Version juli 2011

God it-skik

DANSKE REVISORER FSR

ISACA Trust in, and value from, information systems Denmark Chapter

Foreningen af Interne Revisorer The Institute of Internal Auditors - Denmark

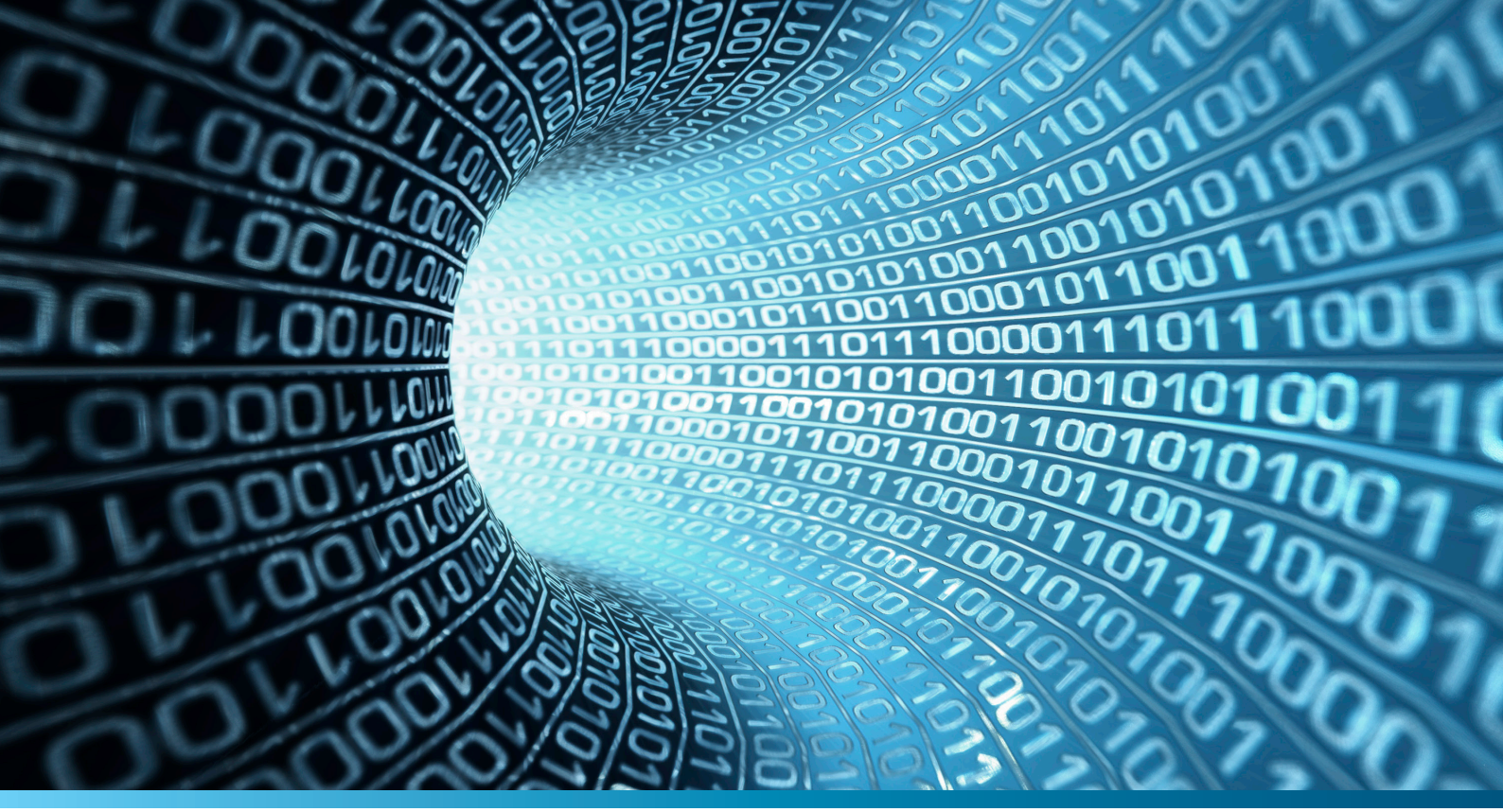
dansk•it

Arbejdsudvalget for God it-skik 2011 består af:
Jess Kjær Mogensen, FSR (formand)
Bo Lind, Dansk IT
Knut Gotfredsen, FSR
Thomas B. Joensen, IIA
Niels Thor Mikkelsen, IIA
Frank S. Nielsen, ISACA
Knud Fiil Nielsen, Dansk IT
Hans Henrik Aabenhus Berthing, ISACA

Tilblivelsen af publikationen er sket med støtte fra:
A-2, Beierholm, Capacent, Danske Bank, Deloitte, Nordea, Nets og PwC.

