Cobit 5 - Alignment

Kandidatafhandlingen er udarbejdet af:
Mette Blanner Holleufer & Marie Krupsdahl Andreasen Elling

Aalborg Universitet – 15 maj 2012
Cand.merc.aud., Kandidatafhandling
Vejleder Hans Henrik Aabenhus Berthing

Titelblad

Aalborg Universitet – Cand.merc.aud 10. Semester

Vejleder:	Hans Henrik Aabenhus Berthing
Betegnelse:	Kandidatafhandling
Titel:	Cobit 5 - Alignment
Emne:	It ledelse
Afleveringstidspunktet:	15 maj 2012
Antal tegn og side antal:	334.951 tegn svarende til 139,56 normalsider

Kandidatafhandlingen er udarbejdet af[1]:

Marie Krupsdahl A. Elling _____

Mette Blanner Holleufer _____

[1] For ansvarsområder se *Bilag 9*

Executive Summary

The new age and information society caused information technology (IT) to become one of the foundations of today's businesses where competition in the market triggers new opportunities. These opportunities can provide competitive advantages and achieve optimal utilization of company resources, resulting in an increase of company productivity. If companies can exploit and manage their IT in a reasonable manner, they are able to increase company profits.

Thus, today's companies rely on IT and are compelled to recognize the IT challenges that exist in order to control the IT security within a company. Since management does not always have the necessary insight into the threats and opportunities in the IT field, they can seek advice from an auditor. It is necessary to distinguish the auditor's function between advising the company in decisions and performing the audit of company accounts.

Frameworks have been a part of enterprise IT management because of the managements and stakeholders' desires for an improved return from IT investments, concern about rising costs of IT and the need to fulfill more strict regulatory requirements.

Businesses establish frameworks and standards to control the quality and reliability in IT application and regulatory requirements. It may have implications for the company, it the introduction of frameworks and standards are not focused and processed too in-depth in relation to business needs, thereby becoming too costly for the company. Thus, implementation of frameworks and standards should be considered in relation to the company's risk management, to what is most beneficial in relation to the individual company and to the methods the company already uses, creating a perfect synergy between the existing methods and potentially implemented standards.

IT addresses not only technology but also the entire enterprise approach to IT and IT security. This has to be done from the top management all the way down to the individual employee. The Board of Directors and the management therefore need to expand IT management, thereby ensuring that the overall

goals and strategies of the company is maintained. In this way, IT management should not be separated from the remaining leadership of the company, but instead become an integrated part of overall management. IT should be incorporated into the company's business like any other strategic considerations.

The purpose of this thesis is to investigate: *How can an auditor counsel the board of directors to obtain the best utilization of the IT resources within the enterprise?*

When operating within the IT field, auditors and management should be aware of published frameworks and standards that can serve as inspiration and guidance for managing IT. The frameworks and standards presented in this thesis are:

- ISACA's Cobit 5
- COSO's Enterprise Risk Management (ERM)
- ISO/IEC 27001 and 27002
- ISO/IEC 20000-series
- ISO/IEC 38500
- SEI's CMMI
- OGC's Prince2
- OGC's ITILv3
- ISF's The 2011 Standard

Since companies are now aware of the importance of IT processes, Cobit 5 is an optimal tool for controlling and understanding all levels of internal controls. Therefore; Cobit 5 and its processes is the overall framework and has been the base for alignment with the other frameworks and standards.
The presented frameworks and standards contain different focus areas, and it may be necessary for the company to build a model that is tailored to the specific needs of the business. In addition, it is necessary to align the various frameworks and standards. Auditors must agree with the company they advise, while the auditor must have insight into the various frameworks and standards in order to provide the best possible advice for the specific company. Since no companies are alike, there is no single frame-

work or one standard that is optimal for all businesses. It is necessary that the company selects processes from the various frameworks and standards, and puts together its own model to create an ideal set of standards, so that the company utilizes their IT resources in the best possible way.

Indholdsfortegnelse

Indledning

1. Problemfelt

Informationssamfundet bevirker, at informationsteknologi (it) er en af grundstenene for virksomheder, når de skal konkurrere på markedet, og medfører derved muligheder for virksomhederne. Muligheder som konkurrencemæssige fordele samt at opnå optimal udnyttelse af virksomhedens ressourcer, så produktiviteten i virksomheden således øges. Hvis virksomhederne forstår at udnytte og administrere deres it på en fornuftig måde, kan de derved øge virksomhedens overskud.[2]

Derfor er virksomheder i dag afhængige af it og er nødsaget til at erkende de it relaterede udfordringer, som eksisterer for derved at styre it sikkerheden i virksomheden. Da ledelsen ikke altid har den nødvendige indsigt i virksomhedens trusler og muligheder på it området, kan de søge rådgivning hos en revisor. Dog er revisors opgave ikke blot at rådgive ledelsen, men også at revidere virksomhedens it kontroller. Som revisor er det ifølge den International Standards of Auditing (ISA) 315: *Identifikation og vurdering af risici for væsentlig fejlinformation igennem forståelse af virksomheden og dens omgivelser* et krav, at der opnås en forståelse af virksomhedens interne kontroller og vurderer de potentielle risici, som eksisterer, heriblandt it relaterede risici, så der kan udformes og implementeres reaktioner på risiciene. Andre revisionsstandarder end ISA 315 indeholder ligeledes it relaterede overvejelser revisor skal vurdere ved revision.[3] Det er nødvendigt at skelne mellem om revisor skal rådgive virksomheden i beslutninger, eller om revisor skal udføre revision af virksomhedens regnskabsaflæggelse. Der skal ifølge International Standard on Quality Control (ISQC) 1: *Kvalitetsstyring i firmaer, som udfører revision og review af regnskaber, andre erklæringer med sikkerhed og beslægtede opgaver* etableres politikker og procedurer, for at opnå en høj grad af sikkerhed for om revisionsfirmaet og dets personale, som er underlagt uafhængighedskravene, også opretholder denne uafhængighed. Disse politikker og procedurer skal identificere og vurdere omstændigheder og relationer, som kan udløse en trussel mod uafhængigheden. Derudover skal disse politikker og procedurer muliggør eliminering af disse trusler eller reducere dem til et acceptabelt niveau ved at indføre sikkerhedsforanstaltninger. Derfor kan det

[2] ITGI: *IT Governance Using CobiT and Val IT Student Book s. 3*
[3] Karnov Group: *Revisorhåndbogen 2011 s. 1111*

påvirke revisors uafhængighed, hvis samme revisor er ansvarlig for at rådgive virksomheden, såfremt revisoren ligeledes skal udføre revision af regnskabsaflæggelsen.[4]

It omhandler ikke blot teknik, men handler også om hele virksomhedens holdning til it og it sikkerhed. Dette er helt oppe fra øverste ledelsesniveau og ned til den enkelte medarbejder. It bør indarbejdes i virksomhedens forretning ligesom alle andre strategiske overvejelser. Bestyrelsen og direktionen har derfor behov for at udvide it styringen, så virksomhedens overordnede mål og strategier bliver opretholdt. Således skal it ledelse ikke adskilles fra den resterende ledelse af virksomheden, men i stedet blive en integreret del af den samlede styring.[5]

Frameworks er blevet en del af virksomhedens it ledelse på grund af ledelsens og interessenternes ønske for et bedre afkast fra it investeringer, bekymring for stigende udgifter til it og behovet for at opfylde strengere lovgivningsmæssige krav som blandt andet US Sarbanes-Oxley Act.[6]

US Sarbanes-Oxley Act blev i 2002 vedtaget som ny lov i USA, der indeholder krav om nøjagtighed og troværdighed til de informationer, som virksomheden skal videregive til offentligheden. Årsagen til regelsættet var erhvervsskandaler som blandt andet Enron-skandalen, hvor de finansielle resultater ikke var pålidelige på grund af regnskabssvindel. US Sarbanes-Oxley Act ændrede kravene til interne processer som offentlige virksomheder havde anvendt i deres ledelse og til udarbejdelse af årsrapporten til Securities and Exchange Commission (SEC). Desuden havde US Sarbanes-Oxley Act betydning for såvel ekstern revisor som intern revisors aktiviteter og ansvar, selvom disse revisorer skal overholde forskellige standarder som Public Company Accounting Oversight Board (PCAOB) og har forskellige målsætninger. PCAOB introducerede på baggrund af US Sarbanes-Oxley Act den risikobaserede Auditing Standard No. 5[7], som fastlægger krav og retningslinjer for revisors revision af den interne kontrol ved regnskabsaflæggelsen.[8]

[4] Karnov Group: *Revisorhåndbogen 2011 s. 924 punkt 21*
[5] ITGI: *IT Governance Using CobiT and Val IT Student Book s. 3*
[6] ITGI: *Aligning CobiT 4.1, ITIL v3 and ISO/IEC 27002 for Business Benefit s. 8*
[7] Robert R. Moeller: *Sarbanes-Oxley Internal Controls –Effective Auditing with AS5, CobiT and ITIL s. 1 + 2*
[8] PCAOB: *Auditing Standard No. 5*

Virksomheder indfører frameworks for at styre kvaliteten og pålideligheden af it anvendelse samt lovgivningsmæssige krav. Det kan få konsekvenser for virksomheden, hvis indførelsen af frameworks ikke er fokuseret og behandles for dybdegående i forhold til virksomhedens behov, og derved bliver for omkostningsfuldt for virksomheden. Derfor bør implementeringen af frameworks overvejes i forhold til virksomhedens risikostyring, hvad der er mest fordelagtig i forhold til den enkelte virksomhed samt de metoder virksomheden i forvejen anvender.[9]

1.1 Problemformulering

Således er it et af fundamenterne for virksomheder og bør indarbejdes i virksomhedens forretning ligesom andre strategiske overvejelser. It ledelse skal være en integreret del af virksomhedens samlede styring når der foretages ledelsesmæssige beslutninger. Det får betydning for produktiviteten i virksomheden, om ledelsen formår at få det optimale ud af virksomhedens it ressourcer, så konkurrencemæssige fordele bliver potentielle.

Med udgangspunkt i ovenstående problemstilling vil nedenstående problemformulering være udgangspunktet for denne kandidatafhandling:

Hvordan kan revisor rådgive ledelsen til at få det optimale ud af virksomhedens it ressourcer?

Når der i problemformuleringen nævnes revisor, relaterer dette både til interne og eksterne revisorer, da ledelsen i deres beslutningsproces har mulighed for at tilegne sig informationer fra såvel interne revisorer som eksterne revisorer. Ordet rådgivning i problemformuleringen sidestilles med revisors kendskab til diverse love, standarder og frameworks indenfor it området, og revisors mulighed for at videreføre disse i ledelsens beslutningsgrundlag og som inspiration til ledelsen. Med ledelsen refereres der til virksomhedens øverste ledelse, som varetager udarbejdelsen af virksomhedens overordnede forretningsstrategi.[10] Når ordet optimal anvendes i problemformuleringen, er det et udtryk for, at der opnås det mest fordelagtige alternativ på baggrund af omstændighederne. Virksomhedens it ressourcer relaterer sig til, at alt afhængig af hvilken virksomhed der tages udgangspunkt i, har virksomhederne forskel-

[9] ITGI: *Aligning CobiT 4.1, ITIL v3 and ISO/IEC 27002 for Business Benefit s. 6*
[10] Selskabsloven § 115

lig it kapacitet. Derved er målet at få det mest fordelagtige ud af den kapacitet, som den enkelte virksomhed disponerer over. Kapaciteten omfatter blandt andet personer, procedurer, software, udstyr, information, forbrug og tid.[11]

For at besvare problemformuleringen opstilles der undersøgelsesspørgsmål, som skal danne ramme for den teori og analyse, der præsenteres i denne afhandling:

- *Hvilke standarder kan anvendes til styring af virksomhedens it?*
- *Hvilke frameworks kan anvendes til styring af virksomhedens it?*
- *Hvordan kan revisor rådgive virksomheden om frameworks og standarder?*

Første undersøgelsesspørgsmål skal afdække, hvilke standarder samt krav fra omverdenen, som både revisor og ledelsen skal være opmærksom på, når de opererer indenfor it området. Dertil skal det afdækkes, hvilke relevante frameworks for it ledelse, som kan være inspiration til ledelsen ved styring af virksomhedens it, så de derved får det optimale ud af virksomhedens it ressourcer. Det sidste undersøgelsesspørgsmål omhandler, hvorledes revisor kan rådgive ledelsen i anvendelsen af de publicerede frameworks og standarder i forhold til den pågældende virksomhed.

2. Begrebsforklaring

Der anvendes i denne kandidatafhandling litteratur, som er udformet på engelsk. Nogle begreber kan ved oversættelse miste indhold og for at undgå misforståelser eller betydning ved oversættelse, redegøres der i dette afsnit for de mest anvendte begreber, som igennem afhandlingen kan forekomme på engelsk. Disse er:

- Begrebet *framework* anvendes for de forskellige publicerede udgivelser fra ISACA, ISF med videre.
- Begrebet *alignment* anvendes, når processerne i diverse frameworks og standarder i afhandlingen bliver sammenholdt og afstemt for om de understøtter hinanden.

[11] *ISO/IEC 38500 s. 4*

- Begrebet *compliance* anvendes, når der henvises til lovgivningsmæssige og regulerende bestemmelser, som virksomheden skal overholde.
- Begrebet *good pratice / best practice* anvendes, når der i litteraturen redegøres for branchemæssige sædvaner, og hvordan virksomheder efterkommer dette i praksis samtidig med overholdelse af de lovgivningsmæssige bestemmelser.
- Begrebet *management* refererer til virksomhedens daglige ledelse eller virksomhedens styring af it.
- Begrebet *governance* refererer til virksomhedens øverste ledelse eller virksomhedens ledelse af it.
- Begrebet *enabler* anvendes, hvor der eksisterer en drivende kraft bag ved en aktivitet, som bidrager til positiv effekt.

3. Afgræsning

I dette afsnit vil der blive redegjort for de overvejelser, som ligger bag de valg og derved fravalg, som har været nødvendige under udarbejdelsen af denne kandidatafhandling, på baggrund af den fremsatte problemformulering.

Hvordan revisor skal håndtere it i udførelsen af revision og andre erklæringsopgaver med sikkerhed for en virksomhed er vedtaget i de internationale standarder om revision og andre erklæringsopgaver med sikkerhed. Revisor skal være opmærksom på specifikke afsnit i ISA 315, ISA 402, ISA 620 og International Standard on Assurance Engagements 3402, der omhandler it når der foretages revision eller andre erklæringsopgaver med sikkerhed. Som tidligere beskrevet er det nødvendigt at skelne mellem om revisor skal rådgive eller revidere en virksomhed, da kravene til uafhængighed skal opretholdes for at opnå pålidelig regnskabsaflæggelse.[12] Derfor fokuserer denne kandidatafhandling udelukkende på revisors rådgivning til virksomheder af håndtering af frameworks og standarder, som kan anvendes ved styring af virksomhedens it. En vurdering af revisors revision af it, hvilken betydning it kan få for revisors påtegning samt en redegørelse af de internationale standarder om revision og andre erklæringsopgaver med sikkerhed vil ikke blive gennemgået yderligere.

[12] Karnov Group: *Revisorhåndbogen 2011 s. 924 punkt 21*

De forskellige frameworks og standarder indeholder processer, som refererer til outsourcing. Derfor vil outsourcing af it i denne afhandling blive anvendt i det omfang, det indgår i diverse frameworks og standarders processer, som omhandler outsourcing. Behandling af virksomheders eventuelle fordele eller ulemper ved anvendelse af serviceleverandører afgrænses der fra.

Da US Sarbanes-Oxley Act blev vedtaget i USA, indførte det et krav for alle SEC registrerede virksomheder om at etablere processer for at opbygge, styre og overvåge virksomhedens interne kontroller. Det var ofte nødvendigt for virksomhedens ledelse for effektiv og optimal overholdelse af US Sarbanes-Oxley Act at modtage vejledning omkring håndtering af virksomhedens interne kontroller. Her blev en tidligere version af Control Objectives for IT (Cobit) et framework, som nogle amerikanske virksomheder anvendte for at opnå en effektiv US Sarbanes-Oxley Act compliance, da Cobit ligeledes havde fokus på styring af virksomhedens interne kontroller. Fordi virksomheder har opnået kendskab til betydningen af it processer er Cobit et optimal værktøj til styring og forståelse af alle niveauer af interne kontroller.[13] Derfor er seneste udgave af Cobit 5 det overordnede framework og udgangspunktet for denne kandidatafhandling. Øvrige anvendte frameworks og standarder vil blive sammenholdt med processerne i Cobit 5 på detailniveau.

Denne afhandling afgrænses til udelukkende at omhandle de senest tilgængelige publicerede frameworks og standarder under udfærdigelsen af denne afhandling, da senere udgivelser end afleveringsdatoen ikke er mulig at indarbejde.

Kandidatafhandlingen afgrænses fra at behandle finansielle virksomheder, da der i lovgivningen eksisterer specielle krav til it i finansielle virksomheder jævnfør *Bekendtgørelse af lov om finansiel virksomhed* § 71 stk. 1 nr. 8 og dertilhørende vejledning og bekendtgørelse.

Kandidatafhandlingens problemformulering besvares til dels ved hjælp af kvalitativ data. Som kvalitative data inddrages interview med udvalgte personer, men kvalitative data som spørgeskemaundersøgelse fravælges, da interview giver mulighed for mere dybdegående spørgsmål og dialog mellem den

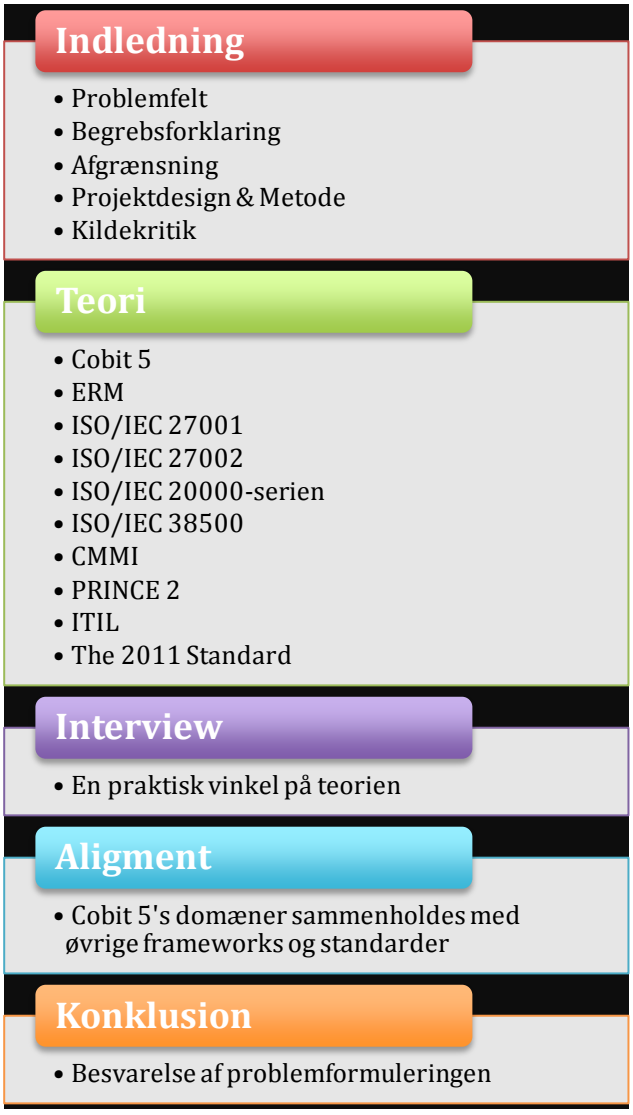
[13] Robert R. Moeller: *Sarbanes-Oxley Internal Controls –Effective Auditing with AS5, CobiT and ITIL s. 7 + 8*

interviewede og intervieweren. Mulige påvirkninger som kan have indflydelse på oprigtigheden af den indsamlede data bliver uddybet i afsnittet *Kildekritik*.

4. Projektdesign & Metode

Dette afsnit er inddraget med det formål at give et illustrativt overblik med tilhørerende forklaring af, hvordan denne kandidatafhandling er opbygget og struktureret. Nedenstående projektdesign demonstrerer opbygningen af afhandlingen:

Figur 1 - Projektdesign



Kilde: Egen tilvirkning

Afhandlingen består af fem kapitler, hvoraf første kapitel består af en indledning, hvori der præsenteres et problemfelt, som leder op til afhandlingens overordnede problemformulering. I problemformuleringsafsnittet bliver problemformuleringens centrale betegnelser defineret, så der ikke opstår misforståelser igennem afhandlingen. Endvidere indeholder afsnittet tre undersøgelsesspørgsmål til den overordnede problemformulering, som er udarbejdet for at opnå en optimal besvarelse på problemformuleringen. Herefter er der inddraget et begrebsforklaringsafsnit, som redegør for anvendte engelske begreber i kandidatafhandlingen. Indledningskapitlet indeholder desuden en afgræsning, som behandler overvejelserne omkring valg og derved fravalg, der er foretaget under udarbejdelsen af denne afhandling. Projektdesign og metodeafsnittet er som beskrevet medtaget for illustrativt med tilhørende forklaring at redegøre for, hvordan denne kandidatafhandling er struktureret. Endvidere indeholder indledningskapitlet en redegørelse for en kritisk stillingstagen til diverse kilder, som er anvendt i afhandlingen.

Anden kapitel indeholder afhandlingens teoretiske afsnit, som er en redegørelse og beskrivelse af diverse frameworks og standarder. Formålet er efterfølgende at sammenholde processerne i Cobit 5 med øvrige frameworks og standarders processer, så det muliggør en besvarelse af, hvilke muligheder revisorer har, når de rådgiver virksomheder indenfor it området.

I interviewkapitlet redegøres der for de afholdte interview i forbindelse med kandidatafhandlingen. Formålet er at give en teoretisk afhandling en praktisk vinkel.

Efter en præsentation af frameworks, standarder og interview inddrages kapitlet *Alignment.* Dette er afhandlingens analyseafsnit, som vil sammenholde Cobit 5's domæner og processer med de øvrige inddragede frameworks og standarders processer, principper og lignede for at udlede, hvilke af processerne i Cobit 5 der ligeledes bliver understøttet af de resterende frameworks og standarder.

Afslutningsvis vil hele kandidatafhandlingen opsummeres i en konklusion, som derved besvarer den overordnede problemformulering.

5. Kildekritik

Dette afsnit er medtaget for at skildre bevidstheden omkring forhold, som kan have indflydelse på kandidatafhandlingens endelige konklusion og derved præsenteres områder, hvor det er nødvendig med en kritisk stillingstagen.

I denne kandidatafhandling er der fokus på, at den anvendte litteratur kan være præget af forfatternes subjektive overbevisninger. Ved at inddrage revisorers opfattelser i afhandlingen, kan der ikke foretages konklusioner vedrørende revisorer generelt. I stedet fortolkes de inddragede revisorers udtalelser, som et udtryk for de pågældende personers opfattelser til enten at underbygge eller modsvare den anvendte teori. Formålet med afhandlingen er således ikke at udforme en generel konklusion af revisor rådgivning til ledelsen gennem induktion ud fra enkelte revisorers udtalelser, men i stedet at et teoretisk projekt tilføres en praktisk vinkel.

Ligeledes er de anvendte frameworks i denne afhandling anset som ”best practice”. Alligevel er der i afhandlingen taget kritisk stilling til de inddragede frameworks, da intet er fejlfrit, og der kontinuerlig foretages forbedringer for at opnå det mest fordelagtige resultat til brugerne af de publicerede frameworks.

Endvidere er der ved at benytte kvalitative data som teknik ved hjælp af interview en række forbehold, som er nødvendige at være opmærksom på. Opfattelser som er udtrykt igennem interview kan være påvirket af såvel omgivelserne som stemningen under interviewet. Ligesom interviewet kan blive påvirket af intervieweren. Hvis der anvendes ledende spørgsmål i interviewet kan svarerne blive påvirket heraf, som hvis den interviewede opfatter spørgsmålene anderledes end disse var tiltænkt. Dette bliver i denne afhandling forsøget undgået ved, at hovedemnerne til de interviewede bliver sendt via mail, så selve interviewet fungerer som et supplement til de sendte emner. På den måde er de interviewede indforstået med, hvad interviewet skal omhandle på forhånd og indstille sig på indholdet.

Teori

Hensigten med dette kapitel er at demonstrere teorien omkring udvalgte frameworks og standarder for derved at generere et teoretisk udgangspunkt for den efterfølgende behandling af, hvordan revisor kan rådgive ledelsen til at få det optimale ud af virksomhedens it ressourcer. Her er formålet at få en forståelse af, hvilke processer i Enterprise Risk Management (ERM), The International Organization for Standardization (ISO) og The International Electrotechnical Commission (IEC) 27001, ISO/IEC 27002, ISO/IEC 20000-serien, ISO/IEC 38500, Capability Maturity Model Integration (CMMI), Project In a Controlled Environment (Prince2), Information Technology Infrastructure Library (ITIL) og The 2011 Standard of Good Practice for Information Security (The 2011 Standard), der understøtter Cobit 5's 37 processer, som muliggør en besvarelse af afhandlingens overordnede problemformulering.

6. Cobit 5 som det overordnede Framework

Som tidligere beskrevet er anvendelsen af frameworks blevet en del af virksomhedens it ledelse, som følge af behovet for at opfylde lovgivningsmæssige krav ved indførelsen af US Sarbanes-Oxley Act.[14] Denne vedtagelse havde betydning for amerikanske børsnoterede virksomheder og for de tilhørende koncernforbundne virksomheder. Kravet til at etablere processer for at opbygge, styre og overvåge de interne kontroller i virksomheden er nødvendigt for en effektiv overholdelse af US Sarbanes-Oxley Act. Cobit frameworket fokuserer på alle niveauer af virksomhedens interne kontroller, så virksomheder ved anvendelsen af frameworket kan opnå en optimal og effektiv forståelse af disse interne kontroller. Cobit understøtter kontrollerne i US Sarbanes-Oxley Act ved at opsætte en model og standard for it ledelse med konceptet om, at forretningsmæssige it ressourcer burde være sammenholdt med den overordnede virksomhed, at disse ressourcer burde anvendes optimal, og at it relaterede risici burde styres på en hensigtsmæssig måde.[15] Derfor er Cobit 5, som er den seneste publikation fra Information System Audit Control Association (ISACA), det overordnede framework i denne kandidatafhandling og vil blive præsenteret i efterfølgende afsnit.

[14] Robert R. Moeller: *Sarbanes-Oxley Internal Controls –Effective Auditing with AS5, CobiT and ITIL s. 1 + 2*
[15] Robert R. Moeller: *Sarbanes-Oxley Internal Controls –Effective Auditing with AS5, CobiT and ITIL s. 8*

Cobit 5

Dette afsnit har til formål at præsentere ISACA's senest publicerede Cobit framework indenfor it ledelse. ISACA er en global formidler af viden, certificering, rådgivning og uddannelse indenfor informationssikkerhed, virksomhedsledelse og styring af it og relaterede it relaterede risici samt overholdelse af lovgivningsmæssige krav.[16] I en undersøgelse udarbejdet af PricewaterhouseCoopers Belgium i 2010, efterspurgt af IT Governance Institute (ITGI), fremkommer det, at ud af undersøgelsens 800 respondenter, anvendte 12,9 procent Cobit (ISACA), 12 procent Risk IT (ISACA), 9,8 procent IT Assurance Framework (ISACA), 7,8 procent BMIS (ISACA) og 4,9 procent anvendte Val IT (ISACA) i virksomhedens it ledelse.[17]

Information er en nødvendig ressource for virksomheder og fra det tidspunkt, hvor oplysningerne er opnået til de ødelægges har teknologi indflydelse på informationen. Som et resultat af dette bestræber virksomhederne sig på at opretholde information af kvalitet for at understøtte virksomhedens beslutninger, generere værdi for virksomheden igennem it investeringer, optimere driften gennem pålidelige og effektive teknologi, opretholde it relaterede risici på et acceptabelt niveau for virksomheden, optimere omkostningerne der anvendes til it service og teknologi og overholde lovgivningsmæssige krav og reguleringer. Virksomheders bestyrelse er blevet opmærksomme på, at it skal inkluderes i den resterende ledelse og styring af virksomheden, og derfor anvendes frameworks for at tilvejebringe at it bliver en integreret del af virksomheden.[18]

Anvendelse af Cobit 5 sikre et udførlig framework, som er behjælpelig med opnå virksomhedens målsætning for ledelsen og styringen af it. Således at opnå optimal værdi fra it ved at fastholde en balance mellem at realisere mulige fordele og minimere virksomhedens risikoniveau og ressourceforbrug så såvel interne interessenter som eksterne interessenters interesser opretholdes.[19]

[16] ISACA: *Cobit 5 – A Business Framework for the Governance and Management og Enterprise IT s. 2*
[17] ITGI: *Global Status Report on the Governance of Enterprise IT s. 29, figure 26*
[18] ISACA: *Cobit 5 – A Business Framework for the Governance and Management og Enterprise IT s. 13*
[19] ISACA: *Cobit 5 – A Business Framework for the Governance and Management og Enterprise IT s. 13*

Cobit 5 er baseret på fem principper for styring og ledelse af virksomhedens it:

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

7 Princip 1: Imødegå Interessenternes Behov.

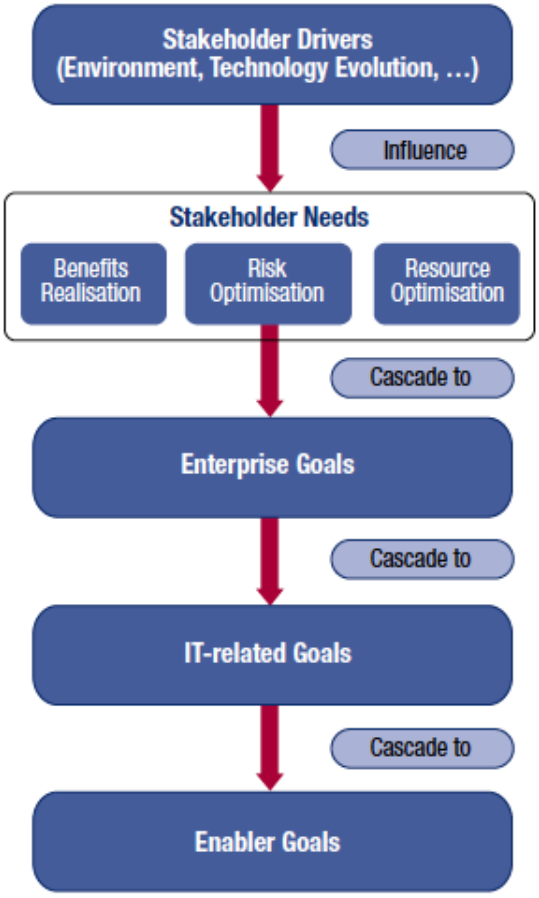
Værdiskabelse er et ledelsesmål virksomheder opererer med, da virksomheden eksisterer for at opnå værdi for interessenterne. Værdiskabelse opnås når fordelene ved optimal ressourceudnyttelse realiseres imens risiciene optimeres. Cobit 5 opdeler værdiskabelse i henholdsvis realisering af fordele, risikooptimering og ressourceoptimering. Virksomheder kan have forskellige interessenter, som alle har en forskellig opfattelse af, hvad værdiskabelse betyder for netop dem. Ledelse omhandler at foretage beslutninger omkring, hvilke af disse forskellige interessentbehov, som skal forsøges at opnås. Alle de forskellige interessenters behov skal overvejes i forbindelse med ledelsens fordele-, risiko- og ressourcevurdering. Cobit 5 fremsætter tre spørgsmål som burde besvares ved hver vurdering: Hvem får udbytte af fordelene? Hvem påtager risikoen? Hvilke ressourcer er påkrævet?[20]

Det er nødvendigt, at interessenternes behov bliver indarbejdet i virksomhedens overordnede strategi. Cobit 5 opererer med et målvandfald, som omsætter interessenternes behov til specifikke, tilpassede og handlingsrettede virksomhedsmål, it mål og enabler mål. På den måde opnår virksomheden en specifik målsætning til hvert niveau og område i virksomheden, som understøtter virksomhedens overordnede målsætning, og derved opnås en effektiv alignment mellem virksomhedens behov og it løsninger.[21]

Nedenstående figur illustrerer Cobit 5's målvandfald:

[20] ISACA: *Cobit 5 – A Business Framework for the Governance and Management og Enterprise IT s. 17*
[21] ISACA: *Cobit 5 – A Business Framework for the Governance and Management og Enterprise IT s. 17*

Figur 2 – Cobit 5's Målvandfald



Kilde: ISACA: *Cobit 5 – A Business Framework for the Governance and Management og Enterprise IT* s. 18

Første step omhandler, hvad der påvirker interessenternes behov. Interesserenters behov bliver påvirket af en række forhold som blandt andet ændringer i virksomhedens strategi, lovgivningsmæssige krav og ny teknologi.

Derefter bliver virksomhedens mål påvirket af interessenternes behov i andet step i Cobit 5's målvandfald, hvor virksomhedens mål kan blive udarbejdet baseret op Kaplan og Norton's Balanced Scorecard (BSC) dimensioner, som repræsenterer ofte anvendte mål. Disse mål er ikke udtømmende, men virksomhedsspecifikke opsatte mål kan ofte placeres indenfor de samme områder. Cobit 5 definerer 17 generiske mål som både indeholder BSC's finansielle dimension, kundedimension, interne dimension

og lærings- og udviklingsdimension, virksomhedens mål og forholdet til de tre overordnede ledelsesmål for værdiskabelse.[22]

Andet step i Cobit 5's målvandfalds fører til tredje step omhandlende it relaterede mål. For opnåelse af virksomhedens mål er det blandt andet nødvendigt med it relaterede resultater, der afspejles i de it relaterede mål. Cobit 5 opsætter 17 it relaterede mål, som bliver struktureret efter de fire dimensioner i BSC.[23]

Sidste step i Cobit 5's målvandfald er enabler mål. For at opnå virksomhedens it relaterede mål skal der implementeres og anvendes enablers, som blandt andet inkluderer *Processer*, *Virksomhedsstruktur og Information*. For hver enabler skal der opsættes mål, som kan blive defineret og understøttet af de it relaterede mål.[24]

Fordelene ved at anvende Cobit 5's målvandfald er, at den muliggør en fastlæggelse af prioriteter for implementering, forbedring og styring af sikkerheden i virksomhedens it strategiske mål og relaterede risici. Derudover skal virksomheder, der anvender Cobit 5 være opmærksom på, at målvandfaldet er en vejledning, som skal tilpasses virksomhedens individuelle behov, da enhver virksomhed har forskellige mål og prioriteter. I praksis betyder dette, at for optimal udnyttelse af målvandfaldet burde virksomheder opbygge et målvandfald, som er tilpasset virksomheden, hvorefter den sammenlignes med Cobit 5's målvandfald for til sidst at finpudse den.[25]

8 Princip 2: Dække Virksomheden "End-to-End"

Cobit 5 omhandler governance og management af information og relateret teknologi fra en virksomheds "end-to-end" perspektiv. Dette betyder, at it ledelse bliver en integreret del af virksomhedens samlede governance, og dækker alle nødvendige funktioner og processer til at lede og styre virksomhedens information og relateret teknologi, hvor denne information bliver behandlet. Som det fremgår i neden-

[22] *Bilag 1*
[23] *Bilag 2*
[24] ISACA: *Cobit 5 – A Business Framework for the Governance and Management og Enterprise IT s. 17 + 18*
[25] ISACA: *Cobit 5 – A Business Framework for the Governance and Management og Enterprise IT s. 20*

stående princip sikre Cobit 5 en holistisk og helhedsorienteret tilgang til governance og management af virksomhedens it, som er baseret på enablers. Disse enablers er ligeledes dækket af virksomhedens "end-to-end" perspektiv. *Information* er en af enabler kategorierne og den model, hvor Cobit 5 definerer enablers tillader, at enhver interessent kan nedsætte omfattende krav til virksomhedens information og informationsproces således, at virksomhedens information er tilstrækkelig og korrekt til at understøtte virksomhedens fokus.[26]

Virksomhedens "end-to-end" governance perspektiv inkluderer foruden governance målet omkring værdiskabelse elementerne governance enabler, governance anvendelsesområde, roller, aktiviteter og sammenhæng. Governance enabler er ressourcer for governance som for eksempel frameworks, principper, strukturer og processer, hvorefter vurderinger foretages så virksomhedens mål forsøges at opnås. Derudover indeholder begrebet enablers ligeledes virksomhedens ressourcer, som blandt andet infrastrukturen, personer og information, hvor en manglende ressource eller enabler kan have betydning for om virksomheden formår at skabe værdi for interessenterne. Governance kan blive anvendt i hele virksomheden eller blot på et enkelt område. Det er nødvendigt for virksomheden at definere anvendelsesområdet for governancesystemet, hvor Cobit 5 antager, at hele virksomheden er anvendelsesområdet for governance og ikke blot en enkelt afdeling. Det sidste element i virksomhedens "end-to-end" governance perspektiv er som tidligere beskrevet roller, aktiviteter og sammenhæng. Dette definerer hvem som er involveret i governance, hvordan de er involveret og hvordan de interagerer indenfor anvendelsesområdet i enhver governancesystem. Cobit 5 differentierer mellem governance og management aktiviteter i et governance- og managementdomæne ligesom der skelnes mellem, hvordan disse to domæner kommunikerer med hinanden, og hvilke personer som er involveret.[27]

9 Princip 3: Anvende Ét Integreret Framework

Cobit 5 er ét integreret framework fordi frameworket sammenholdes med de seneste publicerede standarder og frameworks således, at Cobit 5 kan anvendes af virksomheder som det overordnede governance- og managementframework. Desuden er tidligere publicerede ISACA frameworks indarbejdet i Cobit 5, som indebærer Cobit, Val IT, Risk IT og BMIS. Dette framework leverer derved en opdateret

[26] ISACA: *Cobit 5 – A Business Framework for the Governance and Management og Enterprise IT s. 23*
[27] ISACA: *Cobit 5 – A Business Framework for the Governance and Management og Enterprise IT s. 23+24*

vejledning til virksomhedens it governance og management ved at anvende denne integrerede tilgang, hvor tidligere ISACA publikationer er indarbejdet i frameworket. Cobit 5 er opdateret på de områder, der havde behov for yderligere bearbejdning, samt er der foretaget alignment med andre frameworks og standarder som blandt andet ITIL og ISO/IEC standarderne. Derudover bidrager governance og management enablers til et struktureret vejledningsmateriale.[28]

10 Princip 4: Muliggør en Holistisk Tilgang

Enablers er en drivende kraft bag ved en aktivitet, som bidrager til en positiv effekt, hvad enten disse enablers er individuelle eller samlet og er i dette tilfælde virksomhedens it governance og management. Som tidligere beskrevet i Cobit 5's målvandfald indgår enablers ved, at det højere liggende it relaterede mål definerer, hvad de forskellige enablers burde opnå.[29]

Cobit 5 frameworket definerer syv enablerkategorier:

- *Principper, politikikker og frameworks*, som er værktøjerne til at overføre den ønskede adfærd til en praktisk vejledning for den daglige ledelse.
- *Processer,* beskriver organiserede kutymer og aktiviteter for at opnå og vedholde virksomhedens mål samtidig med, at processerne producerer et resultat, som understøtter opnåelsen af it relaterede mål.
- *Virksomhedsstruktur,* er de beslutningstagende enheder i en virksomhed.
- *Kultur, etik og adfærd* af individer og af virksomheden i governance- og managementaktiviteter, er ofte undervurderede faktorer i forhold til virksomhedens fremgang.
- *Information* er udbredt i enhver virksomhed og omfatter alle oplysninger, der produceres og anvendes i virksomheden. Derudover er information nødvendig for at oppebærer virksomheden, og på et operationelt niveau kan information være dét væsentligste for virksomheden.
- *Service, infrastruktur og applikationer,* omfatter infrastrukturen, teknologien og applikationer, som tilfører virksomheden informationsteknologisk behandling og service.

[28] ISACA: *Cobit 5 – A Business Framework for the Governance and Management og Enterprise IT s. 25+26*
[29] ISACA: *Cobit 5 – A Business Framework for the Governance and Management og Enterprise IT s. 27*

- *Personer, færdigheder og kompetencer,* relaterer til personer i virksomheden, som er nødvendige for at opnå optimale beslutningstagninger og handlinger.

Information, Personer, færdigheder og kompetencer og *Service, infrastruktur og applikationer* er enablers, der ligeledes er virksomhedens ressourcer, som også er nødvendige at foretage governance og management på. [30]

Det er for enhver virksomhed nødvendigt at forstå interaktionen imellem disse enablers for at opnå virksomhedens målsætning. Enablers har behov for input fra en anden enabler for at fungere effektivt. Eksempelvis har *Processer* behov for *Information,* og en *Virksomhedsstruktur* har behov for *Personer, færdigheder og kompetencer* for at fungere optimalt. Derudover bidrager enablers til positiv output fra en enabler til en anden. *Processer* leverer *Information* og *Personer, færdigheder og kompetencer* gør *Processer* effektive. Derfor opnås optimale og effektive beslutninger i governance og management af virksomhedens it, når denne holistiske tilgang til governance og management overvejes. Dette betyder, at når der foretages beslutninger omkring interessenters behov skal alle disse enablers vurderes, og hvis nødvendigt håndteres.[31]

Enablers kan derfor inddeles i fælles dimensioner, som tilfører en fælles, simpel og struktureret tilgang til håndtering af enablers, tillader virksomheden at styre interaktioner enablers imellem og muliggør positive resultater fra disse enablers. Disse fire dimensioner er interessenter, mål, livcyklus og ”good practice”. Hver enabler har interessenter, som har en interesse i den enabler. Disse virksomhedsinteressenter kan være såvel interne som eksterne, og have egne interesser og behov, som kan være modstridende. Interessenterne og disses ansvarsområde kan ved enablerkategorien *Processer* inddeles efter, hvem som er ”responsible”, ”accountable”, ”consulted” eller ”informed” (RACI), hvor interne interessenter inkluderer den øverste ledelse, den daglige ledelse og medarbejdere, og hvor eksterne interessenter omfatter kunder, forretningspartnere, aktionærer og myndigheder.[32] Enabler mål er det sidste step i Cobit 5’s målvandfald, og er værdiskabende ved opnåelse af disse mål, som kan være et forventet re-

[30] ISACA: *Cobit 5 – A Business Framework for the Governance and Management og Enterprise IT s. 27*
[31] ISACA: *Cobit 5 – A Business Framework for the Governance and Management og Enterprise IT s. 28*
[32] ISACA: *Cobit 5 – Enabling Processes s. 19*

sultat af en enabler. Derudover har hver enabler en livcyklus fra de anskaffes til de afskaffes. Den sidste dimension er den tidligere nævnte "good pratices", som understøtter opnåelsen af enabler mål. "Good practices" sikrer eksempler og foreslag til, hvordan virksomheden effektivt kan implementere disse enablers, samt hvilken metode som er nødvendig. Cobit 5 leverer en "good practice" for processer. Virksomheden forventer et positivt resultat ved anvendelse af enablers, og for at opnå dette er det nødvendigt med spørgsmål, som: Er interessenternes behov dækket? Er enabler målene opnået? Er enablernes livcyklus håndteret? Er der foretaget "good practice"?[33]

11 Princip 5: Adskille Governance fra Management

Cobit 5 frameworket differentierer mellem governance og management. Disse omfatter forskellige aktiviteter, kræver forskellig virksomhedsstruktur og repræsenterer forskellige formål. Governance sikrer, at interessenternes behov, vilkår og muligheder bliver vurderet, og for at fastsætte om de aftalte virksomhedsmål opnås, opsættes der bestemmelser gennem prioritering og beslutningstagning samt ved at overvåge præstationer og compliance mod aftalte bestemmelser og mål. I virksomheder varetages governance ofte af virksomhedens bestyrelse. Management planlægger, udfører, driver og overvåger aktiviteter i sammenhold med de bestemmelser, som er nedsat af personerne, der udøver governance, for at opnå virksomhedens mål. I virksomheder er det den daglige ledelse, der ofte udfører management.

Cobit 5 anbefaler, at virksomheder implementerer governance- og managementprocesser så fokusområderne for governance og management bliver behandlet. Governanceprocessernes fokusområder er *Evaluate, Direct & Monitor* og managementprocessernes fokusområder er *Plan, Build, Run & Monitor*. En virksomhed kan tilpasse disse processer, så de håndterer governance- og managementmålene. Cobit 5 inkluderer en procesreferencemodel, som i detaljer definerer og beskriver governance- og managementprocesser. Denne vil blive gennemgået senere i afhandlingen og repræsenterer processer, som ofte eksisterer i virksomheder i relation til it aktiviteter. Denne procesreferencemodel er ikke den eneste mulige model, og hver virksomhed burde definere tilpassede processer til virksomheden, hvor virksomhedens situation vurderes og overvejes. At integrere en operationel model og en fælles tilgangsvin-

[33] ISACA: *Cobit 5 – A Business Framework for the Governance and Management og Enterprise IT s. 29*

kel til it aktiviteter for hele virksomheden er nødvendig for optimal governance. Det er behjælpeligt til en ensartethed for måling og overvågning af it præstationer, at sikre it sikkerhed og at kommunikere med virksomhedens serviceleverandører.[34]

12 Implementeringsvejledning

For at opnå optimal værdi af Cobit 5 frameworket er det nødvendigt at være opmærksom på, at frameworket tilpasses virksomhedens behov. Hver implementeringstilgang har udfordringer som blandt andet styring af ændringer i virksomhedens kultur og adfærd. ISACA har udarbejdet publikationen *Cobit 5 Implementation*, som er baseret på en kontinuerlig livcyklusforbedring. Publikationen er tiltænkt som en vejledning til at undgå faldgruber, levere "good practices" og bidrage til et positivt resultat.

Hver virksomhed skal derfor designe en implementeringsvejledning, der er tilpasset dennes behov. Denne skal designes så vejledningen er optimal for såvel virksomhedens interne miljø som virksomhedens eksterne miljø. Dette omfatter blandt andet virksomhedens etik og kultur, compliance, værdier, governancepolitikker, risikoappetit, ressourcer og brancheforhold.

