UHASSELT

KNOWLEDGE IN ACTION

Faculteit Bedrijfseconomische Wetenschappen

master in de toegepaste economische wetenschappen: handelsingenieur in de beleidsinformatica

Masterthesis

Het toepassen van ISO-normen op IT managementsprocessen

Charley Medaer

Scriptie ingediend tot het behalen van de graad van master in de toegepaste economische wetenschappen: handelsingenieur in de beleidsinformatica

PROMOTOR :
Prof. dr. Mieke JANS

COPROMOTOR :
dr. Maarten CORTEN

2017
2018

UHASSELT
KNOWLEDGE IN ACTION

www.uhasselt.be
Universiteit Hasselt
Campus Hasselt:
Martelarenlaan 42 | 3500 Hasselt
Campus Diepenbeek:
Agoralaan Gebouw D | 3590 Diepenbeek

UHASSELT

KNOWLEDGE IN ACTION

Faculteit Bedrijfseconomische Wetenschappen

master in de toegepaste economische wetenschappen: handelsingenieur in de beleidsinformatica

Masterthesis

Het toepassen van ISO-normen op IT managementsprocessen

Charley Medaer

Scriptie ingediend tot het behalen van de graad van master in de toegepaste economische wetenschappen: handelsingenieur in de beleidsinformatica

PROMOTOR :
Prof. dr. Mieke JANS

COPROMOTOR :
dr. Maarten CORTEN

Woord vooraf

Met deze masterproef rond ik mijn opleiding in de richting handelsingenieur in de beleidsinformatica aan de Universiteit Hasselt af. In dit onderzoek werd een mapping ontwikkeld waarmee ik hoop dat bedrijven in de toekomst COBIT en ISO 9001 vlotter kunnen implementeren. Daarnaast hoop ik dat VITO met behulp van de mapping een stapje dichter staat bij het behalen van een certificatie van de ISO norm en wens hun nog veel succes met het bereiken van dit doel.

In dit woord vooraf wil ik ook graag een aantal mensen bedanken. Te beginnen met mijn promotoren aan de Universiteit Hasselt, namelijk professor dokter Mieke Jans en dokter Maarten Corten, voor hun begeleiding en de tijd die zij hebben vrijgemaakt voor het leveren van feedback tijdens het schrijven van deze masterproef. Daarnaast wil ik ook de werknemers van VITO, met meneer Klaas Leijssen in het bijzonder, bedanken voor de succesvolle samenwerking en het voorzien van al de nuttige en nodige informatie. Verder zou ik ook professor dokter Koen Vanhoof willen bedanken voor het aanbrengen van het onderwerp.

Tenslotte wil ik ook graag mijn ouders, zussen en vrienden bedanken voor de steun tijdens deze masterproef en gedurende de voorbije vijf jaren aan de universiteit. Zonder hun zou dit avontuur een pak lastiger zijn geweest en zouden mijn lachspieren een pak minder getraind zijn.

Charley Medaer

Samenvatting

Informatietechnologie (IT) speelt vandaag de dag een onmisbare rol in bedrijven. Niet alleen op operationeel vlak maar ook op strategisch vlak zal deze rol alsmaar belangrijker worden. Bedrijven vragen zich af hoe ze de kwaliteit van informatie kunnen bevorderen en tegelijk ook de tevredenheid van klanten of gebruikers hoog kunnen houden. Om aan eisen zoals deze te voldoen bestaan er allerlei frameworks en standaarden die bedrijven ondersteunen bij het realiseren van hun doelstellingen. Het is echter niet ongewoon dat een organisatie meerdere van zulke frameworks in werking heeft. Vele van deze frameworks vertonen echter overlappingen in hun gebruik. Het is daarom dat vaak een combinatie van deze frameworks mogelijk is en zelfs een versterkend effect kan hebben.

Deze masterproef hoopt bedrijven te helpen bij het combineren van specifiek twee van deze frameworks: Het COBIT framework en de ISO 9001 norm uit 2015. Er wordt op zoek gegaan naar een methode waarop de implementatie van deze twee frameworks bevorderd wordt. Specifiek wordt er naar een manier gezocht waarmee het ene framework geïmplementeerd kan worden wanneer het andere reeds in werking is, zodat bedrijven op een eenvoudigere manier de vruchten kunnen plukken van beide frameworks.

Met behulp van een design science methodologie wordt er een weg gebakend naar de ontwikkeling van een artefact dat het combineren van de twee vergemakkelijkt. Dit artefact zal een mapping bedragen tussen het COBIT framework en de ISO 9001 norm. Aan de hand van een zoektocht in de literatuur zal een methode ontworpen worden waarmee de constructie van de mapping volbracht zal worden.

Eens de mapping is opgesteld, zal deze met behulp van een case study gedemonstreerd worden bij het Vlaams Instituut voor Technologisch Onderzoek (VITO). VITO wenst namelijk een certificatie te behalen van de ISO 9001 norm en levert het ideale scenario om de mapping uit te testen. Bij VITO zullen een aantal COBIT processen in kaart gebracht worden. Aan de hand van deze COBIT processen zal met behulp van de ontworpen mapping aangetoond kunnen worden in welke mate aan de eisen van de ISO norm voldaan zijn. Op deze manier zal de toegevoegde waarde van de mapping aangetoond kunnen worden.

De demonstratie van de mapping bij VITO heeft aangetoond dat het gebruik ervan een duidelijke indicatie geeft in welke mate aan de eisen van de ISO 9001 norm voldaan werden. Bijkomend werd aan de verantwoordelijke bij VITO gevraagd of hij de meerwaarde van de mapping inzag en of de mapping daadwerkelijk een beter inzicht gaf in de mate waaraan hun processen aan de eisen van de ISO norm voldaan werd. Deze vraag werd positief bevestigd door te stellen dat het maken van de mapping een waardevolle oefening kan zijn voor bedrijven.

Met behulp van deze mapping wordt er gehoopt dat in de toekomst het combineren van het COBIT framework en de ISO 9001 norm binnen bedrijven vergemakkelijkt wordt en dat bedrijven met behulp hiervan een stap dichter kunnen zetten bij het realiseren van hun bedrijfsdoelstellingen.

Inhoudsopgave

Lijst van figuren

Lijst van tabellen

1. Inleiding

Binnen de huidige competitieve markt is de IT infrastructuur van bedrijven onmisbaar geworden. Informatie dient als een cruciale voedingsbron voor bedrijven en technologie speelt een significante rol gedurende de levensduur van deze informatie. Informatietechnologie wordt alsmaar geavanceerder en belangrijker in bedrijven en in sociale of publieke omgevingen (ISACA, 2012). Bedrijven streven er dan ook naar om de kwaliteit van informatie hoog te houden en hieruit bedrijfswaarde te creëren. Het optimale gebruik van informatietechnologie brengt natuurlijk ook kosten, risico's en regulatie met zich mee. Om met deze factoren rekening te kunnen houden, dient IT-Governance gehanteerd worden.

Selig (2008) definieert IT-Governance als onderdeel van het bedrijfsbestuur dat toezicht, verantwoording en beslissingsrechten voor IT gerelateerde strategieën, middelen en controleactiviteiten formaliseert en verduidelijkt. Het is een verzameling van management, planning en prestatiegerichte praktijken en processen met bijbehorende beslissingsrechten die gezag, controle en prestatie-indicatoren tot stand brengt met betrekking tot investeringen, plannen, budgetten, verbintenissen, diensten, belangrijke wijzigingen, beveiliging, privacy, bedrijfscontinuïteit en de naleving van wetten en het organisatiebeleid (Selig, 2008). IT-governance maakt deel uit van het integrale Corporate Governance dat een stelsel van regels, praktijken en processen beschrijft waardoor een bedrijf bestuurd wordt (Cadbury Report, 1992).

IT-Governance moet niet enkel een initiatief zijn binnen nieuwe bedrijven. Ook bestaande bedrijven hebben er baat bij IT-Governance te implementeren en er een concurrentieel voordeel uit te halen. Bedrijven moeten zich afvragen in welke mate hun IT-Governance gerelateerde processen erin slagen om waarde te creëren. Het is onwaarschijnlijk dat een enkel IT-governance proces zal werken voor alle IT-bedrijfsprocessen. Daarom is het vereist dat er meerdere IT-Governance processen overwogen moeten worden (Moeller, 2013).

Een belangrijk element van IT-Governance binnen een bedrijf is volgens Moeller een sterke en effectieve interne controle. Interne controle is een proces dat door het personeel van het bedrijf beïnvloed wordt en ontworpen is om met een redelijke zekerheid te kunnen zeggen in welke mate doelstellingen behaald kunnen worden in verband met de bedrijfsuitvoering, de financiële verslaggeving en de IT-systemen en processen, en dit alles in overeenstemming met de wet en regelgeving.

Er bestaan verschillende frameworks om deze interne controle processen te beheren. Een IT georiënteerd framework dat begeleiding biedt bij het identificeren van deze processen is het *Control Objectives for Information and related Technology* (COBIT) framework. COBIT biedt begeleiding voor het evalueren en begrijpen van interne controle aspecten binnen het bedrijf met een nadruk op IT (Moeller, 2013). Het helpt een bedrijf met het creëren van optimale waarde vanuit IT door een balans te handhaven tussen het realiseren van baten en het optimaliseren van risiconiveaus en het gebruik van middelen (ISACA, 2012). Kortom is COBIT een framework voor governance en interne controle

dat zich specifiek op IT richt en beschrijft wat er gedaan moet worden om een sterke en effectieve interne controle te bereiken. Het voordeel van COBIT is dat het een breed IT-Governance framework aanbied dat verschillende IT-Governance onderdelen behandelt zoals informatiebeveiliging of risico. Een nadeel is dat COBIT zich enkel richt op 'wat' er gedaan moet worden en niet 'hoe' het gedaan moet worden (Von Solms, 2005).

Met het toenemende belang van IT in ondernemingen, is het beheren van de kwaliteit binnen IT een belangrijk aspect geworden. Het ontwikkelen van competenties die zorgen voor een afstemming op kwalitatieve effectiviteit en efficiëntie is een complex en soms kost-intensieve opgave (Pfeifer & Schmitt, 2010). Daarom ontwikkelden organisaties en industrieën hulpmiddelen die de implementatie van de noodzakelijke kwaliteitsmanagementsystemen vergemakkelijkt. Een kwaliteitsmanagementsysteem kan gedefinieerd worden als een reeks activiteiten om een organisatie te sturen en te besturen om het continue verbeteren van de effectiviteit en de efficiëntie van de prestaties te bevorderen (British Department of Trade & Industry, 2015). De Internationale Organisatie voor Standaardisatie (ISO) is een internationale organisatie die internationale normen voor organisaties vaststelt. Een specifieke norm van ISO die gericht is op het opzetten van kwaliteitsmanagementsystemen is de ISO 9001 norm. Wanneer een bedrijf aan de normen van toepassing voldoet, kan deze organisatie voor bepaalde ISO normen een ISO certificatie behalen (ISO, 2015). Volgens ISO is het invoeren van een kwaliteitsmanagementsysteem een strategische beslissing voor een bedrijf dat kan bijdragen tot het verbeteren van de algemene prestaties van het bedrijf en een goede basis kan bieden voor initiatieven op het gebied van duurzame ontwikkeling.

Verder specifieert de norm eisen voor een organisatie die moet aantonen dat zij in staat is om consistent producten en diensten te leveren die voldoen aan de eisen van de klant en dat de organisatie zich ten doel moet stellen om de klanttevredenheid te verhogen door haar kwaliteitsmanagementsysteem doeltreffend toe te passen, met inbegrip van processen voor het continu verbeteren van het systeem (ISO, 2015). Er moet, volgens de norm, de inputs en outputs samen met de volgorde en interacties tussen de processen bepaald worden. Daarnaast moeten er ook criteria en methoden opgesteld worden om de kwaliteit van de uitvoering en beheersing van de processen te overzien. Ook moeten de middelen en verantwoordelijkheden van de processen toegewezen worden alsook de risico's en kansen die de processen met zich meebrengen. Tenslotte moeten de processen geëvalueerd worden en eventueel de nodige wijzigingen doorgevoerd worden om de beoogde resultaten van de processen te behalen en het kwaliteitsmanagementsysteem te verbeteren. Het voordeel van het toepassen van ISO is dat de standaard gedetailleerd is, een nadeel is dat het een alleenstaande standaard is en niet deel uitmaakt van een groter IT-Governance geheel (Von Solms, 2005).

1.1 Research gap

Naast het apart gebruik van de COBIT en ISO frameworks en standaarden, zoals ISO 17799, 9001 of 15504, bestaat ook de mogelijkheid tot het combineren van het high level COBIT framework en de meer gedetailleerdere ISO normen. Von Solms (2005) geeft aan dat er op het vlak van informatiebeveiliging een zekere synergie bestaat tussen COBIT en ISO. COBIT biedt een breed IT-

Governance framework aan en geeft aan 'wat' er moet gebeuren maar 'hoe' het moet gebeuren, wordt minder concreet besproken. Ook Gehrmann (2012) stelt het gebruik van een combinatie van COBIT en ISO voor om bedrijfsdoelstellingen te bereiken. Volgens deze studie levert de combinatie een duidelijkere en efficiëntere benadering op, in tegenstelling tot het apart gebruik van de frameworks, waarmee meer aspecten benaderd en gecontroleerd kunnen worden die men anders over het hoofd zou zien. Lin et al. (2012) verklaard dat, aangezien IT ondersteuning biedt voor veel bedrijfsprocessen en interne procedures, bedrijven meerdere frameworks in achting moeten nemen om IT vlot te kunnen combineren met deze processen en procedures. Sahibudin et al. (2008) vat samen dat het individueel gebruik van frameworks en standaarden binnen ondernemingen niet uitgebreid genoeg is om als een efficiënt IT management systeem te dienen.

Uit de literatuur blijkt dat er bij het combineren van verschillende frameworks frequent de combinatie tussen COBIT en ISO genomen. In het verleden is er slechts weinig onderzoek verricht naar de combinatie tussen COBIT en de ISO 9001 norm. In een competitieve wereld zoals de dag van vandaag, is de combinatie van een framework dat het managen van IT bevordert en een framework dat klantvriendelijkheid en continue verbetering bevordert echter helemaal niet uit de lucht gegrepen. Uit het literatuuronderzoek blijkt dat enkel Bürgy (2016) de combinatie van deze twee frameworks nagaat en test. In zijn onderzoek giet hij de ISO 9001 norm in een procesmodel om deze norm vervolgens te kunnen mappen met de COBIT processen en uiteindelijk de mate van integratie na te gaan. Dit procesmodel werd opgesteld op basis van processen van een Zwitserse, software gerichte KMO dat gecertificeerd is voor de ISO 9001 norm. Ook zal in dit onderzoek gebruik gemaakt worden van een mapping om de mate van integratie van beide frameworks na te gaan. Het doel is een meer theoretischere mapping te ontwerpen dan de mapping van Bürgy door vanuit de ISO norm zelf te vertrekken in plaats van een procesmodel op te stellen dat bestaat uit processen die gebaseerd zijn op de ISO norm. Op deze manier wordt, in tegenstelling tot het werk van Bürgy, enerzijds de ISO norm zelf letterlijk mee in rekening genomen in haar potentiële relatie met COBIT en anderzijds wordt het opstellen van de mapping niet gelimiteerd door het feit dat er rekening gehouden moet worden met het type of de bedrijfsvoering van een onderneming. Deze mapping dient enerzijds een blik te werpen op de mate waarin beide frameworks overeenkomen en anderzijds zal het als hulpmiddel dienen voor ondernemingen die het brede COBIT framework willen combineren met de gedetailleerde ISO 9001 norm om de kwaliteit van IT binnen hun onderneming te beheren.

1.2 Onderzoeksvragen

Omwille van het beperkte onderzoek dat verricht is naar het combineren van COBIT en de ISO 9001 norm en het belang van zowel IT-Governance als kwaliteitsmanagement in organisaties en afdelingen, luidt de centrale onderzoeksvraag van het onderzoek als volgt:

- *Hoe kan de ISO 9001 norm uit 2015 een aanvulling zijn op COBIT voor het managen van IT-afdelingen?*

Om doorheen dit onderzoek een weg te banen tot een antwoord op deze onderzoeksvraag, werden de volgende deelvragen opgesteld:

- *Wat houden COBIT en de ISO 9001 norm in?*

- *Hoe kan een overzicht verkregen worden van de overeenkomsten tussen COBIT 5 en de ISO 9001 norm?*

Deze twee deelvragen zullen eerst en vooral opgelost worden door middel van de bestaande literatuur en bestaande onderzoeken. Daarnaast zal er, om het antwoord op de tweede deelvraag te bevestigen, in de praktijk op zoek gegaan worden naar het confirmeren van de potentiële meerwaarde van het bekomen overzicht.

1.3 Relevantie van het probleem

Zoals eerder vermeld, is informatietechnologie van cruciaal belang voor bedrijven om enerzijds te kunnen overleven en anderzijds ook om te kunnen groeien en uit te breiden in een competitieve markt (Eloff & Von Solms, 2000). Het optimale gebruik van informatietechnologie brengt natuurlijk ook kosten, risico's en regulatie met zich mee. Om met deze factoren rekening te kunnen houden, dient IT-Governance en een sterke interne controle gehanteerd te worden. Om deze op een efficiënte en effectieve manier in een organisatie uit te kunnen voeren, zouden bedrijven verschillende frameworks (zoals COBIT, ITIL, ISO, COSO) kunnen overwegen. Als gevolg hebben organisaties vaak meerdere frameworks geïmplementeerd om interne controle en IT te beheren (Lin, Cefaratti, & Wallace, 2012). Zo kan het bijvoorbeeld zijn dat twee verschillende departementen, twee verschillende frameworks geïmplementeerd hebben of dat er reeds een framework in werking is wanneer er een tweede geïmplementeerd wordt. Deze frameworks kunnen enerzijds volledig los van elkaar staan maar anderzijds ook overlappingen tonen. Wanneer een organisatie meerdere standaarden of frameworks wil toepassen, moet de vraag gesteld worden of deze frameworks overlappingen tonen en indien ja, moet er nagegaan worden in welke mate deze frameworks en standaarden met elkaar geïntegreerd kunnen worden en hoe deze integratie uitgevoerd zal worden. Wanneer de integratie van de frameworks niet mogelijk is, omdat de frameworks elkaar bijvoorbeeld kunnen tegenspreken of andere doelen voor ogen hebben, is het moeilijk om een consistente combinatie te creëren (Von Solms, 2005). Ook wanneer frameworks niet direct met elkaar in contact komen, omdat ze bijvoorbeeld in verschillende departementen toegepast worden, is het nuttig om een vergelijking op te stellen omdat concepten verschillend gedefinieerd kunnen zijn en om de communicatie te bevorderen.

Scenario's

Net zoals Sheikhpour (2012) en von Solms (2005) voorstellen in hun onderzoeken naar mappings, worden hier kort enkele scenario's beschreven waarin het gebruik van de mapping tussen COBIT en ISO 9001 die in dit onderzoek ontworpen zal worden van pas kan komen.

Scenario 1

Stel dat een bedrijf in zijn geheel COBIT heeft geïmplementeerd als IT Governance framework. Een bepaald departement van dit bedrijf wil haar kwaliteitsmanagement bevorderen door ISO 9001 te implementeren. Met behulp van de mapping kan het departement makkelijk bepalen welke

onderdelen van de ISO norm reeds zijn geïmplementeerd omwille van het gebruik van COBIT en welke nog bijkomend vereist zijn, ook om een ISO certificatie te kunnen behalen.

Scenario 2

Stel dat een bepaald departement van een bedrijf ISO 9001 heeft geïmplementeerd om haar kwaliteit te managen. Er wordt plots beslist dat het hele bedrijf COBIT zal implementeren als een high level IT Governance framework en verwacht dat het departement in kwestie dit ook zal doen. Met behulp van de mapping kan het departement onmiddellijk identificeren welke COBIT processen reeds onrechtstreeks onderdeel uitmaken van de bedrijfsvoering omdat het de ISO norm reeds in werking heeft en hoeft het daartoe geen extra kosten aan te gaan.

Scenario 3

Stel dat opnieuw een departement ISO 9001 heeft geïmplementeerd. Een IT audit zal worden uitgevoerd door het audit departement of een extern auditbureau en de auditors maken gebruik van COBIT als hun IT audit framework. Met behulp van de mapping kan de communicatie tussen het auditbureau en het departement bevorderd worden en kan er makkelijker geïdentificeerd worden aan welke eisen reeds voldaan zijn.

Scenario 4

Stel dat bedrijf A een IT Governance framework geïmplementeerd heeft dat op gebaseerd is op COBIT en plant bedrijf B over te nemen. Bedrijf B heeft een kwaliteitsmanagementsysteem geïmplementeerd in overeenstemming met de ISO 9001 norm. Gebruik makend van de mapping kunnen de frameworks van beide bedrijven op elkaar afgestemd worden en de overname vergemakkelijkt worden.

1.4 Onderzoeksverloop

Bepaalde concepten zoals IT-Governance, COBIT en ISO die cruciaal zijn voor deze studie zullen grondig toegelicht worden in de literatuurstudie. Ook de link tussen deze begrippen zal uitgediept worden. Verder zullen in dit onderzoek wetenschappelijke studies gebruikt worden, alsook gedocumenteerde, in de praktijk uitgevoerde toepassingen binnen de relevante domeinen. Voor het zoeken naar wetenschappelijke bronnen zal er gebruik gemaakt worden van Google Scholar en de UHasselt bibliotheek zowel digitaal, dat meerdere databanken omvat, als de bibliotheek op de campus. De voorkeur bij digitale bronnen zal gegeven worden aan academische publicaties, binnen het IT-Governance domein, waarvan de volledige tekst online beschikbaar is. Aan de hand van de bovenstaande concepten zullen de trefwoorden bepaald worden om naar artikels te zoeken. Trefwoorden die in verschillende combinaties nuttige resultaten kunnen opleveren, zijn onder andere: IT-Goverance, COBIT, ITIL, ISO, ISO:9001, mapping, combination COBIT & ISO, IT-managementproces, application IT-Governance, application IT-managementproces, ISO certified en COSO.

Na de literatuurstudie zal in het methodologie gedeelte in detail uitgelegd worden met welke methodologie de mapping opgesteld zal worden, alsook hoe deze geëvalueerd zal worden. Daarna zal de mapping tussen het COBIT framework en de ISO 9001 norm opgesteld worden. Hiervoor zal er eerst een overzicht gegeven worden van bestaande mappings tussen COBIT en ISO normen. Op basis hiervan zal het ontwerp gekozen worden waarmee de mapping zelf opgesteld zal worden. Eens de mapping is opgesteld, zal deze gedemonstreerd worden. Dit zal gebeuren in samenwerking met de IT afdeling van een bedrijf dat zelf COBIT processen heeft geïmplementeerd en ook een ISO certificatie wil behalen. Dit geeft de kans om aan te tonen in welke mate de opgestelde mapping erin slaagt om de afdeling te helpen identificeren aan welke vereisten uit de ISO norm het reeds voldoet. Op basis van deze demonstratie zal een conclusie gevormd kunnen worden over het functioneren van de mapping en of er al dan niet voordeel uit gehaald kan worden.

2. Literatuurstudie

In deze literatuurstudie zullen een aantal concepten verklaard worden waarop de case study zich op zal baseren. Als eerste zal IT-Governance onder de loep genomen worden, gevolgd door een toelichting van kwaliteitsmanagement en tot slot zal de combinatie van de twee toegelicht worden.

2.1 IT-Governance

Binnen de huidige competitieve markt is de IT infrastructuur van bedrijven onmisbaar geworden. Informatie dient als een cruciale voedingsbron voor bedrijven en technologie speelt een significante rol gedurende de levensduur van deze informatie. Informatietechnologie wordt alsmaar meer gevorderd en belangrijker in bedrijven en in sociale of publieke omgevingen (ISACA, 2012). Bedrijven streven er dan ook naar om de kwaliteit van informatie hoog te houden en hieruit bedrijfswaarde te creëren. Het optimale gebruik van informatietechnologie brengt natuurlijk ook kosten, risico's en regulatie met zich mee. Om met al deze factoren rekening te kunnen houden, dient er IT-*Governance* gehanteerd worden.

Selig (2008) definieert IT-Governance als onderdeel van het bedrijfsbestuur dat toezicht, verantwoording en beslissingsrechten voor IT gerelateerde strategieën, middelen en controleactiviteiten formaliseert en verduidelijkt. Het is een verzameling van management, planning en prestatiegerichte praktijken en processen met bijbehorende beslissingsrechten die autoriteit, controle en prestatie-indicatoren tot stand brengt met betrekking tot investeringen, plannen, budgetten, verbintenissen, diensten, belangrijke wijzigingen, beveiliging, privacy, bedrijfscontinuïteit en de naleving van wetten en het organisatiebeleid (Selig, 2008). IT-governance maakt deel uit van het integrale Corporate Governance dat een stelsel van regels, praktijken en processen beschrijft waardoor een bedrijf bestuurd wordt (Cadbury Report, 1992).

IT-Governance moet niet enkel een initiatief zijn binnen nieuwe bedrijven. Ook bestaande bedrijven hebben er baat bij IT-Governance te implementeren en er een concurrentieel voordeel uit te halen. Het mag niet aanzien worden als een project dat een begin en eindpunt heeft maar eerder als een belangrijk aspect dat een invloed heeft over het hele bedrijf. Bedrijven moeten zich afvragen in welke mate hun IT-Governance gerelateerde processen erin slagen om waarde te creëren. Het is onwaarschijnlijk dat een enkel IT-governance proces zal werken voor alle IT-bedrijfsprocessen. Daarom is het vereist dat er meerdere IT-Governance processen overwogen moeten worden (Moeller, 2013).

Een belangrijk element van IT-Governance binnen een bedrijf is volgens Moeller (2013) een sterke en effectieve interne controle. Interne controle is een proces dat door het personeel van het bedrijf beïnvloed wordt en ontworpen is om met een redelijke zekerheid te kunnen zeggen in welke mate doelstellingen behaald kunnen worden in verband met de bedrijfsuitvoering, de financiële verslaggeving en de IT-systemen en processen. Dit alles in overeenstemming met de wet en regelgeving (COSO, 2013).

Er bestaan verschillende frameworks om deze interne controle processen te beheren. Een frequent gebruikt referentiekader voor interne controle is het COSO framework. Hier wordt in de volgende

sectie verder op ingegaan. Een meer IT georiënteerd framework dat begeleiding biedt bij het identificeren van interne controle processen is het *Control Objectives for Information and related Technology* (COBIT) framework. COBIT biedt begeleiding voor het evalueren en begrijpen van interne controle aspecten en zal verder bestudeerd worden later in deze literatuurstudie.

2.1.1 COSO

Het *Committee of Sponsoring Organizations* (COSO) is een comité dat in 2002 naar aanleiding van enkele boekhoudkundige en fraude schandalen is opgericht met als missie de prestaties en governance van organisaties verbeteren. Dit doen ze door richtlijnen te geven inzake *enterprise risk management* (ERM) en interne controle processen (COSO, 2014). Volgens COSO (2014) zijn goed risicomanagement en interne controle noodzakelijk om het lange termijn succes van organisaties te kunnen garanderen. In het kader van dit onderzoek, zal het interne controle framework van COSO verder onder de loep genomen worden om hier een duidelijk beeld over te scheppen.

Het interne controle framework van COSO werd origineel in 1992 vrijgegeven en is sindsdien een leidinggevend framework voor het ontwikkelen, implementeren en uitoefenen van interne controle en om de effecten van interne controle binnen een organisatie te beoordelen (COSO,2013). Concreet is interne controle een proces van taken en activiteiten dat met een bepaalde zekerheid moet kunnen zeggen in welke mate doelstellingen inzake de bedrijfsactiviteit, verslaggeving en de naleving van regelgeving behaald kunnen worden. Dit proces is van toepassing op alle niveaus van een organisatie en wordt beïnvloed door de beslissingen die genomen worden door mensen op elk van deze niveaus.

Sinds de eerste uitgave van het interne controle framework is de bedrijfswereld enorm veranderd. Om vandaag de dag op een efficiënte manier aan interne controle te doen, moeten organisaties volgens COSO (2013) vijf componenten mee in rekening genomen worden. Deze vijf componenten zijn de volgende:

- Controleomgeving: De controleomgeving is een reeks van standaarden, processen en constructies die als basis dienen voor het uitvoeren van interne controle doorheen de organisatie. De controleomgeving omvat de waarden, de cultuur en regels binnen de organisatie en wordt door de directors en senior management vastgelegd afhankelijk van het belang dat interne controle gaat hebben binnen de organisatie. Het management trekt deze waarden dan door tot de verschillende niveaus binnen de organisatie.
- Risicobeoordeling: De risicobeoordeling is een dynamisch en iteratief proces dat er op toeziet dat risico's met betrekking tot het behalen van bedrijfsdoelstellingen geïdentificeerd en ingeschat worden. Deze risico's worden als relatief beschouwd tegenover vooropgestelde risicotoleranties. De risicobeoordeling vormt dus de basis om de manier te bepalen hoe er met geïdentificeerde risico's omgegaan wordt.
- Controleactiviteiten: Controleactiviteiten zijn acties en procedures die opgesteld aan de hand van het gevoerde beleid om er voor te zorgen dat richtlijnen die er toe dienen risico's te verminderen ook daadwerkelijk toegepast worden. Deze kunnen zowel preventief als opsporend zijn en zijn toepasbaar op zowel geautomatiseerde als manuele activiteiten.

Segregation of duties is een voorbeeld van een controleactiviteit waarbij een bepaalde verantwoordelijkheid over meer dan één persoon verdeeld wordt.

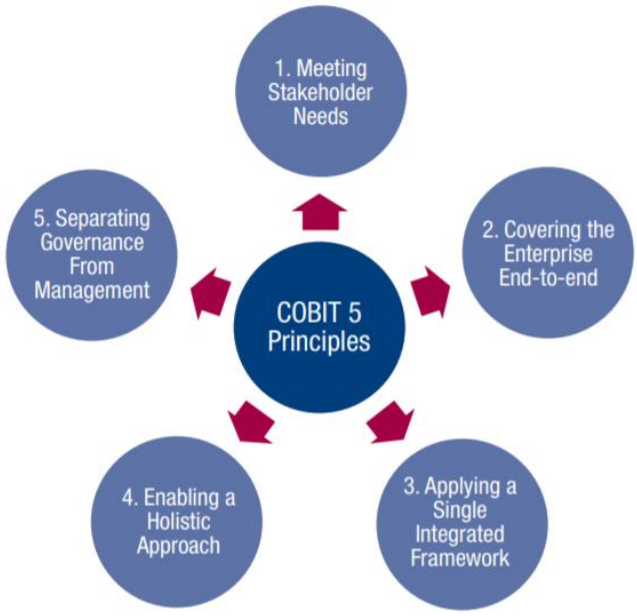
- Informatie en communicatie: Dit zijn essentiële bestanddelen om interne controle juist te kunnen uitvoeren. Het management verkrijgt en gebruikt informatie uit zowel interne als externe bronnen om de andere componenten van interne controle te ondersteunen. Voor een optimale toepassing van de controleactiviteiten is het vereist dat deze informatie relevant, tijdig, actueel, accuraat en toegankelijk is. Communicatie is het leveren, delen en verkrijgen van de nodige informatie zowel opwaarts als neerwaarts doorheen de organisatie.
- Monitoring: Dit zijn evaluaties die er op toezien dat elk van de andere componenten van interne controle aanwezig zijn en correct en efficiënt uitgevoerd worden. Dit kan gaan van continue evaluaties die in de processen ingebouwd zijn, tot periodieke evaluaties die variëren in opzet afhankelijk van de beoordeling van de risico's, de effectiviteit van de evaluaties of andere door management overwogen criteria. De bevindingen die voortkomen uit deze evaluaties moeten vergeleken worden met bepaalde criteria die intern of extern aan de organisatie opgelegd worden om vervolgens aan belanghebbende gecommuniceerd te worden.

COSO (2013) legt een directe relatie tussen de doelstellingen die een organisatie wenst te behalen, de vijf componenten, die vertegenwoordigen wat gedaan moet worden om de doelstellingen te behalen, en de organisatiestructuur. Deze relatie kan worden weergegeven in de vorm van een kubus zoals in figuur 1. De kolommen geven de doelstellingen weer, de rijen geven de componenten weer en de derde dimensie geeft de organisatiestructuur weer. Het COSO framework maakt gebruik van 17 principes (bijlage 1) verdeeld over de drie dimensies om de fundamentele concepten van elke component duidelijk te maken. Door het toepassen van deze 17 principes kan een effectieve interne controle bereikt worden. Senior managers komen vandaag de dag regelmatig vereisten tegen die het COSO interne controle framework behandelt zoals bijvoorbeeld bij interne of externe audits. Dit framework levert een basis voor het begrijpen van verschillende IT-Governance problemen. Het is daarom belangrijk voor senior managers om een algemene kennis te hebben van het COSO interne controle framework om bijgevolg een algemene kennis te hebben van de interne controle van hun organisatie en de relevante IT-Governance onderwerpen (Moeller, 2013).

Figuur 1: De COSO relaties in kubus vorm

2.1.2 COBIT

Zoals eerder vermeld bestaan er verschillende frameworks om deze interne controle processen te beheren. Een IT georiënteerd framework dat begeleiding biedt bij het identificeren van deze processen is het *Control Objectives for Information and related Technology* (COBIT) framework. COBIT biedt begeleiding voor het evalueren en begrijpen van interne controle aspecten binnen het bedrijf met een nadruk op IT (Moeller, 2013). Het helpt een bedrijf met het creëren van optimale



Figuur 2: De COBIT 5 principes

waarde vanuit IT door een balans te handhaven tussen het realiseren van baten en het optimaliseren van risiconiveaus en het gebruik van middelen (ISACA, 2012). Kortom, COBIT is een framework voor governance en interne controle dat zich specifiek op IT richt en beschrijft wat er gedaan moet worden om een sterke en effectieve interne controle te bereiken. Binnen de omvang van dit onderzoek zal er dieper ingegaan worden op het COBIT 5 procesmodel. COBIT 5 is gebaseerd op vijf principes voor governance en het managen van IT (figuur 2). De combinatie van deze vijf principes stelt volgens ISACA (2012) de organisatie in staat om een effectief governance en management framework op te bouwen dat de IT investeringen en de baten voor stakeholders optimaliseert.

Principe 1: *Meeting stakholder needs*. Een organisatie heeft als doel waarde te creëren voor haar belanghebbenden door de balans te vinden tussen het realiseren van opbrengsten en het optimaliseren van risico en het gebruik van middelen. COBIT 5 geeft een overzicht van processen die het creëren van deze waarde ondersteunen door middel van IT.

Principe 2: *Covering the enterprise end-to-end*. COBIT 5 integreert het beheer van IT met het algemeen bestuur van een organisatie. Dit door enerzijds met alle functies en processen binnen het bedrijf rekening te houden en niet enkel met de IT gerelateerde processen en anderzijds door alles wat IT-Governance gerelateerd is als end-to-end te beschouwen, dus voor alles en iedereen die relevant is voor het beheer van IT, zowel intern als extern.

Principe 3: *Applying a single integrated framework.* Omdat er verschillende IT gerelateerde standaarden en frameworks bestaan, mikt COBIT 5 erop om op high level overeen te komen met andere frameworks om zo te kunnen dienen als een overkoepelend framework voor IT-Governance.

Principe 4: *Enabling a holistic approach*. Om effectief en efficiënt aan IT-Governance te doen moeten al de verschillende componenten die relevant zijn mee in rekening genomen worden. COBIT 5 definieert een aantal manieren om de implementatie van IT-Governance te ondersteunen. Deze manieren worden omschreven als alles dat kan bijdragen tot het behalen van de bedrijfsdoelstellingen. Er wordt hierbij een onderscheid gemaakt tussen zeven categorieën:

1. Principes, besturen en frameworks
2. Processen
3. Organisatie structuren
4. Cultuur, ethiek en gedrag
5. Informatie
6. Diensten, infrastructuur en toepassingen
7. Mensen, vaardigheden en competenties

Principe 5: *Separating governance from management*. Government en management omvatten beide verschillende types van activiteiten, eisen een verschillende organisatiestructuur en hebben verschillende doeleneinden. COBIT 5 maakt een duidelijk onderscheid tussen deze twee domeinen:

- Governance staat ten eerste in voor de evaluatie van de stakeholders hun behoeften om deze te kunnen transformeren naar bedrijfsdoelstellingen. Ten tweede bepaalt het de richting waar de organisatie naartoe wil door middel van besluitvorming en door prioriteiten te stellen. Tenslotte zorgt het voor een overzicht van de geleverde prestaties en de naleving van de overeengekomen richting en doelstellingen.
- Management plant, bouwt, controleert en voert (PDCA) de activiteiten uit om bedrijfsdoelstellingen te bereiken die in overeenstemming zijn met de visie van de organisatie.

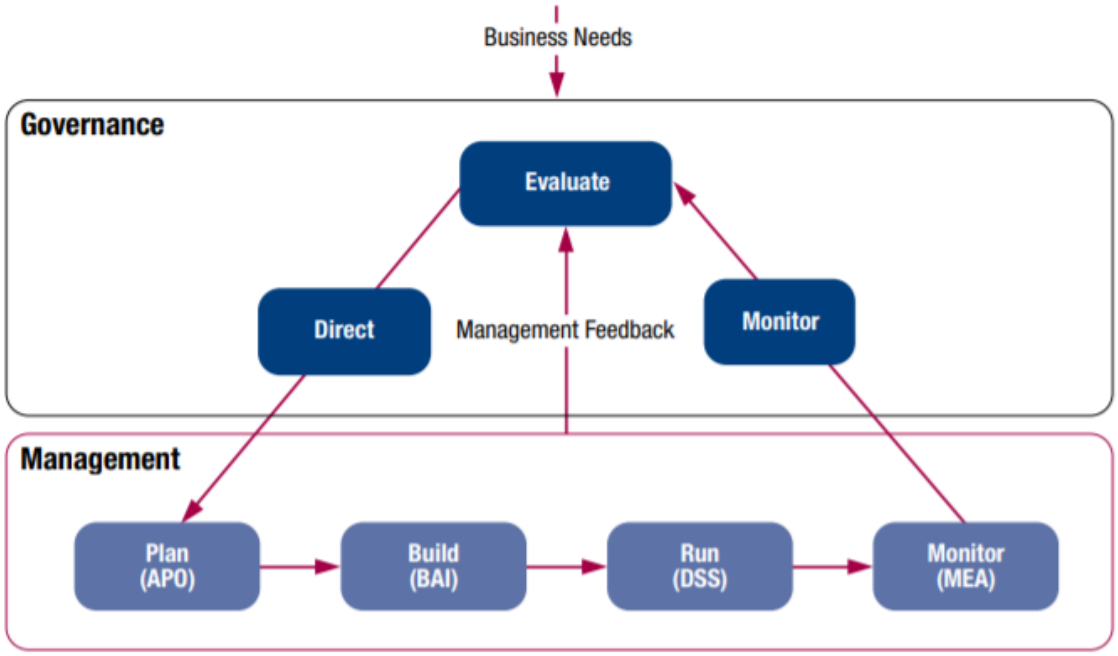
COBIT 5 stelt een aantal belangrijke gebieden voor die governance en managementprocessen moeten behandelen. Deze gebieden worden weergegeven in figuur 3. COBIT 5 bevat een proces referentie model dat 37 governance en managementprocessen in detail omschrijft. Governance bevat vijf processen waarin *evaluate, direct en monitor* (EDM) toepassingen worden gedefinieerd. Management heeft voor elk van haar vier gebieden ook een aantal processen gedefinieerd die toepasbaar zijn binnen dat domein. Deze vier gebieden zijn:

- Align, Plan and Organise (APO)
- Build, Acquire and Implement (BAI)
- Deliver, Service and Support (DSS)
- Monitor, Evaluate and Assess (MEA)

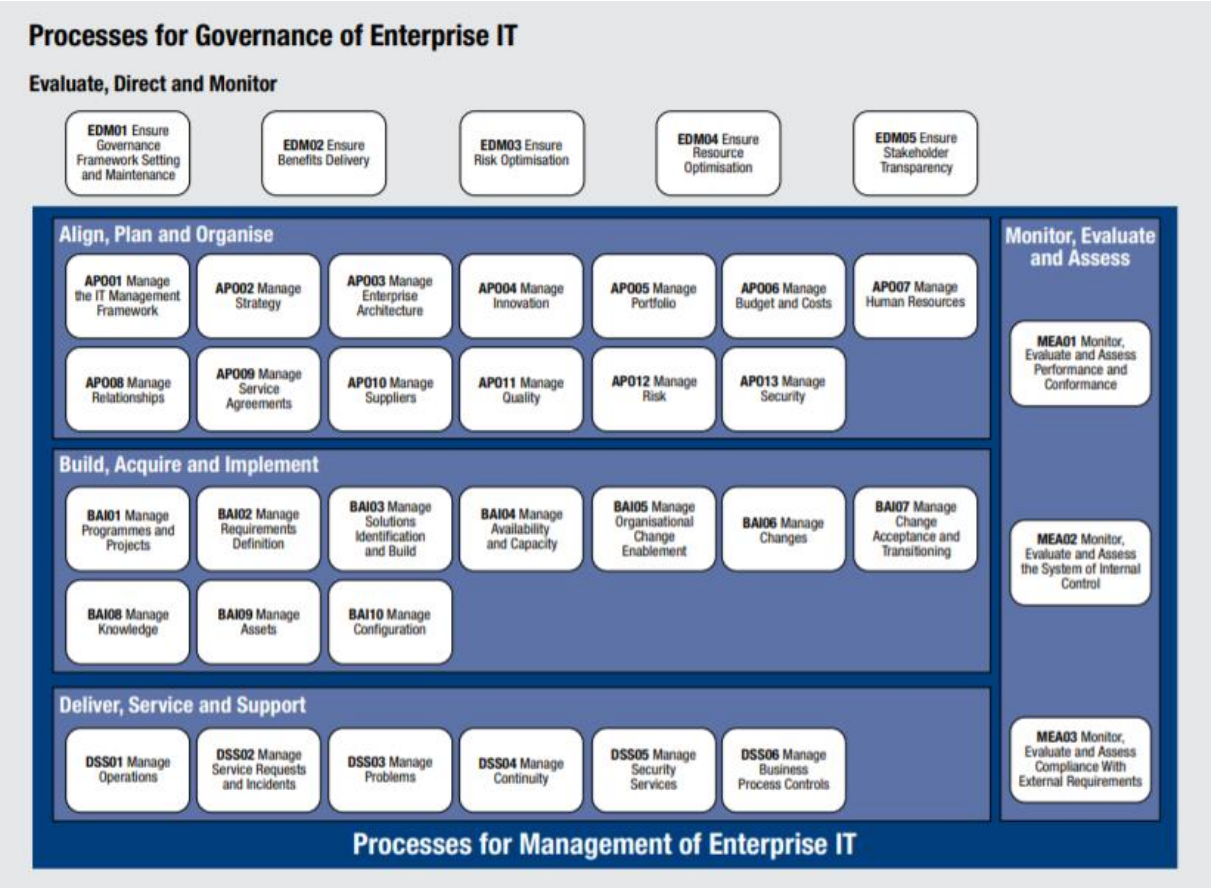
De processen per gebied worden in figuur 4 weergegeven. Uit beide figuren kan afgeleid worden dat de EDM processen binnen governance eerder strategisch van aard zijn en dienen om de managementprocessen aan te sturen, terwijl de processen binnen het management gebied eerder voor het operationeel managen van IT gebruikt worden (Bürgy, 2016). De implementatie van de voorgestelde processen leidt tot een geheel en begrijpbaar procesmodel, hoewel dit niet het enige procesmodel is dat kan geïmplementeerd worden. Ieder bedrijf moet voor zichzelf bepalen welke processen het mee in rekening neemt, afhankelijk van de situatie waarin het zich bevindt (ISACA, 2012).

