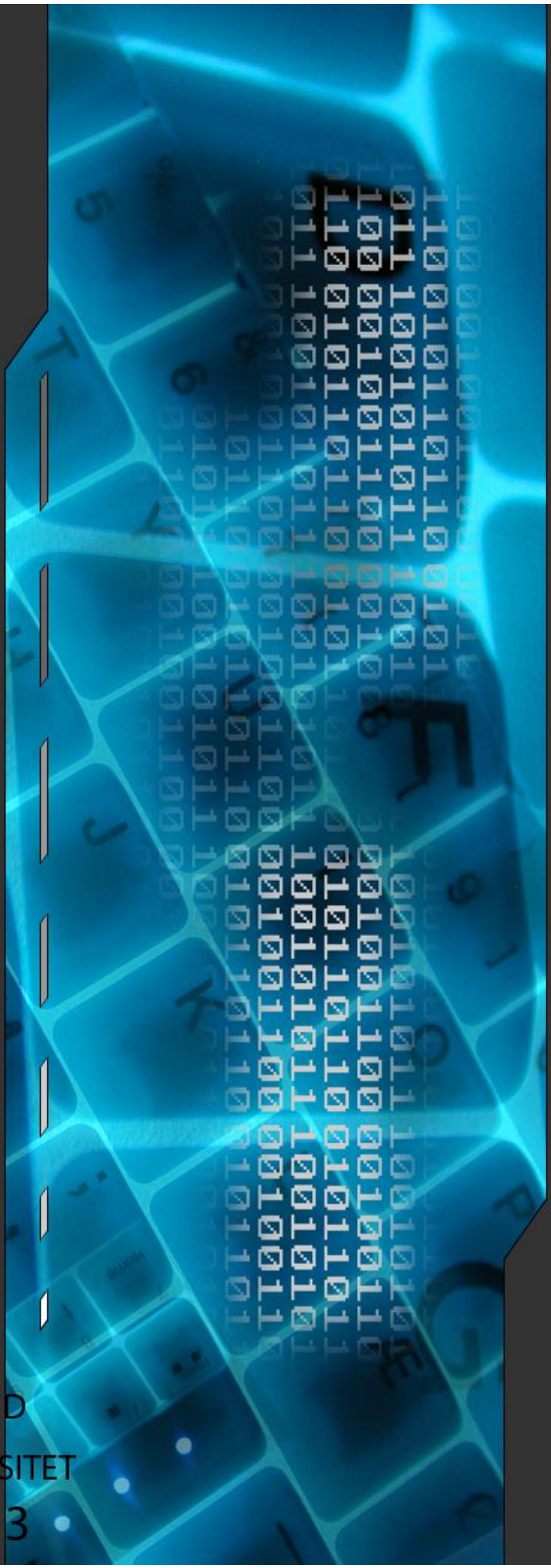
IT Governance



Kandidatafhandling

Udarbejdet af Jakob Bøgh

Cand. Merc. Aud
Aalborg Universitet
28 Februar 2013

Forord

Dette projekt er skrevet i forbindelse med afslutningen af Cand. Merc. Aud og dette projekt er under vejledning af Hans Henrik Aabenhus Berthing. Der udover skal der sendes et stor tak til familie og venner som har været tålemodige og behjælpelige i forbindelse med mit speciale skrivning.

Specialet er skrevet i faget it-ledelse. Specialet omhandler behandling af frameworks og guidelines til it-governance.

En større selvstændig afhandling af relevans for en statsautoriseret revisors virke. Specialet skal dokumentere den studerendes færdigheder i at anvende videnskabelige teorier og metoder under arbejdet med et afgrænset fagligt emne.[1]

Der skal herfra lyde en stor tak til Rambøll for at have sponsoreret bogen It i Praksis 2012 til mig.

Kandidatafhandlingen er udarbejdet af:

Jakob Bøgh

_____

[1] Studievejledning for Cand. Merc. Aud. – Studiet 2011 – side 13

Executive Summary

IT as a resource is often overlooked as a competitive factor which is why it doesn't receive much attention from the management of a company. This is further substantiated by the following passage from the book IT-Revision, 4. edition 2008. *"The common problem in this area is the lack of awareness and interest in the subject of IT from the Governance"*[2].

Information is an important resource in all companies. From the time of its creation to its destruction, the technology plays a vital role. Information technology is becoming more and more advanced and more widely used in companies and other business environments.

In this thesis the following problem will be answered: **"What role does the governance play in the management of IT, what tools are available for this task, how can risk assessment of projects be handled, and, lastly, why does all of the aforementioned hold any relevance?**

Both theory and empirical data will be used in the process of answering these questions.

This thesis consists of five chapters. The first chapter revolves around establishing the motivation for the chosen problem statement through a problem area, and, furthermore, the chapter describes the process of narrowing in on the subject of focus, also explaining the choices made with regards to discarded alternative subjects. Method and project design explains the structure of this thesis so as to give the reader an insight into which position on methodology is chosen. The last section of the chapter seeks to give a critical review of the information sources used in this thesis to establish if, and why, they hold any validity.

Chapter two of this thesis deals with theoretical aspects of the problem and it aims to explain the motivation for choosing the specific frameworks and standards which serve the purpose of providing the management with tools to handle IT and related risk assessment.

- COSO – Enterprise risk management.
- COBIT 5 – Framework for it-governance
- God it skik 2011 – Framework for it-governance
- ISO 38500 - *Corporate governance of Information Technology*

[2] IT-Revision side.21

Chapter three deals with describing the empirical data which has the purpose of establishing why the use of frameworks is an important practice for companies.

It i praksis 2012 *strategi, trends og erfaringer i danske virksomheder*

Global Status Report on the Governance of Enterprise IT (GEIT)

Chapter four will be a short linking together of the empirical data compared to the relevant theory to provide insight into whether there are any specific points that theory can remedy.
The chapter on empirical data shows that the subject of IT is a complex one, and the complexity itself is not expected to lessen in the foreseeable future, which further stresses the relevance of using methods to help structure the use of IT in companies.

Finally, chapter five will seek to reach a conclusion to the original problem statement.

Based on the theory outlined in this thesis, it is crucial that the governance introduces IT as early in the process as possible in their strategic planning so as to realize the high potential of synergy between IT and business instead of focusing solely on the business component. Since decisions are made at the highest level of the organization, it is of great importance that the governance is open to input and suggestions from the IT governance, and the IT governance, in turn, must be able to provide solid documentation that they are able to offer more value for the business as a whole. To achieve this, a certain level of maturity is required of the IT governance, and the CIO is expected to be able to facilitate and control the discussion of value creation through IT and provide the relevant information.

The available tools for managing IT are many and in this thesis only a few of them are addressed, namely two frameworks and one standard. The ultimate purpose of this theory is to introduce a structure in the management of IT in a given organization and also to ensure a solid communication between the IT-governance and governance. Considering the fact that each company is different, these frameworks cannot serve as a standalone solution by themselves and therefore need the support from one or several inputs in the form of standards or guides/instructions to be able to accommodate a given company structure.
Additionally, I have described COSO, which can be applied to the structure of a company in its entirety. It can be utilized to create a basis for solid risk assessment by way of Internal Environment, Monitoring, Information & Communication etc.

It is generally agreed upon that an important element of achieving a vision for a company is the usage of IT, but also that the primary function of IT is to support the current business strategy and not serve as an innovative part of the business. Also, it should be treated as a tool to minimize overall cost. Therefore, it is important to focus on IT as a competitive parameter to maximize overall competitiveness of a company, and the tools mentioned in this thesis helps this task. Lastly, it is vital that a given company understands how to utilize the information resulting from the introduction of these frameworks into the company environment.

Indhold

Kap 1 - Indledning

1.1 Problemfelt

I dette kapitel vil jeg redegøre for, hvorfor jeg finder it-ledelse relevant som problemstilling. Efter relevansafsnittet bliver der redegjort for mit valg af metode, og hvordan projektet er opbygget. Efter at have læst kapitel 1 og problemformuleringen, bør læseren have en klar opfattelse af, hvad dette projekt gerne vil.

Det har været fremme i medierne at it-ledelse er et overset aspekt i mange danske virksomheder. Blandt andet har Jyllandsposten bragt en artikel omkring emnet i september 2012. Her fremgår det at it-strategien er en stor mangel samt en overset ressource blandt større danske virksomheder. I artiklen siger Flemming Lindløv som tidligere stod i spidsen for Carlsberg og COOP Flemming Lindløv: "*Det er let at komme til at sætte en række dygtige mennesker sammen i en bestyrelse og så tro, at den hellige grav er velforvaret. Det er bare ikke nok at have dygtige mennesker. De skal også besidde den rette sammensætning af kompetencer, så der ikke opstår blinde pletter i forhold til virksomhedens situation og placering på markedet*"[3] og "*Du bliver nødt til at have tillid til dine medarbejdere og lytte til deres ekspertise. Det er jo derfor, de er der. Så når it-direktør kommer med et projekt, om end det koster mange penge, så bliver du nødt til at stole på, at der er fornuft i det.*". Roger Söderberg, vicepresident i Orange Business Solutions, forklarer i samme artikel følgende "*Det afgørende for at kunne lave de optimale it-løsninger er, at mennesker kender din branche. Det kan godt være, den første i køen er verdens bedste it-mand, men at nummer to eller tre faktisk er den bedste for dig, fordi de kender og forstår din business*.".[4]

En analyse foretaget blandt 100 it-chefer og it-direktører i større danske virksomheder viser at det kun er hver anden virksomhed som udnytter de it-strategiske muligheder.[5] Dette er med til at fremhæve at it-strategi er et overset parameter i mange virksomheder.

Information er en vigtig ressource i alle virksomheder, fra det tidspunkt hvor informationen er skabt til det tidspunkt hvor den skal destrueres, har teknologien en væsentlig rolle.

[3] JP karriere 2 september 2012 - side 6-7
[4] JP karriere 2 september 2012 - side 6-7
[5] JP karriere 2 september 2012 - side 6-7

Informationsteknologien bliver mere og mere avanceret og er blevet mere og mere udbredt i virksomheder og forretningsmiljøer.

Dette resulterer i at virksomhederne og virksomhedslederne, mere end nogen sinde før, har et behov for at:

- Opretholde information af høj kvalitet som skal understøtte de forretningsmæssige beslutninger.
- Generere forretningsværdi fra it etablerede investeringer, det vil sige at opnå de strategiske mål og realisere forretningsværdi igennem en effektiv og innovativ brug af it.
- Opnå operationel ekspertise gennem en pålidelig og effektiv anvendelse af it.
- Holde de it relaterede risici på et acceptabelt niveau.
- Overholde den relevante lovgivning.[6]

De virksomheder som har succes i dag er klar over at it har en vigtig rolle på bestyrelses- og ledelsesniveau. Bestyrelsen og ledelsen skal samarbejde for derved at inkludere it, it governance og management strategien. [7]

It som ressource bliver ofte overset som værende en konkurrenceparameter, derfor er det ikke et område som ledelsen har fokus på. Dette underbygges af følgende udsagn fra bogen it-revison, 4. udgave fra 2008. "*Det almindeligste problem på dette område er manglende bevidsthed og interesse for it hos ledelsen*".[8] Ud fra denne oplysning antager jeg at anvendelsen af standarder eller frameworks til styring og kontrol af it ikke er hyppigt anvendt og der ofte vil opstå manglende kommunikation mellem den it ansvarlige og ledelsen, hvilket vil føre til en usammenhængende virksomhed. At it-strategien og forretningsstrategien ikke stemmer overens kan medføre at man ikke udnytter sin it optimalt og de virksomheder/organisationer som gør dette vil have et forspring i forhold til deres konkurrenter.

1.2 Problemformulering:

Ud fra det overståenden afsnit finder jeg det relevant at undersøge følgende:

[6] COBIT 5 – *A Business Framework for the Governance and Management of Enterprise IT* – side 13
[7] COBIT 5 – *A Business Framework for the Governance and Management of Enterprise IT* – side 13
[8] Carsten W, Heilbuth og Carsten Tjagvad (2011); *IT-revision* - side 21

Hvad er ledelsens rolle i håndteringen af it, og hvilke værktøjer kan denne benytte sig af samt hvordan kan man bedst beherske risikoen af projekter og hvorfor er alt dette relevant?

Når der tales om ledelsen i problemformuleringen, hentydes der til den samlede enhed af ledere fra topledelses-niveau, dagligledelse og ledelserne i de forskellige afdelinger. Ved værktøjer menes der de frameworks, standarder, guidelines og principper der findes. Med ordet projekter, menes der de forskellige nye tiltag der tages, inden de indtræder i den normale drift.
Grundet den store mængde af materiale omkring it, eksistere på engelsk, vil der i denne afhandling blive benyttet en række engelske udtryk.

1.3 Afgrænsning

I dette afsnit vil jeg redegøre for nogle af de fravalg jeg har gjort under udarbejdelsen af denne kandidatafhandling, i henhold til den fremsatte problemformulering.

Omkostninger til at implementere sådan et framework, som COBIT 5 eller tilsvarende, kunne godt gå hen at være høje. Jeg har valgt ikke at fokusere på mindre virksomheder, da der er en del omkostninger forbundet med at implementere de givne frameworks. Disse omkostninger betyder at det ikke ville være rentabelt for en mindre virksomhed og ud fra dette har jeg valgt at de virksomheder som er fokus i denne afhandling er nødt til at have en størrelse hvor det i henhold til cost-benefit er forsvarligt at implementere de givne frameworks.

På grund af begrænsningerne for afhandlingens omfang[9], har jeg ikke valgt at tage det "tekniske" lag med, hvor man ellers kunne have aspekter med som statistik på hvor gammelt eller nyt software og hardware der benyttes, hvilket ydermere kunne udvikles til, hvorledes virksomheder bør gribe større forandringsprocesser an, ved hjælp af f.eks. John. P. Kotters 8-trins model.
Ligeledes har jeg fravalgt det aspekt af opgaven der omhandler it-sikkerhed og igen er årsagen hertil at det ville betyde at omfanget af afhandlingen ville være for stort.

[9] Her tænkes på sidetal og den givne tidsramme som afhandlingen har skullet udarbejdes indenfor.

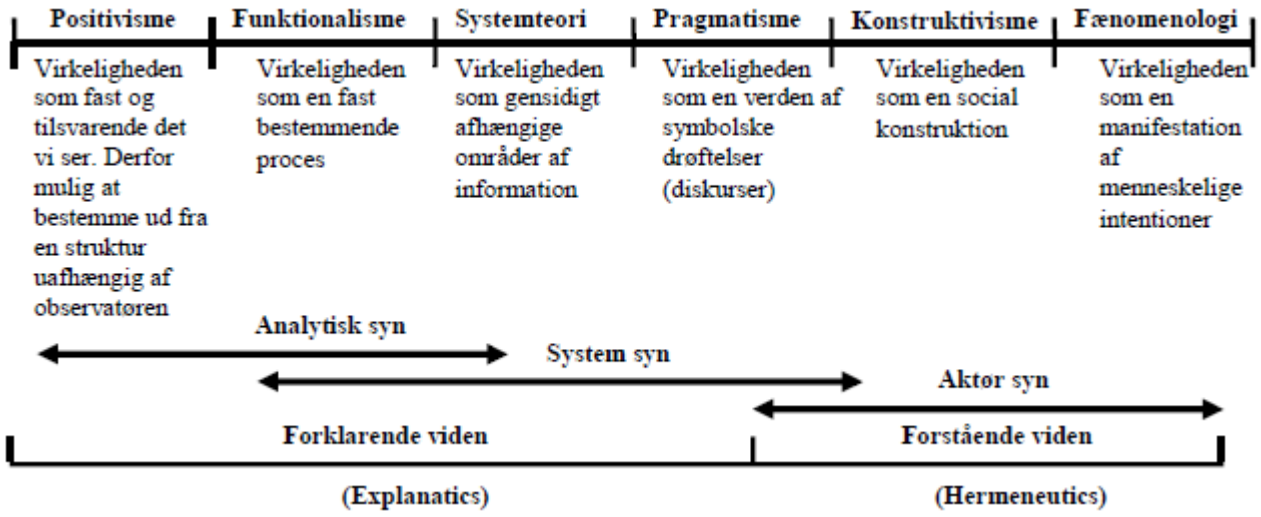
1.4 Metode

Valget af metode påvirker undersøgelsens resultat, både den måde hvorpå data indsamles, hvilken type data, der indsamles, og hvilke teorier, der anvendes til analysen. Derfor skal man være bevidste om, hvordan metoden anvendes. Begrebet metode dækker over, hvordan en problemløsning koordineres og gennemføres. Der er gennem projektets udarbejdelse sket bevidste valg og fravalg af anvendte teknikker og teorier. I de efterfølgende afsnit bliver der redegjort for den metodemæssige tilgang, hvorudfra projektet er blevet udarbejdet, samt det anvendte projektdesign.

1.2.1 De 3 metodetilgange

Herunder vil der blive set på de samfundsvidenskabelige paradigmer, og hvilke metodetilgange de hører under. Arbnor & Bjerke opererer med seks overordnede samfundsvidenskabelige paradigmer; positivisme, funktionalisme, systemteori, pragmatisme, socialkonstruktivisme og fænomenologi. Det fremgår af nedenstående figur, at disse inddeles i følgende tre erhvervsøkonomiske metodesyn: det analytiske, det systemiske og det aktørmæssige metodesyn.

Figur 1 – De seks paradigmer i forhold til metodesyn



Kilde: Bachelor HA – 2008 – "Forandringsledelse – en nødvendighed" side 17

Som det ses af ovenstående figur, er der fællestræk mellem metodetilgangene, og disse kan derfor godt eksistere inden for det samme paradigme. Det analytiske og systemiske syn har fx flere ens træk ved paradigme, men er meget forskellige med hensyn til metode.[10]

I det efterfølgende opstilles der en tabel med generelle oplysninger om de 3 metodetilgange med hensyn til ontologi, epistemologi og videnskabelig idealer. Herunder ambitionsniveau, teknikker, metoder og undersøgelseskriterier. Denne model forklarer kort og præcist, hvad de tremetodetilgange overordnet går ud på og vil ikke blive forklaret nærmere.

[10] *Bachelor HA – 2008 – "Forandringsledelse – en nødvendighed" side 18*

Figur 2 – Tabel over metodetilgangene

De 3 metodetilganges verdensbillede og typer af viden			
	Analytisk	**Systemiske**	**Aktør**
Ontologi/forestilling om verden	Verden er objektiv. Udgøres af uafhængige dele. Helheden er en sum af delene. Kausale relationer mellem delene. Mennesket er enten irrationelt/rationelt: - stimuli reaktion - beslutningsorienteret -instrumentalt	Verden er objektiv/objektiv tilgængelig. Udgøres af et system forbundet af dele og komponenter. Helheden er ikke summen af delene(synergi) Finale relationer mellem dele; målet er objektivt. Mennesket er socialt, et komponent: - tilpasningsevne - socialiseret - system adfærd	Verden er subjektiv, der er mange verdener. Den sociale verden er en social konstruktion lavet af aktørerne via interaktion. Verden består af meningsstrukturer som er socialt konstrueret. Dialektiske relationer mellem delene og helheden. Mennesket er en aktiv skaber af virkelighedn: - skaber/fremkalder - aktør -forsætligt(intentionelt)
Epistemologi/Type viden	Unik og kvantitativ. Genereres af kausale love, mekanik og logiske strukturer. Helheden fås gennem forklaring af delene. Nomotetisk viden: Søger den generelle sandhed, principper og universaliteter.	Unik og kvalitativ. Genereres gennem den unikke systemmodel og dens type af sammenhængskraft. Helheden fås gennem forklaring af delene gennem karakteristika af helheden som de er en del af. Ideografisk viden: Søger det unikke.	Unik og kvalitativ. Genereres omkring sociale konstruktioner, subjektive meningsstrukturer og dialektiske relationer. Helheden fås gennem forståelse af aktørerne og deres begrænsede områder af mening. Ideografisk viden: Søger det unikke.
Videnskabelig idealer og metodologier ved de 3 metodetilgange.			
Ambitionsniveauer	Udforske. Beskrive. Forklare. Forudse. Rådgive/vejlede/guide	Beskrive, forklare systemer. Systemanalyse: - positiv eller negativ synergi Diagnosticering af systemets problem: - stabilisering, socialisering (tilpasning af komponenter og dele.)	Forstå Diagnosticere Frigøre (Emancipation)
Teknikker/værktøjer	Eksperimenter, observationer, interviews, spørgeskemaer, analyse, statistikker, matematik, logik.	Interviews, case studier, historiske studier, system teorier.	Udvikle sproget, dialog, observationer, eksperimenter.
Metode	Proces af forklaring via statistik årsag-effekt, gensidige forhold eller logiske relationer.	Forklarende proces gennem at relatere komponenters relationer til deres ender	Proces af forståelse. Fortsatte skift mellem interaktion og fortolkning.
Undersøgelses kriterier	Validitet, pålidelighed, objektivitet, repræsentativitet.	Validitet, objektivitet. Reproduktions kriterier: - Nyttig, pålidelig, sammenhæng, baggrund	Validitet, gennemskueligt, ærlighed, frigørelse fra fordomme.

Kilde: Bachelor HA – 2008 – "Forandringsledelse – en nødvendighed" side 19

1.2.2 Mit valg af metodetilgang

Det valg jeg har foretaget er at benytte det analytiske syn, der bygger på virkeligheden som den der. Dette betyder at virkeligheden er givet og verden ses objektivt. Derudover bygger det analytiske syn på modeller til at simplificere et givent budskab. Derfor skal jeg se objektiv på virkeligheden og der skal ikke inddrages subjektive vurderinger, da disse kan betragtes som værende ustabile i forbindelse med at bevise sandenheden. [11]

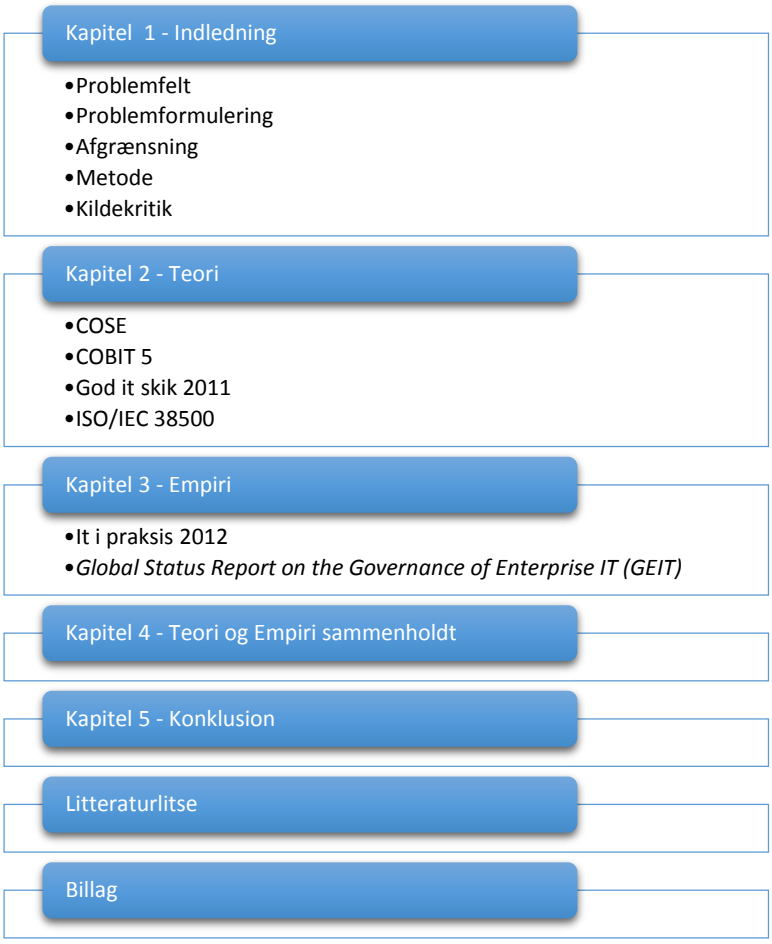
På baggrund af det førnævnte vil der blive benytte et analytisk metodesyn i dette speciale. Det skyldes at jeg benytter standarder og vejledninger som benyttes efter bestemte regler, så disse skal benyttes som retningslinjer, hvorpå der skal indføres data som bliver behandlet. Dette stemmer godt overens med det analytiske metode syn.