Den optimale tilgang til governance og management af virksomhedens it vil være individuelt fra virksomhed til virksomhed, og Cobit 5 er understøttet af andre standarder og frameworks inden for it, hvor det ligeledes er nødvendigt at tilpasse den enkelte virksomheds behov. For at opnå en optimal implementering skal der sikres en effektiv kommunikation og tilgang til ændringerne, den øverste ledelse skal udvise initiativ og opbakning omkring ændringerne, og der skal fokuseres på de fordelagtigste områder, som er enklest at implementere.[35]

It relaterede initiativer mislykkes ofte på grund af utilstrækkelig styring, opbakning, forsømmelse af de forskellige interessenter og manglende opbakning fra interessenterne. Ved at udnytte enablers burde virksomhedens reelle behov blive håndteret. Eventuelle faldgruber skal identificeres og accepteres af

[34] ISACA: *Cobit 5 – A Business Framework for the Governance and Management og Enterprise IT s. 31+32*
[35] ISACA: *Cobit 5 – A Business Framework for the Governance and Management og Enterprise IT s. 35*

den daglige ledelse som områder, der er nødvendige at håndtere. Engagement fra de forskellige interessenter skal indhentes fra begyndelsen af implementeringen, og for at opnå dette skal gennemførelsen af mål og fordele udtrykkes i forretningsbetingelserne og sammenfattes i en businesscase. Når engagementet fra interessenterne er opnået kan de nødvendige ressourcer anvendes til at understøtte implementeringen.[36]

Der eksisterer faktorer, der kan indikere, at governance og management af virksomhedens it ikke fungere tilstrækkelige. Ved at anvende "pain point" eller "trigger events", som begyndelsen til en implementering af virksomhedens governance- og managementforbedring samt gennemførelse af nye initiativer, kan virksomheden opnå fordele på de områder, som ikke fungerede optimalt. Eksempler på "pain points" for virksomheder er mislykkede initiativer, øget it omkostninger, spildte ressourcer, budgetoverskridelse og for kompleksanvendte it modeller. Derudover eksisterer andre begivenheder, der skal fokuseres på i virksomhedens interne og eksterne miljø i forbindelse med governance og management af virksomhedens it. Eksempelvis nye lovgivningsmæssige krav, ændringer i branchen, økonomien og konkurrencesituationen eller ny teknologi, som har betydning for virksomheden. [37]

12.1 Livscyklus

Implementeringslivscyklussen sikrer en måde, hvorpå virksomheder kan håndtere udfordringerne, der ofte opstår, når nye initiativer skal implementeres. De tre relaterede komponenter i livcyklussen er kernen, som en kontinuerlig forbedring, ændringshåndtering og programstyring. Disse komponenter inddeles i syv faser:

1. Denne fase begynder med at anerkende og acceptere, at der foreligger et behov for implementering eller forbedring af initiativer. Den identificerer virksomhedens nuværende "pain points" og udløser ønsket om ændring på managementniveau.
2. Denne fase er fokuseret på at definere anvendelsesområdet for implementeringen eller forbedringen af initiativerne ved at anvende Cobit 5's mapping af virksomhedens mål, som fører til it

[36] ISACA: *Cobit 5 – A Business Framework for the Governance and Management og Enterprise IT s. 36*
[37] ISACA: *Cobit 5 – A Business Framework for the Governance and Management og Enterprise IT s. 36*

relaterede mål, der senere fører til de tilhørende processer. Derudover overvejes mulige risici så der fokuseres på de mest optimale processer.

3. I denne fase bliver forbedringsmålene fastsat, efterfulgt af en analyse til at identificere faldgruber samt potentielle løsninger. Initiativer burde inddeles efter prioritet, så det muliggør fordelagtige løsninger.
4. I denne fase planlægges praktiske løsninger ved at definere projekter, som er understøttet af businesscases, og der udformes en ændringsplan for implementeringen.
5. Den fundne løsningsmodel bliver i denne fase implementeret. Måling kan defineres og overvågning etableres ved at anvende Cobit 5's mål for at sikre, implementeringen kontinuerligt er i overensstemmelse virksomheden. For at opnå denne fase på en fordelagtig måde, er det nødvendigt, at den øverste ledelse fremviser engagement, og interessenterne er involveret.
6. Denne fase fokuserer på driften af de nye eller forbedrede enablers, samt der fokuseres på overvågning af opnåelse af de forventede resultater.
7. I denne fase revideres den samlede succes af initiativet, samt yderligere krav til governance og management af virksomhedens it identificeres.

Livcyklussen bør være en kontinuerlig proces til virksomhedens tilgang af governance og management af it.[38]

13 Process Capability Model

Virksomheder der anvender Cobit 4.1, Risk IT og Val IT er bekendte med modenhedsmodellen, som er inkluderet i disse frameworks. Denne model anvendes til at måle virksomhedens nuværende it relaterede processer for at definere det ønskede modenhedsniveau, så forskellen mellem disse kan fastlægges. Dette muliggør, at virksomheden kan etablere løsningsforslag til forbedring af processerne, så de opnår det ønskede modenhedsniveau.

Cobit 5 inkluderer i stedet en "Proces Capability Model", som opnår samme overordnede mål for procesvurderingen og understøttelse af procesforbedring, altså sikre en metode til at måle præstationerne

[38] ISACA: *Cobit 5 – A Business Framework for the Governance and Management og Enterprise IT s. 38*

fra governance- eller managementprocesserne så områderne, hvor forbedring er nødvendigt identificeres. Dog er processer blot én af Cobit 5's syv enablers, og det er nødvendigt med en vurdering af samtlige af virksomhedens enablers.[39]

Cobit 5's "Proces Capability Model" er inddelt i seks egnethedsniveauer for, hvornår en proces er opnået:

- *Ufuldstændig proces (0):* På dette niveau er processen ikke implementeret eller opfylder ikke hensigten med processen.
- *Udført proces (1):* Den gennemførte proces opnår på dette niveau ikke formålet med processen.
- *Håndteret proces (2):* Den udførte proces på det foregående niveau er nu implementeret på et planlagt, overvåget og justeret niveau, og processen er tilpas etableret, kontrolleret og opretholdt.
- *Etableret proces (3):* Processen fra foregående niveau bliver på dette niveau implementeret ved at anvende en defineret proces, der opnår de ønskede resultater.
- *Forudsigelig proces (4):* Den etablerede proces fra foregående niveau fungerer nu indenfor de definerede grænser for at opnå de ønskede resultater.
- *Optimeret proces (5):* Den forudsigelige proces fra foregående niveau er kontinuerlig forbedret så processen opfylder de nuværende og planlagte virksomhedsmål.

Hvert egnethedsniveau kan kun realiseres, hvis det foregående niveau er fuldt opnået. Derudover er der for virksomheder forskel på at realisere niveau 1 og en af de højere liggende niveauer, da opnåelse af dette niveau for en virksomhed alene kan anses som en bedrift. Hver virksomhed skal bestemme det ønskede niveau for processerne på baggrund af en cost/benefit vurdering.

Der er forskel på Cobit 4.1's modenhedsniveau og Cobit 5's egnethedsniveau ved, at målene for at opnå et højere liggende niveau i Cobit 5 er vanskeligere at opnå end i Cobit 4.1. Processer i Cobit 4.1 kan

[39] ISACA: *Cobit 5 – A Business Framework for the Governance and Management og Enterprise IT s. 41*

realiseres på niveau 1 eller 2 uden fuldstændig opnåelse af alle processens mål, hvor samme anstrengelse i Cobit 5 vil resultere i realisering af niveau 0 eller 1.[40]

14 Cobit 5 - Processerne

Cobit 5 definerer i alt 37 processer for styring af virksomheds it, heraf fem governanceprocesser på domænet *Evaluate, Dirct & Monitor* (EDM) og 32 managementprocesser fordelt på fire domæner: *Align, Plan & Organise* (APO), *Build, Acquire & Implement* (BAI), *Deliver, Service & Support* (DSS) og *Monitor, Evaluate & Assess* (MEA). *Bilag 3* illustrerer en oversigt over de forskellige domæner og processer, og i det følgende vil en beskrivelse af processerne blive gennemgået.

14.1 Evaluate, Direct & Monitor.

14.1.1 EDM01 – Ensure Governance Framework Setting and Maintenance

Denne proces har til formål at sikre, at it relaterede beslutninger er i overensstemmelse med virksomhedens forretningsstrategi og mål. Processerne har ligeledes til formål at sikre at tilsyn med it relaterede processer bliver ført effektivt og gennemskueligt, i compliance med lovepligtige og regulerede krav samt at governance kraverne til bestyrelsen opfyldes. Underprocesserne er:

- EDM01.01: Evaluere governancesystemet.
- EDM01.02: Dirigere governancesystemet.
- EDM01.03: Overvåge governancesystemet.[41]

14.1.2 EDM02 – Ensure Benefits Delivery

Formålet med denne proces er at sikre en optimal værdi fra it initiativer, service og aktiver, omkostningseffektiv levering af løsninger og service og et pålideligt og akkurat billede af virksomhedens omkostninger og fordele således, at forretningsbehovene understøttes effektivt. Underprocesserne er:

[40] ISACA: *Cobit 5 – A Business Framework for the Governance and Management og Enterprise IT s. 43*
[41] ISACA: *Cobit 5 – Enabling Processes s. 31-33*

- EDM02.01: Evaluere værdioptimering.
- EDM02.02: Dirigere værdioptimering.
- EDM03.03: Overvåge værdioptimering.[42]

14.1.3 EDM03 – Ensure Risk Optimisation

Formålet med denne proces er at sikre, at it relaterede forretningsrisici ikke overstiger risikoappetitten og toleranceniveauet, at konsekvensen af it relaterede hændelser er identificeret og styret samt at potentialet for compliance fejl er minimeret. Underprocesserne er::

- EDM03.01: Evaluere risikostyring.
- EDM03.02: Dirigere risikostyring.
- EDM03.03: Overvåge risikostyring.[43]

14.1.4 EDM04 – Ensure Ressource Optimisation

Denne proces har til formål at sikre, at forretningens behov for ressourcer opnås på mest optimal vis, it omkostninger optimeres, der er en større sandsynlighed for at realisere fordele samt mulighed for tilpasning til fremtidige forandringer. Underprocesserne er::

- EDM04.01: Evaluere ressourcestyring.
- EDM04.02: Dirigere ressourcestyring.
- EDM04.03: Overvåge ressourcestyring.[44]

14.1.5 EDM05 – Ensure Stakeholder Transparency

Denne proces har til formål at sikre, at kommunikationen til interessenterne er effektiv, rettidig og der er etableret en basis for rapportering for derved at øge ydeevnen, identificere forbedringsområder samt

[42] ISACA: *Cobit 5 – Enabling Processes s. 35-37*
[43] ISACA: *Cobit 5 – Enabling Processes s. 39-41*
[44] ISACA: *Cobit 5 – Enabling Processes s. 43-45*

at bekræfte, at it relaterede mål og strategier er i overensstemmelse med forretningsstrategien. Underprocesserne er:

- EDM05.01: Evaluere interessentrapporteringskrav.
- EDM05.02: Dirigere interessentkommunikation og rapportering.
- EDM05.03: Overvåge interessentkommunikation.[45]

14.2 Align, Plan & Organise

14.2.1 APO01 – Manage the IT Management Framework

Formålet med denne proces er at tilvejebringe en konsistent management tilgang for at gøre det muligt at opnå målene for virksomhedens governance. Herunder vejledende principper, som dækker managementprocesser, organisationsstrukturer, roller og ansvar, pålidelige og kontinuerlige aktiviteter samt kompetencer. Underprocesserne er:

- APO01.01: Definere organisationsstrukturen.
- APO01.02: Etablere roller og ansvar.
- APO01.03: Vedligeholde enablers for managementsystemet.
- APO01.04: Kommunikere management mål og retning.
- APO01.05: Optimere placeringen af it funktionen.
- APO01.06: Definere information- og systemejerskab.
- APO01.07: Styre løbende forbedring af processer.
- APO01.08: Sikre compliance med poltikker og procedurer.[46]

14.2.2 APO02 – Manage Strategy

Denne proces har til formål at sikre, at strategiske planer for it er konsistente med forretningsmål, og at målene og det relaterede ansvar er klart og forstået af alle. De strategiske planer skal være konsistente

[45] ISACA: *Cobit 5 – Enabling Processes s 47-48*
[46] ISACA: *Cobit 5 – Enabling Processes s. 51-56*

med de it strategiske muligheder, der er defineret, struktureret og integreret med forretningsplanerne. Underprocesserne er:

- APO02.01: Forstå retningen for virksomheden.
- APO02.02: Vurdere det nuværende miljø, evne og præstation.
- APO02.03: Definere den tilsigtede it kapabilitet.
- APO02.04: Udføre en "gap" analyse.
- APO02:05: Definere den strategiske plan og "road map".
- APO02.06: Kommunikere it strategien og retningen.[47]

14.2.3 APO03 – Manage Enterprise Architecture

Denne proces har til formål at præsentere de forskellige blokke, der danner grundlag for virksomheden og blokkenes relationer såvel som principperne, der vejleder deres design og udvikling over tid. Dette tilvejebringer en standardiseret, lydhør og effektiv levering af operationelle og strategiske mål. Underprocesserne er:

- APO03.01: Udarbejde virksomhedens arkitekturvision.
- APO03.02: Definere referencearkitektur.
- APO03.03: Udvælge muligheder og løsninger.
- APO03.04: Definere arkitekturimplementering.
- APO03.05: Levere virksomhedsarkitekturservice.[48]

14.2.4 APO04 – Manage Innovation

Formålet med at styre innovationen er at opnå en konkurrencemæssig fordel, forretningsinnovation og forbedre operationel effektivitet ved at udnytte informationsteknologiens udvikling. Underprocesserne er:

[47] ISACA: *Cobit 5 – Enabling Processes s. 57-62*
[48] ISACA: *Cobit 5 – Enabling Processes s. 63-67*

- APO04.01: Opsætte et miljø der understøtter innovation.
- APO04.02: Vedligeholde en forståelse af virksomhedsmiljøet.
- APO04.03: Overvåge og scanne teknologimiljøet.
- APO04.04: Vurdere potentialet af fremspirende teknologier og innovative idéer.
- APO04.05: Foreslå hensigtsmæssige yderligere initiativer.
- APO04.06: Overvåge implementeringen og anvendelsen af innovation.[49]

14.2.5 APO05 – Manage Portfolio

Formålet er at optimere præstation af den overordnede portefølje af programmer som reaktion på program- og servicepræstationer samt ændringer i virksomhedsprioriteter og krav. Underprocesserne er:

- APO05.01: Etablere det ønskede investeringsmix.
- APO05.02: Fastlægge tilgængeligheden og kilden til midler.
- APO05.03: Evaluere og udvælge programmer der skal finansieres.
- APO05.04: Overvåge, optimere og rapportere på investeringsportefølje præstationer.
- APO05.05: Vedligeholde porteføljer.
- APO05.06: Styre opnåelse af fordele.[50]

14.2.6 APO06 – Manage Budget and Costs

Formålet med denne proces er at fremme samarbejdet mellem it- og forretningsinteressenter for at tilvejebringe effektiv anvendelse af it relaterede ressourcer. Formålet er derved at give en gennemsigtighed af ansvar for omkostninger og den værdi forretningen opnår fra løsninger og service. Dette gør virksomheden i stand til at foretage informerede beslutninger angående anvendelsen af it løsninger og service. Underprocesserne er:

- APO06.01: Håndtere finansiering og regnskabsførelse.
- APO06.02: Prioritere ressourceallokering.

[49] ISACA: *Cobit 5 – Enabling Processes s. 69-72*
[50] ISACA: *Cobit 5 – Enabling Processes s. 73-77*

- APO06.03: Udarbejde og vedligeholde budgetter.
- APO06.04: Allokere omkostninger.
- APO06.05: Styre omkostninger.[51]

14.2.7 APO07 – Manage Human Ressources

Formålet med denne proces er at optimere den menneskelige ressources evne til at opnå virksomhedens mål. Underprocesserne er:

- APO07.01: Opretholde tilstrækkelig og passende personale.
- APO07.02: Identificere nøgle it personale.
- APO07.03: Vedligeholde kompetencerne hos personalet.
- APO07.04: Evaluere de ansattes jobpræstationer.
- APO07.05: Planlægge og spore anvendelsen af it og forretningens menneskelige ressourcer.
- APO07.06: Håndtere kontraktansatte.[52]

14.2.8 APO08 – Manage Relationships

Formålet med at styre relationerne mellem virksomheden og it er at forbedre resultaterne, forbedre tilliden til it og effektiv anvendelse af ressourcer. Underprocesserne er:

- APO08.01: Forstå forretningsforventninger.
- APO08.02: Identificere muligheder, risici og begrænsninger for it til at forstærke forrentningen.
- APO08.03: Håndtere forretningsrelationen.
- APO08.04: Koordinere og kommunikere.
- APO08.05: Bidrage med input til kontinuerlig forbedring af service.[53]

[51] ISACA: *Cobit 5 – Enabling Processes s. 79-82*
[52] ISACA: *Cobit 5 – Enabling Processes s. 83-87*
[53] ISACA: *Cobit 5 – Enabling Processes s. 89-92*

14.2.9 APO09 – Manage Service Agreements

Denne proces sikre, at it service og serviceniveauer opnår nuværende og fremtidige forretningsbehov. Underprocesserne er:

- APO09.01: Identificere it service.
- APO09.02: Kategorisere it baserede service.
- APO09.03: Definere og klargøre serviceaftaler.
- APO09.04: Overvåge og rapportere serviceniveauer.
- APO09.05: Gennemgå serviceaftaler og kontrakter.[54]

14.2.10 APO10 – Manage Suppliers

Formålet med denne proces er at minimere risikoen relateret til ikke-ydedygtige leverandører og at sikre en konkurrencedygtig prisfastsættelse. Underprocesserne er:

- APO10.01: Identificere og evaluere leverandørrelationer og kontrakter.
- APO10.02: Udvælge leverandører.
- APO10.03: Håndtere leverandørrelationer og kontrakter.
- APO10.04: Håndtere leverandørrisici.
- APO10.05: Overvåge leverandørydeevne og compliance.[55]

14.2.11 APO11 – Manage Quality

Når kvaliteten bliver styret sikres der konsistent levering af løsninger og service, der opnår kvalitetskravene hos virksomheden og opfylder interessenternes behov. Underprocesserne er:

- APO11.01: Etablere et kvalitetsstyringssystem.
- APO11.02: Definere og styre kvalitetsstandarder, kutymer og procedurer.
- APO11.03: Fokusere kvalitetshåndtering af kunder.

[54] ISACA: *Cobit 5 – Enabling Processes s. 93-95*
[55] ISACA: *Cobit 5 – Enabling Processes s. 97-99*

- APO11.04: Foretage kvalitetsovervågning, kontrol og gennemgang.
- APO11.05: Integrere kvalitetshåndtering med løsninger for udvikling og servicelevering.
- APO11.06: Opretholde kontinuerlige forbedringer.[56]

14.2.12 APO12 – Manage Risk

Formålet med denne proces er at integrere styringen af it relaterede risici med virksomhedens overordnede forretningsrisikostyring samt at balancere omkostningerne og fordelene ved styring af it relaterede forretningsrisici. Underprocesserne er:

- APO12.01: Indhente data.
- APO12.02: Analysere risiko.
- APO12.03: Vedligeholde en risikoprofil.
- APO12.04: Formulere risiko.
- APO12.05: Definere en risikostyringshandlingsportefølje.
- APO12.06: Reagere på risiko.[57]

14.2.13 APO13 – Manage Security

Formålet med denne proces er at holde konsekvensen og tilfældet af informationssikkerhedshændelser indenfor virksomhedens risikoappetit. Underprocesserne er:

- APO13.01: Etablere og vedligeholde et informationssikkerhedsstyringssystem.
- APO13.02: Definere og styre en informationssikkerhedsrisiko behandlingsplan.
- APO13.03: Overvåge og gennemgå informationssikkerhedsstyringssystemet.[58]

[56] ISACA: *Cobit 5 – Enabling Processes s. 101-105*
[57] ISACA: *Cobit 5 – Enabling Processes s. 107-111*
[58] ISACA: *Cobit 5 – Enabling Processes s. 113-115*

14.3 Build, Acquire & Implement

14.3.1 BAI01 – Manage Programs and Projects

Styring af programmer og projekter har til formål at opnå forretningsfordele samt reducere risikoen for uventede forsinkelser, omkostninger og værdinedbrydning ved at forbedre kommunikationen til og involveringen af virksomheden og slutbrugerne. Dette sikre værdien og kvaliteten af projektresultaterne og maksimere deres bidrag til investerings- og serviceporteføljen. Underprocesserne er:

- BAI01.01: Opretholde en standardiseret tilgang til program- og projektstyring.
- BAI01.02: Påbegynde et program.
- BAI01.03: Håndtere interessentinvolvering.
- BAI01.04: Udvikle og vedligeholde programplanen.
- BAI01.05: Udgive og udføre programmet.
- BAI01.06: Overvåge, kontrollere og rapportere på programresultaterne.
- BAI01.07: Opstart og påbegyndelse projekter indenfor et program.
- BAI01.08: Planlægge projekter.
- BAI01.09: Styre program- og projektkvalitet.
- BAI01.10: Styre program- og projektrisiko.
- BAI01.11: Overvåge og kontrollere projekter.
- BAI01.12: Styre projektressourcer og arbejdspakker.
- BAI01.13: Afslutte et projekt.
- BAI01.14: Afslutte et program. [59]

14.3.2 BAI02 – Manage Requirements Definition

Formålet med at definere krav er at udvikle optimale løsninger, der opnår forretningsbehov samtidig med minimering af potentielle risiko. Underprocesserne er:

- BAI2.01: Definere og vedligeholde forretningsfunktionelle og tekniske krav.
- BAI2.02: Udføre et tænkt studie og formulere alternative løsninger.

[59] ISACA: *Cobit 5 – Enabling Processes s. 117-127*

- BAI2.03: Styre risikokrav.
- BAI2.04: Opnåelse af accept af krav og løsninger.[60]

14.3.3 BAI03 – Manage Solutions Identification and Build

Formålet med denne proces er at etablere tids- og omkostningseffektive løsninger, der er i stand til at understøtte virksomhedens strategi og operationelle mål. Underprocesserne er:

- BAI03.01: Designe løsninger på højt niveau.
- BAI03.02: Designe detaljerede løsningskomponenter.
- BAI03.03: Udvikle løsningskomponenter.
- BAI03.04: Producere løsningskomponenter.
- BAI03.05: Konstruere løsninger.
- BAI03.06: Udføre kvalitetssikring.
- BAI03.07: Forberede test af løsninger.
- BAI03.08: Udføre test af løsninger.
- BAI03.09: Håndtere ændringer til krav.
- BAI03.10: Opretholde løsninger.
- BAI03.11: Definere it service og vedligeholde serviceporteføljen.[61]

14.3.4 BAI04 – Manage Availability and Capacity

Denne proces har til formål at vedligeholde servicetilgængeligheden, effektiv styring af ressourcer og optimering af systempræstationer gennem forudsigelse af fremtidige præstationer og kapacitetskrav. Underprocesserne er:

- BAI04.01: Vurdere den nuværende tilgængelighed, præstation og kapacitet og udforme en ”baseline” for disse.
- BAI04.02: Vurdere konsekvensen for virksomheden.

[60] ISACA: *Cobit 5 – Enabling Processes s. 129-132*
[61] ISACA: *Cobit 5 – Enabling Processes s. 133-139*

- BAI04.03: Planlægge efter nye og ændrede servicekrav.
- BAI04.04: Overvåge og gennemgå tilgængeligheden og kapaciteten.
- BAI04.05: Undersøge og håndtere tilgængeligheden, præstationen og kapacitetsproblemer.[62]

14.3.5 BAI05 – Manage Organisational Change Enablement

Formålet med denne proces er at forberede og forpligte interessenterne til virksomhedsforandringer samt reducere risikoen for fejl. Underprocesserne er:

- BAI05.01: Etablere ønsket om forandring.
- BAI05.02: Forme et effektivt implementeringsteam.
- BAI05.03: Kommunikere den ønskede vision.
- BAI05.04: Autorisere rolleindehavere og identificere kortsigtet vinding.
- BAI05.05: Muliggøre operation og anvendelse.
- BAI05.06: Forankre nye tilgange.
- BAI05.07: Bevare forandringer.[63]

14.3.6 BAI06 – Manage Changes

Denne proces muliggør at tilvejebringe hurtig og pålidelig levering af forandringer til virksomheden samt reducere risikoen for negativ påvirkning af stabiliteten eller integriteten af det forandrede miljø. Underprocesserne er:

- BAI06:01: Evaluere, prioritere og autorisere forandringsforespørgsler.
- BAI06:02: Håndtere forandringer ved nødstilfælde.
- BAI06:03: Spore og rapportere forandringsstatus.
- BAI06:04: Afslutte og dokumentere forandringerne.[64]

[62] ISACA: *Cobit 5 – Enabling Processes s. 141-144*
[63] ISACA: *Cobit 5 – Enabling Processes s. 145-148*
[64] ISACA: *Cobit 5 – Enabling Processes s. 149-151*

14.3.7 BAI07 – Manage Change Acceptance and Transitioning

Formålet med denne proces er at implementere løsninger sikkert og i overensstemmelse med de aftalte forventninger og resultater. Underprocesserne er:

- BAI07.01: Etablere en implementeringsplan.
- BAI07.02: Planlægge forretningsproces-, system- og datakonvertering.
- BAI07.03: Planlægge accepteringstest.
- BAI07.04: Etablere et testmiljø.
- BAI07.05: Udføre accepteringstest.
- BAI07.06: Overføre til produktion og håndtere udgivelse.
- BAI07.07: Tildele tidlig produktionsstøtte.
- BAI07.08: Udføre en før-implementeringsgennemgang.[65]

14.3.8 BAI08 – Manage Knowledge

Denne proces har til formål at levere den viden til virksomhedens personale, som de har behov i deres arbejdsaktiviteter, samt tilvejebringe den nødvendige viden for at tage informerede beslutninger og styrke produktiviteten. Underprocesserne er:

- BAI08.01: Pleje og muliggøre en videndelingskultur.
- BAI08.02: Identificere og klassificere kilder til information.
- BAI08.03: Organisere og kontekstualisere information til viden.
- BAI08.04: Anvende og del viden.
- BAI08.05: Evaluere og udfasning af information.[66]

14.3.9 BAI09 – Manage Assets

Formålet med denne proces er at redegøre for alle it aktiver og optimere værdien, der fremkommer fra disse aktiver. Underprocesserne er:

[65] ISACA: *Cobit 5 – Enabling Processes s. 153-158*
[66] ISACA: *Cobit 5 – Enabling Processes s. 159-161*

- BAI09.01: Identificere og registrere nuværende aktiver.
- BAI09.02: Håndtere kritiske aktiver.
- BAI09.03: Håndtere aktivets livscyklus.
- BAI09:04: Optimere aktivomkostninger.
- BAI09.05: Håndtere licenser.[67]

14.3.10 BAI10 – Manage Configuration

Formålet med denne proces er at levere tilstrækkelig information angående serviceaktiver til at muliggøre effektiv styring af service, vurdere konsekvensen af ændringer og håndtere servicehændelser. Underprocesserne er:

- BAI10.01: Etablere og vedligeholde en konfigurationsmodel.
- BAI10.02: Etablere og vedligeholde et konfigurationsdepot og "baseline"
- BAI10.03: Vedligeholde og kontrollere konfigurationselementer.
- BAI10.04: Producere status- og konfigurationsrapporter.
- BAI10.05: Verificere og gennemgå integriteten af konfigurationsdepotet.[68]

14.4 Deliver, Service & Support

14.4.1 DSS01 – Manage Operations

Formålet er med denne proces at levere it operationelle serviceresultater som planlagt. Underprocesserne er:

- DSS01.01: Udføre driftsprocedurer.
- DSS01.02: Styre outsourcede it service.
- DSS01.03: Overvåge it infrastruktur.

[67] ISACA: *Cobit 5 – Enabling Processes s. 163-166*
[68] ISACA: *Cobit 5 – Enabling Processes s. 167-169*

- DSS01.04: Håndtere miljøet.
- DSS01.05: Styre faciliteter.[69]

14.4.2 DSS02 – Manage Service Requests and Incidents

Formålet med denne proces er at opnå forbedret produktivitet samt minimere forstyrrelser gennem hurtig løsning af brugerforespørgsler og hændelser. Underprocesserne er:

- DSS02.01: Definere hændelse- og serviceforespørgselsklassifikationsskemaer.
- DSS02.02: Registrere, klassificere og prioritere forespørgsler og hændelser.
- DSS02.03: Verificere, acceptere og udfylde serviceforespørgsler.
- DSS02.04: Undersøge, diagnostikere og allokere hændelser.
- DSS02.05: Udbedring og genoprettelse efter hændelser.
- DSS02.06: Afslutte serviceforespørgsler og hændelser.
- DSS02.07: Spore status og producere rapporter.[70]

14.4.3 DSS03 – Manage Problems

Denne proces har til formål at øge tilgængeligheden, forbedre serviceniveauer, reducere omkostninger, forbedre kundekomforten og tilfredsheden ved at reducere antallet af driftsproblemer. Underprocesserne er:

- DSS03.01: Identificere og klassificere problemer.
- DSS03.02: Undersøge og diagnostikere problemer.
- DSS03.03: Optage kendte fejl.
- DSS03.04: Udbedring og afslutning af problemer.
- DSS03.05: Udføre proaktiv problemstyring.[71]

[69] ISACA: *Cobit 5 – Enabling Processes s. 171-175*
[70] ISACA: *Cobit 5 – Enabling Processes s. 177-180*
[71] ISACA: *Cobit 5 – Enabling Processes s. 181- 183*

14.4.4 DSS04 – Manage Continuity

Denne proces har til formål at sikre forsættelse af kritiske forretningsoperationer i tilfælde af signifikante forstyrrelser og vedligeholde tilgængeligheden af information på et niveau, der er acceptabelt for virksomheden. Underprocesserne er:

- DSS04.01: Definere forretningskontinuitetspolitikken, mål og anvendelsesområde.
- DSS04.02: Vedligeholde en kontinuitetsstrategi.
- DSS04.03: Udvikle og implementere en forretningskontinuitetsreaktion.
- DSS04.04: Træne, teste og gennemgå forretningskontinuitetsplanen.
- DSS04.05: Gennemgå, vedligeholde og forbedre kontinuitetsplanen.
- DSS04.06: Udføre kontinuitetsplanstræning.
- DSS04.07: Håndtere back-up aftaler.
- DSS04.08: Udføre efter-genoptagelsesgennemgang.[72]

14.4.5 DSS05 – Manage Security Services

Formålet med denne proces er at minimere forretningskonsekvensen af sårbarheder og hændelser i forbindelse med driftsinformationssikkerhed. Underprocesserne er:

- DSS05.01: Beskytte mod malware.
- DSS05.02: Håndtere netværks- og forbindelsessikkerhed.
- DSS05.03: Håndtere slutpunktssikkerhed.
- DSS05.04: Håndtere brugeridentitet og adgang.
- DSS05.05: Håndtere den fysiske adgang til it aktiver.
- DSS05.06: Håndtere følsomme dokumenter og outputapparater.
- DSS05.07: Overvåge infrastrukturen for sikkerhedsrelaterede begivenheder.[73]

[72] ISACA: *Cobit 5 – Enabling Processes s. 185-189*
[73] ISACA: *Cobit 5 – Enabling Processes s. 191-195*

14.4.6 DSS06 – Manage Business Process Controls

Formålet med denne proces er at vedligeholde informationsintegritet og sikkerhed af informationsaktiver, der håndteres i forretningsprocesser i virksomheden eller som er outsourcet. Underprocesserne er:

- DSS06.01: Sammenholde kontrolaktiviteter indlagt i forretningsprocesser med forretningsmål.
- DSS06.02: Kontrollere behandlingen af information.
- DSS06.03: Håndtere roller, ansvar, adgangsrettigheder og autoritetsniveauer.
- DSS06.04: Håndtere fejl og undtagelser.
- DSS06.05: Forsikre sporbarheden af informationsevents og ansvarligheder.
- DSS06.06: Sikre informationsaktiver.[74]

14.5 Monitor, Evaluate & Assess

14.5.1 MEA01 – Monitor, Evaluate and Assess Performance and Conformance

For denne proces er formålet at tilvejebringe gennemsigtighed af præstationer og overensstemmelser samt at fremme opnåelse af mål. Underprocesserne er:

- MEA01.01: Etablere en overvågningstilgang.
- MEA01.02: Fastsætte præstation- og overensstemmelsesmål.
- MEA01.03: Samle og bearbejde præstation- og overensstemmelsesdata.
- MEA01.04: Analysere og rapportere på præstation.
- MEA01.05: Sikre implementeringen af korrigerende handlinger.[75]

14.5.2 MEA02 – Monitor, Evaluate and Assess the System of Internal Control

Formålet med denne proces er at opnå gennemsigtighed for nøgle interessenter angående tilstrækkeligheden af systemet for interne kontroller. Derigennem at opnå tillid til operationer, tillid til opnåelse af virksomhedens mål og en korrekt forståelse af resterende risici. Underprocesserne er:

[74] ISACA: *Cobit 5 – Enabling Processes s. 197- 200*
[75] ISACA: *Cobit 5 – Enabling Processes s. 203-206*

- MEA02.01: Overvåge interne kontroller.
- MEA02.02: Gennemgå effektivteten af forretningsproceskontroller.
- MEA02.03: Udføre selvvurderingskontroller.
- MEA02.04: Identificere og rapportere kontrolmangler.
- MEA02.05: Sikre at forsikringsgivere er uafhængige og kvalificerede.
- MEA02.06: Planlægge forsikringsinitiativer.
- MEA02.07: Afgrænse forsikringsinitiativerne.
- MEA02.08: Udføre forsikringsinitiativer.[76]

14.5.3 MEA03 – Monitor, Evaluate and Assess Compliance with External Requirements

Denne proces har til formål at sikre, at virksomheden er i compliance med alle relevante eksterne krav. Underprocesserne er:

- MEA03.01: Identificere eksterne compliance krav.
- MEA03.02: Optimere responsen på eksterne krav.
- MEA03.03: Bekræfte ekstern compliance.
- MEA03.04: Opnå garanti for ekstern compliance.[77]

[76] ISACA: *Cobit 5 – Enabling Processes s. 207-211*
[77] ISACA: *Cobit 5 – Enabling Processes s. 213-215*

Enterprise Risk Management

Dette afsnit er medtaget for at redegøre for Committee of Sponsoring Organizations of the Treadway Commissions (COSO): *Enterprise Risk Management – Intergrated Framework* med det formål at vurdere om dette framework understøtter Cobit 5's processer og i givet fald, hvilke processer det omhandler.

Internal Control – Intergrated framework er udarbejdet af COSO for, at virksomheder kan vejledes i at vurdere og forbedre de interne kontrolsystemer, som eksisterer i virksomheden. Dette framework er efterfølgende blevet indarbejdet i lovgivning samt standarder. På den måde kan virksomheder styre deres nuværende aktiviteter ligesom dette framework er behjælpelig til at opfylde virksomhedens fastlagte målsætninger.

I 2001 indledte COSO og PricewaterhouseCoopers et nyt framework, som virksomheder burde anvende til at evaluere og forbedre virksomhedens risikostyring. Dette framework blev udarbejdet på baggrund af virksomhedernes behov for at identificere, vurdere og håndtere risici, som udfordrede virksomhederne, og for at give virksomhederne et fælles værktøj og vejledning til at forbedre risikostyringen i virksomheden.

En udfordring for ledelsen kan være at fastslå, hvor højt et risikoniveau virksomheden kan håndtere. Dette Enterprise Risk Management (ERM) – Integrated Framework udvider den interne kontrol fra Internal Control – Intergrated framework, som derved fokuserer mere omfattende på risikostyringsemnet, og derved indgår den interne kontrol i risikostyringen.[78]

Dette framework anlægger det perspektiv, at virksomheders formål er at tilføre værdi for virksomhedens interessenter. I denne værdi for interessenterne skal virksomheden tage stilling til, hvor meget usikkerhed virksomheden vil acceptere for at opnå det mest fordelagtige alternativ for interessenterne. Denne usikkerhed indeholder både risici og muligheder og har indvirkning på interessentværdien, da

[78] COSO: *Enterprise Risk Management —Integrated Framework: Executive Summary and Framework s. V*

disse har mulighed for at påvirke den i en såvel negativ som positiv retning. Ledelsen har derfor, med dette framework, mulighed for at håndtere disse risici og muligheder, der eksisterer i virksomheden, på en effektiv og fordelagtig måde. Strategier og mål kan med fordel øge værdien i virksomheden, da disse tilfører en balance mellem målopfyldelse og muligheder, som skal tilføre optimalt vækstpotentiale med de ressourcer, der figurerer i virksomheden.

Begivenheder kan have såvel negativ indflydelse på virksomheden som positiv indflydelse. Den negative indflydelse repræsenterer risici, der kan forringe værdiskabelsen i virksomheden samt eventuelt mindske den eksisterende værdi. På den anden side kan den positive indflydelse fra begivenheder være en mulighed for virksomheden, som denne kan udnytte til dens fordel ved enten at udligne den negative effekt, støtte værdiskabelse for virksomheden eller hjælpe til opfyldelse af den overordnede målsætning i virksomheden.[79]

Det er muligt med ERM at tilføre sammenhæng mellem virksomhedens risikoappetit og strategi ved, at ledelsen håndterer potentielle risici ved at vurdere virksomhedens risikoappetit igennem mål og andre strategiske handlinger. Endvidere gør dette framework det muligt at identificere og derved vælge forskellige reaktioner på at minimere, undgå eller acceptere den identificerede risiko, som ligeledes kan have tværorganisatorisk karakter. Samtidig bliver det muligt at reducere potentielle operationelle tab og udgifter, når virksomheden kan identificere tænkelige begivenheder så virksomheden, derved kan være opmærksom på eventuelle tab og udgifter, som begivenheden medfører. Når virksomheden med ERM har mulighed for at identificere potentielle risici bliver virksomheden herigennem ligeledes opmærksom på de muligheder, som foreligger, og derved udnytte disse muligheder så det får positiv indvirkning på virksomheden. Derved bliver virksomheden også i stand til at forbedre sin kapitalspredning ved at fastsætte virksomhedens behov. Overordnet set er dette framework behjælpelig med at undgå faldgruber og overraskelser, som virksomheden kunne blive udsat for og i stedet finde vejledning til at få det optimale ud af en given situation.[80]

Dette framework omhandler disse risici og muligheder, der eksisterer for virksomheder, og virksom-

[79] COSO: *Enterprise Risk Management —Integrated Framework: Executive Summary and Framework* s. 2
[80] COSO: *Enterprise Risk Management —Integrated Framework: Executive Summary and Framework* s. 1

hedens risikostyring er her defineret som: ”*Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”*[81] Denne definition fokuserer således på målopfyldelse, som virksomheden gennem en fastsat vision og mission tilstræber at opnå gennem strategiske mål og strategiudvælgelse. Dette framework har en målsætningsorienteret tilgang for at opnå virksomhedens mål og opstiller derfor fire kategorier:

- Strategi
- Drift
- Rapportering
- Lovgivning

Kategorien strategi er virksomhedens overordnede mål, der understøtter missionen, hvor driften er virksomhedens effektivisering af de aktuelle ressourcer. Kategorien rapportering redegør for om rapporteringen er pålidelig, tilsvarende refererer lovgivning til om der eksisterer overensstemmelse mellem de gældende love og standarder på de enkelte områder. Disse kategorier kan være overlappende, og derved kan et mål tillægges flere kategorier, ligesom forskellige enheders behov kan hører til forskellige ansvarsområde i virksomheden. De to første kategorier er ikke udelukkende underlagt virksomhedens kontrol, men en virksomhed der anvender ERM kan nå at blive opmærksom på begivenheder, som har indvirkning på virksomhedens overordnede målopfyldelse, og derved få det optimale ud af situationen.[82]

Udover de fire kategorier består dette framework af otte fælles forbundet elementer. Disse elementer er en del af ledelsesprocessen og er en måde, hvorpå ledelsen kan administrere virksomheden. Dog kan det ikke konstateres, at et element påvirker det næste. Det skal i stedet gennemgås som en kontinuerlig proces, der kan have flere udfald, samt at elementerne kan have indflydelse på hinanden.

[81] COSO: *Enterprise Risk Management —Integrated Framework: Executive Summary and Framework* s. 2
[82] COSO: *Enterprise Risk Management —Integrated Framework: Executive Summary and Framework* s. 3

- *Internt miljø:* I dette element skabes der overblik over miljøet i form af atmosfære, etiske værdier, omgangstone og arbejdsforhold medarbejderne imellem samt den organisatoriske opbygning af virksomheden. Det interne miljø er grundlaget for, hvordan medarbejderne i virksomheden opfatter de eventuelle risici.
- *Målsætning:* For at ledelsen kan identificere begivenheder, som kan influere virksomhedens opsatte mål, er de nødt til at have opsat nogle mål for virksomheden. Dette framework sikrer, at ledelsen opstiller relevante mål, som understøtter virksomhedens overordnede mission, ligesom de skal være i overensstemmelse med den eksisterende risikoappetit i virksomheden.
- *Identificering af begivenheder:* Dette relaterer til interne og eksterne begivenheder, som kan have indflydelse på opfyldelse af virksomhedens målsætning. Disse begivenheder skal opdeles i henholdsvis risici eller muligheder for virksomheden.
- *Risikovurdering:* Der vurderes og analyseres på sandsynlige risici for virksomheden, da dette er grundlag for, hvordan de potentielle risici håndteres.
- *Risikoreaktion:* Ud fra risikovurderingen vælger ledelsen om de vil forsøge at undgå, reducere eller om de vil acceptere de konstaterede risici. Alt afhængig af udfaldet udvikles en handlingsmetoden til, hvordan virksomheden skal forene disse risici med virksomhedens risikotolerance samt risikoappetit.
- *Kontrolaktiviteter:* Dette element skal sikre en effektiv reaktion på risici gennem formulerede og aktiverede procedurer samt politikker.
- *Information og kommunikation:* Efterfølgende skal informationen kommunikeres ud til medarbejderne i virksomheden på en effektiv måde således, at den rette information bliver videregivet til de personer, som det er relevant for.
- *Opfølgning:* Risikostyringen i virksomheden skal følges op på, så der på den måde kan udarbejdes modifikationer, hvis dette er nødvendigt.[83]

Disse otte elementer, fire kategorier, samt virksomhedens enheder er i ERM skildret i en tredimensionel kube, hvor elementerne befinder sig i den horisontale række, kategorierne er placeret i den vertikale række og virksomhedens enheder er placeret i den tredje dimension som subsidiær, forretningsenhed, afdeling og virksomhedsniveau. Virksomhederne kan ved at fokusere på denne kube få alle dimensio-

[83] COSO: *Enterprise Risk Management —Integrated Framework: Executive Summary and Framework* s. 4

ner med af dette framework og derved få det optimale ud af deres risikostyring, hvis de forstår at benytte kuben på den korrekte måde. Der kan dog forekomme begrænsninger ved for eksempel menneskelig dømmekraft som grundlag for beslutninger, fejlantagelser eller misforståelser.[84]

[84] COSO: *Enterprise Risk Management —Integrated Framework: Executive Summary and Framework* s. 5

ISO/IEC 27001

Dette afsnit har til formål at præsentere ISO/IEC 27001 på et overordnet niveau for senere at betragte ISO/IEC 27001 i forhold til Cobit 5 frameworket og derigennem vurdere hvilke dele af Cobit 5, der kan understøttes af ISO/IEC 27001.

ISO og IEC er udgiverne af ISO/IEC 27000 serien. Denne serie indeholder blandt andet ISO27001:2007 og ISO 27002:2005. I det følgende vil hver af de to standarder indenfor informationssikkerhed blive gennemgået hver for sig.

ISO/IEC 27001 omhandler etablering, drift, overvågning, revurdering, implementering, vedligeholdelse og forbedring af et ledelsessystem for informationssikkerheden. Standarden fokuserer på en procesorienteret forståelse, der opfordrer brugeren til at:

- Forstå virksomhedens krav til informationssikkerhed samt behovet for at fastsætte politikker og mål for informationssikkerhed.
- Implementerer foranstaltninger der styrer informationssikkerhedsrisici indenfor rammerne af virksomhedens samlede forretningsmæssige risici.
- Overvåge og gennemgå præstationen og effekten af systemet samt fokusere på kontinuerlig forbedring. [85]

For at skabe struktur til alle processerne i denne standard benyttes Plan-Do-Check-Act (PDCA) modellen, som er en model, der sikre, at alle Information Secutity Management System (ISMS) processerne gennemgår faser for planlægning, udførsel, kontrol og handling. Denne ISO/IEC 27001 standard anbefaler, at virksomheden indledende skal etablere mål og politikker for deres ISMS, der støtter op om at styre risiko og forbedre informationssikkerheden i virksomheden. Derefter skal politikkerne implementeres og drives i form af foranstaltninger, processer og procedurer. Herefter skal ISMS'et overvåges og revurderes ved eksempelvis måling af procespræstationer, og afslutningsvist

[85] *ISO/IEC 27001* s. V

skal ISMS'et vedligeholdes og forbedres baseret på resultater af foregående faser.[86]

Et af hovedelementerne i denne standard er, at virksomheden skal anvende ISMS, så dette er i overensstemmelse med virksomhedens øvrige forretningsaktivitet og relaterede risici.