In COBIT 5: *Enabling Processes* (ISACA, 2012b) worden de 37 processen verder in detail beschreven. Per proces wordt aangegeven binnen welk van de vijf gebieden het hoort, gevolgd door een beschrijving van het proces en wat het proces beoogt te bereiken. Daarnaast omvat het ook een referentie naar de IT doelstellingen en de proces gerelateerde doelstellingen die het proces ondersteunen. Tenslotte worden ook maatstaven meegegeven hoe deze doelstellingen bereikt kunnen worden. Meer informatie over deze IT en proces gerelateerde doelstellingen volgt in sectie 1.2.1.

Voor elk COBIT proces worden er enkele governance of management praktijken gegeven die meer begeleiding geven bij het uitvoeren van het proces. Voor elk van deze praktijken wordt er vervolgens een RACI-matrix (Responsible, Accountable, Supportive, Consulted) gegeven. Dit geeft een indicatie hoe de verantwoordelijkheid van het proces binnen de posities van de onderneming verdeeld kan worden. Tot slot wordt er per proces praktijk een gedetailleerde beschrijving gegeven die bestaat uit een samenvatting van de praktijk, de benodigde inputs, de verwachte outputs met een indicatie vanwaar deze vandaan kunnen komen of naartoe moeten gaan. Als laatste worden de activiteiten weergegeven die per praktijk uitgevoerd dienen te worden (ISACA, 2012b). Een voorbeeld van wat in deze alinea beschreven werd kan teruggevonden worden in bijlage 2. Concreet presenteert COBIT een reeks van processen en maakt per proces duidelijk aan welke eisen er voldaan moet worden, uit welke activiteiten het proces moet bestaan en wat de verwachte inputs en outputs zijn.



Figuur 3: COBIT 5 Governance en Management gebieden



Figuur 4: COBIT 5 proces referentie model

De COBIT mapping

Nu er een beeld geschetst is van de mogelijkheden die COBIT biedt met betrekking tot processen, is de volgende stap het identificeren van de processen die van toepassing kunnen zijn binnen een specifieke organisatie. Hiervoor heeft COBIT een mapping voorzien dat de noden van de stakeholders omvormt tot verschillende bedrijfsdoelstellingen, die op hun beurt vertaald worden in IT gerelateerde doelstellingen, die vervolgens leiden tot de identificatie van de verschillende COBIT processen.

Elk bedrijf heeft als doel de waarde die zij creëren voor hun stakeholders te maximaliseren. De vorm van deze waarde kan verschillen voor verschillende stakeholders. Het is aan het bestuur van een organisatie om alle stakeholders mee in rekening te nemen wanneer winst wordt gerealiseerd, het risico wordt geoptimaliseerd of het gebruik van bronnen wordt geoptimaliseerd (ISACA, 2012). Eisen van stakeholders dienen als input voor het vormen van een bedrijfsstrategie. De COBIT mapping voorziet als eerste een manier om deze eisen te vertalen in bedrijfsdoelstellingen. Deze door COBIT gedefinieerde bedrijfsdoelstellingen worden samengevat in een lijst van 17 doelstellingen (Bijlage 3) die frequent door bedrijven gedefinieerd en vooropgesteld worden (ISACA, 2012).

Eens de bedrijfsdoelstellingen geïdentificeerd zijn, kunnen deze vervolgens gemapt worden met 17 IT gerelateerde doelstellingen (Bijlage 4). Het realiseren van een bedrijfsdoelstelling moet, binnen de COBIT context, de output van deze IT gerelateerde doelstellingen mee in rekening nemen. Voor elke bedrijfsdoelstelling voorziet COBIT een aantal IT gerelateerde doelstellingen die al dan niet van primair of secundair belang zijn voor deze bedrijfsdoelstelling. Eens de IT gerelateerde doelstellingen

geïdentificeerd zijn, kunnen deze gemapt worden met de 37 COBIT processen (bijlage 5), onderverdeeld in de eerder besproken vijf gebieden. Opnieuw wordt er per IT gerelateerd doelstelling een onderscheid gemaakt welke processen van primair en secundair belang zijn (ISACA, 2012).

De COBIT mapping staat dus toe om op een simpele manier de behoeften van de stakeholders te vertalen naar IT processen. ISACA (2012) maant toch voorzichtig om te springen met de mapping en om het eerder als richtlijn te gebruiken dan als handleiding. Ten eerste heeft elk bedrijf andere prioriteiten voor zijn doelstellingen en deze prioriteiten kunnen veranderen. De verschillende mappings houden ook geen rekening met de grootte van het bedrijf of de industrie waar het zich in bevindt. Het geeft een soort algemene indruk hoe de verschillende doelstellingen op verschillende niveaus binnen een bedrijf met elkaar in verband staan. Een derde opmerking is dat bij mappings elke keer met slechts twee factoren rekening gehouden wordt. In de werkelijkheid kunnen dit er meerdere zijn. Idealiter zou elk bedrijf zijn eigen, bedrijfsspecifieke mapping moeten opstellen en deze vergelijken en bijschaven aan de hand van de COBIT mapping.

2.2 Kwaliteitsmanagement

Kwaliteitsmanagement is een tak van het management dat een zo hoog mogelijke kwaliteit en productiviteit van producten, processen of diensten binnen organisaties nastreeft. Hierbij wordt er voornamelijk gefocust op het continu verbeteren van de desbetreffende producten of processen en om op deze manier de klanttevredenheid te vergroten (Chen et al., 2016). Een kwaliteitsmanagementsysteem omvat de activiteiten waarmee een organisatie haar doelstellingen bepaalt en beslist over de processen en bronnen die nodig zijn om de gewenste resultaten te bereiken. Hierbij wordt het gebruik van bronnen geoptimaliseerd en geplande of ongeplande effecten van beslissingen op korte en lange termijn mee in rekening genomen (ISO,2015). Het toepassen van kwaliteitsmanagement is essentieel om kwaliteitsvolle producten en diensten te leveren, wat op zijn beurt leidt tot een grotere klanttevredenheid, wat vervolgens dan weer tot een grotere klantloyaliteit en marktaandeel zal leiden (ISO,2015).

Er bestaan verschillende standaarden en frameworks die helpen bij het implementeren en toepassen van kwaliteitsmanagement. Hammar (2015) vat enkele van deze standaarden en frameworks samen en in de volgende tabellen wordt hier een overzicht van weergegeven. Een eerste set van standaarden is de ISO 9000 familie. In tabel 1 wordt hier een overzicht van geschetst.

ISO 9000	Het eerste document binnen de ISO 9000 familie met als doelen het definiëren van termen die doorheen de standaard gebruikt worden en het beschrijven van kwaliteitsmanagement principes.
ISO 9001	Deze standaard bevat een reeks vereisten voor het ontwerpen van een kwaliteitsmanagementsysteem. Binnen deze standaard staat vooral klanttevredenheid centraal.

ISO 9004	Deze standaard bevat begeleiding voor een organisatie dat haar kwaliteitsmanagementsysteem succesvoller wil maken. In tegenstelling tot de ISO 9001 standaard kan men voor deze standaard geen certificatie ontvangen.

TABEL 1: KWALITEITSMANAGEMENT STANDAARDEN UIT DE ISO 9000 FAMILIE

Naast de ISO 9000 standaard worden in tabel 2 nog drie andere standaarden opgesomd die specifiek voor een bepaalde industrie zijn opgesteld. Deze leveren de vereisten die gebruikt kunnen worden bij het opstellen van een kwaliteitsmanagementsysteem binnen die industrie.

AS9100	Deze standaard is gebaseerd op de ISO 9001 standaard maar richt zich specifiek op de lucht en ruimtevaart industrie.
ISO 13485	Deze door ISO gepubliceerde standaard richt zich vooral op kwaliteitsmanagementsystemen binnen de medische sector.
ISO/TS 16949	Deze standaard bevat vereisten voor de auto-industrie waaraan voldaan moet worden bovenop de ISO 9001 standaard.

TABEL 2: KWALITEITSMANAGEMENT STANDAARDEN VOOR SPECIFIEKE INDUSTRIEËN

In tabel 3 worden ten slotte nog enkele frameworks opgesomd die kwaliteitsmanagement ondersteunen. Deze dienen slechts als hulpmiddel voor kwaliteitsmanagement en niet als vereisten waarrond een kwaliteitsmanagementsysteem opgesteld kan worden.

Lean	Het hoofddoel van dit framework is het maximaliseren van waarde voor de klant met het minimaliseren van verspilling of waste in het productieproces. Het idee is dat door het elimineren van waste het proces verbeterd wordt met als gevolg dat er ook efficiënter te werk gegaan wordt.
Six Sigma	Dit zijn een aantal technieken die gebruikt kunnen worden om een proces te verbeteren door te focussen op statistische cijfers die uit het proces voortvloeien. Deze technieken kunnen het kwaliteitsmanagementsysteem ondersteunen in het verbeteren van processen.
TQM	Total Quality Management zijn best practices die gebruikt kunnen worden om een proces te verbeteren. De nadruk binnen deze practices

	ligt op efficiëntie, probleem oplossend denken en het standaardiseren van processen. TQM kan gebruikt worden als begeleiding bij kwaliteitsmanagement maar levert geen framework voor een kwaliteitsmanagementsysteem.

TABEL 3: KWALITEITSMANAGEMENT ONDERSTEUNENDE FRAMEWORKS

Binnen dit onderzoek zal er specifiek gefocust worden op de ISO 9001 standaard en meer bepaald op de link tussen deze standaard en het COBIT framework en de mate waarin het gebruik van beide een positief effect kan hebben op een organisatie. In de komende secties wordt hier verder op ingegaan.

2.2.1 ISO

De Internationale Organisatie voor Standaardisatie (ISO) is een internationale organisatie die normen voor organisaties vaststelt. Met behulp van experts worden marktrelevante internationale normen opgesteld die als doel hebben innovatie te ondersteunen en oplossingen te bieden voor wereldwijde uitdagingen. Binnen het kader van kwaliteitsmanagement, mikt deze studie zich op de ISO 9001-norm en meer bepaald op de versie die in 2015 uitgegeven werd. Deze norm specifieert eisen voor een organisatie die moet kunnen aantonen dat zij in staat is om consistent producten en diensten te leveren die voldoen aan de eisen van de klant en dat de organisatie zich ten doelen moet stellen om de klanttevredenheid te verhogen door haar kwaliteitsmanagementsysteem doeltreffend toe te passen, met inbegrip van processen voor het continu verbeteren van het systeem (ISO, 2015). Verder is de norm gebaseerd op zeven principes van kwaliteitsmanagement die beschreven worden in ISO 9000. Deze principes achten de prestaties van de organisatie te verbeteren indien ze correct toegepast worden. Deze zeven principes zijn de volgende:

- Klantgerichtheid
- Leiderschap
- Betrokkenheid (engagement) van medewerkers
- Procesbenadering
- Continue verbetering
- Op bewijs gebaseerde besluitvorming
- Relatiemanagement

Het ontwikkelen en onderhouden van een kwaliteitsmanagementsysteem wordt door het toepassen van deze principes vergemakkelijkt. Daarom krijgen de ISO 9000 familie en de ISO 9001 standaard in het algemeen de voorkeur in vergelijking met andere standaarden (Bürgy, 2016).

Binnen het opzet van dit onderzoek zal het principe rond procesbenadering verder onder de loep genomen worden. ISO 9001 verkiest een procesbenadering bij het ontwikkelen, implementeren en verbeteren van de doeltreffendheid van een kwaliteitsmanagementsysteem, om de

klanttevredenheid te verhogen door te voldoen aan de eisen van klanten. Daarnaast draagt het begrijpen en het managen van onderling samenhangende processen als een systeem bij tot de doeltreffendheid en doelmatigheid van de organisatie in het behalen van de door haar beoogde resultaten (ISO, 2015). De procesbenadering gaat gepaard met het op systematische wijze definiëren en managen van processen en de onderlinge interacties om zo de beoogde resultaten te behalen. Het toepassen van de procesbenadering in een kwaliteitsmanagementsysteem maakt het volgende mogelijk (ISO, 2015):

- inzicht en consistentie bij het voldoen aan eisen.
- het nadenken over processen in termen van toegevoegde waarde.
- de realisatie van doeltreffende procesprestaties.
- verbetering van processen op basis van evaluatie van gegevens en informatie.

Daarnaast stelt ISO voor om bij het managen van de desbetreffende processen gebruik te maken van de Plan-Do-Check-Act (PDCA) cyclus. De ISO 9001 norm omschrijft de PDCA-cyclus als volgt:

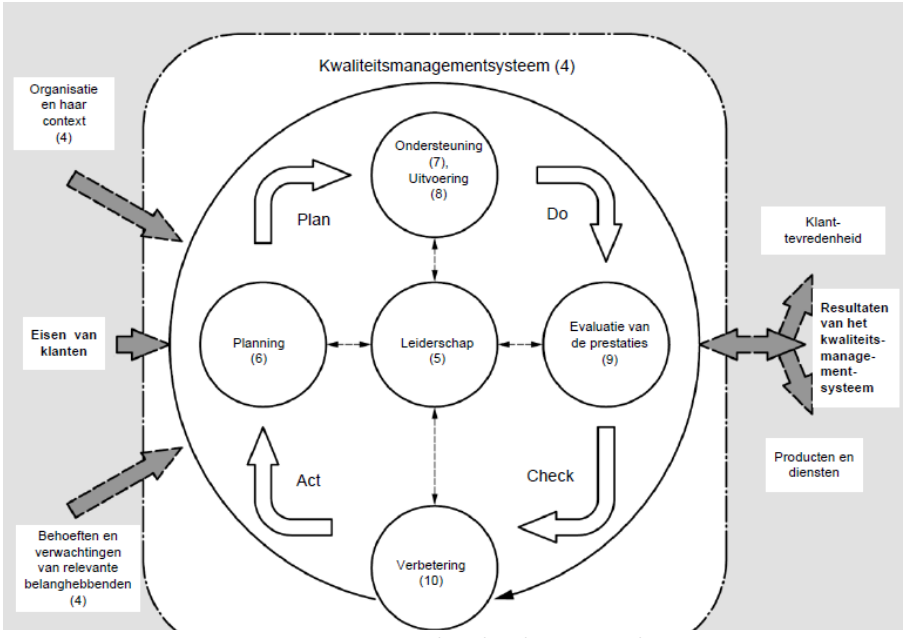
Plan: het vaststellen van de doelstellingen van het systeem en zijn processen en de middelen die nodig zijn om resultaten te leveren die in overeenstemming zijn met de eisen van klanten en het beleid van de organisatie, en de risico's en kansen vast te stellen en aan te pakken.

Do: het implementeren van wat gepland is.

Check: het monitoren en meten van processen en de resulterende producten en diensten ten opzichte van het beleid, doelstellingen, eisen en geplande activiteiten, en verder ook het rapporteren van de resultaten.

Act: het ondernemen van acties om de prestaties te verbeteren waar nodig.

Figuur 5 geeft een schematische weergave van de PDCA-cyclus weer, samen met de overeenkomstige hoofdstukken binnen de ISO 9001-norm tussen haakjes. Het geeft duidelijk weer



Figuur 5: Weergave structuur ISO 9001 standaard in de PDCA-cyclus

dat de norm aandacht besteed aan elk deel van de PDCA-cyclus, inclusief de input van de klant en de resultaten van het kwaliteitsmanagementsysteem. Verder kan opgemerkt worden dat de cyclus binnen het overkoepelende hoofdstuk rond kwaliteitsmanagementsystemen valt.

Risicogebaseerd denken

In eerdere versies van de ISO 9001 standaard was het concept van risicogebaseerd denken reeds impliciet aanwezig. Vanaf de 2015 versie wordt hier specifiek extra aandacht aan geschonken omdat het aanpakken van risico's en kansen een basis legt voor het vergroten van de doeltreffendheid van het kwaliteitsmanagementsysteem waardoor betere resultaten worden behaald en negatieve effecten worden voorkomen. Specifiek eist deze norm dat de organisatie haar context begrijpt, risico's vaststelt als basis voor planning en rekening houdt met de risico's bij het opstellen en implementeren van processen van kwaliteitsmanagementsystemen (ISO,2015).

Ondanks dat een belangrijk doel van een kwaliteitsmanagementsysteem preventief optreden is, bevat deze ISO norm geen hoofdstuk dat specifiek op preventie gericht is. Dit wordt mee in rekening genomen binnen het risicogebaseerd denken bij het formuleren van de eisen voor een kwaliteitsmanagementsysteem (ISO, 2015).

Verschil ISO 9001:2008 en ISO 9001:2015

De ISO standaarden worden om de vijf jaren herzien en indien nodig bijgewerkt zodat de standaard nauw blijft aansluiten bij de marktsituatie en de uitdagingen waarmee bedrijven geconfronteerd worden (ISO, 2015b). In dit deel worden kort de voornaamste verschillen tussen de ISO standaard uit 2008 en 2015 geschetst.

Het voornaamste verschil zit in de structuur waaruit de standaard is opgebouwd. De standaard uit 2015 bestaat uit 10 hoofdstukken in plaats van 8 en volgt nu dezelfde structuur als andere ISO managementsysteem standaarden, zoals de ISO standaarden rond veiligheid en beveiliging of algemeen management. Dit maakt het makkelijker om een overzicht te behouden wanneer men met verschillende managementsystemen werkt en wordt de integratie ertussen bevorderd. Een tweede verschil is de extra nadruk die gelegd wordt op het risico gebaseerd denken in de standaard uit 2015. Risico gebaseerd denken kwam in de standaard uit 2008 reeds aan bod maar in de 2015 standaard gaat men hier dieper op in (ISO, 2015b). Tenslotte wordt er in de laatste standaard nog een overzicht gegeven van de termen die een kleine verandering in betekenis krijgen of anders gebruikt worden in de norm uit 2015 tegenover de norm uit 2008.

Volgens ISO (2015b) brengt de 2015 versie verschillende voordelen met zich mee. Zo helpt de 2015 versie op een gestructureerde manier risico's en kansen aan te pakken. Daarnaast zorgt het voor een betere integratie met de andere managementsystemen en de productieketen van de organisatie. Ten slotte is de 2015 versie gebruiksvriendelijker voor dienstgerichte en kennisintensieve organisaties.

2.3 Combinatie COBIT en ISO 9001

Nu er een beter zicht verkregen is over de inhoud van COBIT en ISO 9001, zal er in deze sectie dieper ingegaan worden op een mogelijke combinatie tussen de twee.

2.3.1 Overzicht van combinaties tussen COBIT en ISO

Indien een organisatie of een deel van een organisatie meerdere frameworks wil implementeren, is het aan te raden om na te gaan indien een combinatie tussen deze frameworks een extra toegevoegde waarde kan leveren, in vergelijking met het apart gebruik van de frameworks. Wanneer de integratie van de frameworks niet mogelijk is, omdat de frameworks elkaar bijvoorbeeld kunnen tegenspreken of andere doelen voor ogen hebben, is het moeilijk om een consistente combinatie te creëren (Von Solms, 2005). Hieronder wordt een overzicht gegeven van onderzoeken die COBIT combineren met een ISO norm. Voor elk onderzoek wordt de redenen gegeven waarom de combinatie mogelijk is of wat de meerwaarde van de combinatie is.

Von Solms (2005) geeft aan dat er op het vlak van informatiebeveiliging een zekere synergie bestaat tussen COBIT en ISO. COBIT biedt een breed IT-Governance framework aan en geeft aan 'wat' er moet gebeuren maar 'hoe' het moet gebeuren, wordt minder concreet besproken. De ISO normen, in dit geval de ISO 17799 norm omtrent informatiebeveiliging, zijn zeer gedetailleerd en geven meer begeleiding rond de 'hoe' vraag maar ze beschikken niet over het breder platform dat COBIT aanbiedt. Ook Gehrmann (2012) stelt het gebruik van een combinatie van COBIT en ISO 27002, ook een norm omtrent informatiebeveiliging, voor om bedrijfsdoelstellingen te bereiken. Volgens deze studie levert de combinatie een duidelijkere en efficiëntere benadering op, in tegenstelling tot het apart gebruik van de frameworks, waarmee meer aspecten benaderd en gecontroleerd kunnen worden die men anders over het hoofd zou zien. Lin et al. (2012) stelt dat het combineren van COBIT en ISO 27002 interessant is om de efficiëntie en effectiviteit van interne controle te verbeteren. Zij verklaren dat de mapping laat zien op welke manier informatiebeveiliging ondersteunt kan worden door het gebruik van interne controle. Sheikhpour (2012) kaart ook het voordeel van het gebruiken van een high level framework in combinatie met een specifiek en gedetailleerd framework. De kwesties die door het high level framework worden aangekaart, worden behandeld in het gedetailleerde framework. Het combineren van COBIT en ISO 27001 zal volgens haar de gemiddelde kosten verlagen omtrent het behouden van toegestane beveiligingsniveaus, het beheren van risico's en het verlagen van de globale risico niveaus. Tenslotte maken ook het IT Governance Instituut (ITGI) en het Office of Governance Commerce (OGC) (2005 & 2008) gebruik van een mapping om een overzicht te schetsen in welke mate COBIT en ISO 17799 enerzijds en COBIT en ISO 27001 anderzijds overeenkomen met de doelstellingen van COBIT. Ook zij gebruiken COBIT als een overkoepelend controle framework met de nadruk op IT processen en ISO 17799/ISO 27001 als standaard die concreter is voor bepaalde expertisegebieden (ITGI & OGC, 2005). Op deze manier wordt de manier van begeleiding door de frameworks meer hiërarchisch voorgesteld.

Zoals uit de vorige alinea afgeleid kan worden, zijn vooral combinaties tussen COBIT en ISO normen die met informatiebeveiliging te maken hebben (e.g. ISO 17799, ISO 27002 of ISO 27001)

onderzocht. In dit onderzoek ligt de interesse voornamelijk op de combinatie tussen COBIT en de ISO 9001 norm in verband met kwaliteitsmanagementsystemen. Hieromtrent was slechts een enkel onderzoek relevant. Daarom wordt dit onderzoek in de volgende sectie meer in detail besproken.

2.3.2 De mapping tussen COBIT en ISO 9001 van Bürgy

Om de overeenkomsten tussen COBIT en ISO 9001 aan te kaarten, ontwikkelde Bürgy (2016) in zijn onderzoek een mapping tussen deze twee frameworks. Bij het opstellen van deze mapping goot hij de ISO norm in een procesmodel. Dit procesmodel werd opgesteld op basis van processen die geïmplementeerd waren bij een ISO gecertificeerde, Zwitserse KMO die software ontwikkelde. Bijgevolg is het opgestelde procesmodel zwaar beïnvloed door de processen en de activiteiten van deze onderneming. Van de geanalyseerde mappings tussen COBIT en ISO, is Bürgy ook de enige die gebruik maakt van een procesmodel. Meer over de geanalyseerde mappings in sectie 4.1. Omdat hij echter de enige is die een mapping tussen COBIT en ISO 9001 uitvoerde, is het interessant om deze mapping in deze sectie verder onder de loep te nemen zodat de mapping die voort zal komen uit dit onderzoek met de mapping van Bürgy vergeleken en verschillen aangekaart kunnen worden.

Vooraleer Bürgy aan zijn mapping begint, ontwikkelde hij een mappingsbenadering om twee frameworks met elkaar te combineren. Hij stelt dat wanneer twee standaarden of frameworks binnen het IT-Governance domein gecombineerd worden, de mapping ertussen beïnvloed wordt door twee dimensies (Bürgy, 2016): enerzijds is er de mate waarin de frameworks op mekaar lijken, anderzijds is er ook de granulariteit van de mapping. Met het eerste bedoelt hij de mate waarin elementen van het ene framework zonder problemen overgenomen kunnen worden binnen het andere framework. Met de granulariteit van de mapping wordt de mogelijkheid tot mapping van een enkel element van het ene framework met een gelijkaardig element van het andere framework nagegaan. Tabel 4 beschrijft deze twee dimensies verder in detail.

Dimensie	Lage graad van overeenkomst	Hoge graad van overeenkomst
Gelijkenissenpotentieel	Een lage graad van gelijkenissenpotentieel betekent dat er slechts enkele elementen van het ene framework gebruikt kunnen worden in het andere. Bijgevolg moeten de meeste concepten apart ontwikkeld of aangepast worden.	Een hoge graad van gelijkenissenpotentieel betekent dat veel elementen van het ene framework gebruikt kunnen worden in het andere. Bijgevolg moeten geen of slechts enkele elementen apart ontwikkeld of aangepast worden.
Mapping-granulariteit	Bij een lage graad van granulariteit verloopt de samenwerking tussen de frameworks stroef. Gelijkaardige elementen van	Bij een hoge graad van granulariteit kunnen gelijkaardige elementen met elkaar gemapt worden tot in de

	beide frameworks kunnen niet of slechts oppervlakkig met mekaar gemapt worden waardoor de combinatie soms moeilijk te begrijpen valt.	details. Dergelijke mapping is bijgevolg helder en duidelijk.

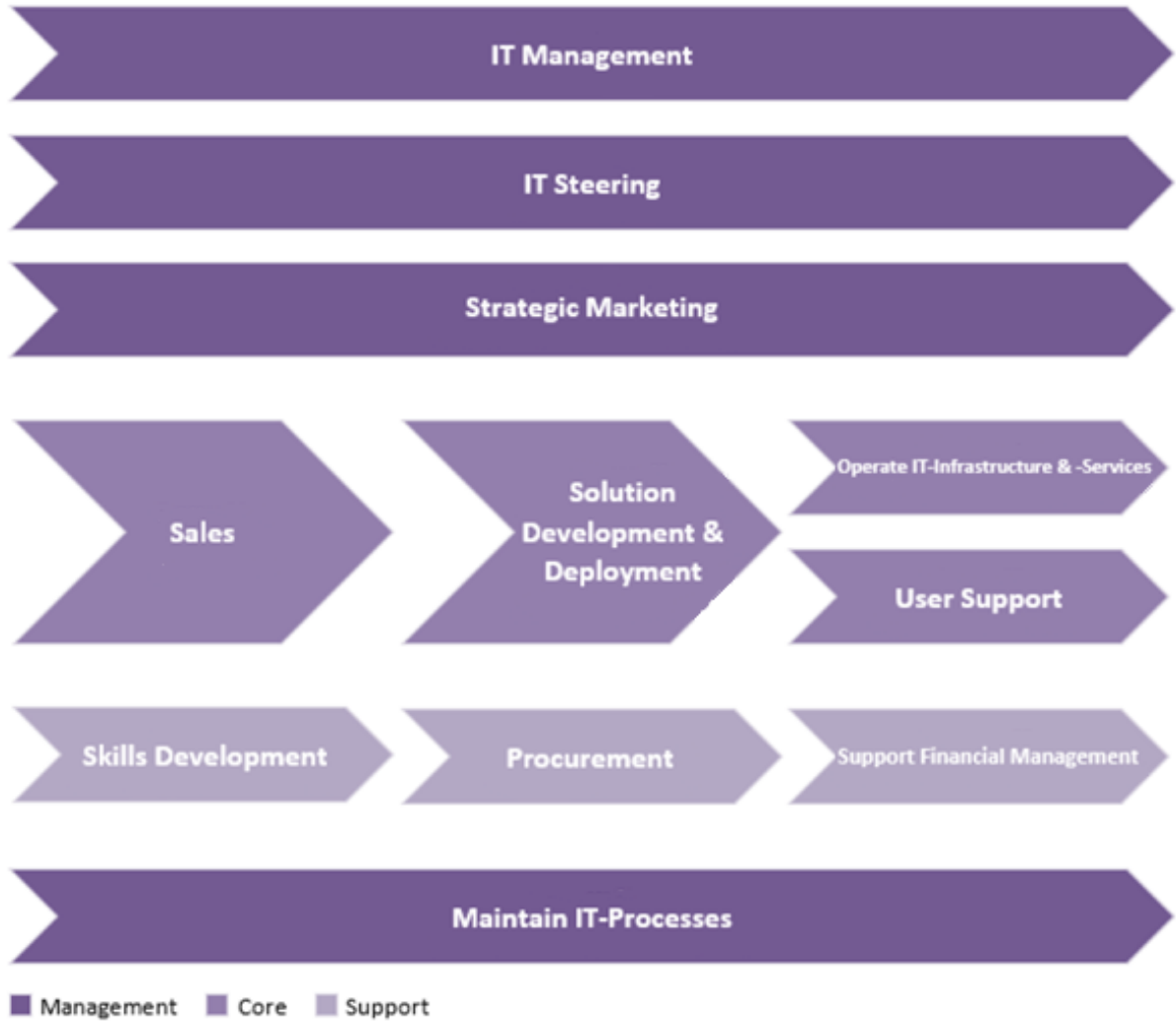
TABEL 4: COMBINATIE DIMENSIES

Bürgy merkt op dat het gelijkenissenpotentieel en de granulariteit van de mapping tussen de frameworks op elkaar inwerken. Dit betekent dat een hoge graad van gelijkenissen potentieel vaak gepaard gaat met een lage mapping granulariteit en omgekeerd. Wanneer de frameworks slechts op high level met elkaar vergeleken worden, is de kans groot dat er veel gelijkenissen gevonden zullen worden maar dan kan er geen gedetailleerde mapping tussen de frameworks plaatsvinden. Bijgevolg wordt er aangeraden om voor elke combinatie van frameworks een afweging te maken tussen de twee dimensies.

Wanneer twee frameworks enkel op high level met elkaar vergeleken worden, komt dit dus neer op een hoog gelijkenissen potentieel en een lage mapping granulariteit. Een vergelijking op low level heeft een hoge mapping granulariteit en een kleinere kans op gelijkenissen tot gevolg. Er moet dus een keuze gemaakt worden op welk level de vergelijking uitgevoerd zal worden. Bürgy stelt voor om de combinatie tussen COBIT en ISO 9001 op proces level uit te voeren. Dit omdat beide op procesvlak een redelijk hoog gelijkenissen potentieel hebben maar er toch een zekere mapping in detail mogelijk is, ondanks dat beide frameworks soms een verschillende focus hebben, zoals bijvoorbeeld voor productieprocessen die in ISO 9001 vervat zitten en niet zodanig in COBIT (Bürgy, 2016).

Om COBIT en ISO 9001 op een proces level met elkaar te combineren werd er door Bürgy dus een op ISO 9001 gebaseerde procesmodel opgesteld. Dit procesmodel deelt de verschillende aspecten die de ISO 9001 norm behandelt op in verschillende processen. Op deze manier is het volgens hem makkelijker om de vergelijking te maken met de COBIT processen. Dit procesmodel werd dus opgesteld vanuit de processen van een Zwitsers bedrijf. Deze ISO 9001 processen worden weergegeven in figuur 6.

Het procesmodel bestaat uit 11 processen die onderverdeeld zijn in vier managementprocessen die op strategische uitdagingen focussen, vier core processen die de dagdagelijkse activiteiten behandelen en drie support processen die de overige acht processen bijstaan met specifieke oplossingen en diensten. Bijlage 6 geeft een beschrijving van de functies van deze 11 processen. Nu ISO 9001 verdeeld is in processen, kunnen deze gemapt worden met de COBIT processen. In deze mapping werden enkel de COBIT processen mee opgenomen die een voldoende hoge mappingsaccuraatheid hadden. Tabel 5 geeft deze mapping tussen COBIT en ISO weer volgens Bürgy (2016).



FIGUUR 6: ISO 9001 PROCESMODEL (BÜRGY 2016)

ISO processen	**COBIT processen**
IT Management	EDM01 Ensure Governance Framework Setting and Maintenance APO01 Manage the IT Management Framework APO02 Manage Strategy APO03 Manage Enterprise Architecture MEA03 Monitor, Evaluate and Assess Compliance With External Requirements
IT Steering	APO05 Manage Portfolio

	APO09 Manage Service Agreements
Maintain IT-Processes	MEA02 Monitor, Evaluate and Assess the System of Internal Control
Strategic Marketing	EDM05 Ensure Stakeholder Transparency
Solution Development & Deployment	APO04 Manage Innovation BAI01 Manage Programmes and Projects BAI06 Manage Changes BAI07 Manage Change Acceptance and Transitioning
Operate IT-Infrastructure & -Services	BAI04 Manage Availability and Capacity BAI10 Manage Configuration DSS01 Manage Operations DSS03 Manage Problems DSS04 Manage Continuity DSS05 Manage Security Services
User Support	DSS02 Manage Service Requests and Incidents
Sales	Geen vergelijkbaar COBIT proces beschikbaar.
Skills Development	APO07 Manage Human Resources
Procurement	APO10 Manage Suppliers BAI09 Manage Assets
Support Financial Management	APO06 Manage Budget and Costs

TABEL 5: MAPPING COBIT EN ISO 9001 VOLGENS BÜRGY (2016)

Uit de tabel kan afgeleid worden dat elk ISO proces buiten het salesproces een mapping heeft met minstens één COBIT proces. Ook kan er uit afgeleid worden dat er geen ISO processen zijn die enkel op governance of op management niveau plaatsvinden. De governance processen (EDM-processen) worden gemapt met IT-Managment, IT-Steering, Strategic Marketing en Solution Development & Deployment. Deze vier ISO processen worden naast de governance processen echter ook nog met managementprocessen gemapt. Er kan wel opgemerkt worden dat drie van deze vier ISO processen zich focussen op strategisch niveau en één dat op operationeel niveau plaatsvindt. Het feit dat de meeste governance processen bijgevolg op strategisch niveau plaatsvinden is wat er in eerste instantie verwacht wordt.

De grote beperking van deze mapping van Bürgy is dat deze is opgesteld op basis van processen van een IT gerichte onderneming. Omdat de mapping niet werd opgesteld door te vertrekken vanuit de ISO norm zelf, kan de toepasbaarheid van de mapping in vraag gesteld worden bij ondernemingen die niet volledig IT gericht zijn. Ook kan er geargumenteerd worden dat de mapping enkel een overzicht geeft aan welke COBIT processen voldaan wordt, wanneer alle of enkele van deze 11 ISO processen geïmplementeerd zijn. Er wordt minder duidelijk weergegeven hoe vanuit COBIT vertrokken kan worden om een overzicht te schetsen in welke mate aan de ISO norm voldaan wordt. Daarnaast worden ook enkele COBIT processen uit de mapping gefilterd, waardoor de toepassing van de mapping in bedrijven gelimiteerd wordt.

Bij het ontwerpen van de mapping in dit onderzoek zal met deze beperkingen rekening gehouden worden. De mapping zal zowel COBIT als de volledige ISO norm zelf mee in rekening nemen, zodat ten eerste de mapping algemener is dat de mapping van Bürgy en in principe door alle ondernemingen gebruikt zal kunnen worden. Ten tweede zal de mapping zowel vertrekkende vanuit COBIT als de ISO norm gebruikt kunnen worden, afhankelijk van welk framework reeds in werking is, en ten derde zullen geen COBIT processen uit de mapping gefilterd worden.

In het volgende hoofdstuk zal de methodologie besproken worden aan de hand waarvan de mapping opgesteld zal worden. Daarna volgt het ontwerpen van de mapping zelf en in sectie 4.3 zal de vergelijking gemaakt worden met het resultaat van de ontworpen mapping en de mapping van Bürgy, waarbij de verschillen en gelijkenissen aangekaart zullen worden.

3. Methodologie

In dit hoofdstuk zal de methodologie besproken worden waarmee de mapping zal ontworpen worden. Er zal gebruik gemaakt worden van een design science methodologie aangezien het doel de ontwikkeling van een mapping is. Om de bijdrage van deze mapping te testen, zal er gewerkt worden met een case study. Om deze redenen zal er in dit hoofdstuk dieper ingegaan worden op design science en case study onderzoek.

3.1 De design science methodologie

Als eerste zal er een context geschetst worden van design science zodat er een beter beeld gevormd kan worden van wat dit precies inhoudt. Daarna zal de rol van design science binnen informatie systemen onder de loep genomen worden. Ten slotte zal er een design science framework voorgesteld worden met een aantal richtlijnen die ertoe dienen een design science project tot een goed einde te brengen.

3.1.1 Design Science

Sinds het doel van de studie het opstellen van een mapping is met als mikpunt het combineren van frameworks binnen organisaties, zal er doorheen de studie een design science methodologie toegepast worden. Design science is een onderzoeksmethodologie dat IT artefacten ontwerpt en evalueert met als doelstelling problemen in organisaties op te lossen (Hevner et al., 2004). Het omvat een strikt proces om artefacten te ontwerpen waarmee geobserveerde problemen opgelost kunnen worden, bijdragen geleverd kunnen worden aan onderzoek, ontwerpen geëvalueerd kunnen worden en de resultaten gecommuniceerd kunnen worden met het desbetreffende doelpubliek. Deze artefacten kunnen constructies, modellen, methoden en instanties bevatten (Hevner et al., 2004). Verder kunnen ze ook sociale innovaties (van Aken, 2004) of nieuwe eigenschappen voor technische, sociale of informatie bronnen bevatten (Järvinen, 2007). Kortom wil men met behulp van design science een object ontwerpen dat een oplossing biedt voor een gekende onderzoekskwestie.

Om een design science project uit te voeren moeten volgens Wieringa (2014) twee grote componenten begrepen worden. Enerzijds is er het doel van de studie en anderzijds de twee voornaamste activiteiten. Het doel van de studie bestaat kortweg uit een artefact in zijn context. De twee voornaamste activiteiten zijn het ontwikkelen en het onderzoeken van dit artefact in de context. Voor het ontwikkelen van het artefact zijn de sociale context van de stakeholders en de doelstellingen van het project belangrijk aangezien deze stakeholders het onderzoeksbudget bepalen en degene zijn waaraan de onderzoeksresultaten gerapporteerd worden. Voor de onderzoekende activiteit is het belangrijk om vertrouwd te raken met de context van het project aangezien kennis uit deze context gebruikt zal worden en er bijgedragen zal worden aan deze context door het project. Concreet voor dit onderzoek is het doel de ontwikkeling van een mapping tussen COBIT en de ISO 9001 norm die de integratie van de twee binnen ondernemingen vergemakkelijkt. Bij het ontwikkelen van het artefact is de onderneming waar de mapping getest zal worden belangrijk. Op basis van hun feedback zal bepaald worden of er een meerwaarde gevonden kan worden in de mapping. Zij zijn ook de

bestemming van het resultaat. Wat de onderzoekende activiteit betreft is het enerzijds belangrijk om vertrouwd te geraken met bestaande mappings tussen deze twee frameworks, hoe deze bestaande mappings opgebouwd zijn en wat hun bijdrage is. Anderzijds is ook de context binnen de onderneming waar de mapping getest zal worden belangrijk aangezien zij informatie zullen leveren die de bijdrage van de ontworpen mapping zal bepalen.

Artefacten zijn bepaalde methoden, technieken, notaties of algoritmen die ontworpen worden om een bijdrage te leveren aan hun context. Deze context bevat onder meer mensen, waardes, verlangen, normen, doelstellingen oftewel elementen waar het artefact rekening mee moet houden en die niet door de onderzoeker zelf ontwikkeld of gewijzigd kunnen worden. Verder moet er opgemerkt worden dat het artefact zelf geen probleem oplost maar dat het de interactie is tussen het artefact en zijn context dat tot de oplossing van een probleem bijdraagt *(*Wieringa, 2014). Een artefact kan namelijk verschillend reageren in een verschillend context. De oplossing die de ontworpen mapping uit dit onderzoek biedt, is ook afhankelijk van de context waarin de mapping gebruikt wordt. In de inleiding werden reeds vier verschillende scenario's gegeven waarin de mapping van pas kan komen. Ook het moment waarop de mapping gebruikt wordt om de twee frameworks te integreren kan een verschillend resultaat opleveren. Wanneer een onderneming de mapping aan het begin van de integratie toepast en de mapping als een leidraad gebruikt om de integratie uit te voeren, zal dit een verschillende uitkomst hebben als wanneer een onderneming eerst zelf bepaald welke processen de integratie van beide frameworks mogelijk maakt en de mapping slechts gebruikt als een soort checklist aan het einde van de integratie.

De twee onderdelen van design science, ontwikkelen en onderzoeken, komen overeen met twee type onderzoeksproblemen, namelijk *design problems* en *knowledge questions (*Wieringa, 2014). Design problems mikken op een verandering te brengen in de echte wereld en vereisen een analyse van werkelijke of hypothetische stakeholder goals. De oplossing bestaat uit een of meerdere designs die geëvalueerd worden met de stakeholder goals om vervolgens de beste oplossingen hieruit te selecteren. Knowledge questions gaan op zoek naar kennis over de wereld maar verlangen geen verandering in de wereld. Het antwoord op de vraag is een voorstel. Op voorhand is niet geweten in welke richting het antwoord zal liggen en bestaat er vaak veel onzekerheid over het antwoord. Ook is er niet geweten of het antwoord dat gevonden wordt correct is of niet. Antwoorden op knowledge questions of oplossingen van een design problem kunnen beide nieuwe problemen voortbrengen. Op deze manier bestaat er een iteratie tussen de twee binnen design science. Startende van een design problem kunnen er knowledge questions gesteld worden over het bekomen artefact, context of de interactie tussen het artefact en de context. Andersom kan het antwoord op een knowledge question leiden tot nieuwe design problems zoals bijvoorbeeld het bouwen van een prototype van een artefact of het simuleren van de context *(*Wieringa, 2014). Dit onderzoek hoort thuis binnen de design problems aangezien het doel is dat de ontworpen mapping een verandering teweeg kan brengen, namelijk dat het integreren van het COBIT framework en de ISO 9001 norm vergemakkelijkt wordt.