1.5 Projektdesign

Problemformulering er opdelt i to områder. Første del er en teori del hvor jeg går ind og forklarer de værktøjer som ledelsen kan anvende. Anden del er hvorfor dette har en relevans, hvilket bliver forklaret igennem min empiri. Det giver følgende projektstruktur:

[11] Arbnor, Ingeman & Bjerke, Björn (1997); *Methodology for Creating Business Knowledge* – side 15

Figur 3 – Projektstruktur.



Kilde: Egen tilvirkning

Afhandlingen består af fem kapitler, hvor det første kapitel har til formål at belyse valget af problemformuleringen igennem et problemfelt, desuden indeholder kapitlet en afgrænsning som beskriver de fravalg jeg har foretaget. Metode og projektdesign er en beskrivelse af hvorledes kandidatafhandlingen er struktureret og for at give læser et indblik i hvilket metodesyn der er anvendt i udarbejdelsen af denne afhandling. Som det sidste punkt i dette kapitel er der et kildekritik afsnit, hvor der tages stilling til de anvendte kilder.

Kapitel to er kandidatafhandlingens teoretiske afsnit, her vil der blive redegjort for og beskrevet de valgte frameworks og standarder, som har til formål at give ledelsen værktøjer til at håndtere it og risici.

Tredje kapitel bestå af den empiri som er fundet for at klargøre hvorfor det er relevant for virksomhederne at benytte sig af frameworks.

Kapitel fire vil være der blive det teorien blive holdt op mod det empiriske data.

Afslutnings vis vil der i kapitel fem være en konklusion som besvarer afhandlingens overordnede problemformulering.

1.6 Kildekritik

Generelt om hjemmesider som kilde:
I projektet er hjemmesider fra internationalt anerkendte organisationer instanser anvendt som primære kilder, da det har været ønsket, at have de nyeste og mest opdaterede informationer som kilde. Dette var bedst muligt gennem hjemmesider, da disse har mulighed for konstant opdatering. Der er dog mulighed for at visse kilder kan have særlige interesser der kan farve indholdet af oplysningerne til egen fordel. Eksempelvis med salgsøjemed. Herunder vil jeg præsentere og argumentere for mit valg af et par af mine kilder.

http://www.iso.org/iso/home.html
ISO er en international organisation der sørger for, at produkter og services overholder visse standarter der skal sikre disses ensartethed og kvalitet. ISOs standarter følges af 163 lande. Dette betyder at de informationer der er tilgængelige på hjemmesiden, skal være meget valide, og konstant opdateret. Derfor må hjemmesiden anses som værende særdeles valid og uden særlige interesser der kan subjektivere de oplysninger der står. Dog kan man drage tvivl om hvorvidt

http://www.isaca.org/about-isaca/Pages/default.aspx
ISACA er en uafhængig non profit organisation, der er specialister i at hjælpe og udvikle værktøjer og tests til brug for it sikkerheden i større virksomheder og organisationer. De har 52 års erfaring inden for feltet, og benyttes af nogle af verdens største virksomheder.

Derforuden fremgår det af deres hjemmeside, at de er certificeret af CISA, CISM, CGEIT; CRISC. Derfor forventer jeg at oplysningerne herfra er objektive og valide, samt at deres løsninger er høj international standart. Dog kan der på trods af deres erklæring om at være en uafhængig

nonprofit organisation, være forretningsmæssige interesser indblandet. Dette begrunder jeg med at de netop tilbyder egne selvudviklede services og produkter.

http://www.ramboll-management.dk/ydelser

Rambøll er et internationalt rådgivningsfirma, der blandt andet varetager analyser og rådgivning inden for ledelse og it styring. Blandt andet effektivisering af it strategi, it sikkerhed og ledelses strategi, hvilket netop er blandt de områder jeg beskæftiger mig med i projektet. En kritik af min brug af Rambøll som kilde, kan være, at de er en organisation der tjener penge på deres vejledning og de ydelser de tilbyder.

Generelt om skriftlige kilder:

Generelt er de nyeste skriftlige kilder de mest troværdige, eftersom de har haft mulighed for at medtage de nyeste informationer, og kan have været genstand for nylig revidering. De skriftlige kilder i projektet har været anvendt under min uddannelse, hvilket må betyde at de er af en kvalitet både faglektorerne og Aalborg universitet kan stå inde for. Jeg har dog valgt at anvende de i litteraturlisten, angivne publikationer som sekundære kilder, idet jeg har ønsket at anvende de mest opdaterede informationer. En undtagelse er dog:

Davidsen, Christina Maria (2008); Intern kontrol i revisionsprocessen; Forlag Thomson.

Christina Maria Davidsen er statsautoriseret revisor ved Ernst & Young og beskæftiger sig blandt andet med uddannelse af revisorer, og revisionslovgivning, hvilket gør, at hun ser mit problemfelt fra det perspektiv, jeg har brug for i projektet. Eftersom hun er med til at uddanne nye revisorer, har jeg stor tillid til hendes materiale.

Så alt i alt antager jeg det for at være nogen fornuftige kilder jeg har benyttet til at skrive denne kandidatafhandling med.

Kap 2 – Teori

2.1 Governance Layer

I dette lag er der teori som kan gøre sig gældende for hele selskabet og på alle processer. Og der vil her blive forklaret ganske simpelt om COSO kuben og dens formål derudover vil der blive beskrevet lidt om risikostyringen i hovedtræk.

2.1.1 COSO

COSO(Committe of Sponsoring Organizations') er en komite der har sin oprindelse i 1985, og dets hovedformål er at lave "frameworks and guidance" til selskaber for at kunne kontrollere risikostyringen.

Ved brug af COSO's begrebsramme er der også en begrænsning, denne begrænsning ses her:

1. *Kvaliteten af intern kontrol er afhængig af ledelsens kapacitet.*
2. *Kontroller er ofte rettet mod forventede forhold/transaktioner og tager ikke højde for det uventede.*
3. *Muligheder for fejl såsom mangel på påpasselighed, vurderingsfejl eller misforståelse af instruktioner*
4. *Ledelsens krav om, at kontrollerne skal være omkostningseffektive.*
5. *Muligheden for omgåelse af kontroller ved samarbejde med personer uden for virksomheden eller med medarbejder inden for denne.*
6. *Muligheden for at en person, som er ansvarlig for en kontrol, tilsidesætter denne.*
7. *Muligheden for at kontrol bliver utilstrækkelig på grund af ændringer i forudsætningerne for denne, eller at udførelsen deraf forringes.*[12]

Ad 1) Intern kontrol skal bruges som et hjælpeværktøj til ledelsen, for at kunne opnå de fastlagte strategier og mål, mens de interne kontrollers kvalitet er afhængig af ledelsens kvalitet. Det er ikke ensbetydende med at de interne kontroller kan sikre en virksomheds succes eller gøre en dårlig ledelse til en god ledelse, men det er et værktøj til at kunne hjælpe.

[12] Davidsen, Christina Maria (2008); *Intern kontrol i revisionsprocessen* – side 32

Ad 2) Der kan ikke indføres en intern kontrol som kan reagere over for uventede påvirkninger, det er derfor vigtigt at de indføres som et middel til at sikre mod fremtidige risici. Desuden spiller de interne kontroller sjældent nogen rolle ved afværgelsen af potentielle erhvervsskandaler.

Ad 3) Intern kontrol kan ikke sikrer mod menneskelig fejl 100 %, den kan kun afhjælpe, bl.a. ville intern kontrol kunne opdage fx fejlindtastning. Derimod vil menneskelige fejl som dårlige instruktioner som misforstås kun kunne opdages ved efterfølgende kontrol.

Ad 4) Det er vigtigt at ledelsen er opmærksom på at, de interne kontroller er omkostningseffektive, at de giver mere nytte til virksomheden end det koster at etablere og vedligeholde dem. Derfor er det vigtigt at ledelsen løbende tager stilling til om de interne kontroller forbliver omkostningseffektive, da både det interne og eksterne vurderingsgrundlag løbende vil ændre sig.

Ad 5) De etablerede interne kontroller kan omgås af medarbejderne, dette vil kun kunne opdages af en løbende overvågning fra ledelsen på de interne kontroller. Der er så det problem, hvordan indføres der interne kontroller til ledelsen og overvågningen af disse, hvor det skal være andre personer end ledelsen som overvåger disse.

Ad 6) Virksomheder er ofte struktureret således at medarbejdere på forskellige niveauer bliver ansvarlig for at overholde bestemte interne kontroller. Det er derfor muligt at den enkelte medarbejder kan tilsidesætte en intern kontrol som de er ansvarlig for, dette vil igen kun kunne opdages ved ledelsens overvågning, som således også er en intern kontrol.

Ad 7) Som også nævnt i punkt 4, er det vigtigt at analysere på hvor vidt de eksisterende interne kontroller er tilstrækkelige da. grundlaget ændres løbende. Så der skal udføres jævnlige opfølgninger og kontrollerne skal tilrettes eller afvikles, afhængigt af virksomhedens situation.[13]

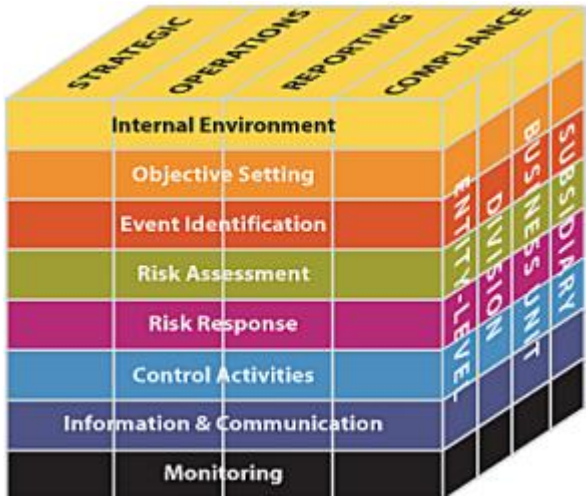
Disse begrænsninger er listet i forhold til hvor vigtige de hver især antages for at være. De nævnte forhold i 1-3, kan karakteriseres som værende menneskelig kapacitet og styring af fremtidige risici, som kan være svære for de interne kontroller at opdage/fange. Forhold 4-7 kan imødegås ved at lave en hensigtsmæssige kontrolprocedure samt en gennemført og god implementering. [14]

[13] Davidsen, Christina Maria (2008); *Intern kontrol i revisionsprocessen* – side 33-34
[14] Davidsen, Christina Maria (2008); *Intern kontrol i revisionsprocessen* – side 34

2.1.2 COSO kuben

COSO kuben er et værktøj for ledelsen til at kunne håndtere, styre og kontrollere risikoen i selskabet via interne kontroller. Samt en hjælp til at kunne identificere risikoer i forbindelse med virksomheden. De 8 indbyrdes processer er det ikke nødvendigt at skulle udføre i den rækkefølge de nævnes i.[15]

Figur 4 - COSO kuben



Kilde: COSO – Helhetlig risikostyring – et integrert rammeverk – Sammendrag side 4

Kuben er opdelt i 3 dimensioner: 1. dimension*"Objectives categories – strategic, operations, reporting and compliance"* Krav til virksomheden ud til omverden. Virksomhedens målsætning. 2. dimension er det intern kontrolsystem, som består af 8 komponenter der vil blive gennemgået længere nede. 3. og sidste dimension er de enkelte forretningsenheder/-aktiviteter.

De interne kontroller har til formål at give ledelsen, i videst mulige omfang, en sikkerhed for at virksomheden opnår sine mål i forhold til; [16]

- Realiseringen af strategien
- Effektiviteten af virksomhedens operationelle aktiviteter
- Pålidelig rapportering
- Overholdelse af lovgivning mv.

[15] Davidsen, Christina Maria (2008); *Intern kontrol i revisionsprocessen* – side 216
[16] Davidsen, Christina Maria (2008); *Intern kontrol i revisionsprocessen* – side 31-32

2.1.3 De otte komponenter i COSO kuben

Her vil de otte komponenter blive gennemgået, hvad disse har af betydning og formål, for at skabe en forståelse for hvorfor disse er væsentlig at benytte sig af.

1. Internal Environment(Intern kontrolmiljø)

At etablere en filosofi omkring risikostyring og det anerkendes at der kan opstå hændelser der er forventede samt uventede, og det er her den daglig ledelse skal træde til og hvis ikke det sker, bliver det sjældent nogen succes. Sørge for at hele denne filosofi er i hele virksomhedens kultur og overveje alle aspekter hvordan virksomhedens handlinger kan påvirke denne kultur.
Det interne miljø udgør fundamentet for risk management ved at tilføre disciplin og struktur. Hvordan risici identificeres, vurderes og håndteres sker på baggrund af det interne miljø. Derudover påvirker det interne miljø virksomhedens tilrettelæggelse og funktionen af kontrolaktiviteter, informations- og kommunikationssystemer samt overvågningsaktiviteter.[17]

2. Objective Setting (målsætning)

Ledelsen fornemste opgave er at sikre virksomhedens eksistens samt vækst over tid. For at dette kan ske, skal der fastsættes en vision og strategiske mål og udarbejdes strategier og til sidst skal der fastsættes delmål. I COSO kuben kan man betragte virksomhedens mål inden for følgende kategorier: (den vandrette flade i COSO kuben)

- Strategi: Målsætning på højt plan, der skal sikre opfyldelsen af missionen og visionen.
- Drift: opnå en så effektiv drift som muligt i virksomheden.
- Rapporteringen skal gerne være effektiv, både internt og ekstern.
- Overholdelse af gældende love og regler (compliance)[18]

3. Event Identification (identificering af begivenheder)

Identificering af begivenheder er det at identificere de(n) risici der kan påvirker virksomhedens realisation af målsætning, der kan opstå i alle dele af virksomheden interne miljø samt det eksterne. Der skal ligeledes også ses tilbage på tidligere begivenheder; hvad gik der galt og hvilken

[17] Davidsen, Christina Maria (2008); *Intern kontrol i revisionsprocessen* – side 218
[18] Davidsen, Christina Maria (2008); *Intern kontrol i revisionsprocessen* – side 221

betydning har dette for fremtiden? For at skabe en forståelse for hvad der udløste disse begivenheder.[19]

4. Risk Assessment (Risikovurdering)

Det er muligt for virksomheden at identificere i hvilken grad en mulig begivenhed kan påvirke målopfyldelsen ved at gennemføre en risikovurdering. Det er ledelsen der skal vurdere sandsynligheden for at denne risiko kan opstå og påvirke målet og i hvilken grad det vil påvirke virksomheden. Grundlaget for sandsynligheden er et skøn, men det kan være vurderet ud fra informationer fra tidligere begivenheder af samme art, dette vil være et mere objektiv skøn, i modsætning til etudelukkende subjektivt skøn.[20]

5. Risk Response (Risikohåndtering)

Ledelsen bør sætte en risikostyringspolitik op som virksomheden kan og skal agere inden for. I den risikostyringspolitik bør der indgå følgende: de organisatoriske rammer for risikostyring, der skal være klare mål for den risikovillighed virksomheden ønsker og en politik for kontrol og overvågning. Der skal identificeres de områder, såvel eksterne som interne forhold tilhørende virksomheder, som ledelsen bør være særligt opmærksomme på, samt hvordan rapportering af disse risici skal finde sted. [21]

6. Control Activities (Kontrolaktiviteter)

Kontrolaktiviteter består af de principper og procedurer, som vil sikre at en risikorespons gennemføres hensigtsmæssigt, som skal ud i hele organisationen, alle niveauer samt i alle funktioner. Kontrolaktiviteterne er for virksomheden et led i en proces for at opnå de forretningsmæssige mål. Disse kontrolaktiviteter omfatter normalt to elementer:

- En politik for hvad der skal gøres
- Procedurer for effektuering af denne politik.

Hver virksomhed har egne mål og metoder til at opnå disse, derfor vil der være en forskel fra virksomhed til virksomhed på hvordan deres mål og strukturer er samt på de kontrolaktiviteter der er implementerede. I det tilfælde hvor der er to virksomheder som har identiske mål og

[19] Davidsen, Christina Maria (2008); *Intern kontrol i revisionsprocessen* – side 221
[20] Davidsen, Christina Maria (2008); *Intern kontrol i revisionsprocessen* – side 221
[21] Davidsen, Christina Maria (2008); *Intern kontrol i revisionsprocessen* – side 221

strukturer, vil der sandsynligvis være en forskel på deres kontrolaktiviteter. Dette skyldes at de etablerede kontroller afspejler det miljø samt den branche som virksomheden opererer i, derudover har følgende faktorer også en indflydelse; kompleksiteten i organisationen, virksomhedens historie og virksomhedens kultur.
Kontrolaktiviteternes kvalitet påvirkes af den enkelte person i virksomheden, hvor det er personlig skøn der anvendes i effektueringen af den interne kontrol. Derfor er det vigtigt, at hver enkelt medarbejder i virksomheden forstår risk management politikken samt hvilken rolle den enkelte medarbejder har i forhold til den kontrolmæssig sammenhæng. [22]

7. Information & Communication (Information og kommunikation)

Informationer er nødvendig på alle niveauer i organisationen med henblik på at kunne identificere, vurdere og reagere på de risici der kan true virksomhedens realisering af sine mål. Det er vigtigt at den relevant information kommunikeres mellem de niveauer der er relevante. Disse informationer kan både være fra interne og eksterne kilder, der kan præsenteres i enten kvantitativ eller kvalitativ form. Grunden til at disse informationer er vigtige, er muligheden for at kunne tilpasse risk management i forhold til ændrede situationer. Det er ligeledes vigtigt at informationerne går ned i organisationen men også at informationerne går op ad. [23]

8. Monitoring (Overvågning)

Denne proces (risk management) bør overvåges over tid, hvor komponenternes tilstedeværelse og kvalitet vurderes. Denne overvågning kan som udgangspunkt tilrettelægges på to måder:

- Gennem løbende aktiviteter
- Gennem enkeltstående evalueringer på fastlagte tidspunkter.

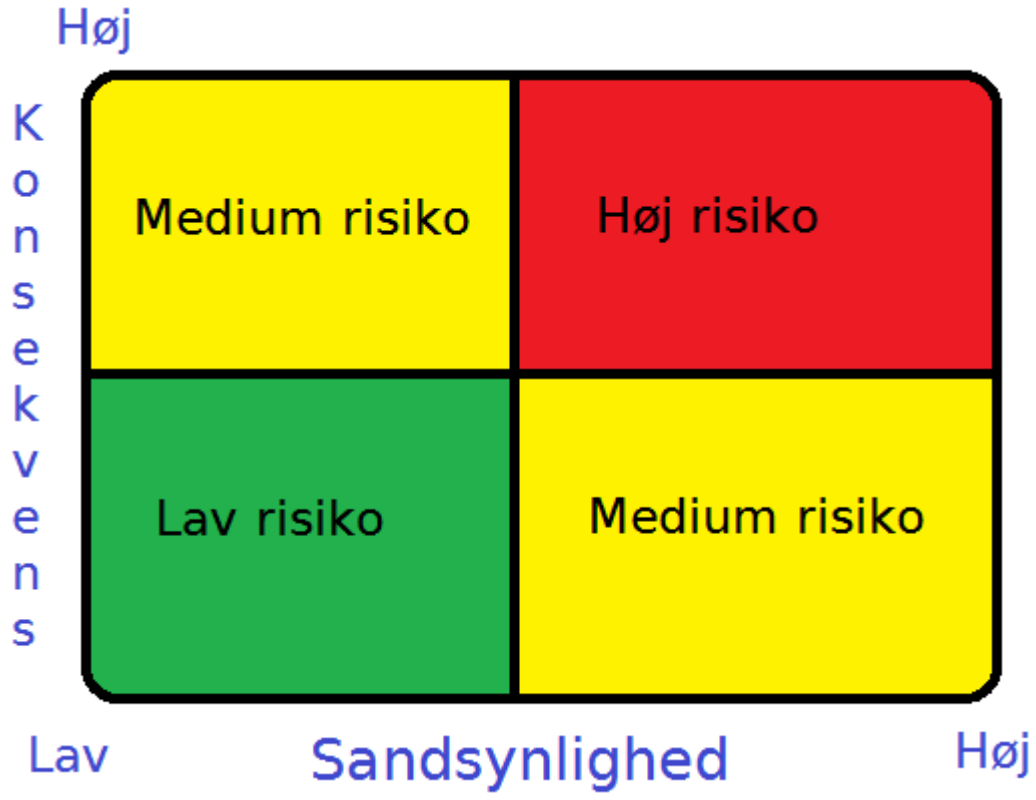
Overvågningen af de løbende aktiviteter inkorporeres i en eller flere af virksomhedens normale og tilbagevendende driftsaktiviteter. [24]

[22] Davidsen, Christina Maria (2008); *Intern kontrol i revisionsprocessen* – side 219 - 220
[23] Davidsen, Christina Maria (2008); *Intern kontrol i revisionsprocessen* – side 219
[24] Davidsen, Christina Maria (2008); *Intern kontrol i revisionsprocessen* – side 220

3.1.1.2 Risikovurdering og håndtering

Efter organisationen har identificerede de risici der kan true dem(risikovurdering), bør den inddele disse efter konsekvens og sandsynlighed. Til dette kan virksomheden benytte sig af en simpel matrix som ser ud som følgende.

Figur 5 – Risikobillede



Kilde: Egen tilvirkning, på basis af DS 484 og undervisning i it-ledelse

Høj risiko er hvor sandsynligheden og konsekvensen er høj, så dette bør og skal der tages hånd om. Dette kan enten være ved at afhjælpe og kontrollere eller at forkaste/undgå projektet (hvis det er i den forbindelse at virksomheden overvejer at opstarte nyt projekt). Ved at afhjælpe og kontrollere, forstås det at der fra ledelses side er taget højde for dette og der derfor er taget sikkerhedsforanstaltninger, dette kunne fx være ved en beredskabsplan. I it sammenhæng kan det være at, man sikrer sig at der er en nødgenerator der slår til, at der udføres jævnligt backup og der hurtigt kan gendannes.

Medium risiko er høj sandsynlighed med lav konsekvens. Her handler det om for virksomheden at kontrollere. Det kan være fejl i data, udstyr der er forældet eller der kommer klager over samme problem. Hvor det for ledelsen er vigtigt at få opsat interne kontroller der fungere samt at

informationen fungere to vejs (top-down og down-top).
Medium risiko er lav sandsynlighed med høj konsekvens. Her vil der ofte være tale om at virksomheden ”deler” denne risiko. Dette kan gøres ved at forsikre sig, brand er et godt eksempel hvor sandsynligheden er ganske lav, men det giver ofte fatale følger, i det ved at virksomheden mister alt data, er udgangspunktet for at starte på ny svær. Ved at dele kan der også outsources til anden part, det kunne fx være al backup der foretages af en anden part.
Lav risiko er lav sandsynlighed og lav konsekvens. Her er der tale om at virksomheden må acceptere at dette kan ske. Det kan være besvigelser, transaktioner der mistes, utilfredse medarbejdere osv. Der vil dog kunne være konsekvenser fra ledelsens side og til fx en ansat der laver besvigelser.

Der vil ofte være mulighed eller sågar nødvendighed for at de forskellige tiltag kombineres. Dette skal gerne tage udgangspunkt i en cost-benefit-betragtning. Lavet ud fra inspiration fra DS 484 – *Standard for informationssikkerhed.*

2. 2 COBIT 5 – IT –governance layer

I dette afsnit vil jeg gennemgå COBIT 5 som er ISACA's nyeste framework inden for it-ledelse.