ISO/IEC 27001 angiver en model til, hvordan en virksomhed kan styre deres informationssikkerhed for derved at mindske risikoen, som denne tilfører virksomheden.[87]

Ved etablering af ISMS-systemet skal virksomheden definere anvendelsesområdet, definere politikken, definere en risikovurderingsmetode til virksomheden og identificere risiciene af ISMS'et.[88] Herefter skal virksomheden analysere og bedømme risiciene, vurdere mulighederne for risikohåndtering samt vælge hvilke styringsmål og foranstaltninger de vil anvende til risikohåndtering. Ledelsen skal godkende de foreslåede risici, så der kan indhentes tilladelse til at implementere og drive ISMS-systemet, og afslutningsvist udarbejde en erklæring om anvendelse og opfyldelse.[89]

Efter virksomheden har gennemgået ovenstående skal den implementere og drive det etablerede ISMS-system samt overvåge, revurdere, vedligeholde og forbedre systemet ved at anvende PDCA. Derudover indeholder ISO/IEC 27001 ligeledes krav angående dokumentation der primært omhandler, at det er nødvendigt at sikre, at alle handlinger er sporbare og de registrerede resultater er repeterbare.[90]

ISO/IEC 27001 angiver ligeledes krav til ledelsens ansvar, der omhandler, hvilke forpligtelser ledelsen har, og hvordan de bør styre ressourcerne. Angående ressourcer er det relevant, at den rette mængde ressourcer anskaffes for at udføre alle PDCA-opgaverne i ISMS-systemet, og at den menneskelige ressource opretholder sin værdi i form af uddannelse, bevidsthed og kompetence.[91]

Virksomheden skal kontinuerligt foretage intern revision af deres ISMS-system for at vurdere om

[86] *ISO/IEC 27001 s. vi*
[87] *ISO/IEC 27001 s. 3*
[88] *ISO/IEC 27001 s. 4*
[89] *ISO/IEC 27001 s. 5*
[90] *ISO/IEC 27001 s. 7*
[91] *ISO/IEC 27001 s. 9*

styringsmål, foranstaltninger, processer og producere opfylder compliance, er effektivt implementeret og vedligeholdt og fungerer som forventet. Ledelsen skal på baggrund af oparbejdet information mindst én gang årligt evaluere virksomhedens ISMS-system og derved sikre, at systemet stadig er fyldestgørende for virksomheden. Dette bliver sikret ved, at ledelsen udformer en plan for, hvordan ISMS-systemet skal reguleres eller forbedres i fremtiden. Virksomheden skal ifølge denne standard kontinuerligt forbedre deres ISMS-system ved korrigerende og forebyggende handlinger.[92]

15. Styringsmål og Foranstaltninger i ISO/IEC 27001

I det følgende præsenteres en overskuelig liste af styringsmål og foranstaltninger i ISO/IEC 27001, med det formål at aligne disse med processerne i Cobit 5. Styringsmålene og foranstaltningerne er direkte afledt af og koordineret med styringsmål og foranstaltninger i ISO/IEC 27002. Nedenstående er udarbejdet på baggrund af ISO/IEC 27001 Annex A.[93]

15.1 Sikkerhedspolitik

Informationssikkerhedspolitik: Målet er, at ledelsen angiver retning for og understøttelse af informationssikkerhed i virksomheden, som desuden er i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter. [94]

15.2 Organisering af informationssikkerhed

Intern Organisering: Målet er, at informationssikkerheden i virksomheden styres.

Eksterne parter: Målet er, at der opnås sikkerhed for virksomhedens informationer og tilhørerende behandlingsudstyr som eksterne parter håndterer eller har adgang til.

[92] *ISO/IEC 27001 s. 11*
[93] *ISO/IEC 27001 s. 13*
[94] *ISO/IEC 27001 s. 13*

15.3 Styring af aktiver

Ansvar for aktiver: Målet er en optimal beskyttelse af virksomhedens aktiver bliver opnået og opretholdt.

Klassifikation af information: Målet er at sikre, at informationer får et optimalt beskyttelsesniveau. [95]

15.4 Sikkerhed af menneskelige ressourcer (medarbejdersikkerhed)

Inden ansættelse: Målet er at sikre, at medarbejdere, kontrahenter og eksterne brugere er egnede til de opgaver de skal håndtere og forstår deres ansvar. Derforuden at nedsætte risikoen for bedrageri, tyveri eller misbrug af faciliteter.

Under ansættelsen: Målet er at sikre, at virksomhedens medarbejdere, kontrahenter og eksterne brugere er bevidste omkring trusler mod sikkerheden, deres ansvar og tilhørerende pligter, formår at understøtte virksomhedens sikkerhedspolitik når de udfører deres arbejde og at nedsætte risikoen for menneskelige fejl.

Ophør eller ændring af ansættelse: Målet er at ophør eller ændring i en medarbejders, kontrahents og eksterne brugeres ansættelse sker på en betryggende måde. [96]

15.5 Fysisk og miljømæssig sikkerhed

Sikre områder: Målet er, at der ikke opstår uautoriseret adgang til virksomhedens informationer samt lokaler så beskadigelse og forstyrrelse forhindres.

Sikring af udstyr: Målet er at undgå afbrydelse af de eksisterende aktiver i virksomheden samt tab, skade, tyveri eller kompromittering af virksomhedens aktiver.[97]

[95] *ISO/IEC 27001 s. 15*
[96] *ISO/IEC 27001 s. 15-16*
[97] *ISO/IEC 27001 s. 17-18*

15.6 Styring af kommunikation og drift

Operationelle procedurer og ansvarsområder: Målet er at opnå en sikker og korrekt drift af virksomhedens informationsbehandlingsudstyr.

Styring af serviceydelser fra tredjepart: Målet er at opretholde og implementere et hensigtsmæssigt niveau af informationssikkerhed og serviceydelser som er i overensstemmelse med aftaler fra tredjeparter.

Systemplanlægning og systemaccept: Målet er, at risikoen for systemnedbrud minimeres.

Beskyttelse mod skadevoldende programmer og mobilkode: Målet er, at integriteten af informationer og software beskyttes.

Sikkerhedskopiering (back-up): Målet er, at tilgængelighed og integritet opretholdes for informationer og informationsbehandlingsudstyr.

Styring af netværkssikkerhed: Målet er at sikre beskyttelse af informationer, som findes i netværket samt den tilhørende infrastruktur.

Mediehåndtering: Målet er at uautoriseret afsløring forhindres samt ændring, destruktion eller fjernelse af aktiver. Derforuden er målet at forhindre afbrydelser af forretningsaktiviteter.

Informationsudveksling: Målet er, at sikkerheden af information og software opretholdes, som udveksles internt eller eksternt i virksomheden.

Elektroniske forretningsydelser: Målet er at sikre sikker anvendelse af elektroniske forretningsydelser.

Overvågning: Målet er, at uautoriserede informationsbehandlingsaktiviteter afsløres.[98]

[98] *ISO/IEC 27001 s. 18 - 22*

15.7 Adgangsstyring

Forretningsmæssige krav til adgangsstyring: Målet er, at adgangen til informationer bliver styret.

Administration af brugeradgang: Målet er at forhindre uautoriseret adgang til virksomhedens informationssystemer samt at sikre adgang for autoriserede brugere.

Brugeransvar: Målet er at forhindre tyveri eller kompromittering af virksomhedens information og informationsudstyr samt at forhindre uautoriseret brugeradgang.

Styring af netværksadgang: Målet er, at uautoriseret adgang til netværkstjenester forhindres.

Styring af adgang til driftssystemer: Målet er, at uautoriseret adgang til virksomhedens driftssystemer forhindres.

Styring af adgang til forretningssystemer og information: Målet er, at uautoriseret adgang til information i virksomhedens systemer forhindres.

Mobilt udstyr og fjernarbejdspladser: Målet er, at informationer ved anvendelse af mobilt udstyr og fjernarbejdspladser sikres.[99]

15.8 Anskaffelse, udvikling og vedligeholdelse af informationssystemer

Sikkerhedskrav til informationssystemer: Målet er at sikkerhed bliver en integreret del af virksomhedens informationssystemer.

Korrekt informationsbehandling i forretningssystemer: Målet er, at uautoriseret ændring, fejl eller misbrug af informationer i forretningssystemer forhindres.

[99] *ISO/IEC 27001 s. 22- 24*

Kryptografi: Målet er, at autenticitet, fortrolighed, og integritet af informationer beskyttes ved hjælp af kryptografiske metoder.

Sikring af systemfiler: Målet er at systemfiler sikres.

Sikkerhed i udviklings- og hjælpeprocesser: Målet er, at sikkerheden af informationer og software i forretningssystemer opretholdes.

Styring af tekniske sårbarheder: Målet er at reducere risici, som skyldes udnyttelse af tekniske sårbarheder.[100]

15.9 Styring af informationssikkerhedshændelser

Rapportering af informationssikkerhedshændelser og svagheder: Målet er, at informationssikkerhedshændelser sikres. Derforuden skal svagheder i forbindelse med informationssystemer kommunikeres således, at der rettidigt kan iværksættes korrigerende handlinger.

Styring af informationssikkerhedsnedbrud og forbedringer: Målet er, at en effektiv og ensartet metode til styring af informationssikkerhedsbrud sikres. [101]

15.10 Beredskabsstyring

Informationssikkerhedsaspekter ved beredskabsstyring: Målet er at modvirke forretningsaktivitetsafbrydelser. Desuden er målet at beskytte virksomhedens forretningsprocesser mod konsekvenserne af nedbrud af informationssystemer eller katastrofer samt at sikre en rettidig retablering. [102]

15.11 Overensstemmelse

Overensstemmelse med lovbestemte krav: Målet er at brud på love eller kontraktlige forpligtelser undgås samt at undgå brud på sikkerhedskrav.

[100] *ISO/IEC 27001 s. 24 - 26*
[101] *ISO/IEC 27001 s. 26*
[102] *ISO/IEC 27001 s. 27*

Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder samt teknisk overensstemmelse: Målet er at systemer opfylder virksomhedens krav til sikkerhedspolitikker og sikkerhedsstandarder.

Overvejelser ved revision af informationssystemer: Målet er at minimere forstyrrelsen ved revision af informationssystemet samt opnå optimal effekt ved processen. [103]

[103] *ISO/IEC 27001 s. 28-29*

ISO/IEC 27002

Informationssikkerhed er i denne standard opfattet som nødvendigt for virksomheder, da informationssikkerhed er afgørende i forhold til, hvordan virksomheden proaktivt og reaktivt kan håndtere skadelige elementer internt i virksomheden og fra omverdenen som eksempelvis naturkatastrofer og uautoriseret adgang til informationer.[104]

ISO/IEC 27002 er struktureret således, at der er defineret 11 områder for informationssikkerhed i en virksomhed. Her er det ifølge standarden nødvendigt, at virksomheden er i stand til at vurdere og behandle de sikkerhedsrisici, der identificeres indenfor de 11 områder. Dette indebære eksempelvis, at virksomheden skal vurdere om de er villige til at acceptere risikoen eller om de i stedet ønsker at mindske denne risiko.[105] En årsag til at acceptere en risiko kan for eksempel være, at det fra et cost/benefit synspunkt ikke ville være fordelagtigt for virksomheden at indføre foranstaltninger til at mindske risikoen. ISO/IEC 27002 angiver praktiske anbefalinger indenfor hver af de 11 områder til, hvordan en virksomhed bør håndtere og reducere risikoen, så denne ikke kompromitterer informationssikkerheden.

16. Clauses i ISO/IEC 27002

I det følgende vil elementer indenfor de 11 områder blive præsenteret, så det senere kan vurderes, hvilke dele af Cobit 5 frameworket disse områder understøtter.

16.1 Security Policy

Målet med dette område er, at virksomheden behandler informationssikkerhed i overensstemmelse med forretningens krav samt relevante love og reguleringer. Dette område omhandler den informationssikkerhedspolitik, som ledelsen skal acceptere og kommunikere til alle medarbejdere og relevante eksterne parter. Informationssikkerhedspolitikken bør udarbejdes i overensstemmelse med virksomhedens mål og gennemgås jævnligt, samt hver gang der opstår en signifikant ændring i

[104] *ISO 27002 s. viii*
[105] *ISO 27002 s. 4-5*

politikken, for derved at sikre, at politikken forbliver effektiv. Informationssikkerhedspolitikken skal have en ejer, der har ansvaret for at udvikle, gennemgå og evaluere politikken, så det sikres, at politikken konstant bliver vedligeholdt.[106]

16.2 Organization Information Security

Dette område er delt op i en intern og en ekstern del, hvor formålet er at organisere informationssikkerheden, så virksomheden opnår den rette kontrol.

Den første del af den interne organisering omhandler, at virksomheden skal styre opbakningen til informationssikkerheden, ved for eksempel at sørge for, at der findes den rette mængde ressourcer til at optimere informationssikkerheden i virksomheden. Den næsten del omhandler at håndtere koordinationen af informationssikkerheden ved at sikre, at interessenter med de rette kompetencer, på tværs af virksomheden er med at identificere, kommunikere og vurdere elementer indenfor informationssikkerhed. Standarden angiver ligeledes, at organisationen skal have defineret en klar fordeling af ansvaret for informationssikkerheden, som der stadig vil være gældende selvom sikkerhedsopgaverne bliver uddelegeret.

Standarden angiver, at virksomheden ved implementering af nye it elementer er opmærksom på om de rette medarbejdere har de rette adgangsrettigheder, og at disse nye elementer er kompatible med allerede eksisterende elementer. Derudover bør virksomheden ligeledes være opmærksom på den risiko det kan være, at en medarbejder eksempelvis anskaffer en ny computer til hjemmearbejde og håndterer denne risiko.

Det er ifølge standarden også nødvendigt, at virksomheden har klare fortrolighedsaftaler, der beskytter de data som anses for følsomme, og at virksomheden har regler for, hvilke myndigheder der kontaktes, hvis et givent sikkerhedsbrud opstår. Det kan være fordelagtigt for virksomheden at være medlem af diverse grupper, der har indsigt i generel informationssikkerhed for derved at holde sig opdateret indenfor området. Standardens sidste punkt under den interne del omhandler, at

[106] *ISO/IEC 27002 s. 7-8*

informationssikkerheden uafhængigt bliver gennemgået jævnligt, og når signifikante ændringer opstår, for på den måde kontinuerligt at sikre, at virksomhedens tilgang til informationssikkerhed er optimal, tilstrækkelig og effektiv.[107]

Formålet med ISO/IEC's regelsæt for organisering af den eksterne del for virksomhedes informationssikkerhed er, at virksomheden bør identificere de risici, der relaterer sig til eksterne parter, såfremt der ønskes at tildele disse parter adgang til virksomhedens informationer. Ligeledes bør virksomheden implementere kontroller og foranstaltninger før de tildeler den omtalte adgang til eksterne parter og sikre, at de eksterne parter gennem aftaler er oplyste om deres ansvar ved adgang til virksomhedens informationer.[108]

16.3 Asset Management

Denne del af ISO/IEC 27002 opstiller et regelsæt for håndtering af aktiver med det formål at beskytte alle virksomhedens væsentligste aktiver, ved at angive et ejerskab og klassificere de enkelte aktiver. Dette ejerskab betyder, at ejeren kan stilles til ansvar for at vedligeholde kontroller selvom disse uddelegeres. Derudover bør virksomheden klarlægge i hvor høj en grad personer med adgang, har ret til at benytte virksomhedens informationer og aktiver. Virksomheden bør klassificere og mærke deres informationer så det sikres, at informationer med differentierende sårbarhed tildeles den fornødne grad af beskyttelse.[109]

16.4 Human Resources Security

ISO/IEC 27002's afsnit angående menneskelige ressourcer er delt op i tre faser: før indgåelse af aftale, under udførelse af aftale og efter/ændring af aftale. Dette område angiver, hvordan medarbejdere, leverandører og tredjeparter håndteres i forhold til informationssikkerhed, afhængigt af hvilken fase aftaleforholdet befinder sig i. Betegnelsen aftaler fastsætter, at der ikke udelukkende findes situationer, hvor medarbejdere ansættes, men også situationer hvor aftaleforholdet ændres ligeledes, hvad angår aftaler med leverandører og tredjeparter.

[107] *ISO/IEC 27002 s. 9-13*
[108] *ISO/IEC 27002 s.14-18*
[109] *ISO/IEC 27002 s.19-22*

Indledningsvis omtales situationen før indgåelse af aftale, hvor det første punkt vedrører, at der skal opstilles, samt dokumenteres klare roller og ansvar for sikkerhed. Det følgende punkt omhandler baggrundscheck, hvor det anbefales, at der foretages baggrundscheck i henhold til love, reguleringer og virksomhedens behov af alle kandidater. Alle kandidater skal i forbindelse med aftalens indgåelse underskrive en kontakt, der tilkendegiver deres og virksomhedens ansvar i henhold til informationssikkerhed.[110]

Under udførelse af aftalen er det nødvendigt, at medarbejderne, leverandørerne og tredjeparter besidder de rette værktøjer til at opretholde virksomhedens krav til informationssikkerhed. For at sikre at informationssikkerheden opretholdes under aftalen, skal alle medarbejdere, leverandører og tredjeparter følge de regler, der findes i virksomhedens sikkerhedspolitik. Samtlige af virksomhedens medarbejdere, og når det er relevant, leverandører og tredjeparter, skal modtage den træning og kontinuerlig information, der er relevant i forhold til deres position. Virksomheden skal have en disciplinær proces, der varetager medarbejdere, som har været indblandet i et sikkerhedsbrud.[111]

Ved afslutning eller ændring af aftaler angiver ISO/IEC 27002, at virksomheden skal have regler udformet og ansvar uddelegeret angående procedurer, når et aftaleforhold afsluttes. Derudover bør alle medarbejdere, leverandører og tredjeparter returnere alle deres it aktiver ved aftaleforholdets afslutning, samt alle adgangsrettigheder skal fra virksomhedens side nulstilles.[112]

16.5 Physical and Environmental Security

Denne del af ISO/IEC 27002 opstiller anbefalinger for sikring af områder og sikring af udstyr i virksomheden. Indledningsvist anbefales det at alle faciliteter, der indeholder informationer eller behandler information skal fysisk sikres. Dette kan tilvejebringes ved at isolere faciliteterne i et lukket rum, benyttelse af alarmsystemer og lignende. Det er nødvendigt, at alle indgange til sikrede områder, herunder også kontorer, er beskyttet af adgangskoder for at sikre, at kun autoriserede medarbejdere har

[110] *ISO/IEC 27002 s. 23-25*
[111] *ISO/IEC 27002 s. 25-27*
[112] *ISO/IEC 27002 s. 27-28*

adgang.

Virksomheden skal ligeledes sikre, at informationen er sikret mod hændelser fra omverdenen som eksempelvis brand, naturkatastrofer eller lignende, og at medarbejdere er informeret om, hvordan de bør gebærde sig i de sikrede områder. Afslutningsvis bør virksomheden isolere områder som på- og aflæsningsområder, hvor uautoriserede personer færdes, fra betydningsfulde informationer og informationsprocesser.[113]

Det næste punkt i ISO/IEC 27002 omhandler sikring af udstyr. Udstyr skal beskyttes fra udefrakommende trusler og fejl i forbindelse med for eksempel strømforsyning. Især kabler der transportere informationer skal sikres mod udefrakommende interaktioner og skader. Udstyr skal vedligeholdes korrekt, og hvis udstyr kasseres skal virksomhedens sikre, at alle følsomme data er blevet slettet.[114]

16.6 Communications and Operations Management

Procedurer for fremgangsmåder skal dokumenteres, vedligeholdes og være tilgængelige for alle, der har behov for dem. Ved ændring i informationsprocesfaciliteter og systemer skal der forestå den rette kontrol i form af for eksempel logs. Virksomheden skal besidde den rette funktionsadskillelse for at reducere muligheden for uautoriseret eller fejlagtig omgang med virksomhedens aktiver. I denne forbindelse er det nødvendigt, at der er funktionsadskillelse mellem udvikling, test og drift.[115]

Den næste del af ISO/IEC 27002 omhandler håndteringen af tredjepartsservices. Organisationen skal sikre, at serviceleverandøren tilvejebringer de aftalte forudsætninger i kontrakten, samt jævnligt gennemgå og udeføre revision på de rapporter og logs, der fremstilles af tredjeparten. I tilfælde af ændring i forholdet til tredjeparter eller den leverede service, skal virksomheden foretage nye risikovurderinger.[116]

[113] *ISO/IEC 27002 s. 29 -32*
[114] *ISO/IEC 27002 s. 32-36*
[115] *ISO/IEC 27002 s.37-39*
[116] *ISO/IEC 27002 s.39-41*

Angående virksomhedens systemer bør der foretages en vurdering af kapaciteten og behovet for fremtidig kapacitet, samt ved udvikling udføres tests af de kommende systemer. For at beskytte virksomhedens systemer mod spyware og andre skadelige koder bør der implementeres systemer, som for eksempel antivirusprogrammer. For at sikre virksomheden mod tab af data skal der jævnligt foretages back-up af virksomhedens data samt vurderes om back-up proceduren tilvejebringer den udformede back-up politik. Det er ligeledes organisationens opgave at sikre deres netværk ved hjælp af for eksempel brugerprofiler og overvågning af trafikken på netværket. Der bør være procedurer for sikker opbevaring, fjernelse og tilintetgørelse af flytbare media, som USB-stiks og cd-rommer. [117]

Når organisationen udveksler information, både fysisk, elektronisk og gennem online portaler, med eksterne parter skal dette foretages i henhold til en klart defineret politik og aftale med den eksterne part, for derved at beskytte den udvekslede information. Virksomhedens offentlige informationer, som eksempelvis oplysninger på hjemmesiden, skal også beskyttes mod uautoriseret adgang. Et primært værktøj til beskyttelse af virksomhedens informationer er overvågning og logføring. Samtlige af virksomhedens systemer bør overvåges og føres i en log, der er sikret mod uautoriseret adgang. For at disse logs kan behandles korrekt skal alle ure i organisationens systemer synkroniseres. Disse logs bør gemmes og bruges, hvis der opstår fremtidige efterforskninger af sikkerheds- eller sikkerhedskontrolmæssige problemstillinger.[118]

16.7 Access Control

Denne del af ISO/IEC 27002 vedrører benyttelse af adgangskontroller for at sikre informationen i virksomheden. Der skal være en adgangskontrolpolitik og klare procedurer for tildeling og fradeling af adgangsrettigheder til virksomhedens systemer. Disse adgangsrettigheder bør jævnligt gennemgås så det sikres, at alle relevante brugere har den tilstrækkelige adgang. Brugernes adgangskoder bør kontrolleres gennem en formel styringsproces, og medarbejderne bør underskrive en erklæring om, at de holder adgangskoderne fortrolige. Brugerne bør følge god sikkerhedsskik, når de konstruerer deres kodeord og sørge for, at udstyr ikke ligger ubeskyttet hen, samt at der ikke ligger følsomme

[117] *ISO/IEC 27002 s. 41-48*
[118] *ISO/IEC 27002 s. 48-59*

informationer frit tilgængelige på deres skrivebord.

Angående netværksservice bør brugerne i virksomheden kun have fjernadgang til elementer de reelt har behov for at have adgang til, og der bør benyttes passende brugeradgangsmetoder ved fjernadgang. [119]

Adgangen til operativsystemer bør sikres med en sikker "log på" procedurer, hvor alle brugere har deres unikke bruger-id, så der kan føres logs på den individuelle bruger. Systemer til at styre adgangskoder bør implementeres for at sikre høj kvalitet af adgangskoder, og der bør implementeres restriktioner mod programmer, der eventuelt kan omgå disse systemer. Virksomheden bør anvende time-out sessioner, der bevirker, at når et udstyr har været inaktivt i en periode lukkes det ned, samt kan de anvende begrænsninger på hvor lang tid, der må være forbindelse til et system eller applikation.[120]

16.8 Information Systems Acquisition, Development and Maintenance

I denne del er det nødvendigt, at der i alle virksomhedens udsagn angående informationssystemer er krav om sikkerhed. Der skal være kontroller, som sikrer, at alle data såvel input som output er underlagt en kontrol for at sikre validiteten. Denne validering skal integreres i virksomhedens applikationer så procesfejl eller fejlagtige handlinger bliver opdaget. Kontroller bør implementeres, der sikrer, at meddelelser som udspringer af virksomhedens applikationer besidder den fornødne integritet. Ydermere bør dataoutput fra applikationerne vurderes så virksomheden er sikker på, at den information der arbejdes videre med i processes er valid og passende.[121]

ISO/IEC 27002 angiver også regelsæt angående virksomhedens kryptografering af deres data og anbefaler, at der udformes en politik for dette samt angivelse af en nøgleperson, der kan yde support omkring virksomhedens kryptograferingsteknikker. Der bør ligeledes være fremlagt procedurer angående fremgangsmåde for installation af nyt software på operationssystemerne. Derudover skal alt testdata sikres, så det ikke bliver mangfoldiggjort, og adgangen til programmernes kildekode skal være restriktiv. I tilfælde af at virksomheden ønsker en ændring i deres nuværende systemer eller at

[119] *ISO/IEC 27002 s.60-66*
[120] *ISO/IEC 27002 s. 69-73*
[121] *ISO/IEC 27002 s. 77-80*

implementere et nyt system, bør dette foretages under formelle ændringsprocedurer, hvor risikovurdering og konsekvensen for ændringen bør analyseres. Efter en operativ systemændring har fundet sted bør kritiske applikationer gennemtjekkes og testes for at sikre, at det ikke har haft sikkerhedskomprimerende konsekvenser. Det anbefales ligeledes, at ændringer udelukkende bliver foretaget, hvis det reelt er nødvendigt, så virksomhedens informationssikkerhed ikke bliver unødigt komprimeret.

Alle trusler der kan forårsage risiko for udslip af følsom information bør undgås, ved for eksempel at scanne udgående data og overvåge medarbejdere og systemaktivitet. Ligeledes bør virksomheden, ved outsourcing af systemudvikling, føre overvågning med leverandørerne, samt være opmærksomme på og reducere risikoen de steder i virksomhedens teknik, hvor der kan forekomme følsomheder.[122]

16.9 Information Security Incident Management

Alle sikkerhedsmæssige situationer bør rapporteres gennem hensigtsmæssige kanaler så hurtigt som muligt. Alle medarbejdere, leverandører og tredjeparter der benytter virksomhedens informationssystem skal opfordres til at notere og rapportere alle observerede mistænkeligheder i virksomhedens informationssystem og services, så der kan foretages en passende, korrigerende og forebyggende handling således, at virksomheden kan lære af fejlene. For at der kan foretages hurtige og effektive handlinger og indsamles de rette beviser, bør der etableres ansvar og procedurer for håndteringen af disse situationer.[123]

16.10 Business Continuity Management

En forsat forretningsdriftsproces bør implementeres for at minimere konsekvensen af tabt information, ved at etablere en kombination af forebyggende og genoprettende kontroller. Virksomheden bør identificere de kritiske forretningsprocesser, samt vurdere sandsynligheden for situationens opstående og de informationssikkerhedsmæssige konsekvenser heraf. Der bør udvikles og implementeres planer for vedligeholdelse og genoprettelse af operationer, samt sikre tilgængeligheden af nødvendige

[122] *ISO/IEC 27002 s. 80-89*
[123] *ISO/IEC 27002 s. 90-94*

informationer i tilfælde af der forekommer forstyrrelser af kritiske forretningsprocesser. Et fastlagt framework bør opretholdes for at sikre, at alle planer er konstante, så informationssikkerhedskrav kontinuerligt kan håndteres, og der kan identificeres prioriteter angående test og vedligeholdelse. Disse planer skal jævnligt testes og opdateres, så det sikres, at de er opdaterede og effektive.[124]

16.11 Compliance

ISO/IEC 27002 anbefaler, at alle relevante love, reguleringer og kontraktmæssige krav som virksomheden skal overholde i henhold til deres informationssystemer bliver defineret, dokumenteret og holdt opdateret, samt at alle kontroller og individuelle ansvar bliver tilkendegivet. Dette gælder også for virksomhedens licensaftaler. Virksomhedens betydningsfulde databaser skal sikres, så der ikke lides tab, falsificering eller destruktion, i henhold til gældende compliance. Virksomheden skal være opmærksom på lovreguleringen angående håndtering af person og andet følsomt data, og det skal sikres, at medarbejderne ikke anvender disse data på uautoriseret vis. Kryptografering af virksomhedens data skal også håndteres i henhold til gældende lov på området.

Personer der har ansvar inden for et givent område bør sikre, at alle sikkerhedsprocedurer bliver udført i henhold til sikkerhedspolitikken og standarder indenfor området. Informationssystemer bør jævnligt tjekkes for om de er tilstrækkelige i henhold til gældende sikkerhedsimplementeringsstandarder.

Revision og andre aktiviteter, til at tilse operative systemer, skal nøje planlægges så de forstyrrer virksomhedens drift mindst muligt. Adgangen til informationssystemsrevisionsværktøjer bør beskyttes for derved at undgå misbrug.[125]

[124] *ISO/IEC 27002 s. 95-99*
[125] *ISO/IEC 27002 s. 100-106*

ISO/IEC 20000-serien

I det følgende vil ISO/IEC 20000-serien overordnet blive præsenteret med det formål senere at vurdere, hvilke dele af ISO 20000, der kan understøtte, hvilke processer i Cobit 5, for derved at konkludere på, hvordan revisor kan rådgive ledelsen af en virksomhed til at få det optimale ud af deres it ressourcer.

Denne serie består af fem dele under titlen *Information technology – Service Management*, hvoraf Part 1, Part 2 og Part 4 vil blive præsenteret*:*

- Part 1: Service management system requirements
- Part 2: Code of practice
- Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1
- Part 4: Process reference model
- Part 5: Exemplar implementation plan for ISO/IEC 20000-1[126]

17 ISO/IEC 20000-1- Service Management System Requirements

Denne del af ISO/IEC 20000-serien opstiller krav til en serviceudbyders produkt angående design, overgang, levering og forbedring af service, der er værdiskabende for både kunden og serviceudbyderen. Dette kræver, at der findes en integreret proces for, hvorledes serviceudbyderen planlægger, etablerer, implementerer, driver, overvåger, gennemgår, vedligeholder og forbedrer et Service Management System (SMS).

Som i ISO/IEC 27001 og ISO/IEC 27002 er denne standard også opbygget på baggrund af PDCA modellen, der skal benyttes på alle dele af SMS'et og service. Plan-delen består i at etablerer, dokumentere og bestemme SMS'et, som inkluderer politikker, mål, planer og processer, der skal imødekomme servicekravene. Do-delen består i at implementere og drive SMS'et vedrørende design, overgang, levering og forbedring af service. I Check-delen skal SMS'et og service overvåges, måles og gennemgås, så de

[126] *ISO/IEC 20000-1 s. v*

er i overensstemmelse med politikkerne, målene, planerne og servicekravene, derforuden skal resulaterne rapporteres. I den sidste Act-del skal der fortages handlinger til kontinuerligt at forbedre SMS'et og service.

Når PDCA modellen anvendes på et SMS, er det væsentligste at sikre forståelsen og møde servicekrav således, at kundernes behov tilfredsstilles. Dette opnås ved at etablere politik og mål for servicehåndtering og at designe og levere service baseret på dét SMS, som er værdiskabende for kunden, samt overvåge, måle og gennemgå ydeevnen af SMS'et og service, mens SMS'et kontinuerligt bliver forbedret. Hvis en serviceudbyder følger PDCA metoderne skaber dette ligeledes grundlag for at integrere deres SMS med andre management standarder, som ISMS'et fra ISO/IEC 27001.[127]

Management Responsibility

Der findes nogle generelle krav til SMS'et, herunder serviceudbyderens ledelses dedikation til at planlægge, etablere, implementere, drive, overvåge, vedligeholde og forbedre SMS'et og service, ved at kommunikere anvendelsesområder, poltikker og mål angående service management. Ledelsen skal sørge for, at service management planen bliver konstrueret, implementeret og vedligeholdt, og kommunikere nødvendigheden af, at servicekravene, lovereguleringen, standarder og kontrakter bliver opfyldt. Ledelsen skal sikre, at der forlægger de rette ressourcer og udføre management gennemgang ved planlagte intervaller, samt sikre at risici angående service bliver vurderet og håndteret.[128]

Governance of Processes Operated by Other Parties

Serviceudbyderen skal identificere de processer eller dele af processer, der håndteres af andre, som for eksempel en intern gruppe, en kunde eller en leverandør. Såfremt processer eller dele af processer bliver styret af en leverandør, skal det håndteres ved hjælp af en leverandørmanagementproces. Såfremt det er en intern gruppe eller en kunde skal det håndteres ved hjælp af en service level management proces.[129]

Documentation Management

[127] *ISO/IEC 20000-1 s. vii -2*
[128] *ISO/IEC 20000-1 s. 7-8*
[129] *ISO/IEC 20000-1 s. 8-9*

Serviceudbyderen skal oparbejde og vedligeholde dokumenter, her inkluderes logs, til at sikre effektiv planlægning, drift og kontrol med SMS'et. Disse dokumenter er for eksempel politikker og mål for service management, Service Level Agreements (SLA) og service management processer. Serviceudbyderen skal have den rette kontrol over dokumenterne så de blandt andet er tilgængelige i de rette versioner.[130]

Ressource Management

Det er serviceudbyderens opgave at fastlægge og tilvejebringe de menneskelige, tekniske, informationsmæssige og finansielle ressourcer, som de behøver for at etablere, implementere og vedligeholde SMS'et og service og kontinuerligt forbedre deres effektivitet, samt at forbedre kundetilfredsheden ved at levere service, der lever op til servicekravene.

Angående menneskelige ressourcer er det nødvendigt, at serviceudbyderens personale skal besidde den fornødne uddannelse, træning og erfaring til at varetage servicekravene. Dette sikres ved at fastlægge og dokumentere de nødvendige kompetencer, og om nødvendigt træne og evaluere personalet så de oparbejder de rette kompetencer. Ledelsen skal informere personalet i sådan en grad, at personalet er overbeviste, hvordan de kan bidrage til, at servicekravene og målene bliver opfyldt. [131]

Establish and Improve the SMS

Serviceudbyderen skal i service management planen definere og inkludere anvendelsesområdet af SMS'et, hvor der tages hensyn til den geografiske lokalisering af serviceudbyder og kunde, samt den teknologi, der anvendes til at varetage servicen.

Serviceudbyderen skal udforme, implementere og vedligeholde en service management plan, hvor der tages hensyn til service management politikken, servicekrav og de retningslinjer, der er opstillet i ISO/IEC 20000-1.[132]

[130] *ISO/IEC 20000-1 s. 9-10*
[131] *ISO/IEC 20000-1 s. 10*
[132] Service management planen skal indeholde de punkter, som er angivet på side 11 i ISO 20000-1.

Serviceudbyderen skal angående design, overgang, levering og forbedring, implementere og drive SMS'et i henhold til service management planen. Dette kan tilvejebringes gennem følgende aktiviteter:

- Allokering og varetagelse af midler og budgetter.
- Tildeling af autoritet, ansvar og proces roller.
- Varetagelse af menneskelige-, teknologiske- og informationsressourcer.
- Identifikation, vurdering og varetagelse af risici angående servicen.
- Varetagelse af service management processer.
- Overvågning og rapportering på ydeevne af service management aktiviteter.[133]

Serviceudbyderen skal anvende intern revision og ledelsesgennemgang til at overvåge og måle SMS'et og service, samt dokumentere målene for disse, for på denne måde at demonstrere, at SMS'et tilvejebringer til service management målene og opfylder servicekravene.

Der skal forelægge en politik for kontinuerlige forbedringer af SMS'et og servicerne, samt en procedurer, der angiver autoritet og ansvar for identificering, dokumentering, evaluering, godkendelse, prioritering, varetagelse, måling og rapportering af forbedringer, samt korrigerende og proaktive handlinger.[134]

Design and Transition of New or Changed Services

En serviceudbyder skal benytte sig af processen i ISO/IEC 20000-1 hver gang, der udføres nye service eller sker ændring til de eksisterende, der har potentiale til at have konsekvens for service eller kunderne. Indledningsvis skal serviceudbyderen planlægge, designe og udvikle den nye eller ændrede service, hvorefter de nye eller ændrede services skal testes for at sikre, at de opfylder servicekravene og designet. [135]

[133] *ISO/IEC 20000-1 s. 11*
[134] *ISO/IEC 20000-1 s. 10-13*
[135] *ISO/IEC 20000-1 s. 13-15*

Service Delivery Processes

Serviceudbyderen skal indgå aftale med kunden om at levere en given service, og der skal i samarbejde med kunden, udarbejdes en eller flere SLA'er for hver service, der leveres. Disse SLA'er skal gennemgås med kunden indenfor planlagte intervaller og ligeledes skal serviceudbyder overvåge trends og ydeevne på servicemål indenfor planlagte intervaller. Såfremt der findes servicekomponenter, der leveres af en intern gruppe eller en kunde er det serviceudbyderens ansvar at overvåge, måle og sammenholde deres ydeevne med de aftalte servicemål.

Serviceudbyderen skal vurdere og dokumentere risici, samt indgå en aftale med kunden og interesserede parter, angående krav til service kontinuitet og tilgængelighed. Der skal udarbejdes, implementeres og vedligeholdes en service kontinuitet og tilgængeligheds plan.

ISO/IEC 20000-1 angiver under serviceleveringsprocesser, tilmed regler for procedurer angående budgettering, kapacitet og informationssikkerhed for service. Ledelse med den rette autoritet skal godkende en informationssikkerhedspolitik, der inddrager servicekrav, lovepligtige og reguleringsmæssige krav, samt aftalte forpligtelser. Det er ledelsens opgave blandt andet at kommunikere politikken, etablere informationssikkerhedsvaretagelsesmål og definere, hvordan informationssikkerheds risici håndteres med videre.[136]

Relationship Processes

Serviceudbyderen skal identificere og dokumentere kunder, brugere og interessenter af servicen og have en dedikeret person til at varetage kunderelationer og kundetilfredshed. Der skal etableres en kommunikationsmekanisme med kunderne, som kan give serviceudbyder en forståelse af forretningsmiljøet. Desuden skal serviceudbyder opnå en forståelse af, om der er behov for nye eller ændrede service. Der skal findes en dokumenteret procedure for håndteringen af kundeklager, og serviceudbyderen skal logføre, undersøge, reagere, rapportere og afslutte serviceklager. Serviceudbyderen skal tilmed jævnligt måle kundetilfredsheden og analysere den med det formål at identificere muligheder for forbedringer.

[136] *ISO/IEC 20000-1 s. 15-19*

Når en serviceudbyder anvender leverandører til at varetage dele af service managementprocesserne, skal der være en dedikeret person, som varetager relationerne. Serviceudbyderen og leverandøren skal være enige om en aftale[137], relationerne til leverandøren skal være dokumenteret, og serviceudbyderen skal overvåge præstationen af leverandøren ved planlagte intervaller.[138]

Resolution Processes

Såfremt en situation opstår, hvor kunden har brug for assistance, bør serviceudbyderen i prioriteringen, inddrage konsekvensen af hændelsen eller serviceforespørgslen for at sikre, at alt personale der er involveret har adgang til relevant information. Serviceudbyderen skal kontinuerligt holde kunden opdateret angående deres rapporterede hændelser eller forespurgte service. Der skal foreligge en aftale med kunden om, hvad der klassificeres som en kraftig hændelse og så snart en væsentlig hændelse rapporteres, skal der udpeges en ansvarlig fra personalet til at varetage hændelsen. Efter hændelsen er blevet varetaget og udbedret, skal den gennemgås for at identificere muligheder for forbedring fremover.

Der skal foreligge en procedure for, hvordan et problem skal håndteres og serviceudbyderen skal foretage analyser af data fra hændelser og problemer for at identificere kilden og eventuelle præventive handlinger. Effektiviteten omkring problemløsning skal overvåges, gennemgås og rapporteres. [139]

Control Processes

Der skal være en dokumenteret definition af hvert konfigurationselement (CI), som indeholder en beskrivelse, relationen til andre CI'er, relationen mellem CI'er og servicekomponenterne, en status, version, lokalisering, forbundene forespørgsler om forandringer, forbundene problemer og kendte fejl. CI'er skal identificeres og samles i en konfigurationsmanagement database (CMDB), hvorpå serviceudbyderen jævnligt bør foretage revision. Såfremt der under revisionen findes utilstrækkeligheder, skal serviceudbyder foretage passende handlinger og rapportere disse.[140]

[137] Denne aftale skal indeholde punkterne på side 20 i ISO/IEC 20000-1.
[138] *ISO/IEC 20000-1 s. 19-21*
[139] *ISO/IEC 20000-1 s. 21-22*
[140] *ISO/IEC 20000-1 s. 22-23*

18 ISO/IEC 20000-2 – Code of practice

Denne del af ISO/IEC 20000-serien beskriver "best practices" for service management processer indenfor virkeområdet af ISO/IEC 20000-1. Betydningen af servicesektoren stiger sideløbende med, at forbrugere kræver mere avancerede faciliteter til den mindste pris til at dække deres forretningsbehov. Service og servicemanagement kan opfattes som nødvendigt for virksomheder til at genere overskud og være omkostningseffektive. Med den stigende afhængighed af supportservice, og den diversificerede mængde teknologi, der er til rådighed, kan det være en udfordring for serviceudbyderne at opretholde et højt kundeserviceniveau. De arbejder reaktivt og bruger for lidt tid på planlæggelse, uddannelse, gennemgang, undersøgelser og at arbejde med kunderne, og derfor bliver de strukturerede proaktive arbejdsgange ikke adopteret. Denne standard giver serviceudbydere muligheden for at forstå, hvordan de kan forbedre kvaliteten af den service de levere til kunderne både internt og eksternt. [141]

The Management System

Det er formålet at præsentere et system, der inkluderer alle politikker samt et framework, som tilvejebringer effektiv ledelse og implementering af alle it service. I denne forbindelse er det ledelsens rolle at sikre, at alle "best practices" bliver fulgt så kravene i ISO/IEC 20000-1 kan imødekommes. Der bør udpeges en ejer, bakket op af en beslutningstagergruppe, som er ansvarlig for service management planen. Ejeren skal sikre, at alt relevant information, der skal benyttes ved revision af politikker, planer og procedurer, er tilgængelig.

Personalet der arbejder med service management skal være kompetent, herunder besidde den rette uddannelse, træning og erfaring. Serviceudbyderen bør definere, hvilke kompetencer der er krævet for at udføre jobbet, samt sikre at alt personale er bevidst om, hvordan de gennem deres funktion, kan bidrage til at opnå mål. Der bør føres logs over uddannelse, træning, kompetencer og erfaring, samt udbydes træning eller foretages andre handlinger til at nå behovet, samt evaluere effektiviteten af de foretagne handlinger. Serviceudbyderen bør varetage deres professionelle udvikling gennem rekruttering, planlægning, træning og udvikling.[142]

[141] *ISO/IEC 20000-2 s. v - vi*
[142] *ISO/IEC 20000-2 s. 2-3*

Planning and Implementing Service Management

Indledningsvist skal ledelsen definere anvendelsesområdet for service management planen, som bør omfatte implementering af service management, levering af service management processer, ændring af service management processer, forbedringer af service management processer og nye service.[143]

Serviceudbyderen bør planlægge og implementere overvågning, måling, analyse og gennemgang af services, service management processer og associerede systemer. De elementer der bør overvåges, måles og gennemgås er opnåelse af definerede service mål, kundetilfredshed, ressourceudnyttelse, trends og kraftige afvigelser.

Der bør føres en politik angående servicekvalitet og forbedringer, som alle medarbejdere er bekendte med for at forbedre effektiviteten og ydeevnen af servicelevering og management. Alle forbedringer bør sammenholdes med tidligere forhold for at vurdere effekten forbedringerne har forårsaget.[144]

Planning and Implementing New or Changed Services

Denne del af ISO/IEC 20000-2 har til formål at sikre, at nye service eller ændring af eksisterende vil blive leveret og håndteret til den aftalte pris og kvalitet. Under planlægningen bør der gennemgås budgetter, personaleressourcer, eksisterende serviceniveau, SLA'er og anden binding, eksisterende service management processer, procedurer, dokumenter og anvendelsesområdet af service management.

Samtlige serviceændringer bør figurere i ændringsmanagement logs, herunder planer for rekruttering, re-lokalisering, brugertræning, kommunikation omkring ændringen, ændring i den teknologi, der understøttes og formel afslutning af service.[145]

Service Delivery Processes

Et servicekatalog bør definere alle service, vedligeholdes og holdes opdateret, samt være tilgængeligt for alle kunder og personale. Den service der aftales bør blive formelt dokumenteret i en SLA, hvor budgettet danner rammer for indholdet, strukturen og målene, defineret fra et kundeperspektiv. Det bør

[143] ISO/IEC 20000-2 side 5 angiver punkter, som service management planen bør imødekomme og definere.
[144] *ISO/IEC 20000-2 s. 4-7*
[145] *ISO/IEC 20000-2 s. 7-8*

undgås at have for mange mål defineret, da dette kan forårsage forvirring og centrale mål forsømmes.[146]

Såfremt der foreligger væsentlige forretningsændringer som eksempelvis en virksomhedsfusion, og derved en ændring i servicebehovene bør serviceniveau management processen (SLM) være fleksible.

Service rapporter bør være opdaterede, klare, pålidelige og kortfattede, samt let overskuelige og anvendes med det formål at skabe nutidig, pålidelig, præcise rapporter til informeret beslutningstagning og effektiv kommunikation. Flere typer af servicerapporter bør udformes:

- En reaktiv rapport der redegør for forandringen.
- En proaktiv rapport der giver forudgående advarsler om signifikante hændelser, og derved gør det muligt at handle forebyggende.
- Fremadrettede rapporter der beskriver de planlagte aktiviteter.

For at sikre at den aftalte servicekontinuitet og tilgængelighed kan imødekommes under alle omstændigheder, bør kravene hertil defineres på baggrund af kundens forretningsprioriteter, SLA'er og vurderede risici. Serviceudbyderen bør udvikle og opretholde en strategi, som definerer den generelle tilgang til at imødekomme servicekravene. Denne strategi bør indeholde en risikovurdering og inddrage de aftalte servicetider og kritiske forretningsperioder.

ISO/IEC 20000-2 indeholder tilmed retningslinjer for budgettering og kapacitetsvaretagelse hos serviceudbyderen, samt informationssikkerhedsmanagement. Informationssikkerhed behandles i ISO/IEC 27002 og udføres på baggrund af en række policer og procedurer designet til at identificere, kontrollere og beskytte information, samt alt udstyr der er forbundet med lagring transmittering og behandling af information.

[146] ISO/IEC 20000-2 indeholder på side 9 minimumsindholdet i en SLA.

