegen bij de controle minder aanvullende gegevensgerichte werkzaamheden uit te voeren. | **Desk research:** boeken, internet searches en (wetenschappelijke) artikelen  +  **Field research:** interviews en observaties | **Desk research:**  - (Bolland, 2011);  - (Bouker, n.d.);  - (Elsinga, 2014);  - (Fijneman, 2006);  - (Fijneman, 2009);  - (ISACA, 2012);  - (Lindgreen, 2005);  - (Looijen, 2011);  - (Noë, 2006);  - (Romney, 2012);  - (Zijlstra, 2002).  **Field research:**  - Interview: Dhr. Wiebrand Cnossen RA, die als controleleider werkzaam is in de controlepraktijk bij MTH te Hoevelaken;  - Interview: Dhr. Chris Steenbeek RA, die werkzaam is in de controlepraktijk bij MTH te Hoevelaken;  - Observatie: Raadplegen van een aantal controledossiers. |

\* **Tabel 1:** Koppeling met de geformuleerde deelvragen voor dit onderzoek

## 2.4 Betrouwbaarheid en validiteit

De geformuleerde deelvragen zijn in dit onderzoek beantwoord met behulp van literatuuronderzoek, interviews en observaties. Om de betrouwbaarheid van dit onderzoek te kunnen waarborgen, zijn de uitwerkingen van de interviews opgenomen in de bijlage van dit rapport. Tevens zijn meerdere personen geïnterviewd en meerdere controledossiers geraadpleegd om uiteindelijk een antwoord te krijgen op de geformuleerde hoofdvraag. Ook dit komt ten goede aan de betrouwbaarheid van het onderzoek.

Tijdens het onderzoek is het van belang dat je meet wat je moet meten. Voorafgaand aan het afnemen van de interviews zijn daarom de gemaakte interviewlijsten ter controle voorgelegd aan de bedrijfsmentor. De bedrijfsmentor heeft de interviewlijsten gecontroleerd en punten van verbetering aangekaart. Dit komt ten goede aan de validiteit. Bovendien hebben ook andere personen in de naaste omgeving, een check verricht op de interviewlijsten. Ten slotte zijn er tijdens de interviews, voortdurend check vragen gesteld om antwoorden te krijgen die relevant zijn voor het onderzoek.

# 3 IT Governance

In dit hoofdstuk zal nader worden ingegaan op het begrip ‘’IT Governance’’, waar bedrijven in de hedendaagse wereld steeds meer aandacht aan (moeten) schenken.

Elk bedrijf dient te streven naar het maximaliseren en waarborgen van de kwaliteit van de informatievoorziening (Fijneman, 2006). Het maximaliseren en waarborgen van de kwaliteit van de informatievoorziening wordt door bedrijven bewerkstelligd door het treffen van organisatorische, technische en procedurele maatregelen.

Daarnaast is het van belang dat een bedrijf voldoende aandacht schenkt aan het beoordelen of de maatregelen voldoende toereikend zijn en het beoordelen of de maatregelen in de dagelijkse praktijk in voldoende mate worden nageleefd. Een adequate informatiebeveiliging maakt hier een belangrijk onderdeel van uit en dient daarom door het management voldoende aandacht te krijgen (Fijneman, 2009).

Hieruit kan dus geconcludeerd worden, dat IT een kritische positie inneemt in het risicobeheersings- en controlesysteem. Er kan rond IT erg veel te beheersen zijn en de belanghebbenden bepalen uiteindelijk hoe tegen beheersing van IT wordt aangekeken. Het begrip ‘’IT Governance’’ speelt hierbij een enorm belangrijke rol. Op het moment dat het begrip ‘’IT Governance’’ verder wordt uitgediept, kan de volgende definitie worden gegeven, die is opgesteld door het Amerikaanse IT Governance Institute (Fijneman, 2006):

*‘’IT Governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization’s IT sustains and extends the organization’s strategies and objectives.’’*

De bovenstaande definitie van ‘’IT Governance’’ wordt in de praktijk het meeste gebruikt. IT Governance betekent eigenlijk niets anders dan een behoorlijk bestuur van de informatievoorziening. De definitie van het begrip ‘’IT Governance’’, is kort samengevat, een samenhangend geheel van verschillende componenten. Deze zijn (Fijneman, 2006):

* Beleid, procedures, management, organisatiestructuren, prestatie-indicatoren en de bijbehorende managementtechnieken die gezamenlijk een bijdrage leveren aan het behalen van de bedrijfsdoelstellingen;
* Een methode die als doel heeft om duidelijke verantwoordelijkheid en verantwoordelijken voor besluitvorming en prestaties te bepalen;
* Een mechanisme die als doel heeft om toegevoegde waarde te creëren voor het bedrijf, voor de beheersing en sturing van prestaties en voor de beheersing van risico’s;
* Een top-down verantwoordelijkheid van bestuurders en het management;
* Aansluiting bij het behalen van de bedrijfsdoelstellingen.

Het doel van ‘’IT Governance’’ is, dat het bestuur van een bedrijf kan laten zien de juiste beheersing van de IT-infrastructuur, de IT systemen en het netwerk te hebben gerealiseerd (Fijneman, 2009). Het is dus duidelijk dat IT beheer een vereiste voorwaarde is voor het realiseren van ‘’IT Governance’’ (Fijneman, 2006).

De IT-werkprocessen dienen effectief en efficiënt te worden geregeld, om uiteindelijk de bedrijfsstrategie te kunnen ondersteunen (Fijneman, 2009). Het is hierbij van belang, dat het bestuur integer en transparant handelt (Fijneman, 2006). Uiteindelijk dient de integriteit van de bedrijfsgegevens en daarmee een goede bedrijfsvoering te zijn gewaarborgd (Loon, 2013). Het is daarom ook van belang dat in een ‘’IT Governance’’ structuur door het bestuur toezicht wordt gehouden op de informatievoorziening en verantwoording wordt afgelegd over het uitgeoefende toezicht (Fijneman, 2006). Hieraan liggen een aantal primaire kwaliteitsaspecten voor de bedrijfsgegevens ten grondslag. Deze zijn (Loon, 2013):

* *Vertrouwelijkheid:* geautoriseerde toegang tot gegevens;
* *Integriteit:* correcte gegevens, waarbij tijdigheid, juistheid en volledigheid een belangrijke rol spelen;
* *Beschikbaarheid:* beschikbaarheid van gegevens voor een constante bedrijfsvoering;
* *Controleerbaarheid:* wie heeft wat gedaan en het afleggen van verantwoording.

Er zijn een aantal redenen, waarom bedrijven voldoende aandacht moeten schenken aan ‘’IT Governance’’. De redenen zijn (Bolland, 2011; Fijneman, 2006):

* Met behulp van geautomatiseerde informatiesystemen wordt tegenwoordig een enorm groot gedeelte van de financiële verslaggeving en beheersingsinformatie: ingevoerd, opgeslagen en bewerkt, en verstrekt;
* Tegenwoordig is in geautomatiseerde informatiesystemen met behulp van geautomatiseerde controles in de programmatuur, een zeer groot gedeelte van het raamwerk van interne controle geïntegreerd;
* De beheersingsmaatregelen in de IT-beheerorganisatie, ook wel general IT-controls genoemd, zijn van grote invloed op de permanente werking van de geautomatiseerde controles;
* De kosten en investeringen met betrekking tot IT, zijn op dit moment al in veel bedrijven enorm hoog en het ziet er naar uit dat dit in de toekomst alleen maar duurder zal worden. Het komt overigens vaak voor dat deze kosten van materieel belang zijn voor de jaarrekening.

Verschillende ‘’IT Governance’’ beheermethodieken en kwaliteitsnormen kunnen worden ingezet om IT beheersbaar te maken en om de kwaliteit van IT naar een hoger niveau te tillen (Fijneman, 2006). Een bekend voorbeeld van zo’n uitgewerkte ‘’IT Governance’’ beheermethodiek, is COBIT. Deze beheermethodiek, tezamen met de beheermethodiek en kwaliteitsnorm ITIL en ISO 20.000, zullen later in dit rapport worden besproken.

# 4 Bronnen voor IT normen

De meeste bedrijfsprocessen binnen bedrijven kunnen niet meer zonder IT ondersteuning uitgevoerd worden (Bolland, 2011). IT is echter enorm kostbaar en zal in de toekomst alleen maar duurder worden, wat al eerder in dit rapport is aangegeven. Voor bedrijven is het dus van belang om grip te krijgen op IT, om zodoende de bedrijfscontinuïteit te kunnen garanderen.

In de praktijk zijn hiervoor verschillende theoretische beheermethodieken en kwaliteitsnormen te gebruiken. Op deze manier kunnen bedrijven IT-processen inrichten, beheersen en verbeteren (Noë, 2006). Deze beheermethodieken en kwaliteitsnormen bevatten verschillende IT-beheersmaatregelen en worden voornamelijk toegepast binnen grote bedrijven. Uit onderzoek blijkt echter dat MKB-bedrijven hierin nog enigszins achterlopen, door de enorm hoge implementatiekosten (Bolland, 2011). Bovendien is het implementeren van beheermethodieken en kwaliteitsnormen over het algemeen een enorm complex proces. Reden genoeg om hier verandering in te brengen en een beheermethodiek te ontwikkelen met algemene IT-beheersmaatregelen, die gebruikt kan worden door MKB-bedrijven om grip te krijgen op IT.

Om deze beheermethodiek te kunnen ontwikkelen, zullen allereerst de beheermethodieken en kwaliteitsnormen: ITIL, ISO 20.000 en COBIT, in dit hoofdstuk worden besproken en vergeleken (Noë, 2006; Looijen, 2011). Voor deze beheermethodieken en kwaliteitsnormen is gekozen, omdat deze op dit moment in de praktijk veelvuldig worden toegepast bij grote bedrijven en actueel zijn.

Uiteindelijk zullen er elementen worden gebruikt uit deze beheermethodieken en kwaliteitsnormen voor de ontwikkeling van de beheermethodiek met algemene IT-beheersmaatregelen, die speciaal is gericht op MKB-bedrijven.

Voordat de beheermethodieken en kwaliteitsnormen in dit hoofdstuk zullen worden besproken, is het even van belang om te melden dat er bij beheer van IT, drie vormen zijn te onderscheiden. Deze zijn (Looijen, 2011):

* *Functioneel beheer:* het management is verantwoordelijk voor de instandhouding van de functionaliteit van de informatiesystemen, waarbij de gebruikerszijde van de informatiesystemen centraal staat. Het functioneel beheer ondersteunt hier het gebruik van de functionaliteiten, het evalueert het gebruik en het reageert op problemen en nieuwe wensen die tot veranderingen kunnen leiden. Onder functioneel beheer wordt verstaan: technische ondersteuning, algemene bedrijfsondersteuning, personeelsmanagement, gebruikersbeheer en functioneel onderhoud;
* *Applicatiebeheer:* op een bedrijfsmatig verantwoorde manier verzorgt het management het beheer, het onderhoud en de vernieuwing van applicaties. Onder applicatiebeheer wordt verstaan: technische ondersteuning, algemene bedrijfsondersteuning, personeelsmanagement en applicatie-onderhoud;
* *Technisch beheer:* op een bedrijfsmatig verantwoorde manier verzorgt het management het beheer van technische infrastructuren. Hierbij kan gedacht worden aan netwerk- en werkplekbeheer etc. Onder technisch beheer wordt verstaan: technische ondersteuning, algemene bedrijfsondersteuning, personeelsmanagement, operationele besturing, onderhoud technische infrastructuur en operationele ondersteuning, en technische dienstverlening.

In dit onderzoek, zal de aandacht voornamelijk uitgaan naar het functionele beheer van IT.

## 4.1 ITIL

ITIL, oftewel Information Technology Infrastructure Library, richt zich primair op het technische beheer van IT (Looijen, 2011). ITIL is een de-factostandaard, wat eigenlijk niets anders betekent dan dat deze methodiek door de markt is bepaald (Noë, 2006). Deze methodiek bestaat uit een aantal richtlijnen, ook wel best practices genoemd, voor het beheer van informatiesystemen (Noë, 2006; Fijneman, 2009). Tevens bevat deze methodiek diverse modules voor het beheer van IT-processen.

Uiteindelijk heeft deze normenset als doel om de IT-beheerorganisaties procesmatig in te richten (Looijen, 2011). ITIL is niet zozeer een model of methodiek, maar meer een opsomming van best practices voor het inrichten van IT-beheersprocessen binnen een organisatie. Het gebruik van deze best practices uit ITIL, levert een doorzichtige en meetbare organisatie op, waarmee IT-services afgestemd kunnen worden met de businessbehoeften (Croon, 2008; Noë, 2006). Uiteindelijk zorgt het gebruik van ITIL voor de creatie van toegevoegde waarde voor een bedrijf.

Binnen ITIL wordt voor het realiseren van afstemming van de IT-services met de businessbehoeften en het sturen van de IT-services, die met het betreffende bedrijf zijn overeengekomen, gebruik gemaakt van ‘’Service Level Management’’ (SLM) als beheersproces. Dit beheerproces richt zich voornamelijk op tactisch en operationeel niveau en is eigenlijk niets anders dan het proces van plannen, coördineren, ontwerpen, onderhandelen en overeenstemming realiseren van servicesniveaus met de klant, en tevens het constant opvolgen, rapporteren en evalueren van servicesniveauprestaties, om eventueel tot verbeteracties te komen, die de overeengekomen servicesniveaus kunnen garanderen.

Door de jaren heen is ITIL wereldwijd enorm gegroeid in populatie en uit onderzoek blijkt dat vrijwel alle IT-beheersorganisaties, zo ook in Nederland, ITIL gebruiken voor de inrichting van hun IT-beheersorganisatie. Het grote voordeel van ITIL is dat de best practices in verschillende soorten bedrijven toepasbaar zijn (Noë, 2006). Uit de praktijk blijkt dat de meest succesvolle implementaties voortkomen uit een flexibele aanpak, waarbij verder wordt gekeken dan alleen naar inhoudelijke procesmatige zaken, als aanpassing van de organisatiestructuur etc. (Looijen, 2011). Hieruit kan dus geconcludeerd worden dat het implementeren van ITIL bij ieder bedrijf weer anders is en afhangt van de specifieke situatie van het desbetreffende bedrijf.

De toepassing van ITIL heeft natuurlijk verschillende voordelen, echter ook een aantal nadelen. Even kort de voor- en nadelen op een rij:

**Voordelen** (Looijen, 2011; Noë, 2006)**:**

* Kostenreductie;
* Verbetering in klanttevredenheid door de toepassing van best practices;
* Verbetering in serviceorganisatie door een meer professionele aanpak;
* Begeleiding en standaardisering;
* Verhoging productiviteit, efficiëntie en effectiviteit;
* Toepasbaar in verschillende soorten organisaties;
* Een zeer toegankelijke beheermethodiek;
* Verhoging van gebruik van ervaring en vaardigheden.

**Nadelen** (Bolland, 2011; Looijen, 2011; Noë, 2006)**:**

* Hoge implementatiekosten;
* Moeilijk te implementeren door vele gecompliceerde regels;
* Voornamelijk gericht op IT-serviceverleners aan de aanbodzijde;
* Er ontbreekt een apart model om risico’s te managen;
* Onvoldoende aandacht voor functioneel beheer.

ITIL heeft zich door de jaren heen verder ontwikkeld. Hieronder zal verder worden ingegaan op de meest actuele versie van ITIL: ITIL versie 3.

### 4.1.1 Service Lifecycle

De kern van ITIL versie 3 wordt gevormd door een ‘’Service Lifecycle’’ en bestaat uit een aantal fasen (Looijen, 2011). De verschillende fasen zijn (Looijen, 2011):

* *Service Strategy:* de fase die zich richt op het ontwerpen, het ontwikkelen en het implementeren van servicemanagement als een strategisch middel;
* *Service Design:* de ontwerpfase die zich richt op het ontwikkelen van IT-services, inclusief processen, architectuur, beleid en documenten. Het uitgangspunt die hierbij gehanteerd wordt is het voldoen aan de huidige en toekomstige businessbehoeften;
* *Service Transition:* deze fase hanteert de ontwikkelde specificaties bij de fase ‘’Service Design’’ als uitgangspunt . Deze specificaties worden omgezet naar nieuwe of gewijzigde IT-services;
* *Service Operation*: de fase die zich richt op de ondersteuning van IT-services en het efficiënter en effectiever inrichten van de IT-services. Op deze manier wordt een zo groot mogelijke toegevoegde waarde voor de klant en de IT-serviceverlener gecreëerd;
* *Continual Service Improvement:* de fase die zich richt op het onderhoud van de toegevoegde waarde voor de klanten. Het gaat hierbij om het draaiende krijgen of houden van het verbeterwiel van een organisatie (Croon; 2008). Dit wordt gerealiseerd door ontwerpverbeteringen door te voeren en nieuwe services te introduceren (Looijen, 2011).

Op het moment dat de verschillende fasen van de ‘’Service Lifecycle’’ in beschouwing worden genomen, kan geconcludeerd worden dat ITIL versie 3 voornamelijk is gericht op een continue verbetering van services, met verschillende verbetermodellen en technieken (Looijen, 2011). Hieronder, ter verduidelijking, een grafische weergave van ITIL versie 3:



\* **Figuur 2:** Grafische weergave van ITIL versie 3 (Stevens & Van Grembergen, 2008)

Tot slot zal een nadere beschrijving van de vijftal fasen van de ‘’Service Lifecycle’’ hier buiten beschouwing worden gelaten. Deze is echter wel opgenomen in de bijlage van dit rapport.

### 4.1.2 ITIL implementaties

In de praktijk gebeurt het vaak dat er een aantal mensen binnen een organisatie, een ITIL-training krijgen, waarna zij aan de slag kunnen gaan met het implementeren van één of meerdere processen uit ITIL. Veel implementaties blijken echter niet te voldoen aan de verwachtingen, waarbij het vaak voorkomt dat verwachtingen te hoog zijn gesteld en/of niet volledig zijn waargemaakt. Bedrijven zijn vaak ontevreden over het rendement van het procesmatige beheer van hun informatiesystemen. In veel gevallen wordt daarom vaak teruggeschakeld naar de ‘’oude’’ manier van werken. Toch realiseren bedrijven zich dat IT beheer enorm van belang is voor het ondersteunen van de bedrijfsprocessen en dat er dus voldoende aandacht moet worden besteed aan het beheersen van IT-processen.

Het implementeren van ITIL binnen IT-organisaties is een enorm tijdrovend proces en voor veel organisaties een moeilijke onderneming (ITSMF, n.d.; Van Beem, n.d.). Veel bedrijven zijn een aantal jaren geleden begonnen met het implementeren van één of meerdere processen uit ITIL en er zijn bedrijven die de implementatie nog steeds niet hebben afgerond.

Er zijn zelfs bedrijven die al meerdere ITIL-implementaties achter de rug hebben. De onsuccesvolle implementaties van ITIL worden vaak veroorzaakt doordat bedrijven teveel bezig zijn met de ITIL-theorie (Jerphanion, n.d.). Het is immers zo dat ITIL een theorie is. Om de implementaties van ITIL echter goed te kunnen laten verlopen, dienen bedrijven niet uit te gaan van de ITIL-theorie maar van een concreet probleem of een concrete verbetering.

Bij de implementatie van ITIL is het van belang dat het doel van de organisatie duidelijk is geformuleerd (Van Veen, n.d.). In een IT-organisatie maakt iedereen continu keuzes. Het is dus van belang dat iedereen binnen een IT-organisatie de verschillende belangen kent, waarmee rekening gehouden moet worden. In het geval van IT-organisaties moeten zij zich richten op de belangen van de klanten.

Bovendien dient bij de implementatie, de samenhang van de verschillende taken en rollen, duidelijk te zijn. Iedereen binnen een IT-organisatie dient een duidelijk beeld te hebben, van wat hij bijdraagt dan wel kan bijdragen aan het uiteindelijke resultaat.

Daarnaast is het bij de implementatie van belang dat iedere medewerker een rol/taak krijgt die bij hem/haar past, waarbij de kennis en ervaring afgestemd is met de betreffende rol/taak. Iedere medewerker moet immers keuzes maken en daarvoor over de juiste kennis en ervaring beschikken. In de meeste gevallen wordt hierbij gekeken naar vakkennis en kennis van ITIL. Er dient echter ook gekeken te worden naar de kennis van de (business van de) klant.

Ten slotte dient bij de implementatie stapsgewijs de manier van werken te worden verbeterd. Dit kan worden gerealiseerd door de medewerkers te leren betere keuzes te maken. Dit is een enorm tijdrovend proces en gaat in kleine stappen. Uiteindelijk zorgt dit wel voor betere keuzes en betere motivatie, en levert het dus een bijdrage aan het verbeterproces in de organisatie. Medewerkers weten waarom ze wat doen en worden tevens serieus genomen.

### 4.1.3 ITIL in de praktijk

ITIL wordt op dit moment, in vergelijking met de andere beheermethodieken en kwaliteitsnormen, veruit in de praktijk het meeste geïmplementeerd en is erg populair in Nederland (Bloemendal, n.d.; Looijen, 2011). De verwachting is nu, dat daar niet zo snel verandering in zal komen.

Uit recent onderzoek van ITSMF, blijkt dat ongeveer 85 procent van de IT-organisaties in Nederland, geheel of grotendeels gebruik maakt van ITIL. Dit is een stijging ten opzichte van het jaar 2005, waarbij dit nog 65 procent was. De reden dat ITIL onder Nederlandse bedrijven zo erg populair is, ligt in het feit dat ITIL altijd publiek eigendom is geweest. Er is immers geen specifieke leverancier of producent van ITIL. Er zijn enorm veel aanbieders op het gebied van consultancy en implementatie. Tevens is er meer dan genoeg documentatie beschikbaar. Een tweede reden dat ITIL onder Nederlandse bedrijven zoveel wordt gebruikt, ligt in het feit dat Nederland immers enorm afhankelijk is van IT (Noë, 2006).

Uit een ander onderzoek, waarbij onderzoek is gedaan naar de mate van ITIL-gebruik binnen verschillende IT-organisaties, blijkt dat ongeveer 39 procent van de onderzochte IT-organisaties, in hoge mate gebruik maakt van ITIL. Hierbij worden vrijwel alle processen uit de ‘’Service Lifecycle’’ gebruikt. Daarentegen maken 33 procent van de onderzochte IT-organisaties, in lage mate gebruik van ITIL, waarbij veelal één of enkele processen uit de ‘’Service Lifecycle’’ worden gebruikt.

Hieronder, ter verduidelijking, een grafische weergave van de resultaten uit dit onderzoek:

\* **Figuur 3:** Mate van ITIL-gebruik binnen de onderzochte IT-organisaties (Noë, 2006)

De laatste jaren groeit ITIL enorm in populariteit. Nederland stond altijd bovenaan de lijstjes voor wat betreft het gebruik en de kennis rondom ITIL. Op dit moment is ITIL echter met een opmars bezig in de Verenigde Staten, Zuid-Afrika, Australië en Oost-Europa (Bloemendal, n.d.).

ITIL wordt in de praktijk door duizenden bekende en internationale bedrijven gebruikt (APM Group Limited, 2010). Deze bedrijven zijn actief in verschillende bedrijfstakken en variëren in grootte.