3.1.2 Design science in informatiesystemen

Informatie systemen (IS) worden in organisaties geïmplementeerd om de effectiviteit en efficiëntie binnen die organisatie te verbeteren (Hevner, 2004). Binnen IS onderzoek moeten onderzoekers ernaar streven om kennis bij te brengen die helpt bij het implementeren en het behalen van de voordelen van informatietechnologie binnen organisaties en hun management (ISR, 2002). Het onderzoek moet bijdragen aan de ontwikkeling en communicatie van kennis betreffende zowel het beheer van informatietechnologie en het gebruik van informatietechnologie voor organisationele of management doeleinde (Zmud, 1997). Volgens March en Smith (1995) impliceert het verwerven van deze kennis twee complementaire maar verschillende gedachtepatronen, namelijk gedragswetenschappen en design science. Gedragswetenschappen heeft zijn roots in natuurwetenschappelijke onderzoeksmethoden en mikt op het ontwikkelen en valideren van theorieën die organisationele of menselijke fenomenen verklaren. Deze theorieën brengen uiteindelijk de interacties tussen mensen, technologie en organisaties in kaart die gemanaged moeten worden om de efficiëntie en effectiviteit van een IS te vergroten. Design science heeft zijn roots in engineering en de wetenschappen die het artificiële bestuderen (Simon, 1996). Het gaat op zoek naar innovaties of artefacten die de ideeën, praktijken, technische mogelijkheden en producten definiëren waarmee de analyse, het ontwerp, de implementatie, het beheer en het gebruik van informatiesystemen effectief en efficiënt uitgevoerd kunnen worden (Denning, 1997; Tsichritzis, 1998). Het ontwikkelen van artefacten is complex omwille van de behoefte aan creatieve voortgang in vakgebieden waarin de bestaande theorie vaak onvoldoende is. Het resulterende artefact verlegt de grenzen van de probleemoplossing en organisationele bekwaamheid door zowel intellectuele als rekenkundige tools te ontwikkelen (Hevner, 2004).

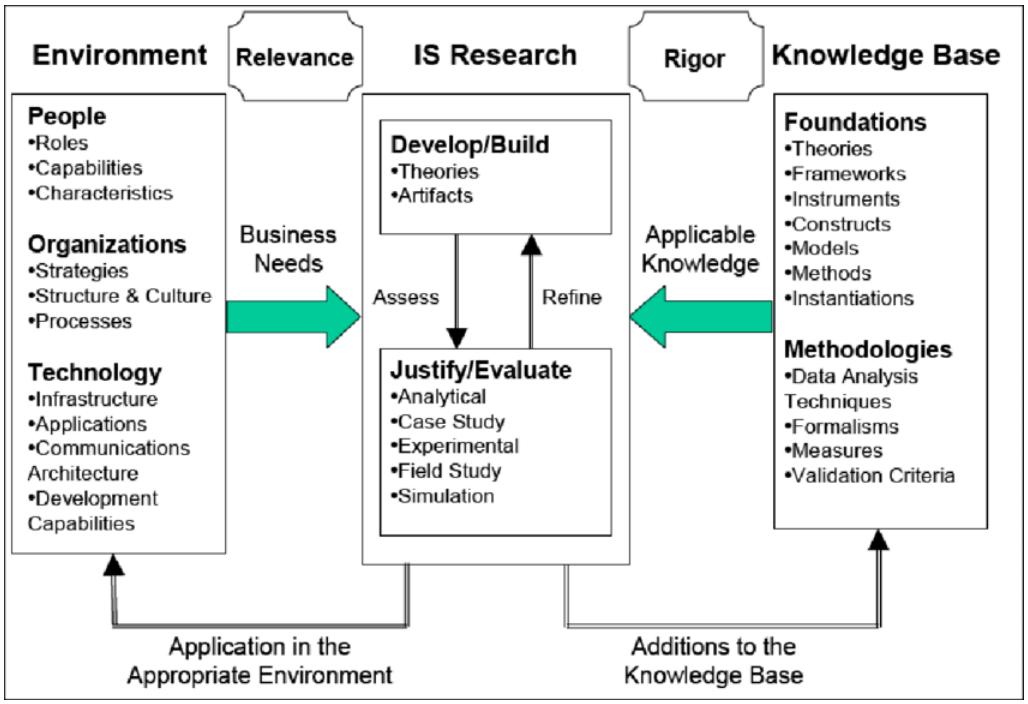
3.1.3 Een design science framework

Om een design science project uit te voeren, bestaan er verschillende frameworks die als leidraad doorheen het IS onderzoek kunnen dienen. Peffers et al. (2008) stellen een framework voor dat bestaat uit zes activiteiten die draaien rond het identificeren en definiëren van het probleem, het opstellen van het artefact en de implementatie en evaluatie van dit artefact. Ook bevat dit framework een proces iteratie waarbij het artefact bij elke iteratie geoptimaliseerd wordt. Wieringa (2014) beschrijft in zijn boek een design science methodologie dat gebruik maakt van een design en een empirische cyclus. Afhankelijk van het doel van het project moet een van deze twee cycli gevolg worden. Het framework dat doorheen deze studie gevolgd zal worden is een vaak terugkomend framework van Hevner et al. (2004) voor het begrijpen, uitvoeren en evalueren van IS onderzoek. Dit framework bestaat uit drie hoofddelen namelijk de *Environment*, *IS Research* en *Knowledge Base* (Figuur 7). Environment definieert de omgeving waarin de verschijnselen die van belang zijn zitten (Simon 1996). Voor IS onderzoek zijn dit mensen, organisaties en hun bestaande of toekomstige technologieën (Silver et al., 1995). Deze bevatten de doelstellingen, taken, problemen en kansen die gedefinieerd worden door de bedrijfsbehoeften. De mensen binnen de onderneming hebben bepaalde rollen, competenties en eigenschappen waardoor ze deze bedrijfsbehoeften op een bepaalde manier interpreteren. Verder worden de bedrijfsbehoeften geëvalueerd binnen de context van de bedrijfsstrategie, structuur, cultuur en processen. De bedrijfsbehoeften worden vergeleken met de bestaande technologische infrastructuur, applicaties, communicatie architectuur en de

ontwikkelingscapaciteiten. Samen definiëren al deze elementen de bedrijfsbehoeften en het plaatsten van de onderzoeksactiviteiten door de onderzoeker binnen dit bedrijfskader verzekert de relevantie van het onderzoek.

Gegeven een bedrijfsbehoeften kan IS research, net zoals March en Smith (1995) vaststelden, uitgevoerd worden in twee complementaire fasen. Enerzijds dragen gedragswetenschappen bij tot het onderzoek door het ontwikkelen en het rechtvaardigen van theorieën die fenomenen gerelateerd aan de geïdentificeerde bedrijfsdoelstellingen verklaren of voorspellen (Hevner, 2004). Anderzijds draagt design science bij door het opstellen en het evalueren van artefacten die ontwikkeld zijn om aan de geïdentificeerde bedrijfsdoelstellingen te voldoen. Het doel van gedragswetenschappen is het leveren van de waarheid en het doel van design science is het leveren van nut (Hevner, 2004).

De knowledge base uit het framework levert de informatie waarmee het IS onderzoek uitgevoerd kan worden. Deze bestaat uit de kennis en de methodologieën uit voorgaand onderzoek die gebruikt worden in de ontwikkel en evaluatie fasen van het huidige onderzoek (Hevner, 2004). Het huidige onderzoek wordt gegrond door het juist toepassen van deze methoden en bestaande funderingen. Om het onderzoek te evalueren, worden in de gedragswetenschappen vaak methoden zoals data verzameling en empirische analyses gebruikt. In design science worden regelmatig rekenkundige en wiskundige modellen gebruikt om de kwaliteit en de effectiviteit van artefacten te meten, hoewel empirische technieken ook toegepast kunnen worden (Hevner, 2004).



Figuur 7: Het informatie systeem onderzoeksframework van Hever et al. (2004).

3.1.4 De richtlijnen van het design science framework

Zoals reeds aangehaald is design science in essentie een probleemoplossend proces. Hevner (2004) heeft zeven richtlijnen opgesteld om een onderzoeker te helpen doorheen dit proces. Deze richtlijnen zijn opgesteld rond het centrale principe dat kennis en begrip van een design probleem en zijn

oplossing verkregen worden bij het opstellen en toepassen van het artefact. Design science vergt om te beginnen het ontwerp van een innovatief, doelgericht artefact (richtlijn 1), voor een specifiek probleemdomein (richtlijn 2). Omdat het artefact doelgericht is, moet het nuttig zijn voor het opgegeven probleem. Vandaar dat een grondige evaluatie van het artefact cruciaal is (richtlijn 3). Nieuwigheid is eveneens cruciaal omdat het artefact innovatief moet zijn, een tot nu toe onopgelost probleem oplost of een gekend probleem op een meer effectieve of efficiënte manier oplost (richtlijn 4). Het artefact zelf moet streng worden gedefinieerd, formeel worden weergegeven, coherent en intern consistent zijn (richtlijn 5). Het proces waarmee het artefact gemaakt is en het artefact zelf moeten een zoekproces bevatten of maken waarbij een probleemruimte wordt geconstrueerd en een mechanisme wordt ingesteld of vastgesteld om een effectieve oplossing te vinden (richtlijn 6). Ten slotte moeten de resultaten van het onderzoek effectief worden gecommuniceerd (richtlijn 7).

Het doel van deze richtlijnen is volgens Hevner (2004) het bijstaan van onderzoekers, beoordelers, editors en lezers bij het begrijpen van de vereisten voor effectieve design science. Hij adviseert tegen het noodzakelijk gebruiken van al deze richtlijnen en stelt dat onderzoekers hun eigen creatieve vaardigheden en oordeel moeten gebruiken om te bepalen wanneer, waar en hoe deze richtlijnen toegepast moeten worden in een onderzoeksproject. Toch stelt hij echter ook dat deze richtlijnen allemaal in bepaalde mate aanwezig moeten zijn in een design science project om compleet te zijn. Hoe gedetailleerd en de mate waarin elk van deze richtlijnen aanwezig is, is aan de onderzoeker om te beslissen.

Richtlijn	Beschrijving
Richtlijn 1: Ontwerp een artefact.	Design science onderzoek moet een levensvatbaar artefact produceren in de vorm van een construct, een model, een methode of een instantie.
Richtlijn 2: Probleem relevantie.	Het doel van een design science onderzoek is om op technologie gebaseerde oplossingen te ontwikkelen voor belangrijke en relevante bedrijfsproblemen.
Richtlijn 3: Ontwerp evaluatie.	Het nut, de kwaliteit en de doeltreffendheid van een artefact moeten rigoureus worden aangetoond via correct uitgevoerde evaluatiemethoden.
Richtlijn 4: Onderzoek bijdrage.	Effectief design science onderzoek moet een duidelijke en verifieerbare bijdragen leveren op

	het gebied van het artefact, ontwerpfundamenten en/of ontwerpmethodologieën.
Richtlijn 5: Onderzoek strengheid.	Design science onderzoek is afhankelijk van de kritische toepassing van methoden bij zowel de constructie als de evaluatie van het artefact.
Richtlijn 6: Ontwerp als een zoekproces.	De zoektocht naar een effectief artefact vereist het gebruik van beschikbare middelen om de gewenste doelen te bereiken terwijl het voldoet aan de wetten in de probleemomgeving.
Richtlijn 7: Communicatie van het onderzoek.	Design science onderzoek moet effectief worden gepresenteerd, zowel voor technologiegerichte als voor managementgerichte doelgroepen.

Tabel 6: De 7 richtlijnen voor een design science onderzoek volgens Hevner et al. (2004).

1. Het ontwerpen van een artefact

Het resultaat van een design science onderzoek in IS is een nuttig IT artefact dat ontworpen is om een probleem in een organisatie aan te pakken. Dit artefact moet op een effectieve manier beschreven worden zodat een implementatie en toepassing in het betreffende domein mogelijk is (Hevner, 2004). Het artefact van dit onderzoek zal een mapping zijn tussen het COBIT framework en de ISO 9001 norm uit 2015 dat een duidelijk overzicht zal geven waarin de twee elkaar overlappen en waar ze van elkaar verschillen. Op deze manier kan de integratie en het aanvullend gebruik van de frameworks nagegaan worden (Sheikhpour, 2012).

In de literatuurstudie werd er reeds een overzicht gegeven van bestaande mappings tussen COBIT en ISO en werd er dieper ingegaan op het werk van Bürgy die reeds een mapping tussen COBIT en ISO 9001 ontworpen heeft. In het volgende hoofdstuk zal er dieper ingegaan worden op de manier waarop deze mappings ontworpen zijn en zullen de verschillen in kaart gebracht worden. Op basis hiervan zal beslist worden hoe de mapping uit dit onderzoek ontworpen zal worden. Het opstellen van de mapping zal hierna dan ook plaatsvinden.

2. Relevantie van het probleem

Bedrijven en organisaties hebben doelstellingen binnen een economische en sociale omgeving. Deze doelstellingen zijn vaak winst of nut gerelateerd. Bedrijfsproblemen en kansen hebben dus vaak te maken met het maximaliseren van winst of het minimaliseren van kosten door middel van het ontwikkelen van effectievere en efficiëntere bedrijfsprocessen. Het ontwerp van een IS speelt een

grote rol binnen het verbeteren van bedrijfsprocessen om deze doelstellingen te verbeteren (Hevner, 2004). Design science probeert deze doelstellingen te benaderen door middel van het creëren van artefacten die organisaties ertoe in staat stellen bedrijfsproblemen op te lossen.

De relevantie en de potentiële bijdrage van de mapping werden reeds besproken in sectie 1.3 van de inleiding. In essentie is het zo dat bedrijven of delen van bedrijven vaak meerdere frameworks hebben geïmplementeerd of willen implementeren om IT te beheren. Omdat het in beeld brengen van overlappingen tussen deze frameworks verschillende voordelen met zich mee kan brengen, wordt er in dit onderzoek een mapping ontworpen die bedrijven de kans geeft om van deze voordelen gebruik te maken. Specifiek wordt de mapping opgesteld tussen het COBIT framework en de ISO 9001 norm omdat naar deze combinatie in het verleden slechts weinig onderzoek verricht is.

3. Evaluatie van het design

Met behulp van evaluatie methoden moet het nut, de kwaliteit en de doeltreffendheid van het artefact nagegaan worden. Deze evaluatie moet de integratie van het artefact binnen de technische infrastructuur van de bedrijfsomgeving omvatten (Hevner, 2004). IT artefacten kunnen geëvalueerd worden op basis van functionaliteit, volledigheid, consistentie, accuraatheid, prestaties, betrouwbaarheid, nut en bruikbaarheid binnen de organisatie. Hiervoor moeten metrieken gedefinieerd worden, relevant aan het artefact, die deze evaluatie mogelijk maken.

Omdat het ontwikkelen van het ultieme artefact een iteratief proces is, dient de evaluatie fase feedback te geven aan de constructie fase om op deze manier de kwaliteit van het design proces en product te verhogen (Hevner, 2004). Het artefact is slechts compleet wanneer het aan de vereisten en beperkingen voldoet van het probleem waar het een oplossing voor dient te bieden.

De evaluatie van een artefact maakt hoofdzakelijk gebruik van methoden die beschikbaar zijn in de knowledge base (figuur 7). Tabel 7 vat deze methoden samen. Afhankelijk van het ontworpen artefact en de vooropgestelde metrieken, moet een toepasselijke evaluatiemethode gekozen worden.

Observationeel	Case Study
	Field Study
Analytisch	Statistische analyse
	Architectuur analyse
	Optimalisatie
	Dynamische analyse
Experimenteel	Gecontroleerd experiment
	Simulatie
Testen	Functionele (black box) testen

	Structurele (white box) testen
Beschrijvend	Geïnformeerd argument
	Scenario's

Tabel 7: Evaluatiemethoden voor een artefact volgens Hevner et al. (2004).

Om in dit onderzoek de opgestelde mapping te kunnen valideren, wordt er de voorkeur gegeven om de mapping te gaan demonstreren in een bedrijfsomgeving en te werken met een case study. Op deze manier wordt het artefact getest in zijn context en aangezien het artefact als doel heeft om in de praktijk twee frameworks te integreren, is het interessant om de mapping reeds een eerste maal in de praktijk uit te voeren en de meerwaarde ervan aan te tonen. Op deze manier wordt de generate/test cyclus (zie richtlijn 6) reeds voor een eerste iteratie uitgevoerd. Een ander belangrijk voordeel van een case study is dat de theorie met de praktijk vergeleken kan worden. Specifiek voor de COBIT processen kan er een verschil zijn tussen de theoretische processen die worden voorgeschreven en de in de praktijk uitgevoerde processen (ISACA, 2012). In sectie 2 van dit hoofdstuk zal er verder ingegaan worden op case study onderzoek.

4. Onderzoeksbijdrage

Een effectief design science onderzoek moet een nieuwe en interessante bijdrage leveren aan het onderzoeksdomein. Hevner (2004) identificeert drie soorten onderzoeksbijdragen dat een artefact kan hebben.

1. De meest voorkomende bijdrage van een design science onderzoek is het artefact zelf. Het artefact moet een oplossing bieden voor een tot nu toe onopgelost probleem. Hiermee kan het enerzijds de knowledge base verbreden of anderzijds bestaande kennis op een nieuwe, innovatieve manier toepassen.
2. De ontwikkeling van nieuwe, goed onderbouwde en geëvalueerde methoden of modellen die een verbetering leveren van de bestaande fundamenten van de knowledge base. In tegenstelling tot de eerste, praktische bijdrage, is deze bijdrage theoretischer van aard.
3. De laatste soort onderzoeksbijdrage is het ontwikkelen en toepassen van nieuwe evaluatiemethoden en metrieken voor design science onderzoeken. Deze methoden en metrieken zijn cruciaal binnen design science en dienen ook geoptimaliseerd en up-to-date gehouden te worden.

Uit deze drie types kan afgeleid worden dat het eerste type een bijdrage wil leveren aan de environment uit figuur 7 door met behulp van een artefact een oplossing te bieden. De andere twee types leveren eerder een bijdrage aan de knowledge base uit figuur 7.

Deze studie dient een bijdrage van het eerste type te voorzien. De mapping die ontworpen zal worden moet ondernemingen ondersteunen bij het integreren van COBIT en de ISO 9001 norm. Zoals eerder vermeld bestaan er in de literatuur reeds verschillende mappings tussen COBIT en ISO normen maar is er slechts weinig onderzoek gedaan naar een mapping tussen COBIT en de ISO 9001 norm. Enkel Bürgy (2016) ontwikkelde een mapping tussen COBIT en ISO 9001. Deze mapping werd uitgevoerd

op basis van een procesmodel van de ISO norm dat werd opgesteld op basis van een IT gerichte onderneming. Dit procesmodel werd gebruikt om de integratie met COBIT na te gaan. Deze studie hanteert op dit gebied een andere aanpak aangezien de mapping opgesteld zal worden vanuit de secties van de ISO norm en de COBIT processen en niet vanuit bedrijfsprocessen. Er wordt wel een vergelijking uitgevoerd tussen beide mappings om eventuele overeenkomsten of verschillen te identificeren en te verklaren.

5. Onderzoek strengheid

Een design science onderzoek vereist een strenge kijk naar de methoden die toegepast worden in zowel de bouw als de evaluatie van het artefact. Een overbenadrukking op strengheid kan echter leiden tot een daling in relevantie van het onderzoek (Lee, 1999). Applegate (1999) stelt dat het mogelijk en noodzakelijk is voor IS onderzoek om zowel streng als relevant te zijn. De mate van strengheid kan afgeleid worden van het effectief gebruik maken van de knowledge base. De onderzoeker moet de juiste technieken selecteren om de theorie of het artefact op te bouwen en de juiste middelen selecteren om deze te evalueren.

Binnen het huidige onderzoek zullen de relevantie, het opstellen en het evalueren van het artefact gebaseerd worden op voorgaand onderzoek. De relevantie wordt duidelijk gemaakt door in de literatuur de meerwaarde van zowel COBIT als ISO individueel op te zoeken, alsook wat de meerwaarde is van de combinatie van de twee. De methode voor het opstellen van het artefact wordt verkregen aan de hand van voorgaande mappings tussen COBIT en ISO en de meerwaarde die uit deze studies is voortgekomen. Voor de evaluatie van het artefact zal er een case study uitgevoerd worden. Ook het toepassen van het design science framework van Hevner draagt bij tot de wetenschappelijkheid van het onderzoek.

6. Ontwerp als een zoekproces

Het ontwerpen van het optimale artefact is een iteratief proces dat een Generate/Test cyclus (Simon, 1996) volgt. In deze cyclus dient het ontwerp als input voor het testen van dit ontwerp, wat op zijn beurt dan weer zorgt voor nieuwe input voor het aanpassen of ontwikkelen van een nieuw ontwerp. Op deze manier kan men op zoek gaan naar het optimale ontwerp tot er weinig of geen verbeteringen meer mogelijk zijn. Design science onderzoek vereenvoudigt vaak een probleem door het probleem op te delen in subproblemen. Deze subproblemen kunnen als startpunt dienen en door middel van de iteratieve cyclus kan voortgang gemaakt worden naar de uiteindelijke oplossing van het probleem.

Deze richtlijn zal in het huidige onderzoek het minst nadrukkelijk aanwezig zijn. Het artefact zal ontworpen worden en eenmalig getest worden om een eerste validatie ervan te voorzien. Het verder ontwikkelen van het artefact op basis van de resultaten en het testen van deze nieuwe ontwikkelingen liggen buiten de scope van dit onderzoek. Afhankelijk van de resultaten van het eerste artefact, kunnen eventuele aanpassingen als input dienen voor toekomstig onderzoek.

7. Communicatie van het onderzoek

Een design science onderzoek moet presenteerbaar zijn aan zowel een technisch als een management georiënteerd publiek. Het technische publiek moet voldoende details voorgeschoteld krijgen zodat het artefact door hun implementeerbaar is binnen de juiste organisationele context. Ook moet dit doelpubliek over de opbouw van het artefact geïnformeerd te worden zodat het project herhaald kan worden en de knowledge base verder kan aanvullen. Het management publiek moet voldoende details krijgen om te kunnen bepalen of het artefact binnen de organisationele context gebruikt kan worden en of ze er de nodige bronnen aan willen besteden. Het is belangrijk dat de nadruk voor hun op het belang van het probleem gelegd wordt en de effectiviteit van de oplossing dat het artefact aanbiedt. Hiervoor kan het soms nodig zijn dat het artefact toch tot op een bepaald detailniveau uitgelegd moet worden aan het management zodat ze het artefact beter kunnen begrijpen en appreciëren.

Dit onderzoek is gericht op een publiek dat een zekere voorkennis heeft van IT-Governance en kwaliteitsmanagement en de personen binnen een organisatie die met deze twee domeinen bezig zijn. In de literatuurstudie worden echter de twee frameworks waarrond de mapping opgesteld wordt onder de loep genomen zodat iedere lezer deze kennis meekrijgt tot op een bepaald niveau. Het opstellen van de mapping zal in detail beschreven worden zodat replicatie mogelijk is voor een technisch publiek voor dezelfde of een combinatie van andere frameworks.

3.2 Case study onderzoek

Case study onderzoek bestudeert op een wetenschappelijke en gedetailleerde manier fenomenen binnen hun ongecontroleerde omgeving en context. Een case kan een individu, een groep, een organisatie, een evenement, een probleem of een anomalie zijn (Burawoy, 2009; Stake, 2005; Yin, 2014). Een case kan gekozen worden omwille van zijn praktisch belang (Stake, 2005) of omwille van theoretische redenen (Eisenhardt en Graebner, 2007). Mogelijke voordelen van een enkele case study zijn een gedetailleerde beschrijving en een analyse die zorgt voor een beter begrip van 'hoe' en 'waarom' dingen gebeuren. In een enkele case study bestaat de mogelijkheid om dieper in detail naar de oorzaken van het fenomeen te kijken (Fiss, 2009). De case data kan leiden tot de identificatie van patronen en relaties, het creëren, uitbreiden of testen van een theorie (Gomm et al., 2000). Mogelijke voordelen van het onderzoeken van meerdere case studies zijn het ontdekken van gelijkenissen en verschillen en hoe deze de bevindingen beïnvloeden. Elke case kan geanalyseerd worden als een enkele case study om vervolgens de bevindingen te vergelijken en theoretische conclusies te trekken (Vaughan, 1992). De mogelijkheid om een breed scala aan bronnen te gebruiken en om een fenomeen in zijn specifieke context te onderzoeken geeft het een unieke sterkte ten opzichte van andere methoden, zoals enquêtes, gegevens en studies.

In het verleden durfden onderzoekers soms een minachting hebben tegenover case studies (Yin, 1984). Case studies werden als een minder wenselijke vorm van onderzoek aanzien dan bijvoorbeeld experimenten of enquêtes. De voornaamste reden voor deze minachting is een tekort aan strengheid en objectiviteit. Onderzoekers lieten dubbelzinnigheid en vooroordelen in hun onderzoek sluipen om bevindingen en conclusies te beïnvloeden. Alhoewel deze vooroordelen ook in experimenten

(Rosenthal, 1966) of enquêtes (Sudman & Bradburn, 1982) aanwezig kunnen zijn. Een tweede punt van kritiek op case studies is dat ze weinig basis bieden voor wetenschappelijke generalisatie. Het is namelijk moeilijk om een generaliserende conclusie te trekken uit een enkele case study. Yin (1984) oordeelt dat multi-case studies, net zoals experimenten, generaliseerbaar zijn voor theoretische proposities en niet voor populaties. Op deze manier representeert de case study geen steekproef maar is het doel van de onderzoeker eerder het uitbreiden en het veralgemenen van theorieën.

Om een potentieel gebrek aan objectiviteit tegen te gaan, hechten Rowley (2002) en Dubé en Paré (2003) veel belang aan een goed onderzoeksontwerp. Ridder (2017) maakt een opsomming van enkele onderzoeksontwerpen voor case studies:

- "No Theory First" door Eisenhardt (1989)
- "Gaps and Holes" door Yin (1984)
- "Social Construction of Reality" door Stake (1995)
- "Anomalies" door Burawoy (1998)

In "No Theory First" is er een brede onderzoeksvraag met enkele voorlopige variabelen in het begin. Deze variabelen kunnen samen met de onderzoeksvraag veranderen doorheen het onderzoek. Eisenhardt wil vertrekken zonder theorie om de observaties zo puur mogelijk te houden zonder beïnvloed te worden door een theorie. De onderzoeksvraag kan voortkomen uit een research gap waardoor deze relevant is voor het onderzoek. Voorlopige a priori constructen of variabelen begeleiden het onderzoek, maar er worden geen relaties tussen dergelijke constructies of variabelen verondersteld.

"Gaps and Holes" kan ook mikken op het vullen van een research gap met als doel de theorie en literatuur vooruit te helpen. Dit soort case studies draaien voornamelijk om de 'hoe' en 'waarom' vragen. Onderzoeksvragen worden opgesteld vertrekkende vanuit de literatuur en bestaande theorieën, die het startpunt zijn van het onderzoek. Frameworks of beweringen geven de richting aan, weerspiegelen het theoretisch perspectief en begeleiden de zoektocht naar relevant bewijsmateriaal voor de studie.

"Social Construction of Reality" is gebaseerd op constructivistische aannames en heeft als doel de sociale constructie van werkelijkheid en betekenis te onderzoeken. Volgens deze filosofische veronderstelling bestaat er geen ''echte wereld'' die bestaat onafhankelijk van menselijke mentale activiteit en symbolische taal. De wereld is een product van sociaal en historisch gerelateerde uitwisselingen tussen mensen (sociale constructie). De onderzoeker is niet op zoek naar objectieve feiten of patronen die gegeneraliseerd kunnen worden. In tegendeel, de constructivist onderzoekt specifieke acties, op specifieke plaatsen, op specifieke tijden. De wetenschapper probeert de constructie en het delen van betekenis te begrijpen.

Bij "Anomalies" komt de onderzoeksvraag voort uit nieuwsgierigheid. Onderzoekers kijken naar wat interessant en verrassend is in een sociale situatie die de bestaande theorie niet kan verklaren. De case study gaat op zoek naar antwoorden op afwijkingen die vorige theorieën niet konden verklaren omwille van contradicties of onderzoeksgaps.

Gegeven de mapping die deze studie wil ontwikkelen met als doel het vergemakkelijken van de integratie tussen COBIT en ISO, lijkt het onderzoeksontwerp van Yin ("Gaps and Holes") toepasbaar op dit onderzoek. Ridder (2017) stelt ook dat de geïdentificeerde gaps en de daaruit volgende relaties als basis kunnen dienen voor het opstellen van frameworks en beweringen, voortkomend uit empirische data. Dit onderzoek beweert namelijk dat ISO en COBIT mekaar overlappen en wil een framework ontwikkelen dat deze overlappingen aankaart, waarmee de integratie tussen de twee bevorderd wordt.

Het onderzoeksontwerp van Yin (1984) bestaat uit vijf componenten:

1. De onderzoeksvragen.
2. Indien aanwezig, de gemaakte beweringen.
3. De entiteit die geanalyseerd wordt.
4. De logica die de gegevens koppelt aan de proposities.
5. De criteria voor het interpreteren van de bevindingen.

De onderzoeksvragen zouden een belangrijke aanwijzing moeten geven welke onderzoeksstrategie gebruikt zou kunnen worden. Afhankelijk of er een antwoord gegeven moet worden op de vragen "Wie", "Wat", "Waar", "Wanneer", "Hoe" en "Waarom" kan de onderzoeksstrategie bepaalt worden. Een case study strategie is het meest geschikt om een antwoord te geven op de vragen "Hoe" en "Waarom".

Wat de tweede component betreft, richt elke bewering de aandacht op iets dat moet onderzocht worden in het kader van het onderzoek. De "Hoe" en "Waarom" vragen uit de onderzoeksvragen wijzen niet direct naar wat onderzocht moet worden. Het maken van beweringen zal de onderzoeker in de juiste richting wijzen naar wat onderzocht moet worden. Sommige studies kunnen redenen hebben om geen beweringen te maken. Dit is in het geval dat het onderwerp verkend moet worden. Een verkennende studie moet desondanks wel een duidelijk doel aangeven, evenals criteria waarmee de verkenning beoordeeld zal worden.

De derde component heeft betrekking op het definiëren wat de case inhoud. De case kan bijvoorbeeld handelen over een individu of beslissingen, programma's, processen, organisaties, enz. Het bepalen van de eenheid die geanalyseerd wordt kan afgeleid worden uit de initiële onderzoeksvragen die werden gedefinieerd. Eens de case in het algemeen bepaald is, moeten bijkomende verduidelijkingen gedefinieerd worden. Dit kan gaan tot het beperken van geografische gebieden of het bepalen van een tijdsinterval waarin de case study uitgevoerd moet worden tot het onderzoeken van bestaande literatuur waarmee de resultaten vergeleken kunnen worden.

De laatste twee componenten representeren de data analyse stappen in het case study onderzoek. Voor deze analyse dient het onderzoeksontwerp de juiste basis te leggen. Om de gegevens te kunnen linken met de proposities is "pattern-matching" volgens Yin een goede methode, waarbij informatie van de case gerelateerd kan zijn aan de theoretische proposities. Wat de evaluatie criteria betreft voor pattern matching, verklaart Yin dat er geen precieze manier is om criteria op te stellen om dit soort resultaten te interpreteren. Hij vermeld dat een onderzoeker moet 'hopen' dat er meerdere patterns zijn die voldoende contrasterend zijn.

Het voldoen aan deze vijf componenten zal leiden tot het objectief opstellen van een theorie gerelateerd aan de studie die wordt uitgevoerd. Bij het opstellen van de case study zal er dus met deze vijf componenten rekening gehouden worden om met de resultaten van de case study een objectieve theorie op te kunnen stellen.

Ondanks de moeilijke generaliseerbaarheid van een enkele case study, zijn er toch verschillende scenario's om hiervoor te kiezen. De drie voornaamste scenario's zijn volgens Yin indien de case een kritische test is van een bestaande theorie, een zeldzame of unieke gebeurtenis is of de case aan een openbaar doel bijdraagt. Rowley (2002) merkt ook op dat een enkele case study kan dienen als inleiding of test voor een reeks van case studies. Gezien de, in vergelijking met de literatuur, unieke combinatie van frameworks in deze studie, is het toepassen van een enkele, inleidende case study mogelijk om eerste inzichten te kunnen verschaffen en het artefact te testen. Op basis van de resultaten kunnen in de toekomst bijkomende case studies uitgevoerd worden.

4. Mapping COBIT – ISO 9001

Dit hoofdstuk bestaat uit vier delen. Allereerst zal er een overzicht geschetst worden van de methoden waarop bestaande mappings tussen het COBIT framework en ISO normen opgesteld zijn. Daarna zal de aanpak van het opstellen van de mapping uit dit onderzoek verder besproken worden. Vervolgens zullen de resultaten besproken worden van de mapping die in deze studie opgesteld werd tussen het COBIT framework en de ISO 9001 norm. Tenslotte zullen enkele verschillen en gelijkenissen tussen deze mapping en de mapping van Bürgy (2016) gegeven worden.

4.1 Een overzicht van ontwerpen

Zoals in de methodologie beschreven, zal er eerst een overzicht gemaakt worden van de methoden waarop bestaande mappings tussen COBIT en ISO normen opgesteld zijn. Om te beginnen heeft Oparaugo (2016) een mapping ontworpen tussen COBIT, de ISO 27001 norm in verband met informatiebeveiliging uit 2013 en IT governance aandachtsgebieden. Deze mapping werd tot stand gebracht door de COBIT processen te linken met een aandachtsgebied en hier een prioriteit (primair of secundair) aan te geven. Het doel was om IT governance te integreren met de algemene bedrijfsgovernance. Uiteindelijk wordt er een percentage bekomen die de mate van overeenkomst tussen het COBIT proces en de ISO norm weergeeft. Von Solms (2005) vergelijkt de doelstellingen van elk COBIT proces met de doelstellingen van de ISO 17799 norm omtrent informatiebeveiliging. Overeenkomstige doelstellingen tussen de twee worden vervolgens met elkaar gemapt op basis van tekstuele overeenkomsten met als doel de twee frameworks met elkaar te synchroniseren. Om een overzicht te schetsen hoe beide frameworks samen kunnen werken om effectievere en efficiëntere interne controle te kunnen garanderen, hebben Lin et al. (2012) hebben een mapping uitgevoerd tussen ISO 27002 in verband met informatiebeveiliging en COBIT. Ze hebben dit gedaan door de secties uit de ISO norm te matchen met de processen uit COBIT. Indien er een match gevonden werd, werd dit op binaire wijze aangeduid waardoor een sectie dus op vlak van inhoud overeen (1) kwam of niet (0) met het COBIT proces. Ook het ITGI en OGC (2005 & 2008) stellen een mapping op tussen COBIT en ISO 27002, alsook tussen COBIT en ISO 17799. In beide werken werden de controle objectieven van het COBIT framework gemapt op basis van inhoud met de subsecties van de ISO normen. Hun doel was om opnieuw begeleiding te bieden bij het integreren van de frameworks. Sheikhpour (2012) heeft elk COBIT proces gemapt met een doelstelling uit de ISO 27001 norm met als doel het verlagen van de kosten omtrent IT risico en beveiliging en het verlagen van het algemeen risico niveau. Tenslotte heeft Bürgy (2016) een mapping opgesteld tussen ISO 9001 en COBIT 5. Deze mapping werd opgesteld tussen de COBIT processen en een ISO 9001 procesmodel dat was opgesteld op basis van de relevante processen die in een ISO 9001 gecertificeerd bedrijf terug te vinden waren. Bürgy beschrijft echter het opstellen van dit procesmodel niet. Voor elk COBIT proces werd de mate van overeenkomst met het ISO proces met behulp van een percentage weergegeven. Tabel 8 geeft een overzicht van de mappings besproken in deze sectie.

Tabel 8: Inhoudelijk overzicht van de mappings uit geraadpleegde werken

Auteur(s)	Frameworks	Doel	Weergave overeenkomst	Granulariteit
Oparaugo (2016)	COBIT 4.1 IT Governance focus areas ISO 27001	Integreren IT governance en bedrijfsgovernance	Prioriteit aanduiden (Primair of secundair) Percentuele weergave van overeenkomst tussen COBIT en ISO 27001.	34 COBIT 4.1 processen 5 ITG focus areas 18 ISO control domains
Von Solms (2005)	COBIT 4.1 ISO 17799	De co-existentie en het complementair gebruik nagaan	Gelijkaardige beschrijvingen tussen beide frameworks worden langs elkaar gezet.	COBIT 4.1 DCO's ISO subobjectives
Lin et al. (2012)	COBIT 4.1 ISO 27002	De overeenkomsten en mate van aanvulling tussen de frameworks nagaan om een sterkere interne controle te bekomen.	Aanvinken in een tabel waar de componenten van de frameworks overeenkomen op basis van de beschrijvingen	133 subsecties van ISO 27002 4 COBIT 4.1 domeinen
ITGI & OGC (2005 & 2008)	COBIT 4.1 ISO 17799 ISO 27002	Een overzicht schetsen hoe een high level framework als COBIT geïntegreerd kan worden met de gedetailleerde ISO norm.	Tabel met een ISO component en de overeenkomstige COBIT component(en) op dezelfde rij.	ISO 27002 subsecties COBIT 4.1 control objectives
Sheikhpour (2012)	COBIT 4.0 ISO 27001	Het complementair gebruik van een algemeen framework zoals COBIT en een meer gedetailleerd framework zoals ISO 27001 op vlak van informatiebeveiliging nagaan.	Tabel met een COBIT proces en de overeenkomstige ISO control objectives op dezelfde rij.	34 COBIT 4.0 processen ISO 27001 Control objectives
Bürgy (2016)	COBIT 5 ISO 9001	De overeenkomsten tussen COBIT 5 en ISO 9001 aankaarten en het testen van een ISO 9001 procesmodel.	Tabel met een ISO proces uit het procesmodel en de overeenkomstige COBIT processen op dezelfde rij. Per COBIT proces wordt er bijkomend een percentage van overeenkomst gegeven.	11 zelf geformuleerde ISO processen 37 COBIT 5 processen

4.2 Het ontwerp van het huidige onderzoek

In dit onderzoek werd een mapping opgesteld tussen COBIT 5 en de ISO 9001 norm uit 2015. Deze twee frameworks zijn recenter dan de meesten uit de geanalyseerde werken beschreven in de vorige sectie. Om te beginnen werd de granulariteit van de ISO norm bepaald. Hiervoor werd er beslist om te werken op sectie niveau (e.g. sectie 4.1, 5.2, 7.5, …). Op deze manier werd de ISO norm opgedeeld in 28 secties die mogelijk gemapt konden worden met het COBIT framework. Zo is de mapping enerzijds gedetailleerder dan op het niveau van de 7 hoofdstukken en anderzijds overzichtelijker dan op subsectie (e.g. 4.1.1) niveau. Het COBIT framework werd opgedeeld in de 37 processen en per proces werden de beschrijving en het doel, samen met de management practices per proces mee in rekening genomen. De gedetailleerde beschrijvingen van de management practices werden echter niet verder in detail opgenomen aangezien de mapping op procesniveau plaatsvindt. Een overzicht van de beschrijvingen van zowel de ISO secties als de COBIT processen waarmee de mapping gemaakt werd kan teruggevonden worden in bijlage 7.

De mapping zelf bestaat uit twee delen. Allereerst wordt er per ISO sectie weergegeven voor welke COBIT processen een overeenkomst gevonden wordt. Uit de ISO norm zijn de secties uit de hoofdstukken 4 tot en met 10 opgenomen in de mapping. De inleiding en de eerste drie korte hoofdstukken zijn niet mee opgenomen omdat deze algemene informatie over de norm zelf bevatten. Ten tweede werd deze mapping herschikt zodat er per COBIT proces een overzicht gegeven wordt welke ISO secties overeenkomen. Op deze manier kan er van zowel COBIT als ISO vertrokken worden, afhankelijk van de behoeften van de gebruiker. Een mapping werd bepaald door de ISO sectie langs de beschrijving van het COBIT proces te leggen (bijlage 7) en de inhoud van de twee te vergelijken. Indien de inhoud overeenkwam, werd de mapping gemaakt. Om te bepalen of de inhoud overeenkwam, werd er gekeken naar de essentie van het proces of sectie en werd er vaak op basis van een overeenkomst tussen kernwoorden bepaald of er een overeenkomst was of niet. Wanneer beide beschrijvingen deze kernwoorden of synoniemen ervan in een gelijkaardige context gebruikten, waarmee duidelijk werd of de inhoud overeen kwam, werd de mapping gemaakt. Omdat COBIT een breder framework is en omdat het uiteindelijke doel een integratie met de ISO norm is, werd de context van de beschrijving van de COBIT processen geïnterpreteerd alsof ze gelinkt konden worden met de ISO norm. Zo werd er bijvoorbeeld wanneer er in een COBIT proces over een framework gesproken werd, de assumptie gemaakt dat hier de ISO norm in verband met kwaliteitsmanagement onder verstaan kan worden.

Om te bepalen welke COBIT processen in aanmerking kwamen voor een mapping met een bepaalde sectie uit de ISO norm werden er verschillende methoden uitgeprobeerd. Als eerste methode werd er na het lezen van een ISO sectie een onderscheid gemaakt tussen de vijf COBIT domeinen (EDM, APO, BAI, DSS, MEA). Op basis van de essentie van de sectie werd deze toegewezen aan een of meerdere van deze vijf domeinen om vervolgens dieper binnen deze domeinen op zoek te gaan naar de werkelijke processen die gemapt konden worden. Tijdens het mappen zelf is echter gebleken dat enerzijds de secties regelmatig met vier of vijf van deze domeinen gemapt kon worden waardoor het filteren zo goed als teniet gedaan werd en anderzijds dat er inconsistenties de mapping binnenslopen en dat er vaak nog andere processen, die buiten de toegewezen domeinen lagen, met de sectie gemapt konden worden.