Serviceudbyder bør vedligeholde en portefølje af informationsaktiver, der er nødvendige for at levere service og klassificere hvert aktiv efter, hvor kritisk det er for servicen og den grad af beskyttelse det behøver. Derforuden udpeges en ejer, der har ansvaret for at tilvejebringe den krævede mængde sikkerhed. Vurderingen af sikkerhedsrisiko bør udføres under aftalte intervaller, logføres, opretholdelse under ændringer, højne forståelse af hvad der kan ramme en service og informere om, hvilke typer kontroller der skal implementeres. Risici forbundet med informationsaktiver bør vurderes ud fra deres natur, sandsynlighed, konsekvens og tidligere erfaringer. Ved vurdering af risici bør serviceudbyder overveje afsløring af følsomt data til uautoriseret personer, unøjagtige, ufuldstændige eller ugyldige informationer, information der ikke er tilgængelige og fysisk skade eller destruktion af udstyr. Ligeledes bør kundens specifikke sikkerhedskrav og hjemmel i lov og reguleringer, også tages i betragtning.

For at imødekomme god sikkerhedsskik bør ledelsen definere og kommunikere sikkerhedspolitikken til personale og kunder, og foretage implementerende handlinger. Ansvar og roller angående informationssikkerhed bør defineres, samt overvågning og vedligeholdelse af sikkerhedspolitikken bør gennemføres. Personale med signifikante sikkerhedsroller bør trænes, og samtlige medarbejdere bør gøres bevidste om nødvendigheden af at overholde sikkerhedspolitikken. Assistance fra eksperter til at risikovurdere og implementere kontroller bør være tilgængelig, og ændringer bør ikke kompromittere driften af kontrollerne. Derudover bør informationssikkerhedshændelser rapporteres og handling fortages. Logs bør analyseres periodisk for at give ledelsen information om effektiviteten af informationssikkerhedspolitikken, trends i informationssikkerhedshændelser, input til en plan om forbedring af servicen og kontrol over adgang til informationer, aktiver og systemer. [147]

Relationship Processes

ISO/IEC 20000-2 indeholder ligeledes ”best practice” for, hvordan en serviceudbyder håndterer rollen som mellemledet mellem en serviceunderleverandør og kunden. Leverandøren kan være ekstern, der kommunikeres med gennem kontrakter, eller en intern, som en del af serviceudbyderens egen virksomhed. I en sådan relationsproces er det nødvendigt, at alle parter forstår, hvordan de opfylder virksomhedens behov, forstår muligheder og begrænsninger samt forstår deres ansvar og forpligtelser. Anvendelsesområderne, roller og ansvar angående forretningsrelationerne bør defineres og dokumenteres.

[147] *ISO/IEC 20000-2 s. 8 -16*

For at opnå en effektiv relation mellem serviceudbyderen og kunden, er det nødvendigt, at kundens forretningsbehov er kendte og forstås af serviceudbyder. For at tilvejebringe en forståelse bør der foretages årligt gennemgang af servicen, samt før og efter forandringer. Serviceudbyderen og kunden bør aftale en formel klageprocedure, og serviceudbyder bør have en fastlagt proces for, hvordan klager håndteres. Kundetilfredshedsundersøgelser bør udføres, så serviceudbyderen kan sammenligne resultater fra kundetilfredshedsmålinger med tidligere tal. Såfremt der er signifikante ændringer i kundetilfredsheden, bør det undersøges nærmere for at klarlægge årsagen. Resultaterne af kundetilfredshedsundersøgelsen skal præsenteres for kunden og en handlingsplan til forbedringer diskuteres. Fremskidt rapporteres tilbage til kunden.

Der bør foreligge procedurer for varetagelse af leverandørrelationer for at sikre, at leveringen er problemfri og af den rette kvalitet. Gennem en leverandør management procedurer kan det sikres at:

- Leverandøren forstår deres forpligtelser overfor serviceudbyder.
- Legitimerede og aftalte krav opnås indenfor det aftalte serviceniveau og anvendelsesområde.
- Forandringer bliver håndteret.
- Forretningstransaktioner mellem alle parter bliver logført.
- Information angående ydeevne af alle leverandører kan blive observeret og handlet på.

Serviceudbyderen bør udpege en person, som er ansvarlig for alle kontrakter og aftaler med leverandører. For hver service og hver leverandør, bør serviceudbyderen have klarlagt en definition af services, roller og ansvar, et anvendelsesområde, en kontrakt management proces, betalingsbetingelser og aftaler for rapporteringsparametre og logføring af opnået ydeevne. [148]

[148] *ISO/IEC 20000-2 s. 17-20*

Resolution Processes

Der differentieres mellem om det er et problem eller en hændelse, der varetages, idet hændelser omhandler genoprettelse af service for kunden, hvor problemer relaterer til identifikation og fjernelse af kilden til hændelserne.

Hvilke hændelser serviceudbyderen vælger at behandle først bestemmes på baggrund af en prioritering, som baseres på konsekvens og væsentlighed. Konsekvens bør vurderes ud fra en skala over faktisk eller potentiel skade på kundens forretning, og væsentlighed vurderes ud fra, hvor lang tid der går fra, at problemet eller hændelsen er opdaget til, at den har konsekvens for kundens forretning.

Såfremt serviceudbyderen skal varetage en hændelse er målet at genoprette den aftalte service hos kunden så hurtigt som muligt. Alt hvad der kan gøres for midlertidigt at stabilisere situationen så kunden kan fortsætte med forretningsførelse bør fortages. Alle hændelser bør logføres, så relevant informationen kan blive vurderet og analyseret.

Målet med varetagelse af problemer er at minimere forstyrrelser i kundens forretning ved proaktivt at identificere og analysere kilden til hændelser. Serviceudbyderen bør forebygge tilbagevendende problemer og kendte fejl. Når kilden til en hændelse er fundet og identificeret, klassificeres den som en kendt fejl og bør derfor logføres. Problemeftersyn bør foretages i tilfælde af uløste problemer eller ualmindelige- eller højkonsekvensproblemer, med det formål at muliggør forbedring og forbygge tilbagevendende problemer eller fejl.[149]

Control Processes

Målet med kontrolprocesser er at definere og kontrollere komponenter i en service og infrastrukturen, og vedligeholde præcis konfigurationsinformation. Konfigurationsmanagement bør planlægges og implementeres med forandrings -og udgivelsesmanagement for at sikre, at serviceudbyderen effektivt kan varetage deres it aktiver og konfigurationer. Alle væsentlige aktiver og konfigurationer bør varetages og have en ansvarlig person, der sikrer den rette beskyttelse og kontrol.[150]

[149] *ISO/IEC 20000-2 s. 20-24*
[150] side 25 i ISO/IEC 20000-2 redegør for en liste over, hvad en konfigurationsmanagementplan bør indeholde.

Alle konfigurationselementer bør identificeres og defineres på baggrund af deres funktion og fysisk karakteristika, og logføres i konfigurationsmanagementdatabasen. Baseret på etablerede udvælgelseskriterier bør elementer, der skal varetages og identificeres og udvælges.[151] Sammenhængen og afhængigheden mellem disse konfigurationselementer bør identificeres for at tilvejebringe det nødvendige kontrolniveau.

Processen burde sikre, at kun autoriserede og identificerbare konfigurationselementer bliver accepteret og logført fra modtagelse til bortskaffelse. Konfigurationselementer burde ikke blive tilføjet, modificeret, erstattet eller fjernet uden passende kontrollerende dokumentation som eksempelvis en accepteret forandringsforespørgsel. For at beskytte integriteten af systemer, services and infrastrukturen bør konfigurationselementer opbevares i et passende og sikkert miljø, der beskytter den mod uautoriseret adgang, ændring, korruption, tilvejebringer midler for genopretning ved katastrofe og tillader kontrolleret genfinding af en kopi af software.

Konfigurationsmanagementrapporter bør være tilgængelige for alle relevante parter og bør omhandle identifikation og statusser på konfigurationselementerne, deres versioner og associeret dokumentation. Konfigurationsverifikation og revisionsprocesser både fysiske og funktionelle bør planlægges, og det bør tjekkes om de rette processer og ressourcer er til stede for at:

- Beskytte de fysiske konfigurationer og den intellektuelle kapacitet i virksomheden.
- Forsikre at serviceudbyder har kontrol over konfigurationerne, kopier og licenser.
- Forsikre at konfigurationsinformation er korrekt, kontrolleret og synlig.
- Forsikre at ændringer, udgivelser, systemer og miljøer er tilpasset deres aftalte eller specificerede krav, og at konfigurationslogs er præcise.

Revision af konfigurationer bør gennemføres jævnligt, samt før og efter forandringer eller katastrofer.

[151] Side 26 i ISO/IEC 20000-2 indeholder en liste over, hvad disse elementer bør være.

ISO/IEC 20000-2 indeholder ligeledes et område for, hvordan ændring bør varetages for at sikre, at alle ændringer vurderes, accepteres, implementeres og gennemgås på kontrolleret vis. Processer og procedurer for ændringer sikre blandt andet, at det udelukkende er ændringer der er til fordel for virksomheden, som accepteres, og at ændringer planlægges på basis af prioritet og risiko. Alle ændringer bør gennemgås efter implementeringen med henblik på at identificere succes eller fejl. En efter-implementeringsgennemgang bør igangsættes ved væsentlige ændringer for at tjekke om ændringen møder dets mål, om kunderne er tilfredse med resultatet og om der har været nogle uventede bivirkninger.[152]

Release Processes

Den sidste del af ISO/IEC 20000-2 omhandler udgivelsesmanagement, hvor målet er at levere, distribuere og spore en eller flere ændringer i miljøet. Opgaven for udgivelsesmanagement er at koordinere aktivitet fra serviceudbyder, flere leverandøre og forretningen, for at planlægge og levere en udgivelse på tværs af hele miljøet.[153]. Serviceudbyderen bør samarbejde med virksomheden for at sikre, at konfigurationselementerne, der bliver udgivet, er kompatible med hinanden, og med de elementer der allerede findes i miljøet. Udgivelsesplanlægning bør sikre, at ændringerne af systemer, infrastruktur, services og dokumentation er aftalte, autoriserede, skematiserede, koordinerede og sporet.

Processen for udvikling og tilegnelse af software bør dokumenteres i konfigurationsmanagementplanen. Udgivelse og distribution bør blandt andet designes og implementeres således, at det er tilpasset serviceudbyderens systemarkitektur, service management og infrastrukturstandarder, og så det sikres, at integriteten vedligeholdes under konstruering, installation, håndtering, pakning og levering, samt at risici er klart defineret.[154]

19 ISO/IEC 20000-4 - Process Reference Model

Denne procesreferencemodel (PRM) er en præsentation af elementer i processer indenfor service management. ISO/IEC 20000-4 beskriver de processer, der inkluderes i et generelt SMS beskrevet i

[152] *ISO/IEC 20000-2 s. 25-29*
[153] Der bør være en udgivelsespolitik indeholdende punkterne på side 30 i ISO/IEC 20000-2
[154] *ISO/IEC 20000-2 s. 29-31*

ISO/IEC 20000-1. De resultater der beskrives i denne del af ISO/IEC 20000-serien er minimumskravene for at opfylde ISO/IEC 20000-1 kravene. [155]

19.1 Processer i ISO/IEC 20000-4

I det følgende vil processerne i ISO/IEC 20000-4 præsenteres med det formål senere at sammenholde dem med processerne i Cobit 5. ISO/IEC 20000-4 indeholder 25 processer angående it service management, hvor hver procesbeskrivelse har et formål og en række resultater. I dette afsnit vil formålene præsenteres.

19.1.1 Audit

Formålet med processen er uafhængigt at fastsætte overensstemmelsen mellem udvalgte service, produkter og processer med passende krav, planer og aftaler.[156]

19.1.2 Budgeting and Accounting for IT Services

Formålet med processen er at budgettere og redegøre for serviceprovision.[157]

19.1.3 Business Relationship Management

Formålet med processen er at identificere og styre kundebehov og forventninger. [158]

19.1.4 Capacity Management

Formålet med processen er at sikre, at serviceudbyderen har tilstrækkelig service kapacitet til at møde nuværende og fremtidige aftalte krav.[159]

[155] *ISO/IEC 20000-4 s. v-vi*
[156] *ISO/IEC 20000-4 s. 3*
[157] *ISO/IEC 20000-4 s. 4*
[158] *ISO/IEC 20000-4 s. 4*
[159] *ISO/IEC 20000-4 s. 5*

18.1.5 Change Management

Formålet med processen er at sikre at alle ændringer er vurderet, godkendt, implementeret og gennemgået på en kontrolleret måde. [160]

19.1.5 Configuration Management

Formålet med processen er at etablere og vedligeholde integriteten af alle identificerede servicekomponenter. [161]

19.1.6 Human Resource Management

Formålet med processen er at forsyne virksomheden med de nødvendige menneskelige ressourcer og vedligeholde deres kompetencer i overensstemmelse med virksomhedens behov og servicekrav. [162]

19.1.7 Improvement

Formålet med processen er, at kontinuerligt forbedre SMS'et, service og processer.[163]

19.1.8 Incident Management and Request Fulfillment

Formålet med processen er at genoprette serviceaftaler og opfylde serviceforespørgsler indenfor aftalte serviceniveauer. [164]

19.1.9 Information Item Management

Formålet med processen er at udvikle og vedligeholde den indhentede information, der produceres af en proces. [165]

---

[160] *ISO/IEC 20000-4 s. 5*
[161] *ISO/IEC 20000-4 s. 6*
[162] *ISO/IEC 20000-4 s. 6*
[163] *ISO/IEC 20000-4 s. 7*
[164] *ISO/IEC 20000-4 s. 8*
[165] *ISO/IEC 20000-4 s. 9*

19.1.10Information Security Management

Formålet processen er at styre informationssikkerheden på et aftalt niveau af sikkerhed indenfor alle service management aktiviteter. [166]

19.1.11 Management Review

Formålet med processen er at vurdere præstationen af SMS'et og identificere potentielle forbedringer.[167]

19.1.12 Measurement

Formålet medprocessen er at identificere, samle, analysere og rapportere data relateret til tilvejebragte services og implementerede processer for at understøtte effektiv styring af processer og for objektivt at demonstrere kvaliteten af den tilvejebragte service. [168]

19.1.13 Organizational Management

Formålet med processen er at etablere service management målene, identificere og tilvejebringe ressourcer og overvåge præstationen af it serviceprovision for at opfylde krav fra kunder og interesserede parter. [169]

19.1.14 Problem Management

Formålet med processen er at minimere serviceforstyrrelser.[170]

[166] *ISO/IEC 20000-4 s. 10*
[167] *ISO/IEC 20000-4 s. 10*
[168] *ISO/IEC 20000-4 s. 11*
[169] *ISO/IEC 20000-4 s. 12*
[170] *ISO/IEC 20000-4 s. 13*

19.1.15 Release and Deployment Management

Formålet med processen er at sætte nyudviklede udgivelser ind i virksomhedens live miljø på kontrolleret vis. [171]

19.1.16 Risk Management

Formålet med processen er at identificere, analysere, evaluere, behandle og overvåge risici kontinuerligt. [172]

19.1.17 Service Continuity and Availability Management

Formålet med processen er at sikre, at aftalte serviceniveauer opnås under forudsigelige omstændigheder. [173]

19.1.18 Service Design

Formålet med processen er at designe og udvikle nye eller ændrede service. [174]

19.1.19 Service Level Management

Formålet med processen er at sikre, at aftalte serviceniveaumål opnås for hver kunde. [175]

19.1.20 Service Planning and Monitoring

Formålet med processen er at planlægge og overvåge provisionen af en ny eller ændret service. [176]

[171] *ISO/IEC 20000-4 s. 13*
[172] *ISO/IEC 20000-4 s. 14*
[173] *ISO/IEC 20000-4 s. 14*
[174] *ISO/IEC 20000-4 s. 15*
[175] *ISO/IEC 20000-4 s. 15*
[176] *ISO/IEC 20000-4 s. 16*

19.1.21 Service Reporting

Formålet med processen er at producere rettidige og akkurate servicerapporter som understøtter en effektiv kommunikation og beslutningstagning. [177]

19.1.22 Service Requirements

Formålet med processen er at etablere og vedtage servicekravene.[178]

19.1.23 Service Transition

Formålet med processen inkluderer opbygningen, test og acceptering af den nye eller ændrede service efterfulgt af at gøre den nye eller ændrede service operationel. [179]

19.1.24 SMS Establishment and Maintenance

Formålet med processen er at levere de service management processer, der aktiverer effektiv implementering og styring af alle it services. [180]

19.1.25 Supplier Management

Formålet med processen er at sikre, at leverandørservice er integreret i serviceleveringen for at opnå de aftalte krav.[181]

[177] *ISO/IEC 20000-4 s. 17*
[178] *ISO/IEC 20000-4 s. 17*
[179] *ISO/IEC 20000-4 s. 18*
[180] *ISO/IEC 20000-4 s. 19*
[181] *ISO/IEC 20000-4 s. 20*

ISO/IEC 38500

I det efterfølgende afsnit vil ISO/IEC 38500 blive gennemgået for derved at sammenholde den med Cobit 5's processer. Derved bliver det muligt, at konkludere om ISO/IEC 38500 understøtter Cobit 5.

Udgifter til it kan udgøre en betydelig udgiftspost for virksomheder, hvor afkastet fra investeringen ikke altid konstateres fuldstændigt. Dette kan have en negativ indvirkning på den tekniske, økonomiske og planlægningsmæssige del af it aktiviteterne i virksomheden, som derved får indvirkning på virksomheden set som helhed. Derfor har ISO og IEC udarbejdet standarden *ISO/IEC 38500 - Corporate governance of information technology* for at give ledelsen et effektivt framework, som kan være behjælpeligt til at få den øverste ledelse til at forstå og derved også opfylde deres etiske, retslige og regulerende forpligtelser overfor virksomhedens anvendelse af it.[182]

Denne standard skelner mellem governance og management.[183] Management er enheden, hvor kontroller og processer bliver udarbejdet, som er krævet for at opnå virksomhedens overordnede strategiske mål, hvilket er formuleret af virksomhedens øverste ledelse, samt er underlagt politiske retningslinjer.[184] Derimod er governanceenheden den, der foreskriver og kontrollerer virksomhedens overordnede retningslinjer.[185]

Standarden fremsætter vejledende principper, som kan være en hjælp til blandt andet bestyrelsen, direktionen og den daglige ledelse med en acceptabel, kompetent og effektiv anvendelse af virksomhedens it ressourcer. Desuden henvender standarden sig til governance- og managementprocesser og beslutninger, der relaterer til informations- og kommunikationsprodukter, som bliver anvendt i virksomheden Dette er såvel, hvis disse processer bliver varetaget af it specialister i virksomheden, som hvis processerne bliver outsourcet til serviceleverandør.[186]

[182] *ISO/IEC 38500 s. V*
[183] *ISO/IEC 38500 s. V*
[184] *ISO/IEC 38500 s. 4*
[185] *ISO/IEC 38500 s. 3*
[186] *ISO/IEC 38500 s. 1*

Standarden opsætter en model som den øverste ledelse bør anvende, når der anvendes it i virksomheden. Denne model indebærer, at der burde fokuseres på tre hovedopgaver, hvad angår it anvendelse.

Den første hovedopgave at *Evaluate* på den nuværende og fremtidige anvendelse af it. Dette udføres ved, at den øverste ledelse kan lave vurderinger og undersøgelser, så der bliver fokus på den anvendte it, og om denne er tilstrækkelig, eller der skal foretages tilrettelæggelser på dette område. I overvejelserne bør indgå såvel ydre som indre påvirkninger som eksempelvis den teknologiske udvikling, lovgivningsmæssige krav eller det økonomiske aspekt. Denne evaluering skal være kontinuerlig, så der således altid opfanges forandringer, der er nødvendige at være opmærksomme på. Virksomhedens nuværende og fremtidige behov er ligeledes et punkt, den øverste ledelse skal være opmærksomme på for at sikre en konkurrencemæssig fordel for virksomheden frem for konkurrenterne, samtidig med disse behov understøtter virksomhedens overordnede strategi.

Den anden hovedopgave er *Direct,* som skal bidrage til, at der bliver implementeret it relaterede beslutninger og målsætninger, som understøtter virksomhedens overordnede forretningsstrategi. Den øverste ledelse bør tildele ansvar for og vejlede tilrettelæggelse samt implementering af planlægning og målsætninger. Desuden bør den øverste ledelse sikre, at overgangen fra it projekter til implementeringen af it projekterne er ordentligt ledet og planlagt, så det ikke influerer negativt på den nuværende it struktur og infrastruktur. Forebyggelse af en virksomhedskultur omkring it ledelse ved at sørge for, at den daglige ledelse tilvejebringer rettidig information omkring implementeringen, som skal understøttes af de seks it principper, er med til at opnå en optimal adfærd, når der skal implementeres it projekter i virksomheden.

Den sidste hovedopgave for den øverste ledelse er at *Overvåge* præstationen af it projektet gennem hensigtsmæssige målingssystemer. Dette skal vise om planlægningen harmonerer med udførelsen, og om it projektet matcher virksomhedens forretningsstrategi.[187]

Standarden indeholder efterfølgende en vejledning for virksomhedsstyring af it, hvor de nedenstående seks principper bliver sammenholdt med den opsatte model i standarden, så *Evaluate, Direct* og *Moni-*

[187] *ISO/IEC38500 s. 7 + 8*

tor bliver bekrevet under hvert princip. Dette giver det inspiration til en fremgangsmåde så enhver type virksomhed kan opnå den vejledning, som er nødvendigt for netop dén virksomhed.

Således er målet med denne standard at fremme en kompetent, acceptabel og effektiv anvendelse af it i alle virksomheder. Dette opnås ved at sørge for, at virksomhedens interessenter kan have tillid til, at virksomheden ved efterlevelse af standarden opnår en sikker anvendelse af virksomhedens it styring. Samtidig sikrer standarden, at den øverste ledelse opnår en balance ved at minimere potentiel risiko og fremme de muligheder, som opstår ved anvendelsen af it.[188]

20 Principper i ISO/IEC 38500

ISO/IEC 38500 opstiller en struktur for optimal virksomhedsstyring af it, hvor der indgår seks principper. Disse principper udtrykker en optimal adfærd, når der skal træffes beslutninger i virksomheden. Principperne er en redegørelse af, hvad der burde forekomme i situationen, men ikke præcist hvornår, af hvem og hvordan de skal implementeres, da alle virksomheder er forskellige. Dog er det nødvendigt, at den øverste ledelse får gennemført en etablering af principperne.

20.1 Responsibility

Inden for virksomheden skal både individer og afdelinger forstå og acceptere deres ansvar i forbindelse med it. De individer eller afdelinger, som har ansvar for en handling vil derved også have autoritet til at udføre denne handling.

20.2 Strategy

Den strategiske it plan for virksomheden skal tilfredsstille det nuværende og kommende behov for at opnå virksomhedens samlede forretningsstrategi.

[188] *ISO/IEC38500 s. 1*

20.3 Acquisition

Der skal være valide begrundelser for, at virksomheden foretager nye it anskaffelser. Det skal foregå på baggrund af hensigtsmæssige og vedvarende analyse med en forståelig og evident beslutningsproces. Virksomheden skal opnå den optimale løsning, hvad angår kortsigtede samt langsigtede fordele, muligheder, risici og ulemper ved anskaffelsen af nye it investeringer.

20.4 Performance

It er optimalt til det formål at understøtte virksomheden i at levere en service, graden af den leverede service samt kvaliteten af denne service, der kræves for at opfylde de nuværende og fremtidige forretningsmæssige krav.

20.5 Conformance

Der skal eksistere overensstemmelse med de lovgivningsmæssige og regulerede krav til it, ligesom politikker og praksis skal være defineret, implementeret og underbygget.

20.6 Human Behaviour

It beslutninger og praksis skal have respekt for den menneskelige adfærd, der eksisterer i virksomheden. Dette inkluderer opmærksomhed omkring nuværende og fremtidige behov hos de personer, der er involveret.[189]

[189] *ISO/IEC38500 s. 6*

CMMI

I dette afsnit vil CMMI frameworket, som en vejledning til virksomheder så de derved har mulighed for at forbedre virksomhedens processer, blive præsenteret og dets processer gennemgået med det formål at sammenholde processerne i CMMI med processerne i Cobit 5.[190] Der er udarbejdet tre frameworks henholdsvis CMMI for Development (CMMI-DEV), CMMI for Acquisition (CMMI-ACQ) og CMMI for Services (CMMI-SVC). Disse frameworks er udarbejdet af medlemmer fra diverse erhverv, det offentlige samt Software Engineering Institute (SEI).[191]

En Capability Maturity Model (CMM), hvor CMMI indgår, er en simplificeret fremstilling af virkeligheden og indeholder de væsentlige elementer fra effektive processer. SEI benytter følgende tilgang til ledelsesprocessen: "*the quality of a system or product is highly influenced by the quality of the process used to develop and maintain it*,"[192] og denne forudsætning understøttes af kvalitetsudviklingen i de publicerede standarder fra ISO/IEC. CMM fokuserer således på at forbedre elementer fra effektive processer, som eksempelvis når umodne processer bliver disciplineret eller i forvejen modne processer bliver effektiviseret og forbedre kvaliteten af processen. CMMI giver en vejledning til at udvikle processer i virksomheden, men hvilke faktiske processer virksomhederne anvender, afhænger af virksomheden, applikationsdomæner, struktur og størrelse.[193]

Begrebet CMMI tilvejebringer den nødvendige struktur til at producere CMMI modelkomponenter, CMMI læringskomponenter og CMMI vurderingskomponenter. For at det bliver muligt at anvende flere modeller indenfor CMMI begrebet er modelkomponenter klassificeret som enten fælles for alle CMMI-modellerne eller anvendelig for en enkelt CMMI-model.[194]

Modelkomponenterne er inddelt i tre kategorier henholdsvis komponentkrav, forventede komponenter

[190] SEI: *CMMI for Development s. XV*
[191] SEI: *CMMI for Development s. XV*
[192] SEI: *CMMI for Development s. 9*
[193] SEI: *CMMI for Development s. 9*
[194] SEI: *CMMI for Development s. 14*

og informative komponenter. Komponentkravene er en CMMI komponent, der er nødvendig for at opnå en procesforbedring på et procesområde, som skal gennemføres indenfor alle virksomhedens processer. Komponentkravene i CMMI er de *specifikke mål*, som beskriver de unikke kriterier, der skal være tilstede for, at det givne procesområde opnås på en tilfredsstillende måde, hvor de *generiske mål* beskriver de kriterier, som skal være tilstede for at institutionalisere processer, der er implementeret på procesområdet.[195] Målopfyldelse er anvendt i den endelige vurdering af om et procesområde er opnået tilfredsstillende. De forventede komponenter er CMMI komponenter, der skildrer de væsentligste aktiviteter for at opnå det krævede CMMI komponent. Disse komponenter vejleder de personer, der gennemfører disse forbedringer eller foretager vurderingerne. De forventede komponenter i CMMI er de *specifikke og generiske fremgangsmåder*, der er væsentlige for at opnå det tilhørende mål, som er beskrevet ovenfor. Før disse mål anses for opfyldte, skal de være præsenteret i de planlagte og gennemførte processer i virksomheden. Til sidst er de informative komponenter CMMI komponenter, der hjælper brugerne af CMMI til at forstå de foregående to modelkomponenter ved hjælp af detaljerede forklaringer og andre oplysninger.[196]

CMMI Model Foundation (CMF) er betegnelsen for det fælles materiale, som ligger til grund for CMMI modellerne. Komponenterne i CMF er en del af alle CMMI-modellerne, som udspringer fra CMMI begrebet. Disse komponenter fra CMF er kombineret med det relevante materiale indenfor hver interesseområde til at producere en CMMI-model. Disse interesseområder er henholdsvis:

- Development: Udvikling af produkter eller service.
- Acquisition: Anskaffelse af produkter eller service.
- Services: Etablere, styre og levere service.

Indenfor begrebet CMMI anvendes betegnelsen *konstellation* for en samling af CMMI komponenter, som anvendes til at konstruere model-, lærings- og vurderingsmateriale indenfor de tre ovennævnte

[195] Med institutionalisere menes den forankrede rutinemæssige og kulturelle måde, som en virksomhed styrer sin virksomhed på.
[196] SEI: *CMMI for Development s. 20*

interesseområder.[197] Alle CMMI-modellerne udspringer fra CMMI frameworket. Dette framework indeholder de formål og den praksis, der skal anvendes til at producere CMMI-modellerne. Disse CMMI-modeller tilhører komponenterne model, læring og vurdering, der er organiseret i de omtalte konstellationer. CMMI-DEV, CMMI-ACQ og CMMI-SVC indeholder alle 16 kerneprocesområder, der er begreber, som er grundlæggende for forbedring af virksomhedens processer på de tre interesseområder. Dele af det anvendte materiale til kerneprocesområderne er det samme i alle konstellationer, hvor andet materiale kan justeres, så det passer til de enkelte interesseområder (development, acquisition eller services).[198]

CMMI modellerne refererer ofte til virksomhedens helhed. Denne helhed er nødvendig for at opnå værdiskabelse, styre indsatser, tilpasse processer og foretage vurderinger. I CMMI-SVC betegnes denne helhed som "work groups", mens det i CMMI-DEV og CMMI-ACQ betegnes som "projects".[199] Derfor er nogle af titlerne af kerneprocesserne forskellige fra CMMI-SVC i forhold til CMMI-ACQ samt CMMI-DEV. Dette omhandler processerne "Work Planning", "Work Monitoring and Control", "Integrated Work Management" og "Quantitative Work Management". Selvom der eksisterer forskelle omhandler processerne det samme.[200]

21 Kerneprocesser i CMMI

21.1 Causal Analysis and Resolution (CAR)

Formålet med denne proces er at identificere årsager til udvalgte resultater og foretage handlinger til at forbedre processens præstation.[201]

[197] SEI: *CMMI for Development s. 14*
[198] SEI: *CMMI for Development s. 19*
[199] SEI: *CMMI for Service s. 17*
[200] SEI: *CMMI for Service s. 19*
[201] SEI: *CMMI for Development s. 233*

21.2 Configuration Management (CM)

Formålet med denne proces er at etablere og vedligeholde integriteten af arbejdsprodukter ved anvendelse af konfigurationsidentifikation, konfigurationskontrol, en redegørelse af konfigurationsstatus redegørelse og konfigurationsrevision.[202]

21.3 Decision Analysis and Resolution (DAR)

Formålet med denne proces er at analysere mulige beslutninger ved anvendelse af en formel evalueringsproces, der evaluerer identificerede alternativer mod etablerede kriterier.[203]

21.4 Integrated Project Management (IPM)

Formålet med denne proces er at etablere og styre projektet og involveringen af relevante interessenter i overensstemmelse med en integreret og defineret proces, som er udformet på baggrund af virksomhedens standardprocesser.[204]

21.5 Measurement and Analysis (MA)

Formålet med denne proces er at udvikle og opretholde en egnethedsmåling, der anvendes til at understøtte ledelsens informationsbehov.[205]

21.6 Organizational Process Definition (OPD)

Formålet med denne proces er at etablere og vedligeholde et brugbart sæt af organisationsprocesaktiver, standarder for arbejdsmiljø og regler samt retningslinjer for teams.[206]

[202] SEI: *CMMI for Development s. 243*
[203] SEI: *CMMI for Development s. 257*
[204] SEI: *CMMI for Development s. 267*
[205] SEI: *CMMI for Development s. 287*
[206] SEI: *CMMI for Development s. 303*

21.7 Organizational Process Focus (OPF)

Formålet med denne proces er at planlægge, implementere og udnytte organisationsprocesforbedringer baseret på en grundig forståelse af virksomhedens processer og procesaktivers nuværende styrker og svarheder.[207]

21.8 Organizational Performance Management (OPM)

Formålet med denne proces er på proaktiv vis at styre virksomhedens præstation for at måle virksomhedens forretningsmål.[208]

21.9 Organizational Process Performance (OPP)

Formålet med denne proces er at etablere og vedligeholde en kvantitativ forståelse af præstationen af udvalgte processer i virksomhedens sæt af standardprocesser, som fundament til at opnå kvalitet og mål for procespræstationen samt tilvejebringe data på procespræstationer, basislinjer og modeller til på kvantitativ vis at styre virksomhedens projekter.[209]

21.10 Organizational Training (OT)

Formålet med denne proces er at udvikle kompetencer og viden for personerne i virksomheden, så de kan anvende deres roller effektivt.[210]

21.11 Project Monitoring and Control (PMC)

Formålet med denne proces er at tilvejebringe en forståelse af projektets fremgang således, at de rette korrigerende handlinger kan blive foretaget, når projektets præstation signifikant afviger fra det tiltænkte.[211]

[207] SEI: *CMMI for Development s. 317*
[208] SEI: *CMMI for Development s. 331*
[209] SEI: *CMMI for Development s. 351*
[210] SEI: *CMMI for Development s. 365*
[211] SEI: *CMMI for Development s. 393*

21.12 Project Planning (PP)

Formålet med denne proces er at etablere og vedligeholde projekter, som definerer projektaktiviteter.[212]

21.13 Process and Product Quality Assurance (PPQA)

Formålet med denne proces er at forsyne personale og ledelsen med objektiv indsigt i processer og associerede arbejdsprodukter.[213]

21.14 Quantitative Project Management (QPM)

Formålet med denne proces er på kvantitativ vis at styre projektet for at opnå projektets fastsatte kvalitets- og procespræstationsmål.[214]

21.15 Requirements Management (REQM)

Formålet med denne proces er at styre kravene til projektets produkter og produktkomponenter samt forsikre overensstemmelse mellem disse krav og projektets planer og arbejdsprodukter.[215]

21.16 Risk Management (RSKM)

Formålet med denne proces er at identificere potentielle problemer før de opstår således, at risikohåndteringsaktiviteter kan planlægges og påkaldes efter behov hen over produktet eller projektets livscyklus for at minimere ufordelagtige konsekvenser i forhold til opnåelse af mål.[216]

22 Capability Levels og Maturity Levels

Virksomhederne, som anvender CMMI frameworket, bør forstå, hvordan procesområderne fungerer for, at de opfylder virksomhedens behov for procesforbedring.[217] Dette understøtter CMMI ved at be-

[212] SEI: *CMMI for Development s. 403*
[213] SEI: *CMMI for Development s. 425*
[214] SEI: *CMMI for Development s. 433*
[215] SEI: *CMMI for Development s. 473*
[216] SEI: *CMMI for Development s. 481*
[217] SEI: *CMMI for Development s. 31*

nytte to fremgangsmåder til at iværksætte forbedring ved at anvende niveauer. Disse to niveauer er henholdsvis egnethedsniveau og modenhedsniveau, hvor de ligeledes kaldes repræsentationer. Repræsentationerne opdeles i løbende repræsentationer og planlagte repræsentationer, hvor den løbende repræsentation skal anvendes for at opnå et egnethedsniveau og den planlagte repræsentation skal anvendes for at opnå et modenhedsniveau. Den planlagte repræsentation anvender modenhedsniveauerne til at karakterisere virksomhedens processer som en helhed, hvor den løbende repræsentation anvender egnethedsniveauerne til at karakterisere tilstanden af virksomhedens processer i forhold til den enkelte proces. Hvis en virksomhed skal opnå et bestemt niveau, skal denne opfylde samtlige mål indenfor procesområdet, som virksomheden har opsat, om det så er et egnetheds- eller modenhedsniveau. Begge repræsentationer angiver løsninger til at forbedre virksomhedens processer og derved opnå de forretningsmæssige mål, der eksisterer i virksomheden, ligesom begge repræsentationer anvender de samme modelkomponenter.[218]

Egnethedsniveauerne er en metode til trinvist at forbedre fremgangsmåderne til et procesområde. Niveauerne er inddelt i fire med numrene 0-3. Modenhedsniveauernes anvendelse på en virksomhedsprocesforbedring er på tværs af flere procesområder og inddeles i fem niveauer på skalaen 1-5 jævnfør nedenstående figur.[219]

Figur 3 – Sammenligning af egnetheds- og modenhedsniveau

Niveau	***Egnethedsniveau***	***Modenhedsniveau***
0	Ufuldstændig	
1	Udført	Foreløbig
2	Håndteret	Håndteret
3	Identificeret	Identificeret
4		Kvantitativt behandlet
5		Optimeret

Kilde: Egen tilvirkning med inspiration fra SEI: *CMMI for Development s. 34*

[218] SEI: *CMMI for Development s. 32*
[219] SEI: *CMMI for Development s. 33*

Et egnethedsniveau er opnået, når samtlige generiske mål er opfyldt. En *ufuldstændig proces* er, når en proces enten ikke er udført eller er delvist udført, samtidig med et eller flere af de specifikke mål ikke er tilfredsstillende, og der ikke eksisterer generiske mål. En *udført proces* er, når det nødvendige arbejde og de specifikke mål til procesområdet er opfyldt. Niveau to er opfyldt, når en proces er *håndteret.* Dette anses for opnået, når processen er i overensstemmelse med virksomhedens politikker, involvering af virksomhedens interesserenter, kontrolleret, revideret, overvåget, virksomheden beskæftiger kompetente medarbejdere samt processen bliver evalueret. En *identificeret proces* er, når en proces er styret og tilpasset virksomhedens standardprocesser og retningslinjer. Forskellen mellem niveau to og tre er omfanget af standarder, procesbeskrivelser og procedurer.[220]

Hvert modenhedsniveau modner en væsentlig delmængde af virksomhedens processer, som er med til at forberede virksomheden til at opnå det næste modenhedsniveau på skalaen. Et modenhedsniveau er opnået, når virksomheden har opfyldt de specifikke og generiske mål, der er tilknyttet procesområdet. Som ovenstående figur illustrerer, er modenhedsniveauer inddelt i niveauerne et til fem, hvor niveau to og tre anvender de samme vilkår som niveauerne to og tre i egnethedsniveauet, da disse er komplementære.[221] *Foreløbige processer* er typisk processer, som virksomheden anvender ad hoc, eller som ikke fungerer optimalt. Virksomheder på dette niveau kan producere velfungerende produkter, men har ofte svært ved at overholde budgetter og tidsplaner, der er opsat. Når en proces er *håndteret,* er processerne planlagte, udføres i overensstemmelse med de politikker, udført af kvalificerede medarbejdere, de relevante interessenter er blevet involveret, de anvendte ressourcer er kontrolleret og revideret samtidig med, at der evalureres på processen. Ved en *identificeret proces* forstås, at processen er velkarakteriseret, forstået samt processen er beskrevet i standarder, procedurer og fremgangsmåder. Standarderne medvirker til at skabe sammenhæng på tværs af virksomheden, og at disse er skræddersyet til et bestemt procesområde. Er processen *kvantitativt behandlet,* bliver der opsat kvantitative mål for kvalitet og præstation af processen. Kvantitative mål er opsat på baggrund af kundens behov, virksomheden og procesinteressenterne. Kvalitet og procespræstationer styres ved at anvende statistiske redskaber og andre kvantitative teknikker. Når en proces er *optimeret* på modenhedsniveau fem, bliver den kontinu-

[220] SEI: *CMMI for Development s. 35+36*
[221] SEI: *CMMI for Development s. 41+42*

erligt vurderet på baggrund af kvantitative forståelser for virksomhedens mål og resultatindikatorer. Dette niveau fokuserer på en løbede procesforbedring gennem gradvis, innovative og teknologiske forbedringer.[222]

Ved at gennemføre en vurdering og måle virksomhedens fremskridt i egnetheds- og modenhedsniveauer, kan virksomheder identificere områder, hvor det vil være fordelagtigt at effektuere forbedringer. Til dette kan virksomheden anvende en "Appraisal Requirements" for CMMI (ARC), som opdeles i klasse A, B og C, hvor klasse A foretager en fuld benchmarking, og de to andre klasser er mindre formelle. The Standard CMMI Appraisal Method for Process Improvement (SCAMPI) er den formelle CMMI-vurderingsmetode, der anvendes til at evaluere virksomhedens processer. [223]

23 CMMI for Development

CMMI-DEV fremsætter et integreret sæt af retningslinjer for udvikling af virksomhedens produkter og serviceydelser, hvor formålet er at levere en vejledning, så virksomheden opnår det optimale ved udvikling af kvalitetsprodukter samt serviceydelser, som skal opfylde slutbrugernes behov.[224]

Virksomheder ønsker at levere hurtigere, bedre og billigere produkter og serviceydelser til deres kunder for at opnå en konkurrencemæssigfordel i forhold til konkurrenterne. Dog er det mere komplekse produkter og serviceydelser, som virksomheden i dag producerer på grund af den teknologiske udvikling. Dette har bevirket, at virksomheder ikke selv udvikler alle de anvendte komponenter til deres produkter, men i stedet anvender serviceleverandører til at aflaste kapaciteten. Derved bliver anvendelsen af en tredjepart en integreret udformningsproces af virksomhedens endelige produkter, hvor denne komplekse udvikling og vedligeholdelsesproces er virksomhedernes ansvar at styre og kontrollere, og en sådan effektiv kontrol og styring er afgørende for virksomhedens succes. Virksomhederne har behov for at udvikle deres aktiviteter, så de understøtter det overordnede forretningsmæssige mål. [225]

[222] SEI: *CMMI for Development s. 43+44*
[223] SEI: *CMMI for Development s. 105*
[224] SEI: *CMMI for Development s. XV*
[225] SEI: *CMMI for Development s. 3*

Ved at anvende CMMI-DEV giver det virksomhederne mulighed for at undgå eventuelle faldgruber, da frameworket fokuserer på udvikling af produkter og tjenesteydelser ligesom der fokuseres på produktets livcyklus fra ide til vedligeholdelse. CMMI-DEV indeholder 22 procesområder, hvoraf ét er et fællesprocesområde Supplier Agreement Management (SAM), som er en proces, der er delt af mindst to af CMMI-modellerne, men ikke af alle modellerne. 16 er kerneprocesområderne, der er nævnt i forrige afsnit, som er ensartet i alle CMMI-modellerne. De resterende fem er udviklingsspecifikke procesområder, henholdsvis Technical Solution (TS), Product Integration (PI), Requirements Development (RD), Verification (VER) og Validation (VAL).[226]

Kerneprocesserne og de processer der er specifikke til CMMI-DEV, er beskrevet i CMMI-DEV part two. Da kerneprocesserne allerede er blevet beskrevet i det forgående afsnit, er det blot de CMMI-DEV specifikke processer, som behandles.

23.1 CMMI-DEV Processerne

23.1.1 Supplier Agreement Management (SAM)

Formålet med denne proces er at styre tilegnelsen af produkter og services fra leverandører.[227]

23.1.2 Product Integration (PI)

Formålet med denne proces er at samle produktet ud fra produktkomponenter, sikre at det integrerede produkt agerer som planlagt, altså besidder den rette funktionalitet og kvalitet samt leverer produktet.[228]

23.1.3 Requirements Development (RD)

Formålet med denne proces er at udløse, analysere og etablere kundekrav, produktkrav og produktkomponentkrav.[229]

[226] SEI: *CMMI for Development s. 4*
[227] SEI: *CMMI for Development s. 497*
[228] SEI: *CMMI for Development s. 377*
[229] SEI: *CMMI for Development s. 455*

23.1.4 Technical Solution (TS)

Formålet med denne proces er at udvælge, designe og implementere løsninger til stillede krav. Løsninger, design og implementeringer omfatter produkter, produktkomponenter og produktrelaterede livscyklusprocesser enten enkeltvis eller passende kombineret.[230]

23.1.5 Validation (VAL)

Formålet med denne proces er at demonstrere, om et produkt eller produktkomponent opfylder produktets tilsigtede anvendelse, når det placeres i det tilsigtede miljø.[231]

23.1.6 Verification (VER)

Formålet med denne proces er at sikre, at udvalgte arbejdsprodukter opnår deres specificerede krav.[232]

24 CMMI for Acquisition

Flere og flere virksomheder anvender serviceleverandører, når de skal anskaffe produkter i den bedste kvalitet, til den laveste pris samt med den optimale teknologi.[233] Når en virksomhed vælger at anskaffe produkter fra en serviceleverandør, er det nødvendigt, at serviceleverandøren har en forståelse af, hvordan ansvaret er fordelt mellem de to parter. Virksomheden, der anskaffer et produkt, har ansvar overfor slutbrugeren af produktet. Virksomheden, der anskaffer et produkt, vil derfor være ansvarlig for produktet, mens serviceleverandøren eksempelvis er ansvarlig for, at dette produkt bliver leveret til tiden. Derfor er det nødvendigt for at imødegå de udfordringer, der kan opstå ved anvendelse af en serviceleverandør, samt at kommunikationen imellem virksomheden og dens leverandører fungerer optimalt.[234]

[230] SEI: *CMMI for Development s. 509*
[231] SEI: *CMMI for Development s. 531*
[232] SEI: *CMMI for Development s. 541*
[233] SEI: *CMMI for Acquisition s. 3*
[234] SEI: *CMMI for Acquisition s. 4*

CMMI-ACQ gør det muligt for virksomheder at undgå eller eliminere barrier i anskaffelsesprocessen. CMMI-ACQ indeholder 22 procesområder, hvoraf 16 af disse processer er kerneprocesser, som tidligere er beskrevet.[235] Kerneprocesserne og de processer der er specifikke til CMMI-ACQ, er beskrevet i CMMI-ACQ part two. Da kerneprocesserne allerede er blevet beskrevet i det forgående afsnit er det blot formålene med de processer, der er specifikke til CMMI-ACQ, der i det følgende præsenteres.

24.1 CMMI-ACQ Processerne

24.1.1 Agreement Management (AM)

Formålet med denne proces er at sikre, at leverandøren og erhververen agerer indenfor rammen af leverandøraftalen.[236]

24.1.2 Acquisition Requirements Development (ARD)

Formålet med denne proces er at udløse, udvikle og analysere kunde- og kontraktkrav.[237]

24.1.3 Acquisition Technical Management (ATM)

Formålet med denne proces er at evaluere leverandørens tekniske løsninger og styre udvalgte interface af løsningen.[238]

24.1.4 Acquisition Validation (AVAL)

Formålet med denne proces er at demonstrere, at et anskaffet produkt eller service opfylder dets tilsigtede anvendelse, når det placeres i dets tilsigtede miljø.[239]

[235] SEI: *CMMI for Acquisition s. 3 - 4*
[236] SEI: *CMMI for Acquisition s. 191*
[237] SEI: *CMMI for Acquisition s. 199*
[238] SEI: *CMMI for Acquisition s. 215*
[239] SEI: *CMMI for Acquisition s. 229*

24.1.5 Acquisition Verification (AVER)

Formålet med denne proces er at sikre, at udvalgte arbejdsprodukter opfylder deres specificerede krav.[240]

24.1.6 Solicitation and Supplier Agreement Development (SSAD)

Formålet med denne proces er at forberede en anmodningspakke, udvælge en eller flere leverandører til at levere produktet eller servicen og etablere samt vedligeholde leverandøraftalen.[241]

25 CMMI for Services

Vejledning for udvikling og forbedring af serviceprocedurer er nødvendigt for at forbedre præstationer, kundetilfredshed og rentabilitet. Disse behov forsøges dækket af CMMI-SVC.