ISACA er en førende global udbyder af viden, certificering, samfund, forvaltervirksomhed og uddannelse om informationssikkerhed, governance og management af it, samt de it relaterede risici og overholdelse af lovgivningen.[25]

Information er en vigtig ressource i alle virksomheder, fra det tidspunkt hvor informationen er skabt til det tidspunkt hvor den skal destrueres, har teknologien en væsentlig rolle. Informations teknologien bliver mere og mere avanceret og er blevet mere og mere udbredt i virksomheder og forretningsmiljøer.[26]

Dette resulterer i at virksomhederne og virksomhedslederne, mere end nogen sinde før, har et behov for at:

- Opretholde information af høj kvalitet som skal understøtte de forretningsmæssige beslutninger.
- Generere forretningsværdi fra it etablerede investeringer, det vil sige at opnå de strategiske mål og realisere forretningsværdi igennem en effektiv og innovativ brug af it.
- Opnå operationel ekspertise igennem en pålidelig og effektiv anvendelse af it.
- Holde de it relaterede risici på et acceptabelt niveau.
- Overholde den relevante lovgivning.[27]

De virksomheder som har succes i dag er klar over at it har vigtig rolle på bestyrelses- og ledelsesniveau. Bestyrelsen og ledelsen skal samarbejde for derved at inkludere it, it governance og management strategien

COBIT 5 sikrer et samlet framework som skal hjælpe virksomheden med at opnå målsætningerne omkring governance og management af virksomhedens it. En optimal værdi fra it skabes ved at opretholde en balance imellem realiseringen af fordele, optimering af risikoniveauet og ressourceforbruget.[28]

[25] COBIT 5 – *A Business Framework for the Governance and Management of Enterprise IT* – side 2
[26] COBIT 5 – *A Business Framework for the Governance and Management of Enterprise IT* – side 13
[27] COBIT 5 – *A Business Framework for the Governance and Management of Enterprise IT* – side 13
[28] COBIT 5 – *A Business Framework for the Governance and Management of Enterprise IT* – side 13

2.2.1 De fem principper i COBIT 5

I COBIT 5 er der fem overordnede principper for styring og ledelse af IT:

- Princip 1: Imødegå interessenternes behov.
- Princip 2: Dække virksomheden "end-to-end".
- Princip 3: Anvende ét integreret framework.
- Princip 4: Muliggøre en holistisk tilgang.
- Princip 5: Adskille governance fra management.

2.2.1.1 Princip 1: Imødegå interessenternes behov.[29]

Virksomheden eksistere for at skabe værdi for dens interessenter, derfor er værdiskabelse et vigtigt element i ledelsens målsætning. At der skabes værdi betyder en realisering af fordele med en optimal ressourceomkostning samtid med at risiciene minimeres. Værdiskabelsen opdeles i realisering af fordele, risikominimering og ressourceoptimering. En virksomheds interessenter har tit vidt forskellige forestillinger om hvad værdiskabelse er. En virksomheds ledelse skal derfor finde ud af hvilke værdiskabelsesbehov der skal opfyldes. De forskellige behov skal vejes op imod fordelene-, risikoerne- og ressourcevurderingerne. For at afhjælpe denne proces er der i COBIT 5 opstillet tre spørgsmål:

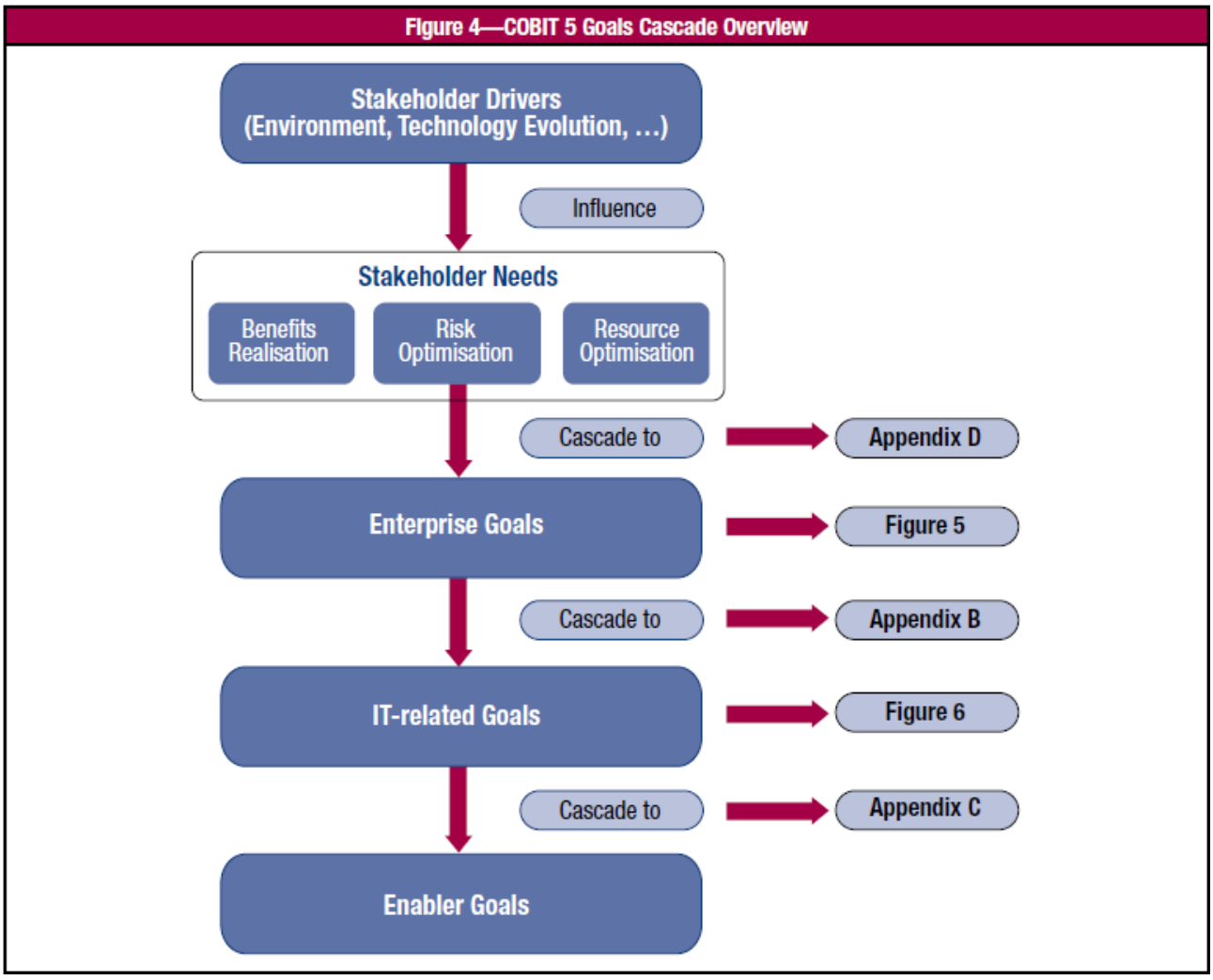
- Hvem får udbytte af fordelene?
- Hvem påtager sig risikoen?
- Hvilke ressourcer er påkrævet?

Interessenternes behov skal være en del af virksomhedens strategi. Ved hjælp af et målvandfald omsættes behovene i COBIT 5 til specifikke, tilpassede og handlingsrettede virksomhedsmål, it mål og enablers mål. Derved opnås en specifik målsætning til hvert enkelt niveau og område i virksomheden, men samtidigt understøtter den overordnede målsætning også. På den måde opnås en optimal tilpasning mellem virksomhedens behov og it løsninger.

Målvandfaldet i COBIT 5 ses i nedenstående figur:

[29] COBIT 5 – *A Business Framework for the Governance and Management of Enterprise IT* – side 17-22

Figur 6 - Målvandfaldet i COBIT 5



Kilde: COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT – side 18

Første element i figuren er de faktorer der har indflydelse på interessenternes behov. Det kan for eksempel være strategien i virksomheden, krav i lovgivningen og ny teknologi.

Det andet element i målvandfaldet omhandler de mål som er påvirket af interessenternes behov. Målene kan udarbejdes ved at anvende Kaplan og Norton's Balanced Scorecard (BSC) dimensioner, hvori nogle af de mest anvendte mål findes. Målene i BSC er ikke udtømmende, men de mål som er specifikke for virksomheden, kan ofte med fordel placeres indenfor de samme områder. Der opstilles 17 generiske mål i COBIT 5, som kan ses i bilag 1.

Det tredje element er de mål der er relateret til it. For at virksomheden kan opfylde sine mål er det afgørende at der eksister nogle it relaterede resultater som kan afspejles i de it relaterede mål.

Der opstilles 17 it relaterede mål i COBIT 5 som er bygget ovenpå de fire dimensioner i BSC, som ses i nedenstående figur.

Figur 7 - IT- Related Goals

IT BSC Dimension	Information and Related Technology Goal	
Financial	01	Alignment of IT and business strategy
	02	IT compliance and support for business compliance with external laws and regulations
	03	Commitment of executive management for making IT-related decisions
	04	Managed IT-related business risk
	05	Realised benefits from IT-enabled investments and services portfolio
	06	Transparency of IT costs, benefits and risk
Customer	07	Delivery of IT services in line with business requirements
	08	Adequate use of applications, information and technology solutions
Internal	09	IT agility
	10	Security of information, processing infrastructure and applications
	11	Optimisation of IT assets, resources and capabilities
	12	Enablement and support of business processes by integrating applications and technology into business processes
	13	Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards
	14	Availability of reliable and useful information for decision making
	15	IT compliance with internal policies
Learning and Growth	16	Competent and motivated business and IT personnel
	17	Knowledge, expertise and initiatives for business innovation

Kilde: COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT – side 19

Det sidste element i målvandfaldet er enabler mål. For at sikre sig at de it relaterede mål opnås, skal virksomheden implementere og bruge enablers. Disse enablers indeholder, processer, virksomhedsstruktur og information. I hver skal der opsættes mål som kan defineres og understøttes af de it relaterede mål.

Målvandfaldet gør det muligt at fastlægge prioriteter for implementeringen, forbedringen og styringen af it-sikkerheden i virksomhedens it-strategiske mål og relaterede risici. Målvandfaldet er dog kun en vejledning, som kræver en tilpasning til virksomhedens specifikke behov. Alle virksomheder har individuelle mål og prioriteter. For at få en effektiv udnyttelse af målvandfaldet bør virksomheden derfor lave et målvandfald som er tilpasset virksomheden. Det tilpassede målvandfald skal sammenlignes det opstillede målvandfald for på den måde at kunne finjustere det.

2.2.1.2 Princip 2: Dække virksomheden ”end to end[30]

Informationen i COBIT 5 omfatter både governance og management hvor den relaterede teknologi ses i et ”end-to-end” perspektiv i virksomheden. It ledelsen skal integreres som en del af virksomhedens governance og skal sikre alle de funktioner og processer som er nødvendige for at kunne lede og styre virksomhedens information og den relaterede teknologi, hvori informationen behandles. COBIT 5 skal sikre en holistisk og helhedsorienteret tilgang til governance og management af it baseret på enablers. Enablerne er også omfattet af virksomhedens ”end-to-end” perspektiv.

Governance ”end-to-end” perspektivet omfatter udover målet med værdiskabelsen elementerne governance enabler, governance anvendelsesområde, roller, aktiviteter, principper, strukturer og processer. Governance enablers kan eksempelvis være ressourcer som frameworks, principper, strukturer og processer som anvendes til evaluering så målene opnås. Governance enablers inkludere desuden virksomhedens ressourcer. Såsom infrastrukturen, personer og information. Ressourcerne og enablerne er vigtige for virksomhedens værdiskabelse til interessenterne. Governance kan anvendes i hele virksomheden eller kun på en enkelt afdeling. Virksomheden skal klarlægge anvendelsesområdet for governancesystemet. I COBIT 5 er anvendelsesområdet for governance hele virksomheden. Den sidste del i princip 2 omhandler roller, aktiviteter og sammenhænge. Her er det defineret hvilke personer som er en del af governance i virksomheden, på hvilken måde de er involveret og hvorledes de skal interagere indenfor anvendelsesområdet i ethvert governancesystem. Der skelnes imellem governance og management aktiviteter i COBIT 5. Ligeledes differentieres mellem hvordan governance- og managementdomænet kommunikerer indbyrdes og hvilke personer der skal stå for kommunikationen.

2.2.1.3 Princip 3: Anvende ét integreret framework[31]

COBIT 5 er et selvstændig framework, det er tilpasset de nyeste relevante standarder og frameworks. Derfor kan det benyttes som et overordnet governance og managementframework . Ligeledes er de tidligere udgivne frameworks af ISACA integreret som en del af COBIT 5, så som COBIT 4.1, Val IT, Risk IT og BMIS.

[30] *COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT – side 23-24*
[31] *COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT – side 25-26*

COBIT 5 framework er den mest komplette og "up-to-date" vejledning til governance og management af virksomhedens it, der er på markedet pt. De områder der havde behov for at blive behandlet yderligere er blevet opdaterede og uddybet, i forhold til COBIT 4.1. COBIT 5 er ligeledes blevet tilpasset til andre relevante standarder og frameworks så som ITIL og ISO standarderne. En række opstillede governance og management enablers, er med til at skabe en struktureret vejledningsmanual.

2.2.1.4 Princip 4: Muliggør en holistisk tilgang [32]

Enablers i COBIT 5 er de faktorer som enten enkeltvis eller samlet har en indflydelse på, om en aktivitet bidrager positivt. Der er her tale om governance og management af virksomhedens it.

Frameworket opdeler enablers i følgende syv kategorier:

- *Principper, politikker, og frameworks*, er de værktøjer som skal overføre den ønskede adfærd til en praktisk vejledning for den daglige ledelse i virksomheden.
- *Processer*, beskriver en række organiserede aktiviteter og kutymer for at opnå og fastholde virksomhedens mål samtidig med at processerne skal benyttes til at producerer nogle resultater som skal være en hjælp til opnåelsen af de it relaterede mål.
- *Virksomhedsstruktur*, er de beslutningstagende enheder i virksomheden.
- *Kultur, etik og adfærd*, af individerne er tit en undervurderet succesfaktor i governance- og managementaktiviteterne.
- *Information*, er udbredt i enhver organisation og omfatter alt information som produceres og bruges af virksomheden. Information er en nødvendighed for at organisationen kan fungere og kan styres. På det operationelle niveau er informationen ofte det væsentligste for virksomheden.
- *Service, infrastruktur og applikationer*, omfatter infrastrukturen, teknologi, og applikationer som tilfører virksomheden med informations teknologiske behandling og services.
- *Personer, færdigheder og kompetencer*, omfatter de personer som er nødvendige for at alle aktiviteter kan færdiggøres succesfuldt og sørger for at korrigere handlingerne og træffe de rigtige beslutninger.

[32] *COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT – side 27-30*

Nogle af de definerede enablers er også en ressource for virksomheden. Det er nødvendigt at disse styres og reguleres af ledelsen. Der er tale om *Information, personer, færdigheder, og kompetencer og services, infrastruktur og applikationer.*

Det er vigtigt at virksomheden har en række sammenkoblingsenablers. De skal bruges til de enablers som kræver inputs fra andre enablers for at være effektive, for eksempel kan det være processer som har behov for information, eller strukturen i organisationen som har brug for færdigheder og adfærd. Derudover skal sammenkoblingsenablerne bruges til at levere outputs til gavn for andre enablers, som for eksempel processer som skal levere information, og færdigheder af adfærd som gør processerne effektive. For at gode beslutninger kan tages omkring governance og management af virksomhedens it, er det nødvendig at den holistiske tilgang til governance og management overvejes. Det betyder at når der skal tages beslutninger omkring interessenternes behov, skal man vurdere om alle sammenkoblingsenablers har relevans og håndteres hvis det er nødvendigt. Tankegangen skal drives af den øverste ledelsen i virksomheden

Enabler Dimensions

I COBIT 5 opdeles alle enablers efter et sæt fælles dimensioner. Disse fælles dimensioner, skal give en fælles, simpel og struktureret måde til håndtering af enablers. De hjælper med at styre det komplekse samspil imellem de forskellige afdelinger i virksomheden, og fremmer et succesfuldt resultat fra enablerne.

De fire fællesdimensioner er:

- **Interessenterne:** Der er forskellige interessenterne tilknytte virksomheden, som har forskellige tilgange til virksomheden og dens mål.
- **Mål:** Der er forskellige enablers, som hver i ser tilføjer en værdi for at opnå målsætningen.
- **Livscyklus:** Alle enablers har en livcyklus, fra plan → udførelse → udfasning.
- **Good practices:** Til hver enabler, er det relevant for organisationen at benytte sig af erfaringer eller viden fra andre standarder, frameworks osv.

Enabler performance Managemt

Resultatstyring af enablers er det sidste element i COBIT 5's målvandfald. Virksomheden forventer et positivt resultat fra applikationerne og fra brugen af enablers. For at styre resultatet fra en enabler er der fire spørgsmål som skal overvåges og besvares:

- Er interessenternes behov dækket?
- Er målene med enablers opnået?
- Er enablers livscyklus håndteret?
- Har man anvendt "good practice"?[33]

De første to spørgsmål er forbundet med det aktuelle resultat fra den enkelte enabler, og de sidste to spørgsmål håndtere den aktuelle funktionalitet af den enkelte enabler.

2.2.1.5 Princip 5: Adskille governance fra management[34]

I frameworket skelnes der tydeligt mellem governance og management. De to områder omfatter forskellige aktiviteter, og kræver forskellige strukturer i organisationen og desuden tjener forskellige formål.

Governance

Governance sikrer at interessenternes behov, vilkår og muligheder vurderes for at fastsætte om virksomhedsmålene opnås og for at fastsætte en retning gennem prioritering af beslutningstagning, samt ved at overvåge resultater og overholdelse af lovgivningen mod de aftalte retninger og mål.

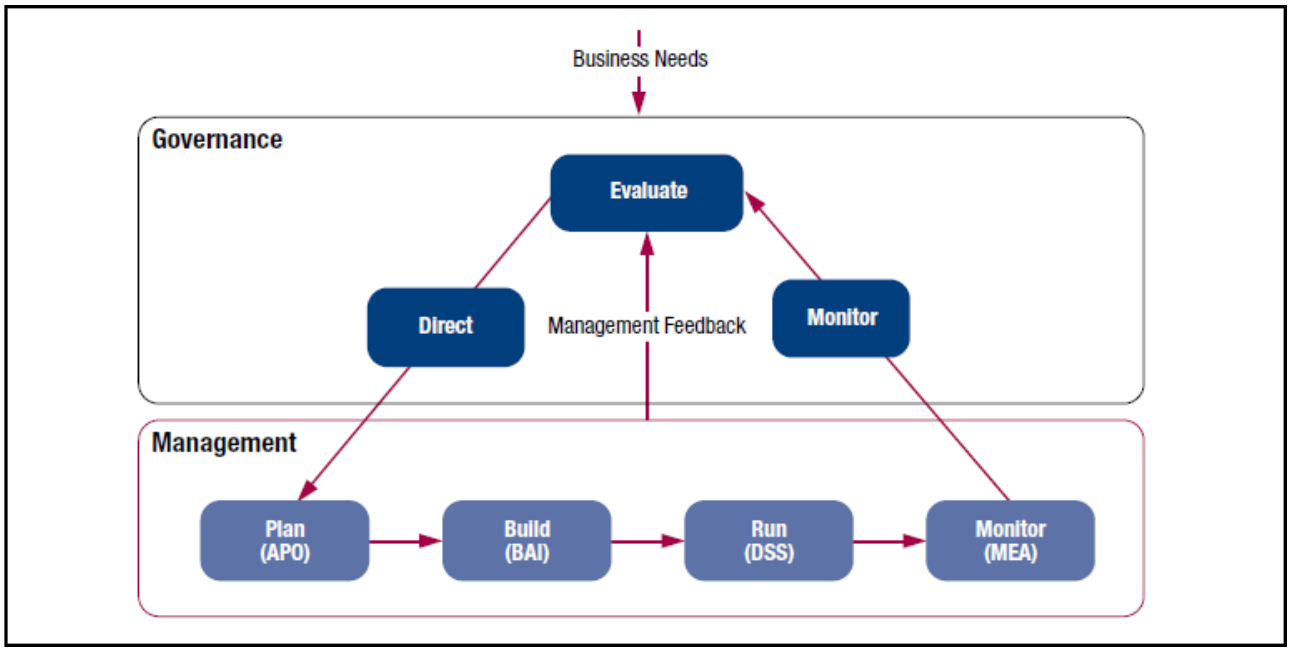
Management

Management planlægger, udfører og overvåger aktiviteterne, ved hjælp af de retningslinjer som er fastsat af governanceorganet for at opnå virksomhedens mål.

Som det ses fra nedstående figur er der er en visualisering af opdelingen mellem governance og management, hvor governance beskæftiger sig med *Evaluate – Direct – Monitor.* Disse punkter vil blive behandlet i afsnittet om ISO 38500. Selve management laget er planen fra governance udføres, opføres, drives(drift) og overvåges som videregives til governance.

[33] *COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT – side 29*
[34] *COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT – side 31-33*

Figur 7 – COBIT 5 Governance and Management Key Areas



Kilde COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT – side 32

2.2.2 Implementeringsvejledningen[35]

For at kunne realisere den optimale værdi fra udnyttelsen af COBIT 5 kræves det at den effektivt tilpasses det specifikke virksomhedsmiljø. Ethvert forsøg på en implementering kræver desuden en løsning til specifikke udfordringer inklusiv management ændringer til kulturen og opførelsen.

Virksomheden skal derfor designe sin egen plan for implementeringen ud fra dens specifikke interne og eksterne miljø så som:

- Etik og kultur
- Gældende lovgivning og politikker
- Mission, vision og værdier
- Governance politikker og praksis
- Forretningsplan og strategi intentioner

[35] *COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT – side 35-37*

- Driftsmodel og modenhedsniveau
- Ledelsesstil
- Risikovillighed
- Kapacitet og tilgængelige ressourcer
- Praksis i branchen[36]

Det er ligeledes vigtigt at designet udnytter og er bygget op omkring virksomhedens governance enablers.

Hvilken tilgang til governance og management af virksomhedens it som er optimal, er forskellig fra virksomhed til virksomhed. Sammenhængen i COBIT skal forstås og overvejes for at kunne tilpasse den effektivt i implementeringen af governance og management af virksomhedens enablers. COBIT er ofte understøttet af andre frameworks, "good practices" og standarder, og disse skal alle tilpasses for at passe til de specifikke ønsker.

Det er vigtigt for implementeringsprocessen at de it relaterede initiativer benytter COBIT for derved kan de blive korrekt reguleret og styret tilfredsstillende. Hovedparten af de it relaterede initiativer som mislykkes, skyldes utilstrækkelig styring, støtte og overvågning fra forskellige interessenter. Desuden skyldes det at implementeringen af governance og management af it enablers i COBIT ikke benyttes korrekt. Opbakning og styring fra de mest betydningsfulde interessenter er nødvendig for at forbedringerne tilpasses og opretholdes

Der er en række faktorer som kan indikere om der er et behov for at forbedre virksomhedens governance og management at it. Ved at anvende de såkaldte "pain points" som lanceringspunkter for implementeringen af de it relaterede initiativer og governanace og managementforbedringer kan man relaterer til de erfaring virksomheden har fra hverdagsproblemer i it. På den måde forbedrer man "buy-in" og det vil give virksomheden en fornemmelse af hvilke problemer der haster og man kan anvende disse i lanceringen af implementeringen.

Her er nogle eksempler på nogle typiske pain points:

- Mislykkede initiativer, forhøjede it omkostninger og en opfattelse af lav virksomhedsværdi.

[36] *COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT – side 35*

- Betydelige uheld relateret til it risikoen, eksempelvis tab af data og fejl i tidligere projekter.
- Problemer med leveringen af outsourcede servicefunktioner.
- It begrænser virksomheden i innovationskapacitet og forretningsfleksibilitet.
- Virksomhedens revisor bemærker at virksomhedens it-performance eller den rapporterede it kvalitet er dårlig for serviceniveauet.
- Høje og skjulte it omkostninger.
- Overlapninger mellem initiativer og spildte ressourcer som for eksempel tidligere projekter som er afsluttet for tidligt.
- Utilstrækkelig it ressourcer, utilstrækkelige færdigheder hos personalet, eller et personale som er overbelastet/utilfredst.
- It relaterede omstruktureringer stemmer ikke overens med forretningsbehovene og sen levering eller overskridelse af budget.
- Bestyrelsesmedlemmer, direktører eller daglige ledere som er tilbageholdende med engagere sig i it, eller mangel engagerede og tilfredse på forretningssponsorer for it.
- Komplekse modeller for it-drift.[37]

2.2.2.1 Livscyklus [38]

Implementeringslivscyklussen skal hjælpe virksomheden med håndteringen af komplekse og typiske udfordringer som kan opstå under implementeringen. De tre relaterede komponenter i livscyklussen er:

1. Kernen som værende en kontinuerlig forbedring.
2. Aktivering af ændringer.
3. Styring af program.[39]

De tre komponenter opdeles i syv faser:

Fase 1: Begynder med en erkendelse af og enighed om behovet for implementering eller forbedring af initiativerne. Her identificeres de nuværende ”pain points” udløser og skaber et ønske om at ændre i de udøvende ledelsesniveauer.