Stel bijvoorbeeld dat op basis van de inhoud van een bepaalde sectie uit de ISO norm, voorspeld werd dat deze sectie gemapt zou kunnen worden met processen uit de domeinen *Align, Plan and Organise* of *Evaluate, Direct and Monitor*. Op basis van deze voorspelling werden de beschrijvingen van de processen binnen deze domeinen (dus APO01 – APO13 en EDM01 – EDM05) vergeleken met de beschrijving van de ISO sectie en indien de beschrijvingen overeenkwamen, werd er een mapping tussen deze ISO sectie en dit COBIT proces gemaakt. Door eerst te filteren op de COBIT domeinen, werd er gehoopt tijd te besparen om de secties uit de ISO norm met de COBIT processen te linken. Tijdens het uitvoeren van deze methode werd er gemerkt dat een ISO sectie regelmatig bij 4 of 5 van deze COBIT domeinen zou kunnen thuishoren, waardoor het effect van het filteren en de tijdwinnende factor teniet gedaan werden. Om daarnaast de correctheid van het filteren op de COBIT domeinen te controleren, werd regelmatig de ISO sectie vergeleken met een COBIT proces dat niet bij een van de voorspelde domeinen thuishoorde. Dus in het geval van het voorbeeld met processen uit de domeinen BAI, DSS en MEA. Hieruit is echter gebleken dat er regelmatig toch nog mappings mogelijk waren tussen deze ISO sectie en een van deze domeinen, waarvan initieel voorspeld werd dat er geen mappings tussen deze twee zouden voorkomen. Op basis hiervan werd geconcludeerd dat het op voorhand voorspellen bij welk COBIT domein de ISO sectie zou kunnen thuishoren een inefficiënte methode was, waarop beslist werd om een andere methode toe te passen.

Om deze redenen werd er dus besloten om het filteren achterwegen te laten. Uiteindelijk werd voor elke ISO sectie, alle 37 COBIT processen en hun beschrijvingen overlopen. Indien de beschrijvingen overeenkwamen, werd de mapping gemaakt tussen die ISO sectie en dat COBIT proces. Op deze manier werden alle ISO secties met alle 37 COBIT processen vergeleken om er zeker van te zijn dat geen potentiële mappings gemist werden. Ter controle werden de gemaakte mappings achteraf nogmaals nagekeken door de beschrijvingen van de ISO sectie en het gemapte COBIT proces opnieuw door te nemen om er zeker van te zijn dat de mapping klopte. Twijfel gevallen of mappings die uiteindelijk niet correct waren, werden vervolgens uit de mapping verwijdert.

Om de uitgevoerde methode concreet aan te tonen, wordt bij wijze van voorbeeld hieronder twee mappings tussen ISO sectie *4.1 Inzicht in de organisatie en haar context* en twee van de gemapte COBIT processen hieronder uitgelegd.

ISO 9001

4.1 Inzicht in de organisatie en haar context: De organisatie moet externe en interne belangrijke punten vaststellen die relevant zijn voor haar doel en strategische richting en die haar vermogen beïnvloeden om de beoogde resultaten van haar kwaliteitsmanagementsysteem te behalen.

De organisatie moet informatie over deze externe en interne belangrijke punten monitoren en beoordelen.

COBIT

EDM01: Analyseer en formuleer de vereisten voor het bestuur van bedrijfs-IT en zorg voor effectieve ondersteunende structuren, principes, processen en werkwijzen met duidelijke verantwoordelijkheden en bevoegdheden om de missie, doelen en doelstellingen van het bedrijf te bereiken.

MEA01: Verzamel, valideer en evalueer bedrijfs-, IT- en procesdoelen en statistieken. Houd er rekening mee dat processen presteren tegen overeengekomen prestatienormen en conformiteitsdoelen en statistieken en bieden rapportage die systematisch en tijdig is.

Sectie 4.1 stelt dat een organisatie externe en interne punten moet vaststellen die het doel en strategie van de onderneming bevorderen. Deze punten worden gelinkt met de vereisten die volgens proces EDM01 moeten opgesteld worden om missie, doel en doelstellingen te bereiken. Verder stelt sectie 4.1 dat deze punten gemonitord en beoordeeld moeten worden. Deze vereiste wordt gelinkt met proces MEA01 omtrent het valideren en evalueren van bedrijfsdoelen. Op deze manier werden alle ISO secties met alle COBIT processen vergeleken en indien ze overeenkwamen, werd de mapping gemaakt.

4.3 De mapping

In tabellen 9 en 10 worden de resultaten weergegeven van de mapping. Tabel 9 geeft voor elke ISO sectie uit het bijhorende hoofdstuk de overeenkomstige COBIT processen weer. Merk op dat de nummering van de hoofdstukken uit de ISO norm behouden zijn om verwijzingen voor gebruikers te vergemakkelijken. Uit de mapping blijkt dat iedere sectie minstens één COBIT proces heeft dat overeenkomt met haar beschrijving. De meeste overeenkomsten werden gevonden bij secties *7.1 Middelen*, *8.2 Eisen voor producten en diensten, 8.3 Ontwerp en ontwikkeling van producten en diensten, 8.5 Productie en het leveren van diensten, 9.1 Monitoren, meten, analyseren en evalueren* en *10.1 Vastellen verbeteringen* die elk met meer dan 14 COBIT processen gemapt konden worden. Het minst aantal overeenkomsten werd gevonden tussen *7.4 Communicatie en 8.6 Vrijgave van producten en diensten*. Deze secties zijn zeer toegespitsts op het kwaliteitsmanagementsysteem, waardoor ze ook enkel met het proces *APO11 Manage Quality* zijn gemapt. Wanneer er per hoofdstuk gekeken wordt, blijkt hoofdstuk *8. Uitvoering* de meeste overeenkomsten te hebben met de COBIT processen met bijna dubbel zoveel mappings als de tweede meeste.

Tabel 10 geeft voor elk COBIT proces de bijhorende secties uit de ISO norm waarvoor een overeenkomst gevonden werd. Ook hier blijkt elk COBIT proces minstens met één ISO sectie gemapt te kunnen worden. De meeste overeenkomsten werden gevonden bij processen *APO01 Manage the IT Management Framework, APO11 Manage Quality* en *MEA01 Monitor, Evaluate and Assess Performance and Conformance* die elk met meer als 10 secties uit de ISO norm gemapt werden. APO11 werd zelfs met 23 secties gemapt. Het minst aantal overeenkomsten werd gevonden bij het proces *APO03 Manage Enterprise Architecture* dat enkel een overeenkomst vond bij sectie *7.1 Middelen*. Wanneer er per domein gekeken wordt, blijkt *Align, Plan and Organise* de meeste overeenkomsten te hebben. Dit domein bevat met 13 processen de meeste processen van de vijf domeinen, maar ook het proces *APO11 Manage Quality* dus is het niet verwonderlijk dat voor dit domein de meeste overeenkomsten gevonden worden. Maar zelfs wanneer de overeenkomsten van *APO11* niet meegerekend zouden worden, heeft het domein *Align, Plan and Organise* nog steeds de meeste mappings.

Op basis van deze resultaten kunnen overeenkomsten tussen de COBIT processen en de secties uit de ISO norm, samen met de hoofdstukken/domeinen geïdentificeerd worden. Deze kunnen voor organisaties die een van deze twee frameworks reeds in gebruik hebben een indicatie geven in welke mate ze reeds voldoen aan het ander. In het resterende deel van dit onderzoek zal deze mapping gedemonstreerd worden om na te gaan in welke mate deze overeenkomsten in de praktijk gelden.

4.4 De vergelijking met de mapping van Bürgy

Omdat Bürgy een mapping voorziet van dezelfde twee frameworks, worden in deze sectie de verschillen en gelijkenissen tussen beide mappings in kaart gebracht.

Het voornaamste verschil is dat Bürgy de COBIT processen mapt met een procesmodel bestaande uit 11 management processen gebaseerd op processen van een ISO gecertificeerd, Zwitserse bedrijf en niet direct met de secties uit de ISO norm. Ook wordt elk COBIT proces hoogstens één maal gemapt met een proces uit het procesmodel, terwijl in de mapping uit het huidige onderzoek een COBIT proces gemapt wordt met elke sectie uit de ISO norm waaraan voldaan wordt door het implementeren van dit proces. Daarnaast geeft Bürgy de mapping in één richting, namelijk vanuit het procesmodel naar de COBIT processen. Aangezien elk COBIT proces slechts eenmaal gemapt wordt zou de andere richting echter weinig meerwaarde bieden. De mapping uit het huidige onderzoek voorziet wel een mapping in beide richtingen zodat makkelijk vertrokken kan worden vanuit het framework dat de gebruiker geïmplementeerd heeft. Ook worden niet alle COBIT processen mee opgenomen in de mapping van Bürgy. Initieel worden alle 37 COBIT processen verdeeld onder de processen uit het procesmodel maar voor de uiteindelijke mapping wordt hier een deel van uitgefilterd omdat de overeenkomst te laag zou zijn. Uiteindelijk worden 24 van de 37 COBIT processen behouden.

Van de processen die eruit gefilterd werden, is het treffend dat *APO11 Manage quality* hierbij zit. In de huidige mapping is dit zelfs het proces dat met het meeste aantal secties uit de ISO norm gemapt werd. In een mapping met een norm die draait om kwaliteitsmanagement, zou men toch verwachten dat een proces genaamd *Manage quality* voldoende overeenkomsten toont om in de mapping opgenomen te worden. APO11 werd origineel gemapt met het proces *Maintain IT-Processes* maar werd weggelaten omdat er niet genoeg overeenkomst gevonden werd op vlak van input, output, doelstellingen en activiteiten. De redenen waarom APO11 met *Maintain IT-Processes* gemapt werd, of elk ander COBIT proces met een proces uit het proces model, wordt in het werk van Bürgy niet gespecifieerd.

Een aantal van de processen uit het procesmodel zijn voornamelijk IT gericht en het is merkbaar dat deze afgeleid zijn van de processen van een IT gerichte onderneming. Dit heeft enerzijds als gevolg dat het makkelijker is om deze te mappen met het COBIT framework, anderzijds limiteert dit het gebruik van deze mapping voor bedrijven wiens processen niet dermate IT gericht zijn. Daarbij is de ISO norm zelf geen IT gerichte norm maar een kwaliteitsnorm. Daarom wordt in de huidige mapping de nadruk gelegd op kernwoorden zoals kwaliteit, monitoren, middelen, klantgerichtheid of continu verbeteren om de ISO norm te mappen met het COBIT framework. In de processen uit het procesmodel die niet dermate IT gericht zijn, zijn dit soort kernwoorden echter wel terug te vinden en kan de link met de ISO norm makkelijker begrepen worden. Het zou bijvoorbeeld niet verwonderlijk zijn als het proces *Solution Development & Deployment* bij het Zwitsers bedrijf opgesteld is geweest met hoofdstuk *10. Verbetering* uit de ISO norm in het achterhoofd. De COBIT processen die Bürgy mapt met dit ISO proces (*Solution Development & Deployment)*, worden in de mapping uit het huidige onderzoek ook allemaal gemapt met secties 10.1 en 10.2 uit de ISO norm.

Wanneer de processen uit het procesmodel duidelijk gelinkt kunnen worden aan een hoofdstuk of secties uit de ISO norm, zijn er overeenkomsten terug te vinden tussen de huidige mapping en de mapping van Bürgy. Wanneer de processen uit het procesmodel te IT gericht zijn en te nauw aansluiten bij de onderneming waar ze op gebaseerd zijn, is het moeilijker om een overeenkomst tussen de mapping van Bürgy en de mapping uit het huidige onderzoek te vinden. Het grote voordeel van de mapping uit het huidige onderzoek is dan ook dat beide frameworks als basis genomen worden voor het opstellen van de mapping, waardoor de mapping uitgevoerd kan worden door elk type onderneming. De enige vereiste om de mapping uit het huidige onderzoek te kunnen gebruiken is namelijk dat de gebruiker COBIT en ISO 9001 uit 2015 wil samen wil implementeren.

Tabel 9: Mapping van de secties uit de ISO norm met de COBIT processen.

ISO Sectie	COBIT Proces
4. Context van de organisatie	
4.1 Inzicht in de organisatie en haar context.	EDM01 APO02 APO11 MEA01 MEA03
4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden.	EDM01 EDM05 APO05 APO06 APO09 APO11 BAI02 MEA02 MEA03
4.3 Het toepassingsgebied van het kwaliteitsmanagementsysteem vaststellen.	EDM01 APO01 APO11
4.4 Kwaliteitsmanagementsystemen en de processen ervan	APO01 APO04 APO11 DSS06 MEA01
5. Leiderschap	
5.1 Leiderschap en betrokkenheid	EDM01 EDM02 EDM03 EDM04 EDM05 APO01 APO08 APO11 APO12 BAI02

5.2 Het kwaliteitsbeleid vaststellen en kenbaar maken	EDM01 EDM05 APO01 APO11 BAI02
5.3 Rollen, verantwoordelijkheden en bevoegdheden binnen de organisatie	EDM04 APO01 APO07 APO11
6. Planning	
6.1 Acties om risico's en kansen aan te pakken	EDM03 APO04 APO08 APO10 APO11 APO12 APO13 BAI02 DSS05 MEA02 MEA03
6.2 Kwaliteitsdoelstellingen en de planning om ze te bereiken	EDM01 APO01 APO11 BAI02 MEA01 MEA02
6.3 Planning van wijzigingen	BAI05 BAI06 BAI07 BAI10
7. Ondersteuning	
7.1 Middelen	EDM01 EDM04 APO01 APO03 APO06 APO07 APO10 APO11 BAI04 BAI08 BAI09 DSS06 MEA01 MEA02
7.2 Competentie	EDM04 APO07 APO10 APO11 BAI05

7.3 Bewustzijn	EDM05 APO01 APO07 APO11
7.4 Communicatie	APO11
7.5 Gedocumenteerde informatie	EDM05 APO05 APO09 APO11 BAI01 BAI06 BAI10 DSS05 DSS06 MEA01
8. Uitvoering	
8.1 Operationele planning en beheersing	APO05 APO11 BAI01 BAI02 BAI09 DSS01 DSS06 MEA01
8.2 Eisen voor producten en diensten	EDM02 EDM05 APO05 APO06 APO08 APO09 APO11 BAI01 BAI02 BAI04 BAI09 DSS02 DSS03 DSS04 MEA01 MEA03
8.3 Ontwerp en ontwikkeling van producten en diensten	EDM02 EDM04 APO05 APO09 APO10 APO11 BAI02 BAI03 BAI06 BAI07 BAI10

	DSS01 MEA01 MEA03
8.4 Beheersing van extern geleverde processen, producten en diensten	APO02 APO10 DSS06 MEA03
8.5 Productie en het leveren van diensten	EDM02 EDM04 EDM05 APO07 APO10 APO11 BAI06 BAI10 DSS01 DSS02 DSS03 DSS04 DSS06 MEA01 MEA02
8.6 Vrijgave van producten en diensten	APO11
8.7 Beheersing van afwijkende outputs	BAI03 DSS02 DSS03 DSS04
9. Evaluatie van de prestaties	
9.1 Monitoren, meten, analyseren en evalueren	EDM01 EDM02 EDM03 EDM04 EDM05 APO04 APO05 APO10 APO11 APO12 APO13 BAI01 BAI07 MEA 01 MEA 02 MEA 03
9.2 Interne audit	APO09 APO11 APO13 BAI01 BAI03 BAI05 BAI09

	BAI10
9.3 Directiebeoordeling	EDM01 EDM02 EDM03 EDM04 EDM05 APO05 BAI05 MEA01 MEA02 MEA03
10. Verbetering	
10.1 Vaststellen verbeteringen	EDM02 APO01 APO04 APO05 APO08 APO11 BAI01 BAI03 BAI05 BAI06 BAI08 DSS02 DSS03 MEA01 MEA02
10.2 Afwijkingen en corrigerende maatregelen	BAI02 BAI03 BAI06 BAI07 DSS02 DSS03 DSS04
10.3 Continue verbetering	APO01 APO08 APO11 APO13 DSS02

Tabel 10: Mapping tussen de COBIT processen en de secties uit de ISO norm

COBIT Proces	**ISO Sectie**
Evaluate, Direct and Monitor	
EDM01: Ensure Governance Framework Setting and Maintenance	4.1 Inzicht in de organisatie en haar context. 4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden.

	4.3 Het toepassingsgebied van het kwaliteitsmanagementsysteem vaststellen. 5.1 Leiderschap en betrokkenheid 5.2 Het kwaliteitsbeleid vaststellen en kenbaar maken 6.2 Kwaliteitsdoelstellingen en de planning om ze te bereiken 7.1 Middelen 9.1 Monitoren, meten, analyseren en evalueren 9.3 Directiebeoordeling
EDM02: Ensure Benefits Delivery	5.1 Leiderschap en betrokkenheid 8.2 Eisen voor producten en diensten 8.3 Ontwerp en ontwikkeling van producten en diensten 8.5 Productie en het leveren van diensten 9.1 Monitoren, meten, analyseren en evalueren 9.3 Directiebeoordeling 10.1 Vaststellen verbeteringen
EDM03: Ensure Risk Optimisation	5.1 Leiderschap en betrokkenheid 6.1 Acties om risico's en kansen aan te pakken 9.1 Monitoren, meten, analyseren en evalueren 9.3 Directiebeoordeling
EDM04: Ensure Resource Optimisation	5.1 Leiderschap en betrokkenheid 5.3 Rollen, verantwoordelijkheden en bevoegdheden binnen de organisatie 7.1 Middelen 7.2 Competentie 8.3 Ontwerp en ontwikkeling van producten en diensten 8.5 Productie en het leveren van diensten 9.1 Monitoren, meten, analyseren en evalueren 9.3 Directiebeoordeling

EDM05: Ensure Stakeholder Transparency	4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden 5.1 Leiderschap en betrokkenheid 5.2 Het kwaliteitsbeleid vaststellen en kenbaar maken 7.3 Bewustzijn 7.5 Gedocumenteerde informatie 8.2 Eisen voor producten en diensten 8.5 Productie en het leveren van diensten 9.1 Monitoren, meten, analyseren en evalueren 9.3 Directiebeoordeling
Align, Plan and Organise	
APO01: Manage the IT management framework	4.3 Het toepassingsgebied van het kwaliteitsmanagementsysteem vaststellen 4.4 Kwaliteitsmanagementsystemen en de processen ervan 5.1 Leiderschap en betrokkenheid 5.2 Het kwaliteitsbeleid vaststellen en kenbaar maken 5.3 Rollen, verantwoordelijkheden en bevoegdheden binnen de organisatie 6.2 Kwaliteitsdoelstellingen en de planning om ze te bereiken 7.1 Middelen 7.3 Bewustzijn 10.1 Vaststellen verbeteringen 10.3 Continue verbetering
APO02: Manage strategy	4.1 Inzicht in de organisatie en haar context. 8.4 Beheersing van extern geleverde processen, producten en diensten
APO03: Manage enterprise architecture	7.1 Middelen
APO04: Manage innovation	4.4 Kwaliteitsmanagementsystemen en de processen ervan 6.1 Acties om risico's en kansen aan te pakken

	9.1 Monitoren, meten, analyseren en evalueren 10.1 Vaststellen verbeteringen
APO05: Manage portfolio	4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden 7.5 Gedocumenteerde informatie 8.1 Operationele planning en beheersing 8.2 Eisen voor producten en diensten 8.3 Ontwerp en ontwikkeling van producten en diensten 9.1 Monitoren, meten, analyseren en evalueren 9.3 Directiebeoordeling 10.1 Vaststellen verbeteringen
APO06: Manage budget and costs	4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden 7.1 Middelen 8.2 Eisen voor producten en diensten
APO07: Manage human resources	5.3 Rollen, verantwoordelijkheden en bevoegdheden binnen de organisatie 7.1 Middelen 7.2 Competentie 7.3 Bewustzijn 8.5 Productie en het leveren van diensten
APO08: Manage relationships	5.1 Leiderschap en betrokkenheid 6.1 Acties om risico's en kansen aan te pakken 8.2 Eisen voor producten en diensten 10.1 Vaststellen verbeteringen 10.3 Continue verbetering
APO09: Manage service agreements	4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden. 7.5 Gedocumenteerde informatie 8.2 Eisen voor producten en diensten 8.3 Ontwerp en ontwikkeling van producten en diensten

	9.2 Interne audit
APO10: Manage suppliers	6.1 Acties om risico's en kansen aan te pakken 7.1 Middelen 7.2 Competentie 8.3 Ontwerp en ontwikkeling van producten en diensten 8.4 Beheersing van extern geleverde processen, producten en diensten 8.5 Productie en het leveren van diensten 9.1 Monitoren, meten, analyseren en evalueren
APO11: Manage quality	4.1 Inzicht in de organisatie en haar context 4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden 4.3 Het toepassingsgebied van het kwaliteitsmanagementsysteem vaststellen 4.4 Kwaliteitsmanagementsystemen en de processen ervan 5.1 Leiderschap en betrokkenheid 5.2 Het kwaliteitsbeleid vaststellen en kenbaar maken 5.3 Rollen, verantwoordelijkheden en bevoegdheden binnen de organisatie 6.1 Acties om risico's en kansen aan te pakken 6.2 Kwaliteitsdoelstellingen en de planning om ze te bereiken 7.1 Middelen 7.2 Competentie 7.3 Bewustzijn 7.4 Communicatie 7.5 Gedocumenteerde informatie 8.1 Operationele planning en beheersing 8.2 Eisen voor producten en diensten 8.3 Ontwerp en ontwikkeling van producten en diensten

	8.5 Productie en het leveren van diensten 8.6 Vrijgave van producten en diensten 9.1 Monitoren, meten, analyseren en evalueren 9.2 Interne audit 10.1 Vaststellen verbeteringen 10.3 Continue verbetering
APO12: Manage risk	5.1 Leiderschap en betrokkenheid 6.1 Acties om risico's en kansen aan te pakken 9.1 Monitoren, meten, analyseren en evalueren
APO13: Manage security	6.1 Acties om risico's en kansen aan te pakken 9.1 Monitoren, meten, analyseren en evalueren 9.2 Interne audit 10.3 Continue verbetering
Build, Acquire and Implement	
BAI01: Manage programmes and projects	7.5 Gedocumenteerde informatie 8.1 Operationele planning en beheersing 8.2 Eisen voor producten en diensten 9.1 Monitoren, meten, analyseren en evalueren 9.2 Interne audit 10.1 Vaststellen verbeteringen
BAI02: Manage requirements definition	4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden 5.1 Leiderschap en betrokkenheid 5.2 Het kwaliteitsbeleid vaststellen en kenbaar maken 6.1 Acties om risico's en kansen aan te pakken 6.2 Kwaliteitsdoelstellingen en de planning om ze te bereiken 8.1 Operationele planning en beheersing 8.2 Eisen voor producten en diensten

	8.3 Ontwerp en ontwikkeling van producten en diensten 10.2 Afwijkingen en corrigerende maatregelen
BAI03: Manage solutions identification and build	8.3 Ontwerp en ontwikkeling van producten en diensten 8.7 Beheersing van afwijkende outputs 9.2 Interne audit 10.1 Vaststellen verbeteringen 10.2 Afwijkingen en corrigerende maatregelen
BAI04: Manage availability and capacity	7.1 Middelen 8.2 Eisen voor producten en diensten
BAI05: Manage organisational change enablement	6.3 Planning van wijzigingen 7.2 Competentie 9.2 Interne audit 9.3 Directiebeoordeling 10.1 Vaststellen verbeteringen
BAI06: Manage changes	6.3 Planning van wijzigingen 7.5 Gedocumenteerde informatie 8.3 Ontwerp en ontwikkeling van producten en diensten 8.5 Productie en het leveren van diensten 10.1 Vaststellen verbeteringen 10.2 Afwijkingen en corrigerende maatregelen
BAI07: Manage change acceptance and transitioning	6.3 Planning van wijzigingen 8.3 Ontwerp en ontwikkeling van producten en diensten 9.1 Monitoren, meten, analyseren en evalueren 10.2 Afwijkingen en corrigerende maatregelen
BAI08: Manage knowledge	7.1 Middelen 10.1 Vaststellen verbeteringen
BAI09: Manage assets	7.1 Middelen

	8.1 Operationele planning en beheersing 8.2 Eisen voor producten en diensten 9.2 Interne audit
BAI10: Manage configuration	6.3 Planning van wijzigingen 7.5 Gedocumenteerde informatie 8.3 Ontwerp en ontwikkeling van producten en diensten 8.5 Productie en het leveren van diensten 9.2 Interne audit
Deliver, Service and Support	
DSS01: Manage operations	8.1 Operationele planning en beheersing 8.3 Ontwerp en ontwikkeling van producten en diensten 8.5 Productie en het leveren van diensten
DSS02: Manage service requests and incidents	8.2 Eisen voor producten en diensten 8.5 Productie en het leveren van diensten 8.7 Beheersing van afwijkende outputs 10.1 Vaststellen verbeteringen 10.2 Afwijkingen en corrigerende maatregelen 10.3 Continue verbetering
DSS03: Manage problems	8.2 Eisen voor producten en diensten 8.5 Productie en het leveren van diensten 8.7 Beheersing van afwijkende outputs 10.1 Vaststellen verbeteringen 10.2 Afwijkingen en corrigerende maatregelen
DSS04: Manage continuity	8.2 Eisen voor producten en diensten 8.5 Productie en het leveren van diensten 8.7 Beheersing van afwijkende outputs 10.2 Afwijkingen en corrigerende maatregelen
DSS05: Manage security services	6.1 Acties om risico's en kansen aan te pakken 7.5 Gedocumenteerde informatie

DSS06: Manage business process controls	4.4 Kwaliteitsmanagementsystemen en de processen ervan 7.1 Middelen 7.5 Gedocumenteerde informatie 8.1 Operationele planning en beheersing 8.4 Beheersing van extern geleverde processen, producten en diensten 8.5 Productie en het leveren van diensten
Monitor, Evaluate and Assess	
MEA01: Monitor, evaluate and assess performance and conformance	4.1 Inzicht in de organisatie en haar context 4.4 Kwaliteitsmanagementsystemen en de processen ervan 6.2 Kwaliteitsdoelstellingen en de planning om ze te bereiken 7.1 Middelen 7.5 Gedocumenteerde informatie 8.1 Operationele planning en beheersing 8.2 Eisen voor producten en diensten 8.3 Ontwerp en ontwikkeling van producten en diensten 8.5 Productie en het leveren van diensten 9.3 Directiebeoordeling 10.1 Vaststellen verbeteringen
MEA02: Monitor, evaluate and assess the system of internal control	4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden 6.1 Acties om risico's en kansen aan te pakken 6.2 Kwaliteitsdoelstellingen en de planning om ze te bereiken 7.1 Middelen 8.5 Productie en het leveren van diensten 9.3 Directiebeoordeling 10.1 Vaststellen verbeteringen
MEA03: Monitor, evaluate and assess compliance with external requirements	4.1 Inzicht in de organisatie en haar context.

	4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden 6.1 Acties om risico's en kansen aan te pakken 8.2 Eisen voor producten en diensten 8.3 Ontwerp en ontwikkeling van producten en diensten 8.4 Beheersing van extern geleverde processen, producten en diensten 9.3 Directiebeoordeling

5. De VITO Case Study

Nu de mapping ontworpen is, zal deze in dit deel getoetst worden bij de IT afdeling van een onderneming. Eerst zal er een overzicht geschetst worden over het bedrijf zelf en daarna zullen een aantal processen in beeld gebracht worden waarop de mapping toegepast kan worden. Tenslotte zal de mapping getest worden aan de hand van deze processen die de afdeling geïmplementeerd heeft. Op die manier zal de potentiële meerwaarde van de mapping nagegaan worden en geconcludeerd kunnen worden of de ontworpen mapping daadwerkelijk een meerwaarde te bieden heeft voor deze onderneming.

5.1 Inleiding Case Study

Voor de case study zal er samengewerkt worden met het Vlaamse Instelling voor Technologisch Onderzoek (VITO). VITO is een onafhankelijke onderzoeksorganisatie dat technologische oplossingen uitwerkt en wetenschappelijk onderbouwde adviezen geeft aan bedrijven en de Vlaamse overheid rond maatschappelijke domeinen. Op dit moment voldoet VITO aan de eisen van de ISO 9001-norm uit 2008 maar zou graag voldoen aan de recentere ISO-norm uit 2015 en hier een certificatie van behalen. VITO zou hieromtrent graag enkele processen en hun interacties in kaart brengen. Specifiek zal er samengewerkt worden met de informatica afdeling van VITO. De processen die in kaart gebracht dienen te worden, zijn gebaseerd op COBIT processen en zijn dus geschikt om de mapping tussen ISO en COBIT op te testen.

De informatica afdeling van VITO heeft als doel intern diensten en projecten uit te voeren ten voordele van de andere afdelingen binnen VITO. De afdeling bestaat uit vier teams:

- GON: Eindgebruiker ondersteuning, verantwoordelijk voor algemene ICT ondersteuning en het voorzien van PC's, laptops, licenties, …
- SNB: Systeem en netwerk beheer, verantwoordelijk voor het ICT netwerk en beveiliging enerzijds en server en opslagcapaciteit anderzijds.
- IAO: informatie, analyse en ontwikkeling, verantwoordelijk voor het ontwikkelen en beheren van VITO specifieke applicaties en het selecteren, implementeren en beheren van softwarepaketten.
- RAD: Research application development, verantwoordelijk voor web en applicatie ontwikkeling voor VITO bedrijfsprojecten.

De informatica afdeling werkt enerzijds aan projecten die van toepassing zijn voor het hele bedrijf en gebruikt worden door alle afdelingen en medewerkers, anderzijds wordt er ook gewerkt aan projecten voor specifieke afdelingen, zoals de HR afdeling. Deze zijn dus enkel van toepassing voor die afdeling.

5.1.1 De VITO bedrijfsdoelstellingen

VITO heeft, zoals COBIT dat voorstelt, voor zichzelf 12 bedrijfsdoelstellingen bepaald. Deze worden weergegeven in tabel 11.

Nr.	Bedrijfsdoelstelling	Nr.	Bedrijfsdoelstelling
1.	VITO is een onafhankelijke organisatie met financiële continuïteit.	7.	Uitmunten in haar onderzoeksdomeinen met een sterke internationale reputatie.
2.	Innovatie en technologisch onderzoek voeren dat leidt tot commerciële producten en spin-offs.	8.	Het toepassen van efficiënte en effectieve bedrijfsprocessen en ondersteunende diensten.
3.	Het nakomen van shareholder KPI's.	9.	Het aanschaffen van state-of-the-art infrastructuur.
4.	Het nakomen van externe wetten en regelgeving.	10.	Een motiverende en stimulerende werkomgeving voorzien.
5.	Innovatie en technologische oplossingen ontwikkelen om een duurzame maatschappij te bouwen.	11.	Uitstekende en gemotiveerde werknemers aannemen.
6.	VITO als betrouwbare en professionele partner die wetenschappelijk advies levert en innovatie in Vlaanderen en omgeving stimuleert.	12.	Een aantrekkelijke werkgever zijn.

TABEL 11: DE BEDRIJFSDOELSTELLINGEN VAN VITO

Het is duidelijk dat de bedrijfsdoelstellingen niet letterlijk zijn overgenomen uit COBIT maar specifiek voor VITO opgesteld zijn. COBIT raadt namelijk ook aan om zijn mapping als richtlijnen te gebruiken en dat elk bedrijf voor zichzelf de bedrijfsdoelstellingen moet uitmaken.

5.1.2 De VITO ICT doelstellingen

Op basis van de bedrijfsdoelstellingen werden 14 ICT gerelateerde doelstellingen opgesteld. Deze worden weergegeven in tabel 12

Ook de ICT doelstellingen zijn specifiek gemaakt voor VITO. Op basis van deze ICT doelstellingen werden een aantal processen geïdentificeerd die door VITO geïmplementeerd zullen worden.

Nr.	ICT doelstelling	Nr.	ICT doelstelling
1.	Een ICT strategie hanteren die relevant is voor al de departementen van VITO.	8.	Het ontwikkelen en implementeren van oplossingen voor effectieve interne en externe communicatie.
2.	State-of-the-art en agile applicaties ontwikkelingen die geïntegreerd zijn met de onderzoeksactiviteiten.	9.	Adequaat gebruik maken van de applicaties, informatie en technologische oplossingen.
3.	Betrouwbare en veilige oplossingen bedenken voor data- en documentbeheer in overeenstemming met de levenscyclus van het project.	10.	Het toepassen van de juiste en voldoende software.
4.	Een agile en veilige ICT infrastructuur aanschaffen die voldoet aan interne en externe noden.	11.	Transparante en goed beheerde operationele ICT diensten voorzien.
5.	Betrouwbare bedrijfsapplicaties implementeren die de interne processen en ondersteunende diensten sterk ondersteunen.	12.	De uitvoering van programma's en projecten moeten op tijd en binnen het budget gebeuren en aan eisen en kwaliteitsstandaarden voldoen.
6.	Het voorzien van management en operationele informatie en rapporten.	13.	Bekwaam en gemotiveerd ICT personeel aanwerven dat open staat voor nieuwe innovatieve toepassingen en oplossingen.
7.	Hulpmiddelen en technologieën voor het bevorderen van effectieve communicatie en samenwerking implementeren.	14.	Onderzoeken en investeren in nieuwe en opkomende technologieën.

TABEL 12: DE ICT DOELSTELLINGEN VAN VITO

5.1.3 VITO en de ISO 9001 certificatie

Zoals eerder in deze inleiding vermeld is VITO van plan om in de nabije toekomst een certificatie te behalen van de ISO 9001 norm uit 2015. Een onderdeel van dit plan is het implementeren van de vernoemde 13 COBIT processen. Dit is het ideale test scenario om de ontworpen mapping in de praktijk toe te passen. VITO wil namelijk weten in welke mate ze conform zijn aan de ISO norm indien ze deze 13 processen toepassen. Met behulp van de ontworpen mapping is het de bedoeling dat er een overzicht geschetst kan worden over welke processen aan welke eisen voldoen. Omdat de processen zelf in de volgende sectie uitgewerkt worden, kan er daarna nagegaan worden aan welke secties de processen van VITO letterlijk voldoen. Op deze manier kan er enerzijds nagegaan worden in welke mate de eerder ontworpen theoretische mapping overeenkomt met een mapping bestaande uit in de praktijk toegepaste COBIT processen en de ISO norm. Anderzijds kan er bij VITO het doel van de mapping nagegaan worden, namelijk of de theoretische mapping aan VITO een meerwaarde biedt bij het leveren van een overzicht in de mate dat er door de huidige processen aan de ISO norm wordt voldaan en welke processen eventueel geïmplementeerd kunnen worden om aan bijkomende eisen te voldoen.

5.2 Uitwerking processen

Nu er een beter beeld geschetst is van VITO als bedrijf, zal er in dit deel overgegaan worden tot het uitwerken van de processen. Eens deze processen in kaart gebracht zijn, kunnen ze dienen om de mapping op te testen.

5.2.1 VITO's IT managementprocessen

VITO heeft in het kader van hun doel om ISO 9001 gecertificeerd te geraken de volgende 13 IT managementprocessen geïdentificeerd om te implementeren:

1. Management of service portfolio
2. Management of budget and cost
3. Management of human resources
4. Management of business relationship
5. Management of supplier relationship
6. Management of ICT security
7. Management of programmes & projects
8. Management of availability
9. Management of capacity
10. Management of Software & hardware assets
11. Management of incidents
12. Management of request fulfillment
13. Management of identity & access

Volgens de ISO 9001 norm moet een organisatie een kwaliteitsmanagementsysteem inrichten, implementeren, onderhouden en continu verbeteren, met inbegrip van de benodigde processen en hun interacties, in overeenstemming met de eisen van de internationale norm (ISO,2015). Dit gaat van het definiëren van de inputs en outputs tot het bepalen van de volgorde en interacties tussen de processen. Ook de kwaliteit van de uitvoering en de beheersing van de processen moet overzien worden. Hiervoor dienen bijkomende criteria en methoden opgesteld te worden. Ook moeten de middelen en verantwoordelijkheden van de processen moeten toegewezen worden alsook de risico's en kansen die de processen met zich meebrengen. Tenslotte moeten de processen geëvalueerd worden en eventueel de nodige wijzigingen doorvoeren om de beoogde resultaten van de processen te behalen en het kwaliteitsmanagementsysteem te verbeteren.

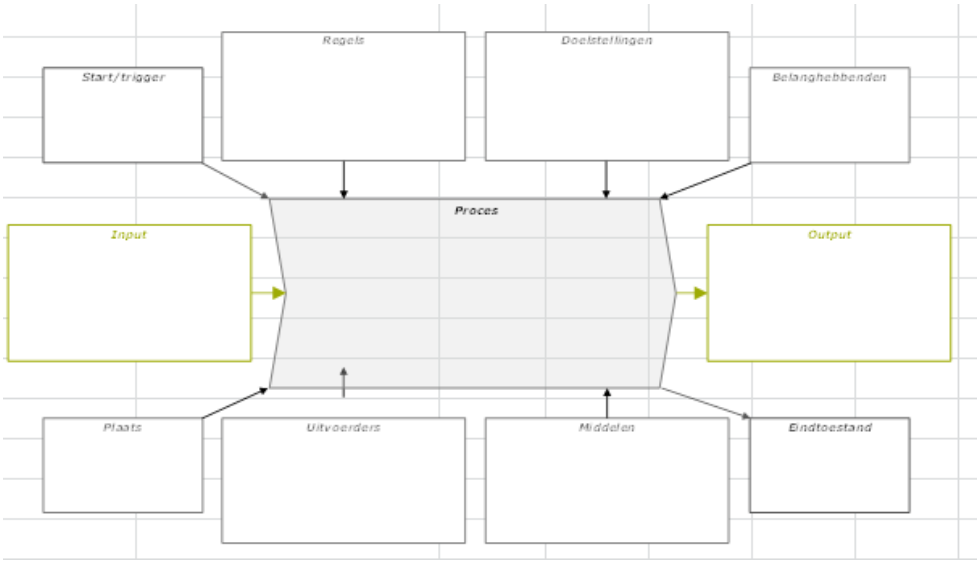
Om aan deze eisen van de ISO norm te voldoen, werd er op zoek gegaan naar mogelijke manier om deze processen zodanig in kaart te brengen zodat ze meteen aan de eisen rond processen uit de ISO norm voldoen. Verschillende bronnen stellen hiervoor het gebruik van schildpaddiagrammen voor om er voor te zorgen dat processen in overeenstemming met de ISO norm in kaart gebracht worden (Jaeger Holland, 2017 & Blackmores, 2018). Een schildpaddiagram is volgens hun een geschikt hulpmiddel om proces karakteristieken visueel voor te stellen en om een effectieve uitvoering en verbetering van processen helpen mogelijk te maken. Kymal (2016) raadt auditors ook aan bij het uitvoeren van een ISO 9001 audit om schildpaddiagrammen te gebruiken om de effectiviteit van processen na te gaan. Daarnaast gebruiken Ruamchat et al. (2017) ook schildpaddiagrammen als kwaliteitsmiddel om proceskarakteristieken visueel voor te stellen en een procesbenadering te

creëren. Ook voor managers is dit een effectieve manier om hun processen in beeld te brengen zonder dat ze hiervoor technische kennis over processen moeten hebben. Om deze redenen werd er ook beslist om de processen van VITO met behulp van schildpaddiagrammen in kaart te brengen.

5.2.2 Uitwerking schildpaddiagrammen

In figuur 8 wordt een sjabloon van het schildpaddiagram weergegeven dat zal gebruikt worden voor het in kaart brengen van de processen. Het diagram krijgt de naam schildpaddiagram omdat het met enige verbeelding op een schildpad lijkt met als staart en hoofd respectievelijk de input en output van de processen en het proces zelf in het midden als schild van de schildpad. Voor elk proces zullen de volgende maatstaven besproken worden:

- Start/trigger: Wat is het event dat het proces doet starten en wanneer?
- Input: Wat is er allemaal nodig als input van het proces?
- Proces: Welke activiteiten worden er in het proces uitgevoerd om de input om te vormen tot de output?
- Output: Wat zijn de resultaten van het proces?
- Eindtoestand: Met welk event eindigt het proces en wanneer?
- Regels: Wat is het kader waarin het proces wordt uitgevoerd en wat zijn de criteria waarbinnen het proces werkt?
- Doelstellingen: Wat moet er gerealiseerd worden door het uitvoeren van het proces?
- Plaats: Waar vinden de activiteiten plaats?
- Uitvoerders: Wie is betrokken bij de uitvoering van het proces?
- Middelen: Welke middelen zijn nodig om het proces uit te kunnen voeren?



FIGUUR 8: VOORBEELD VAN EEN SCHILDPADDIAGRAM

Voor elk proces wordt bijkomstig aangegeven of het gaat om een primair of een secundair proces gaat. Bij een primair proces ligt de uitvoering en verantwoordelijkheid enkel binnen de informatica afdeling, terwijl secundaire processen behoren tot of toepasbaar zijn op andere afdelingen dan de informatica afdeling. Hieronder wordt het eerste proces bij wijze van voorbeeld uitgewerkt. De uitwerking van de voltallige 13 processen kunnen teruggevonden worden in bijlage 8.

1. Manage service portfolio (secundair)

Doelstellingen: Het opstellen en onderhouden van een accuraat overzicht van de diensten die de informatica afdeling van VITO uitvoert en ervoor zorgen dat de geleverde ICT diensten overeenkomen met de behoeften van de business.

Start/trigger: Periodiek, regelmatige update.

Input:

- Overzicht van het service portfolio en de diensten die ze aanbieden.
- Info over de bedrijfsbehoeften en strategie via managementmeetings en dagelijkse bedrijfscontacten.

Proces:

- Regelmatige beoordeling van het portfolio overzicht.
- Toevoegen, veranderen of verwijderen van diensten zodat het portfolio up-to-date blijft met de huidige geleverde diensten.
- Het aanpassen van informatie in verband met de diensten in de relevante bestanden of bedrijfsapplicaties.