Bekende voorbeelden van bedrijven die ITIL gebruiken, zijn (APM Group Limited, 2010):

* *Grote technologiebedrijven:* Microsoft, HP, Fujitsu en IBM;
* *Winkels:* Target, Walmart en Staples;
* *Financiële dienstenorganisaties:* Citi, Bank of America en Barclay’s Bank;
* *Entertainmentbedrijven:* Sony en Disney;
* *Fabrikanten:* Boeing, Toyota en Bombardier;
* *Biowetenschappelijke bedrijven:* Eli Lilly, Pfizer, Takeda en Pharmaceuticals.

## 4.2 ISO 20.000

Serviceorganisaties, oftewel organisaties die IT-diensten aanbieden, gebruiken de norm ISO 20.000 om aan te tonen dat hun IT-dienstverlening voldoet aan de internationale kwaliteitsnormen (Bouker, n.d.). Het is zowel mogelijk om certificering te verkrijgen op diensten als certificering van de gehele serviceorganisatie in zijn geheel (Looijen, 2011). In de praktijk blijkt het steeds vaker voor te komen dat klanten de voorkeur geven of de eis stellen, aan ISO-gecertificeerde serviceorganisaties bij opdrachten voor IT-diensten.

De kwaliteitsnorm ISO 20.000 is voortgevloeid uit de norm BS15.000. Het uitgangspunt van de norm BS15.000 zijn de best practices, uit de beheermethodiek ITIL, met een aantal uitbreidingen vanuit het kwaliteitsmanagementsysteem voor procesmatig werken uit de norm ISO 9.000 : 2.000.

De norm BS15.000, is in tegenstelling tot ITIL, een de-jurestandaard, waar ITIL een de-factostandaard is (Noë, 2006). Het verschil zit hem in het feit dat de-jurestandaard wordt bepaald door een officieel lichaam en de de-factostandaard door de markt. Eigenlijk is de norm BS15.000 niets anders dan een geformaliseerde versie van ITIL. Later is BS15.000 omgezet naar een ISO-norm: ISO 20.000. Tot op heden is ISO 20.000 een internationaal erkende norm voor IT Service Management (ITSM) (Looijen, 2011). ISO 20.000 is gerelateerd aan een aantal andere normen, waaronder BS7.799/ISO 17.799: ‘’Code of practice for Information Security Management’’ en ISO 27.001: ‘’Guidelines for Information Security Management’’ (Fijneman, 2006; Ten Hagen, 2013).

Het toepassen van de norm ISO 20.000 heeft natuurlijk verschillende voordelen, echter ook een aantal nadelen. Even kort de voor- en nadelen op een rij:

**Voordelen** (Fijneman, 2006; Van Bon, 2007)**:**

* Certificering leidt tot kwaliteitsverbetering;
* Certificering bevordert het streven naar het verbeteren van de kwaliteit van een organisatie;
* Certificering kan als marketingmiddel worden gebruikt richting opdrachtgevers;
* Certificering stimuleert om een nog hogere graad van certificering te behalen;
* Continue controle over de IT-processen;
* Grotere efficiency van dienstverlening;
* Creëren van kansen voor continue verbetering.

**Nadelen** (Van Bon, 2007; Van ‘t Hoff, 2008)**:**

* Er ontbreekt een nadere beschrijving over hoe iets geregeld moet worden;
* Er wordt geen uitspraak gedaan over welk type managementsysteem er toegepast moet worden;
* Geen onderkenning van een groeimodel;
* Hoge implementatiekosten;
* Elke kwaliteitsverbetering en ieder certificeringstraject is enorm tijdrovend.

Deze ISO-norm bestaat zelf uit twee delen (Noë, 2006). Enerzijds in ISO 20.000 : 1, waar de eisen worden beschreven waaraan een bedrijf moet voldoen om het certificaat te verkrijgen. Er zijn verschillende terreinen, waar deze eisen betrekking op hebben. Voorbeelden hiervan zijn:

* Requirements for a Management System;
* Planning and Implementation Service Management;
* Planning and Implementation New or Changed Services;
* Service Delivery Process;
* Relationship Processes;
* Resolution Processes;
* Release Processes;
* Control Processes.

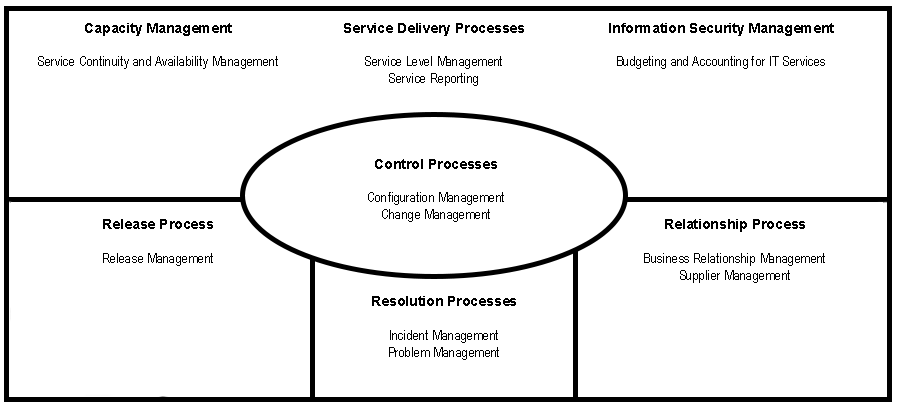
Op het moment dat een dergelijk bedrijf dus voldoet aan de eisen, is de ISO 20.000-certificatie een feit.

Anderzijds is deze ISO-norm onder te verdelen in: ISO 20.000 : 2, waar een beschrijving wordt gegeven van de praktijkcode voor IT Service Management (ITSM) (Looijen, 2011). In dit deel worden procesbeschrijvingen, oftewel best practices, uiteengezet. Deze procesbeschrijvingen kunnen eventueel gebruikt worden om aan de normen van deel één te voldoen. Dit tweede deel is voornamelijk van belang voor bedrijven die erkenning willen hebben van een onafhankelijke partij, en die zich daarop willen voorbereiden, of verbeteringen willen aanbrengen op het terrein van IT Service Management (ITSM) (Noë, 2006). Het uitgangspunt van deze praktijkcode, oftewel ISO 20.000 : 2, zijn de processen die in ITIL worden onderscheden met aanvullingen op het gebied van servicerapportage en relatiebeheer. Alleen het proces ‘’Financial Management’’, dat wel in ITIL is te vinden, is niet gebruikt in de kwaliteitsnorm ISO 20.000. Dit kwam door het feit dat een aantal financiële experts het niet eens konden worden over de invulling van het proces ‘’Financial Management’’. Daarom heeft men besloten om in de kwaliteitsnorm ISO 20.000 alleen aan te geven dat er wat gedaan moet worden aan financial management, zonder aan te geven hoe dit bewerkstelligd moet worden.

Met betrekking op het eerste deel van deze ISO-norm is een certificeringsschema opgesteld, met alle criteria waaraan een bedrijf moet voldoen om een certificaat te kunnen verkrijgen (Looijen, 2011). Het invoeren van een geïntegreerde procesbenadering om diensten aan klanten te kunnen leveren, is één van de uitgangspunten.

De kwaliteitsnorm ISO 20.000 bestaat tevens uit een vijftal processen met een geïntegreerde procesaanpak en normen voor de inrichting van dertien processen. Deze processen geven invulling aan het tweede deel van deze ISO-norm en worden hier niet nader beschreven. In de bijlage van dit rapport is echter wel een nadere beschrijving van deze processen opgenomen.

Hieronder, ter verduidelijking, een grafische weergave van het tweede deel van ISO 20.000 met de bijbehorende vijf processen:



\* **Figuur 4:** Grafische weergave van ISO 20.000 : 2 (Looijen & Van Hemmen, 2011)

Zoals al eerder in dit rapport is gemeld, bestaat ISO 20.000 deels uit de best practices van de beheermethodiek ITIL.

Het is echter bij de certificatie niet van belang om ITIL als beheermethodiek te hanteren. Voor de (externe) auditor is het alleen van belang om aan de hand van de ISO 20.000-certificering, waar te kunnen nemen dat de dienstverlening van de IT-dienstverlener kwalitatief goed is en voldoet aan de businessbehoeften van de klant.

### 4.2.1 ISO 20.000 implementaties

ISO 20.000 is eigenlijk niets anders dan een geformaliseerde versie van ITIL, met als uitgangspunt de processen die in ITIL worden onderscheden en aanvullingen op het gebied van servicerapportage en relatiebeheer (Noë, 2006). Hierdoor is de implementatie van ISO 20.000 bijna gelijk aan de implementatie van ITIL en daarom zal in dit hoofdstuk niet gedetailleerd worden ingegaan op de implementatie van ISO 20.000.

ISO 20.000-certificering is al enorm populair en die populariteit zal in de toekomst alleen maar toenemen (BSI Group, n.d.). IT is voor veel bedrijven van onmisbare waarde en daarom is het van belang dat bedrijven een rendabele en kwalitatief goede IT-service aanbieden.

In elk bedrijf wordt weer een andere aanpak gehanteerd bij het beheersen van de IT-services. Elk bedrijf heeft immers weer speciale afdelingen, functionele uitdagingen en technologische eisen. Bedrijven dienen daarom veel aandacht te schenken aan de implementatie van ISO 20.000, waarbij uiteindelijk aansluiting gevonden moet worden met de specifieke businessbehoeften.

Om de implementatie van ISO 20.000 goed te laten verlopen, dient aan de volgende vereisten te worden voldaan (BSI Group, n.d.):

* De ondersteuning en betrokkenheid van het ‘’Senior Management’’, oftewel het allerhoogste management, is enorm van belang en daar dient daarom ook voor te worden gezorgd;
* Het hele bedrijf dient bij het proces te worden betrokken. Dit kan worden bewerkstelligd door intern goed te communiceren;
* Het is van belang dat de bestaande processen voor IT-servicemanagement worden vergeleken met de eisen voor ISO 20.000;
* Het is van belang dat er feedback wordt gevraagd aan gebruikers, leveranciers en klanten over de realisatie van IT-servicemanagement;
* Om de te behalen resultaten te maximaliseren, dient er een implementatieteam te worden samengesteld;
* Het is van belang dat er duidelijkheid is over de rollen, verantwoordlijkheden en tijdspaden;
* De basisprincipes van ISO 20.000 dienen te worden toegepast;
* Met behulp van het aanbieden van cursussen en beloningen, moeten de medewerkers gemotiveerd worden om te participeren;
* Kennisdeling over de kwaliteitsnorm is enorm van belang. Daarnaast dienen de medewerkers gestimuleerd te worden om zich te laten omscholen tot Internal Auditors;
* Het is van belang dat het ISO 20.000-systeem regelmatig word geëvalueerd, om zodoende constante verbetering van het ISO 20.000-systeem te realiseren.

### 4.2.2 ISO 20.000 in de praktijk

In de praktijk is op dit moment een groei zichtbaar in het aantal bedrijven die ISO 20.000 zijn gecertificeerd (Mulder, 2012).

Volgens itSMF en Gartner, is de verwachting dat er over een aantal jaren geen enkele overheidsorganisatie meer is, die gebruik zal maken van de diensten van een dienstverlener die geen ISO 20.000 certificaat bezit (Polter, n.d.). Tevens is het al jaren zo dat de overheid eisen stelt aan de producten van leveranciers van beheersoftware met betrekking tot de toepassing van de ITIL-processen.

Op dit moment hebben voornamelijk (grote) internationale IT-bedrijven een ISO 20.000 certificaat (Mulder, 2012). Er zijn echter ook veel MKB-bedrijven, die ISO 20.000 gecertificeerd zijn.

Deze grote internationale bedrijven en MKB-bedrijven zijn actief in verschillende branches. Voorbeelden van bedrijven die op dit moment een ISO 20.000 certificaat bezitten, zijn (APM Group, n.d.; Polter, n.d.):

* Capgemini;
* PGGM IFS;
* Imtech ICT Communication Solutions;
* CACI B.V.;
* Info Support B.V..

Uit onderzoek van Quint Wellington Redwood, een managementadviesbureau, blijkt dat veelal Indische Service Providers, ISO 20.000 zijn gecertificeerd (Whizpr, 2007). De reden hiervan ligt in het feit dat Indische IT-dienstenleveranciers hun aanbod hebben geperfectioneerd met ‘’Global Delivery’’ modellen, die IT-diensten tegen lage kosten aanbieden. Daarnaast is de Indische dienstbaarheidscultuur op alle plaatsen populair en gewaardeerd.

Europa scoort enorm laag als het gaat om het aantal bedrijven met een ISO 20.000 certificaat. Duitsland en het Verenigd Koninkrijk staan aan kop voor wat betreft het aantal accreditaties. De Duitse “Gründlichkeit”-cultuur en het feit dat het Verenigd Koninkrijk met haar ‘’British Standards’’ een grondlegger is geweest van ISO 20.000, liggen hieraan ten grondslag. België is op dit moment erg afwachtend. Er zijn immers tot op heden nog weinig Belgische IT-dienstenleveranciers, die beschikken over een ISO 20.000 certificaat. Dit heeft voornamelijk te maken met de Belgische cultuur, die symbool staat voor het nemen van een afwachtende houding. Daarnaast geniet ISO 20.000 nog onvoldoende bekendheid, waardoor ISO 20.000 in de praktijk vaak wordt gerelateerd aan kwaliteitssystemen.

## 4.3 COBIT

COBIT, oftewel Control Objectives for Information and related Technology, heeft als doel om de IT-functie te beheren (Looijen, 2011). COBIT is mede gebaseerd op het algemeen aanvaarde COSO-model voor interne beheersing en biedt structuur voor het inrichten van ‘’IT Governance’’, waar het management verantwoordelijk is voor de inzet van IT (Fijneman, 2005; Bouker, n.d.). De meeste facetten van IT-beheersing worden door COBIT geraakt (Fijneman, 2005). Bedrijven hopen door de inzet van COBIT een antwoord te vinden op de vraag welke IT-beheersmaatregelen zij moeten inrichten om aan de hedendaagse eisen te kunnen voldoen (Lindgreen, 2005). Het is van belang dat die inzet van IT in overeenstemming is met de strategie en de doelstellingen van het desbetreffende bedrijf (Looijen, 2011). Hierbij kan de inzet van COBIT een bijdrage leveren aan de realisatie van de aansluiting tussen de bedrijfsvoering en de manier waarop IT wordt inzet om uiteindelijk de bedrijfsdoelstellingen te kunnen realiseren (Bouker, n.d.).

Deze beheermethodiek bestaat uit gedetailleerde beschrijvingen en richtlijnen voor IT-processen en is dus eigenlijk niets anders dan een geheel van functies, regels en andere disciplines, met als doel om de businessmanager en de IT-manager te ondersteunen (Bouker, n.d.; Looijen, 2011). Op deze manier kan het maximale uit de voordelen van IT worden gehaald. Die ondersteuning heeft daarbij voornamelijk betrekking op het operationele IT beheer, in het belang van de operationele bedrijfsprocessen. COBIT geeft niet echt antwoord op de vraag hoe iets bereikt moet worden, maar richt zich meer op de wat-vraag. Hieruit kan dus worden geconcludeerd dat COBIT, in tegenstelling tot ITIL, voornamelijk is gericht op de beheersing van IT-processen en in mindere mate op de inrichting van IT-processen (Bouker, n.d.). Meestal wordt daarom naast COBIT, ook gebruik gemaakt van andere standaarden, zoals ITIL en COSO, die zich meer richten op de inrichting van IT-processen.

De toepassing van COBIT heeft natuurlijk verschillende voordelen, echter ook een aantal nadelen. Even kort de voor- en nadelen op een rij:

**Voordelen** (Bouker, n.d.)**:**

* Behoefte om ‘’IT Governance’’ te implementeren dan wel te verbeteren;
* IT-doelstellingen verder laten afstemmen met de organisatiedoelstellingen;
* Standaardiseren en automatiseren van IT-processen;
* Noodzaak tot uniformering van processen bij overnames en fusies;
* Voldoen aan de van kracht zijnde wet- en regelgeving (SOX, WFT etc.);
* Uitbesteding, oftewel outsourcing;
* IT-kosten beheersbaar krijgen;
* Implementeren van een IT-control framework.

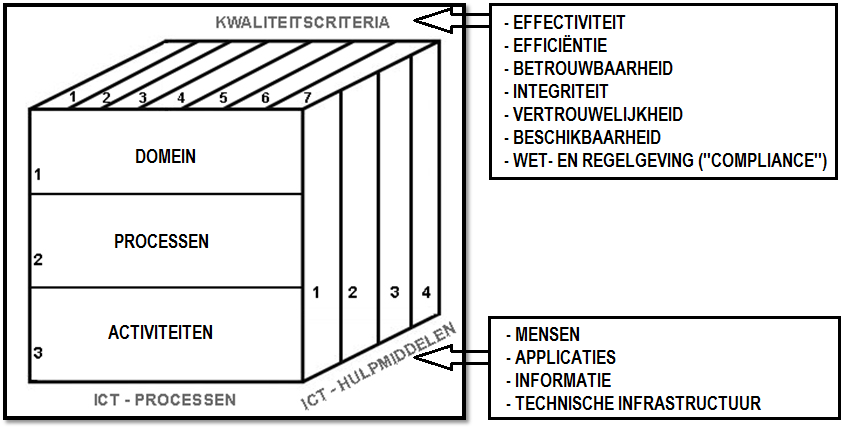
**Nadelen** (Lindgreen, 2005; Fijneman, 2005)**:**

* In sommige opzichten is de beheermethodiek te complex, te omvangrijk en te technisch;
* Op verschillende gebieden gaat de beheermethodiek voorbij aan de-factostandaarden (door de markt bepaald);
* Het belangrijke onderwerp, informatiebeveiliging, krijgt over het algemeen te weinig aandacht;
* De maatregelen in het domein ‘’monitoren en evalueren’’, horen feitelijk thuis in het domein ‘’plannen en organiseren’’.

Door de jaren heen is de beheermethodiek COBIT verder ontwikkeld en inmiddels is het een internationaal geaccepteerde beheermethodiek, die de laatste jaren enorm in populariteit is gegroeid. Dit kwam door het feit dat ‘’compliance’’, oftewel wet- en regelgeving, steeds meer aandacht kreeg. Bedrijven dienen tegenwoordig verplicht een control statement af te geven voor de belangrijke processen, inclusief de algemene IT-beheersprocessen. Hieronder zal verder worden ingegaan op de meest actuele versie van COBIT: COBIT 5.

### 4.3.1 COBIT-kubus

De beheermethodiek COBIT kan worden gepresenteerd in de vorm van een kubus. Deze kubus bestaat uit IT-processen, IT-hulpmiddelen en kwaliteitscriteria. Deze staan weergegeven in het voorvlak, het zijvlak en het bovenvlak van de kubus.

Hieronder, ter verduidelijking, een grafische weergave van de COBIT-kubus. Tevens is in de bijlage een grafische weergave van het gehele COBIT-5-principe opgenomen (figuur 6 en 7).

\* **Figuur 5:** Grafische weergave van de COBIT-kubus (Looijen & Van Hemmen, 2011)

Het uitwerken of overnemen van de bedrijfs- en compliance doelstellingen, is het vertrekpunt van COBIT (Bouker, n.d.). Zonder dit vooraf te doen, is er geen garantie meer dat de volgende stappen in het gehele proces een bijdrage zullen leveren aan het realiseren van de bedrijfsdoelstellingen.

Ten slotte zullen hieronder de elementen van de COBIT-kubus nader worden besproken, waarbij de doelstellingen van de IT-functie verder worden uitgewerkt.

#### 4.3.1.1 Voorvlak

In het voorvlak van de COBIT-kubus staan de IT-processen weergegeven (Looijen, 2011). Het voorvlak is onder te verdelen in een drietal deelvlakken. Deze zijn: domein, processen en activiteiten. Het deelvak domein vertegenwoordigd opeenvolgend weer vier verschillende domeinen. Deze zijn (Bouker, n.d.; Looijen, 2011):

* *Plannen en organiseren (‘’planning and organization’’):* richt zich op het uitwerken van de IT-strategie en IT-architectuur;
* *Verwerken en implementeren (‘’acquisition and implementation’’):* richt zich op het vertalen van de IT-strategie naar de implementatie van IT-oplossingen;
* *Diensten verlenen en ondersteunen (‘’delivery and support’’):* richt zich op het opleveren en beheren van de geïmplementeerde oplossingen;
* *Monitoren en evalueren (‘’monitoring’’):* richt zich op de beoordeling van IT, waarbij wordt bekeken of IT de gewenste bijdrage levert aan de bedrijfsdoelstellingen.

Deze vier domeinen die onderdeel uitmaken van het deelvlak ‘’domein’’, komen op een logische manier overeen met de verschillende fasen in de levenscyclus van informatiesystemen: strategie en planning, ontwikkeling en invoering, en productie en onderhoud (Lindgreen, 2005).

In de bijlage is een grafische weergave van de vier verschillende domeinen van COBIT 5 opgenomen (figuur 8).

Het deelvlak ‘’processen’’ vertegenwoordigd een aantal gestelde beheersingsdoelstellingen (‘’Control Objectives’’) op procesniveau (Lindgreen, 2005). Deze beheersingsdoelstellingen op procesniveau beschrijven de domeinen gedetailleerder (Bouker, n.d.; Looijen, 2011). In totaal zijn het zo’n 34 beheersingsdoelstellingen op procesniveau. In de bijlage is een vrij vertaald overzicht van deze beheersingsdoelstellingen op procesniveau opgenomen (figuur 9). De individuele beheersingsdoelstellingen sluiten erg goed aan op verschillende algemeen aanvaarde beheermethodieken, zoals ITIL (Lindgreen, 2005).

De 34 beheersingsdoelstellingen op procesniveau worden in het deelvlak ‘’activiteiten’’ verder uitgewerkt in doelstellingen op het niveau van activiteiten (‘’Minimum Controls’’). Het uiteindelijke gevolg is een raamwerk dat meer dan 300 verschillende beheersingsmaatregelen (‘’Control Measures’’) telt. Deze beheermaatregelen zijn gedocumenteerd in een document van maar liefst 155 pagina’s. Elk bedrijf streeft naar het realiseren van de 34 beheersingsdoestellingen, echter hoeven vanuit het efficiëntie-oogpunt niet alle beheersingsmaatregelen in alle diepgang te worden ingevoerd. Ten slotte bevat COBIT een verzameling van algemene auditrichtlijnen, inclusief 34 specifieke auditrichtlijnen die in overeenstemming zijn met de beheersingsdoelstellingen op procesniveau.

#### 4.3.1.2 Zijvlak

Het zijvlak van de COBIT-kubus is onder te verdelen in een viertal deelvlakken en richt zich primair op het technische beheer van IT (Looijen, 2011). In het zijvlak staan een viertal IT-hulpmiddelen weergegeven, die de activiteiten moeten uitvoeren dan wel ondersteunen. Deze IT-hulpmiddelen zijn (Looijen, 2011):

* *Mensen:* uitvoeren van de vier domeinen;
* *Applicaties:* ondersteunende informatiesystemen en procedures;
* *Informatie:* invoer en uitvoer van ondersteunende informatiesystemen;
* *Technische infrastructuur:* techniek voor de ondersteuning van de operationele processen.