[37] *COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT – side 36*
[38] *COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT – side 37-39*
[39] *COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT – side 37*

Fase 2: Handler om at definere meningen med implementeringen eller forbedring af initiativerne ved at bruge COBIT's kortlægning af virksomhedens mål som sammensættes med de it relaterede mål og målene for it processerne og overveje hvordan risiko scenarierne kan fremhæve hvilke nøgleprocesser virksomheden skal lægge fokus på.

Fase 3: I denne fase sættes et mål for forbedringer, efterfulgt af flere detaljerede analyser som udnytter COBIT's vejledning til at identificere mangler og potentielle løsninger. Nogle løsninger kan være en "quick win" mens andre er mere udfordrende og tager lang tid at implementer. De initiativer som er nemmest at opnå og dem som giver de største fordele bør have den første prioritet.

Fase 4: Her planlægges de praktiske løsninger ved at definere projekter som er understøttet af begrundende forretningsplaner. En ændringsplan for implementeringen skal også udarbejdes. En veludviklet forretningsplan er med til at sikrer at fordelene fra projekterne identificeres og overvåges.

Fase 5: De forslåede løsninger implementeres i denne fase, ved at anvende en "day-to-day" fremgangsmåde. Foranstaltninger kan defineres ved at overvåge det som er etableret ved at anvende COBIT's mål og målinger til at sikre at forretningstilpasninger opnås, vedholdes og forbedres ved hjælp af foranstaltninger. For at opnå succes kræves det at den øverste ledelse viser engagement.

Fase 6: Fokusere på de bæredygtige aktiviteter fra de nye eller forbedrede enablers og overvågninger af om de forventede fordele opnås.

Fase 7: Igennem denne fase skal den samlede succes fra initiativerne revurderes. Yderligere behov for governance og management af virksomhedens it identificeres, og behovet for løbende forbedringer styrkes.

Med tiden skal livscyklussen følges op og gentages, samtidig med at der opbygges en bæredygtig tilgang til governance og management af virksomhedens it.

2.2.3 Process capability model[40]

Virksomheder som anvender COBIT 4.1, Risk IT og Val IT er fortrolige med de procesmodenhedsmodeller som er i disse frameworks. Disse modeller anvendes til måling af den nuværende modenhed af virksomhedens it relaterede processer, for at definere en krævet status af modenheden i virksomheden samt for at bestemme gabet imellem dem, og for at finde ud af hvordan man skal forbedre processer, for at opnå det ønskede modenhedsniveau.

COBIT 5 indeholder en procesegnethedsmodel som er baseret på den internationalt anerkendte ISO/IEC 15504 *Software Engineering – Process Assess standard*. Modellen vil opnå samme samlede målsætning af procesvurdering og procesforbedrings support hvilket vil sige, at det vil give værdi, så det er til at måle præstationen fra governance processerne eller management processerne og på den måde gøre det muligt at identificere de områder der skal forbedres.

Procesegnethedsmodellen i COBIT 5 opdeles i seks egnethedsniveauer som en proces kan opnå:

- **0 Ufuldstændig proces:** Processen er ikke blevet implementeret eller det er ikke lykkedes at opnå formålet med processen. På dette niveau er der lidt eller ingen dokumentation for en systematisk gennemførelse af processens formål.
- **1 Udført proces:** Den implementerede proces opnår dens formål.
- **2 Håndteret proces:** Den udførte proces er nu implementeret og administreres det vil sige planlagt, overvåget og justeret og dens arbejdsprodukt er korrekt etableret, kontrolleret og vedligeholdt
- **3 Etableret proces:** Den håndterede proces er nu implementeret og bruger en defineret proces som er i stand til at opnå de ønskede resultater.
- **4 Forudsigelig proces:** Den etablerede proces operer nu inden for de definerede grænser for at opnå de ønskede resultater.
- **5 Optimeret proces:** Den forudsigelige proces er kontinuerligt forbedret til at møde relevante nuværende og forventede forretningsmål.

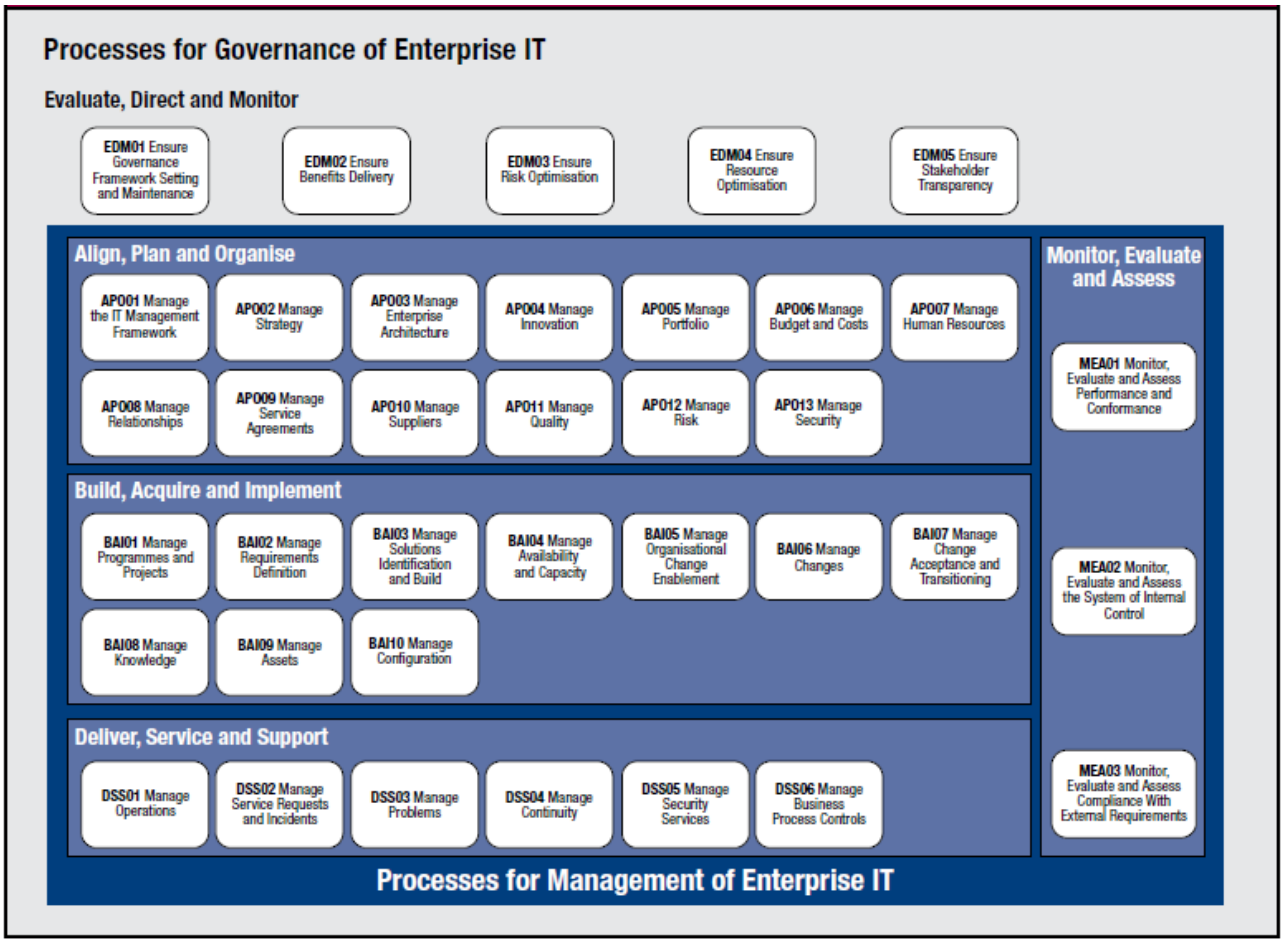
[40] *COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT – side 42-43*

Hvert egnethedsniveau kan opnås når niveauet ovenover fuldt ud er opnået. Hver enkelt virksomhed skal vælge hvilket niveau der ønskes opnås, det vil dog sjældent være en af de højeste.[41]

2.2.4 Processerne i COBIT 5

Nedenstående figur viser hvordan processerne i COBIT 5 er inddelt under hver deres domæne

Figur 8 - COBIT 5 Process Reference Model



Kilde: COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT – side 33

Som det kan ses i ovenstående figur er der i alt 37 processer for styring af virksomhedens it i COBIT 5. Processerne opdeles på fem domæner.

[41] *COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT – side 43*

2.3 God it-skik 2011

God it-skik har til formål at skulle hjælpe virksomhedens øverste ledelse med at få et overblik over de discipliner inden for it-området som de analyserer, beslutter inden for og planlægger, samt at implementerer og følge op den it-anvendelse der er i virksomheden i overensstemmelse med god it-skik. Ved god it-skik har ledelsen et fokus på informationsteknologi, systemer og de resultater der opnås samt på risikostyring. Der er et stigende behov til ledelsen om overholdelse af initiativer og regler og at det erkendes at it-projekter har indflydelse på virksomheders succes. It-området skal ikke bare betragtes af ledelsen som værende en "sort boks" i virksomheden, men derimod er det vigtigt at topledelsen involveres i vigtige it-beslutninger og ikke bare sender det ansvar videre til it-fagfolk, men derimod inddrager disse i beslutningsprocessen. Derudover er det vigtigt i beslutningsprocessen, at alle interessenters input af relevans inddrages herunder er der tale om ledelsen, brugerne og it-fagfolk.[42]

2.3.1 Ledelsens ansvar [43]

Det er vigtigt at der træffes beslutninger omkring de muligheder virksomheden har for it-anvendelse i forretningsstrategien og dette skal ske på øverste ledelsesniveau. Ledelsen har til ansvar at skabe effektiv interaktion og integration imellem forretningen og it-afdelingen. Den øverste ledelse bør, med udgangspunkt i forretningsstrategien, drøfte hvordan it anvendes til at understøtte virksomhedens forretningsfunktioner, samt til at udvikle forretningen. Til dette vil en grundlæggende SWOT-analyse være et godt udgangspunkt.
Der skal fastlægges rammer for it-anvendelse i form af visioner, strategier, mål og planer. Der bør ydermere tages stilling til kompetencebehov og sourcing-strategi. Ved styring af it-anvendelse er det nødvendigt at følgende aktivitetsområder indgår; porteføljestyring og it-risikostyring.

Lovgivning til ledelsen

Ifølge selskabslovgivningen fremgår det at ansvaret for selskabets forsvarlige organisation samt tilrettelæggelse af de interne kontroller tilfalder bestyrelsen. Bestyrelsen/tilsynet bør tage stilling til virksomhedens it-organisation, da det må antages af denne del har en væsentlig betydning for styring af virksomheden. "I andre dele af lovgivning stilles der krav til it-systemer og data,

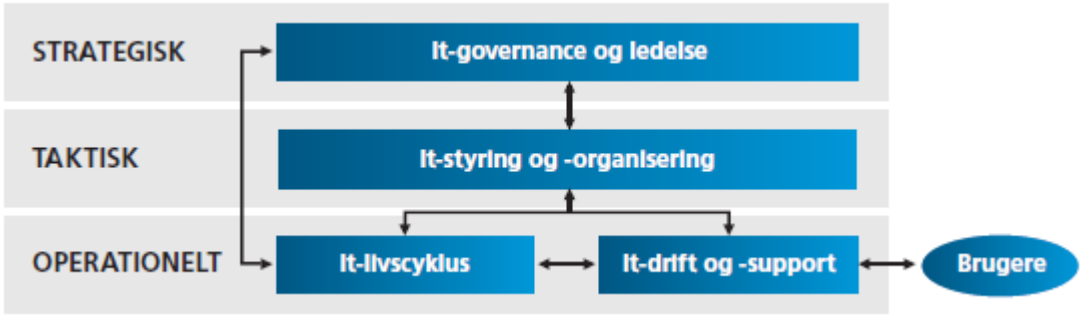
[42] God it skik 2011 – side 4-5
[43] God it skik 2011 – side 6

registrerede personoplysninger samt ophavsret til systemer og indretning af (it-) arbejdspladser." *(god it skik side 6).* Der er ligeledes virksomhedstyper hvor der stilles særlige krav, fx offentlige og finansielle virksomheder. Derudover vil selskaber, hvor moderselskabet befinder sig i udlandet i større eller mindre grad benytte sig af lovgivning i moderselskabets hjemland.
Love og regler er under konstant udvikling og det er derfor vigtigt at de enkelte selskaber er opmærksom på dette og har fokus på at kunne implementere disse så effektivt som muligt.

2.3.2 It-aktiviteter i processer[44]

De enkelte processer der her bliver beskrevet er på et overordnet niveau, men er relevant for de fleste virksomheder. Disse processer skal således tilrettelægges efter den enkelte virksomheds vision, mål, kultur og kapacitet.

Figur 9 – De fire hovedprocesser



Kilde: God-it-skik side 7

Som det fremgår af ovenstående figur bør en virksomheds it-processer deles op i fire fordelt på tre niveauer; hhv. strategiske, taktiske og operationelt. Disse fire vil blive uddybet i et senere afsnit og nedenstående er derfor kun til at skabe en overordnet forståelse.

1. **It-governance og -ledelse**
   Det er virksomhedens øverste ledelse som har med den strategiske planlægning og opfølgning af it-anvendelse at gøre. Denne proces skal være den der sikrer at virksomhedens øvrige it-processer drives og udvikler sig målrettet.
2. **It-styring og –organisering**

[44] God it skik 2011 – side 7-9

Her fastlægges rammen for virksomhedens teknologiske udvikling, organiseringen af de menneskelig ressourcer samt styring af risici og de eksterne krav, dvs. styring af virksomhedens ressourcer indenfor informationsteknologi.

3. **It-livscyklus**

   De processer som håndterer anskaffelsen, udviklingen, implementeringen og udfasningen af de valgte it-løsninger inden for de valgte rammer i virksomheden.

4. **It-drift og –support**

   Det skal her sikres at de it-løsninger der er implementerede i virksomheden afvikles indenfor de rammer der er givet samt at den ønskede kvalitet opretholdes.[45]

I en virksomhed skal der være klar adskillelse mellem de 4 ovenstående hovedprocesser, men det er vigtigt at der stadig er en relation mellem disse og at de inddrager viden fra hinanden. Organisationen skal have et realistisk ambitionsniveau, så det muligt at opnå og ogs¨så det er muligt at vedligeholde, indføre og justere processerne, så der opstår en optimal anvendelse. Internt bør en virksomheden dokumentere, hvorledes opgaver i de forskellige ansvarsområder håndteres og hvordan disse arbejder sammen på tværs af organisationen samt hvem der er den ansvarlige for de enkelte processer. Til dette kan der med fordel anvendes et relevant metodeværk, som kan understøtte ledelsen. Eksempler på sådan et metodeværk kunne være COBIT, ISO, MSP, PRINCE2, PMI, CMMI og ITIL. Et fællestræk for disse er, at de alle er udarbejdet af internationale anerkendte institutter med en global forankring. Det skal dog pointeres at disse tager udgangspunkt i forskellige filosofier som kan give konflikter mht. god it-skik. Derfor bør it-ledelsen og forretningsledelsen i samarbejde vurdere hvilken af disse metodeværker der har relevans for virksomheden.

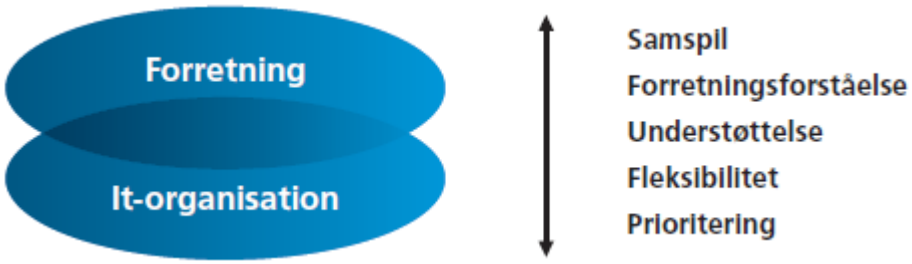
Som enhver proces i virksomheden, bør det løbende vurderes om de enkelte processer er implementerede i en tilstrækkelig grad, i dette ligger der blandt andet følgende; at skabe værdi, optimere arbejdsgangene og minimere relevant risici. Desuden må det forventes at der ligger en plan for den videre modning og at denne anvendes.

Det er vigtigt at it-organisationen sikrer at de nødvendige og hensigtsmæssige processer rækker ind i basisorganisationen hvor det er relevant. Dette kan begrundes på baggrund af at organisationen ønsker at kunne følge fremdrift, have muligheden for at kunne adressere behov og

[45] God it skik 2011 – side 7

problemer eller fordi it ønsker at inddrage basisorganisationen i fx beslutningsprocesser(kunne være i forbindelse med opgaveprioritering).

Figur 10 – samspil mellem forretning og it-organisationen.



Kilde: God it-skik, side 9.

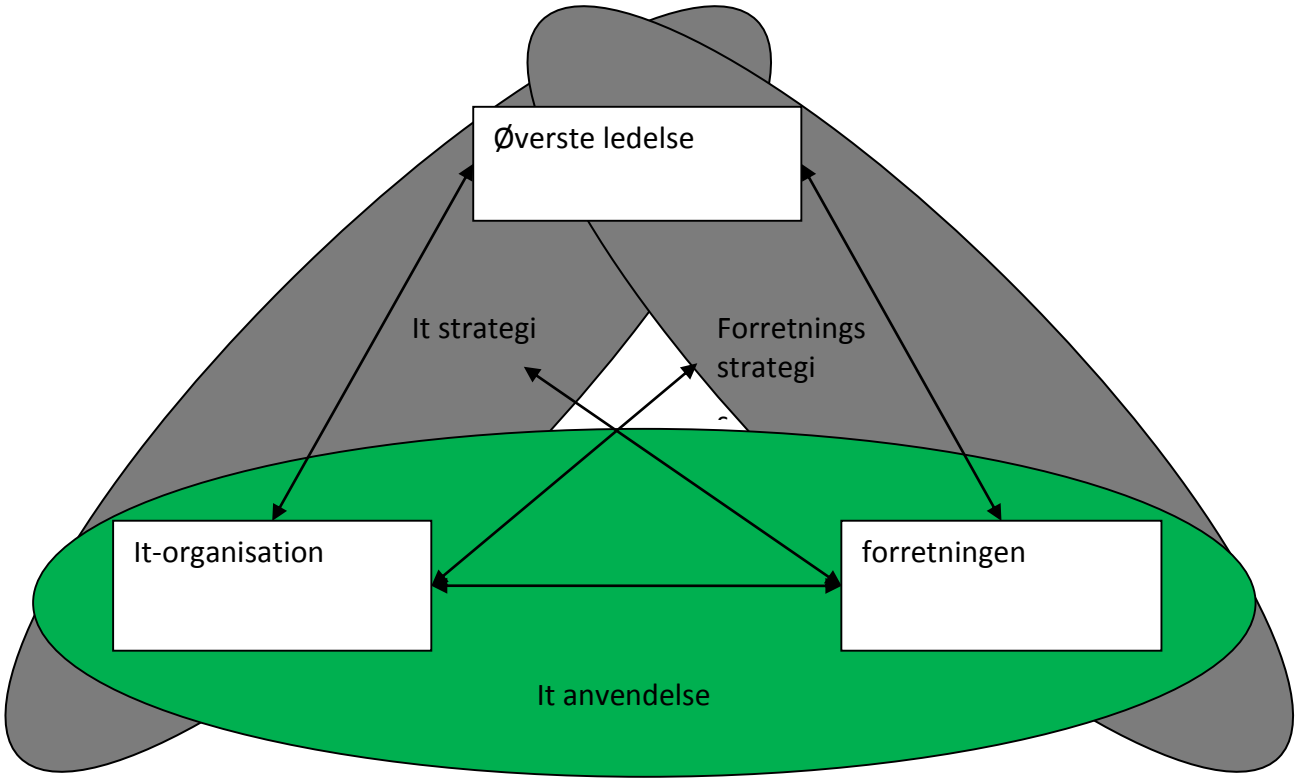
Der skal være en klar definition af de processer der skal sikre et tæt samspil mellem de forretningsmæssige mål og den it der skal understøtte disse. Herunder skal der være realistiske tidsintervaller, rolle- og ansvarsfordeling og beslutningskompetenceniveauer. Det er topledelsen der har ansvaret for it-governance og it-organisationen vil normalt være der ansvaret er placeret mht. at gøre processerne lettere for det givne område. It-organisationen forventes også at have kompetencer til at kunne se it-disciplinen fra et forretningsmæssigt perspektiv, samt at forstå den proces og interaktion der er mellem forretning og it-afdeling.

2.3.3 It-governance og ledelse[46]

Formålet med dette afsnit er at virksomheden sikrer at deres it-anvendelse understøtter virksomheden forretningsstrategi og politikker. For at dette kan lade sige gøre og for at it-anvendelsen udvikler sig hensigtsmæssigt med forretningen og er med til at skabe udvikling er det vigtigt der er et tæt sammenspil mellem den øverste ledelse og ledelsen af it-aktiviteterne. Derfor er det vigtigt at it-organisationen tilfører viden til forretningen om it-anvendelsen og ligeledes er det vigtigt at forretningsdelen tilfører viden til it-organisationen omkring forretningen. Dette er illustreret i nedenstående figur.

[46] God it skik 2011 – side 10-15

Figur 11 – Samspillet i organisationen



Kilde: Egen tilvirkning

Jeg har valgt at lave en omfortolkning af god it-skik, og forklare det på en lidt anden måde. Den øverste ledelse skaber i samarbejde med it-organisationen en it-strategi som ender ud i en plan om it-anvendelse. Den øverste ledelse = It-governance og ledelse. It-organisation = It-styring og –organisering. It anvendelse = it-livscyklus samt it-drift og –support. Det følgende vil så kun være udpluk fra god it-skik som jeg anser for at være relevante og ikke nogen fuldstændig gennemgang af hvad god it-skik er.

It-strategien:

Det er her it-organisationen i samarbejde med den øverste ledelse planlægger og fastsætter mål for it-anvendelsen, så disse bidrager til virksomheden på den mest optimale måde i forhold til den

forretningsmæssige og organisatoriske udvikling. For at dette skal lykkes, kræves det at der er tæt samklang mellem visionen og de aktiviteter, som it-organisationen iværksætter til at understøtte virksomhedens vision. Det er den øverste ledelse som skal skabe bindeleddet mellem it- og forretningsstrategien og sørge for at der er fastsat klare mål der bliver kendt og accepteret i hele organisationen. En del af planlægning er også at skabe et overblik over den modenhed it-anvendelsen har, som blandt andet består af den nuværende situation og de fremadrettede forventninger, samt af tiltag, som kan sikre den nødvendige vækst. Til dette forudsættes blandt andet følgende punkter:

- *Bevidsthed og ansvarlighed om de risici, der er forbundet med beslutninger om it-anvendelse*
- *Bevidsthed om og nedbringelse af risikomomenter*
- *Standardiseret systemarkitektur*
- *Dokumenterede processer og målrettet anvendelse af branchespecifikke metodeværk*
- *Stærk udviklings- og ændringshåndtering*
- *Målbare og aftalte serviceniveauer*
- *Prissætning af ydelser og services*[47]

Det forventes ydermere at der tages stilling til om der kan opnås yderlige fordele ved at outsource til en eller flere samarbejdspartnere, som har en større kapacitet og kompetence. En outsourcing skal dog stadig løbende ledes og der må derfor afsættes ressourcer internt som har de rette kompetencer til at lave løbende opfølgning og ændringshåndtering.

Den strategiske planlægning af it-anvendelse vil se forskellig ud fra virksomhed til virksomhed samt fra branche til branche og der vil derfor være forskellige indgangsvinkler og fokus alt efter hvilken type af forretning der er tale om.