Output:

- Een portfolio van diensten die de informatica afdeling van VITO levert.
- Project overzichten in Maconomy[1].
- Een slide met het service portfolio in de introductie presentatie van de informatica afdeling.

Eindtoestand: Wanneer de lijst van services overeenkomt met de huidig geleverde diensten.

Regels/kader: De lijst moet overal accuraat gebruikt worden.

Plaats: De informatica afdeling

Uitvoerders: Het management van de informatica afdeling.

Middelen: Master file in sharepoint[2] en data voorzien door Maconomy (ERP systeem).

KPI: Het portfolio bevat een compleet en accuraat overzicht van de diensten die de informatica afdeling van VITO levert en dient als basis voor andere processen.

[1] Maconomy is het ERP systeem dat VITO gebruikt.
[2] Sharepoint is een online platform dat informatie-uitwisseling binnen een organisatie toestaat.

Meting KPI: Het service portfolio komt overeen met de gerelateerde bestanden en informatie in de bedrijfsapplicaties zoals Maconomy.

Risico:

1. Het service portfolio komt niet overeen met de behoeften en doelstellingen van het bedrijf. De beschrijvingen van de activiteiten in het portfolio zijn niet duidelijk voor gebruikers of stakeholders.
2. Het service portfolio komt niet overeen met de activiteiten die de informatica afdeling uitvoert.

Verhelpen risico:

1. Met de belangrijkste bedrijfsstakeholders de informatica diensten regelmatig overlopen zodat ze overeenkomen met hun behoeften.
2. Het regelmatig nagaan of de activiteiten in het service portfolio nog overeenkomen met de werkelijk uitgevoerde activiteiten.

5.3 Mapping VITO – ISO

Nu met behulp van de schildpaddiagrammen een duidelijk beeld gevormd is van de 13 COBIT processen die VITO geïmplementeerd heeft, zal er in deze sectie overgegaan worden tot het mappen van deze 13 processen met de ISO 9001 norm op dezelfde manier als bij de theoretische mapping tussen de 37 COBIT processen en de ISO norm. Zo kunnen verschillen en gelijkenissen aangekaart worden en kan er nagegaan worden in welke mate de mapping geldt in de praktijk. Daarnaast zal de vereiste van de mapping nagegaan worden, namelijk of er een overzicht geschetst wordt in welke mate VITO aan de ISO norm voldoet met behulp van de 13 processen en welke processen bijkomend geïmplementeerd kunnen worden.

5.3.1 De mapping tussen VITO en ISO 9001

Tabel 14 geeft in de eerste twee kolommen de mapping tussen de op COBIT gebaseerde processen van VITO en de ISO 9001 norm weer. Naast de titel van elk proces van VITO wordt het overeenkomstige COBIT proces tussen haakjes weergegeven. Uit deze mapping kan in eerste instantie afgeleid worden dat elk proces overeenkomt met minstens drie secties uit de ISO norm. Voor de processen *Manage service portfolio, Availability management* en *Capacity management* werden de meeste overeenkomsten gevonden. Deze konden namelijk respectievelijk met 11, 11 en 10 secties gemapt worden. Het proces dat met het minst aantal secties gemapt kon worden is het proces *Identity & access management.* Dit proces kon maar met drie secties uit de norm gemapt worden. Over het algemeen geeft dit al een eerste indicatie dat de processen van VITO, in verband met het aantal secties waarmee de processen overeenkomen, een goede overeenkomst tonen met de ISO norm in vergelijking met de theoretische mapping.

In de derde kolom van tabel 14 worden per proces de overeenkomsten met de ISO norm van de theoretische mapping tussen COBIT en ISO 9001 herhaald. Op deze manier kan er makkelijker een beeld geschetst worden van de verschillen en overeenkomsten tussen de mapping met de processen van VITO en de COBIT processen. Op het eerste zicht zijn er veel gelijkenissen te observeren tussen de secties uit de ISO norm waar de processen van VITO en de COBIT processen mee overeenkomen.

Acht van de 13 VITO processen verschillen slechts twee of minder secties van de originele mapping en vaak ontstaan de verschillen omdat de processen van VITO met meer secties overeenkomen dan de COBIT processen. Processen die aanzienlijk verschillen zijn *Availability management* en *Capacity management.* Deze zijn beide gebaseerd op proces *BAI04 Manage availability and capacity* en verschillen negen en acht secties respectievelijk. Redenen hiervoor kunnen zijn dat de processen van VITO in werkelijkheid worden toegepast en daardoor specifieker zijn, waardoor het beter aansluit bij een gedetailleerdere norm zoals de ISO norm dan de theoretische processen uit het bredere COBIT framework. In tegenstelling tot het COBIT proces, bevat de beschrijving van deze twee processen van VITO expliciet het evalueren, implementeren, monitoren en managen van de beschikbaarheid en de capaciteit waardoor aan meerdere secties van de ISO norm voldaan wordt. Dit verklaart het grote verschil in secties waarin de processen overeenkomen. De processen *APO13 Manage security* en *ICT security management* zijn de enige die aan exact dezelfde secties voldoen. De beschrijvingen van deze processen zijn dan ook zeer gelijkend op elkaar, met dezelfde overeenkomsten tot gevolg.

Dit laatste doet misschien vermoeden dat er gestreefd moet worden naar het bereiken van exact dezelfde mapping zoals de in dit onderzoek ontworpen mapping. Dit is echter niet het geval. Wanneer een organisatie of een deel van een organisatie de ISO norm wil implementeren, is het natuurlijk beter indien ze reeds aan zoveel mogelijk secties van de norm voldoen. De overeenkomende secties uit de mapping kunnen als richtlijn gezien worden. Aan deze secties zou een geïmplementeerd COBIT proces voldoen indien het net zoals het in het COBIT framework omschreven staat, geïmplementeerd zou worden. In de werkelijkheid worden de doelen en de omschrijvingen van de COBIT processen eerst eigen gemaakt aan de organisatie vooraleer ze geïmplementeerd worden. Dit heeft als gevolg dat de processen vaak specifieker zijn dan het high level COBIT framework voorschrijft. Hieruit kan de redenering gemaakt worden dat COBIT processen die in de werkelijkheid geïmplementeerd worden dichter kunnen aanleunen bij een gedetailleerder framework zoals een ISO norm net omdat ze specifieker zijn dan de theoretische processen.

Wat kan er nu op basis van de vergelijking met de processen van VITO geconcludeerd worden over de opgestelde mapping tussen het COBIT framework en de ISO 9001 norm? In eerste instantie kan er geconcludeerd worden dat er duidelijke gelijkenissen en terugkomende secties uit de ISO norm zijn tussen de processen van VITO en de COBIT processen. Enerzijds is dit logisch aangezien de processen van VITO op COBIT gebaseerd zijn, anderzijds zijn de processen duidelijk eigen gemaakt aan VITO. Dit zou een indicatie kunnen geven dat er bepaalde basis overeenkomsten zijn tussen de theoretische mapping en de mapping met de processen van VITO. Tenslotte worden er ook bij de processen van VITO minstens evenveel en vaak ook meer ISO secties gemapt als bij de standaard COBIT processen.

5.3.2 De meerwaarde van de mapping

Tenslotte wordt er op zoek gegaan naar het antwoord op de vraag of de theoretische mapping aan VITO een meerwaarde biedt bij het leveren van een overzicht in de mate dat er door de huidige processen aan de ISO norm wordt voldaan en welke processen eventueel geïmplementeerd kunnen worden om aan bijkomende eisen te voldoen? Om te beginnen werd de mapping als een waardevolle oefening beschouwd door de verantwoordelijke bij VITO om een beter zicht te krijgen in de mate dat

de 13 processen van VITO aan de eisen van de ISO norm voldoen. Om extra na te gaan of de mapping in het geval van VITO waardevol zou zijn, wordt opnieuw de vergelijking gemaakt tussen de theoretische COBIT – ISO mapping en de VITO – ISO mapping om na te gaan welke ISO secties gemist zouden zijn, indien de theoretische mapping door VITO werd toegepast en de VITO – ISO mapping niet bestond.

In tabel 13 worden de secties van de ISO norm per hoofdstuk weergegeven waar VITO aan voldoet vergeleken met de secties waar VITO volgens de theoretische mapping aan voldoet. Secties in het groen aangeduid willen zeggen dat de mapping uit deze kolom aan deze sectie voldoet, terwijl de andere mapping hier niet aan voldoet, waarbij deze sectie in het rood wordt aangeduid. Uit de tabel kan afgeleid worden dat VITO in werkelijkheid aan secties *4.1 Inzicht in de organisatie en haar context* en *8.6 Vrijgave van producten en diensten* voldoet, terwijl de theoretische mapping zou stellen dat ze hier niet aan zouden voldoen. Daarnaast voldoet VITO niet aan sectie *7.3 Bewustzijn* maar zou de mapping wel zeggen dat ze hier aan voldoen. Het is moeilijk te zeggen of het verschil in deze drie secties een significant verschil is of niet aangezien in geen van de geraadpleegde werken uit de literatuur de mapping in de praktijk toegepast wordt. Vooral het feit dat VITO volgens de mapping aan sectie 7.3 voldoet, terwijl ze dat in werkelijkheid niet doen zou eventueel voor problemen kunnen zorgen voor een ISO certificatie. Langs de andere kant dient de mapping als richtlijn aanzien te worden en niet als iets dat in steen geschreven staat. Om deze reden wordt er voorlopig vanuit gegaan dat de theoretische mapping een goede reflectie van de realiteit weergeeft, totdat toekomstig onderzoek dit kan bevestigen of tegenspreken.

Gegeven dit kleine verschil in overeenkomst tussen de twee mappings en het feit dat de verantwoordelijke van VITO de mapping als een waardevolle oefening beschouwd, kan uit deze sectie geconcludeerd worden dat de theoretische mapping tussen het COBIT framework en de ISO 9001 norm uit 2015 wel degelijk een meerwaarde biedt in het geven van een overzicht aan welke secties uit de ISO norm voldaan zijn, gegeven een aantal COBIT processen.

VITO – ISO mapping	COBIT – ISO mapping
Hoofdstuk 4	Hoofdstuk 4
4.1	4.1
4.2	4.2
Hoofdstuk 5	Hoofdstuk 5
5.1	5.1
5.3	5.3
Hoofdstuk 6	Hoofdstuk 6
6.1	6.1
Hoofdstuk 7	Hoofdstuk 7
7.1	7.1
7.2	7.2
7.3	7.3
7.5	7.5
Hoofdstuk 8	Hoofdstuk 8
8.1	8.1
8.2	8.2
8.3	8.3
8.4	8.4

8.5	8.5
8.6	8.6
8.7	8.7
Hoofdstuk 9	Hoofdstuk 9
9.1	9.1
9.2	9.2
9.3	9.3
Hoofdstuk 10	Hoofdstuk 10
10.1	10.1
10.2	10.2
10.3	10.3

Tabel 13: Secties waar VITO aan voldoet vergeleken met de secties waarvan de mapping zegt dat VITO aan voldoet.

Dit is natuurlijk gebaseerd op een enkele case study bij een enkel bedrijf. Het zou mogelijk kunnen zijn dat wanneer dezelfde studie uitgevoerd wordt bij een ander bedrijf dat er meer of minder gelijkenissen in mappings zijn. Daarnaast werd deze case study enkel uitgevoerd bij een bedrijf dat COBIT reeds in werking had en ISO 9001 wou implementeren. Om ook de andere richting te valideren zou de mapping ook getest moeten worden bij een bedrijf dat de ISO 9001 norm reeds in werking heeft en graag enkele COBIT processen wil implementeren. Deze eerste case study duidt alvast aan dat de opgestelde mapping een duidelijke indicatie geeft in welke mate aan de ISO 9001 norm is voldaan wanneer er COBIT processen geïmplementeerd zijn.

5.3.3 Suggesties van bijkomende processen voor VITO

Op basis van tabel 13 kan ook afgeleid worden aan welke secties niet worden voldaan door VITO. Er vanuit gaande dat enkel de COBIT - ISO mapping beschikbaar zou zijn, worden hier de secties weergegeven waar VITO nog niet aan voldoet en enkele processen voorgesteld die bijkomend geïmplementeerd zouden kunnen worden om alsnog aan deze secties te voldoen.

De secties waar VITO volgens de mapping nog niet aan voldoet zijn de volgende:

- 4.1 Inzicht in de organisatie en haar context
- 4.3 Het toepassingsgebied van het kwaliteitsmanagementsysteem vaststellen
- 4.4 Kwaliteitsmanagementsystemen en de processen ervan
- 5.2 Het kwaliteitsbeleid vaststellen en kenbaar maken
- 6.2 Kwaliteitsdoelstellingen en de planning om ze te bereiken
- 6.3 Planning van wijzigingen
- 7.4 Communicatie
- 8.6 Vrijgave van producten en diensten

Het proces dat het meest voor de hand liggend is om bijkomend te implementeren, is het proces *APO11: Manage quality*. Dit proces zorgt meteen dat VITO aan zeven van de acht ontbrekende secties voldoet. Enkel aan sectie *6.3 Planning van wijzigingen* wordt dan nog niet voldaan. Sectie 6.3 kan teruggevonden worden in de mapping bij vier COBIT processen, namelijk:

- BAI05: Manage organisational change enablement
- BAI06: Manage changes
- BAI07: Manage change acceptance and transitioning.

- BAI10: Manage configuration

Geen van deze vier COBIT processen worden gemapt met andere secties waar VITO nog niet aan voldoet dus puur op dit vlak zou het niet uitmaken welk van de vier bijkomend geïmplementeerd zou worden. Natuurlijk moet er in de realiteit de link met de behoeften van het bedrijf gemaakt worden.

Een ander proces dat mogelijk geïmplementeerd zou kunnen worden is *EDM01: Ensure Governance Framework Setting and Maintenance*. Met dit proces wordt bijkomend voldaan aan secties 4.1, 4.3, 5.2 en 6.2. Ook proces *APO01 Manage the IT management framework* zorgt ervoor dat aan de helft van de ontbrekende secties nog voldaan wordt, meer bepaald aan secties 4.3, 4.4, 5.2, 6.2.

In ieder geval kan volgens de mapping enkel aan secties 8.6 en 7.4 voldaan worden wanneer proces *APO11 Manage quality* geïmplementeerd wordt. Dus, concreet wordt er aan VITO aangeraden, indien zij aan alle secties uit de ISO norm willen voldoen, om met dit proces te werken in combinatie met een van de vier BAI processen.

Tabel 14: Mapping tussen de processen van VITO en de ISO norm en de overeenkomstige originele mapping

VITO Proces	Mapping VITO proces met ISO Sectie	Mapping COBIT proces met ISO sectie
1. Manage service portfolio (APO05)	4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden. 7.5 Gedocumenteerde informatie 8.1 Operationele planning en beheersing 8.2 Eisen voor producten en diensten 8.3 Ontwerp en ontwikkeling van producten en diensten 8.5 Productie en het leveren van diensten 9.1 Monitoren, meten, analyseren en evalueren 9.3 Directiebeoordeling 10.1 Vaststellen verbeteringen 10.3 Continue verbetering	4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden 7.5 Gedocumenteerde informatie 8.1 Operationele planning en beheersing 8.2 Eisen voor producten en diensten 8.3 Ontwerp en ontwikkeling van producten en diensten 9.1 Monitoren, meten, analyseren en evalueren 9.3 Directiebeoordeling 10.1 Vaststellen verbeteringen
2. Manage budget and costs (APO06)	7.1 Middelen	4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden

	7.5 Gedocumenteerde informatie 8.1 Operationele planning en beheersing 9.1 Monitoren, meten, analyseren en evalueren	7.1 Middelen 8.2 Eisen voor producten en diensten
3. Manage human resources (APO07)	5.3 Rollen, verantwoordelijkheden en bevoegdheden binnen de organisatie 7.1 Middelen 7.2 Competentie 8.5 Productie en het leveren van diensten 10.1 Vaststellen verbeteringen	5.3 Rollen, verantwoordelijkheden en bevoegdheden binnen de organisatie 7.1 Middelen 7.2 Competentie 7.3 Bewustzijn 8.5 Productie en het leveren van diensten
4. Business relationship management (APO08)	4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden. 5.1 Leiderschap en betrokkenheid 6.1 Acties om risico's en kansen aan te pakken 8.2 Eisen voor producten en diensten 8.6 Vrijgave van producten en diensten 9.1 Monitoren, meten, analyseren en evalueren	5.1 Leiderschap en betrokkenheid 6.1 Acties om risico's en kansen aan te pakken 8.2 Eisen voor producten en diensten 10.1 Vaststellen verbeteringen 10.3 Continue verbetering
5. Supplier relationship management (APO10)	7.1 Middelen 7.2 Competentie 8.3 Ontwerp en ontwikkeling van producten en diensten 8.4 Beheersing van extern geleverde processen, producten en diensten	6.1 Acties om risico's en kansen aan te pakken 7.1 Middelen 7.2 Competentie 8.3 Ontwerp en ontwikkeling van producten en diensten 8.4 Beheersing van extern geleverde processen, producten en diensten 8.5 Productie en het leveren van

	8.5 Productie en het leveren van diensten 9.1 Monitoren, meten, analyseren en evalueren	diensten 9.1 Monitoren, meten, analyseren en evalueren
6. ICT security management (APO13)	6.1 Acties om risico's en kansen aan te pakken 9.1 Monitoren, meten, analyseren en evalueren 9.2 Interne audit 10.3 Continue verbetering	6.1 Acties om risico's en kansen aan te pakken 9.1 Monitoren, meten, analyseren en evalueren 9.2 Interne audit 10.3 Continue verbetering
7. Manage programmes & projects (BAI01)	4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden. 7.5 Gedocumenteerde informatie 8.1 Operationele planning en beheersing 8.2 Eisen voor producten en diensten 8.3 Ontwerp en ontwikkeling van producten en diensten 8.5 Productie en het leveren van diensten 9.1 Monitoren, meten, analyseren en evalueren 9.2 Interne audit	7.5 Gedocumenteerde informatie 8.1 Operationele planning en beheersing 8.2 Eisen voor producten en diensten 9.1 Monitoren, meten, analyseren en evalueren 9.2 Interne audit 10.1 Vaststellen verbeteringen
8. Availability management (BAI04)	4.1 Inzicht in de organisatie en haar context. 4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden. 6.1 Acties om risico's en kansen aan te pakken	7.1 Middelen 8.2 Eisen voor producten en diensten

	7.1 Middelen 7.5 Gedocumenteerde informatie 8.2 Eisen voor producten en diensten 8.3 Ontwerp en ontwikkeling van producten en diensten 8.5 Productie en het leveren van diensten 9.1 Monitoren, meten, analyseren en evalueren 10.1 Vaststellen verbeteringen 10.2 Afwijkingen en corrigerende maatregelen	
9. Capacity management (BAI04)	6.1 Acties om risico's en kansen aan te pakken 7.1 Middelen 8.2 Eisen voor producten en diensten 8.3 Ontwerp en ontwikkeling van producten en diensten 8.4 Beheersing van extern geleverde processen, producten en diensten 8.5 Productie en het leveren van diensten 9.1 Monitoren, meten, analyseren en evalueren 10.1 Vaststellen verbeteringen 10.2 Afwijkingen en corrigerende maatregelen 10.3 Continue verbetering	7.1 Middelen 8.2 Eisen voor producten en diensten

10. Software and hardware asset management (BAI09)	7.1 Middelen 7.5 Gedocumenteerde informatie 8.1 Operationele planning en beheersing 8.2 Eisen voor producten en diensten 9.1 Monitoren, meten, analyseren en evalueren 9.2 Interne audit	7.1 Middelen 8.1 Operationele planning en beheersing 8.2 Eisen voor producten en diensten 9.2 Interne audit
11. Incident management (DSS02)	8.2 Eisen voor producten en diensten 8.5 Productie en het leveren van diensten 8.7 Beheersing van afwijkende outputs 9.1 Monitoren, meten, analyseren en evalueren 10.1 Vaststellen verbeteringen 10.2 Afwijkingen en corrigerende maatregelen 10.3 Continue verbetering	8.2 Eisen voor producten en diensten 8.5 Productie en het leveren van diensten 8.7 Beheersing van afwijkende outputs 10.1 Vaststellen verbeteringen 10.2 Afwijkingen en corrigerende maatregelen 10.3 Continue verbetering
12. Request fulfilment (DSS02)	8.2 Eisen voor producten en diensten 8.5 Productie en het leveren van diensten 8.7 Beheersing van afwijkende outputs 9.1 Monitoren, meten, analyseren en evalueren 10.1 Vaststellen verbeteringen 10.2 Afwijkingen en corrigerende maatregelen	8.2 Eisen voor producten en diensten 8.5 Productie en het leveren van diensten 8.7 Beheersing van afwijkende outputs 10.1 Vaststellen verbeteringen 10.2 Afwijkingen en corrigerende maatregelen 10.3 Continue verbetering

	10.3 Continue verbetering	
13. Identity & access management (DSS05)	6.1 Acties om risico's en kansen aan te pakken 7.5 Gedocumenteerde informatie 9.1 Monitoren, meten, analyseren en evalueren	6.1 Acties om risico's en kansen aan te pakken 7.5 Gedocumenteerde informatie

6. Conclusie

Omdat het belang van IT in ondernemingen steeds blijft toenemen en klanten of gebruikers steeds veeleisender worden, werd in dit onderzoek een mapping opgesteld tussen het COBIT framework en de ISO 9001 norm uit 2015. Met behulp van een design science methodologie werd een mapping ontworpen die beide frameworks met elkaar vergelijkt zodat het combineren van beide frameworks bij de implementatie bevorderd kan worden.

Het onderzoek begon met de vraag: '*Hoe kan de ISO 9001 norm uit 2015 een aanvulling zijn op COBIT voor het managen van IT-afdelingen?'* Om een antwoord op deze vraag te bekomen werden enkele deelvragen opgesteld. De eerste deelvraag luidde: '*Wat houden COBIT en de ISO 9001 norm in?'* Om op deze eerste deelvraag te antwoorden, werd er in de literatuurstudie onder meer met behulp van de frameworks zelf een overzicht geschetst van de belangrijkste zaken uit deze twee frameworks. Naast COBIT werd er ook een overzicht van het overkoepelende begrip IT-Governance en het interne controle framework COSO geschetst. Ook werd er naast de ISO norm dieper ingegaan op kwaliteitsmanagement in het algemeen om ook hierrond een breder kader te schetsen. Al deze informatie was nodig om een goede basiskennis op te bouwen om doorheen de rest van het onderzoek deze frameworks te kunnen combineren.

Eens die goede basis rond COBIT en ISO 9001 gelegd was, kon er op zoek gegaan worden naar een antwoord op de tweede deelvraag: '*Hoe kan een overzicht verkregen worden van de overeenkomsten tussen COBIT 5 en ISO 9001?'.* Om op deze vraag een antwoord te vinden, werd er allereerst in de literatuur op zoek gegaan naar manieren waarmee eerder uitgevoerde onderzoeken overeenkomsten tussen COBIT en ISO normen in kaart brachten. Al snel werd duidelijk dat het ontwerpen van een mapping voor onderzoekers de voorkeur kreeg om de overeenkomsten in kaart te brengen. De gevonden werken werden geanalyseerd en hun methoden om de twee frameworks met elkaar te mappen werden samengevat. Uiteindelijk werd er besloten om zelf een mapping op te stellen tussen COBIT en de ISO 9001 norm door de ISO norm op te delen in 28 secties, die elk op vlak van inhoud vergeleken werden met de 37 COBIT processen. Om de overeenkomst te bepalen, werd er gekeken naar de essentie van het proces of van de sectie en werd er op basis van een overeenkomst tussen kernwoorden en hun context bepaald of er een gelijkenis was op inhoudelijk vlak of niet. De mapping werd weergegeven voor zowel elke sectie uit de ISO norm als voor elk COBIT proces zodat zowel vanuit COBIT als vanuit ISO vertrokken kan worden, afhankelijk van de behoeften van de gebruiker.

Om vervolgens aan te tonen dat de mapping wel degelijk een antwoord voorziet op de bijvraag, werd er overgegaan tot het demonstreren van de mapping en de meerwaarde ervan. Hiervoor werd er samengewerkt met het bedrijf VITO, dat op basis van enkele COBIT processen wou weten in welke mate ze conform waren aan de ISO norm, met als hoger doel het behalen van een ISO certificatie. Dit was de ideale gelegenheid om aan de hand van de mapping na te gaan in welke mate VITO aan de eisen van de ISO norm voldeed en om op deze manier de richting van COBIT naar ISO te testen. Allereerst werden de processen van VITO met behulp van schildpaddiagrammen in kaart gebracht. Aan de hand hiervan kon gecontroleerd worden in welke mate de mapping in een werkelijke

omgeving van toepassing was. Hiervoor werd een nieuwe mapping opgesteld tussen de processen van VITO en de ISO norm. Uit de vergelijking van de mappings werd er slechts een afwijking van drie secties vastgesteld, waaruit de conclusie getrokken werd dat het gebruik van de originele mapping een duidelijke indicatie geeft in welke mate dat VITO aan de eisen van de ISO norm voldoet. Om na te gaan of het gebruik van deze mapping werkelijk een waardevolle meerwaarde bood, werd bij de verantwoordelijke binnen VITO nagegaan of de mapping daadwerkelijk een beter inzicht gaf in de mate waaraan de eisen van de ISO norm voldaan werd. Op deze vraag werd positief gereageerd en bevestigd dat het maken van de mapping een waardevolle oefening kan zijn voor VITO. Op basis van de mapping konden vervolgens voor VITO potentiële processen geïdentificeerd worden die de overeenkomst met de ISO norm in de toekomst kunnen bevorderen.

Om tenslotte een antwoord te formuleren op de onderzoeksvraag: '*Hoe kan de ISO 9001 norm uit 2015 een aanvulling zijn op COBIT voor het managen van IT-afdelingen?'* kan men stellen dat in de realiteit vaak meerdere frameworks gecombineerd worden en dat deze combinatie een versterkend effect kan hebben. In het geval van COBIT en ISO 9001 kan COBIT ervoor zorgen dat het gebruik van IT geoptimaliseerd wordt en hieruit optimale bedrijfswaarde te creëren. ISO, langs de andere kant, mikt op het continue verbeteren van het systeem en klanttevredenheid te bevorderen. Om deze frameworks op een effectieve en efficiënte manier te combineren kan er overgegaan worden tot het gebruik van een mapping die de overlappende gebieden tussen de twee blootlegt. Met deze mapping wordt enerzijds een aanvulling van de literatuur geleverd aangezien er tot op heden weinig onderzoek verricht werd naar de mogelijke combinatie van deze twee frameworks. Anderzijds levert de mapping een beter zicht aan organisaties in de mate waarop aan het ene framework voldaan wordt wanneer het andere geïmplementeerd is. Op deze manier kan de bijkomende implementatie van het tweede framework vergemakkelijkt worden of de communicatie met entiteiten die een verschillend framework implementeren, bevorderd worden. Deze mapping werd gedemonstreerd bij de IT afdeling van VITO, die de meerwaarde ervan kon bevestigen.

Limitaties en toekomstig onderzoek

De grootste limitatie is dat de mapping slechts getest is geweest bij een enkel bedrijf. Bijgevolg konden ook enkel de processen die dit bedrijf toepast gebruikt worden om de mapping te testen waardoor de mapping van meer als de helft van de 37 COBIT processen niet getest kon worden. Bijkomend werd de mapping enkel vertrekkende vanuit COBIT getest. In de toekomst zou de omgekeerde richting ook toegepast moeten worden bij een omgeving die de ISO 9001 norm reeds in werking heeft en graag enkele COBIT processen wil implementeren. Op deze manier kan de meerwaarde van de mapping ook in deze richting aangetoond worden.

Het uitvoeren van deze bijkomende studies zal uitsluitsel moeten geven over de mate waarin de mapping effectief als hulpmiddel door bedrijven toegepast zal kunnen worden en in de mate dat aanpassingen vereist zijn.

Naast de mapping zelf zou de methodologie en de manier waarop de mapping werd opgesteld opnieuw voor COBIT en ISO 9001, maar ook voor andere combinaties van frameworks getest kunnen worden. Op deze manier kan enerzijds de mate nagegaan worden waarin de mapping uit dit

onderzoek opnieuw bekomen wordt door het toepassen van dezelfde methodologie op dezelfde twee frameworks. Anderzijds kan er hiermee nagegaan worden of de methodologie ook voor een combinatie van andere frameworks een nuttige mapping kan opleveren.

Tenslotte zou achteraf bij VITO nagegaan kunnen worden of ze daadwerkelijk de ISO certificatie gehaald hebben omwille van de processen die in dit onderzoek worden aangeraden om bijkomend te implementeren, indien deze ook werkelijk geïmplementeerd werden.

Lijst van geraadpleegde werken

Applegate, L. M. (1999) Rigor and Relevance in MIS Research.Introduction, *MIS Quarterly* (23:1), March 1999, pp. 1-2.

Blackmores. (2018). The Power of Using 'Turtle Diagrams'.

British Department of Trade & Industry (2015): Quality Management Systems, Definition, Available: http:// www.businessballs.com/dtiresources/quality_management_systems_QMS.pdf (Access: 13. April 2018).

Burawoy, M. (1998). The extended case method. Sociological Theory 16: 4–33.

Burawoy, M. (2009). The extended case method. Four countries, four decades, four great transformations, and one theoretical tradition. Berkeley: University of California Press.

Bürgy, P. (2016). *Measure Process Maturity for Quality Management Systems COBIT 5 PAM for ISO 9001:2015 Maturity Measurement*.

Cadbury Report. (1992). *Financial Aspects of Corporate Governance*.

Chen, C., Anchecta, K., Lee, Y., & Dahlgaard, J. (2016). A STEPWISE ISO-BASED TQM IMPLEMENTATION APPROACH USING ISO 9001:2015. *Management and Production Engineering Review*, *7*(4), 65-75.

COSO. (2013). *Internal Control — Integrated Framework: Executive Summary*.

COSO. (2014). *Improving Organizational Performance and Governance*.

Denning, P. J. (1997). A New Social Contract for Research, *Communications of the ACM*, February 1997, pp. 132-134.

Dubé, L., & Paré, G. (2003). Rigor in information systems positivist case research: current practices, trends, and recommendations. MIS Quarterly, 27 (4), 597-635.

Eisenhardt, K.M. (1989). Building theories from case study research. Academy of Management Review 14: 532–550.

Eisenhardt, K.M., and M.E. Graebner. (2007). Theory building from cases: opportunities and challenges. Academy of Management Journal 50: 25–32.

Fiss, P.C. (2009). Case studies and the configurational analysis of organizational phenomena. In The SAGE handbook of case-based methods, ed. D.S. Byrne, and C.C. Ragin, 424–440. London/Thousand Oaks: SAGE.

Gehrmann, M. (2012). Combining ITIL, COBIT and ISO/IEC 27002 for structuring comprehensive information technology for management in organizations. *Navus*, *2*(2), 66-77.

Gomm, R., M. Hammersley, and P. Foster. (2000). Case study method. Key issues, key texts. London/ Thousand Oaks: Sage Publications.

Hammar, M. (2015, 8 juni). List of Quality Management Standards and Frameworks. Geraadpleegd op 25 februari 2018, van https://advisera.com/9001academy/knowledgebase/list-of-quality-management-standards-and-frameworks/

Hevner, A.R.; March, S.T.; Park, J.; and Ram, S. (2004). Design research in information systems research*. MIS Quarterly*, 28, 1, 75–105.

ISACA. (2012). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT.*

ISACA. (2012b). *COBIT 5: Enabling processes.*

ISO, & NBN. (2015). *Kwaliteitsmanagementsystemen - Eisen (ISO 9001:2015)*.

ISO. (2015b). *Moving from ISO 9001:2008 to ISO 9001:2015*.

ISR. (2002). Editorial Statement and Policy. *Information Systems Research*, December 2002.

ITGI, & OGC. (2005). *Aligning COBIT, ITIL and ISO 17799 for business benefit: Management summary*.

ITGI, & OGC. (2008). *Aligning COBIT 4.1, ITIL V3 and ISO 27002 for business benefit: A Management Briefing From ITGI and OGC*.

Jaeger Holland. (2017). The Turtle Diagram - Will it meet the process approach requirements in ISO 9001:2015 © ISO 2015?

Järvinen, P. (2007) Action research is similar to design science*. Quality & Quantity*, 41, 1, 37–54.

Kymal, C. (2016). Auditing Strategy for ISO 9001. *The Journal for Quality and Participation*, *39*(3), 25–28.

Lee, A. (1999). Inaugural Editor's Comments, *MIS Quarterly* (23:1), March 1999, pp. v-xi.

Lin, H., Cefaratti, M., & Wallace, L. (2012). Enterprise risk management, COBIT and ISO 27002: A conceptual analysis. *Internal Auditing*, *27*(2), 3-12.

M. M. Eloff and S. H. von Solms. (2000). Information Security Management: A Hierarchical Framework for Various Approaches, *J Computers & Security*, Vol. 19, 2000, pp.243-256.

March, S. T., en Smith, G. (1995). Design and Natural Science Research on Information Technology, *Decision Support Systems*, December 1995, pp. 251-266.

Moeller, R. (2013). *Executive's guide to IT Governance: Improving system processes with Service management, COBIT and ITIL*. New Jersey, United States of America: John Wiley & Sons Inc..

Oparaugo, C. (2016). COBIT 5 Mapping Exercise for Establishing Enterprise IT Strategy. *COBIT Focus*, *1*(1), 1-18.

Peffers, K., Tuunanen, T., A Rothenberger, M., & Chatterjee, S. (2008). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45-77.

Pfeifer, Tilo; Schmitt, Robert (2010): Qualitätsmanagement, Strategien Methoden Techniken, 4nd Edition, Carl Hanser Verlag GmbH & Co. KG, Munich (Germany).

Rosenthal, R. (1966). Experimenter effects in behavioral research. East Norwalk, CT, US: Appleton-Century-Crofts.

Rowley, J. (2002). Using case studies in research. Management Research News, 25 (1), 16-27.

Ruamchat, K., Thawesaengskulthai, N., & Pongpanich, C. (2017). DEVELOPMENT OF QUALITY MANAGEMENT SYSTEM UNDER ISO 9001:2015 AND JOINT INSPECTION GROUP (JIG) FOR AVIATION FUELLING SERVICE. *Management and Production Engineering Review*, *8*(3), 50–59.

Sahibudin, S., Sharifi, M., & Ayat, M. (2008). Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations. *2008 Second Asia International Conference on Modelling & Simulation (AMS)*, .

Selig, G. (2008). *Implementing IT Governance: A pratical guide to global best practices in IT management*. Zaltbommel, Nederland: Van Haren Publishing.

Sheikhpour, R. (2012). An approach to map COBIT processes to ISO/IEC 27001 information security management controls. *International Journal of Security and its Applications*, *6*(2), 13-28.

Silver, M. S., Markus, M. L., and Beath, C. M. (1995). The Information Technology Interaction Model: A Foundation for the MBA Core Course*. MIS Quarterly*, September 2004, pp. 361-390.

Simon, H. A. (1996). The sciences of the Artificial (3rd ed.). *MIT Press*, Cambridge, MA.

Stake, R.E. (1995). The art of case study research. London, Thousand Oaks: Sage Publications.

Stake, R.E. (2005). Qualitative case studies. In The SAGE handbook of qualitative research, 3rd ed, ed. N.K. Denzin, and Y.S. Lincoln, 443–466. London, Thousand Oaks: Sage Publications.

Sudman, S., and Bradburn, N. (1982). *Asking questions: A practical guide to questionnaire design, San Francisco*: Jossey-Bass.

Tsichritzis, D. (1998). The Dynamics of Innovation, *Beyond Calculation: The Next Fifty Years of Computing, P. J. Denning and R. M. Metcalfe (eds.)*, Copernicus Books, New York, 1998, pp. 259-265.

van Aken, J.E. (2004). Management research based on the paradigm of the design sciences: The quest for field-tested and grounded technological rules*. Journal of Management Studies*, 41, 2, 219–246.

Vaughan, D. 1992. Theory elaboration: The heuristics of case analysis. In What is a case?, ed. C.C. Ragin, and H.S. Becker, 173–202. Exploring the foundations of social inquiry: Cambridge University Press, Cambridge, New York.

Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both? *Computers & Security*, *24*, 99-104.

Wieringa, R. (2014). *Design Science Methodology for Information Systems and Software Engineering*. Berlijn, Duitsland: Springer.

Yin, R.K. (1984). Case study research (2nd ed.). Thousand Oaks, U.S.: SAGE Publications.

Yin, R.K. (2014). Case study research. Design and methods, 5th ed. London, Thousand Oaks: Sage Publications.

Zmud, R. (1997). Editorís Comments, *MIS Quarterly*, June 1997, pp. xxi-xxii.

Bijlagen

Bijlage 1: De 17 COSO principes

Interne controle: 5 principes:

1) Commitment met integriteit en ethische waarden.

2) Bestuur en toezicht zijn onafhankelijk van het management en houden toezicht op de inrichting en werking van de interne beheersing.

3) Organisatie- en verantwoording structuur met de bijbehorende verdeling verantwoordelijkheden, taken en bevoegdheden.

4) Adequaat HRM.

5) Bevorderen van de lijnverantwoordelijkheid voor interne beheersing.

Risicobeoordeling: 4 principes:

6) Bepalen van SMART geformuleerde doelen.

7) Identificatie en analyse van risico´s met betrekking tot de realisatie van de doelen.

8) Bewustzijn van frauderisico´s.

9) Identificatie en beoordeling van veranderingen die de interne beheersing significant beïnvloeden.

Controlactiviteiten: 3 principes:

10) Selectie en ontwikkeling van beheersingsmaatregelen voor de mitigatie van risico's.

11) Selectie en ontwikkeling van algemene beheersingsmaatregelen over (IC)T.

12) Beheersingsmaatregelen zijn gebaseerd op beleid en worden uitgewerkt in adequate procedures.

Informatie en communicatie: 3 principes:

13) Inrichting van een adequate informatievoorziening voor de ondersteuning van de interne beheersing.

14) Inrichting van een ondersteunende interne communicatiestructuur.

15) Inrichting van een externe communicatiestructuur.

Monitoring: 2 principes:

16) Inrichten en uitvoeren van continue of periodieke evaluatie van het bestaan en de werking van de interne beheersingsmaatregelen.

17) Tekortkomingen in de interne beheersing worden tijdig gerapporteerd aan partijen die verantwoordelijk zijn voor correctieve maatregelen.

Bijlage 2: Gedetailleerde beschrijving van een COBIT proces en een governance praktijk van dit proces.

EDM01 Ensure Governance Framework Setting and Maintenance	Area: Governance Domain: Evaluate, Direct and Monitor
Process Description Analyse and articulate the requirements for the governance of enterprise IT, and put in place and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprise's mission, goals and objectives.	
Process Purpose Statement Provide a consistent approach integrated and aligned with the enterprise governance approach. To ensure that IT-related decisions are made in line with the enterprise's strategies and objectives, ensure that IT-related processes are overseen effectively and transparently, compliance with legal and regulatory requirements is confirmed, and the governance requirements for board members are met.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
01 Alignment of IT and business strategy	• Percent of enterprise strategic goals and requirements supported by IT strategic goals • Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services • Percent of IT value drivers mapped to business value drivers
03 Commitment of executive management for making IT-related decisions	• Percent of executive management roles with clearly defined accountabilities for IT decisions • Number of times IT is on the board agenda in a proactive manner • Frequency of IT strategy (executive) committee meetings • Rate of execution of executive IT-related decisions
07 Delivery of IT services in line with business requirements	• Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT service delivery
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. Strategic decision-making model for IT is effective and aligned with the enterprise's internal and external environment and stakeholder requirements.	• Actual vs. target cycle time for key decisions • Level of stakeholder satisfaction (measured through surveys)
2. The governance system for IT is embedded in the enterprise.	• Number of roles, responsibilities and authorities that are defined, assigned and accepted by appropriate business and IT management • Degree by which agreed-on governance principles for IT are evidenced in processes and practices (percentage of processes and practices with clear traceability to principles) • Number of instances of non-compliance with ethical and professional behaviour guidelines
3. Assurance is obtained that the governance system for IT is operating effectively.	• Frequency of independent reviews of governance of IT • Frequency of governance of IT reporting to the executive committee and board • Number of governance of IT issues reported

EDM01 RACI Chart

Governance Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
EDM01.01 Evaluate the governance system.	A	R	C	C	R		R				C		C	C	C	C	C	R	C	C	C					
EDM01.02 Direct the governance system.	A	R	C	C	R	I	R	I	I	I	C	I	I	I	I	C	C	R	C	I	I	I	I	I	I	I
EDM01.03 Monitor the governance system.	A	R	C	C	R	I	R	I	I	I	C	I	I	I	I	C	C	R	C	I	I	I	I	I	I	I

EDM01 Process Practices, Inputs/Outputs and Activities				
Governance Practice	**Inputs**		**Outputs**	
EDM01.01 Evaluate the governance system. Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements, and make a judgement on the current and future design of governance of enterprise IT.	**From**	**Description**	**Description**	**To**
	MEA03.02	Communications of changed compliance requirements	Enterprise governance guiding principles	All EDM APO01.01 APO01.03
	Outside COBIT	• Business environment trends • Regulations • Governance/decision-making model guidance • Constitution/bylaws/ statutes of organisation	Decision-making model	All EDM APO01.01
			Authority levels	All EDM APO01.02
Activities				
1. Analyse and identify the internal and external environmental factors (legal, regulatory and contractual obligations) and trends in the business environment that may influence governance design.				
2. Determine the significance of IT and its role with respect to the business.				
3. Consider external regulations, laws and contractual obligations and determine how they should be applied within the governance of enterprise IT.				
4. Align the ethical use and processing of information and its impact on society, natural environment, and internal and external stakeholder interests with the enterprise's direction, goals and objectives.				
5. Determine the implications of the overall enterprise control environment with regard to IT.				
6. Articulate principles that will guide the design of governance and decision making of IT.				
7. Understand the enterprise's decision-making culture and determine the optimal decision-making model for IT.				
8. Determine the appropriate levels of authority delegation, including threshold rules, for IT decisions.				