De totstandkoming van de technische infrastructuur, heeft geen invloed op het gebruik van COBIT binnen een bedrijf (Bouker, n.d.). COBIT beoordeelt alleen of gemaakte beslissingen, met betrekking tot IT, de gewenste bijdrage leveren aan de bedrijfsdoelstellingen.

#### 4.3.1.3 Bovenvlak

Het bovenvlak van de COBIT-kubus is onder te verdelen in een zevental deelvlakken (Looijen, 2011). In het bovenvlak staan de kwaliteitscriteria weergegeven. Hierin zijn de eisen gedefinieerd, waaraan de output van IT moet voldoen (Bouker, n.d.). Een aantal voorbeelden hiervan zijn (Looijen, 2011):

* Effectiviteit;
* Efficiëntie;
* Betrouwbaarheid;
* Integriteit;
* Vertrouwelijkheid;
* Beschikbaarheid;
* In overeenstemming met de van kracht zijnde wet- en regelgeving (‘’compliance’’).

De deelvlakken van de COBIT-kubus zijn een samenhangend geheel en snijden elkaar. Een grafische weergave van alle samenhangende elementen van COBIT 5 is opgenomen in de bijlage (figuur 10). In zijn totaliteit is de COBIT-kubus hierdoor onder te verdelen in 3 x 4 x 7 = 84 kubusjes, die elk een lading hebben met een afgeleide van de IT-processen, de in te zetten IT-hulpmiddelen en de bijbehorende kwaliteitscriteria. Een aantal kubusjes is eigenlijk in werkelijkheid meer dan 84, doordat het voorvlak, met de IT-processen, opeenvolgend weer onder te verdelen is in een drietal deelvlakken.

### 4.3.2 COBIT implementaties

Op het moment dat IT-gebruikers en IT-medewerkers tevreden zijn over de werking van de IT en de toegevoegde waarde van de IT-functie, dan is alleen het kennisnemen van COBIT meer dan voldoende (Bouker, n.d.). Echter, op het moment dat bedrijven overwegen om met ‘’IT Governance’’ aan de slag te gaan of om een andere reden, dan is de implementatie van COBIT zeker het overwegen waard.

De duur van het implementeren van COBIT, hangt af van factoren als: de grootte van de organisatie en het gekozen vertrekpunt. Meestal kan het wel enkele jaren duren, voordat COBIT volledig is geïmplementeerd binnen een bedrijf. De implementatie zal sneller verlopen op het moment dat een bedrijf al bestaat en streeft naar structuur, dan wanneer een bedrijf nog in de startfase zit en de IT-organisatie wil inrichten. Tevens dient rekening gehouden te worden met het ambitieniveau (‘’Maturity Level’’), dat door het bedrijf wordt nagestreefd. Bij het implementeren van COBIT, is de betrokkenheid van alle belanghebbenden, oftewel alle stakeholders, enorm van belang. Kijkend naar de structuur van COBIT, is voornamelijk in de startfase van de implementatie deze betrokkenheid het belangrijkst. In de startfase worden immers de bedrijfsdoelstellingen vertaald naar IT-doelstellingen. COBIT hierbij beschouwen als een typisch IT-project, zal niet bijdragen aan het behalen van de bedrijfsdoelstellingen.

### 4.3.3 COBIT in de praktijk

COBIT is de afgelopen jaren enorm in populatie gegroeid (Lindgreen, 2005). Uit recent wereldwijd onderzoek van het IT Governance Institute en PwC onder 335 topmanagers, blijkt echter dat deze IT norm nog niet enorm veel wordt geïmplementeerd. Van de ondervraagde IT-organisaties, heeft immers 5 procent, COBIT geïmplementeerd. Hieruit kan dus worden geconcludeerd dat de acceptatiegraad van COBIT nog enorm beperkt is.

In Nederland zijn een aantal grote bedrijven en instellingen die gebruik maken van COBIT. Zo maken bijvoorbeeld PGGM en het UWV gebruik van COBIT, om interne auditwerkzaamheden te structureren. Philips, Fortis en Akzo Nobel maken daarentegen gebruik van COBIT, om IT-processen in te richten, te beheersen en te verbeteren.

Daarnaast blijkt uit de praktijk, dat veel bedrijven en instellingen gebruik van COBIT om ‘’Self Assessments’’ en normenkaders voor IT-auditors te ontwikkelen. Vaak wordt COBIT door bedrijven en instellingen, niet direct gebruikt. Er wordt vaker kennisgenomen van COBIT. In de praktijk wordt over het algemeen dus veel gepraat over COBIT, maar er wordt eigenlijk nog niet zoveel mee gedaan.

## 4.4 Vergelijking ITIL, ISO 20.000 en COBIT

In dit hoofdstuk zullen de beheermethodieken en kwaliteitsnormen: ITIL, ISO 20.000 en COBIT, die hiervoor reeds zijn besproken, worden vergeleken.

|  |  |  |  |
| --- | --- | --- | --- |
|  | ITIL | ISO 20.000 | COBIT |
| Eerste publicatie/ aantal versies | 1989/3 | 2003/1 | 1996/5 |
| Ontwikkelaar | Central Computer and Telecommunications Agency (CCTA) | International Organization for Standardization (ISO) | - IT Governance Institute (ITGI)  - Information Systems Audit and Control Association (ISACA) |
| Korte omschrijving | Een opsomming van best practices voor het inrichten van IT-beheersprocessen binnen een organisatie, met als doel om IT-services af te stemmen met de businessbehoeften. Uiteindelijk zorgt het gebruik van ITIL voor de creatie van toegevoegde waarde voor een bedrijf. | Een kwaliteitsnorm voor het certificeren van de IT-dienstverlening van organisaties om aan te tonen dat hun IT-dienstverlening voldoet aan de internationale kwaliteitsnormen. | Een beheermethodiek die bestaat uit gedetailleerde beschrijvingen en richtlijnen om de IT-processen te beoordelen op risico’s, volwassenheid en mogelijkheden. COBIT biedt structuur voor het inrichten van ‘’IT Governance’’, zodat het maximale uit de voordelen van IT kan worden gehaald. De meeste facetten van IT-beheersing worden door COBIT geraakt. |
| Theoretische achtergrond / gehanteerde theorie | - Best practices;  - Deming;  - Procestheorie;  - Publiek domein. | - BS7.799/ISO;  - BS8.600;  - BS/ISO 10.007;  - ISO 9.001;  - ISO 27.001;  - ITIL;  - Total Quality Management (TQM). | - BS7.799;  - COSO;  - ISO;  - ITIL. |
| Standaard | De-facto (bepaald door de markt) | De-jure (bepaald door een officieel lichaam) | De-facto (bepaald door de markt) |
| Focus | Inrichting van IT-processen (technisch beheer) | Het kwaliteitsniveau van de IT-dienstverlening naar een hoger niveau tillen | Beheersing van IT-processen (functioneel beheer) |
| Procesbreedte | Service- en Infrastructuur Management | De processen die in ITIL worden onderscheden, uitgezonderd het proces ‘’Financial Management’’, met aanvullingen op het gebied van servicerapportage en relatiebeheer | Veel verschillende IT-processen, waaronder gebruikersgerichte processen zoals ‘’Data Management’’ en ‘’Interne Audit’’ |
| Processen | - Hoe-vraag (gehele processen en functies in detail beschrijven);    - Er worden geen meetbare eisen gesteld aan de inrichting van processen. Aan de hand van praktijkervaringen (best practices) worden vele processen en de daar bijbehorende activiteiten beschreven;    - Werken de COBIT-domeinen “Acquisition and Implementation’’ en ‘’Delivery and Support’’, met de bijbehorende processen, verder uit;  - Werken het COBIT-domein ‘’Planning and Organization’’, met vijf processen, waaronder ‘’PO1. Definieer een strategisch IT-plan’’, verder uit;  - Software-  ontwikkelings-  processen en het proces “Supplier Management’’ komen aan bod in de COBIT-domeinen “Acquisition and Implementation’’ en ‘’Delivery and Support’’, met de processen ‘’A12. Acquireer en onderhoud de applicatiesoftware’’ en ‘’DS2. Beheers diensten die door derden worden geleverd’’;  - Besteedt te weinig aandacht aan het proces ‘’Human Resource Management’’;  - Besteedt te weinig aandacht aan het proces ‘’Compliance Management’’;  - Besteedt geen aandacht aan cultuur in termen van aansprakelijkheid en verantwoordelijkheid;  - Besteedt aandacht aan structuur in termen van rollen en verantwoordelijkheden. | - Hoe-vraag (gehele processen en functies in detail beschrijven);  - Er worden meetbare kwaliteitseisen gesteld aan de inrichting van de ITIL-processen. Met de ITIL-processen worden hier de processen bedoeld die rechtstreeks invloed kunnen uitoefenen op de relatie tussen klant en leverancier;  - Werken de COBIT-domeinen “Acquisition and Implementation’’ en ‘’Delivery and Support’’, met de bijbehorende processen, verder uit;  - Werken het COBIT-domein ‘’Planning and Organization’’, met vijf processen, waaronder ‘’PO1. Definieer een strategisch IT-plan’’, verder uit;  - Software-  ontwikkelings-  processen en het proces “Supplier Management’’ komen aan bod in de COBIT-domeinen “Acquisition and Implementation’’ en ‘’Delivery and Support’’, met de processen ‘’A12. Acquireer en onderhoud de applicatiesoftware’’ en ‘’DS2. Beheers diensten die door derden worden geleverd’’;  - Besteedt te weinig aandacht aan het proces ‘’Human Resource Management’’;  - Besteedt te weinig aandacht aan het proces ‘’Compliance Management’’;  - Besteedt geen aandacht aan cultuur in termen van aansprakelijkheid en verantwoordelijkheid;  - Besteedt aandacht aan structuur in termen van rollen en verantwoordelijkheden. | - Wat-vraag (alleen eisen stellen aan processen, zonder gehele processen in detail te beschrijven);  - De domeinen “Acquisition and Implementation’’ en ‘’Delivery and Support’’, met de bijbehorende processen, worden door de ITIL-processen verder uitgewerkt;  - Het domein ‘’Planning and Organization’’, met vijf processen, waaronder ‘’PO1. Definieer een strategisch IT-plan’’, worden door de ITIL-processen verder uitgewerkt;  - In de COBIT-domeinen “Acquisition and Implementation’’ en ‘’Delivery and Support’’, met de processen ‘’A12. Acquireer en onderhoud de applicatiesoftware’’ en ‘’DS2. Beheers diensten die door derden worden geleverd’’, komen de softwareontwikkelings- processen en het proces “Supplier Management’’ uit ITIL aan bod;  - Besteedt aandacht aan het proces ‘’Human Resource Management’’ ;  - Besteedt aandacht aan het proces ‘’Compliance Management’’;  - Aan de organisatiedoelstellingen, zo ook met betrekking tot Compliance, worden IT-doelstellingen en de daarbij bijbehorende processen gekoppeld;  - Besteedt geen aandacht aan cultuur in termen van aansprakelijkheid en verantwoordelijkheid;  - Besteedt aandacht aan structuur in termen van rollen en verantwoordelijkheden. |
| Certificering (als individu) | - EXIN;  - ISEB. | Niet mogelijk | - AB Consulting;  - KPMG;  - ITSM Consulting;  - Conlea;  - Wakaru. |
| Certificering (als organisatie) | PinkVerify | - BSI Management Systems;  - BVQI;  - DNV Certification;  - KPMG Audit;  - DQS;  - LRQA. | - Business Beam;  - Deltamine;  - DUX Diligens;  - itService;  - Netaccess Consulting Services;  - Peter Davis;  - Vyom Labs. |

\* **Tabel 2:** Vergelijking ITIL, ISO 20.000 en COBIT (Bouker, n.d.; Croon, 2008; Fijneman, 2005; Fijneman, 2009; ISACA, n.d.; Lindgreen, 2005; Looijen, 2011; Noë, 2006; Stevens, 2008; Ten Hagen, 2013 & Van Gils, 2005)

Hieruit kan geconcludeerd worden, dat ITIL, in tegenstelling tot COBIT, met betrekking tot de verschillende processen, meer antwoord geeft op de vraag hoe iets bereikt moet worden. Waar ITIL meer is gericht op de inrichting van IT-processen en dus op het technische beheer van IT, is COBIT meer gericht op de beheersing van IT-processen en dus op het functionele beheer van IT.

Ook de kwaliteitsnorm ISO 20.000, is net als ITIL, meer gericht op de inrichting van IT-processen. ISO 20.000 is immers een geformaliseerde versie van ITIL, met de processen die in ITIL worden onderscheden als uitgangspunt en aanvullingen op het gebied van servicerapportage en relatiebeheer. Het proces ‘’Financial Management’’, dat te vinden is in ITIL, komt daarentegen niet aan bod in ISO 20.000.

COBIT besteedt in de processen veel aandacht aan ‘’Compliance Management’’ en ‘’Human Resource Management’’. ITIL en ISO 20.000 doen dat daarentegen niet. De domeinen ‘’Planning and Organization’’, “Acquisition and Implementation’’ en ‘’Delivery and Support’’, die in COBIT worden onderscheden, met de bijbehorende processen, komen in veel gevallen ook aan bod in de ITIL-processen of worden nader uitgewerkt in de ITIL-processen.

Zoals al eerder in dit rapport is aangegeven, maken voornamelijk grote ondernemingen gebruik van ITIL, ISO 20.000 en COBIT. De redenen hiervan zijn in dit rapport reeds besproken. Dat betekent niet dat het voor MKB-bedrijven niet interessant is om deze beheermethodieken en kwaliteitsnormen te gebruiken. MKB-bedrijven hebben zeker wel wat aan deze beheermethodieken en kwaliteitsnormen en zouden deze bronnen voor IT normen kunnen gebruiken, door niet alle processen integraal over te nemen maar een selectie te maken van de processen, die van belang zijn voor het bedrijf. Het gebruik van deze beheermethodieken en kwaliteitsnormen draagt immers bij aan het realiseren van een correct en fatsoenlijk IT beheer en zorgt ervoor dat MKB-bedrijven in ieder geval bezig zijn met ‘’IT Governance’’ en hier dus voldoende aandacht aan schenken. Doordat ITIL, ISO 20.000 en COBIT, met betrekking tot de verschillende processen, elkaar aanvullen, is het tevens aan te raden, om als MKB-bedrijf, deze bronnen voor IT normen naast elkaar te gebruiken.

# 5 Bronnen voor IT normen in relatie tot IT Governance

In dit hoofdstuk zal worden beschreven hoe de verschillende beheermethodieken en kwaliteitsnormen, invulling geven aan het begrip ‘’IT Governance’’.

Verschillende ‘’IT Governance’’ beheermethodieken en kwaliteitsnormen, zoals ITIL, ISO 20.000 en COBIT, kunnen worden ingezet om ‘’IT Governance’’ te realiseren (Fijneman, 2006).

ITIL en ISO 20.000 leveren een bijdrage aan het realiseren van “IT Governance’’, door te streven naar het creëren van toegevoegde waarde voor een bedrijf (Croon, 2008; Noë, 2006). In ITIL versie 3 en ISO 20.000 komt dit erg goed naar voren in de twee componenten: ‘’Utility’’ (Fitness for Purpose: geschiktheid voor het doel) en ‘’ Warranty ‘’ (Fitness for Use: geschiktheid voor gebruik).

Het is van belang dat een IT-service voldoet aan de wensen van de gebruikers (‘’Use’’) en tevens de realisatie van de bedrijfsdoelstellingen waarborgt (‘’Purpose’’) (Croon, 2008).

Bovendien is het van belang dat een IT-service stuurbaar is, met als gevolg dat dit weer een groot aantal criteria oplevert om IT-prestaties (‘’IT-Performance’’) te kunnen beheersen.

De beheermethodiek COBIT vult ITIL weer aan met een extra kwaliteitscriterium, namelijk ‘’Compliance’’. Bedrijfsprocessen zijn onderworpen aan wettelijke en contractuele regelingen. Binnen het kwaliteitscriterium ‘’Compliance’’, is het van belang dat het interne beleid is afgestemd met de van buitenaf opgelegde wettelijke en contractuele regelingen. Hieruit kan worden geconcludeerd, dat COBIT zowel naar interne als externe factoren kijkt, die invloed hebben op de sturing van een bedrijf.

De bedrijfsdoelstellingen, die gerelateerd zijn aan ‘’Compliance’’, worden door COBIT erkend. Tevens associeert COBIT de IT-doelen en de daar bijbehorende processen aan de bedrijfsdoelstellingen, om zodoende de bedrijfsdoelstellingen te kunnen behalen. Die combinatie tussen enerzijds prestaties, oftewel ‘’Performances’’, en anderzijds wet- en regelgeving, oftewel ‘’Compliance’’, zorgt voor ‘’IT Governance’’. In de praktijk is COBIT hierdoor goed te gebruiken in combinatie met ITIL, om invulling te geven aan ‘’IT Governance’’ en de fase ‘’Continual Service Improvement’’.

IT-organisaties dienen niet één van de beheermethodieken en kwaliteitsnormen te gebruiken, om te zorgen dat de IT-organisatie een hoger of beter kwaliteitsniveau behaald (Fijneman, 2006). Het is juist van belang dat een IT-organisatie meerdere beheermethodieken en kwaliteitsnormen gebruikt. Veel beheermethodieken en kwaliteitsnormen vullen elkaar immers aan, zoals ITIL en COBIT. De componenten van de verschillende beheermethodieken en kwaliteitsnormen dienen uiteindelijk op zodanige wijze gebruikt te worden, dat er als geïntegreerd onderdeel van de ‘’normale’’ governancestructuur, een IT-beheersorganisatie kan worden gerealiseerd, die als het gaat om sturing en beheersing perfect is afgestemd op de rest van de organisatie. Om dit te kunnen bewerkstelligen is het van belang, dat er wordt verwezen naar meer algemene (niet-IT-specifieke) modellen, zoals het COSO-model, en de primaire kwaliteitsaspecten voor de bedrijfsgegevens: vertrouwelijkheid, integriteit, beschikbaarheid en controleerbaarheid.

# 6 Informatiebeveiliging

In dit hoofdstuk zal worden ingegaan op het belang van informatiebeveiliging, waarna in het volgende hoofdstuk de resultaten van het empirisch onderzoek zullen worden besproken.

Tegenwoordig is een belangrijk onderdeel van de bedrijfsstrategie, de informatievoorziening, en in de toekomst zal dat belang zeker niet minder worden (Fijneman, 2006). De meeste bedrijfsprocessen binnen bedrijven worden immers ondersteund door IT systemen. Het gevolg hiervan is dat door fouten in de programmatuur of operationele problemen in de computerverwerking, de bedrijfscontinuïteit in gevaar kan komen.

De laatste jaren hebben bedrijven steeds meer te maken met bedreigingen en kritische toepassingen als het gaat om IT (Romney, 2012). Veranderingen in de IT dienen zich in hoog tempo aan en de mogelijkheden van IT nemen steeds meer toe (Fijneman, 2009). Dit leidt tot enorm grote zorgen voor het management van een bedrijf. Veel bedrijven hebben steeds meer te maken met grootschalig verlies aan data en/of het regelmatig niet beschikbaar zijn van een website. Dit leidt tot enorm veel negatieve publiciteit, wat weer imagoschade tot gevolg kan hebben, en financiële schades. Uiteindelijk kan dit alles ervoor zorgen dat een bedrijf niet ‘’in control’’ is, waardoor de bedrijfscontinuïteit in gevaar kan komen.

In dit geval is het dus van belang dat bedrijven bij dit soort incidenten, direct actie ondernemen en zoeken naar samenhangende oplossingen. Op bestuursniveau dienen uiteindelijk beslissingen te worden genomen om acties daadwerkelijk te bewerkstelligen.

Snelle en adequate reactieve handelingen verrichten bij incidenten, met betrekking tot IT, is dus enorm belangrijk (Looijen, 2011). Bedrijven willen echter liever zoveel mogelijk incidenten, met betrekking tot IT, voorkomen. Hiervoor dienen bedrijven preventieve handelingen te verrichten, zoals het opstellen van een duidelijk IT-beleid, om een adequate informatiebeveiliging te kunnen realiseren.

Informatiebeveiliging bestaat uit het geheel van apparatuur, programmatuur, gegevens, procedures en technische voorzieningen (Looijen, 2011). De volgende definitie kan voor het begrip ‘’informatiebeveiliging’’ worden gegeven (Looijen, 2011):

*‘’Het treffen en onderhouden van een samenhangend pakket maatregelen ter waarborging van de betrouwbaarheid van gegevensverwerking en informatievoorzieningsprocessen.’’*

Uiteindelijk gaat het er dus om, dat er binnen bedrijven voldoende en adequate maatregelen worden genomen om de primaire kwaliteitsaspecten voor de bedrijfsgegevens te kunnen ondersteunen.

Op het moment dat het begrip ‘’informatiebeveiliging’’ verder wordt uitgediept, kan worden gesteld dat informatiebeveiliging zich bezighoudt met (Looijen, 2011):

* Het omschrijven van informatiebeveiligingseisen- en randvoorwaarden;
* Het bepalen van informatiebeveiligingsniveaus, de daar bijbehorende risico’s en de mate waarin de risico’s acceptabel zijn;
* Het omschrijven en implementeren van een informatiebeveiliging beleid, informatiebeveiligingsarchitectuur en informatiebeveiligingsmaatregelen;
* Het controleren en evalueren van informatiebeveiligingsmaatregelen en het daar bijbehorende beveiligingsniveau.

Op het moment dat het informatiebeveiligingsniveau van een te lage kwaliteit is, is het risico op verstoring van de IT systemen groter, dan wanneer de kwaliteit van het informatiebeveiligingsniveau hoger is (Looijen, 2011). Het is dus van belang dat er op bestuursniveau bewust wordt omgegaan met risico’s en risicobeheersing, oftewel informatiebeveiliging. Op bestuursniveau moet men weet hebben van de risico’s die men loopt en hoe groot die risico’s zijn. Zo dient men bijvoorbeeld de bedreigingen in kaart te brengen, met de kans van uiting van de verschillende bedreigingen. De bedreigingen kunnen in vier categorieën worden onderscheden (Looijen, 2011):

* *Bedreigingen van natuurlijke aard:* aardbeving, bliksem, overstromingen en storm;
* *Bedreigingen van niet-opzettelijke aard:* brand, explosies, graafwerkzaamheden, lucht- en wegverkeer, onopzettelijk handelen, schokken, straling, stroomstoring, vervuiling en wateroverlast;
* *Bedreigingen van opzettelijke aard:* bruut geweld, computervirussen, diefstal, opzettelijk handelen en stakingen;
* *Bedreigingen van technische aard:* storingen in apparatuur, fouten in programmatuur en storingen in technische voorzieningen.