Omgivelserne til en virksomhed har en masse krav og forventninger. Fra virksomhedens side er det en balancegang mellem på den ene sideforventningerne om en innovativ, værdiskabende og effektiv virksomhed og på den anden side er der kravene om at der er styring af risici, overholdelse af lovgivning, myndighedskrav samt en god virksomhedsledelse. Disse forventninger og krav skal virksomheden vurdere og afbalancere og alt dette afspejles i strategiske styrings-, compliance- og

[47] God it skik 2011 – side 11

sikkerhedsmæssige tiltag i forhold til virksomhedens anvendelse af it.

Forhold som ledelsen bør inddrage i business casen:

1. *Identifikation af de dele af forretningsstrategierne, som skal understøttes eller muliggøres ved brug af it-løsninger.*
2. *Overvejelser om nye it-løsninger og –systemer kan anvendes til at skabe nye forretningsmuligheder.*
3. *Hvilke forventninger kunder, investorer, kreditorer og myndigheder har til virksomhedens brug af it-systemer.*
4. *Analyse af styrker, svagheder, muligheder og trusler.*
5. *Identifikation af de Key Performance Indicators, der skal anvendes som målepunkter og understøtte virksomhedens kritiske succesfaktorer.*
6. *Identifikation og styring af risici relateret til it-anvendelsen.*
7. *Krav til fortrolighed, integritet og tilgængelighed ved virksomhedens behandling og anvendelse af information.*
8. *Regler og lovkrav der skal opfyldes vedrørende virksomhedens it-systemer og data.*
9. *Økonomiske rammer for omkostningerne ved anskaffelse og løbende drift samt de økonomiske og personalemæssige gevinster, som implementering af et it-initiativ kan give mulighed for.*[48]

For en virksomhed der skal til at lave en større forandring, er det en god ide at etablere et program, som derefter består af mindre projekter, således sikres det at størrelsen og kompleksiteten bliver mindre for de enkelte projekter og det gør det derfor nemmere at overskue dem når de bliver mere håndterbare, ligeledes øger det chancen for at de også gennemføres i rette tid indenfor de aftalte økonomiske rammer.

2.3.4 It-styring og organisering[49]

I dette afsnit har vi med ledelsen på det taktiske plan at gøre, dette er bindeleddet fra den øverste ledelse og ned til den praktiske udførelse af "it-anvendelse". Det er her vigtigt at det sikres at virksomhedens it-ressourcer og it-udvikling styres, således at disse understøtter virksomhedens

[48] God it skik 2011 – side 12
[49] God it skik 2011 – side 16-20

strategi optimalt. Der anvendes her metoder og værktøjer, som er afpasset til de forhold og den branche virksomheden befinder sig i.

Projektstyrings model: Det er her bør betyde, at virksomheden fastlægger sig på en model som dækker de forskellige behov for styring af de forskellige projekter der vil opstå over tid i virksomheden. Her er der tale om fx anskaffelse, systemudvikling, organisationsudvikling og vedligeholdelse af driftsmiljø og sourcing. Denne model skal blandt andet sikre, at:

1. *Hvert projekt er vurderet og prioriteret i forhold til forretningsværdi, benefits, initialomkostninger, og løbende driftsomkostninger*
2. *levering af projektresultaterne sker indenfor de fastlagte tider og budgetter og i den aftalte kvalitet*
3. *projekterne bruger it-ressourcerne effektivt i forhold til mulighederne og det besluttede risikoniveau*
4. *alle relevante interessenter bliver involveret (i forhold til ansvar og ejerskab) på rette niveau og til rette tid i projektet*
5. *ændringshåndteringen foretages løbende baseret på de erfaringer, der opnås undervejs i processen*
6. *projekter, der viser sig ikke at være rentable, stoppes og afvikles på forsvarlig vis tidligst muligt i forløbet*
7. *såvel de enkelte projekter som porteføljen af projekter koordineres og overvåges af en faglig instans (f.eks. i projekt- eller programkontoret) efter sammenlignelige principper og standarder*
8. *der sker en løbende opfølgning og tilpasning af modellens effektivitet og organisatoriske implementering baseret på de indhøstede erfaringer*
9. *der sker en afklaring og tilpasning i forhold til den mulige kapacitet og kapabilitet*[50]

Styring og vedligeholdes.

Virksomheden kan med fordel anvende standardiserede drifts-, vedligeholdelses- og afviklingsmetoder, som giver en velstruktureret og dokumenteret it-anvendelse. Ydermere bør der

[50] God it skik 2011 – side 17

enten udvikles eller anskaffes værktøjer til at effektivisere og dette bør understøttes af metoder og standarder. Arkitekturen af it bør fastlægges således at virksomhedens behov dækkes samt iten sikrer en effektiv genbrug og udnyttelse af it-løsningerne.

Standarder for system-, drifts- og brugerdokumentation bør medvirke til at sikre, at:

1) *Systemerne til stadighed kan vedligeholdes og afvikles uafhængigt af enkeltpersoner*
2) *Der blandt andet i fejlsituationer hurtigt kan opnås et overblik over den samlede hardware-, netværks- og softwarekonfiguration*
3) *Brugerne (inkl. kunderne) kan betjene it-systemerne korrekt ud fra brugervejledningerne*
4) *Der hurtigt og effektivt kan følges op på it-driften*
5) *Dokumentationen lever op til regler og lovkrav*[51]

Det er vigtigt at der skabes og anvendes en struktureret metode til versionsstyring og –kontrol, som skal sikre at, den version som benyttes er den samme, som ledelse og systemets ejer har godkendt. Derudover skal den tilhørende dokumentation til den gældende version stemme overens samt der skal være en backup af ældre versioner således det er muligt at kunne genfinde tidligere versioner i det omfang dette er nødvendigt.

Versionsstyring: Er til for at kunne holde styr på de mange parallelle versioner af et programs kildekode, da der i mange virksomheder ofte benyttes samme program, database osv., på en gang af flere personer. Det er her relevant at disse data, fra de forskellige medarbejder, ikke overskriver hinanden men at disse sammenflettes. Versionsstyringssystemer kan også anvendes til andet end programmer, fx til håndtering af dokumentation og tekster i almindelighed.[52]

It-organisering

Organisationsstrukturen bør være gennemskuelig med klare kommandoveje og en informationsstruktur samt med klare definitioner af hvem der har mandat, rolle og ansvar, gældende for alle der medvirker. Dette skulle gerne medføre at virksomheden undgår at skulle suboptimere og forhindre afhængighed af enkeltpersoner, således at it-ressourcerne anvendes optimalt og koordineret. Endvidere bør dette også sikre at både ledelsen og brugerne har indflydelse på it-anvendelse, når det er relevant.

[51] God it skik 2011 – side 17
[52] version2.dk 13/01-2013

I organisationsstrukturen er det yderst vigtigt at der er funktionsadskillelse(meget relevant for revision) således at der er en adskillelse af brugerfunktioner, udviklings-/vedligeholdelsesfunktioner, driftsfunktioner og sikkerhedsfunktioner, disse bør etableres og overvåges således at ingen enkeltperson har eller kan få kontrol over en eller alle faserne i it-anvendelse. Dette er også med til at afhjælpe afhængighed af enkeltpersoner.
I tilfælde at virksomheden har outsourcet it-aktiviteter, bør det sikres, at en organisatorisk funktion forhandler, optimerer, overvåger og styrer indgåede aftaler med hensyn til serviceniveau, forretningsmæssigt udbytte, ændringshåndtering og risici.

Medarbejder, kommunikation og fastlægges af ejerskab

Medarbejderne bør oplæres og kvalificeres således de enkelte personer passer til deres arbejdsfunktion, her kan der benyttes efteruddannelse samt træning. Er der ikke en kompetent viden til stede, vil dette være kritisk og derfor yderst vigtigt at tilføje organisationen, dette kan ske gennem ansættelse af nye medarbejder med den kompetence der er nødvendig, få en ekstern konsulent eller lade en leverandør varetage opgaven.
Kommunikationen spiller en stor rolle i en organisation. Det er vigtigt at den information der videregives er relevant for den enkelte modtager, og at informationen kan gå begge veje. Rapporteringen og opfølgningen skal være målrettet de behov, således at de enkelte medarbejdere kan holde sig tilstrækkeligt orienterede, hvilket ligeledes giver dem bedre mulighed for at reagere og rette/ændre på ikke hensigtsmæssige aktiviteter. For ledelsen er det vigtigt at kommunikere den fornødne forståelse af holdninger, mål, strategier, politikker, retningslinjer, forventninger til performance, kvalitet og sikkerhed ud til medarbejderne.
Der bør organisatorisk set være en ejer af de systemer, udstyr, netværksressourcer og faciliteter, som er ansvarlig for anskaffelse, vedligeholdelse og anvendelse. Ved outsourcede aktiviteter bør der stadig være et ejerskab der er forankret internt i virksomheden.

Virksomheden bør regelmæssigt lave en analyse, vurdering og håndtering af risici vedrørende den samlede it-anvendelse, ved dette bruges gerne den samme metode. Derudover bør virksomheden etablere regelsæt og procedurer, som kan sikre at lovgivning, aftaler, branchestandarder og lignende reguleringer overholdes af virksomheden.

2.3.5 Ledelsens it-værktøjskasse[53]

Den øverste ledelse har ansvaret for at der sker en forsvarlig organisering af selskabets regnskabsfunktion, intern kontrol, it-organisering, budgettering og særlige risici, jf. selskabsloven § 115. It spiller i de fleste virksomheder en væsentlig rolle, og derfor bør den øverste ledelse have fokus på it-organisation, it-sikkerhed og it-anvendelse.
Der bør ved enhver form for væsentlig ændring og/eller minimum en gang årligt, fra bestyrelsens side tages stilling til følgende forhold. It-strategi og politik, virksomhedens informationssikkerhedspolitik samt it-risikovurdering.

It-strategien er den øverste ledelses beskrivelse af de strategiske beslutninger der skal finde sted omkring it-anvendelse, og dette bør ske i overensstemmelse med forretningens strategi. Det er vigtigt at it-strategien også underbygges og rammer på de andre ledelsesniveauer, det taktisk og operationelle niveau, således at it-strategien efterleves i praksis.
Til udarbejdelsen af it-strategien skulle følgende områder behandles, på det strategiske niveau.

- *Visioner og pejlemærker*
- *Serviceniveau*
- *Arkitektur og forretningsunderstøttelse*
- *Styring, organisering og politikker*
- *Kompetencer*
- *Risikostyring og informationssikkerhed*
- *Økonomi*[54]

Taktisk niveau:

Der bør formuleres politikker der sikrer at adfærden og kulturen er gennemgribende, således at det strategiske niveau opfyldes. Disse dokumenter skal helst udarbejdes på gruppeleder- og team niveau, ud fra anbefalinger fra længere oppe i organisationen.

Operationelt niveau:

Her bør der laves klare definitioner af følgende; instrukser, manualer, procedurer og processer, således der sker en effektiv og ensartet udførelse af de daglig rutiner. Der bør løbende tages

[53] God it skik – side 32-36
[54] God it skik – side 32

stilling til om der skabes et overflødigt administrativt eller arbejdsmæssigt bureaukrati, ligeledes bør der ske en løbende vedligeholdelse af de eksisterende materialer og ansvarlige for dette bør udpeges.

It-risikovurdering.

Dette er en proces, der tager sit udgangspunkt i analysen af de it-mæssige risici, der er foretaget på de eksisterende forretningsprocesser. Det er her relevant at overveje hvilke begivenheder der kan påvirke gennemførelsen af strategien. Der skal både tages hensyn til interne og eksterne forhold, som er knyttet til:

En effektiv risikovurderingsproces bør sikre, at:

- *Processen er organisatorisk forankret, og der er udpeget en ansvarlig herfor*
- *Processen er koordineret med de øvrige risikovurderingsprocesser i virksomheden*
- *Processen identificerer relevante risici, og der sker en passende kvantificering i overensstemmelse med en godkendt model*
- *Der ved væsentlige ændringer i risikobilledet og mindst en gang årligt gennemføres en fornyet vurdering forhold til virksomhedens eksponering*
- *Der udarbejdes mitigeringsplaner for identificerede risici, som overstiger virksomhedens risikoappetit*
- *Der er en backtest-opfølgning på risikovurderingsprocessen ved registrering af indtrufne risikohændelser.*[55]

Man bør fra ledelsens side, i risikoanalysen, forholde sig til fortrolighed, integritet og tilgængelighed, når der skal vurderes relevante trusler og sårbarhed. Dette kan gøres ved at opliste forskellige hændelser der kan påvirke sikkerheden og derefter vurdere disse i forhold til sandsynlighed og konsekvens.

Sikkerhedstruende hændelser kan f.eks. være:

- *Menneskelig fejl*
- *Systemfejl*
- *Driftsproblemer*
- *Manglende efterlevelse af procedurer*

[55] God it skik side 34

- *Personafhængighed*
- *Uautoriserede eller kriminelle interne aktiviteter*
- *Eksterne angreb*
- *Organisatoriske problemer*
- *Uforudsete konsekvenser af ændringer.*[56]

De allerede eksisterende sikringsforanstaltninger i virksomheden bør eftertestet for at bedømme om de er tilstrækkelig i forhold til den ønskede risikovillighed. Hvis disse ikke efterlever den ønskede risikovillighed bør virksomheden supplere med yderligere sikringsforanstaltninger.

Informationssikkerhed er efterhånden en proces/disiciplin i virksomheder og bør derfor være integreret i forretningsprocesserne, teknologianvendelsen og udviklingen samt kulturen for både ledelsen og medarbejder. Det virksomheden bør tage hensyn til, som kan true virksomheden er:

- Vira/virus
- Fysisk angreb
- Spam-mails
- Hacking
- Manglende back-up
- Tyveri
- Manglende beskyttelse af data, her er der tale om både fysisk tilgang såvel som virtuel.

Denne liste er ikke udtømmende, men en dårlig håndtering af ovenstående kan give en negativ effekt på virksomhedens drift, økonomi og omdømme.
Ledelsen bør sikre at der er en virksomhedspolitik omkring informationssikkerheden, som dels er lavet på baggrund af risikoanalysen og det ovenstående, samt sund fornuft. Det er kritisk for virksomheden at denne politik er kendt og følges i hele organisationen, således at det er en generel holdning der er. Sikkerhedsniveauet bør fastlægges på et passende niveau med hensynstagen til relevante trusler, ressourcer, konsekvenser, relevant lovgivning, forretningsmæssige mål og aftalemæssige forpligtigelser.

[56] God it skik side 34

Analysen og politikken bør jævnligt efterses og det bør gennemgås om de til stadighed lever op til teknologien og virksomhedens forventninger. Dette bør igen også ske med jævne mellemrum, fx med en frekvens på et år, eller ved større ændringer, såvel som interne som eksterne, der kan påvirke trusselsbilledet.

2.4 ISO/IEC 38500 - Corporate governance of information technology.

Indledning

ISO *(International Organization for Standardization)* og IEC (*International Electrotechnical Commission)* er specialiserede standarder verden over. ISO og IEC har forskellige arbejdsområder, men har et samarbejde hvor der en fælles interesse.[57]

ISO har til formål at sørge for der en international harmonisering på verdensplan for at kunne nedbryde barriere med henblik på international samarbejde, samt at give virksomhederne forskellige værktøjer til at forbedre og optimere driften osv.

Formål med ISO/IEC 38500

Standardens mål er at give ledelsesniveuaet et framework med principper til at vurdere, lede og overvåge brugen af IT i virksomheden. Da de fleste virksomheder benytter sig af IT, som en stor del af driften og det i fremtiden vil spille en stor rolle, er det relevant at have fokus på hvordan man anvender dette effektiv.

Denne standard skulle gerne give det højeste ledelsesniveau en forståelse for hvorfor IT er så vigtig for virksomheden og at IT-governance bør være et fokusområde.[58]

Denne standard giver viden og vejledende principper til organisationens top ledelse, bestyrelse, direktion og den daglige ledelse(vil i dette afsnit blive omtalt som "*direktionen*") omkring en acceptabel, kompetent og effektiv anvendelse/udnyttelse af IT i virksomheden. Standarden har ligeledes mulighed for at kunne anvendes på små og store virksomheder samt privat og offentlige, hvilket gør den meget anvendelig og universel.[59]

Formålet med ISO/IEC 38500 er at forbedre effektiviteten, kompetencen og fremme acceptabel brug af IT, som giver interessenter (forbruger, investorer og ansatte) tillid til organisationens it

[57] ISO/IEC 38500 side iv
[58] ISO/IEC 38500 side v
[59] ISO/IEC 38500 side v

ledelse. Derudover kan denne ISO bruges til at informere og guide direktørerne om hvilken retning it'en styres i, samt til at give virksomhedsledelsen et basis hvorpå de kan evaluere brugen af IT.[60]

Overensstemmelser i virksomheden

Det er vigtigt at virksomhedens it-anvendelse overholder den lovgivning og de regulativer, som er gældende i de forskellige brancher og lande som de opererer i. Virksomhedens direktører kan blive holdt ansvarlige for it-anvendelsen, såderfor bør ansvaret placeres korrekt, og ved brug af ISO38500 sikrer man at brud på lovgivningen formindskes. [61]

Performance i organisationen[62]

Ved en fornuftig håndtering af it, fra it-governance siden, skulle det gerne medføre at it'en tilfører virksomheden mere værdi og ISO 38500 skulle gerne kunne klargøre hvilke hensigter it kan skabe merværdi ved, overfor direktørerne, således der kan ske en forbedring af it'en, igennem;

- En korrekt implementering og brug af it
- Klarhed omkring ansvar og ansvarlighed for både brugen og levering af IT med henblik på opfyldelse af organisationens mål.
- At virksomheden drives kontinuerligt og bæredygtigt.
- Sammenhæng mellem it og virksomhedens behov
- At ressourcerne benyttes effektiv
- At organisationen er innovation inden for service, branche og forretning.
- Reducere omkostninger af it i organisationen samt at it investeringerne giver fordele.

2.4.1 Framework[63]

I ISO/IEC38500 er frameworket baseret på seks principper til at opnå god corporate governance i it. Det er muligt at tilføje disse principper til de fleste organisationer. De seks principper beskriver hvilket resultat som kan forventes, men ikke hvordan og hvornår eller hvem der skal implementere disse, da dette afhænger af den konkrete organisations naturlige principper. Det bør være direktionen som efterspørger at disse tilføjes organisationen.

[60] ISO/IEC 38500 side 1
[61] ISO/IEC 38500 side 2
[62] ISO/IEC 38500 side 2
[63] ISO/IEC 38500 side 6-8

Princip 1: Responsibility

Organisationen er bestående af individer og afdelinger, som bør acceptere og forstå deres ansvarsområder i forhold til udbud og efterspørgsel med hensyn til it. Dem som har ansvar for en given handling, har også beføjelserne til at udføre denne handling.

Princip 2: Strategy

Forretningsstrategien i virksomheden skal indregne nuværende samt fremtidige muligheder for IT, og den it-strategiske plan skal inkorporeres i forretningens strategi.

Princip 3: Acquisition

It-erhvervelser sker på baggrund af valide grunde, som er baseret på passende og løbende analyser, med klar og transparent beslutningstagning. Der er en passende balance mellem fordele, muligheder, omkostninger og risici, både langsigtet og kortsigtet.

Princip 4: Performance

Behovet for IT er at det skal understøtte organisationen ved at bidrage med serviceydelser, serviceniveau samt kvalitet, både til nuværende situation men også til fremtidige forretningsbehov.

Princip 5: Conformance

It skal stemme overens med gældende regulativer og love inde for IT samt der skal være definerede, implementerede og underbyggede politikker og praksis.

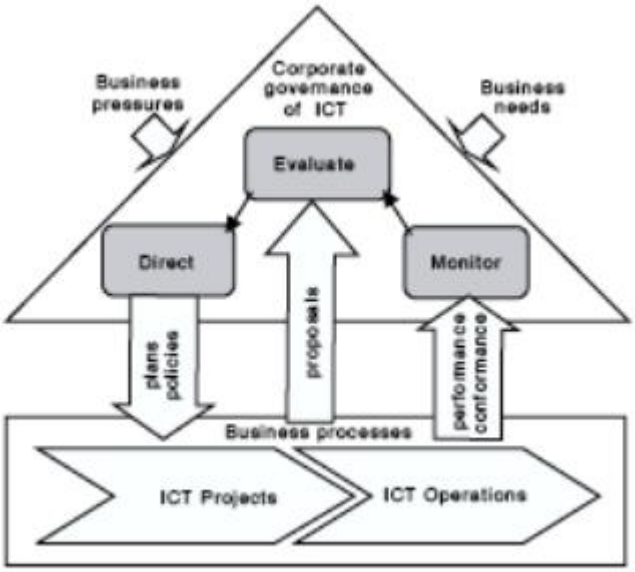
Princip 6: Human Behaviour

It-politikker, -praksisser og -beslutninger udviser respekt over for menneskelig ageren; dette inkluderer alle nuværende og fremtidige behov for de individer som er involveret i processen.

Model: *for Corporate Governance of IT*

Der er tre hovedopgaver som direktionen bør regulere ud fra, *Evalute, Direct* og *Monitoring.* Der skal ske en evaluering af den nuværende brug af IT samt den fremtidige brug, derudover skal der være udarbejdelser og implementerings planer og politikker, for at sikre den rette brug af it i forhold til forretningens målsætning og endelig skal det overvåges om der er overensstemmelse mellem planen, politikken og præstationerne.

Figur 12 – Model for Corporate Governance of IT



Kilde: ISO/IEC 38500 side 7

I figuren forklares det hvordan disse tre skaber en cyklus og nedenfor følger en forklaring af disse tre elementer og relationer som vist i figuren.

Evaluate:

Direktørerne bør evaluere og tage beslutninger om den nuværende samt den fremtidige brug af it, herunder strategi, kapacitet og leveringsaftaler, såvel internt som eksternt. Af de interne og eksterne faktorer, bør ledelsen overveje hvilket pres der ligges på organisationen, såsom teknologiens udvikling, økonomiske og sociale trends og om der kan være politisk indflydelse. Direktørerne bør lave løbende evaluering for at kunne tage hånd om problemer som er på vej og der skal også tages hensyn til nuværende og fremtidige målsætninger således man kan bibeholde eller få konkurrencemæssige fordele.

Direct:

Der skal ske en ansvarsfordeling fra direktørernes side og der skal være planer og politikker omkring forberedelse og implementeringen.

- Planer: Bør sætte retningslinjer op omkring investeringen i it-projekter og it-drift.
- Politik: Bør etablere en sund fornuft i brugen af it.

Det er direktionen som skal sikre at overgangen fra projekt til den faktiske drift sker på forsvarlig vis og er korrekt planlagt. Der skal her tages hensyn til hvordan dette påvirker den eksisterende

drift i organisationen, herunder it-systemerne og infrastrukturen.
Der bør fra direktionens side stilles krav til de daglige ledere om at give rettidig information samt om at overholde de seks principper for god it-ledelse. Hvis der opstår specifikke behov eller problemer skal disse indsendes til godkendelse hos direktionen.

Monitor:

Direktionen bør overvåge udførelsen og brugen af it, gennem passende målesystemer, for derved at konstatere om udviklingen forløber passende i henhold til de planer og politikker, som er vedtaget, således at projektet lever op til de forretningsmæssige målsætninger. Og hvis dette ikke lykkes er der mulighed for at kunne korrigere eller i værste tilfælde afvikle projektet.

2.4.2 Vejledning til it-ledelsen[64]

I det efterfølgende afsnit vil der være en generel vejledning i god it-governance i forhold til de seks principper som et forslag til hvordan det kan implementeres i praksis. Det er ikke fyldestgørende, men det er derimod tænkt som et oplæg til en diskussion af it-governance i direktionen centreret omkring de tre nøgle elementer i de seks principper. Det er op til den enkelte virksomhed at identificere hvilke handlinger der skal udføres for at implementering kan gennemføres, da det kommer an på organisationens opbygning og branche. Derudover anbefales det at lave en analyse af risiko og muligheder for it-anvendelsen. De følgende illustrationer vil det være muligt at tilføje de fleste virksomheder, men andre muligheder bør overvejes.