Bijlage 3: de 17 bedrijfsdoelstellingen van COBIT

1. Stakeholder value of business investments
2. Portfolio of competitive products and services
3. Managed business risk (safeguarding of assets)
4. Compliance with external laws and regulations
5. Financial transparency
6. Customer-oriented service culture
7. Business service continuity and availability
8. Agile responses to a changing business environment
9. Information-based strategic decision making
10. Optimisation of service delivery costs
11. Optimisation of business process functionality
12. Optimisation of business process costs
13. Managed business change programmes
14. Operational and staff productivity
15. Compliance with internal policies
16. Skilled and motivated people
17. Product and business innovation culture

Bijlage 4: Mapping bedrijfsdoelstellingen naar IT gerelateerde doelstellingen.

			Enterprise Goal																
			Stakeholder value of business investments	Portfolio of competitive products and services	Managed business risk (safeguarding of assets)	Compliance with external laws and regulations	Financial transparency	Customer-oriented service culture	Business service continuity and availability	Agile responses to a changing business environment	Information-based strategic decision making	Optimisation of service delivery costs	Optimisation of business process functionality	Optimisation of business process costs	Managed business change programmes	Operational and staff productivity	Compliance with internal policies	Skilled and motivated people	Product and business innovation culture
			1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
		IT-related Goal	Financial					Customer					Internal					Learning and Growth	
Financial	01	Alignment of IT and business strategy	P	P	S			P	S	P	P	S	P	S	P			S	S
	02	IT compliance and support for business compliance with external laws and regulations			S	P											P		
	03	Commitment of executive management for making IT-related decisions	P	S	S					S	S		S		P			S	S
	04	Managed IT-related business risk			P	S			P	S		P			S		S	S	
	05	Realised benefits from IT-enabled investments and services portfolio	P	P				S		S		S	S	P		S			S
	06	Transparency of IT costs, benefits and risk	S		S		P				S	P		P					
Customer	07	Delivery of IT services in line with business requirements	P	P	S	S		P	S	P	S		P	S	S			S	S
	08	Adequate use of applications, information and technology solutions	S	S	S			S	S		S	S	P	S		P		S	S
Internal	09	IT agility	S	P	S			S		P			P		S	S		S	P
	10	Security of information, processing infrastructure and applications			P	P			P								P		
	11	Optimisation of IT assets, resources and capabilities	P	S						S		P	S	P	S	S			S
	12	Enablement and support of business processes by integrating applications and technology into business processes	S	P	S			S		S		S	P	S	S	S			S
	13	Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	P	S	S			S				S		S	P				
	14	Availability of reliable and useful information for decision making	S	S	S	S			P		P		S						
	15	IT compliance with internal policies			S	S											P		
Learning and Growth	16	Competent and motivated business and IT personnel	S	S	P			S		S						P		P	S
	17	Knowledge, expertise and initiatives for business innovation	S	P				S		P	S		S		S			S	P

Bijlage 5: De mapping van IT-gerelateerde doelstellingen naar COBIT processen.

			IT-related Goal																
			Alignment of IT and business strategy	IT compliance and support for business compliance with external laws and regulations	Commitment of executive management for making IT-related decisions	Managed IT-related business risk	Realised benefits from IT-enabled investments and services portfolio	Transparency of IT costs, benefits and risk	Delivery of IT services in line with business requirements	Adequate use of applications, information and technology solutions	IT agility	Security of information, processing infrastructure and applications	Optimisation of IT assets, resources and capabilities	Enablement and support of business processes by integrating applications and technology into business processes	Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	Availability of reliable and useful information for decision making	IT compliance with internal policies	Competent and motivated business and IT personnel	Knowledge, expertise and initiatives for business innovation
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
	COBIT 5 Process		Financial						Customer		Internal							Learning and Growth	
Evaluate, Direct and Monitor	EDM01	Ensure Governance Framework Setting and Maintenance	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S
	EDM02	Ensure Benefits Delivery	P		S		P	P	P	S			S	S	S	S		S	P
	EDM03	Ensure Risk Optimisation	S	S	S	P		P	S	S		P			S	S	P	S	S
	EDM04	Ensure Resource Optimisation	S		S	S	S	S	S	S	P		P		S			P	S
	EDM05	Ensure Stakeholder Transparency	S	S	P			P	P						S	S	S		S
Align, Plan and Organise	APO01	Manage the IT Management Framework	P	P	S	S			S		P	S	P	S	S	S	P	P	P
	APO02	Manage Strategy	P		S	S	S		P	S	S		S	S	S	S	S	S	P
	APO03	Manage Enterprise Architecture	P		S	S	S	S	S	S	P	S	P	S		S			S
	APO04	Manage Innovation	S			S	P			P	P		P	S		S			P
	APO05	Manage Portfolio	P		S	S	P	S	S	S	S		S		P				S
	APO06	Manage Budget and Costs	S		S	S	P	P	S	S			S		S				
	APO07	Manage Human Resources	P	S	S	S			S		S	S	P		P		S	P	P
	APO08	Manage Relationships	P		S	S	S	S	P	S			S	P	S		S	S	P
	APO09	Manage Service Agreements	S			S	S	S	P	S	S	S	S		S	P	S		
	APO10	Manage Suppliers		S		P	S	S	P	S	P	S	S		S	S	S		S
	APO11	Manage Quality	S	S		S	P		P	S	S		S		P	S	S	S	S
	APO12	Manage Risk		P		P		P	S	S	S	P			P	S	S	S	S
	APO13	Manage Security		P		P		P	S	S		P				P			

			IT-related Goal																	
			Alignment of IT and business strategy	IT compliance and support for business compliance with external laws and regulations	Commitment of executive management for making IT-related decisions	Managed IT-related business risk	Realised benefits from IT-enabled investments and services portfolio	Transparency of IT costs, benefits and risk	Delivery of IT services in line with business requirements	Adequate use of applications, information and technology solutions	IT agility	Security of information, processing infrastructure and applications	Optimisation of IT assets, resources and capabilities	Enablement and support of business processes by integrating applications and technology into business processes	Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	Availability of reliable and useful information for decision making	IT compliance with internal policies	Competent and motivated business and IT personnel	Knowledge, expertise and initiatives for business innovation
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
		COBIT 5 Process	Financial						Customer		Internal							Learning and Growth	
Build, Acquire and Implement	BAI01	Manage Programmes and Projects	P		S	P	P	S	S	S			S		P			S	S
	BAI02	Manage Requirements Definition	P	S	S	S	S		P	S	S	S	S	P	S	S			S
	BAI03	Manage Solutions Identification and Build	S			S	S		P	S			S	S	S	S			S
	BAI04	Manage Availability and Capacity				S	S		P	S	S		P		S	P			S
	BAI05	Manage Organisational Change Enablement	S		S		S		S	P	S		S	S	P				P
	BAI06	Manage Changes			S	P	S		P	S	S	P	S	S	S	S	S		S
	BAI07	Manage Change Acceptance and Transitioning				S	S		S	P	S			P	S	S	S		S
	BAI08	Manage Knowledge	S				S		S	S	P	S	S			S		S	P
	BAI09	Manage Assets		S		S		P	S		S	S	P			S	S		
	BAI10	Manage Configuration		P		S		S		S	S	S	P			P	S		
Deliver, Service and Support	DSS01	Manage Operations		S		P	S		P	S	S	S	P			S	S	S	S
	DSS02	Manage Service Requests and Incidents				P			P	S		S				S	S		S
	DSS03	Manage Problems		S		P	S		P	S	S		P	S		P	S		S
	DSS04	Manage Continuity	S	S		P	S		P	S	S	S	S	S		P	S	S	S
	DSS05	Manage Security Services	S	P		P			S	S		P	S	S		S	S		
	DSS06	Manage Business Process Controls		S		P			P	S		S	S	S		S	S	S	S
Monitor, Evaluate and Assess	MEA01	Monitor, Evaluate and Assess Performance and Conformance	S	S	S	P	S	S	P	S	S	S	P		S	S	P	S	S
	MEA02	Monitor, Evaluate and Assess the System of Internal Control		P		P		S	S	S		S				S	P		S
	MEA03	Monitor, Evaluate and Assess Compliance With External Requirements		P		P	S		S			S					S		S

Bijlage 6: Benoeming procesinhoud Bürgy

1. IT Management

Input:

- Financiële verslaggeving
- Informatica portfolio
- Procesvereisten
- Bedrijfsdoelstellingen
- Wetgevingen
- Controle verslagen
- Uitzonderingsvereisten

Output:

- Uitzonderingsbesluiten
- Verslagen van ICT testen en vereisten
- Masterplan van ICT-strategie en bijhorende meetgegevens
- Programma informatie en handleiding
- Studiebehoeften

Doelstellingen

- Optimale IT ondersteuning voor bedrijfsprocessen.
- Actualiseren ICT vereisten met respect voor ICT normen.
- Implementeren ICT programma's.

Proces:

- Ontwikkelen en (controle op het) nakomen van ICT strategieën en normen binnen het bedrijf.
- Uitzonderingen op deze vereisten identificeren en vrijstellingen toestaan.
- Opstellingen volgen van IT infrastructuur.
- Identificeren behoeften aan en het implementeren van ICT programma's.

Belanghebbende:

- Business process manager
- ICT auditor
- IT security officer
- Solution architect
- Programmabeheerder
- Strategy officer
- Enterprice architect
- Project manager
- Eindgebruiker

2. IT Steering

Input:

- Afwijkingen
- ICT diensten en behoeften
- Operationele vereisten voor SLA's
- Financiële cijfers en verslagen
- Procesvereisten
- ICT programma's, vereisten en masterplan
- Diensten portfolio en verbeteringsplan

Output:

- SLA overeenkomsten
- Change requests
- Controle verslagen
- IT portfolio
- Serviceverbeteringsplan
- Informatie over klanttevredenheid en trends
- Project beslissingen

Doelstelling:

- Ondersteuning en optimalisatie van bedrijfsprocessen door gebruik van ICT-middelen.

Proces:

- Studies uitvoeren
- Het leiden van projecten
- Sturen van het IT portfolio
- Implementeren van ICT applicaties
- Aan SLA's voldoen wat betreft ICT diensten
- Opvolgen van prestaties

Belanghebbende:

- Accountmanager
- Verantwoordelijke voor bedrijfsprocessen
- IT security officer
- Solution architect
- Product manager
- Project manager
- Service portfolio verantwoordelijke
- Service manager
- Enterprise architect

3. Maintain IT-Processes

Input:

- ICT specificaties
- Meetgegevens
- Suggesties van gebruikers
- Goedkeuringsproces

Output:

- Proces wijzigingen
- Gebruiker trainingen
- Meetgegevens
- Verbeteringsverzoeken

Doelstelling:

- Het definiëren van het procesmanagementsysteem en zorgen voor een continue verbetering van de ICT processen.

Proces:

- Periodieke en individuele procesbeoordelingen
- Verbeteren van het proces
- Introduceren van procesveranderingen

Belanghebbende:

- Proceseigenaar
- Procesverantwoordelijke
- Procesmanager

4. Strategic Marketing

Input:

- ICT vereisten
- Kredieten

Output:

- Gerichte communicatie
- Marketinginformatie
- Meetgegevens

Doelstelling:

- Zorgen voor een niveau- en doelgroepgerichte, tijdige, continue en betrouwbare communicatie.

Proces:

- Het beheren van informatie -en communicatieplatformen
- Het definiëren van CI/CD (Continuous integration / Continuous delivery) specificaties

Belanghebbende:

- Marketing manager

5. Solution Development & Deployment

Input:

- Operationele en ICT vereisten
- ICT opleidingsbehoeften
- Projectinformatie
- Kredieten
- Ondersteuningsvereisten en informatie voor oplossingen
- Behoeften
- Informatie over de huidige configuratie

Output:

- Toepasbare oplossingen
- Operationele vereisten voor SLA
- Wijzigingsplan
- Meetgegevens en specificaties
- Project specifieke trainingsvereisten
- Project status en overeenkomst
- Informatie over de gewijzigde configuratie

Doelstelling:

- Het definiëren van processen om ICT projecten en veranderingen in termen van kwaliteit, duur, kosten, klanttevredenheid af te handelen en in te voeren.

Proces:

- Initiëren van ICT projecten
- Bedenken van oplossingsvoorstellen
- Oplossingen opstellen en implementeren
- Veranderingen en oplossingen in de ICT omgeving doorvoeren die niet project gerelateerd zijn

Belanghebbende:

- De gebruiker
- Account manager
- Change manager
- IT security officer
- Integration manager
- Solution architect
- Project manager
- Service manager

6. Operate IT-Infrastructure & -Services

Input:

- Vraag informatie

- Financiële cijfers en verslagen
- Serviceverbeteringsplan
- ICT vereisten
- Service portfolio
- Oplossingen
- Gewijzigde configuraties

Output:

- Geanalyseerde informatie en problemen
- Evaluatie ICT diensten
- Operationele vereisten en informatie
- Bestaande configuraties
- Meetgegevens
- Service improvement plan
- Voorraadinformatie

Doelstelling:

- Het voorzien van operationele ICT diensten in overeenstemming met SLA's en budgetten.
- Het bereiken van een bepaalde klanttevredenheid.
- Het zorgen voor gegevensbescherming en beveiliging.
- Het opstellen van een inventaris van de ICT objecten.

Proces:

- Definiëren van ICT configuraties
- Beschikbaarheid controleren en analyseren
- Een overzicht houden van de behoeften
- Analyse van de werking en de capaciteit
- Meting van de prestaties en capaciteit
- Diensten uitvoeren, laten uitvoeren en onderhouden
- Opstellen inventaris procedures en evalueren van voorraad informatie

Belanghebbende:

- Gebruiker
- Change manager
- IT security officer
- Integration manager
- Product manager
- Service manager

7. User Support

Input:

- Probleemmeldingen

- Operationele informatie en veranderingen
- ICT vereisten
- Informatie over klanttevredenheid
- Gebruiker meldingen
- Standaard oplossingen voor ondersteuning

Output:

- Evaluatie van de geleverde diensten
- Informatie over problematische diensten of delen van diensten
- Meetgegevens
- Rapporten over diensten en capaciteiten
- Status probleemoplossing
- Ondersteuning en informatie voor een oplossing
- Ondersteuningsplan

Doelstelling:

- Het garanderen van gebruikersondersteuning volgens SLA's en het snelst mogelijk herstel van ICT-diensten in geval van verstoringen.
- Het opzetten van een communicatiecentrum met correcte informatie en hoge toegankelijkheid.
- Een efficiënte en tijdige probleemoplossing met optimaal gebruik van middelen.
- Het bepalen van oorzaken en gevolgen van storingen om deze in de toekomst te verminderen.

Proces:

- Gebruikers ondersteunen
- Diensten die oplossingen bieden plannen en voorbereiden
- Incidenten en problemen oplossen
- De ondersteuningsdiensten evalueren

Belanghebbende:

- Gebruikers
- Gebruiker ondersteunende diensten

8. Sales

Input:

- Sales opportuniteiten
- Klant beslissingen
- ICT vereisten

Output:

- Aanbod aan klant
- Wijzigingen in bestelling
- Infrastructuur

- Meetgegevens

Doelstelling:

- Het afsluiten van contracten en een lange termijn en winstgevende relatie met klanten.

Proces:

- Verkoopproces

Belanghebbende:

- Account manager
- Verkoop manager
- Project manager
- Servicedesk

9. Skills Development

Input:

- Algemene, ICT en project specifieke opleidingsvereisten
- ICT vereisten
- Werknemersprofielen
- Functiebeschrijvingen

Output:

- Bijgewerkte aanbevelingen voor ICT training
- De mate waarin aan de behoeften is voldaan
- Individuele opleidingsbehoeften

Doelstelling:

- Het ondersteunen van managers bij het ontwikkelen van ICT personeel.

Proces:

- Trainingsaanbevelingen voorbereiden
- Analyse van de tekortkomingen

Belanghebbende:

- Procesverantwoordelijke

10. Procurement

Input:

- Offertes van leveranciers
- Aanvraag van diensten
- ICT vereisten
- Informatie over problematische diensten of delen van producten of diensten
- Specificaties

Output:

- Demand fulfillment
- Aankooporder
- Aankoopinformatie
- Meetgegevens
- Leverancierscontracten

Doelstelling:

- Het op behoeften gebaseerd leveren van IT infrastructuur en diensten.

Proces:

- Vraagaanvraag
- Opstellen offertes
- Verwerken bestellingen
- Leveren dienst of product
- Factuurverwerking
- Bestelling controle

Belanghebbende:

- Klant
- Aankoopverantwoordelijke
- Integration manager
- Aankoopafdeling

11. Support Financial Management

Input:

- Goedgekeurd IT portfolio
- ICT vereisten
- Inventaris informatie
- Projectovereenkomsten
- Informatie over diensten en capaciteiten

Output:

- Financiële kerncijfers en kostengegevens
- Meetgegevens
- Status van kredieten
- Lening informatie

Doelstelling:

- De benodigde IT resources kunnen gepland, beheerd en weergegeven worden.
- Het economisch verbruik van informatica middelen.
- Het financiële ondersteuningsproces moet de IT processen ondersteunen.

Proces:

- Financiële planning en begroting
- Uitvoeren van de begroting
- Opstellen jaarrekening

Belanghebbende:

- Account manager
- CFO
- IT account manager
- Integratie manager
- Verantwoordelijke van kost objecten

Bijlage 7: De documentatie op basis waarvan de mapping werd ontworpen

ISO 9001

1. Context van de organisatie

I. Inzicht in de organisatie en haar context

De organisatie moet externe en interne belangrijke punten vaststellen die relevant zijn voor haar doel en strategische richting en die haar vermogen beïnvloeden om de beoogde resultaten van haar kwaliteitsmanagementsysteem te behalen.

De organisatie moet informatie over deze externe en interne belangrijke punten (issues) monitoren en beoordelen.

II. Inzicht in de behoeften en verwachtingen van belanghebbenden

Vanwege hun effect of mogelijke effect op het vermogen van de organisatie om op consistente wijze producten en diensten te leveren die voldoen aan de eisen van de klant en de van toepassing zijnde eisen uit wet- en regelgeving, moet de organisatie het volgende vaststellen:

a) welke belanghebbenden relevant zijn voor het kwaliteitsmanagementsysteem;

b) welke eisen van deze belanghebbenden relevant zijn voor het kwaliteitsmanagementsysteem.

De organisatie moet informatie over deze belanghebbenden en hun relevante eisen monitoren en beoordelen.

III. Het toepassingsgebied van het kwaliteitsmanagementsysteem vaststellen

De organisatie moet de grenzen en toepasselijkheid van het kwaliteitsmanagementsysteem bepalen om het toepassingsgebied ervan vast te stellen. Bij het vaststellen van dit toepassingsgebied moet de organisatie het volgende overwegen:

a) de genoemde externe en interne belangrijke punten;

b) de genoemde eisen van relevante belanghebbenden;

c) de producten en diensten van de organisatie.

De organisatie moet alle eisen van deze internationale norm toepassen indien deze van toepassing zijn binnen het vastgestelde toepassingsgebied van haar kwaliteitsmanagementsysteem. Het toepassingsgebied van het kwaliteitsmanagementsysteem van de organisatie moet beschikbaar zijn en als gedocumenteerde informatie worden onderhouden. In het toepassingsgebied moet worden aangegeven welke soorten producten en diensten eronder vallen en moet worden voorzien in een motivering voor elke eis van deze internationale norm waarvan de organisatie bepaalt dat deze niet van toepassing is in het toepassingsgebied van haar kwaliteitsmanagementsysteem. Op het voldoen aan deze internationale norm mag alleen aanspraak worden gemaakt indien de eisen waarvan wordt

bepaald dat deze niet van toepassing zijn niet van invloed zijn op het vermogen of de verantwoordelijkheid van de organisatie om de conformiteit van haar producten en diensten en het verhogen van klanttevredenheid te bewerkstelligen.

IV. Kwaliteitsmanagementsystemen en de processen ervan

De organisatie moet een kwaliteitsmanagementsysteem inrichten, implementeren, onderhouden en continu verbeteren, met inbegrip van de benodigde processen en hun interacties, in overeenstemming met de eisen van deze internationale norm. De organisatie moet de processen bepalen die nodig zijn voor het kwaliteitsmanagementsysteem en de toepassing ervan door de hele organisatie en moet:

a) de benodigde inputs en de verwachte outputs van deze processen vaststellen;

b) de volgorde en interacties van deze processen vaststellen;

c) de criteria en methoden (inclusief monitoring, metingen en bijbehorende prestatie-indicatoren) vaststellen die nodig zijn om een doeltreffende uitvoering en beheersing van deze processen te bewerkstelligen;

d) de middelen vaststellen die nodig zijn voor deze processen en de beschikbaarheid ervan bewerkstelligen;

e) de verantwoordelijkheden en bevoegdheden voor deze processen toewijzen;

f) de risico's en kansen aanpakken zoals vastgesteld overeenkomstig de eisen van 6.1;

g) deze processen evalueren en eventueel benodigde wijzigingen doorvoeren die nodig zijn om de realisatie van hun beoogde resultaten te bewerkstelligen;

h) de processen en het kwaliteitsmanagementsysteem verbeteren.

Voor zover nodig moet de organisatie:

a) gedocumenteerde informatie onderhouden om de uitvoering van haar processen te ondersteunen;

b) gedocumenteerde informatie bijhouden om het vertrouwen te hebben dat de processen worden uitgevoerd zoals gepland.

2. Leiderschap

I. Leiderschap en betrokkenheid

De directie moet leiderschap en betrokkenheid tonen met betrekking tot het kwaliteitsmanagementsysteem door:

a) de verantwoordelijkheid te nemen voor de doeltreffendheid van het kwaliteitsmanagementsysteem;

b) te bewerkstelligen dat het kwaliteitsbeleid en de kwaliteitsdoelstellingen worden vastgesteld voor het kwaliteitsmanagementsysteem en compatibel zijn met de context en de strategische richting van de organisatie;

c) te bewerkstelligen dat de eisen van het kwaliteitsmanagementsysteem in de bedrijfsprocessen van de organisatie worden geïntegreerd;

d) het gebruik van de procesbenadering en het risicogebaseerd denken te bevorderen;

e) te bewerkstelligen dat de voor het kwaliteitsmanagementsysteem benodigde middelen beschikbaar zijn;

f) het belang van doeltreffend kwaliteitsmanagement en van het voldoen aan de eisen van het kwaliteitsmanagementsysteem te communiceren;

g) te bewerkstelligen dat het kwaliteitsmanagementsysteem zijn beoogde resultaten behaalt;

h) mensen te betrekken (engageren), aan te sturen en te ondersteunen om een bijdrage te leveren aan de doeltreffendheid van het kwaliteitsmanagementsysteem;

i) verbetering te bevorderen;

j) andere relevante managementfuncties te ondersteunen om hun leiderschap te tonen binnen hun verantwoordelijkheidsgebieden.

De directie moet leiderschap en betrokkenheid tonen met betrekking tot klantgerichtheid door te bewerkstelligen dat:

a) de eisen van klanten en van toepassing zijnde wet- en regelgeving worden vastgesteld, begrepen en dat er op consistente wijze aan wordt voldaan;

b) de risico's en kansen die van invloed kunnen zijn op het voldoen aan de eisen van producten en diensten en het vermogen om de klanttevredenheid te verhogen worden vastgesteld en aangepakt;

c) de focus op het verhogen van de klanttevredenheid wordt behouden.

II. Het kwaliteitsbeleid vaststellen en kenbaar maken

De directie moet een kwaliteitsbeleid vaststellen, implementeren en onderhouden dat:

a) passend is voor het doel en de context van de organisatie en de strategische richting ervan ondersteunt;

b) een kader biedt voor het vaststellen van kwaliteitsdoelstellingen;

c) een verbintenis bevat om te voldoen aan van toepassing zijnde eisen;

d) een verbintenis bevat tot continue verbetering van het kwaliteitsmanagementsysteem.

Het kwaliteitsbeleid moet:

a) beschikbaar zijn en worden onderhouden als gedocumenteerde informatie;

b) worden gecommuniceerd, begrepen en toegepast binnen de organisatie;

c) op een geschikte manier beschikbaar zijn voor relevante belanghebbenden.

III. Rollen, verantwoordelijkheden en bevoegdheden binnen de organisatie

De directie moet bewerkstelligen dat de verantwoordelijkheden en bevoegdheden voor relevante rollen worden toegekend, gecommuniceerd en begrepen binnen de organisatie. De directie moet de verantwoordelijkheid en bevoegdheid toekennen met betrekking tot:

a) het bewerkstelligen dat het kwaliteitsmanagementsysteem voldoet aan de eisen van deze internationale norm;

b) het bewerkstelligen dat de processen hun beoogde outputs leveren;

c) het rapporteren over de prestaties van het kwaliteitsmanagementsysteem en over verbeterkansen, in het bijzonder aan de directie;

d) het bewerkstelligen dat klantgerichtheid binnen de gehele organisatie wordt bevorderd;

e) het bewerkstelligen dat de werking en samenhang van het kwaliteitsmanagementsysteem behouden blijven wanneer er wijzigingen met betrekking tot het kwaliteitsmanagementsysteem worden gepland en doorgevoerd.

3. Planning

I. Acties om risico's en kansen aan te pakken

Bij het plannen voor het kwaliteitsmanagementsysteem moet de organisatie de genoemde belangrijke punten en de genoemde eisen overwegen, en de risico's en kansen vaststellen die moeten worden aangepakt om:

a) de zekerheid te geven dat het kwaliteitsmanagementsysteem zijn beoogde resultaten kan behalen;

b) gewenste effecten te verhogen;

c) ongewenste effecten te voorkomen of te verminderen;

d) verbetering te bereiken.

De organisatie moet:

a) acties plannen om deze risico's en kansen aan te pakken;

b) plannen op welke manier:

1) de acties in haar kwaliteitsmanagementsysteemprocessen worden geïntegreerd en geïmplementeerd.

2) de doeltreffendheid van deze acties wordt geëvalueerd.

De acties die worden genomen om risico's en kansen aan te pakken moeten in verhouding staan tot de mogelijke gevolgen voor het voldoen aan de eisen van producten en diensten.

II. Kwaliteitsdoelstellingen en de planning om ze te bereiken

De organisatie moet voor relevante functies, niveaus en processen kwaliteitsdoelstellingen vaststellen die nodig zijn voor het kwaliteitsmanagementsysteem. De kwaliteitsdoelstellingen moeten:

a) consistent zijn met het kwaliteitsbeleid;

b) meetbaar zijn;

c) rekening houden met van toepassing zijnde eisen;

d) relevant zijn voor het voldoen aan eisen van producten en diensten en voor het verhogen van de klanttevredenheid;

e) worden gemonitord;

f) worden gecommuniceerd;

g) passend bij de situatie worden geactualiseerd.

De organisatie moet gedocumenteerde informatie over de kwaliteitsdoelstellingen onderhouden.

Bij het opstellen van plannen voor het bereiken van de kwaliteitsdoelstellingen moet de organisatie vaststellen:

a) wat er zal worden gedaan;

b) welke middelen er nodig zijn;

c) wie er verantwoordelijk is;

d) wanneer het zal zijn voltooid;

e) hoe de resultaten zullen worden geëvalueerd

III. Planning van wijzigingen

Indien de organisatie vaststelt dat er behoefte is aan wijzigingen in het kwaliteitsmanagementsysteem, moeten de wijzigingen op geplande wijze worden uitgevoerd. De organisatie moet nadenken over:

a) het doel van de wijzigingen en hun mogelijke gevolgen;

b) de eenheid en samenhang van het kwaliteitsmanagementsysteem;

c) de beschikbaarheid van middelen;

d) de toewijzing of hernieuwde toewijzing van verantwoordelijkheden en bevoegdheden.

4. Ondersteuning

I. Middelen

De organisatie moet de middelen vaststellen en beschikbaar stellen die nodig zijn voor het inrichten, implementeren, onderhouden en continu verbeteren van het kwaliteitsmanagementsysteem.

De organisatie moet bepalen welke personen nodig zijn voor de doeltreffende implementatie van haar kwaliteitsmanagementsysteem en voor het uitvoeren en beheersen van haar processen en deze personen beschikbaar stellen.

De organisatie moet de infrastructuur bepalen, beschikbaar stellen en onderhouden die nodig is voor de uitvoering van haar processen en om te voldoen aan eisen van producten en diensten.

De organisatie moet bepalen welke omgeving nodig is voor de uitvoering van haar processen om het voldoen aan eisen voor producten en diensten te realiseren, in deze omgeving voorzien en deze onderhouden.

De organisatie moet de middelen bepalen en beschikbaar stellen die nodig zijn om voor geldige en betrouwbare resultaten te zorgen indien monitoring of meting wordt gebruikt voor het verifiëren of producten en diensten aan de eisen voldoen.

Wanneer de naspeurbaarheid van metingen een eis is of door de organisatie als een essentieel onderdeel wordt gezien van het geven van vertrouwen in de geldigheid van meetresultaten, moet meetuitrusting:

a) met gespecificeerde tussenpozen of voorafgaand aan gebruik worden gekalibreerd of geverifieerd, of beide, volgens meetstandaarden die herleidbaar zijn tot internationale of nationale meetstandaarden; wanneer dergelijke standaarden niet bestaan, dan moet de basis die is gebruikt voor de kalibratie of verificatie als gedocumenteerde informatie worden bijgehouden;

b) worden geïdentificeerd om de status ervan vast te stellen;

c) worden beveiligd tegen aanpassingen of afstellingen, schade of achteruitgang waardoor de kalibratiestatus en latere meetresultaten niet langer geldig zouden zijn.

De organisatie moet vaststellen of de geldigheid van eerdere meetresultaten negatief is beïnvloed als blijkt dat meetuitrusting niet geschikt is voor het beoogde doel en moet, indien nodig, passende maatregelen treffen.

De organisatie moet bepalen welke kennis nodig is om haar processen uit te voeren en te voldoen aan de eisen voor producten en diensten. Deze kennis moet op peil worden gehouden en beschikbaar worden gesteld in de mate waarin dit nodig is. Wanneer veranderende behoeften en trends worden gesignaleerd, moet de organisatie nadenken over de huidige kennis van de organisatie en bepalen hoe zij eventueel benodigde aanvullende kennis en vereiste updates kan verwerven of er toegang tot verkrijgen.

II. Competentie

De organisatie moet:

a) de benodigde competentie vaststellen van de personen die onder haar gezag werkzaamheden verricht(en) die de prestaties en doeltreffendheid van het kwaliteitsmanagementsysteem beïnvloeden;

b) bewerkstelligen dat deze personen competent zijn op basis van de juiste opleiding, training en/of ervaring;

c) indien van toepassing, acties ondernemen om de benodigde competentie te verwerven, en de doeltreffendheid van de ondernomen acties evalueren;

d) geschikte gedocumenteerde informatie als bewijs van competentie bijhouden.

III. Bewustzijn

De organisatie moet bewerkstelligen dat personen die werkzaamheden verrichten onder het gezag van de organisatie, zich bewust zijn van:

a) het kwaliteitsbeleid;

b) relevante kwaliteitsdoelstellingen;

c) hun bijdrage aan de doeltreffendheid van het kwaliteitsmanagementsysteem, met inbegrip van de voordelen van verbeterde prestaties;

d) de gevolgen van het niet voldoen aan de eisen van het kwaliteitsmanagementsysteem.

IV. Communicatie

De organisatie moet vaststellen welke interne en externe communicatie relevant is voor het kwaliteitsmanagementsysteem, inclusief:

a) waarover te communiceren;

b) wanneer te communiceren;

c) met wie te communiceren;

d) hoe te communiceren;

e) wie er communiceert.

V. Gedocumenteerde informatie

Het kwaliteitsmanagementsysteem van de organisatie moet onder andere bevatten:

a) de gedocumenteerde informatie die de norm vereist;

b) de gedocumenteerde informatie die de organisatie nodig acht voor de doeltreffendheid van het kwaliteitsmanagementsysteem.

Bij het creëren en actualiseren van gedocumenteerde informatie moet de organisatie zorgen voor een passende:

a) identificatie en beschrijving (bijv. een titel, datum, auteur of referentienummer);

b) format (bijv. taal, softwareversie, afbeeldingen) en media (bijv. papier, elektronisch);

c) beoordeling en goedkeuring van geschiktheid en toereikendheid.

Gedocumenteerde informatie zoals het kwaliteitsmanagementsysteem en deze internationale norm vereisen, moet worden beheerst om te bewerkstelligen dat:

a) de informatie beschikbaar is en geschikt is voor gebruik, waar en wanneer het nodig is;

b) de informatie voldoende is beveiligd (bijv. tegen verlies van vertrouwelijkheid, oneigenlijk gebruik en aantasting).

Voor het beheersen van gedocumenteerde informatie moet de organisatie, voor zover van toepassing, invulling geven aan de volgende activiteiten:

a) distributie, toegang, het terugvinden alsmede het gebruik;

b) opslag en behoud, inclusief behoud van leesbaarheid;

c) beheersing van wijzigingen (bijv. versiebeheer);

d) het bewaren en vernietigen.

Gedocumenteerde informatie van externe oorsprong die de organisatie nodig acht voor de planning en uitvoering van het kwaliteitsmanagementsysteem, moet bij de situatie passend worden geïdentificeerd, en worden beheerst.

Gedocumenteerde informatie die wordt bijgehouden als bewijs van voldoen aan de eisen moet worden beschermd tegen onbedoelde wijzigingen.

5. Uitvoering

I. Operationele planning en beheersing

Om te voldoen aan de eisen voor de levering van producten en diensten en om de vastgestelde acties te implementeren moet de organisatie de benodigde processen plannen, implementeren en beheersen, door:

a) de eisen voor de producten en diensten vast te stellen;

b) criteria vast te stellen voor:

1) de processen;

2) het goedkeuren van producten en diensten;

c) de middelen vast te stellen die nodig zijn om te voldoen aan de eisen voor de producten en diensten;

d) procesbeheersing te implementeren in overeenstemming met de criteria;

e) gedocumenteerde informatie vast te stellen, te onderhouden en bij te houden in de omvang die nodig is om:

1) het vertrouwen te hebben dat de processen volgens planning zijn uitgevoerd;

2) aan te tonen dat de producten en diensten aan de eisen voldoen.

De output van deze planning moet geschikt zijn voor de activiteiten van de organisatie. De organisatie moet geplande wijzigingen beheersen en de consequenties van onbedoelde wijzigingen beoordelen, en zo nodig maatregelen treffen om nadelige effecten tegen te gaan. De organisatie moet bewerkstelligen dat uitbestede processen worden beheerst.

II. Eisen voor producten en diensten

Communicatie met klanten moet bestaan uit:

a) het verstrekken van informatie met betrekking tot producten en diensten;

b) het behandelen van aanvragen, contracten of opdrachten, met inbegrip van wijzigingen;

c) het verkrijgen van feedback van de klant met betrekking tot producten en diensten, waaronder klachten van klanten;

d) het omgaan met of beheren van eigendom van klanten;

e) het vaststellen van specifieke eisen aan maatregelen bij onvoorziene omstandigheden, wanneer relevant.

Bij het vaststellen van de eisen voor de aan klanten aan te bieden producten en diensten moet de

organisatie bewerkstelligen dat:

a) de eisen voor de producten en diensten zijn gedefinieerd, waaronder:

1) elke van toepassing zijnde eis uit wet- en regelgeving;

2) de eisen die door de organisatie noodzakelijk worden geacht;

b) de organisatie kan voldoen aan de beweringen ten aanzien van de producten en diensten die zij aanbiedt. De organisatie moet bewerkstelligen dat zij het vermogen heeft om te voldoen aan de eisen voor aan klanten aan te bieden producten en diensten. De organisatie moet, alvorens zich ertoe te verbinden producten en diensten aan een klant te leveren, een beoordeling uitvoeren die volgende elementen omvat:

a) de door de klant gespecificeerde eisen, met inbegrip van de eisen voor levering en nazorg;

b) eisen die niet door de klant zijn gesteld, maar die wel nodig zijn voor gespecificeerd of beoogd gebruik, wanneer dat bekend is;

c) eisen gespecificeerd door de organisatie;

d) eisen vanuit wet- en regelgeving die van toepassing zijn op de producten en diensten;

e) eisen uit het contract of uit opdrachten die afwijken van eisen die eerder kenbaar zijn gemaakt.

De organisatie moet bewerkstelligen dat er een oplossing wordt gevonden voor eisen uit het contract of uit opdrachten die afwijken van eisen die eerder kenbaar zijn gemaakt. De eisen van de klant moeten voorafgaand aan aanvaarding door de organisatie worden bevestigd wanneer de klant geen gedocumenteerde verklaring van diens eisen bezorgt.

De organisatie moet, voor zover van toepassing, gedocumenteerde informatie bijhouden:

a) over de resultaten van de beoordeling;

b) over eventuele nieuwe eisen voor de producten en diensten.

Wanneer de eisen voor producten en diensten worden veranderd moet de organisatie bewerkstelligen dat relevante gedocumenteerde informatie wordt aangepast en dat relevante personen op de hoogte worden gesteld van de gewijzigde eisen.

III. Ontwerp en ontwikkeling van producten en diensten

De organisatie moet een ontwerp- en ontwikkelproces vaststellen, implementeren en onderhouden dat passend is om de aansluitende levering van producten en diensten te bewerkstelligen.

Bij het vaststellen van de stappen en beheersmaatregelen voor ontwerp en ontwikkeling moet de organisatie

rekening houden met:

a) de aard, duur en complexiteit van de ontwerp- en ontwikkelactiviteiten;

b) de vereiste processtappen, waaronder de van toepassing zijnde ontwerp- en ontwikkelingsbeoordelingen;

c) de vereiste activiteiten voor verificatie en validatie in het kader van ontwerp en ontwikkeling;

d) de bij het ontwerp- en ontwikkelingsproces betrokken verantwoordelijkheden en bevoegdheden;

e) de behoeften aan interne en externe middelen voor het ontwerpen en ontwikkelen van producten en diensten;

f) de noodzaak interfaces tussen personen die betrokken zijn bij het ontwerp- en ontwikkelproces te beheersen;

g) de noodzaak klanten en gebruikers bij het ontwerp- en ontwikkelproces te betrekken;

h) de eisen voor de aansluitende levering van producten en diensten;

i) de mate van beheersing die door klanten en andere relevante belanghebbenden wordt verwacht voor het ontwerp- en ontwikkelproces;

j) de gedocumenteerde informatie die nodig is om aan te tonen dat aan de ontwerp- en ontwikkeleisen is voldaan.

De organisatie moet de eisen vaststellen die essentieel zijn voor de specifieke soorten producten en diensten die moeten worden ontworpen en ontwikkeld. De organisatie moet rekening houden met:

a) functionele en prestatie-eisen;

b) informatie die is verkregen van eerdere, vergelijkbare ontwerp- en ontwikkelactiviteiten;

c) eisen uit wet- en regelgeving;

d) normen of gedragscodes tot de implementatie waarvan de organisatie zich verbonden heeft;

e) de mogelijke gevolgen van falen vanwege de aard van de producten en diensten.

Inputs moeten toereikend zijn voor ontwerp- en ontwikkeldoeleinden, volledig en ondubbelzinnig. Tegenstrijdigheden ten aanzien van ontwerp- en ontwikkelingsinputs moeten worden opgelost. De organisatie moet gedocumenteerde informatie over ontwerp- en ontwikkelingsinputs bijhouden.

De organisatie moet beheersmaatregelen op het ontwerp- en ontwikkelproces toepassen om te bewerkstelligen dat:

a) de te behalen resultaten worden gedefinieerd;

b) beoordelingen worden uitgevoerd om te evalueren of de resultaten van ontwerp en ontwikkeling in staat zijn te voldoen aan de eisen;

c) verificatieactiviteiten worden uitgevoerd om ervoor te zorgen dat de ontwerp- en ontwikkelingsoutputs aan de inputeisen voldoen;

d) activiteiten voor validatie worden uitgevoerd om ervoor te zorgen dat de resulterende producten en diensten aan de eisen voor de gespecificeerde toepassing of het beoogde gebruik voldoen;

e) eventueel benodigde maatregelen worden getroffen voor problemen die worden vastgesteld tijdens de beoordelingen of tijdens verificatie- en validatieactiviteiten;

f) er gedocumenteerde informatie van deze activiteiten wordt bijgehouden.

De organisatie moet bewerkstelligen dat de ontwerp- en ontwikkelingsoutputs:

a) voldoen aan de inputeisen;

b) toereikend zijn voor de aansluitende processen voor het leveren van producten en diensten;

c) geschikte eisen voor monitoren en meten en acceptatiecriteria omvatten of daarnaar verwijzen;

d) de kenmerken specificeren van de producten en diensten die essentieel zijn voor het beoogde doel ervan en voor veilige en juiste levering ervan.

De organisatie moet gedocumenteerde informatie over ontwerp- en ontwikkelingsoutputs bijhouden.

De organisatie moet wijzigingen identificeren, beoordelen en beheersen die zijn aangebracht tijdens of na het ontwerpen en ontwikkelen van producten en diensten, in de mate die nodig is om te bewerkstelligen dat er geen nadelige gevolgen zijn voor het voldoen aan eisen. De organisatie moet gedocumenteerde informatie bijhouden over:

a) wijzigingen met betrekking tot ontwerp en ontwikkeling;

b) de resultaten van beoordelingen;

c) de goedkeuring van de wijzigingen;

d) de maatregelen die zijn genomen om nadelige gevolgen te voorkomen.

IV. Beheersing van extern geleverde processen, producten en diensten

De organisatie moet bewerkstelligen dat extern geleverde processen, producten en diensten aan de eisen voldoen. De organisatie moet de beheersmaatregelen vaststellen die moeten worden toegepast op extern geleverde processen, producten en diensten wanneer:

a) producten en diensten van externe aanbieders bedoeld zijn om opgenomen te worden in de eigen producten en diensten van de organisatie;

b) producten en diensten rechtstreeks door externe aanbieders namens de organisatie aan de klant(en) worden geleverd;

c) een proces of deel van een proces door een externe aanbieder wordt geleverd als gevolg van een besluit door de organisatie.

De organisatie moet criteria vaststellen en toepassen voor het evalueren, selecteren, monitoren van de prestaties van, en het opnieuw evalueren van externe aanbieders, op basis van hun vermogen om overeenkomstig eisen in processen of producten en diensten te voorzien. De organisatie moet gedocumenteerde informatie bijhouden over deze activiteiten en over eventuele benodigde maatregelen die voortkomen uit deze evaluaties.