Na het in kaart brengen van de bedreigingen en het inschatten van de risico’s met betrekking tot de uiting van de verschillende bedreigingen, dienen adequate maatregelen te worden getroffen om de risico’s te mitigeren en gevolgschade aan informatiesystemen en bedrijfsprocessen te voorkomen. De maatregelen kunnen in drie categorieën worden onderscheden (Fijneman, 2006; Looijen, 2011):

* *Preventieve maatregelen:* maatregelen die ervoor moeten zorgen dat een bedreiging niet optreedt, bijvoorbeeld onbrandbare materialen en beveiligingsprogrammatuur;
* *Repressieve maatregelen:* maatregelen die ervoor moeten zorgen dat na een incident, als gevolg van een tot uiting gekomen bedreiging, acties tot uitvoering worden gebracht om de geautomatiseerde informatievoorziening zo min mogelijk te doen remmen, bijvoorbeeld een account of netwerkadres wordt tijdelijk geblokkeerd op het moment dat er teveel foutieve login-pogingen zijn gedaan;
* *Reactieve maatregelen:* maatregelen nadat een bedreiging tot uiting is gekomen, bijvoorbeeld uitwijkvoorzieningen die pas na een incident worden gebruikt. Deze maatregelen zijn een reactie op de repressieve maatregelen.

De bovenstaande maatregelen zijn achtereenvolgens weer te splitsen in (Fijneman, 2006; Romney, 2012)):

* *General IT controls:* beheersingsmaatregelen die zorg moeten dragen voor de betrouwbaarheid van de geautomatiseerde informatievoorziening, bijvoorbeeld logische toegangsbeveiliging;
* *Application IT controls:* beheersingsmaatregelen in de programmatuur, bijvoorbeeld invoercontroles.

Doordat niet elke bedreiging een grote schade tot gevolg heeft, is het uit kostenoogpunt, verstandig om de geautomatiseerde informatievoorziening niet tegen elke bedreiging te beveiligen (Looijen, 2011). Daarnaast is de keuze van beveiliging mede afhankelijk van het belang dat aan de informatie wordt gehecht (Fijneman, 2006).

Op het moment dat vertrouwelijkheid als belangrijke aspect wordt genomen, zal voornamelijk de focus liggen op het treffen van preventieve maatregelen. Daarentegen zullen reactieve maatregelen zwaarder wegen op het moment dat integriteit belangrijk is. Repressieve maatregelen zijn belangrijker op het moment dat beschikbaarheid als belangrijkste aspect wordt genomen. De cultuur van een bedrijf is ook mede bepalend voor de keuze van maatregelen. Uiteindelijk draait alles om risico-acceptatie, oftewel de mate waarin je als bedrijf bereidt bent om risico te nemen.

Voordat er een IT-beleid, met maatregelen, kan worden ingevoerd, dient er een beveiligingsorganisatie te zijn (Fijneman, 2006). Dit is van belang om te voorkomen dat tijdens het traject van invoering onduidelijkheden ontstaan over de taken, verantwoordelijkheden en bevoegdheden. Beveiligingsfunctionarissen en participanten in een beveiligingsunit moeten, afhankelijk van de grootte en de aard van het bedrijf, benoemd zijn (Looijen, 2011).

# 7 Resultaten van het empirisch onderzoek

De bronnen voor IT-normen: ITIL, ISO 20.000 en COBIT, zijn reeds besproken. Deze zijn tevens onderling met elkaar vergeleken. Een aantal elementen uit deze bronnen voor IT normen zullen worden gebruikt voor de realisatie van het uiteindelijk op te leveren product, in dit geval een beheermethodiek met IT-beheersmaatregelen, die speciaal is gericht op MKB-bedrijven.

Eerst dienen echter wel de problemen, als het gaat om IT beheer, bij MKB-bedrijven, in kaart te worden gebracht, om passende IT-beheermaatregelen te kunnen treffen. Om dit onderzoek enigszins af te bakenen, zal de aandacht voornamelijk uitgaan naar problemen met betrekking tot informatiebeveiliging.

In dit hoofdstuk zullen allereerst de verzwakkingen alsmede de versterkingen van de interne controle met betrekking tot IT, die accountants veelal bij de controle van MKB-bedrijven tegenkomen, in kaart worden gebracht. Hiervoor zijn een tweetal registeraccountants geïnterviewd, die werkzaam zijn in de controlepraktijk bij MTH te Hoevelaken. Tevens zijn er een aantal controledossiers geraadpleegd, die geheel willekeurig zijn geselecteerd of door een registeraccountant zijn voorgesteld. Er is hierbij een checklist gebruikt, die is gekoppeld aan de theorie; in dit geval ISO 27.002: Code voor Informatiebeveiliging. Bovendien is er literatuuronderzoek gedaan. Tot slot zullen er, met betrekking tot de in kaart gebrachte IT-problemen, passende IT-beheersmaatregelen worden getroffen, die tevens in dit hoofdstuk zullen worden besproken.

## 7.1 IT versterkt de kwaliteit van de AO/IC bij MKB-bedrijven

Uit dit onderzoek, blijkt dat IT de kwaliteit van de AO/IC bij MKB-bedrijven versterkt. Bij AO/IC gaat het om zaken als: vastleggingen van taken, verantwoordelijkheden en bevoegdheden, procesbeschrijvingen, risicobeheersing, kwaliteitsbeheersing en managementrapportages. Uit dit onderzoek, blijkt dat accountants bij de controle van MKB-bedrijven veelal het volgende aantreffen, wat de kwaliteit van de AO/IC versterkt:

1. Perioderapportages die standaard ingeregeld zijn;
2. Standaard doorlopende nummering van in- en verkooporders, waarbij orders niet verwijderd kunnen worden;
3. Standaard interfaces tussen de verschillende IT systemen;
4. Inrichting van controletechnische functiescheiding in de IT systemen;
5. Inrichting van betaalbevoegdheden in het bankpakket.

## 7.2 IT verzwakt de kwaliteit van de AO/IC bij MKB-bedrijven

IT leidt dus tot versterking van de kwaliteit van de AO/IC, maar echter ook tot verzwakking van de kwaliteit van de AO/IC. Uit dit onderzoek, blijkt dat accountants bij de controle van MKB-bedrijven veelal de volgende problemen aantreffen, die de kwaliteit van de AO/IC verzwakken:

1. Ontbreken van een formeel opgesteld IT beleid: binnen het MKB wordt IT te vaak als bijzaak gezien en de normen en inrichting worden vaak bepaald op basis van gebruikersgemak;
2. Softwarematige fouten in de IT-infrastructuur;
3. Beperkt gebruik van proces- en/of systeemdocumentatie bij de invoering van nieuwe systemen/pakketten: binnen het MKB gebeurt het regelmatig dat wijzigingen in systemen/pakketten ongecontroleerd tot stand komen, met verwarring bij gebruikers en IT medewerkers als gevolg;
4. Onvoldoende periodieke monitoring van de kwaliteit van systemen;
5. Onvoldoende back-uppen van gegevensdragers met behulp van een data back-up systeem;
6. Niet goed ingeregelde competenties (autorisatie): gebruikers/medewerkers hebben vaak te veel bevoegdheden, doordat veel MKB-bedrijven ‘’gebruikersgemak’’ als uitgangspunt hanteren bij het bepalen van de normen en inrichting met betrekking tot IT. IT systemen moeten immers een inrichting hebben die praktisch is;
7. Tekortkomingen in de authenticatie: regelmatig komt het bij MKB-bedrijven voor dat er gebreken zijn in het versleutelen/coderen tegen bedreigingen, waarbij het regelmatig voorkomt dat meerdere gebruikers/medewerkers hetzelfde wachtwoord gebruiken, met ongeautoriseerde toegang tot informatiesystemen of bepaalde vertrouwelijke informatie als gevolg;
8. Beperkt gebruik van proces- en/of systeemdocumentatie met betrekking tot informatiebeveiliging: binnen het MKB gebeurt het regelmatig dat gebruikers/medewerkers niet weten welke acties zij moeten verrichten, op het moment dat er zich ernstige incidenten of storingen voordoen met betrekking tot de IT systemen;
9. Gebreken in de inrichting van de logische toegangsbeveiliging;
10. Gebreken in de inrichting van de fysieke beveiliging en beveiliging van de omgeving: het gebeurt regelmatig dat er onverwachte/illegale componenten op een netwerk zijn aangesloten. Tevens komt het regelmatig voor dat een server in de bezemkast onvoldoende wordt gekoeld, met brandgevaar of elektriciteitsonderbreking als gevolg.

Uit de in kaart gebrachte problemen, met betrekking tot IT, bij MKB-bedrijven, valt op dat de meeste problemen enorm vanzelfsprekend zijn. Toch blijkt dit bij veel MKB-bedrijven nog niet op orde te zijn. MKB-bedrijven ondervinden veelal problemen in de ‘’application IT controls’’, die het primaire kwaliteitsaspect ‘’vertrouwelijkheid’’ (‘’confidentiality’’) moet ondersteunen (Romney, 2012). Bij veel MKB-bedrijven ontbreekt een controletechnische functiescheiding, die is ingeregeld in de competenties (‘’application IT controls’’). De ’’general IT controls’’ zijn hierbij van ondergeschikt belang.

## 7.3 Betere IT-control bij MKB-bedrijven realiseren

### 7.3.1 Aanknopingspunten van beheermethodieken en kwaliteitsnormen voor betere IT-control bij MKB-bedrijven

De reeds besproken bronnen voor IT-normen: ITIL, ISO 20.000 en COBIT, kunnen worden gebruikt om te komen tot passende IT-beheermaatregelen. De processen uit deze bronnen voor IT normen zijn zeker van toegevoegde waarde voor MKB-bedrijven. Deze dienen echter niet allemaal integraal te worden overgenomen, maar selectief te worden gebruikt. De te gebruiken processen moeten immers wel voor het bedrijf van belang zijn. Uiteindelijk gaat het erom dat MKB-bedrijven bezig zijn met ‘’IT Governance’’ en hier dus voldoende aandacht aan schenken.

**ITIL**

ITIL geeft in het proces ‘’Information Security Management’’, invulling aan informatiebeveiliging (Noë, 2006; Fijneman, 2009). Met behulp van dit proces kunnen antwoorden worden verkregen op vragen als: waar moet de security officer worden gepositioneerd en waar moeten andere governance-aspecten van beveiliging worden behandeld? Het proces ‘’Information Security Management’’, dat onderdeel uitmaakt van de ontwerpfase ‘’Service Design’’, heeft als doel om beveiligingseisen te realiseren in de verschillende ‘’Service Level Agreements’’ (SLA’s) (Looijen, 2011; Zijlstra, 2002). In de ‘’Service Level Agreements’’ (SLA’s) worden de afspraken vastgelegd, die met de klant zijn overeengekomen. Bovendien heeft dit ITIL-proces als doel om andere externe vereisten te realiseren in andere contracten, wetgeving en eventueel intern of extern opgelegd beleid. Ten slotte heeft dit proces als doel om een basisniveau aan beveiliging te realiseren. Dit is van belang om de eigen continuïteit van de beheerorganisatie te waarborgen. Tevens is dit nodig om vereenvoudiging van het ‘’Service Level Management’’ voor informatiebeveiliging te bewerkstelligen. Immers, hoe meer verschillende ‘’Service Level Agreements’’ (SLA’s) er beheert worden, hoe complexer het is.

Het ITIL-proces ‘’Information Security Management’’ is mede gebaseerd op ISO 27.002: Code voor Informatiebeveiliging en heeft binnen ITIL de meeste onderlinge relaties met de andere ITIL-processen.

Binnen ITIL zijn eigenlijk drie verschillende besturingslagen te onderscheiden (Zijlstra, 2002). In de bovenste laag: strategie, wordt de strategie voor het IT-beheer geformuleerd. Daarentegen bevinden zich in de middelste laag: tactiek, de processen ten behoeve van het opstellen van ‘’Service Level Agreements’’ (SLA’s) en die de services verzorgen, volgens de afspraken in deze ‘’Service Level Agreements’’ (SLA’s). De beveiligingsafspraken worden tevens vastgelegd in de ‘’Service Level Agreements’’ (SLA’s). Het proces ‘’Information Security Management’’ bevindt zich grotendeels in deze besturingslaag. Ten slotte bevinden zich in de onderste laag: operationeel, de processen die het daadwerkelijk operationeel beheer van de IT-middelen moeten verzorgen.

Zoals al eerder in dit rapport is aangegeven, heeft het proces ‘’Information Security Management’’ veel onderlinge relaties met de andere ITIL-processen. Zo dienen bijvoorbeeld, beveiligingsincidenten te worden herkend door het proces ‘’Incident Management’’. Het proces ‘’Problem Management’’ analyseert vervolgens de oorzaken van deze beveiligingsincidenten en doet voorstellen om deze incidenten in de toekomst te kunnen voorkomen. Ten slotte voert het proces ‘’Change Management’’ de wijzigingsvoorstellen daadwerkelijk door.

Er kan dus geconcludeerd worden, dat in de andere processen activiteiten moeten plaatsvinden om een adequate informatiebeveiliging te kunnen realiseren. Vanuit het proces ‘’Information Security Management’’ worden alleen aanwijzingen gegeven aan deze processen, voor de inrichting van de activiteiten. De verantwoordelijke manager voor het proces ‘’Information Security Management’’, is de ‘’Security Manager’’, waar de andere procesmanagers in de praktijk veel overleg mee voeren.

Het proces ‘’Information Security Management’’ verzorgt dus de aansturing voor de implementatie binnen een ander ITIL-proces en kan onderverdeelt worden in een drietal sub-processen. Deze zijn (Zijlstra, 2002):

* + *Sturing:* dit sub-proces bestaat uit het beleid en de organisatie van het beheerraamwerk voor informatiebeveiliging. De maatregelen uit de ‘’Code voor Informatiebeveiliging’’, op het gebied van beleid en organisatie voor de informatiebeveiliging, worden hierbij geïmplementeerd. Sturing beschrijft sub-processen, als: op welke manier de beveiligingsplannen tot stand komen, hoe deze worden geïmplementeerd, hoe de evaluatie van de implementatie wordt verricht en hoe de resultaten van deze evaluaties vervolgens weer worden omgezet in actieplannen. Tevens beschrijft het sub-proces ‘’sturing’’ de beveiligingsfuncties, de rollen en de verantwoordelijkheden, de organisatiestructuur, alsmede de rapportagelijnen en ‘’bevels’’-lijnen (wie geeft opdrachten aan wie? wie voert de opdrachten uit? hoe wordt er gerapporteerd over de uitvoering?);
  + *Plan:* dit sub-proces bestaat uit de activiteiten die resulteren in de beveiligingsparagraaf in een ‘’Service Level Agreement’’ (SLA). Tevens bestaat dit proces uit de activiteiten in relatie tot de ’’Underpinning Contracts’’ (UC’s), waarbij het onderwerp beveiliging centraal staat. Binnen de ‘’Operational Level Agreements’’ (OLA’s), worden de geformuleerde doelstellingen in de ‘’Service Level Agreements’’ (SLA’s) nader beschreven. Daarmee zijn de ‘’Operational Level Agreements’’ (OLA’s) de basis voor de beveiligingsplannen per organisatie-eenheid binnen de organisatie van de service provider en voor specifieke beveiligingsplannen, bijvoorbeeld voor specifieke applicaties of IT-platforms. Tevens werkt het sub-proces ‘’plan’’, naast de input van een ‘’Service Level Agreement’’ (SLA), ook met de door de service provider zelf ontwikkelde beleidsuitgangspunten, die voortkomen uit het proces ‘’sturing’’. Een voorbeeld van een beleidsuitgangspunt is: iedere gebruiker dient uniek identificeerbaar te zijn;
  + *Implementaties:* dit sub-proces zorgt ervoor dat alle maatregelen, die in de plannen staan beschreven, worden geïmplementeerd. Binnen dit proces worden echter geen maatregelen beschreven of gewijzigd. Dat vindt alleen plaats via het proces ‘’Change Management’’, waarbij tevens afstemming met het sub-proces ‘’Plan’’ gerealiseerd moet worden. Voorbeelden van maatregelen kunnen te maken hebben met: personele beveiliging, veilig beheer, toegangsbeveiliging of rangschikking en beheersing van IT-hulpmiddelen;
  + *Audit en evaluatie:* binnen dit sub-proces worden de geplande maatregelen onafhankelijk geëvalueerd, om het eigen functioneren te bewaken. Daarnaast is de evaluatie ook van belang voor de klanten en eventuele derde-partijen. Bij het verrichten van evaluaties worden activiteiten verricht als, het controleren van de beveiliging op IT systemen of het uitvoeren van EDP-audits voor het onderdeel informatiebeveiliging. De uit dit sub-proces verkregen resultaten, worden gebruikt om de afgesproken maatregelen, in afstemming met de klant, te onderhouden en te implementeren.

Voorbeelden van evaluaties zijn: self assessments (door de lijnorganisatie van de processen uitgevoerd), interne audits (door interne EDP-auditors uitgevoerd), en externe audits (door externe EDP-auditors uitgevoerd);

* + *Onderhoud:* dit sub-proces bestaat zowel uit het onderhoud aan de beveiligingsparagraaf van een ‘’Service Level Agreement’’ (SLA), als het onderhoud aan de beschreven beveiligingsplannen binnen de ‘’Operational Level Agreements’’ (OLA’s). Dit sub-proces is onmisbaar, omdat de risico’s constant veranderen op het moment dat er veranderingen optreden in de IT-infrastructuur, de organisatie en de bedrijfsprocessen;
  + *Rapportage:* dit sub-proces is het resultaat van de andere sub-processen, waarbij verantwoording wordt afgelegd over de geleverde beveiligingsdiensten en om aan klanten relevante informatie te verstrekken voor wat betreft de informatiebeveiliging. Vaak wordt over de rapportage duidelijke afspraken gemaakt met de klant. Een voorbeeld van een onderwerp die in een rapportage aan bod kan komen is: de opgetreden beveiligingsincidenten en de manier van afhandelen daarvan.

Hierbij moet opgemerkt worden, dat ITIL over het algemeen mager ingaat op alle aspecten met betrekking tot informatiebeveiliging (Elsinga, 2014). Het ITIL-proces ‘’Information Security Management’’ hangt voornamelijk aan de kwaliteitsnorm: ISO 20.000 (‘’Service Management’’), waarbij de afhankelijkheid het grootst is van de processen ‘’Incident Management’’, ‘’Problem Management’’, ‘’Change Management’’ en ‘’Configuration Management’’. ITIL is een methodiek die voor een groot deel is gericht op IT beheer. Informatiebeveiliging gaat echter veel verder dan alleen IT beheer.

**ISO 20.000**

De kwaliteitsnorm: ISO 20.000, geeft in het sub-proces ‘’Information Security Management’’, dat onderdeel uitmaakt van de ‘’Service Delivery Processes’’, invulling aan informatiebeveiliging (Looijen, 2011).

Zoals al eerder in dit rapport is gemeld, is de kwaliteitsnorm: ISO 20.000, eigenlijk niets anders dan een geformaliseerde versie van ITIL, met als uitgangspunt de processen die in ITIL worden onderscheden en aanvullingen op het gebied van servicerapportage en relatiebeheer (Noë, 2006).

Hierdoor is de kwaliteitsnorm: ISO 20.000, bijna gelijk aan ITIL, op het moment dat de verschillende processen in overweging worden genomen. Daarom zal hier niet gedetailleerd worden ingegaan op het sub-proces ‘’Information Security Management’’, dat binnen ISO 20.000 invulling geeft aan informatiebeveiliging.

**COBIT**

Uit de gehouden interviews, komt het beeld naar voren dat COBIT in het proces ‘’Manage Security’’, te vinden in het voorvlak van de COBIT-kubus onder het domein ‘’plannen en organiseren’’ (‘’planning and organization’’), invulling geeft aan informatiebeveiliging (Bouker, n.d.; ISACA, 2012; Looijen, 2011). Bovendien wordt in de processen ‘’Manage Continuity’’ en ‘’Manage Security Services’’, te vinden in het voorvlak van de COBIT-kubus onder het domein ‘’diensten verlenen en ondersteunen’’ (‘’delivery and support’’), invulling gegeven aan informatiebeveiliging. Echter, ook in de andere COBIT-processen komt informatiebeveiliging regelmatig aan bod.

De processen ‘’Manage Security’’, ‘’Manage Continuity’’ en ‘’Manage Security Services’’ vertegenwoordigen een aantal gestelde beheersingsdoelstellingen op procesniveau en worden in de vorm van activiteiten verder uitgewerkt in doelstellingen op het niveau van activiteiten (ISACA, 2012; Lindgreen, 2005). Uiteindelijk zorgt dit voor een opsomming van verschillende algemene IT-beheersmaatregelen op het gebied van informatiebeveiliging. De aspecten op het gebied van informatiebeveiliging zijn hierbij, net als in ITIL en ISO 20.000, gebaseerd op ISO 27.002: Code voor Informatiebeveiliging (Bouker, n.d.; Looijen, 2011).

Bedrijven kunnen aan de hand van deze COBIT-processen, de volgende voordelen bewerkstelligen (ISACA, 2012):

* + Informatiebeveiliging, normen, best practices en eventuele sectorspecifieke richtlijnen, kan/kunnen beter en gemakkelijk worden ingericht. Dit heeft mindere complexiteit en hogere kosteneffectiviteit als gevolg;
  + Een grotere tevredenheid bij de gebruiker met betrekking tot informatiebeveiligingsafspraken en resultaten;
  + Een groter risicobewustzijn en snellere besluitvorming met betrekking tot het reduceren van informatiebeveiligingsrisico’s;
  + Verbeterde preventie, opsporing en herstel van informatiebeveiligingsrisico’s;
  + Minder (gevolgen van) informatiebeveiligingsincidenten;
  + Verbeterde ondersteuning voor innovatie en concurrentievermogen;
  + Een beter beheer van de kosten die betrekking hebben op informatiebeveiliging;
  + Informatiebeveiliging beter kunnen begrijpen.

Toch moet hierbij opgemerkt worden, dat COBIT niet gedetailleerd ingaat op alle aspecten met betrekking tot informatiebeveiliging (Elsinga, 2014). COBIT is immers een methodiek, die processen beschrijft op het gebied van IT beheer en zich bezighoudt met ‘’IT Governance’’. Alle controls worden binnen het COBIT raamwerk overgeslagen. Informatiebeveiliging gaat echter veel verder dan alleen IT beheer, wat al eerder in dit rapport is aangegeven.

### 7.3.2 IT-beheersmaatregelen bij MKB-bedrijven

Voor de meest voorkomende problemen, met betrekking tot IT, bij MKB-bedrijven, die hiervoor reeds zijn besproken, kunnen een aantal IT-beheersmaatregelen worden getroffen. De te treffen IT-beheersmaatregelen zullen hieronder nader worden besproken en zijn mede tot stand gekomen aan de hand van de in dit rapport besproken beheermethodieken en kwaliteitsnormen: ITIL, ISO 20.000 en COBIT, alsmede ISO 27.002: Code voor informatiebeveiliging. Zowel ITIL, als ISO 20.000 en COBIT, zijn immers mede gebaseerd op ISO 27.002: Code voor informatiebeveiliging.

1. **Probleem:** Ontbreken van een formeel opgesteld IT beleid

**IT-beheersmaatregel:** Opstellen van een lange termijn IT beleid

Slechts weinig MKB-bedrijven hebben een formeel IT beleid opgesteld. Zo is informatiebeveiliging meestal beperkt tot de standaard zaken als firewalls, afgeschermde servers etc. Binnen het MKB, wordt IT dus te vaak als bijzaak gezien en de normen en inrichting worden vaak bepaald op basis van gebruikersgemak.