Princip 1 – Responsibility:[65]

Evaluate:

Direktionen skal evaluere hvilke mulige kandidater de har til et givent ansvarsområde i forhold til den nuværende og fremtidige situation i organisationens brug af it. Der skal her tages højde at der sikres en acceptabel, kompetent og effektiv udførelse og drift at it, i henhold til organisationen målsætning nu og i fremtiden.
Normalt bør det være mennesker som befinder sig på ledelsesniveau og som har kendskab til organisationens forretningsstrategi og målsætning, der bliver rådgivet af it specialister der ligeledes har forstand på forretningsværdier og processer.

[64] ISO/IEC 38500 side 9-15
[65] ISO/IEC 38500 side 9+10

Direct:

Direktionen bør sikre sig at planen bliver overholdt af dem som er blevet tildelt ansvar som har med it at gøre. Ligeledes er det vigtigt at direktionen modtager information nede fra, således at de kan leve op til deres ansvar.

Monitor:

Der bør ske en overvågning fra direktions side i forhold til om de forventede it-ledelsesmekanikker er etableret tilfredsstillende. Der bør også ske en overvågning af dem som har fået tildelt ansvar, for at sikre sig at de har forstået og anerkendt deres ansvarsområde. Til sidst bør der foregå en overvågning af den performance, hos dem der er blevet tildelt ansvar og om disse lever op til forventningerne.

Princip 2 – Strategy[66]

Evaluate:

Der bør ske en løbende evaluering af den teknologiske udvikling samt forretningsprocesserne, for at sikre sig at disse stadig understøtter hinanden og at it stadig vil understøtte de forretningsmæssige mål i fremtiden. Under overvejelserne omkring planer og politikker bør direktionen overvej it'ens aktiviteter og hvorledes disse kan forsætte med at understøtte de forretningsmæssige mål, ved skiftende omstændigheder. Ydermere skal det sikres at it-anvendelsen er underlagt en passende risikovurdering efter internationale og nationale standarder.

Direct:

Fra direktionens side bør der guides om tilrettelæggelsen og anvendelsen af planer og politikker sikre at organisationen benytte sig af den it-teknologiske udvikling. Ligeledes bør det tilskyndes at direktionen modtager innovative forslag til brug af it, som gør at organisationen kan reagere på nye muligheder eller udfordringer samt at de kan opstarte nye forretningsideer eller forbedringer af processer.

Monitor:

Der bør ske en overvågning, fra direktionens side, af de godkendte it-forslag så man sikrer sig at disse holder tidsrammen, overholder de allokerede ressourcer samt at de overholder de

[66] ISO/IEC 38500 side 11

forventede mål. Desuden bør der ske en overvågning med hensyn til om brugen af it lever op til det ønskede, således at det opfylder de tilsigtede fordele.

Princip 3 – Acquisition[67]

Evaluate:

Direktionen bør evaluere muligheder for at anvende it til at realisere godkendte forslag, balancere risikoer og værdisætte foreslåede investeringer.

Direct:

Direktionen bør vejlede, så it-aktiver (systemer og infrastruktur) kan erhverves på en hensigtsmæssig måde, herunder udarbejdelse af passende dokumentation, samtidig med at nødvendige kapaciteter er til rådighed. Derudover bør det sikres at leverandørers leveringer opfylder forretningens behov.

Monitor:

Direktionen bør overvåge it-investeringer for at sikre, at de giver de nødvendige kapaciteter, samt i hvilket omfang organisation og dens leverandører opretholder en fælles forståelse af organisationens hensigt med at erhverve it.

Princip 4 – Performance[68]

Evaluate:

Direktionen bør evaluere de muligheder, der foreslås af den daglige ledelse for at sikre at it vedvarende understøtter forretningsprocesser med de nødvendige muligheder og nødvendige kapacitet. Disse forslag skal imødegå den fortsatte normale drift i virksomheden samt behandle risikoen der er forbundet med brugen af IT. Direktionen skal tage stilling til deres riskovillighed i forhold til it-aktiviterne.
Direktionen bør evaluere risici forbundet med integriteten af deres informationer og beskyttelsen af it aktiverne, herunder associeret intellektuel ejendom og organisationens samlede historie.

Direktionen skal tage stilling til om mulighederne for at sikre effektivitet sker rettidige og beslutninger omkring it-anvendelsen i forbindelse med forretningens målsætning. Desuden skal der foretages løbende evaluering af effektiviteten og præstationen.

[67] ISO/IEC 38500 side 12
[68] ISO/IEC 38500 side 13

Direct:

Det er nødvendigt at direktionen tildeler tilstrækkelige ressourcer således at it kan opfylde de forretningsmæssige behov, det skal ske efter prioritering og pris. Ligeledes skal de ansvarlige for it "kontrolleres" så man sikrer sig at de overholder deres ansvar om at sikre at dataene er korrekte og opdaterede, samt at de er beskyttede mod tab eller misbrug.

Monitor:

Der skal være overvågning fra direktionens side, af om it understøtter virksomhedens behov, ressourcer, økonomi samt om politikkerne bliver overholdt f.eks. om dataene er præcise nok til at opretholde en effektiv brug af it.

Princip 5 – Conformance[69]

Evaluate:

Der skal ske en regelmæssig evaluering af om it overholder indgåede forpligtigelser (regulativer, lovgivning, basale love og kontrakter) samt interne politikker, standarder og frameworks. Derudover skal det evalueres om de interne bestemmelser overholdes i forhold til it-governance.

Direct:

Direktionen bør vejlede de ansvarlige til at etablere regelmæssige og rutine mekanismer som skal sikre, at anvendelsen af IT sker i overensstemmelse med de relevante forpligtelser (regulativer, lovgivning, basale love og kontrakter) samt interne politikker, standards og frameworks. At de etablerede politikker håndhæves har det formål at it opfylder de interne forpligtigelser samt at it-afdelingen overholder retningslinjerne med hensyn til professionalisme, udvikling og etiske retningslinjer.

Monitor:

Direktionen bør overvåge IT compliance og overholdelsen igennem en passende rapportering og revisionspraksis, som skal sikre at resultaterne er rettidig og af en så omfattende grad at de er egnet til evaluering, således at virksomheden stilles tilfreds.

[69] ISO/IEC 38500 side 14

Direktionen bør overvåge it aktiviteter, herunder disponeringen af aktiver og data, for at sikre sig at de overholder deres forpligtelser i forhold til miljø, privatliv, virksomhedens samlede historie og andre relevante punkter.

Princip 6 – Human Behaviour[70]

Evaluate:

Direktionen bør evaluere it-aktiviteterne for at sikre, at medarbejdernes adfærd er identificeret og tages i betragtning på passende vis.

Direct:

Direktionen bør tilpasse it-aktiviteterne således der er overensstemmelse med den identificeret medarbejders adfærd. Skulle der opstå uhensigtsmæssige risici, problemer, betænkeligheder eller muligheder skal disse identificeres og rapporteres til hver en tid. Denne risiko skal håndteres i overensstemmelse med de vedtagene politikker og procedurer og skal sendes videre til den rette beslutningstager.

Monitor:

Direktionen bør overåge it-aktiviteter for at sikre sig at den tidligere identificerede menneskelige adfærd fortsat er relevant og at den gives den korrekte opmærksomhed.
Der bør ske en overvågning fra direktionens side, for at sikre at arbejdspraksis og brug af it stemmer overens.

Kort resume:

Dette afsnit handler om at virksomheden ved korrekt indførsel af ISO 38500, giver de forskellige interessenter en tryghed om at virksomheden benytter it på forsvarlig vis. Denne tryghed skulle gerne resultere i at virksomheden har nemmere ved at tiltrække investorer osv., samt at virksomheden opnår en mere effektiv styring af it. Derudover baseres denne standard også meget på at det øverste ledelses niveau skal involveres, via seks principper som styrers efter tre elementer. Derfor vil it ikke stå som en ”stand alone” afdeling men i stedet blive inddraget i virksomhedens overordnede målsætning.

[70] ISO/IEC 38500 side 15

2.5 Opsummering af teori

Der er i dette afsnit blevet gennemgået fire teorier; COSO, COBIT 5, God it-skik og ISO 38500. Tre af disse går i hovedtræk ud på at involvere den øverste ledelse i it, og it ikke skal betragtes som værende en "sort boks". Den sidste, COSO, er et overordnet værktøj til hele virksomheden, som kan skabe en helhedsforståelse af virksomheden. Hvor COSO's interne kontroller er et styrende element til at sikre; overholdelse af lovgivning, risikostyring og en mulighed for at få informationer ud fra virksomhedens forskellige processer til brug for den øverste ledelse. Disse informationer bør således bruges i løbende udarbejdelse af forretningsstrategien og til videre analyse af risiko. Til dette kan COBIT 5, ISO 38500 og God it skik, så hjælpe med at få defineret forretningsstrategien i overensstemmelse med it praksis.

COSO kuben er et værktøj for ledelsen til at kunne håndtere, styre og kontrollere risikoen i selskabet via interne kontroller. Samt en hjælp til at kunne identificere risikoer i forbindelse med virksomheden. De 8 indbyrdes processer som udgør COSO er det ikke nødvendigt at skulle udføre i den nævnte rækkefølge.

COBIT 5 sikrer et samlet framework som skal hjælpe virksomheden med at opnå målsætningerne omkring governance og management af virksomhedens it. En optimal værdi fra it skabes ved at opretholde en balance imellem realiseringen af fordele, optimering af risikoniveauet og ressourceforbruget.

God it-skik har til formål at skulle hjælpe virksomhedens øverste ledelse med at få et overblik over de discipliner inden for it-området som de analyserer, beslutter og planlægger inden for, samt at implementerer og følge op den it-anvendelse der er i virksomheden i overensstemmelse med god it-skik.

ISO/IEC 38500's mål er at give ledelsesniveauet et framework med principper til at vurdere, lede og overvåge brugen af IT i virksomheden. Da de fleste virksomheder benytter sig af IT, som en stor del af driften og det i fremtiden vil spille en stor rolle, er det relevant at have fokus på hvordan man anvender dette effektiv. Denne standard skulle gerne give det højeste ledelsesniveau en forståelse for hvorfor IT er så vigtigt for virksomheden og af at IT-governance bør være et fokusområde.

Grunden til at jeg har valgt at benytte mig af disse forskellige ”teorier” er at der oftest benyttes mere end et framework i en organisation, da disse skal tilpasses efter virksomhedens behov og branche. Derfor har det været relevant at gennemgå flere. Da de i store træk har samme formål kan det dog være svært rent teoretisk at vurdere hvilket der er bedst. Der vil dog være fordele ved at anvende COBIT og ISO da disse befinder sig på et internationalt niveau, hvor imod god it skik hovedsagligt er tilpasset danske forhold (da den er på dansk). Det vil derfor være virksomhedernes behov som vil skulle afgøre hvilket af disse der skal benyttes som primært framework. Man kunne her forestille sig at mindre danske virksomheder med fordel kunne benytte sig af God it skik, idet den ikke er helt så ”tung” som f.eks. COBIT. Hvorimod større danske/internationale virksomheder med fordel ville kunne benytte sig af COBIT, da dette er internationalt anerkendt. I begge tilfælde ville ISO og COSO med fordel kunne anvendes.

Kap 3 - Empiri

Indledning

Det it-strategiske niveau i virksomheden har en voksende betydning for virksomhedens muligheder for at kunne realisere sine mål og visioner, derfor bliver det mere relevant for ledelsen at have fokus på it anvendelsen. Det handler for topledelsen om at forholde sig kritisk til virksomhedens it situation og strategi, både mangler/udfordringer, samt hvilke muligheder der kan skabes i forhold til virksomhedens problemstillinger omkring målsætning. Og her vil det blive forsøges belyst hvorledes dette forholder sig.

3.1 Rambøll it i praksis[71]

Metode og datagrundlag[72]

Det følgende afsnit er baseret på en undersøgelse lavet af Rambøll A/S i publikationen It – i praksis. Det datagrundlag og den metode som er benyttet der i, lyder som følger: Undersøgelsen er opdelt i to spørgeskemaer efterfølgende hinanden, til forskellige respondenter. Det første skema er sendt ud til 430 virksomheder, til den it-ansvarlige hvoraf der er en besvarelses procent på 42, svarende til 179 besvarelser. Dernæst er der udsendt et tilpasset og forkortet spørgeskema til de 179 virksomheders forretningsansvarlig, hvor der er en besvarelses procent på 42, svarende til 75 besvarelser.

De private virksomheder er opdelt i tre kategorier; fremstillingssektoren, handel og service samt den finansielle sektor. Besvarelserne er fordelt på de tre kategorier på følgende måde:

Fremstillingssektoren, der har i alt 47 virksomheder besvaret, hvilket svarer til 26 pct.
Handel og service, der har i alt 108 virksomheder besvaret, hvilket svarer til 60 pct.
Den finansielle sektor, der har i alt 24 virksomheder besvaret, hvilket svarer til 13 pct.

3.1.1 It-governance

Der er et øget pres fra bestyrelse, aktionærer og topledelse om at it-governance skal være et af de centrale komponenter i den strategiske planlægning af styringen af virksomheden. En effektiv styring af it-anvendelse og brug af it-ledelse har højere grad en større betydning for virksomheden

[71] Rambøll Management Consulting (2012); *It i Praksis 2012* – Side 67-70
[72] Rambøll Management Consulting (2012); *It i Praksis 2012* – Side 197-198

end hvad den ellers har haft tidligere, og dette vil formentlig ikke blive mindre relevant i fremtiden. Der er derfor flere og flere virksomheder som benytter it som et strategisk våben, men ved mangelfuld it-governance eller ved manglende overensstemmelse i virksomhedskulturen samt ved at it-governancens kompleksitet forøges bliver afstanden større og større mellem it og forretningen.
I virksomheden skal ledelsen sørge for at alle trækker i samme retning, således at it-potentialerne spreder sig på tværs af organisationens forskelligheder. Det er vigtigt at kunne identificere nye anvendelser af de digitale muligheder så tidligt i udviklingsfasen/forløbet som muligt – her skal der så træffes valg om hvilke ideer der skal forfølges. Derudover er det vigtigt at selve implementeringsdelen sker vellykket, dette gælder om det er it eller ej og derfor kræver det fokuseret styring samt en opmærksom ledelse. It-governance skal sørge for at der er klare definitioner af ansvaret for ressourcetildeling og gevinstrealisering – og sikre det understøtter styringsstrukturen.

Ifølge It i praksis 2012, kræves det at virksomheden har øget modenhed på tværs af it-forretningen, før denne kan benyttes som et konkurrence parameter / differentiator. Det potentiale der er ved it, vil variere fra branche til branche, hvor det f.eks. i produktion/industrien oftest vil være robotter samt styrings- og dataopsamlingssystemer og produktionskontrolsystemer.

Dette er vigtigt for at virksomheden kan effektivisere sig, indsamling af data kan analyseres med henblik på at kunne få en mere effektiv arbejdslinje og der vil kunne opnås en mere præcis styring, fx ved at så vidt muligt undgå at der opstår flaskehalse.

Et andet eksempel kan være i den finansielle sektor, med indførelsen af netbank (front-office processer). Her kan mange af transaktionerne mv. fortages af bankens kunders hjemmefra – dette vil medføre at antallet af bankens personlige betjeninger kan mindskes drastisk. Dette vil kun blive forøget i den nærmere fremtid, da flere af de ældre enten begynder at benytte sig af disse muligheder eller denne del af befolkningen mindskes. Derfor vil mange af de ansatte i banken enten kunne spares væk, eller kunne udføre andre opgaver som kan være resultatgivende.

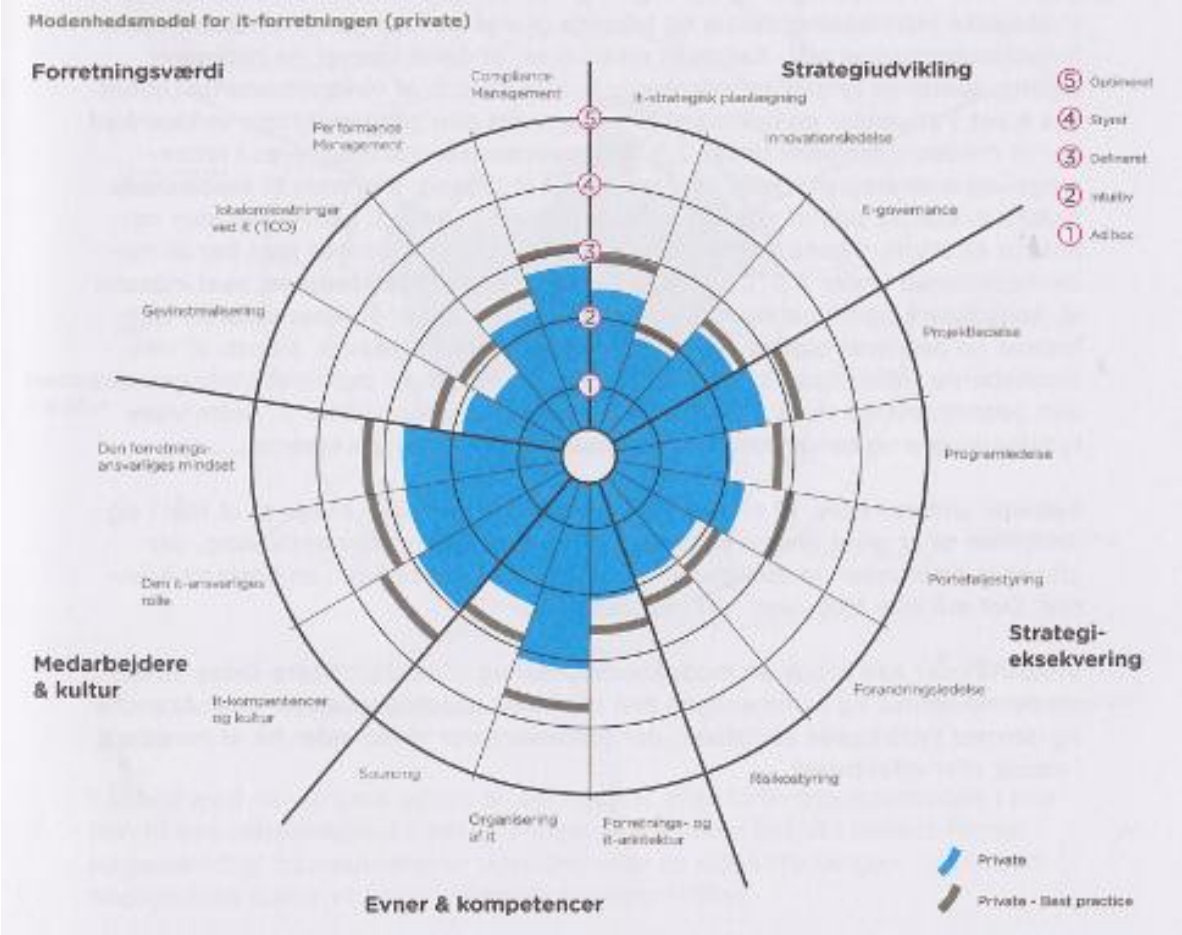
Modenhed.

Som nævnt tidligere nævnt spiller virksomhedens modenhed en væsentlig faktor i forbindelse med

at kunne bruge it som et konkurrence parameter.

I it praksis er der fortaget en ”benchmark” af private virksomheders it-forretning på 18 forskellige områder inddelt i fem kategorier, som det ses her under.

Figur 13 - Modenhedsmodel for it-forretningen (privat)



Kilde: Rambøll Management Consulting (2012); It i Praksis 2012 – Side 69

Det blå i den ovenstående figur er private virksomheder, hvor det grå er ”best practice virksomheder” som er defineret som dem af de 25 pct. med det bedste resultat. Denne modenhedsvurdering kan benyttes til at identificere tydelig afvigelser op til best in practice, således det kan ses hvor virksomheden med fordel kan investere eller effektivisere. Ifølge it i praksis er det nødvendigt at virksomheden fokuserer på kategorien ”Strategiudvikling” med områderne; it-strategisk planlægning, it-governance og innovationsledelse.

Det man se ud af den overstående figur er at der på langt størstedelen af de 18 områder, er en betragtelig forskel fra de bedste og ned til gennemsnitten, men på to ud af de tre, som er relevant

med it forretningen som konkurrence parameter, er forskellen ikke så stor, det er kun it-strategisk planlægning. Alle tre ligger dog under modenhedsniveau tre.

It-strategisk planlægning:

Den it-strategiske planlægning skal integreres i virksomhedens overordnede strategiske planlægningscyklus, erfaringer siger at der til dette kræves et modenhedsniveau svarende til 5, hvilket kun 15 pct. af virksomhederne opfylder, gennemsnittet ligger på under 2,5 på modenhed.[73]

It-governance:

It-governance skal integreres i forretnings- og it-strategien, hvilket kræver et modenhedsniveau svarende til 4. Dette er der kun 22 pct. af virksomhederne som lever op til, gennemsnittet her er ligeledes under 2,5 på modenhed.[74]

Innovationsledelse:

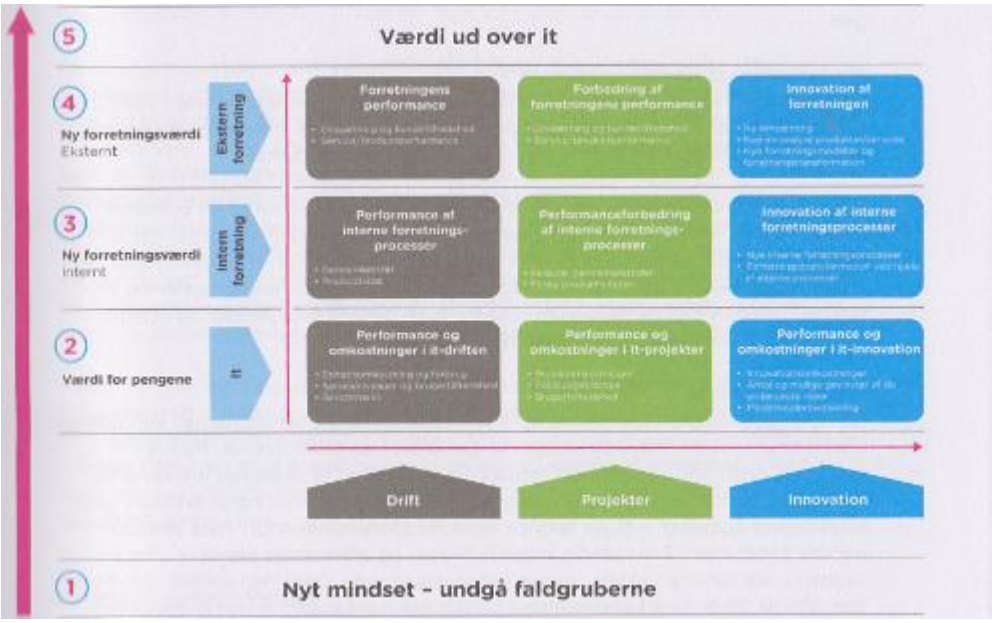
Innovationsledelse skal der indsamle og konsolidere inputs fra medarbejdere, kunder og leverandører. Dette kræver et modenhedsniveau på 3. Kun 19 pct. af virksomhederne lever op til dette og gennemsnittet befinder sig på under 2.[75]

3.1.1.1 Modenhedsmodel

Det er en femtrins modenhedsmodel, hvor der startes i bunden og arbejdes opad. Det er ikke muligt at springe nogen trin over.[76]

[73] Rambøll Management Consulting (2012); *It i Praksis 2012* – Side 70
[74] Rambøll Management Consulting (2012); *It i Praksis 2012* – Side 70
[75] Rambøll Management Consulting (2012); *It i Praksis 2012* – Side 70
[76] Rambøll Management Consulting (2012); *It i Praksis 2012* – Side 14

Figur 14 - Værdi ud over it



Kilde: Rambøll Management Consulting (2012); It i Praksis 2012 – Side 15

Nyt "mindset" – undgå faldgruberne.