De organisatie moet bewerkstelligen dat door externe aanbieders geleverde processen, producten en diensten niet het vermogen van de organisatie nadelig beïnvloeden, om op consistente wijze producten en diensten aan haar klanten te leveren die aan de eisen voldoen. De organisatie moet:

a) bewerkstelligen dat extern geleverde processen binnen de invloedsfeer van haar kwaliteitsmanagementsysteem blijven;

b) zowel de beheersmaatregelen definiëren die zij voornemens is toe te passen op een externe aanbieder als de beheersmaatregelen die zij voornemens is toe te passen op de output die daarvan het gevolg is;

c) rekening houden met:

1) de mogelijke gevolgen van de door externe aanbieders geleverde processen, producten en diensten voor het vermogen van de organisatie om op consistente wijze aan de eisen van de klant en de van toepassing zijnde eisen van wet- en regelgeving te voldoen;

2) de doeltreffendheid van de door de externe aanbieder toegepaste beheersmaatregelen;

d) bepalen welke verificatie- of andere activiteiten nodig zijn om ervoor te zorgen dat de door externe aanbieders geleverde processen, producten en diensten aan de eisen voldoen.

De organisatie moet ervoor zorgen dat de eisen toereikend zijn alvorens deze kenbaar te maken aan de externe aanbieder. De organisatie moet aan externe aanbieders haar eisen kenbaar maken voor:

a) de te leveren processen, producten en diensten;

b) de goedkeuring van:

1) producten en diensten;

2) methoden, processen en uitrusting;

3) de vrijgave van producten en diensten;

c) competentie, inclusief de eventueel vereiste kwalificatie van personen;

d) de interacties van de externe aanbieders met de organisatie;

e) door de organisatie toe te passen beheersing en monitoring van de prestaties van de externe aanbieders;

f) verificatie- of validatieactiviteiten die de organisatie, of haar klant, voornemens is uit te voeren op locatie bij de externe aanbieders

V. Productie en het leveren van diensten

De organisatie moet de productie en het leveren van diensten onder beheerste omstandigheden implementeren. Beheerste omstandigheden moeten, voor zover van toepassing, bestaan uit:

a) de beschikbaarheid van gedocumenteerde informatie waarin wordt gedefinieerd:

1) de kenmerken van de te produceren producten, de te leveren diensten of de uit te voeren activiteiten;

2) de te behalen resultaten;

b) de beschikbaarheid en het gebruik van geschikte middelen voor monitoren en meten;

c) de uitvoering van monitoring- en meetactiviteiten op passende momenten in het proces om te verifiëren of aan de criteria voor het beheersen van processen of outputs en aan de aanvaardingscriteria voor producten en diensten is voldaan;

d) het gebruik van geschikte infrastructuur en een geschikte omgeving voor de uitvoering van processen;

e) de benoeming van competente personen, met inbegrip van de eventueel vereiste kwalificatie;

f) de validatie en periodieke hervalidatie van het vermogen van de processen voor productie en het leveren van diensten om geplande resultaten te behalen, waar de resulterende output niet kan worden geverifieerd door aansluitende monitoring of meting;

g) de implementatie van maatregelen om menselijke fouten te voorkomen;

h) de uitvoering van activiteiten op het gebied van vrijgave, aflevering en nazorg.

De organisatie moet gebruikmaken van geschikte middelen voor het identificeren van outputs als het nodig is om de conformiteit van producten en diensten te bewerkstelligen. De organisatie moet gedurende het gehele proces van productie en het leveren van diensten de status van outputs ten aanzien van eisen aan monitoring en meten identificeren. De organisatie moet de unieke identificatie van de outputs beheersen indien naspeurbaarheid een eis is en moet de gedocumenteerde informatie bijhouden die nodig is om naspeurbaarheid mogelijk te maken.

De organisatie moet zorgvuldig omgaan met eigendom van klanten of externe aanbieders wanneer dit door de organisatie wordt beheerd of gebruikt. De organisatie moet eigendom van klanten of externe aanbieders dat is geleverd voor gebruik of om deel uit te maken van de producten en diensten identificeren, verifiëren, beschermen en beveiligen. Als het eigendom van een klant of externe aanbieder verloren of beschadigd raakt of anderszins ongeschikt wordt geacht voor gebruik, dan moet de organisatie dit aan de klant of externe aanbieder melden en gedocumenteerde informatie bijhouden over wat er zich heeft voorgedaan.

De organisatie moet de outputs tijdens de productie en het leveren van diensten in stand houden in de mate die nodig is om te bewerkstelligen dat aan de eisen wordt voldaan.

De organisatie moet wijzigingen voor productie of het leveren van diensten beoordelen en beheersen in de mate die nodig is om te bewerkstelligen dat aan de eisen blijft worden voldaan. De organisatie moet gedocumenteerde informatie bijhouden over de resultaten van de beoordeling van wijzigingen, de perso(o)n(en) die toestemming geeft/geven voor de wijziging en eventuele noodzakelijke maatregelen die voortkomen uit de beoordeling.

VI. Vrijgave van producten en diensten

De organisatie moet geplande maatregelen implementeren, op passende momenten in het proces, om te verifiëren of aan de eisen die aan de producten en diensten zijn gesteld is voldaan. De vrijgave van producten en diensten aan de klant mag niet plaatsvinden voordat de geplande maatregelen naar tevredenheid zijn afgerond, tenzij dit op andere wijze is goedgekeurd door een relevante autoriteit en, voor zover van toepassing, door de klant. De organisatie moet gedocumenteerde informatie bijhouden over de vrijgave van producten en diensten. De gedocumenteerde informatie moet onder andere bestaan uit:

a) bewijs van het voldoen aan de aanvaardingscriteria;

b) naspeurbaarheid tot de personen die toestemming heeft of hebben gegeven voor de vrijgave.

VII. Beheersing van afwijkende outputs

De organisatie moet bewerkstelligen dat outputs die niet voldoen aan haar eisen worden geïdentificeerd en beheerst om niet-beoogd gebruik of levering ervan te voorkomen. De organisatie moet passende maatregelen nemen op basis van de aard van de afwijking en het effect ervan op het voldoen aan de eisen van producten en diensten. Dit geldt ook voor producten en diensten die na de

levering van producten en/of tijdens of na de verlening van diensten afwijkend blijken te zijn. De organisatie moet op een of meer van de volgende manieren met afwijkende outputs omgaan:

a) herstellen;

b) scheiden, afzonderen, terugzenden of onderbreken van de levering van producten en diensten;

c) de klant op de hoogte stellen;

d) machtiging verkrijgen voor aanvaarding met toestemming (concessie).

Het voldoen aan de eisen moet worden geverifieerd wanneer afwijkende outputs zijn gecorrigeerd.

De organisatie moet gedocumenteerde informatie bijhouden die:

a) de afwijking beschrijft;

b) de genomen maatregelen beschrijft;

c) elke verkregen uitzondering beschrijft;

d) identificeert welke gemachtigde heeft beslist over de maatregel met betrekking tot de afwijking.

6. Evaluatie van de prestaties

I. Monitoren, meten, analyseren en evalueren

De organisatie moet vaststellen:

a) wat moet worden gemonitord en gemeten;

b) welke methoden nodig zijn voor het monitoren, meten, analyseren en evalueren om geldige resultaten te bewerkstelligen;

c) wanneer moet worden gemonitord en gemeten;

d) wanneer de resultaten van het monitoren en meten moeten worden geanalyseerd en geëvalueerd.

De organisatie moet de prestaties en de doeltreffendheid van het kwaliteitsmanagementsysteem evalueren. De organisatie moet geschikte gedocumenteerde informatie bijhouden als bewijs van de resultaten.

De organisatie moet de perceptie van klanten over de mate waarin aan hun behoeften en verwachtingen is voldaan monitoren. De organisatie moet de methoden voor het verkrijgen, monitoren en beoordelen van deze informatie vaststellen.

De organisatie moet geschikte gegevens en informatie analyseren en evalueren die voortkomen uit monitoren en meten. De analyseresultaten moeten worden gebruikt voor het evalueren van:

a) het voldoen aan de eisen van producten en diensten;

b) de mate van klanttevredenheid;

c) de prestaties en doeltreffendheid van het kwaliteitsmanagementsysteem;

d) de doeltreffendheid waarmee plannen zijn geïmplementeerd;

e) de doeltreffendheid van ondernomen acties voor het aanpakken van risico's en kansen;

f) de prestaties van externe aanbieders;

g) de noodzaak van verbeteringen aan het kwaliteitsmanagementsysteem.

II. Interne audit

De organisatie moet met geplande tussenpozen interne audits uitvoeren om informatie te verkrijgen of het kwaliteitsmanagementsysteem:

a) voldoet aan:

1) de eigen eisen van de organisatie voor haar kwaliteitsmanagementsysteem;

2) de eisen van deze internationale norm;

b) doeltreffend is geïmplementeerd en onderhouden.

De organisatie moet:

a) (een) auditprogramma('s) plannen, vaststellen, implementeren en onderhouden, met inbegrip van de frequentie, methoden, verantwoordelijkheden, planningseisen en rapportage, waarbij rekening moet worden gehouden met het belang van de betrokken processen, met veranderingen die van invloed zijn op de organisatie, en met de resultaten van voorgaande audits;

b) de auditcriteria voor en de reikwijdte van elke audit definiëren;

c) auditoren selecteren en audits uitvoeren zodanig dat de objectiviteit en de onpartijdigheid van het auditproces worden bewerkstelligd;

d) bewerkstelligen dat de resultaten van de audits worden gerapporteerd aan het relevante management;

e) zonder onnodig uitstel passende correcties en corrigerende maatregelen doorvoeren;

f) gedocumenteerde informatie bijhouden als bewijs van de implementatie van het auditprogramma en de auditresultaten.

III. Directiebeoordeling

De directie moet met geplande tussenpozen het kwaliteitsmanagementsysteem van de organisatie beoordelen om de continue geschiktheid, toereikendheid, doeltreffendheid en afstemming met de strategische richting van de organisatie te bewerkstelligen.

De directiebeoordeling moet worden gepland en uitgevoerd, waarbij het volgende wordt overwogen:

a) de status van acties die zijn voortgekomen uit voorgaande directiebeoordelingen;

b) wijzigingen in externe en interne belangrijke punten (issues) die relevant zijn voor het kwaliteitsmanagementsysteem;

c) informatie over de prestaties en doeltreffendheid van het kwaliteitsmanagementsysteem, met inbegrip van trends in:

1) klanttevredenheid en feedback van relevante belanghebbenden;

2) de mate waarin kwaliteitsdoelstellingen zijn gerealiseerd;

3) prestaties van processen en het voldoen aan eisen van producten en diensten;

4) afwijkingen en corrigerende maatregelen;

5) resultaten van monitoren en meten;

6) auditresultaten;

7) de prestaties van externe aanbieders;

d) de toereikendheid van middelen;

e) de doeltreffendheid van ondernomen acties voor het aanpakken van risico's en kansen;

f) kansen voor verbetering.

De resultaten van de directiebeoordeling moeten beslissingen en acties omvatten met betrekking tot:

a) kansen voor verbetering;

b) de noodzaak voor wijzigingen in het kwaliteitsmanagementsysteem;

c) behoefte aan middelen.

De organisatie moet gedocumenteerde informatie bijhouden als bewijs van de resultaten van de directiebeoordeling.

7. Verbetering

I. Vaststellen verbeteringen

De organisatie moet kansen voor verbetering vaststellen en selecteren en de benodigde maatregelen implementeren om te voldoen aan de eisen van klanten en de klanttevredenheid te verhogen. Dit moet omvatten:

a) het verbeteren van producten en diensten om zowel te voldoen aan de eisen als in te gaan op de toekomstige behoeften en verwachtingen;

b) het corrigeren, voorkomen of verminderen van ongewenste effecten;

c) het verbeteren van de prestaties en doeltreffendheid van het kwaliteitsmanagementsysteem.

II. Afwijkingen en corrigerende maatregelen

Wanneer zich een afwijking voordoet, waaronder elke afwijking die aan het licht komt door een klacht, moet de organisatie:

a) op de afwijking reageren, en indien van toepassing:

1) maatregelen treffen om de afwijking te beheersen en te corrigeren;

2) de consequenties aanpakken;

b) de noodzaak evalueren om maatregelen te treffen om de oorzaken van de afwijking weg te nemen, zodat de afwijking zich niet herhaalt of zich elders voordoet, door:

1) de afwijking te beoordelen en te analyseren;

2) de oorzaken van de afwijking vast te stellen;

3) vast te stellen of zich gelijksoortige afwijkingen voordoen of zouden kunnen voordoen;

c) de benodigde maatregelen implementeren;

d) de doeltreffendheid van getroffen corrigerende maatregelen beoordelen;

e) risico's en kansen actualiseren die zijn vastgesteld tijdens het plannen, indien nodig;

f) zo nodig, wijzigingen aanbrengen in het kwaliteitsmanagementsysteem.

Corrigerende maatregelen moeten passend zijn voor de effecten van de opgetreden afwijkingen.

De organisatie moet gedocumenteerde informatie bijhouden als bewijs van:

a) de aard van de afwijkingen en de vervolgens genomen maatregelen;

b) de resultaten van corrigerende maatregelen.

III. Continue verbetering

De organisatie moet continu de geschiktheid, toereikendheid en doeltreffendheid van het kwaliteitsmanagementsysteem verbeteren. De organisatie moet rekening houden met de resultaten van analyse en evaluatie en de outputs uit directiebeoordelingen om te bepalen of er behoeften of kansen zijn die in het kader van continue verbetering moeten worden aangepakt.

COBIT

Evaluate, Direct and Monitor

1. EDM01: Ensure Governance Framework Setting and Maintenance

Beschrijving: Analyseer en formuleer de vereisten voor het bestuur van bedrijfs-IT en zorg voor effectieve ondersteunende structuren, principes, processen en werkwijzen met duidelijke verantwoordelijkheden en bevoegdheden om de missie, doelen en doelstellingen van het bedrijf te bereiken.

Doel: Zorg voor een consistente aanpak, geïntegreerd en afgestemd op de aanpak van ondernemingsbestuur. Om ervoor te zorgen dat IT-gerelateerde beslissingen worden genomen in overeenstemming met de strategieën en doelstellingen van de onderneming, moet ervoor worden gezorgd dat IT-gerelateerde processen effectief en transparant worden gecontroleerd, naleving van wettelijke en regelgevende vereisten wordt bevestigd en aan de governancevereisten voor bestuursleden wordt voldaan.

EDM01.01: Evalueer het governance systeem

EDM01.02: Leid het governance systeem

EDM01.03: Monitor het governance systeem

2. EDM02: Ensure Benefits Delivery

Beschrijving: Optimaliseer de toegevoegde waarde aan het bedrijf van de bedrijfsprocessen, IT-services en IT-middelen die resulteren uit investeringen door IT, tegen aanvaardbare kosten.

Doel: Optimale waarde verzekeren van IT-initiatieven, -services en -activa; kostenefficiënte levering van oplossingen en diensten; en een betrouwbaar en accuraat beeld van kosten en waarschijnlijke voordelen, zodat bedrijfsbehoeften effectief en efficiënt worden ondersteund.

EDM02.01: Evalueer de waarde optimalisatie

EDM02.02: Stuur de waarde optimalisatie

EDM02.03: Monitor de waarde optimalisatie

3. EDM03: Ensure Risk Optimisation

Beschrijving: Zorg ervoor dat de risicobereidheid en tolerantie van de onderneming worden begrepen, gearticuleerd en gecommuniceerd en dat het risico voor bedrijfswaarde gerelateerd aan het gebruik van IT wordt geïdentificeerd en beheerd.

Doel: Zorg ervoor dat IT-gerelateerd ondernemingsrisico de risicobereidheid en risicotolerantie niet overschrijdt, dat de impact van IT-risico's op de bedrijfswaarde wordt geïdentificeerd en beheerd, en dat het potentieel voor nalevingsproblemen wordt geminimaliseerd.

EDM03.01: Evalueer risicomanagement

EDM03.02: Stuur risicomanagement

EDM03.03: Monitor risicomanagement

4. EDM04: Ensure Resource Optimisation

Beschrijving: Zorgen voor degelijke en voldoende IT-gerelateerde bronnen (mensen, processen en technologie) om effectieve bedrijfsdoelstellingen te ondersteunen tegen optimale kosten.

Doel: Ervoor zorgen dat aan de resourcebehoeften van de onderneming optimaal wordt voldaan, IT-kosten worden geoptimaliseerd en er een verhoogde kans is op het realiseren van voordelen en de bereidheid voor toekomstige verandering.

EDM04.01: Evalueer resource management

EDM04.02: Stuur resource management

EDM04.03: Monitor resource management

5. EDM05: Ensure Stakeholder Transparency

Beschrijving: Zorg dat de IT-prestaties en conformiteitsmeting en rapportage van ondernemingen transparant zijn, waarbij stakeholders de doelen en statistieken en de noodzakelijke herstelmaatregelen goedkeuren.

Doel: Zorg ervoor dat de communicatie met belanghebbenden effectief en tijdig is en dat de basis voor rapportage is vastgesteld om de prestaties te verbeteren, verbeterpunten te identificeren en te bevestigen dat IT-gerelateerde doelstellingen en strategieën in lijn zijn met de bedrijfsstrategie.

EDM05.01: Evalueer de rapportagevereisten voor belanghebbenden.

EDM05.02: Stuur de stakeholder communicatie en rapportage

EDM05.03: Monitor stakeholder communicatie

Align, Plan and Organise

1. APO01: Manage the IT management framework

Beschrijving: Verduidelijken en onderhouden van het bestuur van de onderneming haar IT missie en visie. Mechanismen en autoriteiten implementeren en onderhouden om informatie en het gebruik van IT in de onderneming te beheren ter ondersteuning van de doelstellingen van het bestuur in overeenstemming met de leidende beginselen en beleidslijnen.

Doel: Zorgen voor een consistente managementaanpak om te voldoen aan de eisen van bedrijfsgovernance met betrekking tot managementprocessen, organisatiestructuren, rollen en verantwoordelijkheden, betrouwbare en reproduceerbare activiteiten en vaardigheden en competenties.

APO01.01: Definieer de organisatiestructuur.

APO01.02: Functies en verantwoordelijkheden vaststellen.

APO01.03: Beheer de enablers van het managementsysteem.

APO01.04: Communiceer management doelstellingen en richting.

APO01.05: Optimaliseer de plaatsing van de IT-functie.

APO01.06: Definieer het eigendom van informatiegegevens en het systeem.

APO01.07: Het continue verbetering van processen beheren.

APO01.08: Het naleven van beleid en procedures.

2. APO02: Manage strategy

Beschrijving: Geef een holistisch beeld van de huidige bedrijfs- en IT-omgeving, de toekomstige richting en de initiatieven die nodig zijn om de gewenste toekomstige omgeving te bereiken. Gebruik bouwstenen en componenten van bedrijfsarchitectuur, inclusief extern geleverde services en gerelateerde mogelijkheden om lenig, betrouwbaar en efficiënt te reageren op strategische doelstellingen.

Doel: Breng strategische IT-plannen op één lijn met zakelijke doelstellingen. Communiceer duidelijk de doelstellingen en bijbehorende verantwoordelijkheden, zodat deze door iedereen worden begrepen, met de strategische IT-opties die zijn geïdentificeerd, gestructureerd en geïntegreerd met de bedrijfsplannen.

APO02.01: begrijp de richting van de onderneming.

APO02.02: Beoordeel de huidige omgeving, mogelijkheden en prestaties.

APO02.03: Definieer de IT-mogelijkheden.

APO02.04: Voer een gap-analyse uit.

APO02.05: Definieer het strategisch plan en de routekaart.

APO02.06: Communiceer de IT-strategie en -richting.

3. APO03: Manage enterprise architecture

Beschrijving: Breng een gemeenschappelijke architectuur tot stand die bestaat uit bedrijfsprocessen, informatie, gegevens, applicatie- en technologie architectuur voor het effectief en efficiënt realiseren van bedrijfs- en IT-strategieën door sleutelmodellen en praktijken te creëren die de basis- en doelarchitecturen beschrijven. Definieer vereisten voor taxonomie, normen, richtlijnen, procedures, sjablonen en hulpmiddelen en zorg voor een link tussen deze componenten. Verbeter de afstemming, verhoog de wendbaarheid, verbeter de kwaliteit van de informatie en genereer potentiële kostenbesparingen door initiatieven zoals het hergebruik van bouwsteencomponenten.

Doel: Vertegenwoordig de verschillende bouwstenen waaruit de onderneming bestaat en hun onderlinge relaties, alsmede de principes die hun ontwerp en evolutie in de loop van de tijd sturen,

waardoor een standaard, responsieve en efficiënte levering van operationele en strategische doelstellingen mogelijk wordt.

APO03.01: Ontwikkel een visie voor de bedrijfsarchitectuur.

APO03.02: De referentiearchitectuur definiëren.

APO03.03: Selecteer kansen en oplossingen.

APO03.04: Architectuurimplementatie definiëren.

APO03.05: Enterprise-architectuurdiensten bieden.

4. APO04: Manage innovation

Beschrijving: Bewust blijven van informatietechnologie en gerelateerde servicetrends, innovatiekansen identificeren en plannen om te profiteren van innovatie in relatie tot bedrijfsbehoeften. Analyseer welke kansen voor bedrijfsinnovatie of -verbetering kunnen worden gecreëerd door opkomende technologieën, diensten of IT gerelateerde bedrijfsinnovatie, evenals door bestaande gevestigde technologieën en door innovatie van bedrijven en IT-processen. Beïnvloeden strategische planning en enterprise-architectuur beslissingen.

Doel: Bereik concurrentievoordeel, bedrijfsinnovatie en verbeterde operationele effectiviteit en efficiëntie door gebruik te maken van ontwikkelingen op het gebied van informatietechnologie.

APO04.01: een omgeving creëren die bevorderlijk is voor innovatie.

APO04.02: begrip van de bedrijfsomgeving behouden.

APO04.03: Bewaak en scan de technologieomgeving.

APO04.04: Beoordeel het potentieel van opkomende technologieën en ideeën voor innovatie.

APO04.05: Beveel passende verdere initiatieven aan.

APO04.06: Monitor de implementatie en gebruik van innovatie.

5. APO05: Manage portfolio

Beschrijving: Voer de strategische richting uit die is opgesteld voor investeringen in lijn met de visie van de bedrijfsarchitectuur en de gewenste kenmerken van de investering en gerelateerde servicesportfolio's en houd rekening met de verschillende categorieën van investeringen en de resources en financieringsbeperkingen. Evalueer, prioriteer en balanceer programma's en diensten, beheer de vraag binnen resource- en financieringsbeperkingen, op basis van hun afstemming op strategische doelstellingen, ondernemingswaarde en risico's. Verplaats geselecteerde programma's naar de actieve dienstenportfolio voor uitvoering. Bewaak de prestaties van de algehele portfolio van services en programma's en dien overeenkomstige aanpassingen voor, in reactie op programma- en serviceprestaties of veranderende bedrijfsprioriteiten.

Doel: Optimaliseer de prestaties van het totale portfolio van programma's als reactie op programma- en serviceprestaties of veranderende prioriteiten en eisen van bedrijven.

APO05.01: Stel de beoogde investeringsmix vast.

APO05.02: Bepaal de beschikbaarheid en bronnen van fondsen.

APO05.03: Evalueer en selecteer programma's om te financieren.

APO05.04: Monitor, optimaliseer en rapporteer over de prestaties van investeringssportefeuilles.

APO05.05: Portefeuilles onderhouden.

APO05.06: Voordelen behalen.

6. APO06: Manage budget and costs

Beschrijving: Beheer de IT-gerelateerde financiële activiteiten in zowel de bedrijfs- als IT-functies, met inbegrip van budget-, kosten- en baten-management en prioriteriseren van uitgaven door het gebruik van formele budgetteringspraktijken en een rechtvaardig systeem voor het toewijzen van kosten aan de onderneming. Raadpleeg belanghebbenden om de totale kosten en baten te identificeren en te beheersen in het kader van de strategische en tactische IT-plannen en corrigeer indien nodig actie.

Doel: Het bevorderen van partnerschappen tussen IT en stakeholders in het bedrijfsleven om effectief en efficiënt gebruik van IT-gerelateerde middelen mogelijk te maken en transparantie en verantwoording te verschaffen over de kosten en zakelijke waarde van oplossingen en diensten. Stel de onderneming in staat weloverwogen beslissingen te nemen met betrekking tot het gebruik van IT-oplossingen en -diensten.

APO06.01: Beheer financiën en boekhouding.

APO06.02: Prioritering van toewijzing van middelen.

APO06.03: Begrotingen maken en onderhouden.

APO06.04: Kosten modelleren en toewijzen.

APO06.05: Kosten beheren.

7. APO07: Manage human resources

Beschrijving: Zorg voor een gestructureerde aanpak om te zorgen voor optimale structurering, plaatsing, beslissingsrechten en vaardigheden van menselijke hulpbronnen. Dit omvat het communiceren van de gedefinieerde rollen en verantwoordelijkheden, leer- en groeiplannen en prestatieverwachtingen, ondersteund door bekwame en gemotiveerde mensen.

Doel: Optimaliseer human resources-capaciteiten om te voldoen aan bedrijfsdoelstellingen.

APO07.01: Zorg voor voldoende en passende personeelsbezetting.

APO07.02: Identificeer het belangrijkste IT-personeel.

APO07.03: De vaardigheden en bekwaamheden van het personeel behouden.

APO07.04: Werkprestaties van werknemers evalueren.

APO07.05: Plan en volg het gebruik van IT en bedrijfspersoneel.

APO07.06: Contractpersoneel beheren.

8. APO08: Manage relationships

Beschrijving: Beheer de relatie tussen het bedrijf en IT op een geformaliseerde en transparante manier die zorgt voor een focus op het bereiken van een gemeenschappelijk en gedeeld doel van succesvolle bedrijfsresultaten ter ondersteuning van strategische doelen en binnen de beperking van budgetten en risicotoleranties. Baseer de relatie op wederzijds vertrouwen, gebruik makend van open en begrijpelijke termen en gemeenschappelijke taal en bereidheid om eigenaar te worden en verantwoording af te leggen voor belangrijke beslissingen.

Doel: Verbeter resultaten, vergroot vertrouwen, vertrouw op IT en effectief gebruik van middelen.

APO08.01: Zakelijke verwachtingen begrijpen.

APO08.02: Identificeer kansen, risico's en beperkingen voor IT om het bedrijf te verbeteren.

APO08.03: Beheer de zakelijke relatie.

APO08.04: Coördineren en communiceren.

APO08.05: Geef input voor de continue verbetering van services.

9. APO09: Manage service agreements

Beschrijving: Breng IT-services en serviceniveaus op één lijn met de behoeften en verwachtingen van het bedrijf, inclusief identificatie, specificatie, ontwerp, publicatie, overeenkomst en bewaking van IT-services, serviceniveaus en prestatie-indicatoren.

Doel: Ervoor zorgen dat IT-services en serviceniveaus voldoen aan de huidige en toekomstige bedrijfsbehoeften.

APO09.01: IT-services identificeren.

APO09.02: Catalogiseren van IT-services.

APO09.03: Servicecontracten definiëren en voorbereiden.

APO09.04: Serviceniveaus controleren en rapporteren.

APO09.05: Servicecontracten en contracten bekijken.

10. APO10: Manage suppliers

Beschrijving: Beheer van IT-gerelateerde services die worden aangeboden door alle typen leveranciers om te voldoen aan de bedrijfsvereisten, waaronder de selectie van leveranciers, het

beheer van relaties, het beheer van contracten en het beoordelen en bewaken van leveranciersprestaties op effectiviteit en naleving.

Doel: Minimaliseer het risico dat verbonden is aan niet-presterende leveranciers en zorg voor concurrerende prijzen.

APO10.01: Identificeer en evalueer leveranciersrelaties en contracten.

APO10.02: Leveranciers selecteren.

APO10.03: Relaties en contracten met leveranciers beheren.

APO10.04: Leveranciersrisico beheren.

APO10.05: Bewaak de prestaties en naleving van leveranciers.

11. APO11: Manage quality

Beschrijving: Definieer en communiceer kwaliteitsvereisten van alle processen, procedures en de gerelateerde bedrijfsresultaten, inclusief controles, monitoring en het gebruik van geteste werkwijzen en standaarden voor continue verbetering en efficiëntie.

Doel: Zorg voor een consistente levering van oplossingen en diensten om te voldoen aan de kwaliteitseisen van de onderneming en aan de behoeften van de belanghebbenden.

APO11.01: een quality management system (QMS) opzetten.

APO11.02: Kwaliteitsnormen, -praktijken en -procedures definiëren en beheren.

APO11.03: Focus kwaliteitsbeheer op klanten.

APO11.04: Kwaliteit monitoren, controleren en beoordelen.

APO11.05: Integreer kwaliteitsmanagement in oplossingen voor ontwikkeling en servicelevering.

APO11.06: Continue verbetering handhaven.

12. APO12: Manage risk

Beschrijving: Voortdurend IT-gerelateerde risico’s identificeren, beoordelen en verminderen binnen tolerantieniveaus die door het uitvoerend management van ondernemingen zijn vastgesteld.

Doel: Integreer het beheer van IT-gerelateerd ondernemingsrisico met het algehele ERM systeem en breng een balans tussen de kosten en baten van het beheer van IT-gerelateerd ondernemingsrisico.

APO12.01: Gegevens verzamelen.

APO12.02: Risico analyseren.

APO12.03: Handhaven van een risicoprofiel.

APO12.04: Risico's blootstellen.

APO12.05: Definieer een actieportfolio voor risicobeheer.

APO12.06: Reageren op risico.

13. APO13: Manage security

Beschrijving: Definieer, bedien en monitor een systeem voor informatiebeveiligingsbeheer.

Doel: Houd de impact en het voorkomen van informatiebeveiligingsincidenten binnen de risicobereidheidsniveaus van de onderneming.

APO13.01: Een Information Security Management System (ISMS) opzetten en onderhouden.

APO13.02: Een plan voor informatiebeveiligingstechnieken definiëren en beheren.

APO13.03: Monitor en beoordeel het ISMS.

Build, Acquire and Implement

1. BAI01:Manage programmes and projects.

Beschrijving: Beheer alle programma's en projecten uit de investeringsportefeuille in lijn met de bedrijfsstrategie en op een gecoördineerde manier. Initiëren, plannen, besturen en uitvoeren van programma's en projecten en afsluiten met een evaluatie na implementatie.

Doel: Realiseer zakelijke voordelen en verminder het risico van onverwachte vertragingen, kosten en waardeverminderingen door de communicatie naar en betrokkenheid van zakelijke en eindgebruikers te verbeteren, de waarde en kwaliteit van de projectresultaten te waarborgen en hun bijdrage aan de investerings- en dienstenportfolio te maximaliseren.

BAI01.01: Een standaardaanpak handhaven voor programma- en projectbeheer.

BAI01.02: een programma starten.

BAI01.03: Betrokkenheid van belanghebbenden beheren.

BAI01.04: Ontwikkel en onderhoud het programmaplan.

BAI01.05: Start en voer het programma uit.

BAI01.06: Monitor, beheer en rapporteer over de resultaten van het programma.

BAI01.07: Start projecten binnen een programma.

BAI01.08: Plan projecten.

BAI01.09: Beheer programma- en projectkwaliteit.

BAI01.10: Beheer van het programma- en projectrisico.

BAI01.11: Projecten controleren en besturen.

BAI01.12: Projectmiddelen en werkpakketten beheren.

BAI01.13: Een project of iteratie afsluiten.

BAI01.14: Een programma sluiten.

2. BAI02: Manage requirements definition.

Beschrijving: Identificeer oplossingen en analyseer vereisten voor acquisitie of creatie om er zeker van te zijn dat ze voldoen aan de strategische bedrijfsvereisten voor bedrijfsprocessen, applicaties, informatie / data, infrastructuur en services. Coördineren met betrokken belanghebbenden van de evaluatie van haalbare opties, waaronder relatieve kosten en baten, risicoanalyse en goedkeuring van eisen en voorgestelde oplossingen.

Doel: Maak haalbare optimale oplossingen die tegemoet komen aan de behoeften van het bedrijf, terwijl het risico wordt geminimaliseerd.

BAI02.01: Definieer en onderhoud zakelijke functionele en technische vereisten.

BAI02.02: Een haalbaarheidsstudie uitvoeren en alternatieve oplossingen formuleren.

BAI02.03: Beheer van het eisenrisico.

BAI02.04: Verkrijgen van goedkeuring van vereisten en oplossingen.

3. BAI03: Manage solutions identification and build.

Beschrijving: Vaststellen en onderhouden van geïdentificeerde oplossingen in overeenstemming met de vereisten van het bedrijf met betrekking tot ontwerp, ontwikkeling, inkoop en samenwerking met leveranciers / verkopers. Beheer configuratie, test voorbereiding, testen, managementvereisten en onderhoud van bedrijfsprocessen, applicaties, informatie / data, infrastructuur en services.

Doel: Tijdige en kost effectieve oplossingen opstellen die de strategische en operationele doelstellingen van het bedrijf kunnen ondersteunen.

BAI03.01: Ontwerpoplossingen op hoog niveau.

BAI03.02: Ontwerp van gedetailleerde oplossingscomponenten.

BAI03.03: Componenten van oplossingen ontwikkelen.

BAI03.04: Componenten van oplossingen kopen.

BAI03.05: Oplossingen bouwen.

BAI03.06: Kwaliteitsgarantie uitvoeren.

BAI03.07: Voorbereiden op testen van de oplossing.

BAI03.08: Testen van oplossingen uitvoeren.

BAI03.09: Wijzigingen in vereisten beheren.

BAI03.10: Oplossingen onderhouden.

BAI03.11: Definieer IT-services en onderhoud de serviceportfolio.

4. BAI04: Manage availability and capacity.

Beschrijving: Breng huidige en toekomstige behoeften in verband met beschikbaarheid, prestaties en capaciteit in evenwicht met kosteneffectieve dienstverlening. Neem beoordelingen op van de huidige mogelijkheden, voorspelling van toekomstige behoeften op basis van bedrijfsvereisten, analyse van bedrijfseffecten en beoordeling van risico om acties te plannen en uit te voeren om aan de vastgestelde vereisten te voldoen.

Doel: Onderhouden van beschikbaarheid van services, efficiënt beheer van resources en optimalisatie van systeemprestaties door voorspelling van toekomstige prestaties en capaciteitsvereisten.

BAI04.01: Beoordeel de huidige beschikbaarheid, prestaties en capaciteit en maak een basislijn.

BAI04.02: Impact van het bedrijf beoordelen.

BAI04.03: Plan voor nieuwe of gewijzigde dienstvereisten.

BAI04.04: Beschikbaarheid en capaciteit controleren en beoordelen.

BAI04.05: Onderzoek en verhelp de beschikbaarheid, prestaties en capaciteitsproblemen.

5. BAI05: Manage organisational change enablement.

Beschrijving: Maximaliseer de waarschijnlijkheid van het snel en met minder risico implementeren van duurzame ondernemingsverandering binnen bedrijven, over de volledige levenscyclus van de verandering en alle betrokken belanghebbenden in het bedrijf en IT.

Doel: Bereid belanghebbenden voor op bedrijfsverandering en beperk ze en verminder het faalrisico.

BAI05.01: Bepaal de wens om te veranderen.

BAI05.02: Vorm een effectief implementatieteam.

BAI05.03: Communiceer de gewenste visie.

BAI05.04: Bepaal de juiste werknemers en identificeer kortetermijnwinst.

BAI05.05: Bediening en gebruik inschakelen.

BAI05.06: Nieuwe benaderingen insluiten.

BAI05.07: Veranderingen in stand houden.

6. BAI06: Manage changes.

Beschrijving: Beheer alle veranderingen op een gecontroleerde manier, inclusief standaardwijzigingen en noodonderhoud met betrekking tot bedrijfsprocessen, applicaties en infrastructuur. Dit omvat wijzigingsnormen en procedures, effectbeoordeling, prioritisatie en autorisatie, noodwijzigingen, tracking, rapportage, afsluiting en documentatie.

Doel: Snelle en betrouwbare verandering van het bedrijf mogelijk maken en het risico van een negatieve invloed op de stabiliteit of integriteit van de gewijzigde omgeving beperken.

BAI06.01: Wijzigingsverzoeken evalueren, prioriteren en autoriseren.

BAI06.02: Noodveranderingen beheren.

BAI06.03: Wijzigingsstatus opvolgen en rapporteren.

BAI06.04: Sluit en documenteer de wijzigingen.

7. BAI07: Manage change acceptance and transitioning.

Beschrijving: Formuleer nieuwe operationele oplossingen en implementeer deze, inclusief implementatieplanning, systeem en dataconversie, acceptatietesten, communicatie, voorbereiding van de release, promotie tot productie van nieuwe of gewijzigde bedrijfsprocessen en IT-services, vroege productiesteun en een evaluatie na implementatie.

Doel: Implementeer oplossingen veilig en in overeenstemming met de overeengekomen verwachtingen en resultaten.

BAI07.01: Stel een implementatieplan op.

BAI07.02: Plan bedrijfsproces, systeem- en gegevensconversie.

BAI07.03: Plan acceptatietests.

BAI07.04: Een testomgeving instellen.

BAI07.05: Acceptatietests uitvoeren.

BAI07.06: Promoot de productie en beheer releases.

BAI07.07: Zorg voor vroege productiesteun.

BAI07.08: Een evaluatie na de implementatie uitvoeren.

8. BAI08: Manage knowledge.

Beschrijving: De beschikbaarheid van relevante, actuele, gevalideerde en betrouwbare kennis behouden om alle procesactiviteiten te ondersteunen en de besluitvorming te vergemakkelijken. Plan voor de identificatie, verzameling, organisatie, onderhoud, gebruik en behouden van kennis.

Doel: Bied de kennis die nodig is om alle medewerkers te ondersteunen bij hun werkzaamheden en voor gefundeerde besluitvorming en verbeterde productiviteit.

BAI08.01 Een kennisuitwisselingscultuur bevorderen en faciliteren.

BAI08.02: Bronnen van informatie identificeren en classificeren.

BAI08.03: Informatie in kennis organiseren en contextualiseren.

BAI08.04: Gebruik en deel kennis.

BAI08.05: Evalueer en behoud informatie.

9. BAI09: Manage assets

Beschrijving: Beheer IT-assets gedurende hun levenscyclus om ervoor te zorgen dat hun gebruik waarde oplevert tegen optimale kosten, ze blijven operationeel (fit for purpose), ze worden administratief en fysiek beschermd en de assets die essentieel zijn voor de ondersteuning van servicemogelijkheden zijn betrouwbaar en beschikbaar. Beheer softwarelicenties om ervoor te zorgen dat het optimale aantal wordt verkregen, bewaard en geïmplementeerd met betrekking tot het vereiste bedrijfsgebruik, en de geïnstalleerde software voldoet aan de licentieovereenkomsten.

Doel: Houd rekening met alle IT-activa en optimaliseer de waarde die door deze activa wordt geleverd.

BAI09.01: Identificeer en noteer de huidige activa.

BAI09.02: Kritieke bedrijfsmiddelen beheren.

BAI09.03: Beheer de levenscyclus van het activa.

BAI09.04: Activakosten optimaliseren.

BAI09.05: Licenties beheren.

10. BAI10: Manage configuration.

Beschrijving: Definieer en onderhoud beschrijvingen en relaties tussen essentiële resources en capaciteiten die vereist zijn voor het leveren van IT-services, waaronder het verzamelen van configuratie-informatie, het vaststellen van basislijnen, het verifiëren en controleren van configuratie-informatie en het bijwerken van de configuratieopslag.

Doel: Verstrek voldoende informatie over service-activa om de service effectief te kunnen beheren, bekijk de impact van wijzigingen en behandel incidenten.

BAI10.01: Stel een configuratiemodel op en onderhoud dit.

BAI10.02: Een configuratieopslagplaats en basislijn opzetten en onderhouden.

BAI10.03: Configuratie-items onderhouden en beheren.

BAI10.04: Status- en configuratierapporten produceren.

BAI10.05: Controleer en herzie de integriteit van de configuratieopslagplaats.

Deliver, Service and Support

1. DSS01: Manage operations.

Beschrijving: De activiteiten en operationele procedures coördineren en uitvoeren die nodig zijn voor het leveren van interne en externe IT-services, inclusief de uitvoering van vooraf gedefinieerde standaard operationele procedures en de vereiste monitoringactiviteiten.

Doel: Lever de resultaten van de operationele IT-service zoals gepland.

DSS01.01: Operationele procedures uitvoeren.

DSS01.02: Beheer van uitbestede IT-services.

DSS01.03: IT-infrastructuur monitoren.

DSS01.04: Beheer de omgeving.

DSS01.05: Beheer faciliteiten.

2. DSS02: Manage service requests and incidents.

Beschrijving: Geef tijdig en effectief antwoord op verzoeken van gebruikers en oplossing van alle soorten incidenten. Herstel de normale service; vastleggen en voldoen aan gebruikersverzoeken; en vastleggen, onderzoeken, diagnosticeren, escaleren en oplossen van incidenten.

Doel: Bereik een hogere productiviteit en minimaliseer storingen door snelle oplossing van gebruikersvragen en incidenten.

DSS02.01: Classificatiestelsels voor incidenten en serviceaanvragen definiëren.

DSS02.02: Verzoeken en incidenten registreren, classificeren en prioriteren.

DSS02.03: Verifiëren, goedkeuren en voldoen aan serviceaanvragen.

DSS02.04: Onderzoek, diagnosticeer en alloceer incidenten.

DSS02.05: Los op en herstel van incidenten.

DSS02.06: Serviceaanvragen en incidenten sluiten.

DSS02.07: Trackstatus en rapporten produceren.

3. DSS03: Manage problems.

Beschrijving: Identificeer en classificeer problemen en hun hoofdoorzaken en zorg voor een tijdige oplossing om terugkerende incidenten te voorkomen. Geef aanbevelingen voor verbeteringen.

Doel: Vergroot de beschikbaarheid, verbeter serviceniveaus, verlaag de kosten en verbeter het gemak en de tevredenheid van de klant door het aantal operationele problemen te verminderen.

DSS03.01: Problemen identificeren en classificeren.

DSS03.02: Onderzoek en diagnosticeer problemen.

DSS03.03: Bekende fouten verhogen.

DSS03.04: Problemen oplossen en sluiten.