Alle processerne i CMMI-SVC fokuserer på serviceaktiviteter, hvoraf 17 er kerneprocesser, og syv er CMMI-SVC specifikke processer tilknyttet service.[242] Da CMMI-SVC beskriver 17 kerneprocesser fremfor 16 kerneprocesser, som i CMMI-ACQ og CMMI-DEV, er det fordi Supplier Agreement Management (SAM), er en proces, der er delt med CMMI-DEV. Formålene med kerneprocesserne er gennemgået tidligere, og de syv specifikke processer for service behandles i nedenstående afsnit.

25.1 CMMI- SVC Processerne

25.1.1 Capacity and Availability Management (CAM)

Formålet med denne proces er at sikre effektive servicesystempræstationer, sikre forsyning af ressourcer og at ressourcerne anvendes effektivt til at understøtte servicekravene.[243]

[240] SEI: *CMMI for Acquisition s. 237*
[241] SEI: *CMMI for Acquisition s. 497*
[242] SEI: *CMMI for Services s. 3*
[243] SEI: *CMMI for Services s. 261*

25.1.2 Service Continuity (SCON)

Formålet med denne proces er at etablere og vedligeholde planer til at sikre kontinuiteten af service under og efter enhver signifikant forstyrrelse af normal drift.[244]

25.1.3 Service Delivery (SD)

Formålet med Service Delivery (SD) er at levere service i overensstemmelse med serviceaftaler.[245]

25.1.4 Incident Resolution and Prevention (IRP)

Formålet med denne proces er at sikre rettidige og effektive løsninger af servicehændelser samt passende undgåelse af servicehændelser.[246]

25.1.5 Service System Transition (SST)

Formålet med denne proces er at udnytte nye eller signifikant ændrede service systemkomponenter samtidig med at styre deres effekt på igangværende servicelevering.[247]

25.1.6 Service System Development (SSD)

Formålet med denne proces er at analysere, designe, udvikle, integrere, verificere og validere servicesystemer, herunder service system komponenter, for at tilfredsstille nuværende og forventede serviceaftaler.[248]

25.1.7 Strategic Service Management (STSM)

Formålet med denne proces er at etablere og vedligeholde standardservice i sammenhæng med strategiske behov og planer.[249]

---

[244] SEI: *CMMI for Services s. 523*
[245] SEI: *CMMI for Services s. 539*
[246] SEI: *CMMI for Services s. 315*
[247] SEI: *CMMI for Services s. 595*
[248] SEI: *CMMI for Services s. 561*
[249] SEI: *CMMI for Services s. 609*

PRINCE 2

I dette afsnit vil The Office of Governance Commence's (OGC) Prince2 framework præsenteres. Prince2 er en procesdrevet projektstyringsmetode, og frameworkets processer gennemgås i det følgende med det formål senere at sammenholde Prince2's processer med processerne i Cobit 5.

Et projekt adskiller sig fra andre processer, fordi det er en midlertidig organisation inden for virksomheden, der er lavet med det formål at levere ét eller flere forretningsprodukter baseret på en udformet business case. Projekter og måden hvorpå virksomheden introducerer forandringer, er tværgående over hele virksomheden, og de er unikke samt risikofyldte. Projektstyring handler om at planlægge, uddelegere, overvåge og kontrollere alle aspekter af et projekt og motivationen af de involverede for at opnå projektets mål, hvad angår tid, omkostninger, kvalitet, rækkevide, fordele og risici. Det der gør Prince2 til en accepteret metode for projektstyring er, at den er generisk, idet managementdelen af projektarbejdet er isoleret fra specialistdelen. [250]

Der er seks variabler involveret i ethvert projekt, og derved er der seks aspekter af projektet, som skal styres. De seks variable er costs, timescales, quality, scope, risk og benefits.[251] Prince2 er et framework bestående af processer og temaer, der håndterer planlægning, delegering, overvågning og kontrol af alle seks aspekter af projektet. Prince2 frameworket er baseret på syv principper og syv temaer. Principperne og temaerne kommer til anvendelse i frameworkets syv processer, og i det følgende gennemgås principperne og processerne.

26 Principper i Prince2

Da Prince2 frameworket er principbaseret er det muligt at tilvejebringe en projektstyringsmetode, der kan anvendes uafhængigt af projektets skala, type, organisation, geografi og kultur. Adopteringen af de syv principper er afgørende for, om en virksomhed anvender Prince2.[252]

[250] OGC: *Managing Successful Projects with PRINCE2 s. 3-5*
[251] OGC: *Managing Successful Projects with PRINCE2 s. 5*
[252] OGC: *Managing Successful Projects with PRINCE2 s. 11*

26.1 Continued Business Justification

Et krav for at starte et projekt på baggrund af Prince2 er, at der er en dokumenteret og vedtaget en forsvarlig grund til at starte projektet. Derforuden skal denne forsvarlighed være opretholdt gennem hele projektforløbet. Denne forsvarlighed dokumenteres i en business case, hvilket sikrer, at projektet konstant er i overensstemmelse med forretningsmål, så virksomheden ikke fortsat arbejder med et projekt, der ikke er fordelagtigt for virksomheden. Hvis et projekt eller forretningen udvikler sig i en sådan grad, at virksomheden ikke længere kan opnå fordel af projektet, bør det stoppes for at hindre ressourcespild.[253]

26.2 Learn from Experience

Projekter er oftest unikke, og arbejdet er baseret på en unik midlertidig funktion inde i virksomheden. Prince2 anbefaler, at inden påbegyndelse af et projekt, betragtes tidligere eller lignende projekter, samt eksterne kilder, med det formål at identificere om tidligere erfaringer kan anvendes på det nystartede projekt. Erfaringer der oparbejdes under projektarbejdet bør løbende dokumenteres og gennemgås med det formål at forbedre projektet gennem hele dets livscyklus. Når projektet afsluttes bør erfaringer fra projektet benyttes i fremtidige projekter, og alle der har taget del i projektarbejdet har ansvar for at identificere erfaringer.[254]

26.3 Defined Roles and Responsibilities

Projektarbejde afhænger af personer, og det er nødvendigt, at det er de rette personer, der deltager i projektarbejdet. Projektarbejde strækker sig typisk på tværs af virksomheden, og der kan derfor være personer med forskellige prioriteter og kompetencer i et projektteam. Projektet skal have en tydelig teamstruktur indeholdende klart definerede roller og ansvar for de, i projektet involverede personer, samt en klar kommunikationskanal.[255]

[253] OGC: *Managing Successful Projects with PRINCE2 s. 11*
[254] OGC: *Managing Successful Projects with PRINCE2 s. 12*
[255] OGC: *Managing Successful Projects with PRINCE2 s. 12*

26.4 Manage by Stages

Prince2 frameworket kræver, at ledelsen deler projektforløbet op i minimum to stadier et ved opstart af projektet og ét eller flere under forløbet. Denne opdeling i stadier sikrer, at ledelsen kan kontrollere projektet i forhold til forretningsprioritet, risiko og kompleksitet. Jo flere stadier et projekt bliver inddelt i desto mere kontrol opnås der, men et mindre antal stadier reducerer ledelsesbyrden. Prince2 håndterer planlægningsdelen ved at opdele projektet i ledelsesstadier, ved at have en high-level projektplan og en detaljeret stadieplan samt ved at planlægge, delegere, overvåge og kontrollere projektet fra stadie til stadie.[256]

26.5 Manage by Exception

Prince2 tilvejebringer den rette governance ved at definere ansvar for dirigering, styring og levering af projektet på hvert niveau. Delegering af autoritet fra ét ledelsesniveau til et andet tilvejebringes ved at fastlægge et toleranceniveau mod seks mål på de enkelte niveauer. Disse mål er time, costs, timescales, quality, scope, risk og benefits. Der skal opsættes kontroller og mekanismer, der sikrer, at disse kontroller er effektive således, at hvis toleranceniveauet for et af disse mål overskrides vil det straks blive kommunikeret op til det næste ledelsesniveau, så det kan besluttes, hvordan der skal fortsættes. På denne måde anvendes seniorledelsen tid effektivt uden, at de mister kontrollen med projektet, da det sikres, at beslutninger bliver taget på det rette niveau i virksomheden.[257]

26.6 Focus on Products

Et succesfuldt projekt er outputorienteret fremfor aktivitetsorienteret. Formålet med et projekt er at opfylde interessenternes behov i overensstemmelse med forretningen. For at tilvejebringe dette skal der være en fælles forståelse af, hvad der forventes af det produkt, der fremkommer af projektet. Et Prince2 projekt benytter produktbeskrivelser til at skabe en fælles forståelse ved at definere hvert produkts formål, sammensætning, oprindelse, format, kvalitetskriterier og kvalitetsmetode. Derved kan det defineres hvor meget tid, ressourcer, aktiviteter med viderer, der skal sættes af til at arbejde med projektet.[258]

[256] OGC: *Managing Successful Projects with PRINCE2 s. 13*
[257] OGC: *Managing Successful Projects with PRINCE2 s. 13*
[258] OGC: *Managing Successful Projects with PRINCE2 s. 14*

26.7 Tailored to suit the project environment

Prince2 frameworket er universelt og kan bruges på alle typer projekter i alle typer miljø, da det er designet til justering i henhold til projektets størrelse, kompleksitet, væsentlighed, kapabilitet og risiko.[259]

27 Processer i Prince2

Prince2 er en procesbaseret tilgang til projektstyring, hvor der eksisterer syv processer, som definerer en række aktiviteter, der er nødvendige for at dirigere, styre og levere et projekt med succes. Processerne i Prince2 er hver struktureret og beskrevet ud fra formål, mål, kontekst og aktiviteter. Hver aktivitet under de syv processer har en tabel, der angiver ansvar for hvert produkt, som fremkommer eller opdateres under aktiviteten.[260]

27.1 Starting up a Project

Formålet med denne proces er at sikre, at det der er baggrunden for "Initiating a Project" processen er fastlagt, ved at stille spørgsmålet: "Har vi et levedygtigt projekt og er det umagen værd?". Den rette information skal samles for at træffe rationelle beslutninger angående anvendelsen af projektet, nøgleroller og ansvarsuddeling. Derigennem er et fundament for en detaljeret planlægning tilgængelig. Målet med denne proces er at præstere det, der minimum er nødvendigt for at beslutte om projektet er fordelagtigt at igangsætte.[261]

27.2 Directing a Project

Formålet med denne proces er at muliggøre, at projektudvalget kan være ansvarlig for projektets succes ved at træffe nøglebeslutninger og træne overordnet kontrol, selvom de uddelegerer dag-til-dag styring af projektet til projektledere.[262]

---

[259] OGC: *Managing Successful Projects with PRINCE2 s. 14*
[260] Producer har ansvar for produktet produktion, Reviewer skal helst være uafhængig af produktionen, Approver bekræfter tilladelsen.
[261] OGC: *Managing Successful Projects with PRINCE2 s. 121-131*
[262] OGC: *Managing Successful Projects with PRINCE2 s. 135-145*

27.3 Initiating a Project

Formålet med denne proces er at etablere et solidt fundament for projektet, hvilket gør det muligt for virksomheden at forstå det arbejde, der skal udføres for at levere projektets produkter, før de forpligter sig til en væsentlig udgift.[263]

27.4 Controlling a Stage

Formålet med denne proces er at uddelegere arbejde, overvåge dette arbejde, håndtere problemer, rapporter fremgang til projektudvalget, og foretage korrigerende handlinger til at sikre, at det pågældende stadie forbliver inden for toleranceniveauet.[264]

27.5 Managing Product Delivery

Formålet med denne proces er at opnå kontrol over linket mellem projektlederen og teamlederen ved at placere formelle krav angående acceptering, eksekvering og levering af projektarbejde. Teamlederen kan enten være intern eller ekstern, og teamlederens rolle er at koordinere et arbejdsområde, der leverer ét eller flere af projektets produkter.[265]

27.6 Managing a Stage Boundary

Formålet med denne proces er at muliggøre, at projektudvalget kan opnå tilstrækkelig information fra projektlederen, så udvalget kan gennemgå successen af det aktuelle stadie, godkende det næste stadie, gennemgå den opdaterede projektplan samt bekræfte fortsat forretningsbelæg og accepten af risici. Denne proces bør derfor udføres i slutningen af hvert ledelsesstadie. Såfremt et projekt ifølge en undtagelsesrapport ikke går som planlagt, kan projektudvalget anmode om at få det nuværende stadie omlagt. Omlæggelsen udfærdiges i en undtagelsesplan, som forelægges for projektudvalgets godkendelse ligesom stadieplanen. [266]

[263] OGC: *Managing Successful Projects with PRINCE2 s. 149-164*
[264] OGC: *Managing Successful Projects with PRINCE2 s. 167-182*
[265] OGC: *Managing Successful Projects with PRINCE2 s. 185-190*
[266] OGC: *Managing Successful Projects with PRINCE2 s. 193-202*

27.7 Closing a Project

Formålet med denne proces er at tilvejebringe et fastlagt punkt, hvorfra acceptering af projektproduktet er bekræftet. Derforuden er formålet at bekræfte om målene, som er opsat i den originale projektigangsættelsesdokumentation, er opnået.[267]

[267] OGC: *Managing Successful Projects with PRINCE2 s. 205-212*

ITIL

I det følgende gennemgås ITIL publikationen med henblik på senere at sammenholde processerne i ITIL med processerne i Cobit 5, for derigennem at besvare afhandlingens problemformulering.

ITIL er del af en række "best-pratice" publikationer for it service management (ITSM). Denne publikation angiver nogle retningslinjer til serviceudbydere angående tilvejebringelsen af høj kvalitet til it services, processer, funktioner og andre elementer, der er nødvendigt for at understøtte disse. Udgiverne af ITIL angiver i introduktionen, at ITIL ikke er en publikation, der skal følges, men derimod en guide der skal læses og forstås, samt benyttes til at skabe værdi for serviceudbyderen og dennes kunder. Virksomheder opfordres til at adoptere ITIL's "best-pratice", såfremt de tilpasser disse til at fungere i deres specifikke miljø på en sådan måde, at virksomhedens behov opnås.[268]

For virksomheder der tilsigter at opnå en certificering efter ISO/IEC 20000-serien, er ITIL en hensigtsmæssig standard til at opnå denne certificering. ITIL frameworket er baseret på fem stadier af en service livscyklus, hvor hver af de fem ITIL publikationer angiver retningslinjer for "best-practice" indenfor hvert stadie. Disse retningslinjer inkluderer nøgle principper, krævede processer og aktiviteter, organisation og roller, teknologi, associerede udfordringer, kritiske succesfaktorer og risici.[269] De fem ITIL publikationer er:

- *ITIL Service Strategy*
- *ITIL Service Design*
- *ITIL Service Transition*
- *ITIL Service Operation*
- *ITIL Continual Service Improvement*[270]

I det følgende vil hver publikations processer gennemgås.

[268] OGC: *ITIL Continual Service Improvement s. 3*
[269] OGC: *ITIL Continual Service Improvement s. 3*
[270] OGC: *ITIL Continual Service Improvement s. 6*

28 ITIL Service Strategy

Kernen i servicelivscyklussen er servicestrategien, og det punkt hvor værdiskabelsen starter. Værdiskabelsen starter med at forstå virksomhedens mål og kundebehov, hvor alle virksomhedens aktiver herunder personer, processer og produkter bør understøtte strategien. ITIL Service Strategy beskriver principper, der understøtter praksis for service management, som er fordelagtigt, når der udvikles service management politikker, guidelines og processer over ITIL service livscyklussen.[271] De fleste af ITIL Service Strategy processerne anvendes gennem hele servicelivscyklussen, men placeres under Service Strategy, da de er centrale for en effektiv servicestrategi.[272] I det følgende gennemgås processerne for ITIL Service Strategy.

28.1 Strategy Management for IT Services

Strategy Management for IT Services er den proces, der anvendes til at definere og vedligeholde en virksomheds perspektiv, position, planer og mønstre angående service og styringen af disse service. Formålet med en service strategi er at formulere, hvordan en serviceudbyder vil muliggøre for virksomheden at opnå dens forrentningsmål. Service strategien etablerer de kriterier og mekanismer, der bestemmer, hvilke service der er hensigtsmæssige til at opnå forretningsmål, og den mest effektive måde at styre service på. Strategi Management for IT Services er den proces der sikre, at strategien er defineret, vedligeholdt og opnår dens formål.[273]

28.2 Service Portfolio Management

Serviceporteføljen er det komplette sæt af service, som styres af en serviceudbyder og anvendes til at håndtere hele livecyklussen af alle service. Serviceporteføljen inkluderer tre kategorier af service. Service der er foreslåede eller under udviklingen, service der er ”live” eller tilgængelige for implementering og service der er udfaset. Serviceporteføljen repræsenterer den investering, der er lavet i en virksomheds service og formulerer værdien, som service tilsigter at realisere. Service Portfolio Management processer er ansvarlige for at styre serviceporteføljen herunder, hvilke service der inkluderes i porteføljen, og hvordan de håndteres gennem livscyklussen. Service Portefølje Management sikre at

[271] *ITIL Service Strategy s. 5*
[272] *ITIL Service Strategy s. 133*
[273] *ITIL Service Strategy s. 133*

serviceudbyderen udelukkende udbyder de service, der bidrager til strategiske mål og møder de aftalte forrentningsmål. Formålet med Service Porteføljе Management er at sikre, at serviceudbyderen har det rette mix af service til at balancere investeringen i it med at opnå forretningsmål.[274]

28.3 Financial Management for IT Services

Formålet med Financial Management for IT Services processen er at sikre, at det eksisterer den rette finansiering til design, udvikling og levering af service, der tilsigter at opnå strategien i virksomheden. Ligeledes skal Financial Management for IT Services sikre, at serviceudbyderen ikke forpligtes til service, som serviceudbyderen ikke kan levere. Financial Management of IT Services identificerer balancen mellem omkostninger og kvaliteten af service, og vedligeholder balancen mellem udbud og efterspørgsel mellem serviceudbyderen og dennes kunder.[275]

28.4 Demand Management

Demand Management er en proces, der omhandler at forstå, forudse og påvirke kunders efterspørgsel på service og anskaffelsen af kapacitet til at dække denne efterspørgsel. Demand Managment fungerer på alle stadier i livscyklussen for at sikre, at service er designet, testet og levereret til at understøtte opnåelsen af forretningsmål ved det rette niveau af aktivitet. Dette er, hvor serviceudbyderen har mulighed for at forstå kundebehovet og indføre disse i servicestrategierne for at realisere kundens servicepotentiale og for at differentiere service mellem kunderne. [276]

28.5 Business Relationship Management

Formålet med Business Relationship Management processen er at etablere og vedligeholde en forretningsrelation mellem serviceudbyderen og kunden, baseret på en forståelse af kunden og dennes forretningsbehov. Processen skal identificere kundebehov og sikre, at serviceudbyderen er i stand til at opnå disse behov eftersom forrentningsbehov ændres over tid og i henhold til situationen. Business Relationship Management processen sikre, at serviceudbyderen forstår disse ændringer i behov og assisterer

[274] OGC: *ITIL Service Strategy s. 170*
[275] OGC: *ITIL Service Strategy s. 200-201*
[276] OGC: *ITIL Service Strategy s. 244-245*

virksomheden i at formulere værdien af en service. Dette betyder, at denne proces sikrer, at kundeforventninger ikke overstiger, hvad kunden er villige til at betale for, og at serviceudbyderen formår at indfri kundens forventninger før de indvilliger i at levere servicen.[277]

29 ITIL Service Design

For at service er værdiskabende for en virksomhed, skal service designes i overensstemmelse med forretningsmål. Design omfatter hele virksomhedens it, da det er virksomheden som en helhed, der leverer og yder support på service. Service Design er det stadie i livscyklussen, der omdanner en service strategi til en plan for levering af forretningsmål. ITIL Service Design angiver vejledning til fremgangsmåden angående design og udvikling af service samt praksis for service management.[278] I det følgende gennemgås processerne for ITIL Service Design.

29.1 Design Coordination

Formålet med Design Coordination processen er at sikre, at målene for servicedesignstadiet opnås ved at levere og vedligeholde et fast punkt for koordination og kontrol for alle aktiviteter og processer indenfor dette stadie af service livscyklussen. [279]

29.2 Service Catalogue Management

Formålet med Service Catalogue Management processen er at levere og vedligeholde en enkelt kilde af konsistent information på alle operative service, og de service der klargøres til at blive operative. Service Caralogue Management processen skal ligeledes sikre, at al information er tilgængelig for autoriserede personer.[280]

[277] OGC: *ITIL Service Strategy s. 256*
[278] OGC: *ITIL Service Design s. 6*
[279] OGC: *ITIL Service Design s. 86*
[280] OGC: *ITIL Service Design s. 97*

29.3 Service Level Management

Formålet med Service Level Management processen er at sikre, at alle nuværende og planlagte it service er leveret til aftalte opnåelige mål. Dette tilvejebringes gennem en konstant cyklus af forhandling, aftaler, overvågning, rapportering på og gennemgang af it servicemål og resultater, samt gennem tilskyndelse af handlinger til at korrigere eller forbedre niveauet på den leverede service.[281]

29.4 Availability Management

Formålet med Availability Management processen er at sikre, at niveauet for tilgængelighed i alle it service indfrier de aftalte tilgængelighedsbehov eller serviceniveaumål på en omkostningseffektiv og rettidig måde. Availability Management processen omhandler at indfri både det nuværende og det fremtidige tilgængelighedsbehov for virksomheden. Availability Management definerer, analyserer, planlægger, måler og forbedrer alle aspekter af tilgængeligheden for it service samt sikre, at alt it infrastruktur, processer, værktøjer, roller med videre er passende til det aftalte tilgængelighedsserviceniveaumål. Processen fastsætter et punkt for fokus og styring af alle tilgængelighedsrelaterede problemer, relateret til såvel service som ressourcer og sikrer, at tilgængelighedsmålene på alle områder er målte og opnåede. [282]

29.5 Capacity Management

Formålet med Capacity Management processen er at sikre, at kapaciteten for it service og it infrastrukturen indfrier de aftalte kapacitets- og præstationsrelaterede krav omkostningseffektivt og rettidigt. Kapacitetsstyring omhandler at opnå såvel nuværende som fremtidige kapacitets- og præstationsbehov for virksomheden.[283]

29.6 IT Service Continuity Management

Formålet med IT Service Continuity Management processen er at understøtte den overordnede forretningskontinuitetsstyring ved at sikre, at ved styring af risici, der kan have konsekvens for it services,

[281] OGC: *ITIL Service Design s. 106*
[282] OGC: *ITIL Service Design s. 125*
[283] OGC: *ITIL Service Design s. 158*

kan it serviceudbyderen altid levere minimum aftalte forretningskontinuitetsrelaterede service. Dette gøres ved at reducere risici angående it service til et aftalt acceptabelt niveau og planlægge og forbedre en genvinding af it service.[284]

29.7 Information Security Management

Formålet med Information Security Management processen er at afstemme it sikkerhed med forretningssikkerhed og sikre at fortroligheden, integriteten og tilgængeligheden af virksomhedens aktiver, informationer, data og it service altid matcher de aftalte forretningsbehov. Målet for denne proces er at beskytte interesserne hos de personer, der har tiltro til og behov for informationen. Ligeledes er målet at beskytte systemerne, der leverer informationerne, mod skade resulteret af fejl angående fortroligheden, integriteten og tilgængeligheden.[285]

29.8 Supplier Management

Formålet med Supplier Management processen er at opnå "value-for–money" fra leverandører og at levere it service af høj kvalitet til virksomheden ved at sikre, at alle kontrakter og aftaler med leverandører understøtter forretningsbehovene, og at leverandøren opfylder deres kontraktlige forpligtelser.[286]

30 ITIL Service Transition

ITIL Service Transition angiver retningslinjer for udvikling og forbedring af evner angående introduktion af nye eller ændrede service i understøttede miljøer. Den beskriver håndteringen af en virksomhedens overgang fra ét stadie til et andet, mens risici kontrolleres og viden, der anvendes ved beslutninger understøttes. ITIL Service Transition sikrer, at værdien som er identificeret i servicestrategien, og som ligeledes er indarbejdet i servicedesignet, på effektiv vis overføres, så denne værdi kan realiseres i servicedriften.[287] I det følgende vil processerne for ITIL Service Transition gennemgås.

[284] OGC: *ITIL Service Design s. 179*
[285] OGC: *ITIL Service Design s. 197*
[286] OGC: *ITIL Service Design s. 207*
[287] OGC: *ITIL Service Transition s. 8*

30.1 Transition Planning and Support

Formålet med Tranisition Planning and Support processen er at levere overordnet planlægning af serviceovergange og at koordinere ressourcerne, som disse overgange behøver.[288]

30.2 Change Management

Formålet med Change Management processen er at kontrollere livscyklussen af alle ændringer, der muliggøre at foretage fordelagtige ændringer med minimum forstyrrelse af it service.[289]

30.3 Service Assets and Configuration Management

Formålet med Service Assets and Configuration Management processen er at sikre, at aktiverne der kræves for at levere service er optimalt kontrolleret, og at nøjagtig og pålidelig information angående disse aktiver er tilgængelig, hvor og når der er behov for informationen. Denne information inkluderer detaljer om, hvordan aktiverne er blevet konfigurerede samt detaljer angående relationerne mellem aktiverne.[290]

30.4 Release and Deployment Management

Formålet med Release and Deployment Management processen er at planlægge, skematisere og kontrollere bygningen, test og indsættelsen af udgivelser, og at levere ny funktionalitet, der behøves af forretningen, mens integriteten af eksisterende service beskyttes. [291]

30.5 Service Validation Management

Formålet med Service Validation Management processen er at sikre, at nye og ændrede it service matcher deres designspecifikationer, og vil opnå forretningsbehovene. [292]

[288] OGC: *ITIL Service Transition s. 51*
[289] OGC: *ITIL Service Transition s. 61*
[290] OGC: *ITIL Service Transition s. 89-90*
[291] OGC: *ITIL Service Transition s. 114*
[292] OGC: *ITIL Service Transition s. 150*

30.6 Change Evaluation

Formålet med Change Evaluation processen er at levere en konsistent og standardiseret metode til at determinere præstationen af serviceændringer set i kontekst med sandsynlig konsekvens på forretningsresultater samt på eksisterende og foreslåede service og it infrastruktur. Den faktiske præstation for en forandring bliver vurderet i forhold til den forventede præstation. Risici og problemer relateret til ændringen identificeres og håndteres. [293]

30.7 Knowledge Management

Formålet med Knowledge Management processen er at dele perspektiver, ideer, erfaring og information. Processen skal sikre, at de delte elementer er til stede på rette tid og sted for at fremme informerede beslutninger, samt forbedring af effektiviteten ved at reducere behovet for at genfinde viden.[294]

31 ITIL Service Operation

ITIL Service Operation beskriver "best practice" for håndtering af service i et understøttet miljø. Den inkluderer vejledning i at opnå effektivitet for levering og support af service for at sikre værdi for kunder, brugere og serviceudbyderen. De strategiske mål realiseres i sidste ende gennem servicedriften, hvilket gør driften central i forhold til realisering af mål.[295] I det følgende vil processerne for ITIL Service Operation blive gennemgået.

31.1 Event Management

Formålet med Event Management processen er at styre hændelser igennem deres livscyklus. Denne livscyklus af aktiviteter angående opdagede hændelser, hændelsernes årsager og determinering af passende kontrolaktiviteter er koordineret af event management processen. Event Management er derfor grundlaget for operationel overvågning og kontrol. Hvis hændelser er programmeret til at kommunike-

[293] OGC: *ITIL Service Transition s. 175*
[294] OGC: *ITIL Service Transition s. 181-182*
[295] OGC: *ITIL Service Operation s. 7*

re operationel information, såvel som advarsler og undtagelser, kan de benyttes som en basis for automatisering af rutineoperationsstyringsaktiviteter.[296]

31.2 Incident Management

Formålet med Incident Management processen er at genvinde normal servicedrift så hurtigt som muligt og minimere den ufordelagtige konsekvens for forretningsdriften, og derigennem sikre at det aftalte service kvalitetsniveau opretholdes.[297]

31.3 Request Fulfilment

Request Fulfilment processen er ansvarlig for styring af livscyklussen for alle serviceforespørgsler fra brugere.[298]

31.4 Problem Management

Formålet med Problem Management processen er at styre livscyklussen for alle problemer, fra første identifikation gennem videre undersøgelse, dokumentation og eventuel fjernelse. Problem Management har til formål at minimere den ufordelagtige konsekvens af hændelser og problemer i forretningen, der er forårsaget af underliggende fejl i it infrastrukturen, samt proaktivt at forhindre gentagelse af hændelser relateret til disse fejl. For at kunne opnå dette, forsøger Problem Management processen at identificere kilder til hændelser, samt dokumentere og kommunikere kendte fejl og påbegynde handlinger til at forbedre eller korrigere situationen. [299]

[296] OGC: *ITIL Service Operation s. 58*
[297] OGC: *ITIL Service Operation s. 73*
[298] OGC: *ITIL Service Operation s. 87*
[299] OGC: *ITIL Service Operation s. 97*

31.5 Access Management

Formålet med Access Management processen er at autorisere retten til brugere til at benytte en service. Processen omhandler derfor udførslen af politikker og handlinger defineret i informationssikkerheds-styring. [300]

32 ITIL Continual Service Improvement

ITIL Continual Service Improvement angiver vejledning angående skabelse og vedligeholdelse af værdi for kunder gennem bedre strategi, design, transition og drift af service. Publikationen kombinerer principper, praksis og metoder for kvalitetsstyring, forandringsstyring og præstationsforbedring[301] I det følgende gennemgås processerne for ITIL Continual Service Improvement.

32.1 The Seven-step Improvement Process

Formålet med The Seven-step Improvement Process er at definere og styre de trin, der er nødvendige for at identificere, definere, samle, behandle, analysere, præsentere og implementere forbedringer.[302]

[300] OGC: *ITIL Service Operation s. 110*
[301] OGC: *ITIL Continual Service Improvement s. 7*
[302] OGC: *ITIL Continual Service Improvement s. 47*

The 2011 Standard of Good Practice for Information Security

I det følgende vil The 2011 Standard gennemgås for at muliggøre en besvarelse af, hvilke af standardens topics, som kan sammenholdes med Cobit 5's processer og domæner for at besvare afhandlingens overordnede problemformulering.

The 2011 Standard er udarbejdet af Information Security Forum (ISF) og indeholder en opdateret version af ISF's tidligere publikation.[303] The 2011 Standard håndterer informationssikkerhed fra et forretningsmæssigt perspektiv og er grundlaget for at vurdere og forbedre virksomhedens informationssikkerhedsforanstaltninger. Derudover indeholder standarden de sikkerhedsforanstaltninger, der er nødvendige for, at den forretningsmæssige risiko i forbindelse med informationssystemer holdes på et minimum. Standarden bidrager såvel til forbedring af kvaliteten og effektiviteten af informationssikkerhedsforanstaltninger som opfyldelse af den lovgivningsmæssige del af informationssikkerhed. The 2011 Standard understøttes blandt andet af ISO/IEC 27001, ISO/IEC 27002 og Cobit 4.1. Derfor kan anvendelsen af standarden eventuelt reducere kompleksiteten af en byrdefuld lovgivning. Hvert år bliver standarden opdateret, så den opfylder behovene hos førerende internationale virksomheder, forbedrer de eksisterende "good practice" samt definerer nye områder indenfor denne praksis, så den forbliver understøttet af andre informationssikkerhedsrelaterede standarder.[304]

Som tidligere beskrevet bliver The 2011 Standard understøttet af kravene fra ISMS, som er fastsat i ISO/IEC 27001 og ISO/IEC 27002, og derfor er denne standard et redskab til at opnå en ISO-certificering. Derudover indebærer understøttelsen af Cobit 4.1, at standarden muliggør compliance med dette framework. De forretningsmæssige fordele som kan opnås ved anvendelse af The 2011 Standard, er fordele som effektivitet ved overholdelse af relevant lovgivning, simplificering ved at harmonere virksomhedens informationssikkerhed, hvilket muliggør omkostningsfordele samt tillid ved

[303] ISF: *The 2011 Standard of Good Practice for Information Security forord*
[304] ISF: *The 2011 Standard of Good Practice for Information Security s. 1*

øget ekstern tiltro til forvaltningen af informationsrisiko og derved forbedring af virksomhedens omdømme.

Derudover kan The 2011 Standard være en fordel for virksomheders informationssikkerhed i forbindelse med relationer til eksterne leverandører, da standarden sikrer, at kravene til informationssikkerheden bliver inddraget i den ordning, som eksisterer med eksterne parter samtidig med, at standarden som helhed er behjælpelig til at forstå og vurdere informationssikkerhed, når virksomheden opererer med eksterne parter. Fordelene ved at anvende The 2011 standard er at give sikkerhed for, at virksomhedens forsyningskæde har et ensartet niveau, hvad angår informationssikkerhed samt at undgå et dårligt omdømme, når virksomheden anvender leverandører.[305]

En informationsrisikovurdering bevirker, at virksomheder kan reducere hyppigheden samt virkningen af informationssikkerhedshændelser ved at forbedre virksomhedens sikkerhedsforanstaltninger. Dette er indarbejdet i The 2011 Standard og derved understøttes standarden af vurdering af risici. Som nævnt er standarden understøttet af ISO/IEC 27001, som ligeledes indeholder dette emne angående risikobehandling. De forretningsmæssige fordele som virksomheden kan opnå ved anvendelse af denne standard er at identificere de forretningsmæssige risici samt opnå kvalitet ved, at virksomheden anvender kontroller for risikovurdering, så virksomheden derigennem kan opnå gennemførelse af en risikoappetit.[306]

The 2011 Standard kan ligeledes anvendes som grundlag for virksomhedens informationssikkerhedspolitik. Standarden kan anvendes til at udfylde de mangler, som eventuelt måtte eksisterer i virksomhedens nuværende politikker, standarder og procedurer, ligesom standarden muliggør udvikling af nye politikker og procedurer. Hvis virksomheden eksempelvis har mange afdelinger eller forretningsenheder, der har udviklet egne poltikker og procedurer kan The 2011 Standard være grundlag for en harmonisering på virksomhedsbasis.[307]

[305] ISF: *The 2011 Standard of Good Practice for Information Security s. 4*
[306] ISF: *The 2011 Standard of Good Practice for Information Security s. 5*
[307] ISF: *The 2011 Standard of Good Practice for Information Security s. 6*

Desuden kan The 2011 Standard forbedre virksomhedens sikkerhedsbevidsthed, samt bevidstheden omkring hvordan informationssikkerheden bør anvendes i virksomhedens lokale miljøer. En forretningsmæssig fordel som virksomheden kan opnå ved anvendelse af standarden kan være en øget troværdighed, da standarden øger forståelsen for informationssikkerhed.[308]

The 2011 Standard kan danne grundlag for en detaljeret vurdering af virksomhedens informationssikkerhed, da anvendelse af benchmarks er en integreret del af standarden. Ud fra disse benchmarks kan der foretages meningsfulde sammenligninger fra lignende virksomheder, og hvordan disse virksomheder anvender informationssikkerhed. Virksomheden kan ved anvendelse af standarden opnå en fordel som tillid ved, at virksomheden bliver kompetente til at afgive en præcis, objektiv og kvantitativ rapportering af virksomhedens informationssikkerhed.[309]

Har en virksomhed behov for at udvikle nye eller forbedre eksisterende oplysninger i sikkerhedsforanstaltningerne, kan The 2011 Standard anvendes som reference. Så snart en forbedring eller udvikling af sikkerhedsforanstaltningerne er foretaget bør disse vurderes og rapporteres, så der er mulighed for at foretage benchmarks. Virksomheden kan opnå forretningsmæssige fordele som at reducere hyppigheden og omfanget af omkostningsmæssige hændelser, opnå omkostningsbesparelser på grund af øget effektivitet igennem anvendelse af standarden og opnå tillid ved at oplysningerne bliver kontrolleret, så opdagede udfordringer bliver håndteret.[310]

33 Kategorier i The 2011 Standard

The 2011 Standard var tidligere opbygget efter et aspektbaseret format, hvor standarden nu er modularopbygget. Det betyder, at standarden nu indeholder fire overordnede kategorier; Security Governance, Security Requirements, Control Framework og Security Monitoring and Improvement. Disse kategorier er inddelt i 26 ”areas”, som derefter er inddelt i 118 ”topics”. Hvert af de 118 ”topics” er designet så muligheden for, at disse kan stå alene eksisterer og omhandler en forretningsaktivitet fra et informationssikkerhedsperspektiv. Security Governance er opdelt i to ”areas” og fem ”topics”, Security

[308] ISF: *The 2011 Standard of Good Practice for Information Security s. 6*
[309] ISF: *The 2011 Standard of Good Practice for Information Security s. 7*
[310] ISF: *The 2011 Standard of Good Practice for Information Security s. 7*

Requirements i to ”areas” og otte ”topics”, Control Framework i 20 ”areas” og 97 ”topics” hvor Security Monitoring and Improvement er inddelt i to ”areas” og otte ”topics”. Det modulære format er velegnet for virksomheder, da dette format er i overensstemmelse med strukturen i ISO/IEC 27000-serien.[311] Standarden skelner mellem specialiserede og fundamentale ”topics”, da denne klassifikation bevirker identificering af, hvilke sikkerhedsforanstaltninger, der har betydning for virksomheden. De fundamentale ”topics” er dem som generelt anvendes til at danne grundlag for virksomhedens informationssikkerhedsprogram og de specialerede ”topics” afhænger af, hvordan virksomheden fungerer.[312] The 2011 Standard har lavet ens ”topic layouts”, så det giver en ensartethed, når standarden anvendes, med en overskrift som indikerer, hvilket ”topic” der bliver behandlet, en kort opsummering af hvilken sikkerhedskontrol, der skal anvendes, formålet med at anvende sikkerhedskontrollen ligesom hver ”topic” bliver nummeret for overskueligheden skyld.[313]

33.1 Security Governance

Security Governance er inddelt i nedenstående to ”areas” og fem ”topics”:

AREA SG1 Security Governance Approach:

- *SG1.1* (S) *Security Governance Framework* – Et framework burde etableres og engagement fremgå fra virksomhedens øverste ledelse for at sikre en overordnet strategi for informationssikkerhed i virksomheden.[314]
- *SG1.2* (F) *Security Direction* – Informationssikkerhedskontrol bør udarbejdes af den øverste ledelse og ledes af den daglige ledelse for, at virksomheden opnår top down struktur og sikre en informationssikkerhedstilgang i virksomheden.[315]

AREA SG2 Security Governance Components:

- *SG2.1* (S) *Information Security Strategy* – Informationssikkerhedsprojekter og tiltag skal være afstemt med virksomhedens strategiske målsætning for at sikre, at informationssikkerheden bi-

[311] ISF: *The 2011 Standard of Good Practice for Information Security s. 8+9*
[312] ISF: *The 2011 Standard of Good Practice for Information Security s. 11*
[313] ISF: *The 2011 Standard of Good Practice for Information Security s. 13*
[314] ISF: *The 2011 Standard of Good Practice for Information Security s. 16*
[315] ISF: *The 2011 Standard of Good Practice for Information Security s. 18*

drager til virksomhedens succes.[316]

- *SG2.2* (S) *Stakeholder Value Delivery* – Virksomheden bør implementere processer til at måle værdien fra informationssikkerhedstiltag samt rapportere resultatet til virksomhedens interessenter for at sikre, at informationssikkerheden bidrager til værdi for disse.[317]
- *SG2.3 I* (F) *Information Security Assurance Programme* – Virksomheden bør indføre en struktureret og kontinuerlig tilgang til informationsrisikostyring for derved at sikre tilstrækkelig behandling af informationsrisikoen.[318]

33.2 Security Requirements

Security Requirements er inddelt i nedenstående to "areas" og otte "topics":

AREA SR1 Information Risk Assessment:

- *SR1.1* (F) *Managing Information Risk Assessment* – Informationsrisikovurderinger bør foretages for virksomhedens tilsigtede forretningsmiljø på en regelmæssig basis, for at identificerede risici holdes indenfor virksomhedens accepterede grænse ved anvendelse af kontroller.[319]
- *SR1.2* (F) *Information Risk Assessment Methodologies* – Informationsrisikovurderinger bør foretages ved anvendelse af strukturerede metoder for at sikre en ensartethed i hele virksomheden samt identificering af de væsentligste risici.[320]
- *SR1.3* (F) *Confidentiality Requirements* – Konsekvenserne ved uautoriseret adgang til informationer i forretningsmiljøet bør vurderes for at sikre, at fortroligheden i forbindelse med disse oplysninger bliver efterlevet.[321]
- *SR1.4* (F) *Integrity Requirements* - Konsekvenserne ved bevidst manipulation af forretningsoplysninger bør vurderes for at sikre, at den anvendte information er gyldig, nøjagtig og fuldstændig.[322]
- *SR1.5* (F) *Availability Requirements* – Konsekvenserne ved utilgængeligt forretningsinformati-

[316] ISF: *The 2011 Standard of Good Practice for Information Security s. 20*
[317] ISF: *The 2011 Standard of Good Practice for Information Security s. 22*
[318] ISF: *The 2011 Standard of Good Practice for Information Security s. 24*
[319] ISF: *The 2011 Standard of Good Practice for Information Security s. 28*
[320] ISF: *The 2011 Standard of Good Practice for Information Security s. 31*
[321] ISF: *The 2011 Standard of Good Practice for Information Security s. 33*
[322] ISF: *The 2011 Standard of Good Practice for Information Security s. 35*

on i længere perioder bør vurderes for at dokumentere og opnå enighed omkring informationstilgængelighed.[323]

- *SR1.6* (F) *Information Risk Treatment* – Informationsrisici bør behandles i overensstemmelse med kravene i virksomheden for at sikre, at informationsrisici bliver minimeret.[324]

AREA SR2 Compliance:

- *SR2.1* (F) *Legal and Regulatory Compliance* – Der bør etableres en proces til at identificere informationssikkerhedsmæssige relevante love og standarder samt for overholdelse af disse.[325]
- *SR2.2* (F) *Information Privacy* – Der bør etableres ansvar for håndtering af personfølsomme oplysninger for at forhindre misbrug af disse samt overholdelse af lovgivningsmæssige krav til beskyttelse af sådanne oplysninger.[326]

33.3 Control Framework

Control Framework er inddelt i nedenstående 20 "areas" og 97 "topics":

AREA CF1 Security Policy and Organisation:

- *CF1.1* (F) *Information Security Policy* – En udførlig dokumenteret informationssikkerhed bør udarbejdes og kommunikeres til alle personer med adgang til virksomhedens informationer samt systemer for at vise den øverste ledelses engagement på informationssikkerhedsområdet.[327]
- *CF1.2* (F) *Information Security Function* – En specialist i sikkerhedsinformations bør eksistere, som har ansvaret for at fremme informationssikkerheden i virksomheden for at sikre "good practice", så informationssikkerheden anvendes effektivt og konsekvent i virksomheden.[328]

[323] ISF: *The 2011 Standard of Good Practice for Information Security s. 37*
[324] ISF: *The 2011 Standard of Good Practice for Information Security s. 39*
[325] ISF: *The 2011 Standard of Good Practice for Information Security s. 41*
[326] ISF: *The 2011 Standard of Good Practice for Information Security s. 43*
[327] ISF: *The 2011 Standard of Good Practice for Information Security s. 50*
[328] ISF: *The 2011 Standard of Good Practice for Information Security s. 52*

AREA CF2 Human Resource Security:

- *CF2.1* (F) *Staff Agreements* – Medarbejdernes ansættelseskontrakt bør omfatte håndtering af informationssikkerhed for at sikre, at medarbejderne understøtter virksomhedens informationssikkerhed og strategi.[329]
- *CF2.2* (F) *Security Awareness Programme* – Der bør gennemføres aktiviteter så bevidsthed omkring sikkerheden opstår hos personer, der har adgang til virksomhedens information og systemer for at sikre en effektiv sikkerhedskultur.[330]
- *CF2.3* (F) *Security Awareness Messages* – Personer, der har adgang til virksomhedens information og systemer, bør have sikkerhedsforanstaltninger kommunikeret på en regelmæssig basis så det sikres, at disse personer kontinuerligt ajourføres og er bevidste omkring væsentligheden af informationssikkerhed.[331]
- *CF2.4* (F) *Security Education / Training* – Medarbejderne bør oplæres i korrekt anvendelse af virksomhedens systemer for, at medarbejderne opnår de nødvendige færdigheder og opfylder deres ansvar, hvad angår informationssikkerhed.[332]
- *CF2.5* (F) *Roles and Responsibilities* – Der bør tildeles individuelt ansvar for virksomhedens kritiske forretningsmiljøer for at opnå optimal beskyttelse af oplysninger, så det bidrager til en ideel forvaltningskultur medarbejderne imellem.[333]

AREA CF3 Asset Management:

- *CF3.1* (S) *Information Classification* – En informationsklassifikationsordning burde etableres i virksomhedens (eksempelvis fortrolig og offentligt) for derved at bestemme, hvilke typer af oplysninger, der skal beskyttes, så uautoriseret videregivelse forhindres. [334]
- *CF3.2* (S) *Document Management* – Dokumenter bør opbevares på en systematisk og struktureret måde samt opfylde kravene for informationssikkerhed for at sikre opfyldelse af lovkrav så oplysninger forbliver tilgængelige, samt følsomme oplysninger forbliver beskyttet fra uautorise-