CIOen skal sikre at it-organisationens "mindset" er at have fokus på forretningen og at alle forstår at forretningen er omdrejningspunkt, derudover er det it-organisationen som leverer bedre performance til forretningen. Der skal nedbrydes barrier i forhold til at it-organisationen ikke ses som en "selvstændig" afdeling som har forretningen som kunder. Dette er en faldgrube som skal brydes, ved at bryde gamle vaner og tænke nyt.[77]

Værdi for pengene

Her skal it-organisationen demonstrere at der skabes værdi for pengene, ved at rapporter omkring performance i it-driften, hvor omkostninger kobles sammen med kvalitet og services. Det er vigtigt at disse informationer kommunikeres med de rette interessenter, topledelsen, ledere af forretningsenhederne og forretningens procesejere. Det er her relevant at it-organisationen formår at rapportere de nødvendige oplysninger, fx ikke tekniske målinger, men hvordan it-performancen bidrager til forretningens performance, gevinster og resultater.[78]

Ny forretningsværdi – internt

Efter at CIOen har bevist at it-organisationens evner kører fornuftigt, er det på tide at tage næste

[77] Rambøll Management Consulting (2012); *It i Praksis 2012* – Side 14
[78] Rambøll Management Consulting (2012); *It i Praksis 2012* – Side 14+15

skridt op i modellen; at skabe ny forretningsværdi internt i organisationen. Dette kan gøres ved at forbedre interne processer samt ved løbende at kommunikere de opnåede resultater til de rette forretnings processejere, desuden skal der også ske henvendelse til virksomhedens topledelse og ledere af forretningsenheder. Det er vigtigt at målrette den konkrete information til modtagerne.[79]

Ny forretningsværdi – eksternt

I dette trin skal it-organisationen kommunikere den forretningsmæssige værdiforøgelse, der er skabt i forrige trin, f.eks. ved at der er øget omsætning, kundetilfredshed eller ved at komme med nye it-baserede produkter. De primære interessenter er topledelsen og ledere af forretningsenhederne, som har behov for at få informationen om den værdi som skabes af it-organisationen ud af til (eksternt). Derudover er det vigtigt at gøre forretningsenhedernes ledergrupper opmærksom på at it-organisationen forbedrer netop deres forretningsområde.[80]

Værdi ud over it

Sidste trin på modellen, efter it organisationen har vist den forbedrede performance, handler her om at genere værdi ud over it.[81]

På denne måde opbygger it-organisationen tilliden til resten af organisationen. Denne model bygger på at der er tre målepunkter for henholdsvis trin 2-4, fordelt på drift, projekter og innovation, og det er her relevant at it-organisationen benytter sig af de målepunkter som er relevante i forhold til forretningens mål.[82]

3.1.1.2 Hvordan CIO kan styre diskussionen om it-værdiskabelsen over for forretningen [83]

Det er her vigtigt at CIO tager ansvar for at styre diskussion om it-værdiskabelse. Til dette er der behov for en rapporteringsmodel, med henblik på forretningens interessenter. Modellen fra det forrige afsnit kan her anvendes som grundlag for møderne med topledelsen. CIOen kan benytte sig af følgende firepunkts rapporteringsmodel til mødets agenda.

[79] Rambøll Management Consulting (2012); *It i Praksis 2012* – Side 15-16
[80] Rambøll Management Consulting (2012); *It i Praksis 2012* – Side 16
[81] Rambøll Management Consulting (2012); *It i Praksis 2012* – Side 16
[82] Rambøll Management Consulting (2012); *It i Praksis 2012* – Side 14
[83] Rambøll Management Consulting (2012); *It i Praksis 2012* – Side 76-77

1. *Its bidrag til de vigtigste forretningsstrategiske initiativer og målsætninger*
2. *Its bidrag til forretningens løbende performance og performance i forretningsprocesser*
3. *It-forbedringer*
4. *Sikre fremdrift og support*

Disse fire punkter er specificeret yderligere i bilag 2.

Delkonklusion

Så dette kan bruges af virksomheden til at identificere hvor det kan være nødvendigt at udvikle sig, således virksomheden opnår en højere konkurrence dygtighed, da en virksomhed helst skal undgå at stagnere er det vigtigt der løbende sker en analyse af virksomhedens situation og det er i høj grad i den it-strategiske planlægning at der kan findes plads til forbedringer.

3.1.2 Forretnings- og it-arkitektur[84]

Når virksomheden udvikler forretning og it i fællesskab, kan det give virksomheden en konkurrencemæssig fordel. Men for at dette kan benyttes, vil det ofte kræve at der skal ske en ændring af arbejdskulturen, hvor forankringen i virksomheden ofte er således at handlen og afslutningen af forretningsudviklingen sker inden it-afdelingen bliver involveret.

De fem niveauer af modenhed inden for forretnings- og it-arkitektur består af: (1 det laveste og 5 det højeste)

1. ***Ad hoc** – Der er ingen opmærksomhed på forretnings- og it-arkitektur i organisationen, eller der er opmærksomhed på behovet for en sammenhængende forretnings- og it-arkitektur, der dækker forretningsprocesser, data, applikationer og infrastruktur*
2. ***Intuitiv** - Processer for arbejdet med forretnings- og it-arkitektur opstår, men de er uformelle og intuitive og har fokus på aktuelle behov*
3. ***Defineret** - Vigtigheden af forretnings- og it-arkitektur er bredt accepteret, og teknikker og metoder er standardiserede, fx identifikation af hvilke forretningsmæssige evner der er kritiske*
4. ***Styret** - Udviklingen og håndhævelsen af forretnings- og it-arkitekturen understøttes fuldt ud af formelle metoder og teknikker*

[84] Rambøll Management Consulting (2012); *It i Praksis 2012* – Side 113-119

5. ***Optimeret*** *- Forretnings- og it-arkitekturen håndhæves konsistent på alle niveauer, forbedres løbende og best practice identificeres og implementeres*[85]

Man kan se punkt 1 og 2 som værende de mest kritiske og der hvor det er væsentligst at sætte fokus på. Punkt 3 befinder sig på et acceptabelt niveau og ved punkt 4 og 5 befinder virksomheden sig i den ende hvor det i forhold til min problemformulering ikke har den store interesse, men dog er det relevant at forblive i det høje modenhedsniveau**.** Dette underbygges af it-praksis hvor der bliver nævnt at des højere modenhed en virksomhed har des bedre vil denne præstere og at få modenheden op på niveau 3 gør en forskel fra 1 og 2.

Den udvikling der er sket inden for modenhed af forretnings- og it-arkitekturen er begrænset fra 2011 til 2012, men det er iøjnefaldende at 69 pct. (1=33 pct. og 2=36 pct.) af virksomhederne befinder sig så lavt nede som det er tilfældet.[86] Ud fra dette kan man konkludere, at det er et stort behov for virksomhederne i bunden at de får sat fokus på hvorledes disse kan avancere op i modenhed.

Men for at der kan ske en ændring kræver det en dedikeret ledelsesindsats for at få lavet en ændring i holdning og kultur, hvilket tager tid. Virksomheder der holder fast i den traditionelle metode, mht. at udvikle og beskrive forretningsmodeller samt at effektivisere først, hvorefter de inddrager it, om end det er internt eller eksternt i forløbet, r vil som ofte sakke bagud, i forhold til deres konkurrenter. Det skyldes at it-ydelser i dag spiller en stor rolle i alle dele af virksomheden.[87] Ifølge it i praksis, er der ligeledes ikke nogen fællesforståelse mellem CEO(Cheif Executive Officer) og CIO (*Cheif Information Officer*) af behovet for en større modenhed og at se it som værende et strategisk aktiv eller en måde at have indflydelse på forretningsstrategi og mål i virksomheden. Her er der 54 pct. af CEO som mener dette bør have indflydelse, hvor i mod at kun 24 pct. af CIO oplever at topledelsen har denne holdning.[88]

Forretningsevner:

Definitionen af forretningsevner er en kombination af de kompetencer som medarbejderne giver og de teknologiske evner eller kapaciteter, som bruges i forbindelse med at udføre forretningens

[85] Rambøll Management Consulting (2012); *It i Praksis 2012* – Side 113
[86] Rambøll Management Consulting (2012); *It i Praksis 2012* – Side 113
[87] Rambøll Management Consulting (2012); *It i Praksis 2012* – Side 115
[88] Rambøll Management Consulting (2012); *It i Praksis 2012* – Side 115+116

aktiviteter. Dette udtryk er måden på hvordan virksomheden forener dens domæneviden, processer, personer, teknologi og strukturer til at give kunden værdi.[89] Denne forretningsevne er ifølge IT i praksis at mere end halvdelen(54 pct.) af virksomhederne er opmærksomme på at have dette defineret hvor 19 pct. ud af de 54 pct. bruger dette systematisk.[90]
Forretningsevnen kan anvendes på alle tre niveauer i organisationen, hvor det fx handler om at få medarbejdernes kompetencer kombineret med it, såsom it-investering, således at dette kan bidrage til virksomheden med en øget konkurrenceevne samt effektivitet.[91]

Kritiske forretningsevner:
Der er her tale om virksomhedens evne til at kunne adskille sig fra deres konkurrenter således at muligheden for at opnå succes forøges og derved kan dette spille en afgørende faktor for opnåelsen af virksomhedens vision/mål. Ved at virksomheden identificerer de kritiske forretningsevner, kan der sørges for at investeringer kanaliseres hen hvor disse fremmer virksomhedens mål bedst. Dette gør sig ligeledes gældende for it-investeringer, så der kan ske en prioritering af hvilke investeringer der er mest relevante, samt der kan ske en udvikling af medarbejdernes kompetencer i forhold til det ønskede mål. Kritiske forretningsevnen befinder sig ofte hos de ledere som har succes, men som tavs viden karakteriseret som erfaringer og mavefornemmelser.[92]

[89] Rambøll Management Consulting (2012); *It i Praksis 2012* – Side 118
[90] Rambøll Management Consulting (2012); *It i Praksis 2012* – Side 117
[91] Rambøll Management Consulting (2012); *It i Praksis 2012* – Side 118
[92] Rambøll Management Consulting (2012); *It i Praksis 2012* – Side 118

Delkonklusion.

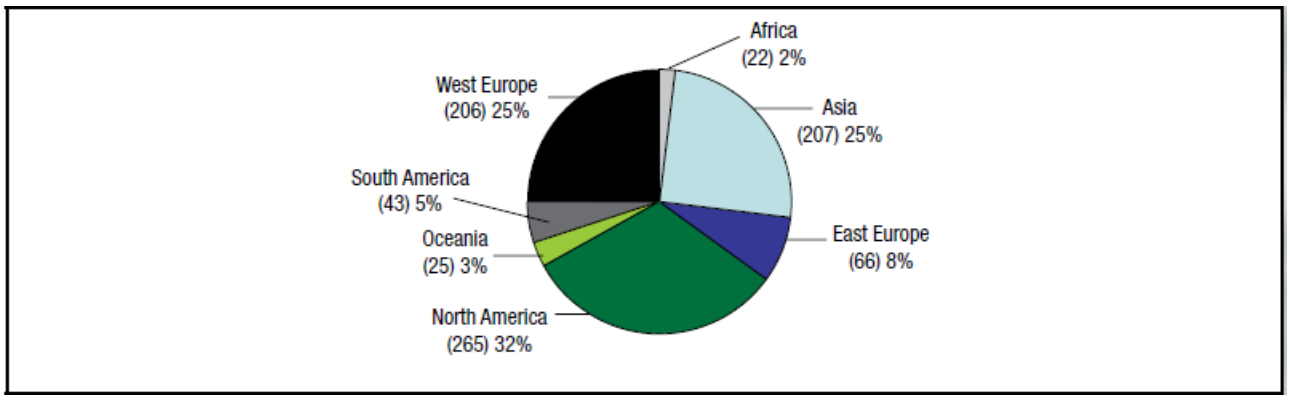
En væsentlig faktor som man kan se som et stort problem for mange virksomheder er at der er en mangelfuld kommunikation mellem topledelsen og it-ledelsen/mellemlederniveauet, som skaber en mangelfuld integration af it-anvendelsen i selve forretningsstrategien.

At udnytte den forretningsevne virksomheden besidder og især den kritiske, kan man anse som værende en altafgørende faktor for at virksomheden opnår succes, denne ses desværre ofte som en tavs viden hos de ledere som har succes (erfaring og mavefornemmelser). Men ved dette sker der en begrænsning, da lederne kun kan anvende dette på vedkommendes eget ansvarsområde, så dette vil medføre at den viden kun bliver udnyttet begrænset. Derfor er det vigtigt at sørge for denne viden kan blive tilgængelig for virksomheden som helhed, således at andre områder (anden ekspertise) kan understøtte samme ide, dette kunne være it-services og -systemer (eller anden teknologi). Forretningsevner er de almindelig færdigheder i branchen hvor de kritiske er det redskab og den viden som skal sikre virksomheden en fordel frem for andre virksomheder.

3.2 Global Status Report on the Governance of Enterprise IT (GEIT) – 2011

Denne rapport er lavet på bases af 834, der har besvaret på et spørgeskema, hvor der er en fordeling på 450 it ansvarlige *(CIO og IT managers)* og 384 af forretningsleder *(CEOs, CFOs, COOs, managing directors [MDs] or equivalent).*[93] Respondenterne er fordelt på verdensbasis, som ses her under.

Figur 15 – Geographic Distribution of Respondents.



Kilde IT Governance Institute (2011); *Global Status Report on the Governance of Enterprise IT (GEIT) side 65*

3.2.1 Vigtigheden mellem it og organisationen for at opnå strategi og vision i virksomheden

Det ses tydeligt af denne rapport, at virksomhederne anser IT som et vigtigt element i at opnå forretningsstrategien og visionen, hele 94 pct. af besvarelserne. Derved kan man se hvor vigtigt IT er for en virksomhed, men dog ikke nødvendigvis i anvendelsen som en decideret konkurrence parameter.

Figur 16 - Vigtigheden mellem it og organisationen for at opnå strategi og vision

Tal er i pct.	IT-ledelse	Forretningsledelse
Meget vigtig	54	49,7
Vigtig	40,7	43,2

Kilde: egen tilvikring på basis fra IT Governance Institute (2011); (GEIT) side 12

[93] GEIT side 65

Der kan her ses at der i høj grad er en fællesforståelse mellem it-ledelsen og forretningsledelsen om vigtigheden af it, som det ses i ovenstående figur. Dette er relevant i forbindelse med at skulle anvende dette som konkurrenceparameter samt at indføre en form for framework.

Figur 17 - *Perceptions of Business and IT stakeholders on the Contribution of IT to Business*

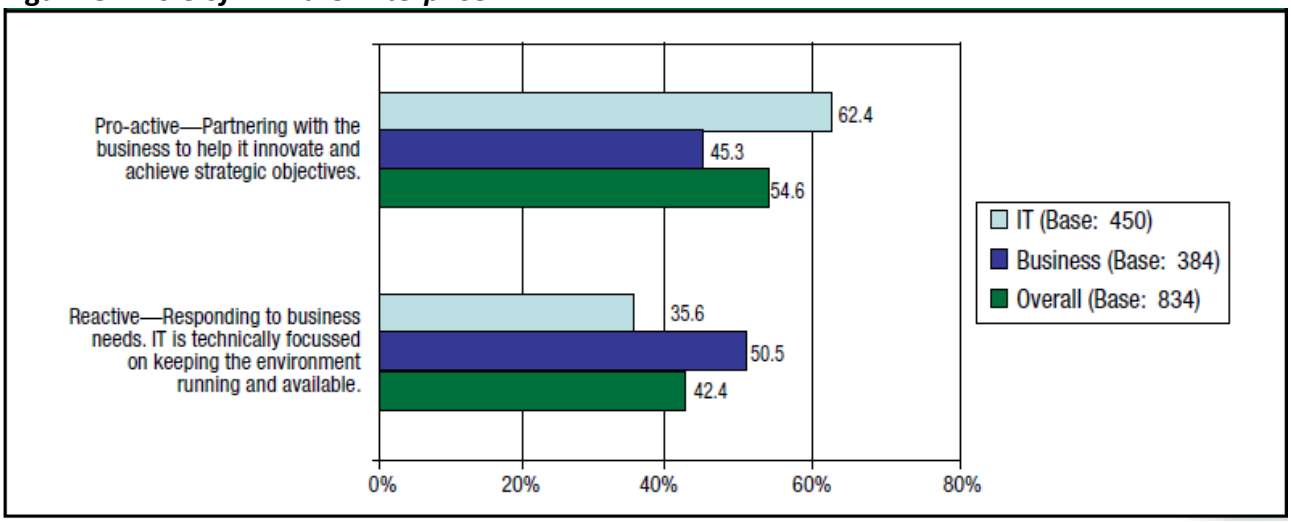
Contribution of IT to the Business	Percent of Business Respondents	Percent of IT Respondents
IT investments create value for the business.	87.8	92.4
IT service levels meet the business needs.	70.0	83.5
IT supports the business strategy.	71.7	89.5
IT enables rapid business change.	80.8	77.1
IT supports business regulation and compliance.	77.1	82.4

Kilde: IT Governance Institute (2011); Global Status Report on the Governance of Enterprise IT (GEIT) side 14

Som det fremgår af ovenstående figur er it-ledelsen langt hen ad vejen mere positiv omkring hvor meget it tilfører til forretningen, end omvendt. Der er dog meget iøjnefaldende at forskellen på hvor meget it-ledelsen og forretningsledelsen ser at "*IT supports the business strategy*", er på knap 28 pct. Dette kunne tyde på at der er opstået et kommunikationsproblem omkring hvad forretningsstrategien helt konkret er.

3.2.2 Hvilken rolle spiller IT i organisationen

Figur 18 – *Role of IT In the Enterprise*



Kilde: IT Governance Institute (2011); Global Status Report on the Governance of Enterprise IT (GEIT) side 17

Her spørges der ind til hvorvidt it er med til at skabe innovation i forretningen eller om denne bare anses for at skulle varetage drift og holde services kørende. Her vises det i ovenstående figur at

der er tydelig forskel i opfattelsen af hvad its rolle er i virksomheden. 62,4 pct. af it-ledelsen mener at den er med til at udvikle forretningens mål, hvor kun 45,3 pct. i forretningsledelsen mener dette. Der vil her være muligheder for at skabe forbedringer i virksomheden, ved at øge kommunikationen.[94]
Dette ville kunne ske igennem et framework, som kunne være COBIT, ved korrekt anvendelse af enablers, for at sikre at it kommer til at spille en større rolle i virksomheden.

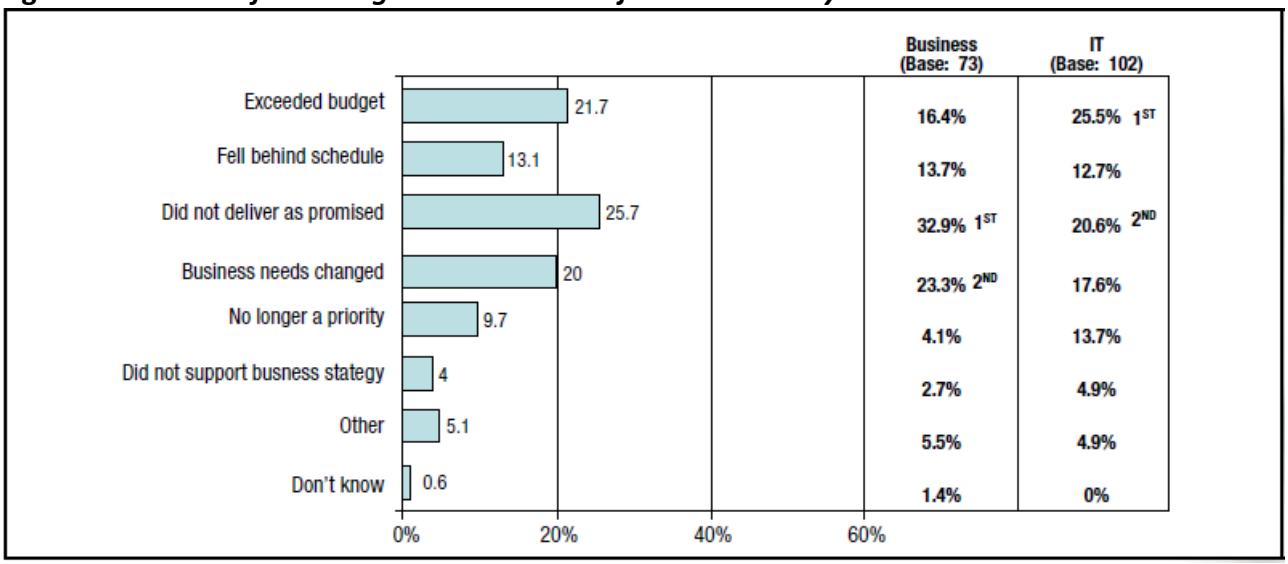
3.2.3 Hvorfor stoppes et projekt før tid?

Det viser sig, at 1 ud af 5 af de adspurgte har måtte afslutte et it-relateret projekt, før det er blevet fuldt implementeret. Det viser dog kun de projektet som er blevet afsluttet og ikke de projekter som det kunne have været oplagt at afslutte før tid.[95]

Som det ses fra nedenstående figur, er der tre hovedårsager til at virksomheden stopper projekterne før tid. Det første er at ”resultatet som aftalt opnås ikke”, det andet er at projektet ”overstiger det forventede budget” og det sidste er at ”forretningen har ændret behov”.[96]
Dette kunne tyde på at der i høj grad er opstået en forventningskløft mellem IT-ledelsen og forretningsledelsen, som giver udslag i fejl-projekter og spild af penge.
Det underbygges af nedenstående figur, som viser at der en tydelig forskel i hvad forretningen ser som årsagen og hvad IT ser som årsagen. IT har ”overstiger det forventede budget” som den største grund, hvor forretningen kun anser dette som tredje højeste grund. Til gengæld er det klart at forretningen ser ”resultatet som aftalt opnås ikke” som den væsentlige årsag, hvor IT har dette som anden højeste grund.

[94] IT Governance Institute (2011); *Global Status Report on the Governance of Enterprise IT (GEIT)* *side 16*
[95] IT Governance Institute (2011); *Global Status Report on the Governance of Enterprise IT (GEIT)* *side 20*
[96] IT Governance Institute (2011); *Global Status Report on the Governance of Enterprise IT (GEIT)* *side 20*

Figur 19 – *Reasons for Ending an IT-related Project Prematurely*



Kilde: IT Governance Institute (2011); Global Status Report on the Governance of Enterprise IT (GEIT) side 21

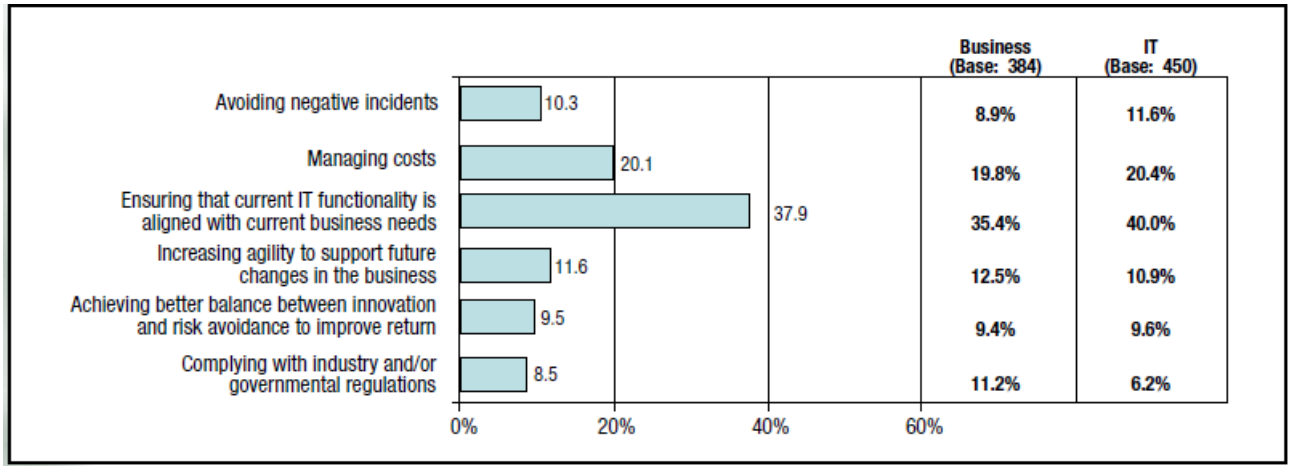
3.2.4 Hvad skal være drivkraften(drivers) bag it-aktiviteter?