Om dit veel voorkomende probleem op te lossen is het van belang dat MKB-bedrijven een formeel IT beleid hebben en dus meer aandacht schenken aan IT. Om een formeel IT beleid op te stellen, kan gebruik worden gemaakt van de beheermethodieken en kwaliteitsnorm: ITIL, ISO 20.000 en COBIT. Zowel ITIL, als ISO 20.000 en COBIT, leggen de nadruk op lange termijn beleid, waarbij de lange termijn plannen worden gemaakt met betrekking tot IT. Met behulp van een lange termijn IT beleid, kan IT worden afgestemd met de businessbehoeften (Noë, 2006). Een lange termijn IT beleid zorgt er dus voor dat de manier waarop IT wordt ingezet, aansluit met de bedrijfsvoering, om uiteindelijk de strategie en de bedrijfsdoelstellingen te kunnen realiseren (Looijen, 2011).

Binnen ITIL kunnen de verschillende processen, die onderdeel uitmaken van de fase ‘’Service Strategy’’ van de ‘’Service Lifecycle’’, worden gebruikt voor het ontwerpen, het ontwikkelen en het implementeren van servicemanagement als een strategisch middel (Looijen, 2011). ISO 20.000 besteedt aandacht aan het opstellen van een strategisch IT beleid, in het eerste deel van deze ISO-norm, waar de eisen worden uiteengezet, om als bedrijf, het certificaat te verkrijgen. Ten slotte besteedt ook COBIT aandacht aan het opstellen van een strategisch IT beleid. COBIT doet dat voornamelijk in het voorvlak van de COBIT-kubus onder het domein ‘’plannen en organiseren’’ (‘’planning and organization’’) en het daar bijbehorende proces ‘’PO1. Definieer een strategisch IT-plan’’. Zoals al eerder in dit rapport is aangegeven, werken de ITIL-processen het domein ‘’plannen en organiseren’’ (‘’planning and organization’’), met de bijbehorende vijf processen, verder uit. Wat tevens al eerder in dit rapport is aangegeven, is het feit dat ITIL en ISO 20.000, bij het opstellen van een strategisch IT beleid, geen rekening houden met relevante wet- en regelgeving en contractuele afspraken, waar de bedrijfsprocessen aan moeten voldoen (Croon, 2008). COBIT doet dat daarentegen wel.

1. **Probleem:** Softwarematige fouten in de IT-infrastructuur

**IT-beheersmaatregel:** Toepassing van de ITIL-processen ‘’Request Management’’ en ‘’Problem Management’’

Veel MKB-bedrijven ondervinden problemen in de IT-infrastructuur (Bolland, 2011). Zo komt het bijvoorbeeld vaak voor dat er in software fouten zitten, met alle gevolgen van dien. Het is hierbij van belang dat er direct actie wordt ondernomen en dat er bijvoorbeeld met betrekking softwarefouten, hogere versies worden geïnstalleerd.

ITIL kan hierbij, voor MKB-bedrijven, hulp bieden met de processen ‘’Request Management’’ en ‘’Problem Management’’, die onderdeel uitmaken van de fase ‘’Service Operation’’ van de ‘’Service Lifecycle’’. Problemen die dusdanig van aard zijn, zoals softwarefouten, kunnen niet opgelost worden in het proces ‘’Incident Management’’ of komen voort uit het proces ‘’Incident Management’’. Deze problemen worden in het proces ‘’Problem Management’’ onderkent, waarna er een wijzigingsverzoek wordt ingediend via het proces ‘’Change Management’’. Problemen en wijzigingen dienen te worden gemeld aan een service desk via het proces ‘’Request Management’’. Via het proces ‘’Request Management’’ kunnen gebruikers informatie, advies, een standaard change of toegang tot een service, verkrijgen. De service desk is eigenlijk niets anders dan een centraal aanspreekpunt voor de IT-gebruikers en staat dus op operationeel niveau in contact met de IT-gebruikers. Een service desk zal over het algemeen beter gaan functioneren op het moment dat er vastgelegde procedures en werkinstructies aanwezig zijn.

Binnen het MKB is de service desk vaak ondergebracht bij de financiële afdeling (hoofd administrateur of controller) of bij een IT-er zonder echte opleiding, maar die “wel handig is met computers”. Een MKB-bedrijf heeft immers vaak te maken met een schaarste aan uren en legt voornamelijk de focus op de core business.

1. **Probleem:** Beperkt gebruik van proces- en/of systeemdocumentatie bij de invoering van

nieuwe systemen/pakketten

**IT-beheersmaatregel:** Gebruik van proces- en/of systeemdocumentatie bij de invoering van nieuwe systemen/pakketten

Veel MKB-bedrijven hebben over het algemeen moeite met het implementeren van nieuwe systemen/pakketten. Zo zijn er bijvoorbeeld veel bedrijven, die een aantal jaren geleden zijn begonnen met het implementeren van het ERP-pakket SAP, en dit nog steeds niet hebben afgerond. Ook zijn er veel bedrijven die al meerdere SAP-implementaties achter de rug hebben. Bij de implementatie van nieuwe systemen/pakketten is het van belang dat er duidelijke proces- en/of systeemdocumentatie beschikbaar is om wijzigingen gecontroleerd tot stand te brengen (Bolland, 2011). Op het moment dat dit ontbreekt, leidt dit tot verwarring bij gebruikers en IT medewerkers, en dus tot verstoringen.

Zowel ITIL, als ISO 20.000 en COBIT, kunnen helpen bij het implementeren van nieuwe systemen/pakketten. Hierbij wordt, zowel door ITIL, als door ISO 20.000 en COBIT, nadrukkelijk ingegaan op zaken als: de voorbereiding bij de implementatie van nieuwe systemen/pakketten, alsmede het testen ervan. ITIL en ISO 20.000 beschrijven de processen die nodig zijn bij de invoering van nieuwe systemen/pakketten tot in detail. ITIL doet dat voornamelijk in de processen ‘’Change Management’’ en ‘’Release & Deployment Management’’, die onderdeel uitmaken van de fase ‘’Service Transition’’ van de ‘’Service Lifecycle’’. De processen ‘’Incident Management’’ en ‘’Problem Management’’ , die onderdeel uitmaken van de fase ‘’Service Operation’’ van de ‘’Service Lifecycle’’, kunnen hierbij ten grondslag liggen aan de invoering van nieuwe systemen/pakketten.

Bovendien biedt het eerste deel van ISO 20.000 (‘’Planning and Implementation New or Changed Services’’), waar de eisen worden uiteengezet, om als bedrijf, het certificaat te verkrijgen, alsmede de processen ‘’Release Process’’ en ‘’Control Process’’ , in het tweede deel van ISO 20.000, ook hulp bij de invoering van nieuwe systemen/pakketten.

Ten slotte wordt ook in COBIT aandacht besteedt aan de invoering van nieuwe systemen/pakketten. COBIT doet dat voornamelijk in het voorvlak van de COBIT-kubus onder het domein ‘’verwerken en implementeren’’ (‘’acquisition and implementation’’) en het daar bijbehorende proces ‘’A15. Installeer en accrediteer systemen’’. COBIT stelt hierbij voornamelijk eisen aan de processen die nodig zijn bij de invoering van nieuwe systemen/pakketten. COBIT geeft in dit geval dus meer antwoord op de wat-vraag, waar ITIL en ISO 20.000 juist meer antwoord geven op de hoe-vraag. Zoals al eerder in dit rapport is aangegeven, werken de ITIL-processen het domein ‘’verwerken en implementeren’’ (‘’acquisition and implementation’’), met de bijbehorende processen, verder uit.

1. **Probleem:** Onvoldoende periodieke monitoring van de kwaliteit van systemen

**IT-beheersmaatregel:** Periodieke monitoring van de kwaliteit van systemen

Voor MKB-bedrijven is het van belang dat de kwaliteit van de systemen periodiek wordt gemonitord. Op deze manier kunnen incidenten tijdig worden herstelt en problemen in de toekomst worden voorkomen. Het is hierbij van belang dat MKB-bedrijven logboeken bijhouden van systeemfouten, inbraken in systemen monitoren, beschikbaarheid van systemen bewaken en de leiding van de huishouding erover informeren. Zowel ITIL, als ISO 20.000, besteden in de processen aandacht aan het monitoren van de kwaliteit van de systemen en beschrijven dit tot in detail.

ITIL doet dat voornamelijk in de processen, die onderdeel uitmaken van de fase ‘’Service Operation’’ van de ‘’Service Lifecycle’’ . Ook de processen ‘’Seven Step Improvement’’ en ‘’Service Reporting’’, die onderdeel uitmaken van de fase ‘’Continual Service Improvement’’ van de ‘’Service Lifecycle’’, en het proces ‘’Availability Management’’, dat onderdeel uitmaakt van de fase ‘’Service Design’’ van de ‘’Service Lifecycle’’, besteden aandacht aan periodieke monitoring van systemen.

ISO 20.000 besteedt voornamelijk aandacht aan periodieke monitoring van de kwaliteit van systemen, in de processen ‘’Resolution Process’’ en ‘’Service Delivery Process’’, die onderdeel uitmaken van het tweede deel van deze ISO-norm.

Ten slotte besteedt ook COBIT aandacht aan periodieke monitoring van de kwaliteit van systemen. COBIT doet dat voornamelijk in het voorvlak van de COBIT-kubus onder het domein ‘’monitoren en evalueren’’ (‘’monitoring’’) en de daar bijbehorende processen. Daarnaast besteedt COBIT ook aandacht aan monitoring in het domein ‘’diensten verlenen en ondersteunen’’ (‘’delivery and support’’) met het daar bijbehorende proces ‘’DS10. Beheers problemen en incidenten’’. Hierbij stelt COBIT voornamelijk eisen aan de processen die van belang zijn bij het monitoren van de kwaliteit van systemen. Zoals al eerder in dit rapport is aangegeven, werken de ITIL-processen het domein ‘’diensten verlenen en ondersteunen’’ (‘’delivery and support’’), met de bijbehorende processen, verder uit.

1. **Probleem:** Onvoldoende back-uppen van gegevensdragers met behulp van een data back-up

systeem

**IT-beheersmaatregel:** Periodiek back-uppen van gegevensdragers met behulp van een data back-up systeem

Elk MKB-bedrijf dient te beschikken over opgestelde procedures met betrekking tot het maken van back-ups en bewaring van gegevensdragers (Fijneman, 2006). Een eenvoudig en adequaat data back-up systeem, dat zorg draagt voor het maken van recente back-ups, wordt vaak onderschat en is voor elk MKB-bedrijf enorm van belang. Het is aan te bevelen om, als MKB-bedrijf, (nieuwe) informatie op meerdere plaatsen, dan alleen in het kantoorpand, te bewaren. Periodiek dient de directeur hierbij een recente back-up mee naar huis te nemen.

Zowel ITIL, als COBIT, besteden aandacht aan het periodiek maken van back-ups. ITIL doet dat voornamelijk in de processen, die onderdeel uitmaken van de fase ‘’Service Operation’’ van de ‘’Service Lifecycle’’. COBIT doet dat voornamelijk in het voorvlak van de COBIT-kubus onder het domein ‘’diensten verlenen en ondersteunen’’ (‘’delivery and support’’) en het daar bijbehorende proces ‘’DS11. Beheers gegevens’’. Zoals al eerder in dit rapport is aangegeven, werken de ITIL-processen het domein ‘’diensten verlenen en ondersteunen’’ (‘’delivery and support’’), met de bijbehorende processen, verder uit.

1. **Probleem:** Niet goed ingeregelde competenties (autorisatie)

**IT-beheersmaatregel:** Ingeregelde competenties (autorisatie)

Bij veel MKB-bedrijven vindt ongewenste vermenging van taken en bevoegdheden bij één en dezelfde persoon plaats. De normen en inrichting van IT systemen, worden vaak bepaald op basis van gebruikersgemak. De inrichting van IT systemen moet immers praktisch zijn, waardoor gebruikers/medewerkers vaak te veel kunnen/mogen. Het ontbreken van controletechnische functiescheiding in de competenties (‘’application IT controls’’), heeft echter als gevolg dat de organisatie hierdoor kwetsbaarder wordt. Daarnaast is kans op het voordoen van fraude, hierdoor een stuk groter.

Op basis van competentietabellen, dient er waar mogelijk, controletechnische functiescheiding ingeregeld te worden in de competenties (‘’application IT controls’’). In een competentietabel staan de toegangsrechten per gebruiker/medewerker beschreven. Functies dienen zo ingericht te worden dat degene die de taken uitvoert, niet dezelfde is als degene die controle uitoefent op de uitvoering (Fijneman, 2006). Het is mogelijk om via proces-ketens, scheiding te realiseren tussen de uitvoering en controle. De proces-ketens dienen zo ingericht te zijn, dat de volgende schakel in het proces er belang bij heeft om het werk wat verricht is in de voorgaande schakel, te controleren. Eventueel is het ook mogelijk de controle uit te laten voeren door de superieur van de ondergeschikte of door een afdeling ‘’interne controle’’.

Binnen IT systemen worden gebruikers/medewerkers gezien als gebruikersaccounts in besturingssystemen en databases, waarbij verschillende autorisaties dienen plaats te vinden.

Zo dienen er autorisaties plaats te vinden voor het opstarten van programma’s, het gebruik van functies binnen programma’s, het raadplegen, wijzigen alsmede het verwijderen van bestanden of gegevens in databases en het gebruik van storedprocedures binnen databases.

Zowel ITIL, als COBIT, gaan nadrukkelijk in op het autoriseren van gebruikers. ITIL doet dat voornamelijk in het proces ‘’Access Management’’, dat onderdeel uitmaakt van de fase ‘’Service Operation’’ van de ‘’Service Lifecycle’’. COBIT besteedt aandacht aan het autoriseren van gebruikers in het domein ‘’diensten verlenen en ondersteunen’’ (‘’delivery and support’’) met het daar bijbehorende proces ‘’DS5. Waarborg de systeemveiligheid’’. Zoals al eerder in dit rapport is aangegeven, werken de ITIL-processen het domein ‘’diensten verlenen en ondersteunen’’ (‘’delivery and support’’), met de bijbehorende processen, verder uit.

1. **Probleem:** Tekortkomingen in de authenticatie

**IT-beheersmaatregel:** Ingeregelde authenticatie

Doordat het informatieaanbod tegenwoordig enorm omvangrijk is, komt het regelmatig bij MKB-bedrijven voor, dat meerdere gebruikers/medewerkers hetzelfde wachtwoord gebruiken, met ongeautoriseerde toegang tot informatiesystemen of bepaalde vertrouwelijke informatie als gevolg.

Het versleutelen/coderen tegen bedreigingen is dus van belang om ervoor te zorgen dat niet iedereen, maar enkelen, bepaalde gegevens kunnen lezen (Looijen, 2011). Coderingen zijn eigenlijk niets anders dan maatregelen om bedreigingen, die kunnen optreden bij het lezen en interpreteren van gegevens, zo veel mogelijk te beperken. Coderingen zijn dus ook van belang om ervoor te zorgen dat niet elke gebruiker/medewerker zomaar toegang heeft tot het informatiesysteem.

MKB-bedrijven dienen gebruik te maken van verschillende coderingen. Zeker door het feit dat het informatieaanbod tegenwoordig enorm omvangrijk is. Voorbeelden van coderingen zijn: wachtwoorden, pincodes, smartcards, pasjes of sleutelhangers (Radio Frequency Identification: RFID), biometrie (irisscan, gezichtskenmerken of een vingerafdruk), hardwaretokens en digitale handtekeningen (Fijneman, 2006; Looijen, 2011; Romney, 2012).

Zowel ITIL, als COBIT, besteden aandacht aan authenticatie van gebruikers. ITIL doet dat voornamelijk in het proces ‘’Access Management’’, dat onderdeel uitmaakt van de fase ‘’Service Operation’’ van de ‘’Service Lifecycle’’. COBIT besteedt aandacht aan authenticatie van gebruikers in het domein ‘’diensten verlenen en ondersteunen’’ (‘’delivery and support’’) met het daar bijbehorende proces ‘’DS5. Waarborg de systeemveiligheid’’. Zoals al eerder in dit rapport is aangegeven, werken de ITIL-processen het domein ‘’diensten verlenen en ondersteunen’’ (‘’delivery and support’’), met de bijbehorende processen, verder uit.

1. **Probleem:** Beperkt gebruik van proces- en/of systeemdocumentatie met betrekking tot

informatiebeveiliging

**IT-beheersmaatregel:** Gebruik van proces- en/of systeemdocumentatie met betrekking tot informatiebeveiliging

Elk MKB-bedrijf dient een duidelijk beveiligingsbeleid op te stellen, te onderhouden en uit te dragen (Looijen, 2011).Het beveiligingsbeleid is niets anders dan een beleidsdocument, waarin de doelstellingen voor beveiliging staan beschreven (Fijneman, 2006). Het management van de organisatie is verantwoordelijk voor dit beleidsdocument en dient actief bezig te zijn met de controle, de naleving en het onderhoud van het beveiligingsbeleid (Looijen, 2011). Er dienen periodiek evaluaties plaats te vinden en er moeten regelmatig rapportages beschikbaar komen, waarin alle relevante aspecten met betrekking tot informatiebeveiliging naar voren komen en waarin van belang zijnde suggesties en acties voor de komende periode zijn uitgewerkt.

Zowel ondersteunend personeel als gebruikers en beslisorganen, dienen te worden gewezen op de verantwoordelijkheid voor beveiliging , door middel van: het beschrijven van duidelijke functieomschrijvingen, het beschrijven van de belanghebbenden in het beslisorgaan, het beschrijven van de uitgangspunten om mee te werken, het beschrijven van de doelstellingen van het beslisorgaan, de screening van nieuwe medewerkers, het tekenen van verklaringen en training en rapportages met betrekking tot informatiebeveiliging. De inrichting van de organisatiestructuur speelt hierbij een hele belangrijke rol. De IT-beslissingen dienen door de juiste organen te worden genomen. Elk MKB-bedrijf moet aan de hand van een duidelijke organisatiestructuur van beslisorganen, personen verantwoordelijk kunnen stellen voor de doelstellingen. Ook moet een MKB-bedrijf de belanghebbenden, die een rol spelen bij de IT-beslissingen, in kaart kunnen brengen. Hiervoor dient een MKB-bedrijf een tabel te gebruiken, die beschrijft wie voor de IT-beslissingen verantwoordelijk is, wie verantwoording kan afleggen, en wie geadviseerd en geïnformeerd is. Zoals al eerder in dit rapport is aangegeven, besteden zowel ITIL, als ISO 20.000 en COBIT, aandacht aan organisatiestructuur in termen van rollen en verantwoordelijkheden (Bolland, 2011).

Bovendien dienen ook de verantwoordelijkheden en procedures voor het omgaan met apparatuur, te zijn vastgelegd en te worden nageleefd. Hier dient controle op te worden uitgeoefend, doordat fouten maken immers menselijk is. Het is van belang dat de planning en acceptatie van nieuwe apparaten en programmatuur volgens de vastgestelde procedures verlopen. Het komt hierbij vaak voor dat er een afweging van de risico’s plaatsvindt. Er dienen huisregels te worden opgesteld voor de verantwoordelijke personen voor het IT beheer. In deze huisregels staan de te verrichten acties beschreven, die bij bepaalde situaties verricht zouden moeten worden.

Zowel ITIL, als ISO 20.00 en COBIT, besteden aandacht aan proces- en/of systeemdocumentatie met betrekking tot informatiebeveiliging. ITIL doet dat voornamelijk in het proces ‘’Information Security Management’’, dat onderdeel uitmaakt van de fase ‘’Service Design’’ van de ‘’Service Lifecycle’’. ISO 20.000 besteedt aandacht aan proces- en/of systeemdocumentatie, met betrekking tot informatiebeveiliging, in het proces ‘’Service Delivery Process’’. Ten slotte besteedt ook COBIT aandacht aan proces- en/of systeemdocumentatie, met betrekking tot informatiebeveiliging, in het domein ‘’diensten verlenen en ondersteunen’’ (‘’delivery and support’’) met het daar bijbehorende proces ‘’DS5. Waarborg de systeemveiligheid’’. Zoals al eerder in dit rapport is aangegeven, werken de ITIL-processen het domein ‘’diensten verlenen en ondersteunen’’ (‘’delivery and support’’), met de bijbehorende processen, verder uit.

1. **Probleem:** Gebreken in de inrichting van de logische toegangsbeveiliging

**IT-beheersmaatregel:** Geregelde logische toegangsbeveiliging

Aan de hand van een autorisatieproces dient toegang te worden gegeven tot informatie en IT systemen (Fijneman, 2006). Elke medewerker/gebruiker dient hierbij in te loggen (‘’login’’) om toegang te krijgen. Er zal in dit geval een gebruikersnaam en wachtwoord ingevoerd moeten worden, om een functiescheiding voor gevoelige gegevensbewerkingen te realiseren. Het uiteindelijke doel van logische toegangsbeveiliging, is om ervoor te zorgen dat alleen personen voor het uitdragen van hun functie, de bevoegdheid hebben om gegevens in te zien, te wijzigen en/of te verwijderen. Bij logische toegangsbeveiliging draait het dus om de toekenning van toegangsrechten aan gebruikers/medewerkers.

Het is van belang dat alle afspraken en richtlijnen schriftelijk zijn vastgelegd en zijn overhandigd aan elke gebruiker/medewerker (Looijen, 2011). Het geniet de voorkeur om elke gebruiker/medewerker te laten tekenen voor acceptatie en naleving van de afspraken en richtlijnen, zodat elke gebruiker/medewerker bewust wordt gemaakt en eventueel achteraf kan worden aangesproken op het niet nakomen van bepaalde afspraken of richtlijnen en de mogelijke gevolgen. Bovendien geniet het de voorkeur om op verschillende niveaus toegangscontrole toe te passen, bijvoorbeeld bij het inloggen op een pc, het netwerk of toegang tot bepaalde gegevensverzamelingen. Het monitoren van de toegang en het gebruik van informatiesystemen kan ervoor zorgen dat ongeautoriseerde activiteiten kunnen worden ontdekt.

Zowel ITIL, als ISO 20.00 en COBIT, besteden aandacht aan logische toegangsbeveiliging. ITIL doet dat voornamelijk in het proces ‘’Information Security Management’’, dat onderdeel uitmaakt van de fase ‘’Service Design’’ van de ‘’Service Lifecycle’’. ISO 20.000 besteedt aandacht aan logische toegangsbeveiliging in het proces ‘’Service Delivery Process’’. Ten slotte besteedt ook COBIT aandacht aan logische toegangsbeveiliging in het domein ‘’diensten verlenen en ondersteunen’’ (‘’delivery and support’’) met het daar bijbehorende proces ‘’DS5. Waarborg de systeemveiligheid’’. Zoals al eerder in dit rapport is gemeld, werken de ITIL-processen het domein ‘’diensten verlenen en ondersteunen’’ (‘’delivery and support’’), met de bijbehorende processen, verder uit.