[329] ISF: *The 2011 Standard of Good Practice for Information Security s. 54*
[330] ISF: *The 2011 Standard of Good Practice for Information Security s. 56*
[331] ISF: *The 2011 Standard of Good Practice for Information Security s. 58*
[332] ISF: *The 2011 Standard of Good Practice for Information Security s. 60*
[333] ISF: *The 2011 Standard of Good Practice for Information Security s. 62*
[334] ISF: *The 2011 Standard of Good Practice for Information Security s. 64*

ret offentliggørelse.[335]

- *CF3.3* (F) *Sensitive Physical Information* – Følsomme oplysninger i fysisk form bør beskyttes mod tab eller udlevering for at sikre informationssikkerheden. Derforuden bør lovkrav på området for håndtering af sådanne oplysninger indfries.[336]
- *CF3.4* (F) *Asset Register* – Hardware og software skal registreres præcist og opdateres i aktivregistreringen, så det bidrager til risikobaserede beslutninger om hardware og software, beskytter aktivet mod tab, opfylder de lovgivningsmæssige krav samt reducerer risikoen for, at informationssikkerheden bliver kompromitteret af svagheder i hardware eller software.[337]

AREA CF4 Business Applications:

- *CF4.1* (S) *Application Protection* – Virksomhedsapplikationer bør beskyttes af fornuftige sikkerhedsprincipper for at sikre konsekvent sikkerhedsfunktionalitet, tilpasning til virksomhedens tekniske infrastruktur samt beskyttelse af oplysninger.[338]
- *CF4.2* (S) *Browser-based Application Protection* – Specialiserede proceduremæssige og tekniske kontroller bør anvendes til interne og browser baserede applikationer samt tilknyttede servere for at sikre, at forbundne risici minimeres.[339]
- *CF4.3* (F) *Information Validation* - Virksomhedsapplikationer bør omfatte sikkerhedskontrol, der beskytter fortroligheden samt integriteten af oplysninger fra disse applikationer [340]

AREA CF5 Customer Access:

- *CF5.1* (F) *Customer Access Arrangements* – Kundernes adgang til virksomhedens applikationer bør fastsættes i forbindelse med forretningsmæssige krav samt godkendelse fra personen, som har ophavsretten til informationen for at sikre, at kundernes adgang opfylder sikkerhedskravene.[341]
- *CF5.2* (S) *Customer Contracts* – Kundernes adgang til virksomhedens applikationer bør under-

[335] ISF: *The 2011 Standard of Good Practice for Information Security s. 66*
[336] ISF: *The 2011 Standard of Good Practice for Information Security s. 68*
[337] ISF: *The 2011 Standard of Good Practice for Information Security s. 70*
[338] ISF: *The 2011 Standard of Good Practice for Information Security s. 72*
[339] ISF: *The 2011 Standard of Good Practice for Information Security s. 74*
[340] ISF: *The 2011 Standard of Good Practice for Information Security s. 76*
[341] ISF: *The 2011 Standard of Good Practice for Information Security s. 77*

støttes af aftaler og godkendte kontrakter for at sikre, at kunderne er juridisk og kontraktmæssig forpligtet til at beskytte virksomhedens oplysninger.[342]

- *CF5.3* (F) *Customer Connections* – Kundernes adgang til virksomhedsapplikationer skal være tydeligt identificeret, registreret og overvåget for at beskytte fortroligheden, integriteten og tilgængeligheden af oplysninger om enten kunden eller virksomheden.[343]

AREA CF6 Access Management:

- *CF6.1* (F) *Access Control* – Der bør indføres adgangskontroller for at begrænse adgangen til virksomhedens systemer for at sikre, at det kun er autoriserede personer, der har adgang til disse systemer, så det muliggør udførelse af deres arbejdsopgaver, men ikke overskridelse af autoritet.[344]
- *CF6.2* (F) *User Authorisation* – Alle personer med adgang til virksomhedens systemer skal godkendes inden adgang til privilegier gives for at begrænse adgangen til virksomhedens systemer til autoriserede personer.[345]
- *CF6.3* (F) *Access Control Mechanisms* – Adgang til virksomhedens systemer bør begrænses til autoriserede personer ved anvendelse af kontrolinstrumenter så det derved sikres, at det kun er disse personer, som har adgang til systemerne.[346]
- *CF6.4* (S) *Access Control Mechanisms – Password* – Computersystemer og netværksenheder, som er konfigurerede med adgangskontroller bør kræve, at brugerne anvender gyldigt brugernavn og adgangskode før adgang til systemer godkendes for at forhindre uautoriseret adgang til virksomhedens systemer og oplysninger.[347]
- *CF6.5* (S) *Access Control Mechanisms – Token* - Computersystemer og netværksenheder, der er konfigureret med adgangskontroller baseret på "token" bør kræve, at brugerne anvender gyldigt "token" som eksempelvis fysisk kendetegn eller chipbaserede kendetegn før adgang til systemerne godkendes for at forhindre uautoriseret adgang til virksomhedens systemer og oplysnin-

[342] ISF: *The 2011 Standard of Good Practice for Information Security s. 80*
[343] ISF: *The 2011 Standard of Good Practice for Information Security s. 82*
[344] ISF: *The 2011 Standard of Good Practice for Information Security s. 84*
[345] ISF: *The 2011 Standard of Good Practice for Information Security s. 86*
[346] ISF: *The 2011 Standard of Good Practice for Information Security s. 87*
[347] ISF: *The 2011 Standard of Good Practice for Information Security s. 89*

ger.[348]

- *CF6.6* (S) *Access Control Mechanisms – Biometric* - Computersystemer og netværksenheder, som er konfigurerede med adgangskontroller baseret på "biometric" bør kræve, at brugerne anvender gyldigt "biometric", som eksempelvis fingeraftryk, irismønster eller stemmekarakteristika før adgang til systemer godkendes for at forhindre uautoriseret adgang til virksomhedens systemer og oplysninger.[349]
- *CF6.7* (F) *Sign-on Process* – Medarbejderne bør have en streng sign-on-proces, før der godkendes adgang til virksomhedens systemer for at sikre autoriseret adgang.[350]

AREA CF7 System Management:

- *CF7.1* (F) *Computer and Network Installations* – Computersystemer og netværksenheder bør udformes, så de opfylder aktuelle og forventede informationsbehandlingskrav.[351]
- *CF7.2* (F) *Server Configuration* – Servere skal konfigureres til at fungere efter virksomhedens behov og for at forhindre uautoriserede eller ukorrekte opdateringer for derved at sikre, at serverene fungerer efter hensigten og ikke kompromitterer sikkerheden af virksomhedens edb-anlæg.[352]
- *CF7.3* (S) *Virtual Servers* – Virtuelle servere skal godkendes og adskille følsomme oplysninger for at forhindre driftsforstyrrelser som følge af overbelastning af systemet.[353]
- *CF7.4* (S) *Network Storage Systems* – Netværkslagringssystemer skal beskyttes ved anvendelse af kontroller for at sikre, at disse systemer fungerer efter hensigten, er til rådighed når behovet opstår og ikke kompromitterer sikkerheden af de oplysninger, som de opbevarer.[354]
- *CF7.5* (F) *Back-up* – Der skal foretages back-up af virksomhedens information og software på en regelmæssigbasis for at sikre, at disse oplysninger og software kan genoprettes ved nedbrud.[355]
- *CF7.6* (F) *Change Management* – Systemændringer bør testes, gennemgås og anvendes ved en

[348] ISF: *The 2011 Standard of Good Practice for Information Security s. 91*
[349] ISF: *The 2011 Standard of Good Practice for Information Security s. 93*
[350] ISF: *The 2011 Standard of Good Practice for Information Security s. 95*
[351] ISF: *The 2011 Standard of Good Practice for Information Security s. 96*
[352] ISF: *The 2011 Standard of Good Practice for Information Security s. 98*
[353] ISF: *The 2011 Standard of Good Practice for Information Security s. 100*
[354] ISF: *The 2011 Standard of Good Practice for Information Security s. 102*
[355] ISF: *The 2011 Standard of Good Practice for Information Security s. 104*

ændringsstyringsproces for at sikre, at ændringerne anvendes korrekt og ikke kompromitterer sikkerheden af virksomhedens systemer.[356]

- *CF7.7* (F) *Service Level Agreements* – Computer- og netværksservice, der understøtter kritiske forretningsprocesser, bør kun leveres af serviceleverandører, hvis disse leverandører opfylder de krævede sikkerhedskontroller for derved at sikre opfyldelse af forretningsmæssige krav til udbyderene.[357]

AREA CF8 Technical Security Infrastructure:

- *CF8.1* (S) *Security Architecture* – En sikkerhedskonstruktion bør etableres, hvilket sikre en ramme for anvendelse af standard informationssikkerhedskontrol, hvor formålet er at systemet opnår sammenhængende og let anvendelige sikkerhedsfunktioner.[358]
- *CF8.2* (S) *Identity and Access Management* – Ordninger til identitets- og adgangsstyring bør indføres så det medfører effektiv og konsistent brugeridentifikation og adgangskontrol i virksomheden for derved at begrænse systemadgangen til autoriserede brugere og sikre integriteten af brugerinformation.[359]
- *CF8.3* (S) *Critical Infrastructure* – Informationssystemer der understøtter infrastruktur bør være beskyttet af sikkerhedsforanstaltninger, der omfatter sikkerhedsplanlægning, vurdering af risici og kontrolaktiviteter.[360]
- *CF8.4* (S) *Cryptographic Solutions* – Kryptografiske løsninger bør godkendes, dokumenteres og anvendes i virksomheden for at beskytte fortroligheden og bevare integriteten af information.[361]
- *CF8.5* (S) *Cryptographic Key Management* – Kryptografiske koder bør styres i overensstemmelse med dokumenterede standarder og beskyttes mod uautoriseret adgang for at sikre, at kritisk information ikke angribes.[362]
- *CF8.6* (S) *Public Key Infrastructure* – Hvor der anvendes offentlig kode infrastruktur (PKI)

[356] ISF: *The 2011 Standard of Good Practice for Information Security s. 106*
[357] ISF: *The 2011 Standard of Good Practice for Information Security s. 108*
[358] ISF: *The 2011 Standard of Good Practice for Information Security s. 110*
[359] ISF: *The 2011 Standard of Good Practice for Information Security s. 113*
[360] ISF: *The 2011 Standard of Good Practice for Information Security s. 115*
[361] ISF: *The 2011 Standard of Good Practice for Information Security s. 117*
[362] ISF: *The 2011 Standard of Good Practice for Information Security s. 119*

skal et certificeringscenter (CA) samt registreringsmyndighed (RA) oprettes og beskyttes for at sikre, at PKI'en fungerer optimal, er tilgængelig når det er nødvendigt og kan inddrives i tilfælde af nødsituationer.[363]

- *CF8.7* (S) *Information Leakage Protection* – Beskyttelse af informationslækage skal anvendes ved systemer og netværk der behandler, opbevarer eller overfører følsomme oplysninger, så det kan identificeres, hvis følsomme oplysninger videregives til uautoriserede personer eller systemer.[364]
- *CF8.8* (S) *Digital Rights Management* – Værdifølsomme oplysninger eller software, der er tilgængelige og anvendes udenfor virksomhedens kontrol, bør beskyttes ved anvendelse af Digital Rights Management (DRM) for at sikre, at adgangen til og behandlingen af oplysningerne er begrænset til bestemte funktioner ved at begrænse antallet af uautoriserede personer[365]

AREA CF9 Network Management:

- *CF9.1* (F) *Network Device Configuration* – Netværksenheder som routere og firewalls skal konfigureres, så de fungerer efter virksomhedens behov og forhindre uautoriserede eller ukorrekte opdateringer for at sikre, at enhederne fungerer korrekt og ikke kompromitterer sikkerheden i netværket.[366]
- *CF9.2* (F) *Physical Network Management* – Netværksenheder bør beskyttes ved fysisk kontrol og understøttes af præcis og opdateret dokumentation så det sikres, at virksomhedens netværk konfigureres korrekt.[367]
- *CF9.3* (F) *External Network Connections* – Eksterne netværksforbindelser til edb-systemer og netværk skal individuelt identificeres, kontrolleres, registreres og godkendes af informationssystemerne for at forhindre, at uautoriserede brugere får adgang til virksomhedens informationssystemer og netværk.[368]
- *CF9.4* (F) *Firewalls* – Netværkstrafik bør sendes via en konfigureret firewall inden der godken-

[363] ISF: *The 2011 Standard of Good Practice for Information Security s. 121*
[364] ISF: *The 2011 Standard of Good Practice for Information Security s. 124*
[365] ISF: *The 2011 Standard of Good Practice for Information Security s. 126*
[366] ISF: *The 2011 Standard of Good Practice for Information Security s. 128*
[367] ISF: *The 2011 Standard of Good Practice for Information Security s. 130*
[368] ISF: *The 2011 Standard of Good Practice for Information Security s. 131*

des adgang til netværket for at forhindre uautoriseret netværkstrafik.[369]

- *CF9.5* (S) *Remote Maintenance* – Fjernvedligeholdelse af systemer og netværk bør begrænses til autoriserede personer for at forhindre uautoriseret adgang til systemer og netværk.[370]
- *CF9.6* (S) *Wireless Access* – Der bør indhentes tilladelse inden trådløs adgang accepteres samt godkendelse af computerenheden. Derudover bør trådløs netværkstrafik krypteres for at sikre, at uautoriserede personer og computerenheder ikke får adgang til virksomhedens netværk for derved at minimere risikoen for, at transmissionerne bliver aflyttet, overvåget eller ændret.[371]
- *CF9.7* (S) *Voice over IP (VoIP) Networks* – IP-telefoni bør godkendes og beskyttes af en kombination af generel netværkskontrol og specifik IP-telefoni kontrol for at sikre tilgængeligheden af IP-telefoni og beskytte fortroligheden og integriteten af informationer i telefonsamtaler.[372]
- *CF9.8* (S) *Telephony and Conferencing* – Faciliteter for telefoni og møder bør beskyttes af fysiske og logiske kontroller, regelmæssig overvågning og begrænset adgang for at forebygge og opdage uautoriseret misbrug af telefoni- og mødefaciliteter.[373]

AREA CF10 Threat and Vulnerability Management:

- *CF10.1* (F) *Patch Management* – En proces bør etableres for indsættelse af system- og softwarepatches for at løse tekniske system- og softwaresårbarheder hurtigt og effektivt for at minimere sandsynligheden for, at sårbarheder udnyttes og får indvirkning på virksomheden, når de opstår. [374]
- *CF10.2* (F) *Malware Awareness* – Personer i virksomheden, der har adgang til virksomhedens information og systemer bør gøres opmærksomme på risici for malware samt foranstaltninger for at mininere risiciene for disse. Derved sikres det, at relevante personer forstår centrale elemeter i beskyttelsen mod malware, samt hvorfor beskyttelsen mod malware er nødvendigt.[375]
- *CF10.3* (F) *Malware Protection Software* – Effektivt software til beskyttelse mod malware skal installeres, konfigureres og vedligeholdes i virksomheden for at beskytte virksomheden mod

[369] ISF: *The 2011 Standard of Good Practice for Information Security s. 133*
[370] ISF: *The 2011 Standard of Good Practice for Information Security s. 135*
[371] ISF: *The 2011 Standard of Good Practice for Information Security s. 136*
[372] ISF: *The 2011 Standard of Good Practice for Information Security s. 138*
[373] ISF: *The 2011 Standard of Good Practice for Information Security s. 139*
[374] ISF: *The 2011 Standard of Good Practice for Information Security s. 140*
[375] ISF: *The 2011 Standard of Good Practice for Information Security s. 142*

angreb fra malware samt sikre, at malwaresmitte kan behandles indenfor den fastsatte tid.[376]

- *CF10.4* (F) *Security Event Logging* – Sikkerhedsrelaterede hændelser skal registreres i logs, beskyttes mod uautoriserede ændringer og analyseres regelmæssigt for at sikre trusselidentifikation, der kan have indvirkning på informationssikkerheden, bevare integriteten af virksomhedens oplysninger og understøtte tekniske undersøgelser.[377]
- *CF10.5* (F) *System / Network Monitoring* – Virksomhedsapplikationer, computersystemer og netværk bør overvåges på regelmæssigbasis og gennemgås fra virksomhedsbrugers perspektiv. Formålet med dette er at vurdere resultaterne fra disse applikationer, systemer og netværk for derved at mindske sandsynligheden for overbelastning og opdage potentiel eller faktisk indtrængen.[378]
- *CF10.6* (F) *Intrusion Detection* – Der bør oprettes instrumenter til at opdage indtrængen i systemer og netværk for at identificere mistanke om eller faktisk angreb, så det muliggør en reaktion inden skaden er sket.[379]

AREA CF11 Incident Management:

- *CF11.1* (F) *Information Security Incident Management* – Informationssikkerhed bør identificeres, reageres på og følges op på med en informationssikkerheds begivenhedsstyringsproces for at identificere og løse informationssikkerhedshændelser hurtigt og effektivt samt minimere effekten og reducere risikoen for lignende hændelser.[380]
- *CF11.2* (S) *Cybercrime Attacks* – Der bør foretages sikkerhedsforanstaltninger for at beskytte virksomhedens oplysninger og systemer mod cybercrime angreb for at reducere hyppigheden og virkningen af cybercrime forsøg og vellykkede angreb.[381]
- *CF11.3* (F) *Emergency Fixes* – Rettelser til edb-udstyr, virksomhedsapplikationer og systemsoftware ved nødssituationer bør afprøves og gennemgås for om det fungerer hurtigt og effektivt for at en reaktion på nødsituationer sker på en rettidig og sikker måde samt reducerer for-

[376] ISF: *The 2011 Standard of Good Practice for Information Security s. 143*
[377] ISF: *The 2011 Standard of Good Practice for Information Security s. 145*
[378] ISF: *The 2011 Standard of Good Practice for Information Security s. 147*
[379] ISF: *The 2011 Standard of Good Practice for Information Security s. 148*
[380] ISF: *The 2011 Standard of Good Practice for Information Security s. 150*
[381] ISF: *The 2011 Standard of Good Practice for Information Security s. 153*

styrrelser i virksomheden.[382]

- *CF11.4* (S) *Forensic Investigations* – En proces bør oprettes til at behandle sikkerhedshændelser, som kræver tekniske undersøgelser for at identificere personerne bag handlingerne og bevare beviser hvis nødvendigt.[383]

AREA CF12 Local Environments:

- *CF12.1* (S) *Local Environment Profile* – En sikkerhedsprofil af hvert lokalmiljø skal dokumenteres og opbevares. Sikkerhedsprofilen skal indeholde erhvervs- og sikkerhedsmæssige detaljer om brugere, information og teknologi for at skildre typen og væsentligheden af virksomheden, hvilket understøtter sikkerhedsmæssige beslutninger relateret til lokalmiljøet.[384]
- *CF12.2* (S) *Local Security Co-ordination* – Tilrettelæggelse bør foretages for at koordinere informationssikkerhedsaktiviteter i de enkelte forretningsenheder for at sikre, at sikkerhedsaktiviteter gennemføres rettidigt og nøjagtigt i virksomheden, og sikkerhedsmæssige komplikationer løses effektivt.[385]
- *CF12.3* (S) *Office Equipment* – Kontorudstyr som netværksprintere bør godkendes, beskyttes af softwarekontrol og være fysisk sikkert placeret for at sikre, at den information, som er lagret eller behandlet i kontorudstyret ikke videregives til uautoriserede personer.[386]

AREA CF13 Desktop Applications:

- *CF13.1* (S) *Inventory of Desktop Applications* – Skrivebordsapplikationer eksempelvis dem som er udarbejdet i regneark eller databaseprogrammer, skal registreres i en inventarliste eller lignende for derved at opretholde en nøjagtig opdateret oversigt over skrivebordsapplikationerne, så de derved kan beskyttes.[387]
- *CF13.2* (S) *Protection of Spreadsheets* – Skrivebordsapplikationer som er udarbejdet i regneark bør beskyttes ved at validere input, gennemføre adgangskontrol og begrænse adgangen til applikationen for derved at sikre nøjagtigheden af oplysningerne, der behandles i regneark og be-

[382] ISF: *The 2011 Standard of Good Practice for Information Security s. 155*
[383] ISF: *The 2011 Standard of Good Practice for Information Security s. 156*
[384] ISF: *The 2011 Standard of Good Practice for Information Security s. 158*
[385] ISF: *The 2011 Standard of Good Practice for Information Security s. 160*
[386] ISF: *The 2011 Standard of Good Practice for Information Security s. 162*
[387] ISF: *The 2011 Standard of Good Practice for Information Security s. 164*

skyttes mod videregivelse til uautoriserede personer.[388]

- *CF13.3* (S) *Protection of Databases* - Skrivebordsapplikationer som er udarbejdet af database-programmer bør beskyttes ved at validere input, gennemføre adgangskontrol og begrænse adgangen til applikationen for derved at sikre nøjagtigheden af oplysningerne, som behandles af databaser og beskytte mod videregivelse til uautoriserede personer.[389]
- *CF13.4* (S) *Desktop Application Development* – Udvikling af skrivebordapplikationer skal udføres i overensstemmelse med en dokumenteret udviklingsmetode for at sikre, at skrivebordapplikationen fungerer optimalt og opfylder sikkerhedskravene.[390]

AREA CF14 Mobile Computing:

- *CF14.1* (S) *Remote Environments* – Medarbejdere, der arbejder andre steder end i virksomhedens lokaler, bør være underlagt krav, bevidste omkring sikkerhedsmateriale og forsynet med sikre og godkendte computerenheder for at sikre, at oplysningerne i fjerntliggende miljøer er beskyttet mod sikkerhedstrusler.[391]
- *CF14.2* (F) *Mobile Device Configuration* – Mobileenheder herunder bærbare computere og smartphones skal konfigureres til at fungere efter behov og beskyttes mod videregivelse af uautoriseret videregivelse af oplysninger for at sikre, at de mobile enheder ikke kompromitterer sikkerheden af de oplysninger, som er lagret på dem samt ved tyveri eller tab.[392]
- *CF14.3* (F) *Mobile Device Connectivity* - Mobileenheder herunder bærbare computere og smartphones skal være forsynet med sikre midler til at oprette forbindelse til netværk for at sikre, at den mobile enhed er beskyttet mod uautoriseret adgang.[393]
- *CF14.4* (S) *Portable Storage Devices* – Anvendelse af bærebare lagerenheder som eksempelvis USB-stik og eksterne harddiske skal godkendes, adgangen til dem begrænses og de lagerede oplysninger beskyttes for at sikre, at oplysningerne er beskyttet mod uautoriseret adgang.[394]
- *CF14.5* (S) *Consumer Devices* – Når en virksomhed tillader forbrugsgoder som eksempelvis

[388] ISF: *The 2011 Standard of Good Practice for Information Security s. 166*
[389] ISF: *The 2011 Standard of Good Practice for Information Security s. 168*
[390] ISF: *The 2011 Standard of Good Practice for Information Security s. 170*
[391] ISF: *The 2011 Standard of Good Practice for Information Security s. 172*
[392] ISF: *The 2011 Standard of Good Practice for Information Security s. 174*
[393] ISF: *The 2011 Standard of Good Practice for Information Security s. 177*
[394] ISF: *The 2011 Standard of Good Practice for Information Security s. 179*

smartphones til erhvervsmæssige formål bør det understøttes af dokumenterede aftaler, at forretningsoplysningerne skal beskyttes for at sikre, at disse oplysninger håndteres på samme måde som, hvis oplysningerne havde befundet sig i virksomhedens udstyr.[395]

AREA CF15 Electronic Communications:

- *CF15.1* (F) *Email* – E-mail-systemer bør beskyttes af sikkerhedsmæssige kontroller som politikker, bevidsthed, proceduremæssige kontroller og tekniske kontroller for at sikre e-mail-tjenester er tilgængelig, når behovet eksisterer, samt meddelelsen er beskyttet af fortrolighed og integritet så risikoen for misbrug minimeres.[396]
- *CF15.2* (S) *Instant Messaging* – Instant messaging tjenester bør beskyttes ved at oprette en politik og implementere instant messaging kontrol for at sikre, at instant messaging tjenester er tilgængelige, når det er påkrævet. Ligeledes skal meddelelsen være fortrolig og integriteten opretholdes så risikoen for misbrug minimeres.[397]

AREA CF16 External Supplier Management:

- *CF16.1* (F) *External Supplier Management Process* – Informationssikkerhedskravene bør overvejes igennem hele forløbet med eksterne leverandører for at beskytte følsomme oplysninger, der overføres i forbindelse med eksterne leverandører.[398]
- *CF16.2* (F) *Hardware / Software Acquisition* – Pålidelig hardware og software skal erhverves under hensyntagen til sikkerhedskrav og identifikation af eventuelle mangler for at sikre, at erhvervet hardware og software fra eksterne leverandører leverer den ønskede funktion og ikke kompromitterer sikkerheden af virksomhedens oplysninger.[399]
- *CF16.3* (S) *Outsourcing*- En proces bør etableres for at styre udvælgelsen og forvaltningen af serviceudbydere herunder dokumenterede aftaleindgåelser, som angiver hvilke sikkerhedsmæssige krav, der skal opfyldes. Dette er for at sikre, at sikkerhedskravene opfyldes og bevares, når driften af en bestemt service er overladt til serviceudbyderen.[400]

[395] ISF: *The 2011 Standard of Good Practice for Information Security s. 181*
[396] ISF: *The 2011 Standard of Good Practice for Information Security s. 183*
[397] ISF: *The 2011 Standard of Good Practice for Information Security s. 185*
[398] ISF: *The 2011 Standard of Good Practice for Information Security s. 186*
[399] ISF: *The 2011 Standard of Good Practice for Information Security s. 189*
[400] ISF: *The 2011 Standard of Good Practice for Information Security s. 191*

- *CF16.4* (S) *Cloud Computing Policy* –En omfattende og dokumenteret proces bør udarbejdes i forbindelse med Cloud Computing tjenester og kommunikeres til alle personer i virksomheden, som kan anvende denne funktion. Dette er for at sikre, at alle virksomhedens medarbejdere er opmærksomme på korrekt anvendelse af Cloud Computing. [401]
- *CF16.5* (S) *Cloud Service Contracts* – Virksomhedens anvendelse af cloud-tjenester bør understøttes af kontrakter, der indeholder særlige cloud-klausuler for at sikre, at cloud-specifikke risici begrænses til et acceptabelt niveau for virksomheden.[402]

AREA CF17 System Development Management:

- *CF17.1* (F) *System Development Methodology* – Udviklingsaktiviteter bør gennemføres i overensstemmelse med en dokumenteret systemudviklingsmetode for at sikre, at virksomhedsapplikationer opfylder forretnings- og informationssikkerhedskrav.[403]
- *CF17.2* (F) *System Development Environments* – Systemudviklingsaktiviteter skal udføres i specialiserede udviklingsmiljøer, som er isoleret fra andre testmiljøer og beskyttes mod uautoriseret adgang for at opnå et sikkert miljø for udviklingsaktiviteter og undgå afbrydelser i virksomhedsaktiviteterne.[404]
- *CF17.3* (F) *Quality Assurance* – Kvalitetssikring af centrale sikkerhedsmæssige aktiviteter bør udføres under systemets udviklingslivcyklus for derved at opnå garanti for, at kravene til sikkerheden er tilstrækkeligt defineret, aftalte sikkerhedskontroller er udviklet samt sikkerhedskravene er opfyldt.[405]

AREA CF18 Systems Development Lifecycle:

- *CF18.1* (F) *Specifications of Requirements* – Forretningsmæssige krav herunder sikkerhedskrav skal dokumenteres og aftales før designet udarbejdes for at sikre, at informationssikkerhedskravene behandles som en integreret del af de forretningsmæssige krav.[406]
- *CF18.2* (F) *System Design* – Informationssikkerhedskravene til systemer under udvikling bør

[401] ISF: *The 2011 Standard of Good Practice for Information Security* s. 193
[402] ISF: *The 2011 Standard of Good Practice for Information Security s. 196*
[403] ISF: *The 2011 Standard of Good Practice for Information Security s. 198*
[404] ISF: *The 2011 Standard of Good Practice for Information Security s. 200*
[405] ISF: *The 2011 Standard of Good Practice for Information Security s. 201*
[406] ISF: *The 2011 Standard of Good Practice for Information Security s. 202*

overvejes, når der designes nye systemer for at producere systemer på velovervejede design-principper, der har indbygget sikkerhedsfunktionalitet, som kan modstå angreb og så systemet ikke indeholder sikkerhedsmæssige svagheder.[407]

- *CF18.3* (F) *System Build* – System opbygningsaktiviteter herunder kodning skal udføres i overensstemmelse med "good practice" og udføres af personer med passende færdigheder samt inspiceres for at identificere uautoriserede modifikationer eller ændringer for at sikre, at systemerne er opbygget korrekt, er i stand til at modstå angreb og opbygningsprocessen ikke indeholder sikkerhedsmæssige svagheder.[408]
- *CF18.4* (F) *Systems Testing* – Systemer under udvikling bør testes i et dedikeret testområde, der simulerer et ægte miljø før systemet anvendes i et ægte miljø for at sikre, at systemet fungerer optimalt og opfylder sikkerhedskravene. [409]
- *CF18.5* (F) *Security Testing* – Systemer under udvikling bør sikkerhedstestes for angreb herunder sårbarhedsvurderinger og adgangskontroltest for at identificere sikkerhedsmæssige svagheder i systemet.[410]
- *CF18.6* (F) *System Promotion Criteria* – Før systemer anvendes i et live miljø skal de opfylde strenge kriterier herunder sikkerhedskrav for at sikre, at det kun er testede systemer som anvendes.[411]
- *CF18.7* (F) *Installation Process* – Nye systemer skal installeres i live miljøet i overensstemmelse med en dokumenteret installationsproces for at minimere forstyrrelser i virksomheden, når nye systemer er installeret i et live miljø.[412]
- *CF18.8* (F) *Post-implementation Review* – Projektopfølgning bør gennemføres for alle nye systemer for at levere garanti for, at informationssikkerheden er behandlet og tilpasset hver fase af systemernes udviklingslivscyklus, samt indbyggede sikkerhedsfunktioner fungerer som forventet.[413]

[407] ISF: *The 2011 Standard of Good Practice for Information Security s. 204*
[408] ISF: *The 2011 Standard of Good Practice for Information Security s. 206*
[409] ISF: *The 2011 Standard of Good Practice for Information Security s. 208*
[410] ISF: *The 2011 Standard of Good Practice for Information Security s. 211*
[411] ISF: *The 2011 Standard of Good Practice for Information Security s. 213*
[412] ISF: *The 2011 Standard of Good Practice for Information Security s. 215*
[413] ISF: *The 2011 Standard of Good Practice for Information Security s. 216*

AREA CF19 Physical and Environmental Security:

- *CF19.1* (F) *Physical Protection* – Steder der indeholder edb-systemer som datacentre, netværk og kommunikationsudstyr bør være fysisk beskyttet mod ulykkestilfælde, angreb eller uautoriseret adgang for at sikre, at det kritiske udstyr er til rådighed for virksomheden, når det er nødvendigt.[414]
- *CF19.2* (F) *Power Supplies* - Steder der indeholder edb-systemer som datacentre, netværk og kommunikationsudstyr bør beskyttes mod strømudfald for at forhindrer ydelser, som leveret af edb-systemer bliver forstyrret af strømafbrydelser.[415]
- *CF19.3* (F) *Hazard Protection* - Steder der indeholder edb-systemer som datacentre, netværk og kommunikationsudstyr bør beskyttes mod brand, oversvømmelser og andre miljømæssige påvirkninger for at sikre, at det kritiske udstyr er til rådighed for virksomheden, når det er nødvendigt.[416]

AREA CF20 Business Continuity:

- *CF20.1* (S) *Business Continuity Strategy* - Der bør etableres en forretningsstrategi, som involverer hele virksomheden, hvilket fremmer behovet for kontinuitet i virksomhedens styring, og derved tilpasser målene for kontinuitetsstyring med virksomhedens forretningsmæssige mål, som giver virksomheden modstandsdygtighed mod forstyrrelser.[417]
- *CF20.2* (S) *Business Continuity Programme* - Der bør fastsættes et virksomhedskontinuitetsprogram, der omfatter udvikling af teknisk infrastruktur, krisestyring og koordinerer og vedligeholder virksomhedskontinuitetsplaner for at virksomheden derved kan modstå manglende adgang til informationer, virksomhedsapplikationer og anden teknisk infrastruktur.[418]
- *CF20.3* (S) *Resilience* – Virksomhedsapplikationer skal køre på pålideligt hardware og software og understøttes af dobbelte faciliteter for at sikre kritiske forretningsprocesser, der er afhængige af, at virksomhedsapplikationer er til rådighed, når der er behov for det.[419]
- *CF20.4* (S) *Crisis Management* – Styring af kriseprocesser bør etableres og understøttes af et

[414] ISF: *The 2011 Standard of Good Practice for Information Security s. 217*
[415] ISF: *The 2011 Standard of Good Practice for Information Security s. 219*
[416] ISF: *The 2011 Standard of Good Practice for Information Security s. 220*
[417] ISF: *The 2011 Standard of Good Practice for Information Security s. 221*
[418] ISF: *The 2011 Standard of Good Practice for Information Security s. 223*
[419] ISF: *The 2011 Standard of Good Practice for Information Security s. 225*

krisestyringsteam, som kan håndtere nødsituationer og angreb. Derved kan der reageres på situationer hurtigere og mere effektivt, samt potentiel indflydelse på virksomheden reduceres.[420]

- *CF20.5* (F) *Business Continuity Planning* – Kontinuitetsplaner skal udvikles og dokumenteres, så planerne understøtter virksomheden forretningsprocesser. Derved kan relevante personer udføre tiltag i tilfælde af nødssituationer, så forretningsprocesserne kan genoptages indenfor normeret tid.[421]
- *CF20.6* (F) *Business Continuity Arrangements* – Alternative virksomhedskontinuitetsarrangementer bør fastsættes for enkelte forretningsområder og være til rådighed efter behov. Derved bliver kritiske forretningsprocesser genoptaget indenfor aftalt tid efter en afbrydelse.[422]
- *CF20.7* (F) *Business Continuity Testing* – Kontinuitetsplaner og arrangementer skal afprøves på en regelmæssig basis, så det giver sikkerhed for, at planerne og arrangementerne vil fungere, så forretningsprocesserne kan genoptages inden for tidsplanerne.[423]

33.4 Security Monitoring and Improvement

Security Monitoring and Improvement er inddelt i nedenstående to "areas" og otte "topics":

AREA SI1 Security Audit:

- *SI1.1* (F) *Security Audit Management* – Informationssikkerhed bør underkastes en grundig, uafhængig og regelmæssig sikkerhedsrevision for at sikre, at sikkerhedskontrollen er gennemført effektivt, risikostyring er håndteret og ledelsen får en uafhængig vurdering af sikkerhedsstatus.[424]
- *SI1.2* (F) *Security Audit Process – Planning* – Sikkerhedsrevision skal underkastes en grundig planlægning, der omfatter identifikation af risici, fastlægge revisionsmål og udarbejde en sikkerhedsrevisionsplan for at sikre, at sikkerhedsrevisionsplanen er udarbejdet efter aftalt metode, kan afsluttes indenfor en acceptabel tidsfrist, og at ingen revisionsaktiviteter mangler.[425]

[420] ISF: *The 2011 Standard of Good Practice for Information Security s. 227*
[421] ISF: *The 2011 Standard of Good Practice for Information Security s. 229*
[422] ISF: *The 2011 Standard of Good Practice for Information Security s. 231*
[423] ISF: *The 2011 Standard of Good Practice for Information Security s. 233*
[424] ISF: *The 2011 Standard of Good Practice for Information Security s. 236*
[425] ISF: *The 2011 Standard of Good Practice for Information Security s. 238*

- *SI1.3* (F) *Security Audit Process – Fieldwork* – Sikkerhedsrevisionsarbejde bør omfatte indsamling af relevant materiale, udføring af test og registrering af resultaterne fra testene for at identificere både ikke-lovmæssige risici og informationsrisici forbundet med forretningsmiljøet.[426]
- *SI1.4* (F) *Security Audit Process – Reporting* – Resultaterne af sikkerhedsrevisionen skal dokumenteres og rapporteres til interessenter for at sikre, at berørte parter er informeret omkring risici, der er forbundet med forretningsmiljøet.[427]
- *SI1.5* (F) *Security Audit Process – Monitoring* – Handlinger til afhjælpning af sikkerhedsrevisionens resultater bør indarbejdes i et arbejdsprogram og løbende overvåges for at sikre, at identificerede risici i forbindelse med sikkerhedsrevisionen behandles effektivt, og at betingelserne er opfyldt.[428]

AREA SI2 Security Performance:

- *SI2.1* (F) *Security Monitoring* – Vilkår for informationssikkerhed skal overvåges kontinuerligt og rapporteres til den øverste ledelse for at forsyne den øverste ledelse med en præcis, omfattende og sammenhængende vurdering af tilstanden for informationssikkerheden i virksomheden.[429]
- *SI2.2* (S) *Information Risk Reporting* – Rapporter om informationsrisiko bør produceres og præsenteres for den øverste ledelse på regelmæssig basis for, at den øverste ledelse får et præcist, omfattende og sammenhængende indblik i informationsrisiciene i virksomheden [430]
- *SI2.3* (S) *Monitoring Information Security Compliance* – En lovgivningsmæssig informationssikkerhedsproces bør etableres for at sikre sikkerhedskontrollen bliver konsekvent og behandles efter informationssikkerheds forpligtelser i forbindelse med love, regler og standarder.[431]

[426] ISF: *The 2011 Standard of Good Practice for Information Security s. 240*
[427] ISF: *The 2011 Standard of Good Practice for Information Security s. 242*
[428] ISF: *The 2011 Standard of Good Practice for Information Security s. 244*
[429] ISF: *The 2011 Standard of Good Practice for Information Security s. 245*
[430] ISF: *The 2011 Standard of Good Practice for Information Security s. 247*
[431] ISF: *The 2011 Standard of Good Practice for Information Security s. 249*

Interview

Som beskrevet i afsnittet *Kildekritik* er der i denne afhandling foretaget interview med personer fra Foreningen af Statsautoriserede Revisorers Informatikudvalg, Kim Stormly Hansen Deputy Chief Audit Executive ved Nykredit, statsautoriseret revisor Thomas Kühn Executive Director hos Ernst & Young, statsautoriseret revisor Claus Thaudahl Hansen Director i KPMG og statsautoriseret revisor Jess Kjær Mogensen Partner i PricewaterhouseCoopers. Formålet med disse interview er at undersøge, hvordan den teoretiske tilgangsvinkel til de gennemgåede frameworks og standarder anvendes i praksis, samt hvordan revisorer kan anvende frameworks og standarder i forbindelse med rådgivning af kunder. Disse interview er foregået på den måde, at de interviewede personer har fået tilsendt de tiltænkte emner via mail, så personerne var forberedte og indstillede på, hvad interviewet ville omhandle.

Angående hvilke frameworks og standarder virksomheder anvender i den daglige ledelse er den generelle opfattelse blandt de interviewede, at det afhænger af virksomheden. Der findes ikke to virksomheder, som er ens, hvad angår størrelse, branche, hovedaktivitet og vilje. Derfor er det også forskelligt, hvilket behov virksomheden har til det framework eller den standard, der skal vejlede ledelsen i styring af it relaterede udfordringer og derved opnå fordel af potentielle muligheder.

Når virksomheder er forskellige findes der ikke ét framework eller én standard, der er optimal for alle virksomheder. Her kan det være nødvendigt for virksomheden at udvælge ideer og processer fra de forskellige frameworks og standarder, og på den måde opbygge virksomhedens egen fortolkning og model til, hvad der er optimalt og væsentligt til brug ved it ledelse i netop den type af virksomhed. Altså kan ledelsen finde inspiration i de publicerede frameworks og standarder til, at udtænke virksomhedens egen gyldne middelvej.

Det er for revisorer nødvendigt at være indforstået med den virksomhed de rådgiver og samtidig have en bred indsigt i de forskellige frameworks og standarder for at yde den mest optimale rådgivning til den individuelle kunde. Dog skal det fremhæves, at det ikke er alle virksomheder, der har behov for rådgivning på it området, da nogle virksomheder enerådigt formår at opnå optimal styring og udnyttel-

se af frameworks og standarder. Det er nødvendigt for virksomheder at have en cost/benefit betragtning med i overvejelserne, når der skal anvendes frameworks og standarder, og især for virksomheder i Danmark grundet virksomhedernes størrelse. Implementeringen af frameworks og standarder skal være omkostningseffektive, så virksomheden opnår optimal udnyttelse af ressourcer, så indsatsen gengældes.

Det kan være en udfordring for virksomheder at udføre vedligeholdelse af de etablerede frameworks og standarder over tid. Én ting er at få implementeret disse frameworks og standarder i virksomheden og en anden er at opnå udbytte fra dem over en længere periode, især hvis de er for omfattende i forhold til, hvad virksomheden kan administrere.[432]

[432] Interview med Kim Stormly Hansen, Thomas Kühn administrerende, Claus Thaudahl Hansen og Jess Kjær Mogensen

Alignment

I teoriafsnittet er udvalgte frameworks og standarder, som revisor kan rådgive ledelsen til at anvende for at få det optimale ud af deres it ressourcer, blevet præsenteret. Disse frameworks og standarder er blevet præsenteret således, at der opnås et overblik over de forskellige frameworks og standarders processer, principper og lignende, hvilket muliggør en sammenligning af disse med domænerne og processerne i Cobit 5.

Denne alignment håndteres således, at hver af Cobit 5's fem domæner er udgangspunktet. Da de, i teorieafsnittet præsenterede frameworks og standarder, er af forskellig opbygning og operationel dybde, er der nogle frameworks og standarder, der kan relateres til enkelte processer indenfor et Cobit 5 domæne, og andre kan relateres til hele domæner. Dette betyder, at der i analysen både vil alignes med hele Cobit 5 domæner, såvel som enkelte processer, såfremt det i forhold til den præsenterede teori er væsentligt.

Bevæggrunden for denne afhandlings analyse er, at hvis en virksomhed vurderer, at der for eksempel er behov for at arbejde med Cobit 5's processer indenfor et bestemt Cobit 5 domæne, så undersøges det hvilke processer, principper eller lignende, fra andre frameworks og standarder, der dækker samme behov for virksomheden. Formålet med denne analyse er, på baggrund af de gennemgåede frameworks og standarder, med Cobit 5 som sammenligningsgrundlag, at præsentere et overblik og illustrere en mapping af disse frameworks og standarder. Derved kan det vurderes, hvordan de forskellige frameworks og standarder understøtter hinanden, og hvordan virksomheden kan anvende disse frameworks og standarder til at håndtere virksomhedens it. Dette er grundlaget for udformning af en konklusion som besvarelse på afhandlingens overordnede problemformulering.

34 Alignment - EDM Domænet

34.1 Enterprise Risk Management

Da formålet med EDM01 er, at der skal foreligge overensstemmelse mellem it relaterede beslutninger og virksomhedens strategi og mål[433], kan dette relateres til ERM frameworket. ERM's framework indeholder ligeledes krav til elementet omkring virksomhedens målsætning, der refererer til, at inden virksomheden kan identificere begivenheder, som kan influere virksomhedens overordnede strategi og herigennem målsætning, er det nødvendigt, at virksomheden har opsat mål. Således opnår virksomheden identifikation af begivenheder, der er relevante for virksomheden, så det kan vurderes om disse begivenheder enten er en risiko eller mulighed. Derved kan ledelsen bestemme en passende reaktion på begivenheden, som skal overvåges for, at information kan videregives og afslutningsvist evalureres så eventuelle modifikationer kan tilpasses risikostyringen.[434]

It relaterede processer skal ifølge EDM01 føres i compliance med lovpligtige og regulerede krav[435], som ligeledes er et krav i ERM, der anbefaler, at der eksisterer overensstemmelse mellem de gældende love og standarder.[436]

Eftersom formålet med EDM02 er at sikre en optimal værdi fra it investeringer, en omkostningseffektiv levering af service og løsninger og et pålideligt indtryk af virksomhedens omkostninger og sandsynlige fordele, så virksomhedens behov kan understøttes effektiv[437], kan denne proces alignes med ERM ved, at dette framework ligeledes er behjælpelig med at undgå mulige faldgruber og overraskelser og i stedet opnå vejledning til at få det optimale ud af enhver situation.[438]

EDM03's formål er at sikre, at it relaterede risici ikke overstiger virksomhedens risikoappetit og toleranceniveau ligesom identificering og styring af it relaterede begivenheder.[439] ERM muliggør sammenhæng mellem virksomhedens risikoappetit og strategi ved, at ledelsen håndterer potentielle risici og

[433] Afsnit: *EDM01 – Ensure Governance Framework Setting and Maintenance*
[434] Afsnit: *Enterprise Risk Management*
[435] Afsnit: *EDM01 – Ensure Governance Framework Setting and Maintenance*
[436] Afsnit: *Enterprise Risk Management*
[437] Afsnit: *EDM02 – Ensure Benefits Delivery*
[438] Afsnit: *Enterprise Risk Management*
[439] Afsnit: *EDM03 – Ensure Risk Optimisation*

vurdere virksomhedens risikoappetit igennem mål og andre strategiske handlinger.[440] Derved understøtter ERM Cobit 5's EDM03 proces, da begge frameworks indeholder vejledning til håndtering af risici samt en vurdering af virksomhedens risikoappetit.

Da EDM04 indeholder håndtering af ressourcestyring [441], kan processen sammenholdes med ERM. ERM indeholder ligeledes kategorien drift, der er virksomhedens effektivisering af de aktuelle ressourcer, som er til rådighed.[442] Ved at begge frameworks behandler, hvordan virksomheden opnår optimal ressourcestyring understøtter disse hinanden.