Her er der blevet spurgt ind til hvad henholdsvis it-ledelsen og forretningsledelsen mener skal være den primære drivkraft bag it-aktiviteter, som det ses i nedenstående figur. Der er forholdsvis enighed omkring at det er at "forsikre at de nuværende funktioner understøtter de nuværende forretningsbehov" samt "at formindske omkostninger", som er de to vigtigste grunde. Hvor sådanne som "it skal forøge fleksibiliteten og understøtte virksomhedens forretningsændringer i fremtiden" ligger nummer tre og tæt derpå er "undgåelse af negative hændelser".[97]

Her kunne det tyde på at man ikke opfatter it-governance som værende en stor medspiller i at udvikle virksomhedens strategi, men at den kun skal understøtte den strategi som er/bliver valgt.

[97] IT Governance Institute (2011); *Global Status Report on the Governance of Enterprise IT (GEIT)* *side 21+22*

Figur 19 – *Drivers for GEIT Activites*



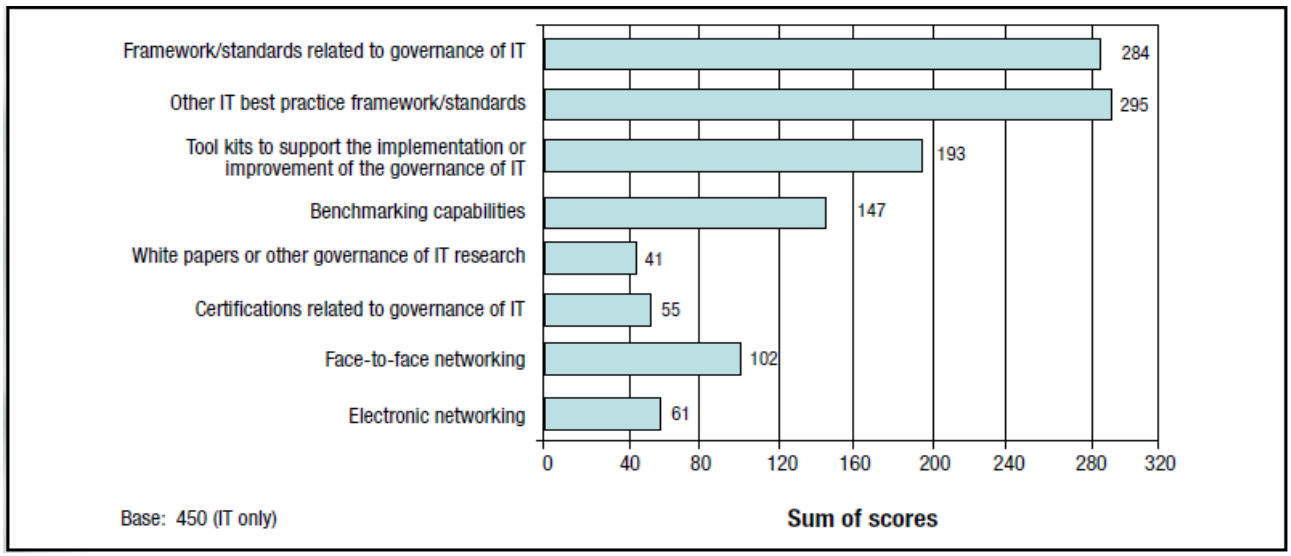
Kilde IT Governance Institute (2011); Global Status Report on the Governance of Enterprise IT (GEIT) side 22

3.2.5 Hvilke enablers skal der til for at skabe en effektiv it-ledelse?

Her er it-lederne blive bedt om at vælge hvilke to enablers der ses som værende de vigtigste for at skabe en effektiv it-ledelse? Resultatet er ganske enslydende at frameworks/standards som har vist sig at være bedst i praksis (f.eks. ITIL), er minimalt foran frameworks/standards med henblik på it-governance (f.eks. COBIT og ISO38500). Se figur nedenfor.[98]

Det skal lige nævnes at denne undersøgelse bygger på anvendelsen af COBIT 4.1.[99]

Figur 20 – *GEIT Enablers*



Kilde: IT Governance Institute (2011); Global Status Report on the Governance of Enterprise IT (GEIT) side 24

[98] IT Governance Institute (2011); *Global Status Report on the Governance of Enterprise IT (GEIT) side 24*
[99] IT Governance Institute (2011); *Global Status Report on the Governance of Enterprise IT (GEIT) side 8*

Overstående figur vises der at der er stor kendskab til hvilke metoder der kan anvendes for at opnå en forbedringen af anvendelsen af it. Sammenholdt med det øvrige statistik her i opgaven, kunne det tyde på at it-ledelsen har svært ved at få kommunikeret op til bestyrelsen.

Delkonklusion:

Der ses et klart billede af at it, både for it-ledelse og forretningsledelse, er vigtigt for at opfylde virksomhedens strategi, men at det ikke er ensbetydende med at it er en del af strategien. Statistikken viser et billede af at der er uoverensstemmelser med it's rolle i virksomheden som langt hen af vejen skyldes en manglende kommunikation. Denne kommunikation kan langt hen af vejen sikres igennem indførelsen af frameworks, standarder og/eller metoder.
Det at virksomhedens it-ledelse skal deltage i udviklingen af forretningsstrategien, er ikke hyppigt anvendt, men derimod bruges det at den skal understøtte virksomhedens strategi og være med til at omkostningsminimere.

3.3 Opsummering:

En væsentlig faktor som man kan se som et stort problem for mange virksomheder er at der er en mangelfuld kommunikation mellem topledelsen og it-ledelsen/mellemlederniveauet, som skaber en mangelfuld integration af it-anvendelsen i selve forretningsstrategien.
At udnytte den forretningsevne virksomheden besidder og især den kritiske, kan man anse som værende en altafgørende faktor for at virksomheden opnår succes, denne ses desværre ofte som en tavs viden hos de ledere som har succes (erfaring og mavefornemmelser). Men ved dette sker der en begrænsning, da lederne kun kan anvende dette på vedkommendes eget ansvarsområde, så dette vil medføre at den viden kun bliver udnyttet begrænset. Derfor er det vigtigt at sørge for denne viden kan blive tilgængelig for virksomheden som helhed, således at andre områder (anden ekspertise) kan understøtte samme ide, dette kunne være it-services og -systemer (eller anden teknologi). Forretningsevner er de almindelig færdigheder i branchen hvor de kritiske er det redskab og den viden som skal sikre virksomheden en fordel frem for andre virksomheder.

Der ses et klart billede af at it, både for it-ledelse og forretningsledelse, er vigtigt for at opfylde virksomhedens strategi, men at det ikke er ensbetydende med at it er en del af strategien. Statistikken viser et billede af at der er uoverensstemmelser med it's rolle i virksomheden som langt hen af vejen skyldes en manglende kommunikation. Denne kommunikation kan langt hen af vejen sikres igennem indførelsen af frameworks, standarder og/eller metoder.
Det at virksomhedens it-ledelse skal deltage i udviklingen af forretningsstrategien, er ikke hyppigt anvendt, men derimod bruges det at den skal understøtte virksomhedens strategi og være med til at omkostningsminimere.

Kap 4 - Teori og Empiri sammenholdt

I mit empiri afsnit er jeg kommet frem til at it er en kompleks størrelse at beskæftige sig med og denne kompleksitet forventes ikke at blive mindre i fremtiden, så derfor bliver det mere og mere relevant at virksomhederne benytter sig af metoder til at kunne strukturer it-anvendelsen. Til dette findes der flere metoder, guidelines, frameworks og dets lige. Som udgangspunkt bør virksomhederne ikke kun benytte sig af én enkelt af disse, men i stedet gerne en kombination af flere forskellige. Som et overordnet værktøj kan COSO anvendes på organisationens samtlige afdelinger og niveauer, dette giver de fordele, 1) indsamle data fra alle afdelinger, som kan krydsrefereres mellem hinanden, 2) bedre kontrol over risiko, 3) mulighed for at reagere nu, end kun på "status"tidspunket.

Rambøll it i praksis 2012

I undersøgelsen fra Rambøll, it i praksis 2012, er der foretaget en modenhedsanalyse hvor det viser sig at *it-strategisk planlægning* er det område hvor der er den største afstand fra den gennemsnitlige virksomhed også op til de bedste og det er ligeledes her erfaringerne siger at et modenhedsniveau på 5 er påkrævet.
Til at opnå dette kunne virksomhederne benytte sig af tilgangen i COBIT 5, *Process capability model* eller modellen som er belyst i *it i praksis 2012.* Disse kunne ligeledes understøttes af principperne i *ISO/IEC* 38500.

Evner og kompetencer er et væsentligt element for at it'en kan udvikle sig, så man kan opnå en konkurrence fordel. Dette skulle de forskellige teorier der er blevet belyst her igennem gerne kunne hjælpe på vej med, for at opnå et bedre resultat. Det er således i Danmark, at 69 pct. af virksomhederne befinder sig på de to laveste niveauer, i modenhed. Det ønskede niveau er omkring de fire, før der er de nødvendige ressourcer til at udvikle og styre forretnings- og it-arkitekturen.

Forretningsevner består i at kombinere de teknologiske evner/kapaciteter og medarbejdernes kompetencer til at bruge forretningens aktiviteter. Her er der 19 pct. af virksomhederne som har en defineret tilgang og anvender dette systematisk hvor yderlig 35 pct. har det defineret. Her kan man tolke det således at der en mangel på kommunikation i virksomheden, samt manglende muligheder for at indsamle brugbart data. Det vil her være relevant at benytte sig af metoder til at

sætte organisationen i faste rammer, således at det er muligt for den øverste ledelse at indsamle de korrekte og nødvendige data, så det er muligt at træffe beslutninger på et solidt grundlag og styre virksomheden i den rigtig retning.

GEIT

94 pct.[100] af de adspurgte i - *Global Status Report on the Governance of Enterprise IT* - anser it som værende et vigtigt eller meget vigtigt element i muligheden for at opnå strategien og visionen i virksomheden. Derfor er det vigtigt at it-ressourcerne bliver udnyttet til fulde, og til dette er det yderst relevant at få indført metoder til at håndtere og strukturere it-governance. It-lederne har en tendens til at se dem selv som værende mere pro-aktive end hvad topledelsen ser dem som værende.[101] Man kunne forestille sig at årsagen hertil er at rolleopfattelens mellem de to, ikke stemmer over ens. Dette kunne man blandt andet anvende et framework/standard til at rette op på, således der kommer en struktureret kommunikation så man kan opnå et fælles informationsniveau.

På internationalt plan stoppes et ud af fem it-relaterede projekter før tid[102], de tre væsentligste grunde til dette er, samlet set af it-ledelse og forretningsledelse, at: 1) projektet lever ikke op til forventningerne[103], 2) projektet overskrider budgettet[104], 3) forretningen har ændret behov[105]. Som jeg ser der kan der være to årsager til dette; 1. Der er i mange virksomheder indført et projektstyringsværktøj, hvilket evt. kunne være COSO, med dens interne kontroller og overvågning, eller et framework/standard ala COBIT 5/ISO/IEC 38500. 2. Grunden til at der ikke er mere end knap 20 pct. projekter der stoppes før tid, er at virksomhederne enten ikke er klar over at der er tale om dårlige projekter eller at virksomhederne affinder sig med at projektet ikke lykkedes optimalt. Hvis det sidste er tilfælde, vil der være et stort behov for at benytte frameworks, retningslinjer, standarder osv.

[100] Afsnit 3.2.1
[101] It-governance 62,4 pct. og Governance 45,3 pct.
[102] Afsnit 3.2.3
[103] 25,7 pct. afsnit 3.2.3
[104] 21,7 pct. afsnit 3.2.3
[105] 20,0 pct. afsnit 3.2.3

I forhold til undersøgelserne er der kun er 11,6 pct[106]. Der mener at it skal være en af drivkræfterne mht. at forbedre forretningens strategi i fremtiden. Jeg anser dette for at være en ret lavt procentsats og mener at virksomhederne forspilder en stor chance for at forbedre deres konkurrenceevner. En mulighed for at gøre dette kunne være at CIO lærer at styre diskussionen i forhold til topledelsen, ved at vise hvilke forbedringer it har bidraget til at skabe for de enkelte afdelinger (internt) samt hvilken værdi der er blevet skabt i forhold til omverdenen, fx kundetilfredshed og/eller større indtægt (eksternt). Her kunne en modenhedsmodel anvendes, som jeg kort har beskrevet i afsnit 3.1.1.1, eller man kunne anvende COBIT 5's model eller dem begge, da det er en fordel at hente inspiration fra flere kilder.

Afslutningsvis viser det sig at der er et forholdsvist stort kendskab til frameworks/standards blandt it-governance men at det for it-governance ikke altid lykkes at få implementeret disse i organisationen. Om dette skyldes at der fejl i implementering eller at it-governance ikke kan få topledelsen med på ideen, kan jeg kun gisne om.

[106] Afsnit 3.2.4

Kap 5 - Konklusion

Virksomhedernes informationer er en vigtig ressource, fra skabelsen af informationen til det tidspunkt hvor den skal destrueres, og i denne proces spiller teknologien en væsentlig rolle. Der sker løbende en forøgelse i informations teknologiens (it) kompleksitet og det bliver mere og mere udbredt at anvende it i virksomheder. Det er vigtigt for organisationen som helhed, at der sker en korrekt styringer af it, da dette er for mange et bærende fundament for driften. Om det enten sker via at understøtte forretningsstrategien eller tilføje merværdi til forretningsstrategien, men at det for mange kun er at understøtte og ikke nytænke. Derved udnyttes ressourcerne ikke optimalt.

Formålet med denne kandidatafhandling har således været at undersøge:
Hvad er ledelsens rolle i håndteringen af it, og hvilke værktøjer kan denne benytte sig af samt hvordan kan man bedst beherske risikoen af projekter og hvorfor er alt dette relevant?

Specialet er konstrueret således at problemformuleringen er opdelt i to dele. første del *Hvad er ledelsens rolle i styringen af it, og hvilke værktøjer kan denne benytte sig af samt hvordan kan man bedst kontrollere risikoen af projekter…* besvares ved hjælp af teorien. Anden del *…hvorfor er alt dette relevant..* besvares via den fundne empiri.

På baggrund af den gennemgåede teori, er det meget relevant at ledelsen formår at inddrage it så tidligt som muligt i forbindelsen med den strategiske planlægning, så det er muligt at skabe synergi mellem iten og forretningen, i stedet for at iten kun bruges til at understøtte forretningen. Beslutningerne skal tages på højeste niveau i organisationen det vil sige topledelsen. Derfor er det vigtigt at topledelsen formår at være lydhør overfor it-ledelsen og it-ledelsen skal kunne dokumentere at de kan tilbyde merværdi til forretningen. Til dette kræves det at it-afdelingen er tilpas moden og at CIO kan styre diskussionen om it-værdiskabelse samt fremvise de relevante informationer.

Værktøjerne som kan benyttes er mange, i dette speciale er der gennemgået et par frameworks og en standard. Hovedformålet med denne teori er at sætte struktur på organisationens it-mæssige håndtering samt at skabe kommunikation mellem it-governance og topledelsen. Disse frameworks kan ikke stå 100 pct. alene, men skal gerne understøttes af flere inputs, dette kunne være standarder eller vejledninger, da ingen virksomheder er ens, og derfor skal der ske tilpasning

af disse frameworks til den enkelte virksomhed, der kan her være tale om COBIT 5, God it skik og ISO/IEC 38500.

COBIT 5 sikrer et samlet framework som skal hjælpe virksomheden med at opnå målsætningerne omkring governance og management af virksomhedens it. En optimal værdi fra it skabes ved at opretholde en balance imellem realiseringen af fordele, optimering af risikoniveauet og ressourceforbruget.

God it-skik har til formål at skulle hjælpe virksomhedens øverste ledelse med at få et overblik over de discipliner inden for it-området som de analyserer, beslutter og planlægger inden for, samt at implementerer og følge op den it-anvendelse der er i virksomheden i overensstemmelse med god it-skik.

ISO/IEC 38500's mål er at give ledelsesniveauet et framework med principper til at vurdere, lede og overvåge brugen af IT i virksomheden. Da de fleste virksomheder benytter sig af IT, som en stor del af driften og det i fremtiden vil spille en stor rolle, er det relevant at have fokus på hvordan man anvender dette effektiv. Denne standard skulle gerne give det højeste ledelsesniveau en forståelse for hvorfor IT er så vigtigt for virksomheden og af at IT-governance bør være et fokusområde.

Yderlige har jeg beskrevet COSO, som kan anvendes på hele virksomhedens struktur, til at danne grundlag for en fornuftigt risikostyring, ved hjælp af interne kontroller, overvågning, information og kommunikation mv.

COSO kuben er et værktøj for ledelsen til at kunne håndtere, styre og kontrollere risikoen i selskabet via interne kontroller. Samt en hjælp til at kunne identificere risikoer i forbindelse med virksomheden. De 8 indbyrdes processer som udgør COSO er det ikke nødvendigt at skulle udføre i den nævnte rækkefølge.

Afslutningsvis er der stor enighed om at it er et vigtigt element for at virksomheden kan opnå sin strategi og vision (94,7 pct.), men at dens primære funktion er at skulle understøtte den nuværende forretningsstrategi (37,9 pct.) og ikke være en innovativ part af forretningen (11,6 pct.). Det ses at it skal i højre grad være et redskab til at skabe omkostningsminimering (20,1 pct.) end at være innovativ.

Det er derfor vigtigt at have fokus på it som et konkurrenceparameter, så det er muligt at forbedre virksomhedens konkurrencevne. Dette kan hjælpes godt på vej ved brug af de værktøjer der er redegjort for i denne afhandling. Ydermere er det vigtig at de forskellige virksomhedsledere forstår at anvende de informationer som er resultatet af indførelsen af disse frameworks.

Efter gennemgangen af denne afhandling har jeg blandt andet kommet til kendskab omkring modenhed og modenhedsanalyse, og her kunne det være interessant at gå lidt mere i dybden med dette, f.eks. ISO/IEC 15504 - *Information technology — Process assessment.* Ydermere kunne ITIL være relevant at inddrage da dette er best practice, og derved at kunne sammenholde den mod COBIT 5. Som det sidste kunne jeg godt have tænkt mig at gå lidt mere i dybden med risikoanalyse og it-sikkerhed, men grundet opgavens omfang er dette fravalgt.

Litteraturliste

Bøger og Publikationer

Arbnor, Ingeman & Bjerke, Björn (1997); *Methodology for Creating Business Knowledge;* Forlag Sage Publications.

Bakka, Jørgen Frode & Fivelsdal, Egil (2004); *Organisations teori, Struktur, Kultur og Processer;* 4. udgave Handelshøjskolens forlag

Bøgh, Jakob – Jacobsen, Bjørn – Knudsen, Jacob Dronninglund & Thomsen, Mikkel Sohn (2008) – *"Forandringsledelse – en nødvendighed;* Bachelor HA

Carsten W, Heilbuth og Carsten Tjagvad (2011); *IT-revision;* 4. udgave, 2. oplag. Karnov Group Denmark

Committe of Sponsoring Organizations (2004-2005) – *Helhetlig risikostyring – et integrert rammeverk – Sammendrag*

Dansk Standard 484 (2005) – *Standard for informationssikkerhed.*

Davidsen, Christina Maria (2008); *Intern kontrol i revisionsprocessen;* Forlag Thomson

Information System Audit Control Association (2012); *COBIT 5 A Business Framework for the Governance and Management of Enterprise IT.*

Information System Audit Control Association (2008); *Aligning CobiT 4.1, ITILv3 and ISO/IEC 27002 for Business Benefit*

International Standard om Revision (2009); *Identifikation og vurdering af risici for væsentlig fejlinformation igennem forståelse af virksomheden og dens omgivesler*

IT Governance Institute (2011); *Global Status Report on the Governance of Enterprise IT (GEIT)*

Jyllands Posten sektion "Karrie" (2012); *It-muligheder går tabt på topledderniveau*

Mogensen, Jess Kjær - Lind, Bo - Gotfredsen, Knut - Joensen, Thomas B. – Mikkelsen, Niels Thor – Nielsen, Frank S. – Nielsen, Knud Fill & Berthing, Hans Henrik Aabenhus (2011); *God it-skik*

Rambøll Management Consulting (2012); *It i Praksis 2012 – strategi, trends og erfaringer i danske virksomheder.*

The International Organization for Standardization and The International Electrotechnical Commission (2008); *ISO/IEC 38500 – Corporate governance of Information Technology*

Internet

version2.dk 13/01-2013
http://www.version2.dk/leksikon/Versionsstyring

Bilag 1 – COBIT 5 Enterprise Goals

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

COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT – side 18

Bilag 2 – CIO's metode til at styre diskussionen

Sådan kan CIO'en styre diskussionen om it-værdiskabelsen over for forretningen

CIO'en skal tage ansvar for og styre diskussionen om it-værdiskabelse. Til dette er der brug for en rapporteringsmodel, der kan benyttes over for forretningens interessenter. Modellen for it-performance og kommunikation, der er beskrevet i den strategiske udfordring *Effektiv måling og kommunikation af it-performance og -værdiskabelse*, giver CIO'en et solidt grundlag for deltagelse i det månedlige møde med topledelsen, lederne af forretningsenhederne og forretningens procesejere.

Rapporteringsmodellen består af fire punkter til mødets agenda, der forenkler kommunikationsprocessen. CIO'en kan bruge modellen som et værktøj til at fremme et image som top performer og pålidelig samarbejdspartner og til at vise virksomheden, at it-afdelingen fokuserer på de områder, der er vigtige for lederne af forretningsenhederne; det hele handler om forretningen.

Punkt 1 – It's bidrag til de vigtigste forretningsstrategiske initiativer og målsætninger	CIO'en præsenterer virksomhedens 5-7 vigtigste strategiske initiativer, must-win battles og målsætninger for at vise deltagerne, at it-afdelingen er opmærksom på de områder, der står øverst på virksomhedens eller forretningsenhedens dagsorden. Dernæst præsenterer CIO'en de it-projekter og initiativer, der understøtter de strategiske initiativer, must-win battles og målsætninger, og beskriver, hvordan it-afdelingen understøtter de initiativer, hvor den er involveret, og hvordan disse bidrager til forretningens resultater. Dette opnås ved at rapportere om, hvordan it-projekter og innovationsaktiviteter er med til at øge omsætningen, øge kundetilfredsheden, drive nye eller forbedrede forretningsprocesser og skabe nye it-baserede produkter mv. Hvis det er nødvendigt, kan teknologiske emner drøftes; alternativt bør CIO'en anlægge en ren forretningsmæssig tilgang til præsentationen.
Punkt 2 – It's bidrag til forretningens løbende performance og performance i forretningsprocesser	CIO'en bruger operationelle målinger til at fremlægge effekten af it for forretningens løbende performance og performance i forretningsprocesser. Mange virksomheder afvikler online-aktiviteter for deres kunder, fx webshops, ekstranet og elektroniske produktkataloger; aktiviteter, der er stærkt afhængige af it-drift. Forretningens performance, som CIO'en skal rapportere om, omfatter derfor online-salg, omsætning pr. besøg, antallet af transaktioner og besøgende, omfang af kundeselvbetjening, kundetilfredshed og leveret serviceniveau. Der er således en lang række muligheder for CIO'ens til at kommunikere den værdi, afdelingen skaber for forretningen. I forhold til performance af forretningsprocesserne bør CIO'en rapportere om processer med en høj grad af it-involvering. Hvis fx en selvbetjeningsproces for medarbejdere er etableret, vil det være relevant at kommunikere effekten på både produktivitet og gennemløbstid.
Punkt 3 – It-forbedringer	CIO'en præsenterer it-forbedringer og giver en kort status på omkostninger og resultater inden for områderne drift, projekter og innovation. Formålet er at vise deltagerne, at it-afdelingen har styr på egen forretning og løbende arbejder på at forbedre den og levere værdi for pengene til virksomheden.
Punkt 4 – Sikre fremdrift og support	Baseret på indholdet fra de tre første punkter på dagsordenen eller andre kritiske forhold, spørger CIO'en til sidst ledelsesteamet til råds om aktuelle valg eller prioriteringer for at sikre fremdrift og support i forhold til it-afdelingen og it-initiativer.