1. **Probleem:** Gebreken in de inrichting van de fysieke beveiliging en beveiliging van de

omgeving

**IT-beheersmaatregel:** Geregelde fysieke beveiliging en beveiliging van de omgeving

IT systemen en gegevens dienen te worden geplaatst in afgesloten ruimten, die niet voor iedereen toegankelijk zijn (Looijen, 2011). Het uiteindelijke doel hiervan is, om te voorkomen dat personen buiten de organisatie zich kunnen voordoen als interne medewerker (Fijneman, 2006). Ook is het van belang dat IT systemen en gegevens in ruimten worden geplaatst, waar de kans op het voordoen van incidenten die ervoor kunnen zorgen dat IT systemen niet meer kunnen functioneren en opgeslagen gegevens verloren kunnen gaan, zo klein mogelijk is (Looijen, 2011).

De fysieke toegangsbeveiliging, van zowel de computerruimten als de kantoorruimte, en de fysieke beveiliging van de omgeving dient hierbij op orde te zijn. De fysieke afscherming van bijvoorbeeld computerruimten, gebouwen en kamers, kan worden bewerkstelligd door het creëren van afgeschermde gebieden, die ook wel domeinen of compartimenten worden genoemd (Fijneman, 2006). Alleen personen die daar voor hun taak moeten zijn, hebben toegang tot deze afgeschermde gebieden. In de praktijk betekent dit het aanbrengen van een ringenstructuur, waarbij bijvoorbeeld een bedrijfsterrein is afgeschermd met een hek en een slagboom. Rond het bedrijfsterrein staan meerdere beveiligingscamera’s opgesteld. Een portier bewaakt de ingang van het gebouw en op het moment dat een persoon de computerruimte wenst te betreden, dient de desbetreffende persoon in het bezit te zijn van een pasje (badge). Deze pasjes (badges) bevatten een toegangsprofiel, waarbij aan de hand van het toegangsprofiel wordt bepaalde of de desbetreffende persoon toegang krijgt tot de computerruimte.

Bovendien dient de kritische apparatuur dusdanig beveiligt te zijn, waarbij het van belang is dat er voldoende aandacht wordt geschonken voor de plaats van de apparatuur, stroomvoorziening, beveiliging van kabels en voor de beveiliging van apparatuur buiten de centrale locaties (Looijen, 2011). Zo dienen bijvoorbeeld de IT systemen voldoende gekoeld te worden, om brandgevaar of elektriciteitsonderbreking te voorkomen. Ook de filters van de koelers dienen regelmatig schoon te worden gemaakt. Bovendien dienen er richtlijnen te zijn voor middelen als organizers, mobiele telefoons, diskettes, tapes en documentatie (Fijneman, 2006).

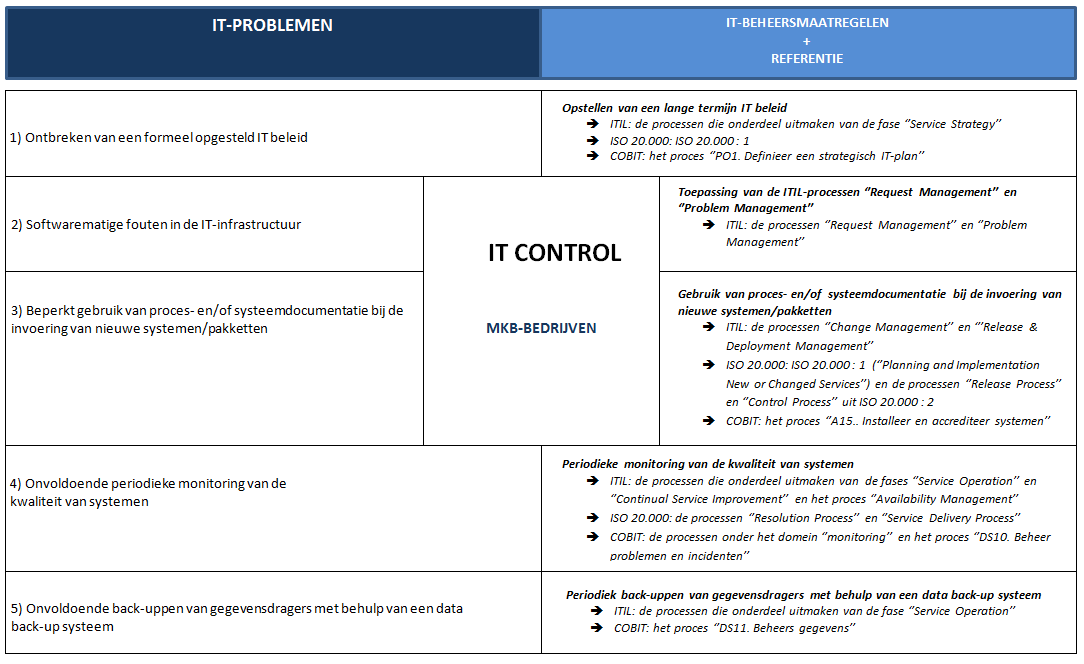
Ten slotte dient een zogenaamde ‘’clear-desk’’ en ‘’clear-screen’’ policy, onderdeel uit te maken van de richtlijnen voor iedere gebruiker/medewerker (Looijen, 2011). Alleen de hiertoe geautoriseerde personen hebben slechts toegang tot bepaalde gegevens, waarbij het dus van belang is dat er aan de beveiligingsvoorschriften wordt voldaan. Het verwijderen van apparatuur, programmatuur en gegevens dient met de nodige zorgvuldigheid bewerkstelligd te worden.

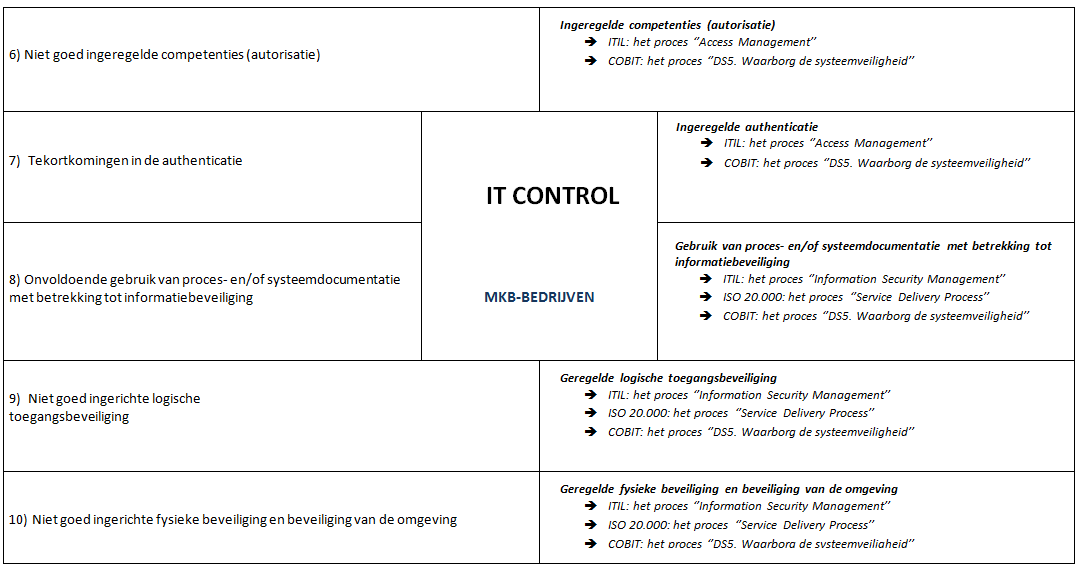
Zowel ITIL, als ISO 20.00 en COBIT, besteden aandacht aan fysieke toegangsbeveiliging. ITIL doet dat voornamelijk in het proces ‘’Information Security Management’’, dat onderdeel uitmaakt van de fase ‘’Service Design’’ van de ‘’Service Lifecycle’’. ISO 20.000 besteedt aandacht aan fysieke toegangsbeveiliging in het proces ‘’Service Delivery Process’’. Ten slotte besteedt ook COBIT aandacht aan fysieke toegangsbeveiliging in het domein ‘’diensten verlenen en ondersteunen’’ (‘’delivery and support’’) met het daar bijbehorende proces ‘’DS5. Waarborg de systeemveiligheid’’. Zoals al eerder in dit rapport is aangegeven, werken de ITIL-processen het domein ‘’diensten verlenen en ondersteunen’’ (‘’delivery and support’’), met de bijbehorende processen, verder uit.

### 7.3.3 Toepasbaarheid van de beheermethodieken en kwaliteitsnormen in het MKB

In de voorgaande paragrafen, zijn de 10 belangrijkste problemen, met betrekking tot IT control in het MKB, geïnventariseerd. Hierbij is een relatie gelegd tussen deze problemen en de verschillende processen/elementen van de beheermethodieken en kwaliteitsnormen: ITIL, ISO 20.000 en COBIT, waarin deze worden behandeld.

Voor een gemiddelde MKB-organisatie zijn deze beheermethodieken en kwaliteitsnormen echter te uitgebreid, te gedetailleerd en te specialistisch om daadwerkelijk in zijn geheel in een MKB-organisatie geïmplementeerd te worden. Daarom is in onderstaand overzicht getracht, om per geconstateerd probleem, een checklist op te nemen met de belangrijkste aandachtspunten voor een MKB-organisatie, die zouden moeten worden geregeld. In het hieronder weergegeven figuur, wordt gerefereerd aan de processen/elementen van de in dit rapport besproken beheermethodieken en kwaliteitsnormen, waarin dit onderwerp wordt behandeld.





\* **Figuur 11:** Zelf ontwikkelde beheermethodiek met IT-beheersmaatregelen, die speciaal is gericht op MKB-bedrijven

# 8 Conclusie en aanbevelingen

In dit hoofdstuk zullen de geformuleerde deelvragen voor onderzoek, in chronologische volgorde en zo beknopt mogelijk, worden beantwoord. De beantwoorde deelvragen zullen tezamen de hoofdvraag voor dit onderzoek beantwoorden. De hoofdvraag voor dit onderzoek luidt als volgt:

*‘’Op welke wijze kunnen organisaties in het MKB, veel voorkomende zwakheden met betrekking tot IT, die tot gevolg hebben dat de accountant tijdens de controle niet kan steunen op de AO/IB, beheersen?’’*

*‘’Wat is het belang van IT Governance voor organisaties?’’*

Elk bedrijf dient te streven naar het maximaliseren en waarborgen van de kwaliteit van de informatievoorziening (Fijneman, 2006). Daarnaast is het van belang dat een bedrijf voldoende aandacht schenkt aan het beoordelen of de maatregelen voldoende toereikend zijn en het beoordelen of de maatregelen in de dagelijkse praktijk in voldoende mate worden nageleefd. IT Governance speelt hierin een enorm belangrijke rol en is dus enorm van belang voor organisaties. Uiteindelijk is het doel van ‘’IT Governance’’, dat het bestuur van een bedrijf kan laten zien de juiste beheersing van de IT-infrastructuur, de IT systemen en het netwerk te hebben gerealiseerd (Fijneman, 2009). De IT-werkprocessen dienen hierbij effectief en efficiënt te worden geregeld, om de bedrijfsstrategie te kunnen ondersteunen (Fijneman, 2009). Uiteindelijk is het van belang dat de integriteit van de bedrijfsgegevens en daarmee een goede bedrijfsvoering is gewaarborgd (Loon, 2013).

Echter, blijken MKB-bedrijven, uit dit onderzoek, te weinig aandacht te schenken aan ‘’IT Governance’’. Dit wordt met name veroorzaakt door de kostbaarheid van IT. MKB-bedrijven zouden aan ‘’IT Governance’’ meer aandacht moeten schenken. Veel MKB-bedrijven zijn immers met betrekking tot hun voortbestaan afhankelijk van IT.

De ‘’IT Governance’’ is vaak bij de financiële afdeling (hoofd administrateur of controller) of bij een IT-er zonder echte opleiding, maar die “wel handig is met computers”, ondergebracht, waardoor er bij de leiding van de huishouding geen kennis is met betrekking tot IT. IT beheer is meestal geen integraal onderdeel van de bedrijfsvoering in het MKB. Slechts weinig MKB-bedrijven hebben een formeel IT-beleid opgesteld. Informatiebeveiliging is meestal beperkt tot de standaard zaken als firewalls, afgeschermde servers etc.

*‘’Welke bronnen voor IT normen worden in de praktijk veelal toegepast?’’*

Om IT beheersbaar te maken en om de kwaliteit van IT naar een hoger niveau te tillen, kunnen verschillende beheermethodieken en kwaliteitsnormen worden ingezet, zoals ITIL, ISO 20.000 en COBIT (Fijneman, 2006). Deze bronnen voor IT normen zijn in dit rapport reeds besproken en worden in de praktijk veelvuldig toegepast en zijn op dit moment actueel.

*‘’Op welke wijze geven de veel gebruikte bronnen voor IT normen invulling aan IT Governance?’’*

Zowel ITIL, als ISO 20.000 en COBIT, geven invulling aan ‘’IT Governance’’. ITIL en ISO 20.000 geven invulling aan “IT Governance’’, door te streven naar het creëren van toegevoegde waarde voor een bedrijf (Croon, 2008; Noë, 2006). ITIL versie 3 en ISO 20.000 doen dat voornamelijk in de twee componenten: ‘’Utility’’ (Fitness for Purpose: geschiktheid voor het doel) en ‘’ Warranty ‘’ (Fitness for Use: geschiktheid voor gebruik). Enerzijds is het van belang dat een IT-service voldoet aan de wensen van de gebruikers (‘’Use’’) en tevens de realisatie van de bedrijfsdoelstellingen waarborgt (‘’Purpose’’) (Croon, 2008). Anderzijds is het van belang dat een IT-service stuurbaar is, met als gevolg dat dit weer een groot aantal criteria oplevert om IT-prestaties (‘’IT-Performance’’) te kunnen beheersen. De beheermethodiek COBIT vult ITIL weer aan met een extra kwaliteitscriterium, namelijk ‘’Compliance’’. Bedrijfsprocessen dienen te voldoen aan verschillende wettelijke en contractuele regelingen. De bedrijfsdoelstellingen, die gerelateerd zijn aan ‘’Compliance’’, worden dus door COBIT erkend. Binnen het kwaliteitscriterium ‘’Compliance’’, is het van belang dat het interne beleid is afgestemd met de van buitenaf opgelegde wettelijke en contractuele regelingen. Tevens associeert COBIT de IT-doelen en de daar bijbehorende processen aan de bedrijfsdoelstellingen, om zodoende de bedrijfsdoelstellingen te kunnen behalen. Die combinatie tussen enerzijds prestaties, oftewel ‘’Performances’’, en anderzijds wet- en regelgeving, oftewel ‘’Compliance’’, zorgt voor ‘’IT Governance’’. In de praktijk is COBIT hierdoor goed te gebruiken in combinatie met ITIL, om invulling te geven aan ‘’IT Governance’’ en de fase ‘’Continual Service Improvement’’.

Hieruit kan dus worden geconcludeerd, dat bedrijven niet één van de beheermethodieken en kwaliteitsnormen volledig moeten toepassen, maar juist meerdere beheermethodieken en kwaliteitsnormen naast elkaar moeten gebruiken. Veel beheermethodieken en kwaliteitsnormen vullen elkaar immers aan, zoals ITIL en COBIT. Tevens is het aan te raden om niet alle processen uit de verschillende beheermethodieken en kwaliteitsnormen integraal over te nemen maar een selectie te maken van de processen, die van belang zijn voor het bedrijf. Het gebruik van beheermethodieken en kwaliteitsnormen draagt op deze manier bij aan het realiseren van een correct en fatsoenlijk IT beheer en zorgt ervoor dat bedrijven in ieder geval bezig zijn met ‘’IT Governance’’ en hier dus voldoende aandacht aan schenken.

*‘’Op welke wijze zijn de veel gebruikte bronnen voor IT normen in de praktijk te implementeren?’’*

Uit dit onderzoek, blijkt echter dat MKB-bedrijven, in tegenstelling tot grote bedrijven, weinig gebruik maken van bronnen voor IT normen om IT-processen in te richten, te beheersen en te verbeteren (Noë, 2006). IT wordt vaak als bijzaak gezien en de normen en inrichting worden vaak bepaald op basis van gebruikersgemak. Tevens zijn de implementaties van bronnen voor IT-normen enorm complexe processen en brengen ze enorm hoge kosten met zich mee (Bolland, 2011). Meestal duurt het wel enkele jaren voordat een bron voor een IT norm volledig is geïmplementeerd binnen een bedrijf.

De totale duur van een implementatie wordt hierbij beïnvloed door factoren als, de grootte van de organisatie en het gekozen vertrekpunt. Er zijn zelfs bedrijven die al meerdere implementaties achter de rug hebben. Vaak worden deze onsuccesvolle implementaties veroorzaakt doordat bedrijven teveel bezig zijn met de theorie en te weinig kijken naar een concreet probleem of een concrete verbetering. De andere vereisten, die de kans op het realiseren van succesvolle implementaties vergroten, zijn in dit rapport reeds besproken.

*‘’Welke versterkingen en verzwakkingen van de interne controle met betrekking tot IT, komen accountants bij de controle van MKB-bedrijven veelal tegen?’’*

In de praktijk zie je dat veel MKB-bedrijven, na/tijdens een implementatie van een bron voor een IT norm, weer op de oude voet doorgaan, met alle gevolgen van dien. Uit dit onderzoek, blijken veel MKB-bedrijven te maken te hebben met tekortkomingen in de getroffen IT-beheersmaatregelen, waarbij de tekortkomingen voornamelijk betrekking hebben op informatiebeveiliging en dus op het primaire kwaliteitsaspect voor de bedrijfsgegevens ‘’vertrouwelijkheid’’ (‘’confidentiality’’) (Bolland, 2011; Fijneman, 2009; Romney, 2012). Deze tekortkomingen, met betrekking tot informatiebeveiliging, bij MKB-bedrijven, die de kwaliteit van de AO/IC verzwakken, zijn reeds in kaart gebracht. Tevens zijn hiervoor passende IT-beheermaatregelen getroffen.

Deze getroffen IT-beheersmaatregelen zijn deels tot stand gekomen door het afnemen van interviews en deels door het verrichten van observaties. Bovendien is er literatuuronderzoek gedaan, waarbij een aantal elementen uit de beheermethodieken en kwaliteitsnormen: ITIL, ISO 20.000 en COBIT, zijn gebruikt. Uit dit onderzoek, blijken zowel ITIL, als ISO 20.000 en COBIT, in de processen invulling te geven aan informatiebeveiliging, waarbij de algemene informatiebeveiligingsmaatregelen veelal zijn gebaseerd op ISO 27.002: Code voor Informatiebeveiliging (Elsinga, 2014). Uit dit onderzoek, blijkt echter dat de invulling aan informatiebeveiliging, bij deze beheermethodieken en kwaliteitsnormen, beperkt is. ITIL, ISO 20.000 en COBIT zijn voor een groot deel gericht op IT beheer. Informatiebeveiliging gaat echter veel verder dan alleen IT beheer. Zoals al eerder in dit rapport is aangegeven, is het daarom aan te raden om ITIL, ISO 20.000 en COBIT, naast elkaar te gebruiken. Het volledig toepassen van één van deze beheermethodieken en kwaliteitsnormen zal niet voldoende zijn.

*‘’Welke IT-beheersmaatregelen, waaronder general en application IT controls, zijn bij de controle van MKB-bedrijven voor de accountant van belang om te kunnen steunen op de AO/IB?’’*

Concluderend, levert dit een beheermethodiek op met IT-beheersmaatregelen, die speciaal is gericht op MKB-bedrijven. Deze is reeds in hoofdstuk 7.3.3 van dit rapport gepresenteerd.

Het is aan te bevelen, om als MKB-bedrijf, deze zelf ontwikkelde beheermethodiek te gebruiken om informatiebeveiliging in te richten, te beheersen en te verbeteren. Op deze manier kan een bijdrage worden geleverd aan het realiseren van een correct en fatsoenlijk IT beheer, dat voldoende is afgestemd met de businessbehoeften (Noë, 2006; Romney, 2012). Informatiebeveiliging is tegenwoordig immers van essentieel belang (ISACA, 2012). Op het moment dat de informatiebeveiliging bij een bedrijf niet op orde is, kan dit desastreuze gevolgen hebben voor een bedrijf. Zo kan dit leiden tot financiële en operationele schades, alsmede imagoschade of juridische risico’s, die klant of werknemer relaties of zelfs de bedrijfscontinuïteit in gevaar kunnen brengen.Daarentegen is het ook sterk aan te bevelen, om als accountant, deze zelf ontwikkelde beheermethodiek met algemene IT-beheersmaatregelen voor te leggen aan klanten, om nu en in de toekomst minder aanvullende gegevensgerichte controlewerkzaamheden uit te hoeven voeren (Wildschut, 2013).

Ten slotte blijkt uit dit onderzoek, dat IT de kwaliteit van de AO/IC bij MKB-bedrijven niet alleen maar verzwakt, maar ook versterkt. Zo treffen veel accountants bij de controle van MKB-bedrijven, bijvoorbeeld standaard doorlopende nummering van in- en verkooporders waarbij orders niet verwijderd kunnen worden en standaard ingerichte betaalbevoegdheden in het bankpakket, aan, wat de kwaliteit van de AO/IC versterkt.

# 9 Reflectie onderzoek

Voor mijn afstudeeropdracht heb ik onderzoek gedaan naar de meest voorkomende IT-problemen bij MKB-bedrijven, op het gebied van informatiebeveiliging. Voor deze IT-problemen heb ik vervolgens, door het afnemen van interviews, het verrichten van observaties en het doen van literonderzoek, passende algemene IT-beheersmaatregelen getroffen. Uiteindelijk heeft dit een eindproduct opgeleverd in de vorm van een beheermethodiek. Deze beheermethodiek is speciaal gericht op MKB-bedrijven en bevat algemene IT-beheersmaatregelen voor het inrichten, beheersen en verbeteren van IT-processen, met betrekking tot informatiebeveiliging.

De context, waarbinnen het onderzoek is uitgevoerd, was goed. De interviews verliepen goed en er werd niet terughoudend gedaan op het moment dat ik antwoorden nader toegelicht wilde hebben. Voor de interviews, werd genoeg tijd vrijgemaakt om mij te helpen met mijn onderzoek. De antwoorden, die de geïnterviewde registeraccountants mij gaven, vielen me wat tegen, omdat ze voldeden aan de verwachting. De IT-voorzieningen, waar ik tijdens mijn onderzoek gebruik van maakte, waren goed. Ik heb zelden last gehad van netwerkstoringen etc. en kon in een goede werkomgeving mijn onderzoek verrichten. Het onderzoek, heb ik geheel onafhankelijk van eventuele eisen van MTH kunnen inrichten en uitvoeren. Ook met betrekking tot de conclusies en aanbevelingen, heb ik van MTH de vrijheid gekregen om deze zelf te formuleren. Ik heb het probleem, met betrekking tot informatiebeveiliging, bij MKB-bedrijven, voorgelegd aan MTH te Hoevelaken, waarna MTH instemde en mij de opdracht gaf. De controlepraktijk binnen MTH te Hoevelaken, zal nu bij de controle van MKB-bedrijven extra alert zijn op de door mij in kaart gebrachte IT-problemen, met betrekking tot informatiebeveiliging. Tevens zullen zij de door mij ontwikkelde beheermethodiek met algemene IT-beheersmaatregelen, gaan voorleggen aan klanten, om nu en in de toekomst minder aanvullende gegevensgerichte controlewerkzaamheden uit te hoeven voeren (Wildschut, 2013).