DSS03.05: Proactief probleembeheer uitvoeren.

4. DSS04: Manage continuity.

Beschrijving: Stel een plan op en onderhoud dit zodat het bedrijf en IT kunnen reageren op incidenten en storingen om de bedrijfsprocessen en vereiste IT-services te kunnen blijven gebruiken en de beschikbaarheid van informatie op een voor de onderneming aanvaardbaar niveau te houden.

Doel: Doorgaan met kritieke bedrijfsactiviteiten en de beschikbaarheid van informatie op een voor de onderneming acceptabel niveau houden in geval van een aanzienlijke verstoring.

DSS04.01: Definieer het bedrijfscontinuïteitsbeleid, de doelstellingen en de reikwijdte.

DSS04.02: Een continuïteitsstrategie handhaven.

DSS04.03: Ontwikkel en implementeer een bedrijfscontinuïteitsreactie.

DSS04.04: Oefen, test en bekijk het bedrijfscontinuïteitsplan.

DSS04.05: Het continuïteitsplan evalueren, onderhouden en verbeteren.

DSS04.06: Training voor continuïteitsplannen uitvoeren.

DSS04.07: Back-upregelingen beheren.

DSS04.08: Beoordeling na hervatting uitvoeren.

5. DSS05: Manage security services.

Beschrijving: Bescherm bedrijfsinformatie om het niveau van informatiebeveiligingsrisico's te behouden dat aanvaardbaar is voor de onderneming in overeenstemming met het beveiligingsbeleid. Opzetten en onderhouden van informatiebeveiligingsrollen en toegangsrechten en uitvoeren van beveiligingsmonitoring.

Doel: Minimaliseer de bedrijfsimpact van kwetsbaarheden en incidenten met betrekking tot operationele informatiebeveiliging.

DSS05.01: Bescherm tegen malware.

DSS05.02: Netwerk- en verbindingsbeveiliging beheren.

DSS05.03: Eindpuntbeveiliging beheren.

DSS05.04: Beheer gebruikersidentiteit en logische toegang.

DSS05.05: Fysieke toegang tot IT-activa beheren.

DSS05.06: Gevoelige documenten en uitvoerapparaten beheren.

DSS05.07: De infrastructuur bewaken voor beveiliging gerelateerde evenementen.

6. DSS06: Manage business process controls.

Beschrijving: Definieer en onderhoud geschikte bedrijfsprocescontroles om ervoor te zorgen dat informatie met betrekking tot en verwerkt door interne of externe bedrijfsprocessen voldoet aan alle relevante informatie beheersvereisten. Identificeer de relevante informatie beheersvereisten en

beheer en voer adequate controles uit om ervoor te zorgen dat informatie en informatieverwerking aan deze vereisten voldoen.

Doel: Handhaven van informatie integriteit en de beveiliging van informatie assets die worden verwerkt in bedrijfsprocessen binnen de onderneming of worden uitbesteed.

DSS06.01: Regelactiviteiten die aanwezig zijn in bedrijfsprocessen afstemmen op bedrijfsdoelstellingen.

DSS06.02: Beheer de verwerking van informatie.

DSS06.03: Beheer rollen, verantwoordelijkheden, toegangsrechten en bevoegdheidsniveaus.

DSS06.04: Fouten en uitzonderingen beheren.

DSS06.05: Zorgen voor traceerbaarheid van informatiegebeurtenissen en verantwoordelijkheden.

DSS06.06: Beveilig de informatiemiddelen.

Monitor, Evaluate and Assess

1. MEA01: Monitor, evaluate and assess performance and conformance.

Beschrijving: Verzamel, valideer en evalueer bedrijfs-, IT- en procesdoelen en statistieken. Houd er rekening mee dat processen presteren tegen overeengekomen prestatienormen en conformiteitsdoelen en statistieken en bieden rapportage die systematisch en tijdig is.

Doel: Zorg voor transparantie van prestaties en conformiteit en het bereiken van doelen.

MEA01.01: Een monitoringbenadering vaststellen.

MEA01.02: Prestatie- en conformiteitsdoelen instellen.

MEA01.03: Gegevens over prestaties en conformiteit verzamelen en verwerken.

MEA01.04: Prestaties analyseren en rapporteren.

MEA01.05: Zorgen voor de implementatie van corrigerende maatregelen.

2. MEA02: Monitor, evaluate and assess the system of internal control.

Beschrijving: Voortdurend toezicht houden op en evalueren van de controleomgeving, inclusief zelfbeoordelingen en onafhankelijke verzekeringsevaluaties. Beheer inschakelen om tekortkomingen en ondoelmatigheden in de besturing te identificeren en verbeteringsacties te initiëren. Plan, organiseer en onderhoud standaarden voor interne controle assessment en verzekeringsactiviteiten.

Doel: Zorg voor transparantie voor de belangrijkste belanghebbenden over de adequaatheid van het systeem van interne controles en dus vertrouwen in de bedrijfsvoering, vertrouwen in het behalen van de ondernemingsdoelstellingen en een goed begrip van residueel risico.

MEA02.01: Monitor interne controles.

MEA02.02: Evaluatie van de effectiviteit van de bedrijfsprocesbesturing.

MEA02.03: Controle gerelateerde zelfevaluaties uitvoeren.

MEA02.04: Controletekortkomingen identificeren en rapporteren.

MEA02.05: Zorg ervoor dat verzekeringsproviders onafhankelijk en gekwalificeerd zijn.

MEA02.06: Plan verzekering initiatieven.

MEA02.07: Scope verzekeringsinitiatieven.

MEA02.08: Verzekeringsinitiatieven uitvoeren.

3. MEA03: Monitor, evaluate and assess compliance with external requirements.

Beschrijving: Evalueer dat IT-processen en IT-ondersteunde bedrijfsprocessen voldoen aan wet- en regelgeving en contractuele vereisten. Verkrijg zekerheid dat de vereisten zijn geïdentificeerd en nageleefd en IT-conformiteit integreren met de algehele naleving van bedrijfsregels.

Doel: Zorg ervoor dat de onderneming voldoet aan alle toepasselijke externe vereisten.

MEA03.01: Identificeer externe compliance-eisen.

MEA03.02: Optimaliseer de reactie op externe vereisten.

MEA03.03: Bevestig externe naleving.

MEA03.04: Zorg voor zekerheid van externe compliance.

Bijlage 8: De schildpaddiagrammen van de processen van VITO

1. Manage service portfolio (secundair)

Doelstellingen: Het opstellen en onderhouden van een accuraat overzicht van de diensten die de informatica afdeling van VITO uitvoert en ervoor zorgen dat de geleverde ICT diensten overeenkomen met de behoeften van de business.

Start/trigger: Periodiek, regelmatige update.

Input:

- Overzicht van het service portfolio en de diensten die ze aanbieden.
- Info over de bedrijfsbehoeften en strategie via managementmeetings en dagelijkse bedrijfscontacten.

Proces:

- Regelmatige beoordeling van het portfolio overzicht.
- Toevoegen, veranderen of verwijderen van diensten zodat het portfolio up-to-date blijft met de huidige geleverde diensten.
- Het aanpassen van informatie in verband met de diensten in de relevante bestanden of bedrijfsapplicaties.

Output:

- Een portfolio van diensten die de informatica afdeling van VITO levert.
- Project overzichten in Maconomy[3].
- Een slide met het service portfolio in de introductie presentatie van de informatica afdeling.

Eindtoestand: Wanneer de lijst van services overeenkomt met de huidig geleverde diensten.

Regels/kader: De lijst moet overal accuraat gebruikt worden.

Plaats: De informatica afdeling

Uitvoerders: Het management van de informatica afdeling.

Middelen: Master file in sharepoint[4] en data voorzien door Maconomy (ERP systeem).

KPI: Het portfolio bevat een compleet en accuraat overzicht van de diensten die de informatica afdeling van VITO levert en dient als basis voor andere processen.

Meting KPI: Het service portfolio komt overeen met de gerelateerde bestanden en informatie in de bedrijfsapplicaties zoals Maconomy.

Risico:

3. Het service portfolio komt niet overeen met de behoeften en doelstellingen van het bedrijf. De beschrijvingen van de activiteiten in het portfolio zijn niet duidelijk voor gebruikers of stakeholders.

[3] Maconomy is het ERP systeem dat VITO gebruikt.
[4] Sharepoint is een online platform dat informatie-uitwisseling binnen een organisatie toestaat.

4. Het service portfolio komt niet overeen met de activiteiten die de informatica afdeling uitvoert.

Verhelpen risico:

3. Met de belangrijkste bedrijfsstakeholders de informatica diensten regelmatig overlopen zodat ze overeenkomen met hun behoeften.
4. Het regelmatig nagaan of de activiteiten in het service portfolio nog overeenkomen met de werkelijk uitgevoerde activiteiten.

2. Manage budget and costs (secundair)

Doelstellingen: Het opstellen en managen van een jaarlijks budget voor de diensten en projecten van de informatica afdeling samen met het managen en accuraat opvolgen van kosten.

Start/trigger:

- Een aanvraag voor het opstellen van het jaarlijkse budget document in Q3.
- Permanent overzicht van de kosten voorzien.

Input:

- Het jaarlijkse budget document met een bottom-up overzicht van alle uitgaven met betrekking tot operationele kosten en investeringen.
- Documenten en informatie van het finance departement in verband met te ontvangen facturen, over te dragen kosten, afschrijvingen, …
- Data uit Maconomy en de gerelateerde Tableau[5] dashboards.

Proces:

- Het opstellen van het budget in Q3 voor het komende jaar gebaseerd op gekende informatie, plannen en voorspellingen over de toekomst. Dit alles in overeenkomst met de regels en timings die opgelegd worden door het finance departement.
- Het goedgekeurde budget wordt in Maconomy ingegeven met een budget voor operationele kosten en investeringen per informatica dienst.
- Er dient permanent een oog gehouden te worden op de budgetten en werkelijke uitgaven op basis van aangemaakte aankoopfacturen en gegenereerde kosten.
- Een bijdrage leveren in het financieel management en de rapportage van instructies (te ontvangen facturen, prognoses, …)

Output:

- Het budget bestand voor de informatica afdeling met dagelijks overzicht en opvolging van de financiën van de informatica afdeling.

[5] Tableau is een data visualisatie tool.

- Actuele financiële informatie die beschikbaar is in de VITO business applications (Maconomy, Tableau)

Eindtoestand: Een document dat het budget voor de informatica afdeling voor het komende jaar beschrijft.

Regels/kader: Het budget moet overeenkomen met de werkelijke uitgaven.

Plaats: Informatica en finance afdeling.

Uitvoerders: Het management van de informatica afdeling.

Middelen: Budget document, Finance documenten, Maconomy data en Tableau data

KPI:

1. Het budget document moet een accuraat overzicht geven van het informatica budget in vergelijking met werkelijke uitgaven.
2. De financiële resultaten op het einde van het jaar moeten overeenkomen met hetgeen wat in het budget document werd opgesteld.

Meting KPI:

1. Registratie en opvolging van het budget document en de financiële rapporteringen en dashboards.
2. De afwijking van het budget mag hoogstens 5% bedragen.

Risico:

1. De info in het budget document komt niet overeen met de financiële informatie in Maconomy.
2. De werkelijke uitgaven verschillen aanzienlijk met het budget.
3. Onvoorziene of uitzonderlijk hoge uitgaven in verband met bedrijf of ICT projecten.

Verhelpen risico:

1. Het doorvoeren van een regelmatige check van de data en verificatie met de finance afdeling.
2. Het regelmatig nakijken van het budget en aanpassingen doorvoeren indien nodig.
3. Discussie met het management en indien het mogelijk, vereist of aanvaardbaar is, het budget aanpassen.

3. Manage Human Resources (secundair)

Doelstellingen: Het begeleiden, coachen en opvolgen van alle ICT teamleden in de uitvoering van hun job zodat een optimale bijdrage aan de ICT doelstellingen, het leveren van diensten en projectuitvoering mogelijk is.

Start/trigger: Jaarlijkse uitvoering van de ontwikkelings -en prestatiecyclus.

Input:

- Tijdsregistratie in Maconomy wanneer er aan bepaalde zaken gewerkt wordt.
- Informatie van de HR afdeling inzake de ontwikkelings -en prestatiecyclus.
- Informatie van de ICT teamleden via verschillende kanalen, zowel formeel als informeel.
- Het VTE budget per team/dienst.

Proces:

- Het uitvoeren van de jaarlijkse ontwikkelings -en prestatiecyclus volgens de HR instructies en processen.
- Een regelmatig overzicht van de VTE capaciteit in vergelijking met de behoeften aan personeel van de ICT diensten en projecten.

Output:

- Team en persoonlijk gerichte doelstellingen voor prestatie, functionering en persoonlijk gerichte ontwikkelingen.
- Plannen en voorstellen voor persoonlijke ontwikkeling en training.
- Jaarlijkse prestatiebeoordelingen.
- Een VTE plan en budget in Maconomy.

Eindtoestand: Einde van de ontwikkelings -en prestatiecyclus.

Regels/kader: De ontwikkelings -en prestatiecyclus moet op tijd uitgevoerd worden en de prestaties moeten in lijn zijn met de ICT goals en doelstellingen.

Plaats: Informatica en HR afdeling.

Uitvoerders: Het management van de informatica afdeling.

Middelen: Maconomy, HR input, ICT werknemer input, trainings -en ontwikkelingsmogelijkheden, eventueel actie plan als de prestaties niet ideaal zijn.

KPI:

1. De ontwikkelings -en prestatiecyclus wordt uitgevoerd volgens het jaarlijkse tijdsrooster.
2. Team en individuele prestaties voldoen aan de ICT goals en doelstellingen.
3. De tijd die gespendeerd wordt door teamleden komt overeen met het voorziene VTE budget.

Meting KPI:

1. De timings worden behaald.
2. Een correcte uitvoering van de ontwikkelings -en prestatiecyclus geeft een inzicht in de prestaties van individuen en teams.

3. De geregistreerde tijden worden vergeleken met het VTE budget met behulp van Maconomy.

Risico:

1. De ontwikkelings -en prestatiecyclus wordt niet op tijd en/of incorrect uitgevoerd.
2. De ICT doelstellingen zijn onduidelijk of worden niet tijdig gecommuniceerd. Deze zijn namelijk vereist voor het definiëren van de individuele en team doelstellingen.
3. VTE capaciteit komt niet overeen met de behoeften van de informatica afdeling.

Verhelpen risico:

1. Evaluatie door het management en het plannen van correcte acties.
2. Het management dient duidelijke richtlijnen te geven.
3. Het herzien van prioriteiten en planningen en het evalueren van de stijging of daling van het interne of externe personeel.

4. Manage Business Relationship (primair)

Doelstellingen: Het verzekeren dat de geleverde informatica diensten overeenkomen met de behoeften en verwachtingen van de business.

Start/trigger: Maandelijkse vergadering en informele conversaties.

Input: Formele of informele informatie en feedback geleverd door alle stakeholders van de informatica dienst.

Proces:

- Regelmatige en periodieke management vergaderingen om de verwachtingen en het leveren van informatica diensten en projecten te bespreken. Dit door middel van een maandelijkse ICT management vergadering met de relevante personen.
- Ad hoc en informele conversaties en discussies met alle stakeholders.

Output:

- Input voor het herzien en wijzigen van het service portfolio van het informatica departement.
- Input voor nieuwe project initiatieven.

Eindtoestand: Een conclusie voor het al dan niet wijzigen van diensten of projecten.

Regels/kader: Informatica stakeholders moeten tevreden zijn met de geleverde diensten.

Plaats: Communicatielijnen tussen het informatica departement en zijn stakeholders.

Uitvoerders: Het management van de informatica afdeling.

Middelen: Meetings, conversaties, discussies, bevragingen.

KPI: De stakeholders zijn tevreden met de geleverde diensten en projecten.

Meting KPI: Een presentatie en discussie van de jaarlijkse ICT doelstellingen op ICT management meetings.

Risico:

1. De diensten en projecten van de informatica afdeling komen niet overeen met de bedrijfsdoelstellingen en verwachtingen van VITO.
2. VITO maakt gebruik van externe ICT oplossingen en diensten die in strijd zijn met de interne ICT omgeving.

Verhelpen risico:

1. Een open en constructieve communicatielijn behouden met de business kant.
2. Een open en constructieve communicatielijn behouden met de business kant.

5. Mannage Supplier Relationship (secundair)

Doelstellingen: Er voor zorgen dat de ICT dienstverleners en leveranciers de vereiste diensten en oplossingen bieden, in overeenstemming met de behoeften en verwachtingen van VITO en tegen een correcte prijs.

Start/trigger:

- Wanneer een nieuwe leverancier wordt aangeworven.
- Periodiek overleg

Input:

- Offertes, contracten en raamovereenkomsten.
- Aankoop informatie.
- Specificaties over de benodigde of gewenste producten en diensten.

Proces:

- Aankoopovereenkomsten worden afgesloten met de leveranciers gebaseerd op regels en instructies die door het aankoopdepartement worden opgelegd.
- Het bij regelmaat houden van accountmanagement vergaderingen met de hoofdleveranciers.
- Het overzien van aankooporders, leveringen en facturen.
- Het bij regelmaat controleren van de markt voor potentiele nieuwe leveranciers.

Output:

- De leveranciers waarmee samengewerkt wordt, leveren hun diensten en oplossingen aan VITO.
- (Raam)Overeenkomsten met leveranciers voor bepaalde periodes.
- Balance score cards voor hoofdleveranciers.

Eindtoestand: Einde leveranciersovereenkomst

Regels/kader:

- Regels opgelegd door het aankoop departement.
- VITO's interne regulering
- Leveranciers moeten aan de vooropgestelde eisen voldoen.

Plaats: Informatica en aankoop departement.

Uitvoerders: Het management van de informatica afdeling.

Middelen: Leverancier documenten, geleverde diensten, balance scorecards.

KPI:

1. De prestaties van de leveranciers moeten voldoen aan de eisen van VITO.
2. Alle overeenkomsten met leveranciers komen overeen met de interne regels van VITO.

Meting KPI:

1. Het opstellen van balance scorecards die besproken worden op de accountmanagement vergaderingen met de hoofdleveranciers.
2. Checks uitgevoerd door het inkoop en finance departement als onderdeel van het aankoopproces.

Risico:

1. De interne regels van VITO zijn niet duidelijk of onjuist.
2. De geleverde diensten of kosten van leveranciers komen niet overeen met de overeenkomst of verwachtingen.

Verhelpen risico:

1. Het aankoop departement is betrokken in het afsluiten van contracten met leveranciers met een specifieke focus op de regels en condities.
2. Regelmatige of ad hoc vergaderingen of communicatie met dienstverleners of leveranciers met een beëindiging van de overeenkomst als de verwachtingen niet ingelost kunnen worden.

6. Manage ICT security (primair)

Doelstellingen: ICT beveiligingsacties en maatregelen worden geëvalueerd, ingezet en beheerd om risico's tegen te gaan betreffende informatie en data beschikbaarheid, vertrouwbaarheid en integriteit.

Start/trigger:

- Wanneer er bedreigingen geïdentificeerd zijn.
- Wanneer updates beschikbaar zijn.

Input:

- ICT beveiligingsincidenten
- Interne en externe informatie over mogelijke ICT bedreigingen en risico's
- Bevindingen en aanbevelingen die voortkomen uit interne en externe ICT audits.

Proces:

- Evalueren van de gebeurtenissen en het overzien van de resultaten die voortkomen uit ICT beveiligingsoplossingen (Firewall, anti-virus).
- Het doorvoeren van regelmatige updates voor ICT beveiligingsoplossingen.
- Het overleggen en evalueren van ICT beveiligingsrisico's en acties in ICT beveiliging vergaderingen.
- Security by design / default: er voor zorgen dat beveiligingsmaatregelen reeds deel uitmaken van de dagelijkse activiteiten.
- Een jaarlijkse ICT beveiligingsaudit (intern of extern) doorvoeren.

Output:

- Evalueren en uitvoeren van corrigerende maatregelen gebaseerd op beveiligingsincidenten, inbreuken of nieuwe risico's.
- Een ICT beveiliging actieplan

Eindtoestand: Wanneer de risico's verholpen kunnen worden.

Regels/kader:

- Het aantal incidenten moet zo laag mogelijk blijven.
- Software moet up-to-date blijven.
- Acties moeten zo snel mogelijk ondernomen worden.

Plaats: Informatica departement

Uitvoerders: Het SNB team

Middelen: Informatie uit historische gebeurtenissen, ICT beveiligingsplan, ICT beleid en procedures

KPI:

1. Het aantal beveiligingsinbreuken en incidenten is zo laag mogelijk.
2. Het ICT beveiligingsplan is up-to-date.
3. De resultaten van de jaarlijkse ICT audit moeten voldoen aan de vereisten.

Meting KPI:

1. Het aantal gerapporteerde beveiligingsincidenten.
2. Is er een meer recentere versie van het beveiligingsplan beschikbaar?
3. Het rapport dat voortkomt uit de ICT audit.

Risico:

1. De geïmplementeerde maatregelen zijn niet adequaat of onvoldoende om ICT beveiligingsrisico's te verhelpen.
2. De geïmplementeerde maatregelen zijn tegenstrijdig met de externe regels of regelgevingen.
3. Vanwege de gefragmenteerde verantwoordelijkheid van VITO's ICT activiteiten, diensten en oplossingen, kan er geen algemene ICT beveiligingsbenadering geïmplementeerd worden.

Verhelpen Risico:

1. Het regelmatig doorvoeren van interne en externe beoordelingen van de ICT risico's en de doorgevoerde maatregelen.
2. Een actieplan moet worden opgesteld om de nakoming van de respectievelijke regels te verzekeren.
3. Het verspreiden van bewustzijn, samenwerking en overeenstemmingen doorheen VITO.

7. Manage Programmes & Projects (primair)

Doelstellingen: De informatica en ICT programma's en projecten zijn afgestemd op de ICT en bedrijfsbehoeften en doelstellingen van VITO. Daarnaast worden deze uitgevoerd op een gecontroleerde, efficiënte en effectieve manier.

Start/trigger: Jaarlijkse uitvoering.

Input:

- VITO bedrijfsdoelstellingen
- Informatie dat voortkomt uit direct contact met alle niveaus binnen VITO.
- Informatie voor de informatica afdeling uit interne en externe bronnen zoals discussies, studies en documentatie.

Proces:

- Er wordt jaarlijks een informatica en ICT plan opgesteld met daarin de hoofddoelen, programma's en projecten.
- Het jaarplan wordt uitgebreid met details en projecten op team niveau dat verzameld wordt in een projectoverzicht.

- Dit projectoverzicht dient als basis voor het opvolgen van projecten op high-level.
- Een standaard projectmanagement methodologie wordt toegepast op de projecten met een onderscheid in projectgrootte (klein, groot of zeer groot).

Output:

- Een informatica en ICT jaarplan met de voornaamste programma's en projecten.
- Een ICT projectoverzicht opgedeeld en beheerd door elk informatica team.
- ICT project documentatie in overeenstemming met de standaard projectmanagement methodologie, afhankelijk van de grootte van het project.
- Tijdsregistratie van de voornaamste projecten in Maconomy.

Eindtoestand: Wanneer het ICT plan is opgesteld.

Regels/kader: De VITO business goals.

Plaats: Het informatica departement met input van alle andere departementen.

Uitvoerders: Het management van de informatica afdeling.

Middelen: VITO bedrijfsdoelstellingen, info van andere departementen, interne en externe bronnen en het project overzicht.

KPI:

1. Het informatica en ICT jaarplan is in overeenkomst met de ICT en bedrijfsdoelstellingen van VITO.
2. Het projectoverzicht is correct en up-to-date.
3. ICT projecten worden uitgevoerd in overeenstemming met de projectmanagement methodologie.

Meting KPI:

1. Het ICT jaarplan is beschikbaar en up-to-date.
2. Het projectoverzicht komt overeen met de projecten die het komende jaar uitgevoerd zullen worden.
3. Het uitvoeren van regelmatige kwaliteitsbeoordelingen van de toegepaste project management methodologieën.

Risico:

1. De informatica en ICT projecten zijn tegenstrijdig met de bedrijfsdoelstellingen.
2. Het projectoverzicht geeft niet de werkelijke project lading voor het komende jaar weer.
3. Er wordt geen adequate projectmanagement methodologie toegepast.

4. Geen goed management van de vraag resulteert in een ongecontroleerde toestroom van nieuwe projectinitiatieven.
5. Veel onvoorzien werk heeft een hoge impact op de projectplanning en uitvoering.

Verhelpen Risico:

1. Het management moet acties en herzieningen doorvoeren om de plannen in overeenstemming te brengen met de bedrijfsdoelstellingen van VITO.
2. Er dient een correct, compleet en actueel projectoverzicht opgesteld te worden.
3. Projectmanagement methodologieën en de respectievelijke applicaties dienen herzien en verbeterd te worden.
4. Het bediscussiëren en het overeenkomen over het stellen van prioriteiten op managementniveau.
5. Het bediscussiëren en het overeenkomen over het stellen van prioriteiten op managementniveau.

8. Manage Availability (primair)

Doelstellingen: Het evalueren, implementeren, overzien en het managen van de beschikbaarheid van software toepassingen, data en ICT infrastructuur componenten, in overeenstemming met interne en externe VITO bedrijf en ICT vereisten en behoeften.

Start/trigger:

- Een behoefte aan beschikbaarheidsvereisten.
- Het continu behouden van het overzicht.

Input:

- Formele of informele bedrijf en ICT behoeften in verband met de vereisten van beschikbare middelen.
- Een overzicht van bedrijfskritieke software applicaties en infrastructuur componenten.
- Een overzicht en informatie van gebeurtenissen met betrekking tot de beschikbaarheid van systemen en applicaties.

Proces:

- Bedrijf en ICT behoeften worden vertaald in technische oplossingen en operationele procedures, inclusief beschikbare back-ups en archivering.
- Meerdere real-time oplossingen met betrekking tot monitoring worden geïmplementeerd. In geval van de beschikbaarheid worden inbreuken, waarschuwingen en gebeurtenissen gegenereerd voor de opvolging, beoordeling en uitvoering van de nodige corrigerende maatregelen.

- Dagelijkse controles worden uitgevoerd en de resultaten worden geregistreerd in de dagelijkse checklist van het SNB team binnen het informatica departement.
- In de wekelijkse team meetings worden beschikbaarheidsproblemen besproken wat vervolgens kan leiden tot eenmalige of permanente acties.

Output:

- Sites en dashboards voor het monitoren van de beschikbaarheid.
- SNB dagelijkse checklist.

Eindtoestand: Wanneer de behoeften ingevuld zijn.

Regels/kader:

- VITO bedrijf en ICT behoeften en vereisten.
- De SNB checklist

Plaats: Het informatica departement

Uitvoerders: Het SNB team

Middelen: ICT vereisten, het kritisch software overzicht, SNB checklist, sites, impact analyse, data back-ups.

KPI: Alle waarden in de operationele SNB checklist hebben status 'OK'.

Meting KPI: Het dagelijks overzicht bewaren van de operationele SNB checklist.

Risico:

1. Gefragmenteerde ICT oplossingen leiden tot een onvolledig overzicht en management van beschikbaarheid van de systemen.
2. De beschikbaarheidseisen zijn onduidelijk.
3. De checklist is onduidelijk of onvolledig.

Verhelpen Risico

1. Het streven naar de beste integratie van systemen en oplossingen met standaardoplossingen voor monitoring en beheer.
2. Het regelmatig nagaan van de (kritieke) bedrijfsapplicaties met een focus op de availability behoeften.
3. Het regelmatig nakijken van de checklist.

9. Manage Capacity (primair)

Doelstellingen: Het evalueren, implementeren, monitoren en managen van de capaciteit van de technische ICT bronnen (CPU, opslag en geheugen) die vereist zijn voor het juist functioneren van de ICT oplossingen en de groeiende behoeften aan deze bronnen in de loop van de tijd.

Start/trigger:

- Wanneer vereisten voor capaciteit veranderen.
- Het continu bewaren van het overzicht.

Input:

- Algemene bedrijf en ICT vereisten in verband met de benodigde capaciteit.
- Het meedelen van systeem vereisten door externe leveranciers zodat hun oplossingen op een juiste manier geïmplementeerd kunnen worden in de ICT omgeving.
- Data en statistieken over het gebruik van bronnen in het verleden.

Proces:

- De installatie van oplossingen in overeenstemming met de beschikbare systeem vereisten.
- Het evalueren van de huidige en toekomstige bedrijf en ICT behoeften voor vervanging, verbetering en aanpassen van de huidige infrastructuur.
- Het permanent overzicht bewaren van de meeste bronnen die worden verbruikt.
- Ingrijpen indien grenswaarden overschreden worden of prestaties onder een acceptabel niveau belanden.

Output:

- Een bestand met historische data en de evolutie van het verbruik van capaciteitsbronnen.
- Meerdere online verbruiksoverzichten.
- Een actieplan voor het vervangen of aanpassen van de huidige infrastructuur.

Eindtoestand: Als aan de vereisten voor capaciteit voldaan is.

Regels/kader:

- Bedrijf en ICT vereisten
- Systeemvereisten van externe leveranciers.

Plaats: Het informatica departement.

Uitvoerders: Het SNB team

Middelen: De huidige capaciteit, bedrijf en ICT vereisten, systeem vereisten, data uit het verleden, actieplan voor vervanging.

KPI:

1. Al het verbruik van bronnen blijft onder de voorgeschreven grenswaarden.
2. Nieuwe oplossingen worden geïnstalleerd in overeenstemming met de technische specificaties die door de leveranciers worden voorgeschreven.

Meting KPI:

1. Maandelijkse opvolging en rapportage van de grootste toewijzingen en verbruik van bronnen.
2. Beoordeling van de installaties tegenover de systeem vereisten.

Risico

1. Onjuiste of onduidelijke capaciteit specificaties.
2. De beschikbare capaciteit is onvoldoende voor een onverwachte of uitzonderlijke vraag naar capaciteit.
3. Capaciteit is moeilijk te beheren omwille van de gefragmenteerde verantwoordelijkheid van de capaciteitsbronnen.

Verhelpen risico

1. Het nakijken van de capaciteitsvereisten met de belangrijkste stakeholders.
2. Indien dit risico zich voordoet, moet het geaccepteerd worden en onmiddellijk gehandeld worden.
3. Goede communicatie en samenwerking met de belangrijkste stakeholders.

10. Manage Software and Hardware Assets (primair)

Doelstellingen: Een correct, volledig en actueel overzicht hebben van al de software en hardware die VITO in bezit heeft. Dit voor optimaal levenscyclusmanagement en om aan contractuele verplichtingen te voldoen.

Start/trigger:

- Een continu overzicht van de hardware en software.
- Wijzigingen in hardware of software.

Input:

- Contractuele informatie over aangekochte hardware en software.
- Voorraad informatie ontvangen van leveranciers.
- Automatisch gegenereerde informatie van activa over geïnstalleerde software en hardware via voorraad en activa managementsystemen.
- Uitoefenen van een jaarlijkse inventaris opname ter plaatse.

Proces:

- Al de aangekochte ICT uitrusting wordt geregistreerd in een centrale Configuration Management Database (CMDB).
- De installatie en gebruik van software wordt tijdelijk gemonitord en beoordeeld. Dit vormt de basis voor licentiemanagement om aan contractuele vereisten te voldoen.
- De informatie uit de CMDB wordt gebruikt om hardware te installeren, te verplaatsen, toe te voegen en los te koppelen (IMACD) volgens de levenscyclus afspraken.
- Een permanente controle over de activa als onderdeel van dagelijkse activiteiten.

Output:

- Real-time informatie over activa voor dagelijks en operationeel gebruik.
- Rapporten over software worden gebruikt bij het evalueren van licenties en compliance.
- Informatie over activa omtrent vervanging, vernieuwing en investeringsprojecten
- Informatie over activa in verhouding met het financieel managen van de ICT uitrusting.

Eindtoestand: Contractuele verplichtingen zijn voldaan.

Regels/kader: Contractuele en levenscyclus afspraken.

Plaats: Het informatica departement

Uitvoerders: Het GON team

Middelen: Contracten, levenscycli en de CMDB.

KPI:

1. Geïnstalleerde hardware en software voldoet aan contractuele verplichtingen.
2. De voorraad van hardware en software is in overeenkomst met de werkelijk geïnstalleerde software.

Meting KPI:

1. Het regelmatig vergelijken van de geïnstalleerde hardware en software in vergelijking met wat in contracten opgelegd wordt.
2. Een jaarlijks fysieke inventarisatie van de geïnstalleerde en beschikbare werkplekken bij VITO.

Risico

1. De werkelijk gebruikte software en hardware komt niet overeen met wat in contracten wordt voorgeschreven.
2. De voorraad informatie komt niet overeen met de werkelijk geïnstalleerde activa.

3. ICT hardware en software wordt aangekocht zonder de betrokkenheid van het informatica departement met als resultaat dat deze activa niet deel uitmaken van dit proces.
4. Alle processtappen zijn moeilijk toe te passen omdat er een zeer breed gamma aan beschikbare en geïnstalleerde software producten aanwezig is.

Verhelpen risico

1. Het de-installeren van hardware en software of het aankopen van extra licenties zodat aan de contractuele voorwaarden voldaan wordt.
2. Het regelmatig checken van de voorraadinformatie en deze informatie indien nodig manueel of automatisch aanpassen.
3. Het manueel of automatisch scannen van onbekende hardware of software.
4. De focus leggen op de 10 meest belangrijke software.

11. Manage Incidents (primair)

Doelstellingen: Een effectieve en efficiënte omgang met ICT incidenten (ongeplande onderbreking of vermindering in de kwaliteit van de IT diensten) met als doel het zo snel en correct mogelijk herstellen van de ICT dienst.

Start/trigger: Wanneer beklag over een incident zich voordoet.

Input:

- Incident tickets van de VITO eindgebruikers worden ontvangen via een Assist self-service portaal of een telefoongesprek, e-mail of verbaal.
- Gebeurtenissen en meldingen van ICT systemen.
- Verschillende inputs van ICT medewerkers.

Proces:

- Het interpreteren van de *Assist*[6] *incident management process flow.*
- Dagelijks bekijken en opvolgen van de status en voortgang van incidenten door de incident manager.
- Wekelijkse discussies van incidenten in GON team meetings.

Output: Een gedetailleerd overzicht van ICT incidenten en gerelateerde informatie.

Eindtoestand: Wanneer informatie over het incident beschikbaar, verzameld en opgelost is

Regels/kader: De Assist incident management process flow.

Plaats: Het informatica departement.

Uitvoerders: Het GON team.

[6] Assist is een manier waarmee werknemers van VITO hun beklag kunnen doen.

Middelen: incident tickets of meldingen, Assist incident management process flow.

KPI:

1. Incidenten worden behandelt en opgelost volgens de verwachtingen van de gebruiker.
2. Alle incidenten worden volledig opgelost of tot aan een aanvaardbare toestand.

Meting KPI:

1. Er komen geen regelmatige klachten over het behandelen van ICT incidenten. Er worden daarnaast periodieke controles uitgevoerd om de tevredenheid van de eindgebruiker of het management over de ICT dienst in kaart te brengen.
2. Er vindt een wekelijkse meeting binnen het GON team plaats om de openstaande incidenten te bespreken.

Risico

1. De verwachtingen van de eindgebruiker omtrent incident management komen niet overeen met de ICT ondersteuningsdienst die geleverd wordt.
2. Het aantal en de verscheidenheid van de incidenten is te groot om een efficiënte oplossing te implementeren door het beschikbare ICT personeel.
3. Incidenten die door de eindgebruikers gemeld worden volgen de processtappen niet.

Verhelpen risico:

1. Een open en constructief gesprek met de gebruiker en het management over de ICT ondersteuningsdienst.
2. Een periodieke herziening door het management dat tot corrigerende acties leidt.
3. Indien de uitzondering de regel wordt, zullen specifieke acties ondernomen moeten worden om informatie over het proces beschikbaar te stellen en een bewustzijn te creëren.

12. Manage Request Fulfilment (primair)

Doelstellingen: Een effectieve en efficiënte behandeling van ICT requests die resulteren in een gepaste en acceptabele situatie of oplossing voor de eindgebruiker.

Start/trigger: Bij binnenkomst van een request.

Input:

- Request tickets van de eindgebruiker die ontvangen worden via het Assist self-service portaal of een telefoongesprek, e-mail of verbaal.
- Verschillende inputs van ICT medewerkers.

Proces:

- Het interpreteren van de *Assist incident management process flow.*
- Een dagelijkse beoordeling en opvolging van de huidige toestand en voortgang van de requests door de request manager.
- Een wekelijkse discussie van de requests in d e INF team meetings.

Output: Een gedetailleerd overzicht van de ICT requests en gerelateerde informatie.

Eindtoestand: Wanneer informatie over de request beschikbaar, verzameld en opgelost is.

Regels/kader: Assist request fulfilment process flow

Plaats: Het informatica departement.

Uitvoerders: Alle teams van het informatica departement.

Middelen: Request tickets en de Assist request fulfilment process flow.

KPI:

1. Requests worden behandelt en op tijd uitgevoerd volgens de verwachtingen van de gebruiker.
2. Alle incidenten worden volledig uitgevoerd of tot aan een aanvaardbare eindtoestand.

Meting KPI:

1. Er komen geen regelmatige klachten over het behandelen van ICT requests. Er dienen periodieke controles uitgevoerd te worden bij de eingebruiker of management over de uitvoering van de ICT dienst.
2. Wekelijkse opvolging van de requests door de verschillende ICT teams.

Risico:

1. De verwachtingen van de eindgebruiker omtrent request management komen niet overeen met de ICT ondersteuningsdienst die geleverd wordt.
2. Het aantal en de verscheidenheid van de incidenten is te groot om een efficiënte oplossing te implementeren door het beschikbare ICT personeel.
3. Requests die door de eindgebruikers gemeld worden volgen de processtappen niet.

Verhelpen risico:

1. Een open en constructief gesprek met de gebruiker en het management over de ICT ondersteuningsdienst.
2. Een periodieke herziening door het management dat tot corrigerende acties leidt.
3. Indien de uitzondering de regel wordt, zullen specifieke acties ondernomen moeten worden om informatie over het proces beschikbaar te stellen en een bewustzijn te creëren.

13. Manage Identity & Access (primair)

Doelstellingen: Toegang tot data, informatie, systemen en applicaties wordt voorzien op een gecontroleerde, effectieve en veilige manier om er voor te zorgen dat de juiste mensen de juiste toegang hebben op elk moment.

Start/trigger: Wanneer een toegangsaanvraag binnenkomt van een bepaalde gebruiker voor toegang tot bepaalde informatie.

Input:

- De HR master database die ingevuld is door het personeelsadministratie systeem van HR.
- Identiteit en toegangsaanvragen door eindgebruikers.

Proces:

- Automatische toegang tot bronnen wordt beheerd (add, change, delete), gebaseerd op regels.
- Het behandelen van toegangsaanvragen gebaseerd op toestemming van de broneigenaar.
- De broneigenaar beheert de toegangsrechten.
- Ad hoc toegangsrechten worden opgeruimd door de systeem administratoren in bijvoorbeeld Tableau of SQL.

Output:

- Gebruikers en groepslidmaatschappen in Active Directory.
- Gebruikers en rechten gedefinieerd en geconfigureerd in de systemen en applicaties.

Eindtoestand:

- Toegang verleend.
- Toegang geweigerd.

Regels/kader: Toegangsrechten worden toegekend op basis van de toestemming van de broneigenaar.

Plaats: Het informatica departement

Uitvoerders: Het SNB team

Middelen: Toegangsaanvragen, Adexus en Drupal

KPI:

1. Toegang tot gegevens en informatie wordt geregeld in overeenstemming met regels en voorschriften.
2. Toegang tot gegevens en informatie wordt geleverd in overeenstemming met de verwachtingen van het bedrijf en de eindgebruiker.

Meting KPI:

1. Het aantal gegevenslekken moet zo laag mogelijk zijn.

2. Het aantal klachten moet zo laag mogelijk zijn.

Risico:

1. Informatie voor eindgebruikers in de personeelsadministratie database is onjuist of niet op tijd geregistreerd.
2. De behandeling van sommige (eindgebruikers) accounts (bijvoorbeeld beheerders- of serviceaccounts) verloopt niet volgens het standaard Identity & Access Management proces.
3. Het beheer van gebruikers in specifieke applicaties volgen het standaard IAM-proces of standaardmaatregelen niet.

Verhelpen risico:

1. Als de uitzonderingen de regel worden, moeten specifieke correctiemaatregelen worden genomen.
2. Als de uitzonderingen de regel worden, moeten specifieke correctiemaatregelen worden genomen.
3. Promoot en gebruik zoveel mogelijk Active Directory-accounts bij eenmalige aanmelding.

Auteursrechtelijke overeenkomst

Ik/wij verlenen het wereldwijde auteursrecht voor de ingediende eindverhandeling:
Het toepassen van ISO-normen op IT managementsprocessen

Richting: **master in de toegepaste economische wetenschappen: handelsingenieur in de beleidsinformatica**
Jaar: **2018**

in alle mogelijke mediaformaten, - bestaande en in de toekomst te ontwikkelen - , aan de Universiteit Hasselt.

Niet tegenstaand deze toekenning van het auteursrecht aan de Universiteit Hasselt behoud ik als auteur het recht om de eindverhandeling, - in zijn geheel of gedeeltelijk -, vrij te reproduceren, (her)publiceren of distribueren zonder de toelating te moeten verkrijgen van de Universiteit Hasselt.

Ik bevestig dat de eindverhandeling mijn origineel werk is, en dat ik het recht heb om de rechten te verlenen die in deze overeenkomst worden beschreven. Ik verklaar tevens dat de eindverhandeling, naar mijn weten, het auteursrecht van anderen niet overtreedt.

Ik verklaar tevens dat ik voor het materiaal in de eindverhandeling dat beschermd wordt door het auteursrecht, de nodige toelatingen heb verkregen zodat ik deze ook aan de Universiteit Hasselt kan overdragen en dat dit duidelijk in de tekst en inhoud van de eindverhandeling werd genotificeerd.

Universiteit Hasselt zal mij als auteur(s) van de eindverhandeling identificeren en zal geen wijzigingen aanbrengen aan de eindverhandeling, uitgezonderd deze toegelaten door deze overeenkomst.

Voor akkoord,

Medaer, Charley

Datum: **22/08/2018**