ERM's rapporteringskategori muliggør, at virksomhedens rapportering anses for pålidelig.[443] Det er nødvendigt for virksomhedens interessenter, at virksomhedens rapportering er troværdig, hvis beslutninger træffes ud fra denne kommunikationsvej. Dette kan sammenholdes med EDM05 processen i Cobit 5, hvis formål er at sikre en effektiv og rettidig kommunikation med virksomhedens interessenter samt etablering af basis for rapportering.[444]

34.2 ISO/IEC 27001 & ISO/IEC 27002

ISO/IEC 27002 indeholder vejledning for risikovurdering og fokuserer på, at virksomheden skal vurdere risici indenfor hvert af ISO/IEC 27002's 11 områder.[445] Dette kan relateres til Cobit 5's EDM03 proces, da begge processer fokuserer på risikostyring af virksomhedens it.[446]

34.3 ISO/IEC 38500

Cobit 5's governance processer behandler interessent governance mål og værdiskabelse, risikooptimering og ressourceoptimering, hvilket inkluderer aktiviteter til at evaluere strategiske muligheder, sikre

[440] Afsnit: *Enterprise Risk Management*
[441] Afsnit: *EDM04 – Ensure Ressource Optimisation*
[442] Afsnit: *Enterprise Risk Management*
[443] Afsnit: *Enterprise Risk Management*
[444] Afsnit: *EDM05 – Ensure Stakeholder Transparency*
[445] Afsnit: *ISO/IEC 27002*
[446] Afsnit: *EDM03 – Ensure Risk Optimisation*

styring af it og overvåge resultaterne.[447] Dette kan sammenholdes med ISO/IEC 38500, da denne standards formål er at opnå en kompetent, acceptabel og effektiv anvendelse af it i alle virksomheder ved, at virksomhedens interessenter kan have tillid til, at virksomheden ved efterlevelse af ISO/IEC 38500 opnår optimal styring af virksomhedens it. Desuden sikrer standarden, at den øverste ledelse opnår den mest optimale løsning til at minimere potentielle risici og fremme virksomhedens muligheder ved anvendelse af it. Da Cobit 5 definerer enablers for virksomhedens governance kan enablerne *Proces* og *Virksomhedsstruktur* kombineret med RACI modellen sammenholdes med ISO/IEC 38500's princip omkring *Responsibility*, der ligeledes omhandler personernes ansvar i virksomheden.[448]

Dette governance domæne indeholder fem EDM processer.[449] ISO/IEC 38500 opsætter en model, som den øverste ledelse bør anvende, når der anvendes it i virksomheden, der ligeledes fokuserer på *Evaluate, Direct og Monitor*.[450]

EDM01 har til formål at sikre overensstemmelse mellem it relaterede beslutninger og virksomhedens overordnede forretningsstrategi og mål. Desuden er EDM01's formål at tilsyn med it relaterede processer bliver ført effektivt og i overensstemmelse med lovgivningsmæssige krav.[451] Denne Cobit 5 proces kan alignes med princippet i ISO/IEC 38500 omkring *Strategy*, der ligeledes beskriver, at virksomhedens strategiske it plan skal tilfredsstille det nuværende og kommende behov for at opnå virksomhedens overordnede forretningsstrategi. Derudover indeholder ISO/IEC 38500's princip omkring *Conformance*, at overensstemmelse med de lovgivningsmæssige og regulerede krav til it skal eksistere.[452]

Da Cobit 5 i processen EDM02 sikrer en vejledning til at opnå optimal værdi fra it investeringer, som samtidig understøtter den overordnede strategi i virksomheden[453], kan dette sammenholdes med ISO/IEC 38500's princip omkring *Strategy*, der redegør for, hvordan virksomhedens strategiske it plan skal opfylde det nuværende og kommende behov for at opnå virksomhedens overordnede strategi.[454]

[447] ISACA: *Cobit 5 – Enabling Processes s. 23*
[448] Afsnit: *ISO/IEC 38500*
[449] Afsnit: *Cobit 5 - Processerne*
[450] Afsnit: *ISO/IEC 38500*
[451] Afsnit: *EDM01 – Ensure Governance Framework Setting and Maintenance*
[452] Afsnit: *ISO/IEC 38500*
[453] Afsnit: *EDM02 – Ensure Benefits Delivery*
[454] Afsnit: *ISO/IEC 38500*

Formålet med EDM03 er at sikre, at de it relaterede risici ikke overstiger virksomhedens risikoappetit og toleranceniveau såvel som at sikre styring og identificering af it relaterede hændelser.[455] EDM03 kan relateres til ISO/IEC 38500's princip omkring *Strategy* ved, at den øverste ledelse skal sikre, at der bliver foretaget den nødvendige risikovurdering og evaluering, når virksomheden anvender it.[456]

EDM04 har til formål at sikre, at virksomheden opnår det optimale af virksomhedens ressourcer gennem evaluering, styring og overvågning af ressourcestyring,[457] hvilket kan sammenholdes med ISO/IEC 38500, da denne ligeledes opsætter en model, der indeholder evaluering, styring og overvågning af virksomhedens it anvendelse.[458]

ISO/IEC 38500's princip omkring *Responsibility*, kan alignes med EDM05 processen, da dette princip omhandler, at personerne i virksomheden bør forstå og accepterer deres ansvar i forbindelse med it. Der redegøres i EDM05 for, at det er governanceenhedens ansvar, at der kan opnås effektiv kommunikation med virksomhedens interessenter samt denne kommunikation bliver evalueret og overvåget, hvilket kan sammenholdes med princippet omkring *Responsibility*.

34.5 The 2011 Standard of Good Practice for Information Security

Cobit 5's EDM01 proces har til formål at sikre overensstemmelse mellem it relaterede beslutninger og virksomhedens overordnede strategi og mål. De it relaterede processer skal føres effektivt og i overensstemmelse med lovgivningsmæssige krav.[459] AREA Security Governance Approach (SG1) i The 2011 Standard indeholder ligeledes topic SG1.1, der foreskriver, at virksomheden burde etablere et framework, samt den øverste ledelse burde udvise engagement omkring beslutningerne for at sikre, virksomheden opnår en overordnet strategi for informationssikkerheden i virksomheden.[460]

AREA SG2 Security Governance Components indeholder SG2.1 og SG2.2, der kan alignes med Cobit 5's proces EDM02. Topic SG2.1 omhandler, at informationssikkerhedsprojekter og tiltag skal være

[455] Afsnit: *EDM03 – Ensure Risk Optimisation*
[456] Afsnit: *ISO/IEC 38500*
[457] Afsnit: *EDM04 – Ensure Ressource Optimisation*
[458] Afsnit: *ISO/IEC 38500*
[459] Afsnit: *EDM01 – Ensure Governance Framework Setting and Maintenance*
[460] Afsnit: *The 2011 Standard - Security Governance*

afstemte med den overordnede målsætning, der eksisterer i virksomheden for derved at bidrage til virksomhedens succes igennem værdiskabelse. Topic SG2.2 fokuserer på at implementere processer til måling af tiltag i forbindelse med informationssikkerhed for derved at sikre, at informationssikkerheden bidrager til værdi.[461] Dette kan alignes med EDM02, da formålet med denne proces er at sikre optimal værdi fra it initiativer, omkostningseffektive løsninger og et pålidelig overblik over omkostninger og mulige fordele, så virksomhedens behov er understøttet effektivt.[462]

Formålet med EDM03 er som tidligere beskrevet at sikre, at de it relaterede forretningsrisici ikke overstiger virksomhedens risikoappetit og toleranceniveau, samt at virkningen af it relaterede risici for virksomheden er identificeret og styret.[463] Denne proces kan sammenholdes med The 2011 Standard topic SG2.3, der fokuserer på, at virksomheden bør indføre en kontinuerlig og struktureret tilgang til håndtering af informationsrisikostyring for at sikre en optimal behandling af informationsrisikoen.[464]

AREA Security Governance Components (SG2) indeholder SG2.2, som anbefaler, at virksomheden bør implementerer processer, som muliggør måling af informationssikkerhedstiltag, samt rapportere disse resultater til virksomhedens interessenter for at sikre, at virksomhedens informationssikkerhed bidrager til at skabe værdi for interessenterne.[465] Dette topic kan sammenholdes med EDM05, hvis formål er, igennem effektiv kommunikation til virksomhedens interessenter, at sikre etablering af basis for rapportering for at bekræfte, at virksomhedens it relaterede mål og strategier er i overensstemmelse med virksomhedens overordnede strategi.[466]

I *Bilag 4* præsenteres en illustrativ oversigt over den udførte alignment for EDM.

[461] Afsnit: *The 2011 Standard - Security Governance*
[462] Afsnit: *EDM02 – Ensure Benefits Delivery*
[463] Afsnit: *EDM03 – Ensure Risk Optimisation*
[464] Afsnit: *The 2011 Standard - Security Governance*
[465] Afsnit: *The 2011 Standard - Security Governance*
[466] Afsnit: Afsnit: *EDM05 – Ensure Stakeholder Transparency*

35 Alignment - APO Domænet

35.1 ISO/IEC 27001 & ISO/IEC 27002

ISO/IEC 27002 området angående *Organization Information Security* har til formål at organisere informationssikkerheden, hvilket kan relateres til Cobit 5's APO01 proces, som ligeledes har til formål at tilvejebringe en konsistent styring af virksomhedens it.[467]

ISO/IEC 27002 området angående *Human Resource Security* angiver krav til virksomhedens håndtering af menneskelige ressourcer[468], hvilket kan relateres til Cobit 5's APO07 proces, som ligeledes fokuserer på at styre de menneskelige ressourcer i virksomheden med det formål at opfylde virksomhedens mål.[469]

ISO/IEC 27001 standarden indeholder under overskriften *Information Security Management Systems* krav til, at virksomheden skal arbejde med ISMS'et, så dette er i overensstemmelse med virksomhedens øvrige forretningsaktivitet og de potentielle risici virksomheden udsættes for. ISO/IEC 27001 angiver en model til, hvordan en virksomhed skal styre deres informationssikkerhed således, at risikoen som informationssikkerheden tilfører virksomheden, mindskes.[470] Dette kan relateres til Cobit 5's APO12 proces, da denne ligeledes fokuserer på at styre it relaterede risici.[471]

ISO/IEC 27002 indeholder vejledning til virksomhedens risikostyring og kan derfor relateres til Cobit 5's APO12 proces.

ISO/IEC 27001 indeholder under overskriften *Information Security Management Systems* krav til at virksomheden etablerer og styrer et ISMS[472], hvilket kan relateres til Cobit 5's APO13 proces, der indeholder, at virksomheden skal overvåge og gennemgå ISMS'et.[473]

[467] Afsnit: *ISO/IEC 27002 - Organization Information Security*
[468] Afsnit: *ISO/IEC 27002 – Human Resource Security*
[469] Afsnit: *APO07 – Manage Human Ressources*
[470] Afsnit: *ISO/IEC 27001*
[471] Afsnit: *APO12 – Manage Risk*
[472] Afsnit: *ISO/IEC 27001*
[473] Afsnit: *APO13 – Manage Security*

ISO/IEC 27002 indeholder ligeledes vejledning til risikostyring og kan således sammenholdes med Cobit 5's APO13 proces.

35.2 ISO/IEC 20000-serien

I afsnittet ISO/IEC 20000-1 angående *Management Responsibility* er der et krav om, at ledelsen hos serviceudbyder, skal sørge for, at en service management plan bliver konstrueret, implementeret og vedligeholdt. Desuden skal ledelsen kommunikere servicekravene og væsentligheden af at lovreguleringer, standarder og kontrakter følges. Ledelsen skal sikre, at der forelægger de rette ressourcer og udføre management gennemgang ved planlagte intervaller samt sikre, at risici angående service bliver vurderet og håndteret.[474] Dette krav kan relateres til Cobit 5's APO01 proces der fokuserer på at tilvejebringe en konsistent management tilgang for at muliggøre opnåelse af målene for virksomhedens governance.[475] Ligeledes kan der relateres til ISO/IEC 20000-2 *The Management System* afsnittet. De processer fra ISO/IEC 20000-4 der, i forbindelse med ledelsens ansvar, kan relateres til Cobit 5's APO01 proces er *Organizational Management, Risk Management, SMS establishment and Maintenance*.

I afsnittet ISO/IEC 20000-1 angående *Establish and Improve the SMS* er der et krav om, at der skal forelægge en politik for løbende forbedringer af SMS'et og service, samt en procedure der angiver autoritet og ansvar for identificering, dokumentering, evaluering, godkendelse, prioritering, varetagelse, måling og rapportering af forbedringer, samt korrigerende og proaktive handlinger.[476] Dette krav kan ligeledes relateres til Cobit 5's APO01 proces, da denne proces fokuserer på at tilvejebringe en konsistent management tilgang. Derudover fokuserer APO01 på at tilvejebringe et framework, der dækker managementprocesser, organisationsstrukturerer, roller og ansvar, pålidelige og repeterbare aktiviteter og kompetencer.[477] Der kan ligeledes relateres til ISO/IEC 20000-2 i afsnittet *Planning and Implementing Service Management*. De processer fra ISO/IEC 20000-4 der, i forbindelse med kontinuerlige for-

[474] Afsnit: *ISO/IEC 20000-1 – Management Responsibility*
[475] Afsnit: *APO01 – Manage the IT Management Framework*
[476] Afsnit: *ISO/IEC 20000-1 – Establish and Improve the SMS*
[477] Afsnit: *APO01 – Manage the IT Management Framework*

bedringer, kan relateres til denne Cobit 5 proces er *Audit, Improvement, Organizational management, SMS Establishment and Maintenance.*

ISO/IEC 20000-4 processen *Service Transition* fokuserer på opbygning, test og acceptering af den nye eller ændrede service efterfulgt af at gøre den nye eller ændrede service operationelle[478], hvilket kan relateres til Cobit 5's APO02 proces, der fokuserer på, at der skal være strategiske planer for virksomhedens it, herunder også planer for fremgangsmåden ved implementering af nye eller ændrede services.[479] Der kan ligeledes relateres til ISO/IEC 20000-2 afsnittet *Planning and Implementing New or Changed Services*, samt til øvrige ISO/IEC 20000-4 processer *Change Management, Management Review, Service Planning and Monitoring, Service Requirements.* Cobit 5's APO02 proces kan tilmed relateres til ISO/IEC 20000-2 i afsnittet *Planning and Implementing Service Management*, samt de relaterede processer fra ISO/IEC 20000-4 *Information Item Management, Organizational Management, Service Planning and Monitoring, SMS Establishment and Maintenance.*

I afsnittet ISO/IEC 20000-1 angående *Management Responsibility* er der krav til, at serviceudbyderens ledelse skal sikre, at der forelægger de rette ressourcer til at vedligeholde SMS'et.[480] Dette kan relateres til APO05's underproces APO05.02, hvor ledelsen skal fastlægge tilgængeligheden og kilden til midler.[481] Relaterede processer fra ISO/IEC 20000-4 er *Organizational Management, Risk Management, SMS Establishment and Maintenance.* Cobit 5's APO05 proces kan ligeledes relateres til ISO/IEC 20000-2 afsnittet *Planning and Implementing New or Changed Services*, samt ISO/IEC 20000-4 processerne *Change Management, Management Review, Service Planning and Monitoring, Service Requirements.*

I ISO/IEC 20000-1 *Establish and Improve the SMS* refereres der til en liste på side 11 i ISO/IEC 20000-1 standarden, som indeholder de punkter som en service management plan skal indeholde eller have en reference til. Et af punkterne omhandler en redegørelse af de finansielle ressourcer, der er nød-

[478] Afsnit: *ISO/IEC 20000-4 – Service Transition*
[479] Afsnit: *APO02 – Manage Strategy*
[480] Afsnit: *ISO/IEC 20000-1 – Management Responsibility*
[481] Afsnit: *APO05 – Manage Portfolio*

vendige for at opnå service management målene.[482] Dette kan relateres til Cobit 5's APO05 proces, da denne proces ligeledes indeholder et punkt, der omhandler finansiering.[483] APO05 kan ligeledes relateres til ISO/IEC 20000-2 i afsnittet *Planning and Implementing Service Management*, samt ISO/IEC 20000-4 processerne *Information Item Management, Organizational Management, Service Planning and Monitoring, SMS Establishment and Maintenance.*

ISO/IEC 20000-4 processen *Budgeting and Accounting for IT Services* kan alignes med Cobit 5's APO06, da begge processer fokuserer på den finansielle del af it styringen.[484] I afsnittet om ISO/IEC 20000-2 findes "best practice" for *Budgeting and Accounting for IT Services* under afsnittet *Serviceleveringsprocesser*. Øvrige relaterede ISO/IEC 20000-4 processer er *Change Management, SMS Establishment and Maintenance.*

ISO/IEC 20000-4 processen *Business Relationship Management*[485] kan alignes med Cobit 5's APO08 proces, da begge processer fokuserer på at identificere kundernes behov, baseret på en forståelse af kunderne og deres forventninger.[486] ISO/IEC 20000-2's "best practice" for Business Relationship Management findes i afsnittet angående *Relationship Processes* og øvrige relaterede ISO/IEC 20000-4 processer er *Change Management Improvement, Information Item Management, Service Planning and Monitoring, SMS Establishment and Maintenance.* I afsnittet om ISO/IEC 20000-2 findes "best practice" for Service Level Management under afsnittet *Service Delivery Processes.*

ISO/IEC 20000-4 processen *Service Level Management* kan relateres til Cobit 5's APO09 proces, da begge processer fokuserer på at sikre, at aftalte mål for serviceniveauet opnås. Denne ISO/IEC 20000 proces har en serviceudbyder vinkel og fokuserer på, at serviceudbyderen opnår de mål, der er aftalt med hver kunde[487], mens Cobit 5 fokuserer på, at it service og serviceniveauer opfylder de nuværende og fremtidige forretningsbehov.[488] Derfor kan det vurderes, at ISO/IEC 20000-4 *Service Level Mana-*

[482] Afsnit: *ISO/IEC 20000-1 – Establish and Improve the SMS*
[483] Afsnit: *APO05 – Manage Portfolio*
[484] Afsnit: *ISO/IEC 20000-4 – Budgetting and Accounting for IT Services*
[485] Afsnit: *ISO/IEC 20000-4 – Business Relationship Management*
[486] Afsnit: *APO08 – Manage Relationships*
[487] Afsnit: *ISO/IEC 20000-4 – Service Level Management*
[488] Afsnit: *APO09 – Manage Service Agreements*

gement og Cobit 5's APO09 proces har det samme formål. Øvrige relaterede ISO/IEC 20000-4 processer er *Business Relationship Management, Change Management, Configuration Management, Improvement, Information Item Management, Measurement, Service Level Management, Service Reporting.*

Cobit 5's APO09 proces kan ligeledes relateres til ISO/IEC 20000-2 afsnittet *Planning and Implementing New or Changed Services*, samt til ISO/IEC 20000-4 processerne *Change Management, Management Review, Service Planning and Monitoring, Service Requirements.*

ISO/IEC 20000-4 processen *Supplier Management* kan alignes til Cobit 5's APO10, da begge processer fokuserer på at håndtere leverandører således, at kundens forretningsbehov opfyldes. Hvor APO10 fokuserer på at håndtere leverandørrisici og sikrer konkurrencedygtig prisfastsættelse[489], fokuserer ISO/IEC 20000 *Supplier Management* processen på at sikre, at service fra leverandører er integreret i serviceleveringen således, at de aftalte krav og dermed kundens behov kan opnås.[490] Tilgangsvinklerne er forskellige, da ISO/IEC 20000 er en vejledning for serviceudbydere, men det overordnede formål med de to processer er ens. Øvrige relaterede ISO/IEC 20000-4 proesser er *Change Management, Configuration Management, Improvement, Information Item Management, Organizational Management, SMS Establishment and Maintenance.* "Best practice" for Supplier Management er præsenteret i ISO/IEC 20000-2 afsnit *Relationship Processes*.

35.3 ISO/IEC 38500

Formålet med APO02 er at sikre, at strategiske it planer er understøttet af virksomhedens mål samt disse mål og det relaterede ansvar er forstået.[491] Dette kan sammenholdes med princippet i ISO/IEC 38500 *Strategy*, da fokus i dette princip ligeledes er, at virksomhedens strategiske it plan skal opfylde virksomhedens behov, og opnå virksomhedens overordnede strategi.[492]

[489] Afsnit: *APO10 – Manage Suppliers*
[490] Afsnit: *ISO/IEC 20000-4 – Supplier Management*
[491] Afsnit: *APO02 – Manage Strategy*
[492] Afsnit: *ISO/IEC 38500*

Derudover kan APO02 ved at fokusere på målsætning sammenholdes med ISO/IEC 38500's princip omhandlende *Performance,* da en effektiv præstationsmåling er afhængig af en optimal model til at kontrollere opnåelsen af de opsatte mål.[493]

APO02's fokus på, at strategiske planer for it er understøttet af virksomhedens mål, kan alignes med ISO/IEC 38500's princip omkring *Conformance,* da dette princip fokuserer på overensstemmelse mellem virksomhedens målsætninger og den anvendte fremgangsmåde.[494]

Processen APO05 definerer, hvordan virksomheden effektivt kan anvende portefølje af programmer og programstyring af investeringer så det sikres, at fordele realiseres og omkostninger optimeres.[495] Denne Cobit proces kan alignes med ISO/IEC 38500 ved, at princippet *Acquisition* ligeledes omhandler at virksomheden skal opnå den optimale løsning, hvad angår fordele, muligheder, risici og ulemper ved anskaffelsen af nye it investeringer.[496]

Formålet med APO07 er at sikre en struktureret tilgang til optimal anvendelse af personerne i virksomheden. Dette inkluderer kommunikation og ansvarsfordeling, en lærings- og udviklingsplan og præstationsforventninger så virksomheden sikrer motiverede medarbejdere.[497] Dette kan alignes med ISO/IEC 38500's princip *Human Behaviour*, da princippet fokuserer på, at it beslutninger burde have respekt for den menneskelige adfærd, som eksisterer i virksomheden herunder de nuværende og fremtidige behov for de involverede personer.[498]

APO09's formål er at sikre optimal service, servicemål samt en dokumenteret serviceaftale, der tilgodeser virksomhedens nuværende og fremtidige behov.[499] Denne proces kan sidestilles med ISO/IEC 38500 ved, at princippet omkring *Performance* ligeledes anser it for optimal til det formål at understøt-

[493] Afsnit: *ISO/IEC 38500*
[494] Afsnit: *ISO/IEC 38500*
[495] Afsnit: *APO05 – Manage Portfolio*
[496] Afsnit: *ISO/IEC 38500*
[497] Afsnit: *APO07 – Manage Human Ressources*
[498] Afsnit: *ISO/IEC 38500*
[499] Afsnit: *APO09 – Manage Service Agreements*

te virksomheden i forbindelse med it service, der kræves for at opfylde virksomhedens nuværende og fremtidige krav.[500]

Eftersom formålet med APO10 er at minimere risiko for anvendelse af ikke-ydedygtige leverandører, skal virksomheden allerede ved anskaffelsen af nye systemer være opmærksomme på at udvælge leverandører, som er ydedygtige.[501] Dette kan sammenholdes med ISO/IEC 38500's princip om *Acquisition*, da virksomheden skal opnå den optimale løsning, når nye anskaffelser foretages og herved minimere risici for virksomheden ved anskaffelsen af nye it investeringer som eksempelvis ikke-ydedygtige leverandører.[502]

35.4 CMMI

Cobit 4.1 inkluderer som beskrevet en modenhedsmodel, der kan anvendes til at måle virksomhedens nuværende it relaterede processer for at definere det ønskede modenhedsniveau, så forskellen mellem disse kan fastlægges, hvilket muliggør, løsningsforslag til forbedring af processerne, så virksomheden opnår det ønskede modenhedsniveau. Samtidig er denne modenhedsmodel erstattet med en "Proces Capability Model" i Cobit 5, der opnår samme overordnede mål for vurderingen af processer og understøttelse af procesforbedring. Denne "Proces Capability Model" sikrer derved en metode til at måle præstationerne fra governance- eller managementprocesserne så områderne, hvor forbedring er nødvendigt, identificeres.[503] Dette kan sammenholdes med CMMI frameworket der, ud fra betegnelsen CMM ligeledes fokuserer på at forbedre virksomhedens processer. Som beskrevet opnås dette eksempelvis når umodne processer bliver disciplineret eller allerede modne processer effektiviseres, samt kvaliteten af processen forbedres. Dertil anvender CMMI frameworket ligesom Cobit 4.1 og Cobit 5 henholdsvis egnethedsniveauer og modenhedsniveauer. Derved angiver CMMI en vejledning til at udvikle processer i virksomheden, men hvilke faktiske processer virksomhederne anvender, afhænger af virksomheden.[504]

[500] Afsnit: *ISO/IEC 38500*
[501] Afsnit: *APO10 – Manage Suppliers*
[502] Afsnit: *ISO/IEC 38500*
[503] Afsnit: *Cobit - Process Capability Model*
[504] Afsnit: *CMMI - Capability Levels og Maturity Levels*

CMMI processen *Organizational Training* (OT) kan alignes med Cobit 5's proces APO07, da OT har til formål at udvikle personerne i virksomhedens kompetencer og viden, så personerne derved understøtter virksomhedens strategiske mål effektivt ved at anvende deres funktion optimalt.[505] Dette kan sammenholdes med formålet med APO07, som ligeledes er at sikre en struktureret tilgang til optimal anvendelse af personerne i virksomheden.

Da formålet med CMMI-SVQ's proces *Service System Development* (SSD) er at analysere, designe, udvikle, integrere, verificere og validere service systemer, herunder komponenter til servicesystemet for at tilfredsstille nuværende og forventede serviceaftaler, kan den sammenholdes med APO09 omkring styring af serviceaftaler.[506] I APO09 skal der sikres optimal service samt en dokumenteret serviceaftale, som tilgodeser de nuværende og fremtidige behov i virksomheden. Disse serviceaftaler og kontrakter skal gennemgås og klargøres kontinuerligt for at sikre, at de er effektive og opdaterede, så de indeholder de aftalte vilkår.[507] Derudover kan APO09 sammenholdes med CMMI-ACQ's proces *Agreement Management* (AM), da formålet ved denne proces er at sikre, at erhververen og leverandøren agerer indenfor den fremsatte leverandøraftale.[508]

Formålet med APO10 er at minimere risiko relateret til ikke-ydedygtige leverandører. Det er nødvendigt, at virksomheden allerede ved nye anskaffelser udvælger, identificerer og evaluerer leverandører og de dertilhørende kontrakter, som er mest fordelagtige for virksomheden.[509] Denne risiko kan minimeres ved, at virksomheden forinden indgåelse af nye aftaler undersøger leverandørens bagland. Derved opnår virksomheden belæg for om leverandøren overholder de aftalte vilkår, der er indeholdt i leverandøraftalen. Dette kan sammenholdes med den føromtalte CMMI-ACQ proces AM, hvis formål er at sikre leverandøren og erhververen agerer indenfor aftalevilkårene.[510]

[505] Afsnit: *CMMI – Kerneprocesser*
[506] Afsnit: *CMMI for Services*
[507] Afsnit: *APO09 – Manage Service Agreements*
[508] Afsnit: *CMMI for Acquisition*
[509] Afsnit: *APO10 – Manage Suppliers*
[510] Afsnit: *CMMI for Acquisition*

Såfremt kvaliteten bliver styret sikres der konsistent levering af løsninger og service, som sikrer virksomhedens kvalitetskrav.[511] Dette er formålet med APO11 i Cobit 5, og denne proces kan sammenholdes med processen *Quantitative Project Management* (QPM), hvis formål er på kvantitativ vis at styre projektet så projektets kvalitetsmål derved opnås.[512] Desuden kan APO11 omhandlende kvalitetsstyring alignes med *Process and Product Quality Assurance* (PPQA). Formålet med denne proces er at forsyne personale og ledelsen med indsigt i processer og associerede arbejdsprodukter, så virksomhedens krav til kvalitet derved sikres.[513] Formålet med processen i CMMI-DEV omhandlende *Product Integration* (PI) er at sikre, at det integrerede produkt fungerer som planlagt samt besidder den forventede funktionalitet og kvalitet.[514] Denne CMMI-DEV proces kan ligeledes sammenholdes med APO11. Afslutningsvis kan APO11 sidestilles med *Validation* (VAL), som også er en CMMI-DEV proces. Denne proces demonstrerer, om et produkt opfylder produktets ønskede anvendelse, når produktet placeres i det tilsigtede miljø.[515]

I Cobit 5's APO12 er formålet at integrere it relaterede risici med virksomhedens overordnede risikostyring. Derudover skal virksomheden afstemme omkostningerne og fordelene ved styring af it relaterede forretningsrisici.[516] Denne proces kan sammenholdes med *Risk Management* (RSKM), hvis formål er at identificere potentielle problemer før de opstår. Derved kan risikohåndteringsaktiviteter planlægges for at minimere ufordelagtige konsekvenser i forhold til opnåelse af virksomhedens mål.[517]

35.5 Prince2

Prince2 kan som en struktureret metode til projektstyring relateres til Cobit 5's processer, der omhandler styring af porteføljer herunder APO05. Både Prince2 og Cobit 5's APO05 proces fokuserer på, at projekter kontinuerligt skal justeres og tilpasses virksomheden og planlægges således, at projekternes produkter opfylder forretningsbehovene.[518] Prince2's syv processer omhandler aktiviteter, der er nød-

[511] Afsnit: *APO11 – Manage Quality*
[512] Afsnit: *CMMI - Kerneprocesser*
[513] Afsnit: *CMMI - Kerneprocesser*
[514] Afsnit: *CMMI for Development*
[515] Afsnit: *CMMI for Development*
[516] Afsnit: *APO12 – Manage Risk*
[517] Afsnit: *CMMI - Kerneprocesser*
[518] Afsnit: *APO05 – Manage Portfolio*

vendige for at dirigere, styre og levere et projekt med succes, fra *Starting up a Projekt* til *Closing a Projekt,* og leverer derved vejledning til den proces, der er optimal for at vedligeholde virksomhedens investeringsmix.[519]

35.6 ITIL

ITIL's *The Seven-step Improvement Process* kan alignes med Cobit 5's APO01, idet begge processer omhandler styring af forbedringer. Formålet med The Seven-Step Improvement Process er at definere og styre de trin, der er nødvendige for at identificere, definere, samle, behandle, analysere, præsentere og implementere forbedringer.[520] APO07's underproces APO01.07 fokuserer på at styre kontinuerlig forbedring af processer, og derfor vurderes det, at der er en overensstemmelse mellem formålene i disse processer.[521]

ITIL's *Strategi Management for IT Services* er den proces, der sikrer, at strategien er defineret, vedligeholdt og opnår dets formål. Denne ITIL proces skal formulere, hvordan en serviceudbyder vil muliggøre for virksomheden at opnå forrentningsmål[522], og kan derved alignes med Cobit 5's APO02, da begge processer har fokus på, at styringen af it skal være i overensstemmelse med forretningens mål.[523]

ITIL's *Service Portefølje Management* skal sikre, at serviceudbyderen udelukkende udbyder de service, der bidrager til strategiske mål og opnår de aftalte forrentningsmål. Formålet med Service Portefølje Management er at sikre, at serviceudbyderen har det rette servicemix til at balancere investeringen i it med opnåelse af forretningsmål.[524] Denne proces kan alignes med Cobit 5's APO05, eftersom begge processer har til formål at optimere investeringsmixet i forhold til, hvad der er passende sammenholdt med forretnings mål.[525]

[519] Afsnit: *Prince2*
[520] Afsnit: *ITIL – ITIL Continual Service Improvement*
[521] Afsnit: *APO01 – Manage the IT Management Framework*
[522] Afsnit: *ITIL – ITIL Service Strategy*
[523] Afsnit: *APO02 – Manage Strategy*
[524] Afsnit: *ITIL – ITIL Service Strategy*
[525] Afsnit: *APO05 – Manage Portfolio*

ITIL's *Financial Management for IT Services* proces har til formål at sikre, at der eksisterer den rette finansiering til design, udvikling og levering af service, som opfylder strategien i virksomheden.[526] Dette formål kan sammenholdes med Cobit 5's APO06 proces, da begge processer fokuserer på den finansielle del af it styring.[527] På trods af at ITIL frameworket har en serviceudbyder vinkel og derfor, forskelligt fra Cobit 5, skal tage stilling til for eksempel, at serviceudbyderen ikke accepterer opgaver, som den ikke har kapacitet til, så kan formålet med ITIL's *Financial Management for IT Services* og Cobit 5's APO06 stadig vurderes til at være relateret.

ITIL's *Demand Management* fokuserer på, at serviceudbyderen har mulighed for at forstå kundebehovet og indfører disse i servicestrategierne for at realisere kundens servicepotentiale, og for at differentiere service mellem kunderne.[528] Dette kan sammenholdes med Cobit 5's APO08, da begge processer indeholder et element af, at ved hjælp af kommunikation, at opnå en forståelse af virksomhedens relationer og derved identificere muligheder, risici og begrænsninger med henblik på at forstærke forretningen.[529]

Ligeledes kan Cobit 5's APO08 sammenholdes med ITIL's *Business Relationship Management*, hvor formålet er at etablere og vedligeholde en forretningsrelation mellem serviceudbyderen og kunden, baseret på en forståelse af kunden og dens forretningsbehov. Processen skal identificere kundebehov og sikre, at serviceudbyderen er i stand til at opfylde disse behov og sikre, at serviceudbyderen forstår ændringer i behov, og assisterer virksomheden i at formulere værdien af en service.[530]

Formålet med Cobit 5's APO09 proces er, at it service og serviceniveauer opfylder nuværende og fremtidige forretningsbehov.[531] De ITIL processer der har et lignede formål er *Demand Management*, der blandt andet fokuserer på en forståelse af kunden og derigennem en opnåelse af forretningsbehov. *Service Portfolio Management* der blandt andet fokuserer på, at serviceudbydere kun skal udbyde den service, der er fordelagtige i forhold til virksomhedens forretningsmål. *Service Catalogue Management*

[526] Afsnit: *ITIL – ITIL Service Strategy*
[527] Afsnit: *APO06 – Manage Budget and Costs*
[528] Afsnit: *ITIL – ITIL Service Strategy*
[529] Afsnit: *APO08 – Manage Relationships*
[530] Afsnit: *ITIL – ITIL Service Strategy*
[531] Afsnit: *APO09 – Manage Service Agreements*

der fokuserer på, at den rette information skal være tilgængelig for den rette autoritet, hvilket gør det muligt at styre serviceaftalerne. *Service Level Management* der har til formål at sikre, at alle nuværende og planlagte it service er leveret til de aftalte opnåelige mål. Dette tilvejebringes gennem en konstant cyklus af forhandling, aftaler, overvågning, rapportering på og gennemgang af it servicemål og resultater, samt gennem tilskyndelse af handlinger til at korrigere eller forbedre niveauet på den leverede service.[532] Samtlige af de nævnte ITIL processer vurderes at være relateret til APO09's overordnede formål.

Formålet med ITIL's *Supplier Management* proces er at skabe "value-for–money" fra leverandører, og at levere it service af høj kvalitet til forretningen ved at sikre, at alle kontrakter og aftaler med leverandører understøtter forretningsbehovene, samt at leverandøren opfylder deres kontraktlige forpligtelser.[533] Dette har en relation til Cobit 5's APO10 proces, da begge processer fokuserer på styring af leverandører, hvor cost/benefit, behov og compliance tages i betragtning.[534]

35.7 The 2011 Standard of Good Practice for Information Security

Formålet med Cobit 5's APO01 proces er at tilvejebringe en konsistent tilgang til management for at understøtte, at virksomhedens governancekrav bliver indfriet, herunder krav til managementprocesser, organisationsstrukturerer, ansvar og kompetencer.[535] Denne Cobit 5 proces kan alignes med AREA *CF20 Business Continuity*, som indeholder CF20.1, der fokuserer på, at der bør etableres en forretningsstrategi, der involverer hele virksomheden. Derved opstår behovet for en kontinuerlig styring af virksomheden, som understøtter virksomhedens overordnede målsætning, hvilket bevirker, at virksomheden bliver modstandsdygtig mod forstyrrelser.[536]

Eftersom APO07's formål er at sikre en struktureret tilgang til en optimal anvendelse af virksomedens personer, inklusiv kommunikation og ansvarsfordeling, en lærings- og udviklingsplan og præstations-

[532] Afsnit: *ITIL – ITIL Service Strategy og ITIL Service Design*
[533] Afsnit: *ITIL – ITIL Service Design*
[534] Afsnit: *APO10 – Manage Suppliers*
[535] Afsnit: *APO01 – Manage the IT Management Framework*
[536] Afsnit: *The 2011 Standard – Control Framework*

forventninger, så virksomheden sikrer motiverede medarbejdere[537], kan dette sammenholdes med AREA CF2 *Human Resource Security*. CF2 omfatter CF2.1, der foreskriver, at medarbejdernes ansættelseskontrakt bør omfatte håndtering af informationssikkerhed, så det derved sikres, at medarbejderne understøtter informationssikkerheden og strategien i virksomheden. Desuden bør der gennemføres aktiviteter så personerne, der har adgang til virksomhedens informationer og systemer, opnår bevidsthed omkring virksomhedens sikkerhed for at garantere en effektiv sikkerhedskultur, hvilket er beskrevet i CF2.2. CF2.3 omhandler kommunikation af sikkerhedsforanstaltninger til personerne i virksomheden. Dette skal foregå på regelmæssig basis, så det sikres, at disse personer kontinuerligt bliver ajourført, og er bevidste omkring væsentligheden af informationssikkerhed. Derudover fremgår det af CF.2.4, at medarbejderne bør oplæres i at anvende virksomhedens systemer korrekt for, at medarbejderne på den måde opnår de nødvendige færdigheder, samt opfylder deres ansvar til informationssikkerheden i virksomheden.[538]

Idet formålet med APO10 er at minimere den risiko, som kan være relateret til ikke-ydedygtige leverandører[539], kan denne proces sammenholdes med The 2011 Standard's AREA CF16 *External Supplier Management*. CF 16 indeholder blandt andet topic CF16.1, der redegør for, at informationssikkerhedskravene bør overvejes kontinuerligt ved anvendelse af eksterne leverandører for derved at beskytte følsomme oplysninger, der overføres, når der anvendes eksterne leverandører. CF16.2 omhandler, at erhvervet hardware og software fra eksterne leverandører skal levere den tiltænkte funktion og ikke kompromitterer sikkerheden af virksomhedens oplysninger. Dette topic kan ligeledes alignes med APO10 ved, at minimering af risiko ved anvendelse af eksterne leverandører håndteres. Endvidere redegør CF16.3 for, at der bør etableres en proces for at styre udvælgelsen og forvaltningen af serviceudbydere herunder dokumenterede aftaleindgåelser, der angiver hvilke sikkerhedsmæssige krav, som skal opfyldes. Denne proces bør etableres for at sikre, at sikkerhedskravene opfyldes og bevares, når driften af en bestemt service er overladt til serviceudbyderen.[540]

Formålet med APO12 er at integrere styringen af it relaterede risici med virksomhedens overordnede

[537] Afsnit: *APO07 – Manage Human Ressources*
[538] Afsnit: *The 2011 Standard – Control Framework*
[539] Afsnit: *APO10 – Manage Suppliers*
[540] Afsnit: *The 2011 Standard – Control Framework*

risikostyring og afstemme fordelene og omkostningerne ved styring af it relaterede forretningsrisici.[541] Denne proces kan sammenholdes med AREA *SR1 Information Risk Assessment*, hvor SR.1.1 omhandler, at informationsrisikovurderinger bør foretages på regelmæssig basis for at identificerede risici holdes indenfor virksomhedens accepterede grænser, som sikrer, at fordelene og omkostningerne ved styring af risici bliver afstemt. Desuden indeholder SR1.6 en beskrivelse af, at informationsrisici bør behandles i overensstemmelse med virksomhedens krav for at sikre håndtering af informationsrisici.[542] APO12 kan endvidere alignes med AREA CF11 *Incident Management*, hvor CF11.1 behandler, at informationssikkerhed bør identificeres og reageres på med en informationssikkerhedsstyringsproces for derved at muliggøre identificering af og løse informationssikkerhedshændelser effektivt, samt at minimere effekten og reducere risikoen for, at lignende hændelser opstår.[543] Desuden kan APO12 relateres til topic SI2.2, der omhandler, at rapporter om informationsrisiko bør produceres og præsenteres for den øverste ledelse, så den øverste ledelse får indblik i informationsrisiciene, der eksisterer i virksomheden.[544]

Formålet APO13 er at definere, styre og overvåge informationssikkerhedsstyring, så virkningerne fra informationssikkerhedsbegivenheder holdes indenfor virksomhedens risikoappetit.[545] Dette kan alignes med kategorien *Security Requirements* (SR), der er inddelt to "areas" og otte "topics", som relaterer til APO13. SR1.1 fokuserer på, at der på regelmæssig basis bør foretages informationsrisikovurderinger for virksomhedens tilsigtede forretningsmiljø for, at identificerede risici kan holdes indenfor virksomhedens accepterede grænser. Desuden foreskriver SR1.2, at disse vurderinger bør foretages ved anvendelse af strukturerede metoder, så det sikrer en ensartethed i hele virksomheden, som muliggør identificering af de væsentligste risici. SR1.5 fokuserer på konsekvenserne ved utilgængelig information i længere perioder. Dette bør vurderes for derigennem at opnå enighed omkring tilgængeligheden af information. Formålet med SR1.6 er at behandle informationsrisici i overensstemmelse med kravene i virksomheden, så det sikres, at informationsrisici minimeres. Endvidere er formålet med SR2.1 at etablere en proces til at identificere informationssikkerhedsmæssige relevante love og standarder, så virk-

[541] Afsnit: *APO12 – Manage Risk*
[542] Afsnit: *The 2011 Standard – Security Requirements*
[543] Afsnit: *The 2011 Standard – Control Framework*
[544] Afsnit: *The 2011 Standard – Security Monitoring and Improvement*
[545] Afsnit: *APO13 – Manage Security*

somheden kan overholde disse.[546]

I *Bilag 5* præsenteres en illustrativ oversigt over den udførte alignment for APO domænet.