Voorafgaand aan het uitvoeren van mijn onderzoek, heb ik een uitgebreid plan van aanpak op papier gezet, relevante bronnen en literatuur verzameld, afspraken gemaakt voor het afnemen van interviews en het verrichten van observaties en een planning gemaakt, met de per week, door mij op te leveren hoofdstukken. Het vooraf maken van een duidelijke planning heeft ervoor gezorgd dat ik elke week getriggerd werd om iets op te leveren.

Tevens was het formuleren van een duidelijke probleemstelling voor mij enorm belangrijk. Op het moment dat ik het probleem goed in kaart had gebracht, was het voor mij gelijk een stuk gemakkelijker om te komen tot aanbevelingen. Dit alles heeft mij uiteindelijk erg geholpen in het gehele proces. Ik liep bij het uitvoeren van mijn onderzoek bijna altijd op schema en heb weinig problemen bij het uitvoeren van mijn onderzoek ondervonden.

Bij het verzamelen van relevante bronnen en literatuur, was ik echter wel ontevreden over het feit dat ik geen selectie had gemaakt van de door mij verzamelde literatuur en bronnen. Ik had op een gegeven moment zoveel literatuur en bronnen verzameld, dat ik eigenlijk niet meer wist welke literatuur en bronnen ik nou moest gaan gebruiken. In veel literatuur en bronnen stond immers hetzelfde. De volgende keer moet ik dit anders aanpakken en vooraf al een selectie maken van de door mij te gebruiken literatuur en bronnen.

# Literatuur

APM Group Limited. (2010, 5). *ITIL ® : De basics*. Opgeroepen op 5 10, 2014, van Axelos.com: http://www.axelos.com/gempdf/ITIL\_The\_Basics\_White\_Paper\_Dutch.pdf

Arnoud van ‘t Hoff. (2008, 12). *Dienstverlening naar hoger niveau*. Opgeroepen op 5 10, 2014, van Vka.nl: http://www.vka.nl/sites/default/files/downloads/ISO20000.pdf

A. van Gils. (2005, 6). *Het gebruik van COBIT binnen Philips*. Opgeroepen op 5 17, 2014, van Finance-Control.nl: [www.finance-control.nl/downloaden/7760/Het-gebruik-van-COBIT-binnen-Philips](http://www.finance-control.nl/downloaden/7760/Het-gebruik-van-COBIT-binnen-Philips)

Drs. C.W.A.M. van Oosterhout. (2010). *Een zoektocht naar een theoretisch kader met praktische meerwaarde.* Opgeroepen op 2 17, 2014, van NOREA: http://www.norea.nl/readfile.aspx?ContentID=65064&ObjectID=659911&Type=1&File=0000031698\_P36%20Regisseren%20van%20inform.pdf

Frank Noë. (2006). *Jaarboek IT beheer en informatiebeveiliging,* Den Haag: Sdu Uitgevers bv.

F. Stevens, W. van Grembergen, S. de Haes. (2008). *De convergentie van ITIL V3 en COBIT 4.1.* Opgeroepen op 4 17, 2014, van ITMG.nl: http://www.itmg.nl/itmg-wp-content/Artikelen/COBIT/Training/ITIL%20V3%20en%20COBIT%204.1.pdf

Prof. Dr. Ir. M. Looijen, Dr. L.J.G.T. van Hemmen. (2011). *Beheer van informatiesystemen – voor onderwijs en praktijk,* Den Haag: Sdu Uitgevers bv.

ISACA. (2012). *COBIT 5 for Information Security - Preview Version*. Opgeroepen op 6 5, 2014, van ISACA: http://www.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf

ISACA. (2012). *COBIT 5 Framework.* Opgeroepen op 2 28, 2014, van ISACA: http://www.isaca.org/COBIT/Pages/COBIT-5-Framework-product-page.aspx

ISACA. (2012). *COBIT 5 Introduction.* p. 8, 25, 35, 36. Opgeroepen op 3 20, 2014, van ISACA: https://www.isaca.org/COBIT/Documents/COBIT5-Introduction.ppt

IT Management Group. (n.d.). *ITIL Best Practice*. Opgeroepen op 4 17, 2014, van ITIL.nl: http://www.itil.nl/itil-best-practice/

Jan van Bon. (2007). *IT Service Management, best practices: Deel 4.* Lunteren: Van Haren Publishing.

J. van Crooij. (2013). *Elf grote en kleine valkuilen bij MKB-gerichte IT-audits.* Opgeroepen op 2 17, 2014, van Accountancynieuws: http://www.accountancynieuws.nl/Uploads/Files/AN-1315-Van-Crooij-Valkuilen-MKB-gerichte-IT-audits\_1.pdf

Prof. Lindgreen, Dr. E.E.O. Roos. (2005). *COBIT: Opkomst, ondergang en oplevering van een raamwerk voor informatiebeheersing* . Opgeroepen op 2 17, 2014, van MAB-online: http://www.mab-online.nl/artikel/384/COBIT-Opkomst,-ondergang-en-opleving-van-een-raamwerk-voor-informatiebeheersing

Marschall B. Romney, Paul J. Steinbart. (2012). *Accounting Information Systems - Twelfth Edition*, Harlow: Pearson Education Limited.

M. Bouker. (n.d.) *De essentials van COBIT.* Opgeroepen op 3 16, 2014, van ITMG.nl: http://www.itmg.nl/itmg-wp-content/Artikelen/COBIT/Training/De%20essentials%20van%20COBIT.pdf

Dr. R.G.A. Fijneman. (2009). *Informatiebeveiliging en Finance & Control – van kopzorg tot hoofdzaak?* Opgeroepen op 2 17, 2014, van MAB-online: http://www.mab-online.nl/artikel/688/Informatiebeveiliging-en-Finance-Control-–-van-kopzorg-tot-hoofdzaak

Rob Fijneman, Edo Roos Lindgreen, Kai Hang Ho. (2006). *IT-auditing en de praktijk,* Den Haag: Sdu Uitgevers bv.

Rob Fijneman, Edo Roos Lindgreen, Piet Veltman. (2005). *Grondslagen IT-auditing,* Den Haag: Sdu Uitgevers bv.

S. Polter. (n.d.). *ISO/IEC 20000, een ITIL-certiﬁcaat voor organisaties*. Opgeroepen op 5 20, 2014, van Ngi-Library.nl: http://www.ngi-library.nl/Player/eKnowledge/iso\_iec\_20000\_een\_itil-certificaat\_voor\_organisaties.pdf

# Bronnen

Accountancy Nieuws. (2010). *‘IT auditor in het MKB: dat bent u!’ en uw collega’s.* Opgeroepen op 5 27, 2014, van Accountancynieuws.nl: http://www.accountancynieuws.nl/Uploads/Files/KREUZE---CONFERENTIEZAAL.PDF

APM Group. (n.d.). *ISO/IEC 20000 Certified Organizations*. Opgeroepen op 5 20, 2014, van Isoiec20000certification.com: http://www.isoiec20000certification.com/home/ISOCertifiedOrganizations/ISOCountryListings.aspx

B. Bolland, K. de Koning. (2011). *Heeft ITIL nog toekomst voor MKB organisaties?* Opgeroepen op 2 17, 2014, van XR Magazine: http://www.xr-magazine.nl/artikelen/1065/beheer/heeft-itil-nog-toekomst-voor-mkb-organisaties-voor-mkb-organisaties

BSI Group. (n.d.). *ISO/IEC 20000 IT Service Management implementeren.* Opgeroepen op 5 10, 2014, van Bsigroup.nl: http://www.bsigroup.com/nl-NL/ISOIEC-20000-IT-Service-Management/ISOIEC-20000-Implementatie/

Elsinga. (2014, 5 8). *De zeven succesfactoren om uw security baseline te implementeren*. Opgeroepen op 5 29, 2014, van Wikkle.nl: http://www.wikkle.nl/blog/de-zeven-succesfactoren-om-uw-security-baseline-te-implementeren.html

G. Bloemendal. (n.d.) *De norm en de praktijk.* *Nieuwe generatie ITIL: een flinke stap vooruit.* Opgeroepen op 5 10, 2014, van TOPdesk Magazine: http://www.topdeskmagazine.nl/artikelen/de-norm-en-de-praktijk.-nieuwe-generatie-itil-een-flinke-stap-vooruit/

G. Van Veen. (n.d.). *Inpassen ITIL in de organisatie*.Opgeroepen op 5 10, 2014, van GVV-Web.nl: http://gvv-web.nl/itil.html

ISACA. (n.d.). *COBIT 5 Training Providers*. Opgeroepen op 5 20, 2014, van ISACA: http://www.isaca.org/education/cobit-education/pages/introduction-to-cobit-5-licensed-training-providers.aspx

ITSMF. (n.d.). *ITIL*. Opgeroepen op 5 10, 2014, van ITSMF.nl: http://www.itsmf.nl/topic/itil

J. Mulder. (2012, 5 8). *ISO 20000 voor cloudprovider Uniserver*. Opgeroepen op 5 10, 2014, van ISPam.nl: http://www.ispam.nl/archives/27428/iso-20000-voor-cloudprovider-uniserver/

J. ten Hagen. (2013, 12 10). *Waar kun je ISO 20000 voor gebruiken?* Opgeroepen op 5 20, 2014, van Computable.nl: http://www.computable.nl/artikel/opinie/management/4948148/2379250/waar-kun-je-iso-20000-voor-gebruiken.html

J. Van Beem. (n.d.). *Implementeren van ITIL®... veranderen OF leren?* Opgeroepen op 5 10, 2014, van iSES.nl: http://www.ises.nl/implementeren-van-itil-veranderen-leren

Loon, R. v. (2013, 9 19). *Powerpointpresentatie BIV 3 voor OAT - College 5 - Donderdag 3/10*. Utrecht, Utrecht, Nederland: Hogeschool Utrecht.

M. Croon.(2008). *ITIL 3 en COBIT 4 gemaakt voor governance?* Opgeroepen op 3 16, 2014, van Computable.nl: http://www.computable.nl/artikel/opinie/softwarebeheer/2627136/4480179/itil-3-en-cobit-4-gemaakt-voor-governance.html

MTH: Drs. J.A. Rijken RA, Mr. S. Riedstra, J.W. Hoek RA MA. (2012). *Maatschappelijk Jaarverslag Meeuwsen Ten Hoopen 2012*. p. 14, 15. Opgeroepen op 2 28, 2014, van MTH: http://www.mth.nl/content/files/Files/MVO/MTH\_Maatschappelijk\_jaarverslag\_2012.pdf

MTH. (n.d.). *Uw accountant en belastingadviseur | MTH*. Opgeroepen op 2 28, 2014, van MTH: http://www.mth.nl

S. Jerphanion. (n.d.). *6 richtlijnen voor het succesvol toepassen van ITIL v3*. Opgeroepen op 5 10, 2014, van TOPdesk Magazine: http://www.topdeskmagazine.nl/artikelen/6-richtlijnen-voor-het-succesvol-toepassen-van-itil-v3/

Whizpr. (2007, 10 16). *Merendeel ISO 20000 certificaties toegekend aan Indische service providers*. Opgeroepen op 5 10, 2014, van Whizpr.nl: http://www.whizpr.nl/persberichten/merendeel-iso-20000-certificaties-toegekend-aan-indische-service-providers

Wildschut. (2013, 4 11). *De IT-auditor komt van Venus*. Opgeroepen op 3 2, 2014, van Accountant.nl: http://www.accountant.nl/Accountant/Weblogs/Wildschut/De+ITauditor+komt+van+Venus.aspx

Zijlstra. (2002, 10 13). [*Informatiebeveiliging en ICT-beheer op basis van ITIL*](http://www.zbc.nu/ict/checklists-review-itil-processen/informatiebeveiliging-en-ict-beheer-op-basis-van-itil/)*.* Opgeroepen op 5 29, 2014, van Zbc.nu: http://www.zbc.nu/ict/checklists-review-itil-processen/informatiebeveiliging-en-ict-beheer-op-basis-van-itil/

# Bijlage 1 ITIL

#### 4.1.1.1 Service Strategy

Deze fase richt zich op het ontwerpen, het ontwikkelen en het implementeren van servicemanagement als een strategisch middel (Looijen, 2011). Het gaat er hierbij om dat het beleid en de strategie daadwerkelijk worden geïmplementeerd en dat de processen die daarvoor nodig zijn, correct worden uitgevoerd (Croon, 2008). Door het leveren van betere prestaties en onderscheidend te zijn, is het uiteindelijke doel van deze fase om de concurrenten vanuit andere IT-serviceverleners te erkennen en deze te beconcurreren (Looijen, 2011). De prestaties dienen door IT-organisaties te worden verantwoord en daarnaast dient te worden voldaan aan de van kracht zijnde wet- en regelgeving (compliance). Dit laatste wordt echter niet binnen deze fase uitgewerkt (Croon, 2008). Deze fase bestaat uit een drietal processen. Deze zijn (Looijen, 2011):

* *Service Portfolio Management:* het proces dat als doel heeft om waarde die door de inzet van IT wordt gecreëerd, te maximaliseren. Dit wordt bewerkstelligd door het definiëren, analyseren, goedkeuren en vastleggen van de services in een portfolio. De risico’s van het niet goed leveren van de services worden beheerst en de kosten worden bewaakt, bij de realisatie van de waardecreatie door de inzet van IT;
* *Financial Management:* het proces heeft als doel om de services zo efficiënt en kosteneffectief mogelijk uit te voeren. Hier ligt de nadruk voornamelijk op de bepaling van de waarde van de IT-service vanuit het klantperspectief;
* *Demand Management:* het proces heeft als doel om de vraag naar IT-producten zo goed mogelijk te bepalen en in goede banen te leiden.

Doordat IT-services geen fysieke producten zijn, dienen er steeds op de juiste momenten voldoende resources aanwezig te zijn om de services te kunnen verlenen.

#### 4.1.1.2 Service Design

Deze ontwerpfase richt zich op het ontwikkelen van passende en innovatieve IT-services, zoals processen, architectuur, beleid en documenten (Looijen, 2011). Het uitgangspunt die hierbij gehanteerd wordt, is het voldoen aan de huidige en toekomstige businessbehoeften. Deze fase heeft als doel om nieuwe of gewijzigde services, alsmede de bijbehorende beheerprocessen, te ontwerpen voor introductie in een productieomgeving. Deze ontwerpfase bestaat uit een zevental processen. Deze zijn (Looijen, 2011):

* *Service Catalog Management:* het proces dat als doel heeft om een servicescatalogus op te stellen en te beheren. De status alsmede de beschrijving, zoals het beleid, de richtlijnen, de prijzen, de dienstafspraken en de leveringsvoorwaarden worden voor elke service afzonderlijk bijgehouden;
* *Service Level Management:* het proces heeft als doel om overeenkomsten (‘’Service Level Agreements’’) tot stand te brengen tussen het beheer van informatiesystemen (IT-beheer) en de IT-gebruikers. Dit wordt bewerkstelligd door de eisen en behoeften vanuit de bedrijfsprocessen in kaart te brengen en dit te vertalen naar de services, door het inventariseren, definiëren, onderhandelen, vastleggen en rapporteren van de in belang zijnde services en servicelevels. Binnen de IT-beheerorganisatie worden de onderlinge afspraken tussen de organisatorische eenheden vastgelegd in ‘’Operational Level Agreements’’ (OLA’s), waarbij het van belang is dat deze vastgelegde afspraken worden bewaakt en geëvalueerd. Dit proces kan weer onderverdeeld worden in een aantal deelprocessen.

Deze zijn: het in kaart brengen van IT-behoeften, het verifiëren van de haalbaarheid, het opstellen van ‘’Service Level Agreements’’ (SLA’s) en het bewaken van de normen en waarden die in de ‘’Service Level Agreements’’ (SLA’s) zijn vastgelegd;

* *Supplier Management:* het proces bestaat uit het relatiebeheer van de leveranciers en de daarbij behorende te leveren prestaties. Tevens bestaat dit proces uit het afstemmen van de externe serviceafspraken, die zijn vastgelegd in ‘’Underpinning Contracts’’ (UC’s), op de businessbehoeften en het bewaken dat de services ook daadwerkelijk verleend worden met de afgesproken prijs en kwaliteit;
* *Capacity Management:* het proces heeft als doel om op elk moment te kunnen voldoen aan de huidige en toekomstige klantvraag, door de juiste capaciteit aan IT-middelen beschikbaar te stellen. Daarnaast heeft dit proces als doel om tegen verantwoorde kosten, de juiste capaciteit aan IT-middelen beschikbaar te stellen. Dit proces kan weer onderverdeeld worden in een aantal deelprocessen. Deze zijn: ‘’Business Capacity’’, ‘’Service Capacity’’, ‘’Resource Capacity Management’’, ‘’Prestatiebeheer’’, ‘’Middelenbeheer’’, ‘’Vraagbeheersing’’, ‘’Werklastbeheersing’’, ‘’Applicatiedimensionering’’ en ‘’Capaciteitsplanning’’;
* *Availability Management:* het proces heeft als doel om de faciliteiten van de infrastructuur, de services- en supportorganisatie te optimaliseren. Om ervoor te zorgen dat het bedrijf de doelstellingen realiseert, is het van belang om ervoor te zorgen dat er een kosteneffectief en gegarandeerd niveau van beschikbaarheid kan worden geboden.

Zoals al in één van de voorgaande processen is uitgelegd, worden in de ‘’Service Level Agreements’’ (SLA’s) verschillende afspraken gemaakt voor wat betreft de ingeplande beschikbaarheid van producten en services.

Echter, op het moment dat de servicenormen niet gehaald worden, gaat het ‘’Availability Management’’ proces een belangrijke rol vervullen. Dit proces kan samen met het ‘’Problem Management’’ proces en het ‘’Capacity Management‘’ proces, de producten en services analyseren. Dit proces kan weer onderverdeeld worden in een aantal deelprocessen. Deze zijn: planning van de beschikbaarheid van IT, bewaking, toezicht en samenwerking met probleembeheer om eventuele voorzorgmaatregelen te nemen;

* *IT Service Continuity Management:* het proces heeft als doelom ervoor te zorgen dat er genoeg technische, financiële en organisatorische voorzieningen zijn getroffen. Op deze manier wordt geprobeerd de continuïteit van de IT-services bij nood te waarborgen. Dit proces kan weer onderverdeeld worden in een aantal deelprocessen. Deze zijn: risicoanalyse, risicobeheersing, calamiteitenplanning en rapportage in kader van calamiteitenbeheersing om alle stakeholders te informeren;
* *Information Security Management:* het proces heeft als doel om afstemming te realiseren tussen het beveiligingsbeleid van de business en de IT. Daarnaast heeft dit proces als doel om de informatiebeveiliging in alle services en beheeractiviteiten effectief te beheren en te besturen. Met behulp van dit proces wordt geprobeerd voldoende aandacht te schenken aan de primaire kwaliteitsaspecten voor de bedrijfsgegevens, namelijk vertrouwelijkheid, integriteit, beschikbaarheid en controleerbaarheid (Romney, 2012).

#### 4.1.1.3 Service Transition

Deze fase hanteert de ontwikkelde specificaties bij het proces ‘’Service Design’’ als uitgangspunt (Looijen, 2011). Deze specificaties worden ontwikkeld en verbeterd, waarna ze worden omgezet naar nieuwe of gewijzigde IT-services.Deze fase heeft als doel om ondersteuning te bieden aan de business bij veranderingen.

Daarnaast heeft deze fase als doel om variaties in de prestaties te verminderen, het aantal fouten te verminderen in nieuwe of gewijzigde services en om ervoor te zorgen dat de services aan de overeengekomen specificaties voldoen. Deze fase bestaat uit een zevental processen. Deze zijn (Looijen, 2011):

* *Transition Planning and Support:* het proces heeft de verzorging van de resourceplanning alsmede de verzorging van de coördinatie voor het realiseren van de servicespecificaties, als doel. Daarnaast heeft dit proces als doel om het risicobeheer van de risico’s die een negatief effect hebben op de services, te verzorgen;
* *Change Management:* het proces heeft als doel om wijzigingen op een bedrijfsmatig verantwoorde manier door te voeren. Het is van belang dat deze wijzigingen zo snel mogelijk worden doorgevoerd, zodat de wijzingen geen negatieve invloed hebben op de kwaliteit van de services. De processen ‘’Incident Management’’ en ‘’Problem Management’’, die betrekking hebben op de bestaande IT en IT-services, kunnen deze voorstellen tot wijzigingen tot gevolg hebben. Daarnaast kunnen eventuele voorstellen tot wijzigingen komen vanuit de gebruikersorganisatie, die behoefte heeft aan nieuwe functionaliteiten en dat ook heeft laten weten. Dit proces kan weer worden onderverdeeld in een aantal deelprocessen. Deze zijn: acceptatie van voorstellen tot wijzigingen, beoordelen en plannen, coördineren en afsluiten op het moment dat wijzigingen zijn doorgevoerd;
* *Service Asset & Configuration Management:* het proces heeft als doel om een logisch model van de IT-infrastructuur te definiëren en te onderhouden. In dit logische model van de IT-infrastructuur dient er een relatie te zijn tussen de IT-services en de bijbehorende IT-componenten, die vereist zijn om de IT-services te kunnen verlenen;
* *Release & Deployment Management:* het proces heeft als doel om ervoor te zorgen dat alleen geteste en juiste versies van geautoriseerde IT-componenten worden geproduceerd. Dit proces kan weer onderverdeeld worden in een aantal deelprocessen. Deze zijn: beheer van de programmatuurbibliotheek, acceptatiefasen, distributie, implementatie en rapportage;
* *Service Validation:* het proces heeft als doel om ervoor te zorgen dat een service toegevoegde waarde levert aan het bedrijf. Dit wordt bewerkstelligd door na te gaan of de service voldoet aan de klantverwachtingen. Daarnaast wordt nagegaan of de service voldoet aan de specificaties van alle betrokkenen, waaronder de klant;
* *Evaluation:* het proces heeft als doel om een inzicht te krijgen in de geleverde prestaties van de service alsmede de changes. Dit inzicht kan worden verkregen aan de hand van wijzigingsverzoeken, serviceontwerpen, testplannen en testresultaten;
* *Knowledge Management:* het proces heeft als doel om betrouwbare en veilige informatie beschikbaar te stellen, gedurende de gehele ‘’Service Lifecycle’’. Dit om ervoor te zorgen dat de kwaliteit van de besluitvorming wordt verbeterd, met bijvoorbeeld als gevolg dat leveranciers worden ondersteund om verbetering aan te brengen in de efficiëntie en kwaliteit van de services en dat medewerkers van de leveranciers van informatie worden voorzien.

#### 4.1.1.4 Service Operation

Deze fase richt zich op de ondersteuning van IT-services en het efficiënter en effectiever leveren van de IT-services (Looijen, 2011). Op deze manier wordt een zo groot mogelijke toegevoegde waarde voor de klant en de serviceverlener gecreëerd. Er worden verschillende processen binnen deze fase uitgevoerd en gecoördineerd, om ervoor te zorgen dat services tegen een vooraf bepaald niveau worden geleverd en worden beheert voor gebruikers.