Version marts 2011
ISBN nr. 978-87-993781-0-4

Indhold



1. Forord

Siden udarbejdelsen af den seneste udgave af God it-skik i 1999 har udviklingen tydeliggjort, at området er ledelsens og organisationens ansvar.

Formålet med nærværende udgave af God it-skik er som for den tidligere udgave at give virksomhedernes øverste ledelse et overblik over de discipliner, det forventes at it-området mestrer, analyserer, beslutter inden for, planlægger, implementerer og følger op på i virksomhedernes it-anvendelse i overensstemmelse med god it-skik.

I forhold til første udgave er der primært sket følgende ændringer:

- Generel opdatering af sprogbrug og metoder.
- Introduktion af governance, der i publikationen anvendes som et bredt begreb.
- Tilføjelse af nye områder, bl.a. "udfasning".

Ændringerne er dels nødvendiggjort af den teknologiske udvikling og dels under hensyntagen til de øgede krav, der gennem perioden er stillet til ledelsens involvering, forståelse og håndtering af it-området.

2. God it-skik

God it-skik er som norm de branchemæssige sædvaner og den praksis, der til enhver tid efterleves af kyndige og ansvarsbevidste fagfolk med henblik på, at it-anvendelsen baseres på forretningsmæssige mål, krav og ønsker, samt at den er i overensstemmelse med lovgivningen og interne regler.

God it-skik er en del af god ledelse med fokus på informationsteknologi, systemer og deres resultater og risikostyring. Der er et særligt behov for ledelsens fokus på god it-skik som følge af øgede krav om overholdelse af initiativer og regler samt en erkendelse af, at it-projekter har stor indflydelse på en virksomheds succes.

God it-skik indebærer, at ledelsen ikke kan betragte it-området som værende en sort boks. Topledelsen bør involveres i vigtige it-beslutninger og kan ikke delegere dette ansvar til virksomhedens it-fagfolk, men skal selvfølgelig inddrage dem i beslutningsprocessen. God it-skik forudsætter en proces, hvor alle interessenter, herunder ledelse og brugere, har det nødvendige input til beslutningsprocessen.

It-anvendelsen skal tilrettelægges på en klar, overskuelig og verificerbar måde, blandt andet skal der implementeres tilstrækkelige og effektive sikkerhedsforanstaltninger.

God it-skik forudsætter bevidsthed i hele organisationen om:

- It-muligheder
- Afhængighed af it-understøttelse
- Risici forbundet med it-anvendelse
- Ansvar ved brug af it-ressourcer

Bevidstheden om disse forhold udmøntes i en klar strategi og politik, samt en hensigtsmæssig styring, organisering og tilrettelæggelse af it-anvendelsen.

God it-skik indebærer at:

1. Udvikling og opretholdelse af it-anvendelsen inddrager relevante parter i en samlet, veltilrettelagt organisatorisk proces med virksomhedens forretningsstrategi som målsætning.
2. Rollerne vedrørende it-anvendelsen, herunder ansvar og arbejdsopgaver, er omhyggeligt opdelt for at sikre, at der er en rimelig og effektiv indbyrdes balance mellem opgaver, ressourcer, råderum og kontrol i overensstemmelse med virksomhedens behov.
3. Beslutninger træffes på en formaliseret måde, og at såvel beslutninger som systemer og procedurer dokumenteres, kommunikeres og følges.
4. De involverede personer har en positiv, ansvarsbevidst og disciplineret holdning til it-mulighederne som vitale redskaber for virksomheden.
5. Medarbejdere bliver tilstrækkeligt uddannet, instrueret og trænet i de opgaver, de skal udføre.
6. Tilrettelæggelsen af it-anvendelsen indeholder effektive sikkerhedsforanstaltninger og beredskab i overensstemmelse med virksomhedens behov.
7. Der er fastlagt rammer, der sikrer effektiv tilpasning til ændrede forudsætninger.

3. Ledelsens ansvar

En forudsætning for god it-skik er, at der på det øverste ledelsesniveau træffes beslutning om de muligheder, it-anvendelsen indebærer for forretningsstrategien. It er i dag et naturligt emne på dagsordenen i forbindelse med ledelsesmøder – i såvel den øverste ledelse som den daglige ledelse.