36 Alignment - BAI Domænet

36.1 ISO/IEC 20000-serien

ISO/IEC 20000-4 processen *Service Continuity and Availability Management* fokuserer på at sikre, at aftalte serviceniveauer opfyldes under forudsigelige omstændigheder[547], hvilket kan relateres til Cobit 5's BAI04, der fokuserer på vedligeholdelse af servicetilgængeligheden og optimering af systempræstationen gennem forudsigelse af behovet for fremtidig præstation og kapacitetskrav[548]. Derudover kan Cobit 5's BAI04 proces ligeledes relateres til ISO/IEC 20000 processen *Capacity Manangement*, som fokuserer på, at serviceudbyder har tilstrækkelig servicekapacitet til at opfylde nuværende og fremtidige aftalte krav. Øvrige relaterede ISO/IEC 20000-4 processer er *Business Relationship Management, Change Management, Information Item Management, Measurement, Risk Management, Service Planning and Monitoring.* "Best practice" for Service Continuity and Availability Management angives i ISO/IEC 20000-2 afsnit *Service Delivery Processes.*

ISO/IEC 20000-4 processen *Change Management* fokuserer på, at alle ændringer er vurderet, godkendt, implementeret og gennemgået på en kontrolleret måde[549], hvilket kan relateres til Cobit 5's BAI06, der ligeledes fokuserer på at tilvejebringe hurtig og pålidelig levering af forandringer til forretningen.[550] Øvrige relaterede ISO/IEC 20000-4 processer er *Improvement, Information Item Management, Measurement, Release and Deployment Management, Risk Management, Service Planning and Monitoring, SMS Establishment and Maintenance.*

[546] Afsnit: *The 2011 Standard - Security Requirements*
[547] Afsnit: *ISO 20000-4 – Service Continuity and Availability Management*
[548] Afsnit: *BAI04 – Manage Availability and Capacity*
[549] Afsnit: *ISO 20000-4 – Change Management*
[550] Afsnit: *BAI06 – Manage Changes*

ISO/IEC 20000-4 processen *Release and Deployment Management* fokuserer på, at udgivelser skal sættes ind i et live miljø på kontrolleret vis[551], hvilket kan relateres til Cobit 5's BAI07 proces, da denne fokuserer på, at løsninger implementeres sikkert og i overensstemmelse med de aftalte forventninger.[552] Øvrige relaterede ISO/IEC 20000-4 processer er *Change Management, Improvement, Information Item Management, Measurement, SMS Establishment and Maintenance.* "Best practice" for Release and Deployment Management angives i ISO/IEC 20000-2 afsnit angående *Release Processes.*

ISO/IEC 20000-4 processen *Configuration Management* fokuserer på at etablere og vedligeholde integriteten af alle identificerede servicekomponenter[553], hvilket kan relateres til Cobit 5's BAI10 proces, da den fokuserer på at levere tilstrækkelig information om serviceaktiver[554], og derigennem også vedligeholde integriteten. Øvrige relaterede ISO/IEC 20000-4 processer er *Information Item Management, Informations Security Management, Organizational Management, SMS Establishment and Maintenance.* "Best practice" for Configuration Management angives i ISO/IEC 20000-2 afsnittet *Control Processes.*

36.2 ISO/IEC 38500

BAI02's formålet er at udvikle og implementere optimale løsninger og analysere virksomhedens behov før anskaffelse, så anskaffelsen er i overensstemmelse med virksomhedens behov.[555] Dette kan alignes med ISO/IEC 38500's princip *Acquisition,* der omhandler, at forud for nye it anskaffelser, skal der foretages analyse med en forståelig og evident beslutningsproces. Virksomheden skal opnå den optimale løsning, hvad angår fordele, muligheder, risici og ulemper ved anskaffelsen af nye it investeringer.[556]

Fokus i processen BAI05 er opnå det optimale ved ændringer i virksomheden, så ændringer implementeres effektivt, og der etableres et ønske om forandring så mulige risici reduceres.[557] Dette kan sam-

[551] Afsnit: *ISO 20000-4 – Release and Deployment Management*
[552] Afsnit: *BAI07 – Manage Change Acceptance and Transitioning*
[553] Afsnit: *ISO/IEC 20000-4 – Configuration Management*
[554] Afsnit: *BAI10 – Manage Configuration*
[555] Afsnit: *BAI02 – Manage Requirements Definition*
[556] Afsnit: *ISO/IEC 38500*
[557] Afsnit: *BAI05 – Manage Organisational Change Enablement*

menholdes med ISO/IEC38500's princip *Human Behaviour*, der foreskriver, at virksomheden skal have respekt for og være opmærksom på de personer, der er involveret i processen.[558]

36.3 CMMI

BAI01 har til formål at styre programmer og projekter for at opnå forretningsfordele og reducere risikoen for uventede forsinkelser, omkostninger og værdinedbrydning. Dette sikrer værdien og kvaliteten af projektresultaterne.[559] Dette kan alignes med CMMI-DEV's proces *Product Integration* (PI), hvis formål er at sikre, at det integrerede produkt virker som planlagt, samt besidder den rette funktionalitet og kvalitet, så optimale resultater derved opnås.[560] Desuden kan BAI01 sammenholdes med CMMI-ACQ processen *Acquisition Verification* (AVER). Formålet med denne proces er at sikre, at de anskaffede produkter opfylder de tiltænkte krav, så mulige fordele og reducering af potentielle risici opnås.[561] Processen *Requirements Management* (REQM) styrer kravene til projektets produkter samt sikrer overensstemmelse mellem disse krav og projektets planer, hvilket ligeledes kan sidestilles med BAI01.[562]

Ved at BAI02 definerer virksomhedens krav, kan virksomheden derved udvikle optimale løsninger, der imødeser virksomhedens behov.[563] Dette er i overensstemmelse med *Requirements Management* (REQM), hvis formål er at styre virksomhedens krav til produkter, service og projektplaner så disse sammenholdes med virksomhedens behov.[564]

Formålet med BAI03 er at etablere omkostningseffektive løsninger, som formår at understøtte virksomhedens strategi, behov og mål.[565] Denne proces kan sammenholdes med *Organizational Performance Management* (OPM), hvis formål er at styre virksomhedens præstationer ved at identificere potentielle risici, der kan påvirke virksomhedens mål, og derved udvælge og implementere løsningsfor-

[558] Afsnit: *ISO/IEC 38500*
[559] Afsnit: *BAI01 – Manage Programs and Projects*
[560] Afsnit: *CMMI for Development*
[561] Afsnit: *CMMI for Acquisition*
[562] Afsnit: *CMMI - Kerneprocesser*
[563] Afsnit: *BAI02 – Manage Requirements Definition*
[564] Afsnit: *CMMI - Kerneprocesser*
[565] Afsnit: *BAI03 – Manage Solutions Identification and Build*

bedringer, der håndterer de mulige risici. Disse løsningsforbedringer omfatter eksempelvis produktkvalitet, produktivitet, effektivitet og tilfredshed blandt kunderne.[566]

Som beskrevet er formålet med *Organizational Training* (OT) at udvikle personerne i virksomhedens kompetencer og viden, så disse personer kan udføre deres roller effektivt og i overensstemmelse med virksomhedens mål.[567] Denne proces kan alignes med BAI08, som fokuserer på at levere den nødvendige viden til virksomhedens medarbejdere, så de kan udføre opgaver effektivt samt foretage optimale beslutninger, som forstærker produktiviteten i virksomheden.[568]

Formålet med BAI10 er at definere og vedligeholde relationer mellem nødvendige ressourcer og kvalifikationer, der muliggør it baserede service herunder konfigurationsinformation og konfigurationskontrol.[569] BAI10 kan derved sidestilles med *Configuration Management* (CM), som fokuserer på at etablere og vedligeholde integriteten af produkter ved anvendelse af eksempelvis konfigurationsidentifikation og konfigurationskontrol.[570]

36.4 Prince 2

Prince2's syv processer omhandler aktiviteter, der er nødvendige for at dirigere, styre og levere et projekt med succes, fra *Starting up a Projekt* til *Closing a Projekt* og leverer derved vejledning til den proces, der er optimal for at vedligeholde virksomhedens investeringsmix.[571]Dette kan relateres til Cobit 5's BAI01 samt underprocesserne, der fokuserer på styring af programmer og projekter for at opnå forretningsfordele og reducere risikoen for uventede forsinkelser, omkostninger og værdierosion. Dette sikrer værdien og kvaliteten af projektresultaterne og maksimere deres bidrag til investerings- og serviceporteføljen.[572]

[566] Afsnit: *CMMI - Kerneprocesser*
[567] Afsnit: *CMMI – Kerneprocesser*
[568] Afsnit: *BAI08 – Manage Knowledge*
[569] Afsnit: *BAI10 – Manage Configuration*
[570] Afsnit: *CMMI – Kerneprocesser*
[571] Afsnit: *Prince2*
[572] Afsnit: *BAI01 – Manage Programs and Projects*

Prince2's princip *Focus on Products* fokuserer på, at et succesfuldt projekt er outputorienteret fremfor aktivitetsorienteret. Formålet med et projekt er at opfylde interessenternes behov i overensstemmelse med forretningen. For at tilvejebringe dette skal der være en fælles forståelse af, hvad der forventes af det produkt, projektet resulterer i. Et Prince2 projekt benytter produktbeskrivelser til at skabe en fælles forståelse ved at definere hvert produkts formål, sammensætning, oprindelse, format, kvalitetskriterier og kvalitetsmetode.[573] Dette kan relateres til Cobit 5's BAI07 proces, der fokuserer på at implementere løsninger i overensstemmelse med de aftalte forventninger.[574]

36.5 ITIL

ITIL's *Availability Management* proces omhandler at opfylde såvel det nuværende som det fremtidige tilgængelighedsbehov for forretningen[575], hvilket kan sammenholdes med formålet med Cobit 5's BAI04, der blandt andet har til formål at vedligeholde servicetilgængeligheden.[576] ITIL's *Capacity Management* skal sikre, at kapaciteten for it service og it infrastrukturen opfylder de aftalte kapacitets- og præstationsrelaterede krav omkostningseffektivt og rettidigt.[577] Denne proces kan også relateres til Cobit 5's BAI04, der fokuserer på tilgængelighed og kapacitetsstyring. [578]

ITIL's *Change Management* proces fokuserer på at kontrollere livscyklussen for alle ændringer med det formål at gøre det muligt at foretage ændringer med minimum forstyrrelse af it service.[579] Denne proces kan relateres til Cobit 5's BAI06 proces, da begge processer fokuserer på at opretholde stabiliteten af det miljø en ændring bliver implementeret i.[580]

Cobit 5's BAI07 proces har til formål at implementere løsninger sikkert og i overensstemmelse med de aftalte forventeringer og resultater. [581] BAI07 kan relateres til nedenstående ITIL processer. *Tranisition Planning and Support* processen kan relateres til BAI07, da de begge fokuserer på at styre overgange-

[573] Afsnit: *Prince2 – Focus on products*
[574] Afsnit: *BAI07 – Manage Change Acceptance and Transitioning*
[575] Afsnit: *ITIL – ITIL Service Design*
[576] Afsnit: *BAI04 – Manage Availability and Capacity*
[577] Afsnit: *ITIL – ITIL Service Design*
[578] Afsnit: *BAI04 – Manage Availability and Capacity*
[579] Afsnit: *ITIL – ITIL Service Transition*
[580] Afsnit: *BAI06 – Manage Changes*
[581] Afsnit: *BAI07 – Manage Change Acceptance and Transitioning*

ne, herunder at levere den servicesupport, der er nødvendig for at gennemføre overgangene. ITIL's *Release and Deployment Management* proces kan relateres til BAI07, da den har til formål at planlægge, skematisere og kontrollere bygningen, test og indsættelsen af udgivelser, og at levere ny funktionalitet, der er nødvendigt for forretningen, mens at integriteten af eksisterende service beskyttes. ITIL's *Service Validation Management* proces relateres til BAI07, da begge processer fokuserer på at nye og ændrede it service skal være i overensstemmelse med de aftalte forventninger, herunder designspecifikationer og vil opfylde forretningsbehovene. ITIL's *Change Evaluation* proces kan relateres til BAI07 processen, da den fokuserer på at levere en metode til at fastsætte præstationen af serviceændringer i forhold til risiko, eksisterende og foreslåede service og it infrastruktur. Ligeledes bliver risici og problemer relateret til ændringen, i overensstemmelse med BAI07, identificeret og håndteret.[582]

ITIL's *Knowledge Management* proces fokuserer på at dele perspektiver, ideer, erfaring og information[583], hvilket kan relateres til BAI08 processen, da begge processer fokuserer på at opsamle, bruge og dele viden til fordel for virksomheden, samt for at foretage informerede beslutninger.[584]

ITIL's *Service Assets and Configuration Management* proces fokuserer på at sikre, at aktiverne der er nødvendige for at levere service er hensigtsmæssigt kontrolleret, og at nøjagtig og pålidelig information angående disse aktiver er tilgængelig, hvor og når der er behov for den. Denne information inkluderer detaljer om, hvordan aktiverne er konfigurerede og relationerne mellem aktiverne[585], hvilket kan relateres til BAI10 processen, der ligeledes fokuserer på at levere tilstrækkelig information angående serviceaktivitet så denne service kan styres effektivt.[586]

36.6 The 2011 Standard of Good Practice for Information Security

Fokus i BAI06 er at muliggøre hurtig og pålidelig levering af forandringer til virksomheden samt minimere risikoen for negativ påvirkning af stabiliteten eller integriteten af det forandrede miljø.[587] Denne

[582] Afsnit: *ITIL – ITIL Service Transition*
[583] Afsnit: *ITIL – ITIL Service Transition*
[584] Afsnit: *BAI08 – Manage Knowledge*
[585] Afsnit: *ITIL – ITIL Service Transition*
[586] Afsnit: *BAI10 – Manage Configuration*
[587] Afsnit: *BAI05 – Manage Organisational Change Enablement*

proces kan sammenlignes med CF7.6, der omhandler systemændringer. Disse systemændringer bør testes og gennemgås ved at anvende en ændringsstyringsproces for at sikre, at ændringerne anvendes korrekt og ikke kompromitterer sikkerheden af virksomhedens systemer.[588]

I *Bilag 6* præsenteres en illustrativ oversigt over den udførte alignment for BAI domænet.

37 Alignment - DSS Domænet

37.1 ISO/IEC 27001 & ISO/IEC 27002

ISO/IEC 27002 området *Information Security Incident Management* fokuserer på at alle medarbejdere, leverandører og tredjeparter, der benytter virksomhedens informationssystem skal opfordres til at notere og rapportere alle observerede mistænkeligheder i virksomhedens informationssystem og service. Derved kan der foretages passende korrigerende og forebyggende handlinger[589], hvilket kan relateres til Cobit 5's DSS02 proces med det formål at opnå forbedret produktivitet og minimere forstyrrelser af driften gennem hurtig løsning af hændelser og forespørgsler.[590]

ISO/IEC 27002 området *Business Continuity Management* fokuserer på, at der udvikles planer således, at konsekvensen af tabte informationer minimeres for forretningen[591], hvilket kan relateres til Cobit 5's DSS04, som fokuserer på, at i tilfælde af signifikante forstyrrelser, skal forsættelsen af kritiske forretningsoperationer sikres.[592]

ISO/IEC 27001 og ISO/IEC 27002 indeholder detaljerede regler for, hvordan en virksomhed bør håndtere informationssikkerhed på de tidligere nævnte 11 forskellige områder, hvilket kan relateres til underprocesserne i Cobit 5's DSS05 proces.[593]

[588] Afsnit: *The 2011 Standard – Control Framework*
[589] Afsnit: *ISO 27002 – Information Security Incident Management*
[590] Afsnit: *DSS02 – Manage Service Requests and Incidents*
[591] Afsnit: *ISO 27002 – Business Continuity Management*
[592] Afsnit: *DSS04 – Manage Continuity*
[593] Afsnit: *ISO 27001 + DSS05 – Manage Security Services*

37.2 ISO/IEC 20000-serien

ISO/IEC 20000-4 processen *Service Level Management* kan relateres til Cobit 5's DSS02, da begge processer fokuserer på, at det serviceniveau, der er aftalt mellem serviceudbyder og virksomheden, altid opnås.[594] Denne opnåelse af det aftalte serviceniveau gælder både under normal drift, når der opstår hændelser, som påvirker virksomheden eller ved implementering af løsninger, som er baseret på forespørgsler. Øvrige relaterede ISO/IEC 20000-4 processer er *Business Relationship Management, Change Management, Configuration Management, Improvement, Information Item Management, Measurement, Service Level Management, Service Reporting.* "Best practice" for Service Level Management angives i ISO/IEC 20000-2 i afsnittet *Service Delivery Processes.*

ISO/IEC 20000-4 processen *Incident Management and Request Fulfillment* fokuserer på at genoprette service og opfylde serviceforespørgsler indenfor aftalte serviceniveauer[595], hvilket kan relateres til Cobit 5's DSS02 proces, der fokuserer på at minimere forstyrrelser ved løsning af hændelser eller forespørgsler.[596] Øvrige relaterede ISO/IEC 20000-4 processer er *Incident Management and Request Fulfilment, Information Item Management, Informations Security Management, SMS Establishment and Maintenance.* "Best practice" for *Incident Management and Request Fulfillment* angives i ISO/IEC 20000-2 i afsnittet angående *Resolution Processes.*

ISO/IEC 20000-4 processen *Problem Management* har til formål at minimere forstyrrelsen ved levering af service til kunden.[597] Dette kan relateres til Cobit 5's DSS03, der fokuserer på generelt at reducere antallet af driftsproblemer.[598] Øvrige relaterede ISO/IEC 20000-4 processer er *Business Relationship Management, Change Management, Improvement, Information Item Management, Measurement, Service Planning and Monitoring, SMS Establishment and Maintenance.* "Best practice" for Problem Management angives i ISO/IEC 20000-2 i afsnittet angående *Resolution Processes.*

[594] Afsnit: *DSS02 – Manage Service Requests and Incidents + ISO 20000-4 – Service Level Management*
[595] Afsnit: *ISO 20000-4 – Incident Management and Request Fulfillment*
[596] Afsnit: *DSS02 – Manage Service Requests and Incidents*
[597] Afsnit: *ISO 20000-4 – Problem Management*
[598] Afsnit: *DSS03 – Manage Problems*

ISO/IEC 20000-4 processen *Service Continuity and Availability Management* fokuserer på, at aftalte serviceniveauer opnås under forudsigelige omstændigheder[599], hvilket kan relateres til Cobit 5's DSS04 proces, der fokuserer på at sikre forsættelse af kritiske forretningsoperationer og vedligeholdelse af tilgængeligheden af information på et niveau, der er acceptabelt for virksomheden.[600] Kritiske forretningsoperationer kan være understøttet af en serviceudbyder, og det kan derfor vurderes, at der er relation mellem ISO/IEC 20000 *Service Continuity and Availability Management* processen og Cobit 5's DSS04 proces. Øvrige relaterede ISO/IEC 20000-4 processer er *Business Relationship Management, Change Management, Information Item Management, Measurement, Risk Management, Service Planning and Monitoring*. "Best practice" for Service Continuity and Availability Management angives i ISO/IEC 20000-2 afsnit *Service Delivery Processes*.

37.3 ITIL

ITIL's *Event Management* proces vurderes som grundlaget for operationel overvågning og kontrol. Hvis hændelser er programmeret til at kommunikere såvel operationel information som advarsler og undtagelser, kan de benyttes som en basis for automatisering af flere rutineoperationsstyringsaktiviteter.[601] Dette kan relateres til Cobit 5's DSS01 proces, der fokuserer på at levere it operationelle serviceresultater som planlagt, blandt andet ved at udføre driftsprocedurer, styre outsourcede it service og overvåge it infrastrukturen.[602]

Formålet med ITIL 's *Incident Management* proces er at genvinde normal service så hurtigt som muligt og minimere den ufordelagtige konsekvens en hændelse kan forårsage for forretningsdriften, og derigennem sikre, at det aftalte servicekvalitetsniveau opretholdes.[603] Dette kan relateres til Cobit 5's DSS02 proces, da begge processer fokuserer på at minimere forstyrrelser gennem hurtig løsning af hændelser.[604]

[599] Afsnit: *ISO 20000-4 – Service Continuity and Availability*
[600] Afsnit: *DSS04 – Manage Continuity*
[601] Afsnit: *ITIL – ITIL Service Operation*
[602] Afsnit: *DSS01 – Manage Operations*
[603] Afsnit: *ITIL - ITIL Service Operation*
[604] Afsnit: *DSS02 – Manage Service Requests and Incidents*

ITIL's *Request Fulfilment* proces er ansvarlig for styring af livscyklussen for alle serviceforespørgsler fra brugere[605], hvilket kan relateres til Cobit 5's DSS02 proces, da begge processer fokuserer på øget produktivitet og minimeret forstyrrelse af driften gennem hurtig løsning af forespørgsler.[606]

ITIL's *Problem Management* proces har til formål at minimere den ufordelagtige konsekvens af hændelser og problemer i forretningen, der er forårsaget af fejl i it, og fokuserer på proaktivt at forhindre gentagelse af hændelser relateret til disse fejl.[607] Dette kan relateres til Cobit 5's DSS03 proces, da begge processer fokuserer på proaktivt at reducere driftsproblemer eksempelvis ved hjælp af dokumentation og kommunikation af kendte fejl.[608]

ITIL's *IT Service Continuity Management* proces skal sikre, at it serviceudbyderen altid leverer minimum aftalte forretningskontinuitetsrelaterede serviceniveauer. Dette gøres ved at reducere risici angående it service til et aftalt acceptabelt niveau samt planlægge og forbedre en genvinding af it service.[609] Dette kan relateres til Cobit 5's DSS04 proces, da denne ligeledes sikre forsættelse af kritiske forretningsoperationer ved hjælp af en kontinuitetsplan.[610]

ITIL's *Information Security Management* proces og Cobit 5's DSS05 kan vurderes til at have det samme formål. Relationen mellem disse processer er dog præget af, at ITIL processen udelukkende har en serviceudbyder vinkel. Dette kommer til udtryk ved, at ITIL fokuserer på, at forretningens behov for informationssikkerhed er opfyldt[611], hvor DSS05 fokuserer direkte på de elementer, der skal håndteres for at minimere forretningskonsekvensen af sårbarheder og hændelser på informationssikkerheden.[612] Det vurderes dog, at disse processer opnå det samme formål.

[605] Afsnit: *ITIL – ITIL Service Operation*
[606] Afsnit: *DSS02 – Manage Service Requests and Incidents*
[607] Afsnit: *ITIL – ITIL Service Operation*
[608] Afsnit: *DSS03 – Manage Problems*
[609] Afsnit: *ITIL – ITIL Service Design*
[610] Afsnit: *DSS04 – Manage Continuity*
[611] Afsnit: *ITIL – ITIL Service Design*
[612] Afsnit: *DSS05 – Manage Security Services*

37.4 The 2011 Standard of Good Practice for Information Security

Formålet med Cobit 5's DSS02 er at opnå en forbedret produktivitet samt minimere forstyrrelser ved hurtig løsning af brugerforespørgsler og hændelser[613], hvilket kan sammenholdes med AREA CF11 *Incident Management* i The 2011 Standard. CF11.1 fokuserer på, at informationssikkerhed bør identificeres samt reageres på med en informationssikkerheds hændelsesstyringsproces for derved at identificere og løse informationssikkerhedshændelser effektivt samtidig med minimering af effekten og reducering af risikoen for, at lignende hændelser opstår. Foruden CF11.1 fokuserer CF11.3 på, at der bør afprøves og gennemgås rettelser til virksomhedens edb-udstyr, virksomhedsapplikationer og systemsoftware for at undersøge om dette fungerer hurtigt og effektivt ved nødssituationer. Virksomheden kan derved opnå en reaktion på nødsituationer, samt reducerer forstyrrelser i virksomheden.[614]

Cobit 5's DSS04 har til formål, i tilfælde af forstyrrelser i driften at sikre forsættelse af forretningsaktiviteter og opretholdelse af tilgængeligheden af information på et niveau, som er acceptabelt for virksomheden.[615] Denne proces kan alignes med AREA CF20 *Business Continuity*. Topic CF20.1 behandler, at der bør etableres en forretningsstrategi, der involverer hele virksomheden, hvilket fremmer behovet for kontinuitet i virksomhedens styring, og gør virksomheden modstandsdygtig mod forstyrrelser. Endvidere beskriver CF20.2, at der bør fastsættes et kontinuitetsprogram, som omfatter udvikling af teknisk infrastruktur, krisestyring og koordinerer og vedligeholder virksomhedens kontinuitetsplaner for, at virksomheden derved kan modstå manglende adgang til information, virksomhedsapplikationer og anden teknisk infrastruktur. CF20.3 fokuserer på, at virksomhedsapplikationer skal køre på pålidelig hardware og software samt understøttes af dobbelte faciliteter for derved at sikre kritiske forretningsprocesser, der er afhængige af virksomhedsapplikationer, er til rådighed, når der foreligger et behov for det. Fokus i CF20.5 er at udvikle og dokumentere kontinuitetsplaner, så disse planer understøtter virksomheden forretningsprocesser. På den måde kan personer udføre tiltag i tilfælde af nødssituationer, så forretningsprocesserne kan genoptages. Desuden bør der fastsættes virksomhedskontinuitetsarrangementer for enkelte forretningsområder samt være til rådighed efter behov. Således bliver kritiske forretningsprocesser genoptaget indenfor aftalt tid efter en afbrydelse, hvilket behandles i CF20.6. Afslutningsvis omhandler CF20.7 afprøvning af kontinuitetsplaner og arrangementer på en regelmæssig ba-

[613] Afsnit: *DSS02 – Manage Service Requests and Incidents*
[614] Afsnit: *The 2011 Standard – Control Framework*
[615] Afsnit: *DSS04 – Manage Continuity*

sis, så det giver sikkerhed for, at planerne og arrangementerne vil fungere, så forretningsprocesserne kan genoptages indenfor den planlagte tid.[616]

Formålet med Cobit 5's DSS05 er at minimere forretningsmæssige konsekvenser af informationssikkerhedsproblemer og hændelser. [617] Denne Cobit proces kan alignes med AREA CF10 *Threat and Vulnerability Management*. CF10 indeholder CF10.1, der omhandler, at en proces bør etableres for indsættelse af system- og softwarepatches for at løse tekniske system- og softwaresårbarheder hurtigt og effektivt. Dette er for at minimere sandsynligheden for, at disse sårbarheder udnyttes og derved får indvirkning på virksomheden. Derudover fokuserer CF10.2 på, at personer i virksomheden, som har adgang til virksomhedens information og systemer bør gøres opmærksomme på risici for malware samt foranstaltninger for at minimere risiciene for disse. Derved sikres det, at personerne forstår centrale elemeter i beskyttelsen mod malware, samt hvorfor beskyttelsen mod malware er nødvendigt. CF10.4 kan ligeledes sammenholdes til DSS05 ved, at hændelser som kan relateres til sikkerhed skal registreres i logs og analyseres regelmæssig for at sikre trusselidentifikation, som kan have indvirkning på informationssikkerheden samt bevare integriteten af virksomhedens oplysninger.[618]

Ved at DSS05 fokuserer på at minimere konsekvenser af informationssikkerhedsproblemer og hændelser kan det ligeledes relateres til The 2011 Standard's AREA CF11 *Incident Management*. CF11.1 beskriver, at informationssikkerhed bør identificeres, reageres på og følges op på med en informationssikkerheds hændelsesstyringsproces for på den måde at identificere og løse informationssikkerhedshændelser effektivt og minimere effekten samt reducere risikoen for lignende hændelser. Desuden omhandler CF11.3, at der bør afprøves og gennemgås rettelser til edb-udstyr, virksomhedsapplikationer og systemsoftware ved nødssituationer for at undersøge om dette fungerer hurtigt og effektivt. Derved kan en reaktion på nødsituationer ske på en rettidig og sikker måde, samt reducerer forstyrrelser i virksomheden.[619]

I *Bilag 7* præsenteres en illustrativ oversigt over den udførte alignment for DSS domænet.

[616] Afsnit: *The 2011 Standard – Control Framework*
[617] Afsnit: *DSS05 – Manage Security Services*
[618] Afsnit: *The 2011 Standard – Control Framework*
[619] Afsnit: *The 2011 Standard – Control Framework*

38 Alignment - MEA Domænet

38.1 ISO/IEC 20000-serien

ISO/IEC 20000-4 *Service Reporting* processen fokuserer på at producere rettidige og akkurate servicerapporter til at understøtte effektiv kommunikation og beslutningstagning i forbindelse med kundens it.[620] Denne rapportering understøtter formålet med Cobit 5's MEA01 proces, som fokuserer på at tilvejebringe gennemsigtighed af præstation og overensstemmelse, og derved fremme opnåelse af mål.[621] Derfor kan det vurderes, at ISO/IEC 20000-4 *Service Reporting* processen og Cobit 5's MEA01 proces fokuserer på det samme formål. Øvrige relaterede ISO/IEC 20000-4 processer er *Service Planning and Monitoring*. "Best practice" for Service Reporting angives i ISO/IEC 20000-2 afsnittet om *Service Delivery Processes*.

38.2 ISO/IEC 38500

For processen MEA01 er formålet at sikre tilvejebringelse af virksomhedens præstationer. Derudover sikrer MEA01 overvågning af om processerne præsterer som forventet, er i overensstemmelse med virksomhedens mål og metoder samt sikre, at virksomhedens rapportering er systematisk og præcis.[622] Denne proces kan derfor sammenholdes med ISO/IEC 38500's princip *performance*, da princippet foreskriver, at det er nødvendigt med en effektiv præstationsmåling for en optimal model til at kontrollere, om de opsatte mål er opnået.[623]

Formålet med MEA02 er at opnå effektive interne kontroller og derigennem opnå tillid til virksomheden, dens mål og håndtering af mulige risici.[624] Dette kan alignes med ISO/IEC 38500's princip *conformance*, der igennem overensstemmelse med lovgivningsmæssige krav og definerede, implementerede og underbyggede målsætninger samt fremgangsmåder, muliggør opnåelse af tillid til virksomheden.[625]

[620] Afsnit: *ISO 20000-4 – Service Reporting*
[621] Afsnit: *MEA01 – Monitor, Evaluate and Assess Performance and Conformance*
[622] Afsnit: *MEA01 – Monitor, Evaluate and Assess Performance and Conformance*
[623] Afsnit: *ISO/IEC 38500*
[624] Afsnit: *MEA02 – Monitor, Evaluate and Assess the System of Internal Control*
[625] Afsnit: *ISO/IEC 38500*

MEA03 sikrer, at virksomheden overvåger, evaluerer og vurderer overensstemmelse med lovgivningsmæssige krav samt andre relevante eksterne krav.[626] Princippet i ISO/IEC 38500 *comformance* kan sammenholdes med denne proces, da fokus ligeledes er overensstemmelse med lovgivningsmæssige krav og regler.[627]

38.3 ITIL

ITIL's *Service Level Management* proces skal sikre, at alle nuværende og planlagte it service er leveret til aftalte opnåelige mål. Dette tilvejebringes gennem en konstant cyklus af forhandling, aftaler, overvågning, rapportering på og gennemgang af it servicemål og resultater, samt tilskyndelse af handlinger til at korrigere eller forbedre serviceniveauet.[628] Dette kan relateres til Cobit 5's MEA01, hvor der gennem overvågning opnås gennemsigtighed angående præstation og overensstemmelse angående it, der gennem rapportering og implementering af korrigerende handlinger kan fremme opnåelse af forretningens mål.[629] Det overordnende formål for begge disse processer kan vurderes til, at det skal sikres, at it service er i overensstemmelse med forretningens mål.

I *Bilag 8* præsenteres en illustrativ oversigt over den udførte alignment for MEA domænet.

[626] Afsnit: *MEA03 – Monitor, Evaluate and Assess Compliance with External Requirements*
[627] Afsnit: *ISO/IEC 38500*
[628] Afsnit: *ITIL – ITIL Service Design*
[629] Afsnit: *MEA02 – Monitor, Evaluate and Assess the System of Internal Control*

Konklusion

Virksomheder er i dag nødsaget til at erkende de udfordringer, som eksisterer ved anvendelse af informationsteknologi (it), da it er et af fundamenterne for virksomheder for at opnå konkurrencemæssige fordele samt udnyttelse af de ressourcer, der er til rådighed i virksomheden. Styringen af it skal være en integreret del af virksomhedens overordnede strategi, og ledelsen skal derfor have indarbejdet denne it styring, så virksomhedens målsætning kan opfyldes. I tilfælde af at ledelsen ikke besidder den nødvendige indsigt i de risici og fordele, som it området kan medføre, kan ledelsen efterspørge rådgivning hos en revisor, som kan assistere ledelsen i it relaterede overvejelser. Det kan få betydning for virksomheden, om ledelsen formår at opnå det optimale af virksomhedens it ressourcer, så fordele kan realiseres og potentielle risici håndteres.

Formålet med denne kandidatafhandling har således været at undersøge: *Hvordan kan revisor rådgive ledelsen til at få det optimale ud af virksomhedens it ressourcer?*

Når der opereres indenfor it området bør revisor og ledelsen være opmærksomme på publicerede frameworks og standarder, som kan fungere som inspiration og vejledning til styring af it, så virksomheden således får det optimale ud af de it relaterede ressourcer. Af disse frameworks og standarder er der i afhandlingen blevet præsenteret Cobit 5, ERM, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 20000-serien, ISO/IEC 38500, CMMI, Prince2, ITIL og The 2011 Standard. Disse frameworks og standarder indeholder forskellige fokusområder, og det kan være nødvendigt for virksomheden at sammensætte en model, som er tilpasset virksomhedens behov. Hertil er det nødvendigt at få alignet de forskellige frameworks og standarder.

Cobit 5 inddeler 37 processer på fem domæner, og dette muliggør en alignment med de resterende standarder og frameworks principper, processer eller lignende. På baggrund af en gennemgang af de udvalgte frameworks og standarder vurderes der at foreligge en åbenbar sammenhæng på visse områder.

Cobit 5's *Evaluate, Direct & Monitor* domæne kan sammenholdes med ERM frameworket, ISO/IEC 38500 og The 2011 Standard. Derved kan virksomheder, der ønsker at anvende governance relaterede processer igennem andre frameworks og standarder benytte eller finde vejledning i både ERM, ISO/IEC 38500 og The 2011 Standard.

På baggrund af domænet *Align, Plan & Organize* vurderes en sammenhæng at eksistere mellem visse af Cobit 5's processer indenfor dette domæne og ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 20000-serien, ISO/IEC 38500, CMMI, Prince2, ITIL og The 2011 Standard. På informationssikkerhed området og andre risikorelaterede processer indenfor APO domænet, kan virksomheder finde inspiration i ISO/IEC 27001, ISO/IEC 27002 og The 2011 Standard, ligesom Prince2 kan anvendes ved de porteføljerelaterede processer. Desuden understøtter CMMI nogle af de organisations- og kvalitetsrelaterede processer fra APO domænet.

Cobit 5's *Build, Acquire & Implement* kan alignes med ISO/IEC 20000-serien, ISO/IEC 38500, CMMI, Prince2, ITIL og The 2011 Standard. Prince2 understøtter Cobit 5's BAI domæne på de program- og projektrelaterede processer, hvor CMMI kan sammenholdes med de anskaffelsesrelaterede processer i domænet.

Der vurderes at være en relation mellem ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 20000-serien, ITIL, The 2011 Standard og Cobit 5's *Deliver, Service & Support* domæne. For ISO/IEC 27001, ISO/IEC 27002 og The 2011 Standard forekommer denne overensstemmelse indenfor de informationssikkerheds- og risikorelaterede processer indenfor DSS domænet.

Afslutningsvis kan det konkluderes, at der på *Monitor, Evaluate & Assess* domænet i Cobit 5 figurerer processer, som kan sammenholdes med henholdsvis ISO/IEC 20000-serien, ISO/IEC 38500 og ITIL, så virksomhederne derved kan opnå vejledning og inspiration fra disse frameworks og standarder, hvis de anvender de relaterede processer fra Cobit 5's DSS domæne.

Det konkluderes, at der foreligger overensstemmelse mellem de udvalgte frameworks og standarder ud fra afhandlingens alignment, og derved vurderes virksomheden at have mulighed for at tilpasse disse

frameworks og standarder til en egen tilpasset it ledelsesmodel til styring af virksomhedens it, så virksomhedens behov opfyldes. Det vurderes ud fra de interview, som er foretaget, at revisorer skal have indgående kendskab til den virksomhed de rådgiver, imens revisor skal have indsigt i de forskellige frameworks og standarder for derved at yde den mest optimale rådgivning for netop dén virksomhed. Eftersom der ikke findes to virksomheder, som er ens, eksisterer der således ikke ét framework eller én standard, som er optimal for alle virksomheder. Det er nødvendigt, at virksomheden udvælger processer fra de forskellige frameworks og standarder, og på den måde sammensætter virksomhedens egen model, så virksomheden får det optimale ud af deres it ressourcer.

Litteraturliste

Publikationer

Information System Audit Control Association (2012): *Cobit 5 – A Business Framework for the Governance and Management og Enterprise IT*, ISBN: 978-1-60420-237-3

Information System Audit Control Association (2012): *Cobit 5 – Enabling Processes,* ISBN: 978-1-60420-241-0

Information Security Forum (2011): *The 2011 Standard of Good Practice for Information Security*

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

IT Governance Institute and Office of Government Commerce (2008): *Aligning CobiT 4.1, ITILv3 and ISO/IEC 27002 for Business Benefit*

IT Governance Institute (2007): *IT Governance Using CobiT and Val IT* (Student Book, 2nd Edition), ISBN 978-1-60420-024-9

Karnov Group A/S (2011): *Revisorhåndbogen 2011 – REVISION II* (1. udgave 1. oplag), ISBN: 978-87-619-3087-3

Robert R. Moeller (2008): *Sarbanes-Oxley Internal Controls –Effective Auditing with AS5, CobiT and ITIL*, ISBN: 978-0-470-17092-2

Software Engineering Institute (2011): *CMMI for Acquisition – Guidelines for Improving the Acquisition of Products and Services* (version 1.3), ISBN: 978-0-321-71151-9

Software Engineering Institute (2011): *CMMI for Development – Guidelines for Proces Intergration and Product Improvement* (version s1.3), ISBN: 978- 0-321-71150-2

Software Engineering Institute (2011): *CMMI for Services – Guidelines for Superior Service* (version 1.3), ISBN: 978-0-321-71152-6

The Committee of Sponsoring Organizations of the Treadway Commission (2004): *Enterprise Risk Management —Integrated Framework: Executive Summary and Framework.*

The Office of Government Commerce (2011): *ITIL Continual Service Improvement*, ISBN: 978-0-11-331308-2

The Office of Government Commerce (2011): *ITIL Service Design*, ISBN: 978-0-11-331305-1

The Office of Government Commerce (2011): *ITIL Service Operation*, ISBN: 978-0-11-331307-5

The Office of Government Commerce (2011): *ITIL Service Strategy*, ISBN: 978-0-11-331304-4

The Office of Government Commerce (2011): *ITIL Service Transition*, ISBN: 978-0-11-331306-8

The Office of Government Commerce (2009): *Managing Successful Projects with PRINCE2*, ISBN: 978- 0-11-331059-3

Internet

Public Company Accounting Oversight Board: *Auditing Standard No. 5*. Lokaliseret d. 20 april 2012 på internettet: http://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_5.aspx#introduction

Love

LBK nr. 322 af 11/04/2011: *Bekendtgørelse af lov om aktie- og anpartsselskaber (selskabsloven)*

Standarder

The International Organization for Standardization and The International Electrotechnical Commission (2011): *ISO/IEC 20000-1 Information techology – Service management – Part 1: Service management system requirements*

The International Organization for Standardization and The International Electrotechnical Commission (2011): *ISO/IEC 20000-2 Information techology – Service management – Part 2: Code of practice*

The International Organization for Standardization and The International Electrotechnical Commission (2010): *ISO/IEC 20000-4 Information techology – Service management – Part 4: Process reference model*

The International Organization for Standardization og The International Electrotechnical Commission (2007): *ISO/IEC 27001 – Informationsteknologi – Sikkerhedsteknikker – Ledelsessystemer for Informationssikkerhed (ISMS) – Krav*

The International Organization for Standardization and The International Electrotechnical Commission (2005): *ISO/IEC 27002 – Information technologi – Security techniques – Code of practice for information security management*

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

Interview

Interview den 26 marts 2012 kl. 9.00 med Kim Stormly Hansen, Deputy Chief Audit Executive ved Nykredit, Kalvebod Brygge 1-3, 1780 København V

Interview den 26 marts 2012 kl. 14.00 med Claus Thaudahl Hansen, Director i KPMG, Osvald Helmuths Vej 4, 2000 Frederiksberg

Interview den 26 marts 2012 kl. 17.00 med Jess Kjær Mogensen, Partner i PricewaterhouseCoopers og formand for FSR – danske revisorers *Informatikudvalg*, Strandvejen 44, 2900 Hellerup

Interview den 27 marts 2012 kl. 9.00 med Thomas Kühn, Executive Director hos Ernst & Young, Gyngemose Parkvej 50, 2680 Søborg

Bilag 1 – Cobit 5's Forretningsmål

Figure 5—COBIT 5 Enterprise Goals

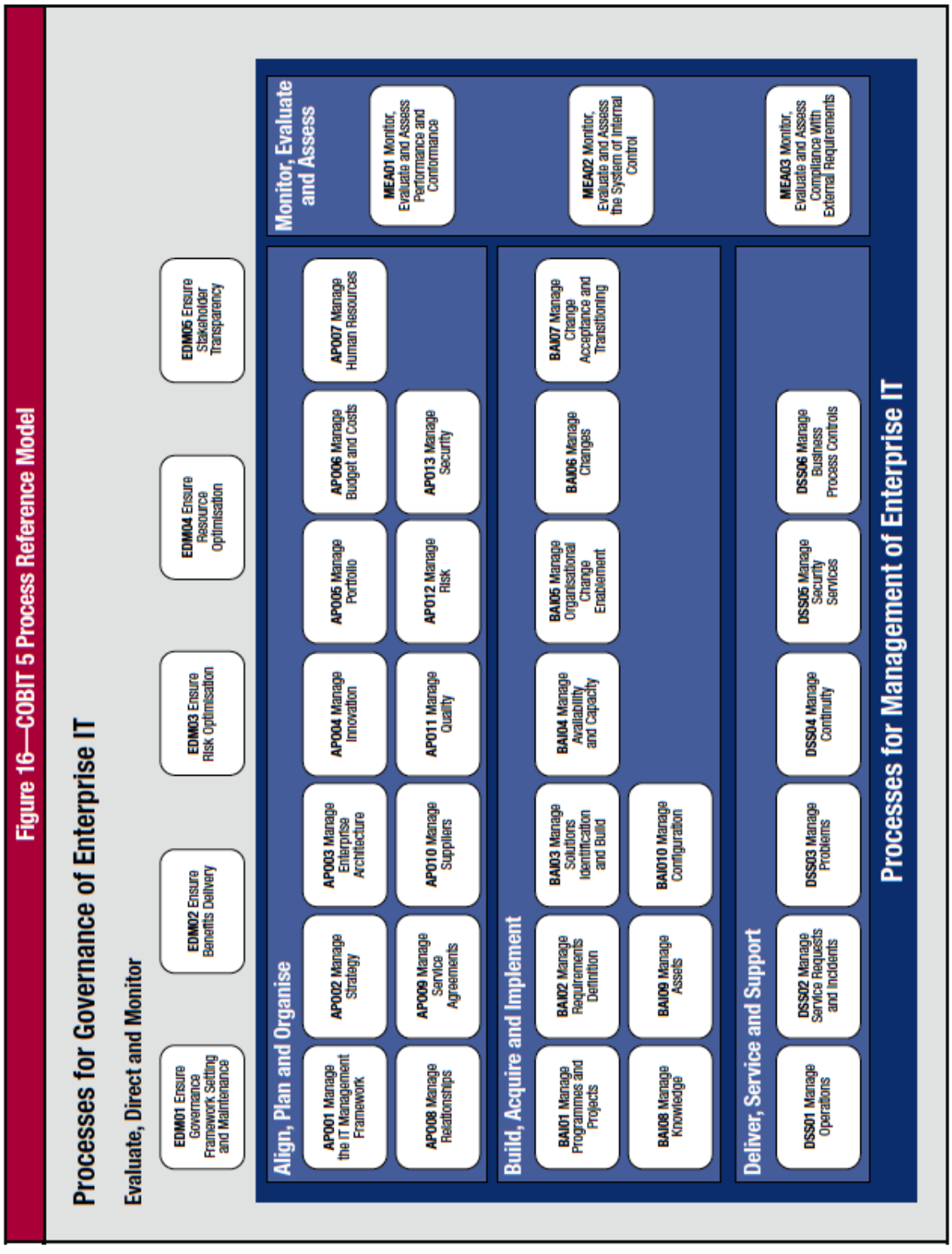
BSC Dimension	Enterprise Goal	Relation to Governance Objectives		
		Benefits Realisation	Risk Optimisation	Resource Optimisation
Financial	1. Stakeholder value of business investments	P		S
	2. Portfolio of competitive products and services	P	P	S
	3. Managed business risk (safeguarding of assets)		P	S
	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		

Bilag 2 – Cobit 5's It relaterede Mål

Figure 6—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

Bilag 3 – Cobit 5's PRM



Bilag 4 – Alignment af EDM Domænet

Alignment af Evaluate, Direct & Monitor domænet								
	ITIL	CMMI	ISO/IEC 27001 & 2	ISO/IEC 38500	ISO/IEC 20000	The 2011 Standard	Prince2	ERM
EDM01: Ensure Governance Framework Setting and Maintenance				x		x		x
EDM02: Ensure Benefits Delivery				x		x		x
EDM03: Ensure Risk Optimisation			x	x		x		x
EDM04: Ensure Ressource Optimisation				x				x
EDM05: Ensure Stakeholder Transparency				x		x		x

Bilag 5 – Alignment af APO Domænet

Alignment af Align, Plan & Organise domænet								
	ITIL	CMMI	ISO/IEC 27001 & 2	ISO/IEC 38500	ISO/IEC 20000	The 2011 Standard	Prince2	ERM
APO01: Manage the IT Management Framework	x		x		x	x		
APO02: Manage Strategy	x			x	x			
APO03: Manage Enterprise Architecture								
APO04: Manage Innovation								
APO05: Manage Portfolio	x			x	x		x	
APO06: Manage Budget and Costs	x				x			
APO07: Manage Human Ressources		x	x	x		x		
APO08: Manage Relationships	x				x			
APO09: Manage Service Agreements	x	x		x	x			
APO10: Manage Suppliers	x	x		x	x	x		
APO11: Manage Quality		x						
APO12: Manage Risk		x	x			x		
APO13: Manage Security			x			x		

Bilag 6 – Alignment af BAI Domænet

Alignment af Build, Acquire & Implement domænet								
	ITIL	CMMI	ISO/IEC 27001 & 2	ISO/IEC 38500	ISO/IEC 20000	The 2011 Standard	Prince2	ERM
BAI01: Manage Programs and Projects		x		x			x	
BAI02: Manage Requirements Definition		x						
BAI03: Manage Solution Identification and Build		x						
BAI04: Manage Availability and Capacity	x				x			
BAI05: Manage Organisational Change Enablement				x				
BAI06: Manage Changes	x				x	x		
BAI07: Manage Change Acceptance and Transitioning	x				x		x	
BAI08: Manage Knowledge	x	x						
BAI09: Manage Assets								
BAI10: Manage Configuration	x	x			x			

Bilag 7 – Alignment af DSS Domænet

Alignment af Deliver, Service & Support DSS domænet								
	ITIL	CMMI	ISO/IEC 27001 & 2	ISO/IEC 38500	ISO/IEC 20000	The 2011 Standard	Prince2	ERM
DSS01: Manage Operations	x							
DSS02: Manage Service Requests and Incidents	x		x		x	x		
DSS03: Manage Problems	x				x			
DSS04: Manage Continuity	x		x		x	x		
DSS05: Manage Security Services	x		x			x		
DSS06: Manage Business Process Controls								

Bilag 8 – Alignment af MEA Domænet

Alignment af Monitor, Evaluate & Assess domænet								
	ITIL	CMMI	ISO/IEC 27001 & 2	ISO/IEC 38500	ISO/IEC 20000	The 2011 Standard	Prince2	ERM
MEA01: M, E & A Performance and Conformance	x			x	x			
MEA02: M. E & A the System of Internal Control				x				
MEA03: M, E & A Compliance with External Requirements				x				

Bilag 9 – Ansvarsområder

Ansvarlig	Marie Elling	Mette Holleufer
Executive Summary	x	x
Indledning		
1 Problemfelt	x	x
1.1Problemformulering	x	x
2 Begrebsforklaring	x	x
3 Afgrænsning	x	x
4 Projektdesign & Metode	x	x
5 Kildekritik	x	x
Teori	x	x
6 Cobit 5 som det overordnede Framework	x	x
Cobit 5	x	x
7 Princip 1: Imødegå Interessenternes Behov	x	
8 Princip 2: Dække Virkosmheden "End-to-End"	x	
9 Princip 3: Anvende ét Integreret Framework	x	
10 Princip 4: Muliggør en Holistisk Tilgang	x	
11 Princip 5: Opdele Governance fra Management	x	
12 Implementeringsvejledning	x	
13 Proces Capability Model	x	
14 Cobit 5 - Processerne		x
Enterprise Risk Management	x	
ISO/IEC 27001		x
ISO/IEC 27002		x
ISO/IEC 20000-serien		x
ISO/IEC 38500	x	
CMMI	x	
Prince2		x
ITIL		x
The 2011 Standard	x	
Interview	x	x
Alignment	x	x
34 Alignment - EDM Domænet		
34.1 ERM	x	
34.2 ISO/IEC 27001 & 27002		x

34.3 ISO/IEC 38500	x	
34.4 The 2011 Standard	x	
35 Alignment - APO Domænet		
35.1 ISO/IEC 27001 & 27002		x
35.2 ISO/IEC 20000-serien		x
35.3 ISO/IEC 38500	x	
35.4 CMMI	x	
35.5 Prince2		x
35.6 ITIL		x
35.7 The 2011 Standard	x	
36 Alignment - BAI Domænet		
36.1 ISO/IEC 20000-serien		x
36.2 ISO/IEC 38500	x	
36.3 CMMI	x	
36.4 Prince2		x
36.5 ITIL		x
36.6 The 2011 Standard	x	
37 Alignment - DSS Domænet		
37.1 ISO/IEC 27001 & 27002		x
37.2 ISO/IEC 20000-serien		x
37.3 ITIL		x
37.4 The 2011 Standard	x	
38 Alignment - MEA Domænet		
38.1 ISO/IEC 20000-serien		x
38.2 ISO/IEC 38500	x	
38.3 ITIL		x
Konklusion	x	x
Litteraturliste	x	x