De processen in deze fase zijn tevens van belang voor het beheer van de techniek, die vereist zijn om de services te kunnen leveren en te ondersteunen. Deze fase bestaat uit een vijftal processen. Deze zijn (Looijen, 2011):

* *Event Management:* het proces heeft als doel om events, oftewel gebeurtenissen, op te sporen en te analyseren, om zodoende tot de juiste beheeractie te kunnen komen. Een event is niets anders dan een willekeurig meetbare en waarneembare gebeurtenis om IT-infrastructuur te kunnen beheren en besturen, om een IT-service te kunnen leveren en om de invloed die een afwijking op de service kan hebben, te evalueren;
* *Incident Management:* het proces heeft als doel om de afgesproken IT-serviceverlening bij eventuele fouten, zo snel mogelijk te herstellen. Op deze manier worden de afgesproken servicenormen in ieder geval nagekomen. Dit proces is weer onder te verdelen in een aantal deelprocessen. Deze zijn: incident registratie, classificatie en toewijzing, onderzoek en diagnose, oplossing en herstel, afsluiting van het incident en de rapportage;
* *Request Management:* het proces heeft als doel om service requests van gebruikers af te handelen. Een service request is niets anders dan informatie, advies, een standaard change of toegang tot een service, die een gebruiker wenst te krijgen;
* *Problem Management:* het proces heeft als doel om problemen die worden veroorzaakt door incidenten, op te merken. Op deze manier kunnen er structurele wijzigingen worden doorgevoerd in de IT-infrastructuur, om dezelfde problemen in de toekomst te kunnen voorkomen. In dit proces worden de incidenten geclassificeerd en wordt onderzocht welke oorzaken ten grondslag liggen aan de problemen. Aan de hand hiervan wordt een wijzigingsvoorstel opgesteld, dat uiteindelijk de fouten moet corrigeren. Dit proces is weer onder te verdelen in een aantal deelprocessen. Deze zijn: probleemidentificatie en –registratie, probleemclassificatie, probleemonderzoek, foutbeheer en rapportage;
* *Access Management:* het proces heeft als doel om geautoriseerde gebruikers toegang te geven om een bepaalde service te gebruiken. Daarentegen dienen niet geautoriseerde gebruikers juist weer geen toegang te krijgen om een bepaalde service te gebruiken. Een ander woord voor dit proces is ook wel ‘’Identity Management’’.

#### 4.1.1.5 Continual Service Improvement

Deze fase richt zich op het creëren en behouden van toegevoegde waarde voor de klanten (Looijen, 2011). Het gaat hierbij om het draaiende krijgen of houden van het verbeterwiel van een organisatie (Croon; 2008). Dit wordt gerealiseerd door ontwerpverbeteringen door te voeren en nieuwe services te introduceren en te produceren (Looijen, 2011). Deze fase heeft als doel om ‘’Service Level Achievements’’ te meten en te analyseren. Dit wordt bewerkstelligd aan de hand van ‘’Service Level Agreements’’ (SLA’s). Daarnaast heeft deze fase als doel om verbeteringen door te voeren in alle fasen, activiteiten in te voeren om services en processen te verbeteren en om kosteneffectiviteit en kwaliteitsmanagement methoden te gebruiken. Deze fase bestaat uit een tweetal processen. Deze zijn (Looijen, 2011):

* *Seven Step Improvement:* het proces heeft als doel om meetgegevens op elk moment te meten en te verwerken, om zodoende de serviceverlening te kunnen verbeteren. Om uiteindelijk de verbetering van de serviceverlening te kunnen realiseren, dienen een zevental stappen te worden uitgevoerd. Deze zijn: wat zou u moeten meten, wat kunt u meten, gegevens verzamelen, gegevens verwerken, gegevens analyseren, presenteren en gebruiken van informatie en herstellende acties uitvoeren;
* *Service Reporting:* het proces dient zorg te dragen voor het opstellen en leveren van ‘’Service Level Agreements’’ (SLA’s).

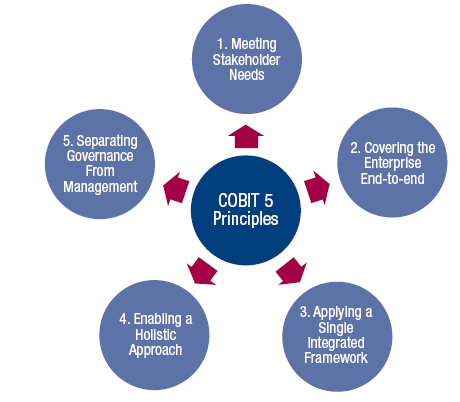
Deze rapportage bestaat naast de bereikte servicenormen en uitzonderingen, ook uit de genomen maatregelen om eventuele toekomstige afwijkingen te kunnen voorkomen.

# Bijlage 2 ISO 20.000

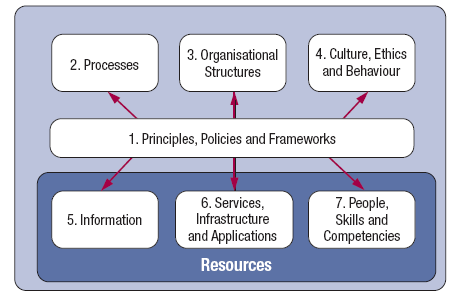
De vijf processen, die invulling geven aan het tweede deel van deze ISO-norm, zijn (Looijen, 2011):

* *Service Delivery Processes:* dit proces kan onderverdeeld worden in de processen ‘’Service Level Management’’, ‘’Service Reporting’’, ‘’Capacity Management’’, ‘’Service Continuity and Availability Management’’, ‘’Information Security Management’’ en ‘’Budgeting and Accounting for IT services’’;
* *Relationship Processes:* dit proces kan onderverdeeld worden in de processen ‘’Business Relationship Management’’ en ‘’Supplier Management’’;
* *Resolution Processes:* dit proces kan onderverdeeld worden in de processen ‘’Incident Management’’ en ‘’Problem Management’’;
* *Release Process:* dit proces kan onderverdeeld worden in één proces en wel in ‘’Release Management’’;
* *Control Processes:* dit proces kan onderverdeeld worden in de processen ‘’Configuration Management’’ en ‘’Change Management’’.

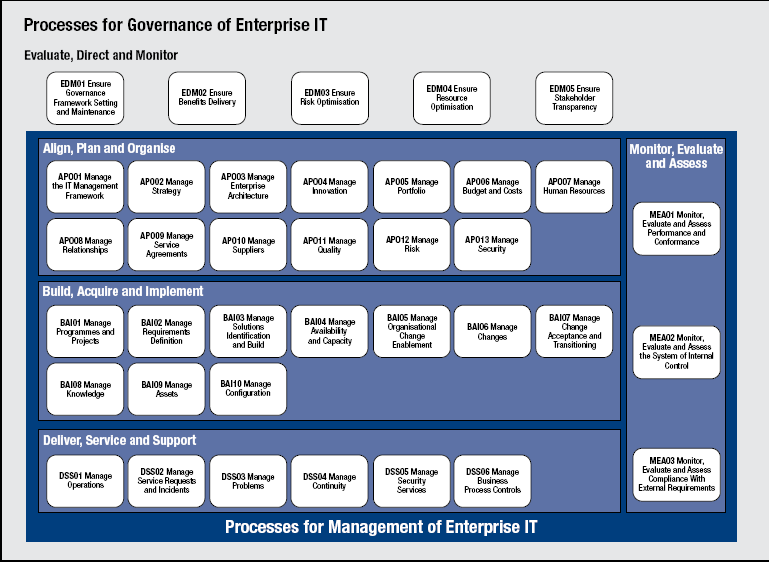
# Bijlage 3 COBIT

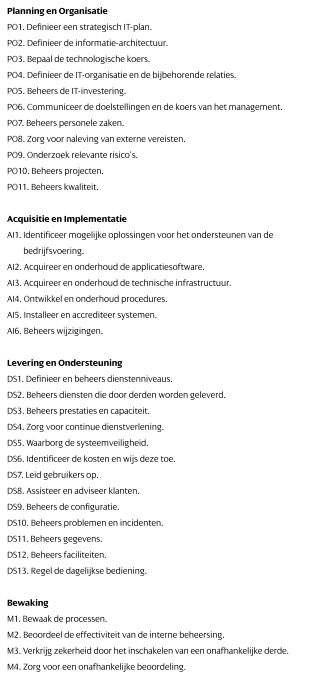


\* **Figuur 6:** Grafische weergave van het gehele COBIT-5-principe (ISACA, 2012, p. 8)

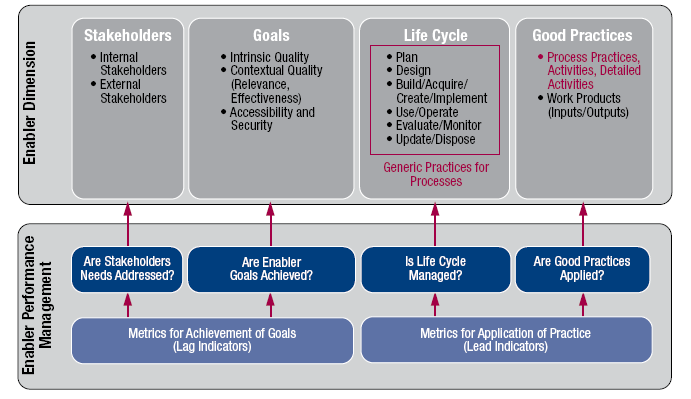


\* **Figuur 7:** Grafische weergave van het gehele COBIT-5-principe (ISACA, 2012, p. 25)

\* **Figuur 8:** Grafische weergave van de vier domeinen van COBIT 5 (ISACA, 2012, p. 36)



\* **Figuur 9:** De 34 beheersingsdoelstellingen op procesniveau van COBIT 5 (Lindgreen & Roos, 2005)



\* **Figuur 10:** Grafische weergave van alle samenhangende elementen van COBIT 5 (ISACA, 2012, p. 35)

# Bijlage 4 Interview

**INTERVIEWVRAGEN ONDERZOEK**

**Interviewer:** Renzo Brinkhof

**Geïnterviewde:** Dhr. Wiebrand Cnossen RA (registeraccountant in de controlepraktijk bij MTH te Hoevelaken)

**Plaats:** Hoevelaken

**Datum:** 19-5-2014

**Even voorstellen**

Mijn naam is Renzo Brinkhof en studeer op dit moment HBO Accountancy aan de Hogeschool Utrecht. Ik doe dit onderzoek als scriptie voor mijn opleiding. Mijn onderzoek gaat over problemen, met betrekking tot IT, bij MKB-bedrijven, die accountants bij de controle van MKB-bedrijven veelal tegenkomen. Het uiteindelijk op te leveren product is een beheermethodiek met algemene IT-beheersmaatregelen, die speciaal is gericht op MKB-bedrijven.

Om de betrouwbaarheid van dit onderzoek te kunnen waarborgen, zullen naast dit interview, ook een aantal andere registeraccountants die werkzaam zijn in de controlepraktijk bij MTH te Hoevelaken, worden geïnterviewd. Tevens zullen er door middel van observaties meerdere controledossiers worden geraadpleegd om informatie te verkrijgen omtrent de bevindingen over de geautomatiseerde omgeving bij verschillende MKB-bedrijven.

**Doel van het onderzoek**

Dit onderzoek heeft als doel om een beheermethodiek te ontwikkelen met algemene IT-beheersmaatregelen, die speciaal is gericht op MKB-bedrijven. Om dit te kunnen realiseren zullen allereerst de meest voorkomende problemen, met betrekking tot IT, bij MKB-bedrijven, in kaart worden gebracht. Deze problemen zullen in dit onderzoek betrekking hebben op informatiebeveiliging.

MKB-bedrijven kunnen aan de hand van deze beheermethodiek, eventueel adequate maatregelen nemen om een correct en fatsoenlijk IT beheer te realiseren dat aansluit met de businessbehoeften (Noë, 2006). Bedrijfsdoelstellingen kunnen op deze manier sneller en gemakkelijker worden gerealiseerd.

Daarentegen kunnen accountants, waaronder de werkzame accountants bij MTH te Hoevelaken, deze zelf ontwikkelde beheermethodiek met algemene IT-beheersmaatregelen voorleggen aan klanten, om nu en in de toekomst minder aanvullende gegevensgerichte controlewerkzaamheden uit te hoeven voeren (Wildschut, 2013). Er kan in dit geval dus gesteund worden op de AO/IB.

Dit onderzoek zal voornamelijk betrekking hebben op het belang van de accountant bij een correct en fatsoenlijk IT beheer binnen een bedrijf.

**Hoofdvraag**

Uit het verlengde van de doelstelling van dit onderzoek, is de volgende hoofdvraag geformuleerd:

*‘’Op welke wijze kunnen organisaties in het MKB, veel voorkomende zwakheden met betrekking tot IT, die tot gevolg hebben dat de accountant tijdens de controle niet kan steunen op de AO/IB, beheersen?’’*

**Interviewvragen**

1. *“Bent u van mening dat MKB-bedrijven voldoende aandacht moeten schenken aan IT Governance?’’*

Over het algemeen wordt er in de praktijk waarin ik werkzaam ben (wettelijke controles), voldoende aandacht besteedt aan ‘’IT Governance’’. Dit wordt met name veroorzaakt doordat veel ondernemingen m.b.t. hun voortbestaan afhankelijk zijn van IT.

Wel is hierbij op te merken dat de ‘’IT Governance’’ vaak bij de financiële afdeling is ondergebracht, waardoor er bij de leiding van de huishouding geen kennis is m.b.t. IT.

1. *“Maken MKB-bedrijven in de praktijk veelvuldig gebruik van bronnen voor IT normen om IT-processen in te richten, te beheersen en te verbeteren?’’*

Gebruikersgemak is vaak het uitgangspunt bij het bepalen van de normen en inrichting m.b.t. IT.

1. *“Welke bronnen voor IT normen zijn in de praktijk onder MKB-bedrijven het meest populair?‘’*

In de praktijk zie je dat er het meeste gebruik wordt gemaakt van standaard normen en inrichtingen vanuit leveranciers (software).Naar mijn inzien is ITIL de meest toepaste beheermethodiek onder MKB-bedrijven. Het gebruik van IT normen binnen het MKB is echter nog wel enorm beperkt.

1. *“Komt het in de praktijk vaak voor dat MKB-bedrijven al meerdere pogingen hebben gedaan om bronnen voor IT normen te implementeren?‘’*

In de praktijk zie je dat veel bedrijven moeite hebben met het implementeren van IT normen. Meestal duurt het wel enkele jaren voordat een IT norm volledig is geïmplementeerd binnen een bedrijf. Ik merk wel dat veel bedrijven gedurende de jaren weer op de oude voet doorgaan.

1. *“Hoe gaan MKB-bedrijven in de praktijk om met IT beheer en in het bijzonder informatiebeveiliging?‘’*

Praktisch, IT beheer is meestal geen integraal onderdeel van de bedrijfsvoering in het MKB.

Ik heb slechts bij enkele klanten dat er een formeel IT beleid is opgesteld. Informatiebeveiliging is meestal beperkt tot de standaard zaken als firewalls, afgeschermde servers etc.

1. *“Maakt u bij de controle van MKB-bedrijven vaak gebruik van IT-auditors en zo ja, merkt u in de praktijk dat er vaak communicatieproblemen zijn tussen de accountants en de IT-auditors doordat ze niet dezelfde taal spreken?‘’*

Binnen de audit maken we denk ik voor 4 op de 10 opdrachten gebruik van een IT auditor.

De communicatieproblemen zijn er zeker, omdat IT auditors meer strategisch gericht zijn op IT gebied.

1. *“Welke versterkingen van de interne controle met betrekking tot IT, komt u bij de controle van MKB-bedrijven veelal tegen?‘’*

* Perioderapportages die standaard ingeregeld zijn;
* Standaard doorlopende nummering van in- en verkooporders, waarbij orders niet verwijderd kunnen worden;
* Standaard interfaces tussen de verschillende systemen.

1. *“Welke verzwakkingen van de interne controle met betrekking tot IT, komt u bij de controle van MKB-bedrijven veelal tegen?‘’*

* Niet goed ingeregelde competenties;
* Niet goed geregelde logische toegangsbeveiliging.

1. *“Welke vervolgstappen onderneemt u over het algemeen, op het moment dat u bij de controle van MKB-bedrijven, problemen met betrekking tot IT, ontdekt, die eventueel van materieel belang kunnen zijn voor de jaarrekening?‘’*

Dan dienen we extra werkzaamheden uit te voeren om de betrouwbaarheid van de informatie die uit het systeem komt, vast te stellen. In het algemeen houdt dit in dat we ‘om het systeem’ heen gaan controleren en meer aansluiting zoeken bij externe documenten en confirmaties.

1. *“Welke IT-beheersmaatregelen, waaronder general en application IT controls, zijn naar uw mening bij de controle van MKB-bedrijven van belang, om te kunnen steunen op de AO/IB?’’*

Puur theoretisch, moet ik zeggen dat de ‘’general controls’’ eerst van belang zijn alvorens de ‘’applications controls’’ beoordeelt worden.

In de praktijk is het van belang dat er controletechnische functiescheiding is ingeregeld in de competenties (‘’application controls’’) en zijn de ‘’general controls’’ van ondergeschikt belang.

# Bijlage 5 Interview

**INTERVIEWVRAGEN ONDERZOEK**

**Interviewer:** Renzo Brinkhof

**Geïnterviewde:** Dhr. Chris Steenbeek RA (registeraccountant in de controlepraktijk bij MTH te Hoevelaken)

**Plaats:** Hoevelaken

**Datum:** 20-5-2014

**Even voorstellen**

Mijn naam is Renzo Brinkhof en studeer op dit moment HBO Accountancy aan de Hogeschool Utrecht. Ik doe dit onderzoek als scriptie voor mijn opleiding. Mijn onderzoek gaat over problemen, met betrekking tot IT, bij MKB-bedrijven, die accountants bij de controle van MKB-bedrijven veelal tegenkomen. Het uiteindelijk op te leveren product is een beheermethodiek met algemene IT-beheersmaatregelen, die speciaal is gericht op MKB-bedrijven.

Om de betrouwbaarheid van dit onderzoek te kunnen waarborgen, zullen naast dit interview, ook een aantal andere registeraccountants die werkzaam zijn in de controlepraktijk bij MTH te Hoevelaken, worden geïnterviewd. Tevens zullen er door middel van observaties meerdere controledossiers worden geraadpleegd om informatie te verkrijgen omtrent de bevindingen over de geautomatiseerde omgeving bij verschillende MKB-bedrijven.

**Doel van het onderzoek**

Dit onderzoek heeft als doel om een beheermethodiek te ontwikkelen met algemene IT-beheersmaatregelen, die speciaal is gericht op MKB-bedrijven. Om dit te kunnen realiseren zullen allereerst de meest voorkomende problemen, met betrekking tot IT, bij MKB-bedrijven, in kaart worden gebracht. Deze problemen zullen in dit onderzoek betrekking hebben op informatiebeveiliging.

MKB-bedrijven kunnen aan de hand van deze beheermethodiek, eventueel adequate maatregelen nemen om een correct en fatsoenlijk IT beheer te realiseren dat aansluit met de businessbehoeften (Noë, 2006). Bedrijfsdoelstellingen kunnen op deze manier sneller en gemakkelijker worden gerealiseerd.

Daarentegen kunnen accountants, waaronder de werkzame accountants bij MTH te Hoevelaken, deze zelf ontwikkelde beheermethodiek met algemene IT-beheersmaatregelen voorleggen aan klanten, om nu en in de toekomst minder aanvullende gegevensgerichte controlewerkzaamheden uit te hoeven voeren (Wildschut, 2013). Er kan in dit geval dus gesteund worden op de AO/IB.

Dit onderzoek zal voornamelijk betrekking hebben op het belang van de accountant bij een correct en fatsoenlijk IT beheer binnen een bedrijf.

**Hoofdvraag**

Uit het verlengde van de doelstelling van dit onderzoek, is de volgende hoofdvraag geformuleerd:

*‘’Op welke wijze kunnen organisaties in het MKB, veel voorkomende zwakheden met betrekking tot IT, die tot gevolg hebben dat de accountant tijdens de controle niet kan steunen op de AO/IB, beheersen?’’*

**Interviewvragen**

1. *“Bent u van mening dat MKB-bedrijven voldoende aandacht moeten schenken aan IT Governance?’’*

Zouden meer aandacht moeten besteden aan IT, maar dit kost geld.

1. *“Maken MKB-bedrijven in de praktijk veelvuldig gebruik van bronnen voor IT normen om IT-processen in te richten, te beheersen en te verbeteren?’’*

IT wordt te vaak als bijzaak gezien en de normen en inrichting worden vaak bepaald op basis van gebruikersgemak.

1. *“Welke bronnen voor IT normen zijn in de praktijk onder MKB-bedrijven het meest populair?‘’*

Standaard normen en inrichtingen vanuit leveranciers (software).

1. *“Komt het in de praktijk vaak voor dat MKB-bedrijven al meerdere pogingen hebben gedaan om bronnen voor IT normen te implementeren?‘’*

Ja, maar dan zie je dat ze vaak toch weer op oude voet doorgaan.

1. *“Hoe gaan MKB-bedrijven in de praktijk om met IT beheer en in het bijzonder informatiebeveiliging?‘’*

Slecht, vaak is dit ondergebracht bij een hoofd administrateur of controller of een IT-er zonder echte opleiding, maar die “wel handig is met computers”.

1. *“Maakt u bij de controle van MKB-bedrijven vaak gebruik van IT-auditors en zo ja, merkt u in de praktijk dat er vaak communicatieproblemen zijn tussen de accountants en de IT-auditors doordat ze niet dezelfde taal spreken?‘’*

Vaak wordt er beperkt gebruik gemaakt van IT auditors, omdat de betrouwbaarheid en de inrichting vaak niet optimaal is. IT-auditors, doen vaak een kunstje wat ze bij alle klanten herhalen. Als ze echt iets moeten uitzoeken voor de accountant ontstaan er vaak communicatieproblemen.

1. *“Welke versterkingen van de interne controle met betrekking tot IT, komt u bij de controle van MKB-bedrijven veelal tegen?‘’*

* Rapportering;
* Inrichting controletechnische functiescheiding in systemen;
* Inrichting betaalbevoegdheden in bankpakket.

1. *“Welke verzwakkingen van de interne controle met betrekking tot IT, komt u bij de controle van MKB-bedrijven veelal tegen?‘’*

* Niet goed ingeregelde competenties;
* Niet goed geregelde logische toegangsbeveiliging.

1. *“Welke vervolgstappen onderneemt u over het algemeen, op het moment dat u bij de controle van MKB-bedrijven, problemen met betrekking tot IT, ontdekt, die eventueel van materieel belang kunnen zijn voor de jaarrekening?‘’*

Dan voeren wij aanvullende gegevensgerichte controlewerkzaamheden uit, welke gericht zijn op originele brondocumenten (bijv. facturen en contracten).

1. *“Welke IT-beheersmaatregelen, waaronder general en application IT controls, zijn naar uw mening bij de controle van MKB-bedrijven van belang, om te kunnen steunen op de AO/IB?’’*

* Inrichting van systemen: wie mag wat doen? (op basis van competentietabellen);
* Goede inrichting van de logische toegangsbeveiliging.

Dit zijn vaak ook de zwaktes van IT systemen, omdat klanten vaak een inrichting hebben welke praktisch moet zijn. Dus medewerkers van klanten kunnen/mogen vaak te veel.