Det er et ledelsesansvar, at der skabes effektiv interaktion og integration mellem it-afdelingen og forretningen. Den øverste ledelse bør derfor med udgangspunkt i forretningsstrategien drøfte, hvorledes it-anvendelsen kan understøtte virksomhedens forretningsfunktioner og anvendes strategisk til at udvikle forretningen. Forretningsforståelse og en grundlæggende analyse af styrker, svagheder, muligheder og trusler er centralt ved disse drøftelser.

Rammerne for it-anvendelsen bør fastlægges i form af visioner, strategier, mål og planer for it-anvendelsen, blandt andet bør der tages stilling til kompetencebehov og sourcing-strategi. Porteføljestyring og it-risikostyring er nødvendige aktivitetsområder, der indgår ved styringen af it-anvendelsen.

Organisationen af it-aktiviteterne bør fastlægges på et overordnet niveau, herunder bør der tages stilling til, om der er behov for særlige it-fora (udvalg, komitéer eller lignende) nedsat af den øverste ledelse til drøftelse af centrale områder vedrørende it-anvendelsen.

På en række områder stilles der lovkrav vedrørende virksomhedens styring og samfundets kontrol med virksomhederne.

Af selskabslovgivningen fremgår, at ledelsen har ansvaret for selskabets forsvarlige organisation og tilrettelæggelse af den interne kontrol, og bestyrelsen/tilsynet bør derfor blandt andet tage stilling til virksomhedens it-organisation, idet denne del af organisationen antages at have væsentlig betydning for styringen af virksomheden.

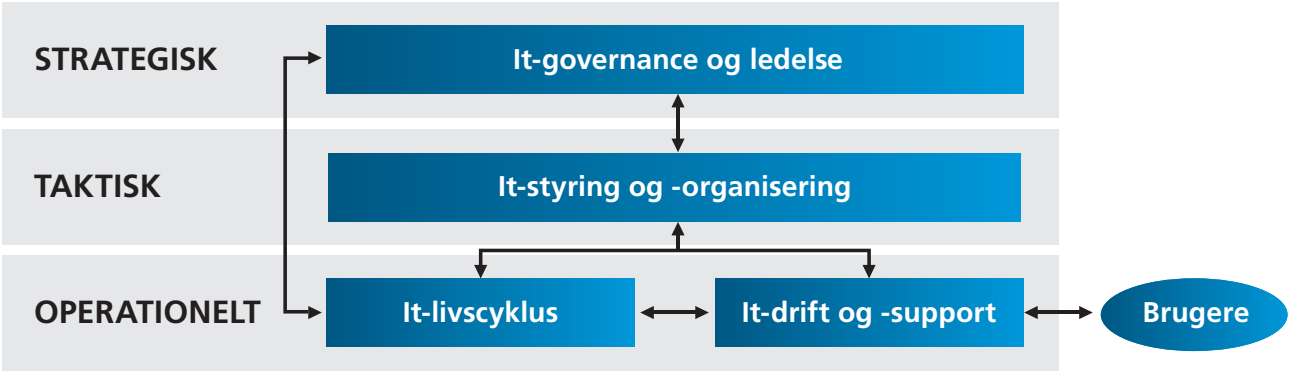
I andre dele af lovgivningen stilles der krav til it-systemer og data, registrerede personoplysninger samt ophavsret til systemer og indretning af (it-)arbejdspladser.

For visse virksomhedstyper, f.eks. offentlige og finansielle virksomheder, stilles der særlige krav. Ligeledes vil en række udenlandsk ejede virksomheder i større eller mindre grad være omfattet af den lovgivning, der gælder i moderselskabets hjemland.

Lovkravene er under stadig forandring, bl.a. som følge af nye og/eller opdaterede EU-direktiver, hvilket nødvendiggør en stadig opmærksomhed herpå. Dette til sikring af at såvel implementeringen som den efterfølgende efterlevelse af lovkravene kan ske med en afbalanceret ressourceindsats og om muligt på en måde, hvorved der tillige opnås forretningsmæssige fordele.

4. Opdeling af it-aktiviteter i processer

Procesbeskrivelserne i dette og de efterfølgende afsnit er på et overordnet niveau og er af relevans for de fleste virksomheder. Processerne tilrettelægges i den enkelte virksomhed i henhold til virksomhedens vision, mål, kultur og kapacitet.



Overordnet bør virksomhedens it-processer opdeles i følgende fire hovedprocesser:

1 **IT-GOVERNANCE OG -LEDELSE** omfatter virksomhedens overordnede it-ledelsesprocesser og bør typisk udmøntes af virksomhedens øverste ledelse. Strategisk planlægning og opfølgning er væsentlige elementer i it-governance og -ledelse. Processerne driver virksomhedens øvrige it-processer og sikrer, at virksomheden udvikler sig målrettet.

2 **IT-STYRING OG -ORGANISERING** omfatter styringen af virksomhedens informationsteknologiske ressourcer, dvs. fastlæggelse af rammer for virksomhedens teknologiske udvikling, organisering af de menneskelige ressourcer og styring af risici og eksterne krav.

3 **IT-LIVSCYKLUS** omfatter processerne omkring håndtering af anskaffelse, udvikling, implementering og udfasning af it-løsninger i virksomheden indenfor de rammer, der er givet, og i overensstemmelse med den kontrakt der er indgået med forretningen om it-understøttelse. Som led i styringen af virksomhedens it-anvendelse bør der ske en løbende overvågning og opfølgning på processerne.

4 **IT-DRIFT OG -SUPPORT** sikrer, at de implementerede it-løsninger afvikles i henhold til ovenstående hovedprocessers fastlagte rammer og i den besluttede kvalitet.

Der bør som udgangspunkt være en klar adskillelse mellem hovedprocessen "it-livscyklus" og "it-drift og -support". "It-livscyklus" bør inddrage viden fra "it-drift og -support" ved planlægning af et projekt, og der bør være klare processer for overdragelse af implementerede it-løsninger til it-drift.

For en it-organisation må det forventes, at der er en klarhed over de opgaver, som it-organisationen skal varetage. Dette bør ske gennem en procesorienteret tilgang, der sikrer, at it-organisationen arbejder målrettet og tværorganisatorisk.

Udarbejdelse, dokumentation og implementering af processer bør ske der, hvor det giver værdi, og på flere niveauer – gerne således, at processerne kan anvendes til flere formål fra ledelsesoverblik til daglige, operationelle rutiner.

It-organisationen bør have et realistisk ambitionsniveau, således at den evner at vedligeholde, indføre og justere processerne på en måde, så en optimal anvendelse opnås. En proces kan først betragtes som implementeret, når der er etableret en proceskultur, og når medarbejderne arbejder efter de vedtagne processer.

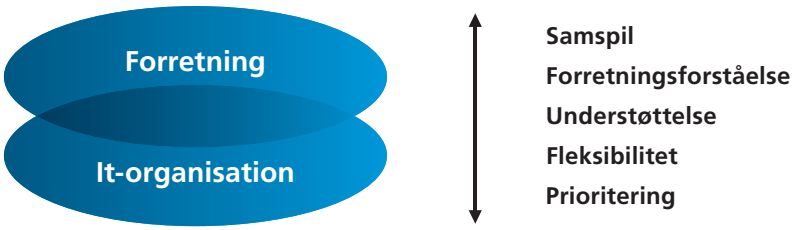
Internt bør it-organisationen kunne dokumentere, hvordan opgaver på tværs af ansvarsområder håndteres, og det bør være klart, hvem der er ansvarlig for de enkelte dele i processen. Til støtte herfor kan ledelsen tage udgangspunkt i et (eller flere) relevante metodeværk. Eksempler på sådanne metodeværk er COBIT, ISO, MSP, PRINCE2, PMI, CMMI og ITIL.

Fælles for disse er, at de er udarbejdet af internationalt anerkendte institutter med global forankring. Det skal dog understreges, at der ligger forskellige filosofier bag disse, som kan være i konflikt, og derfor bør it-ledelsen i samråd med forretningsledelsen vurdere den konkrete relevans af de enkelte metodeværk.

Det bør løbende vurderes, om it-organisationen i tilstrækkelig grad har implementeret processerne på en måde, der sikrer, at processerne skaber værdi, optimerer arbejdsgangene og minimerer relevante risici. Det må desuden forventes, at der ligger en plan for den videre modning – og at planen er taget i anvendelse.

It-organisationen skal sikre, at processerne rækker ind i basisorganisationen de steder, hvor det er hensigtsmæssigt. Enten fordi organisationen skal kunne følge fremdrift, adressere behov og problemer, eller fordi it-afdelingen ønsker basisorganisationen inddraget i bl.a. beslutningsprocesserne (f.eks. i forbindelse med opgaveprioritering).

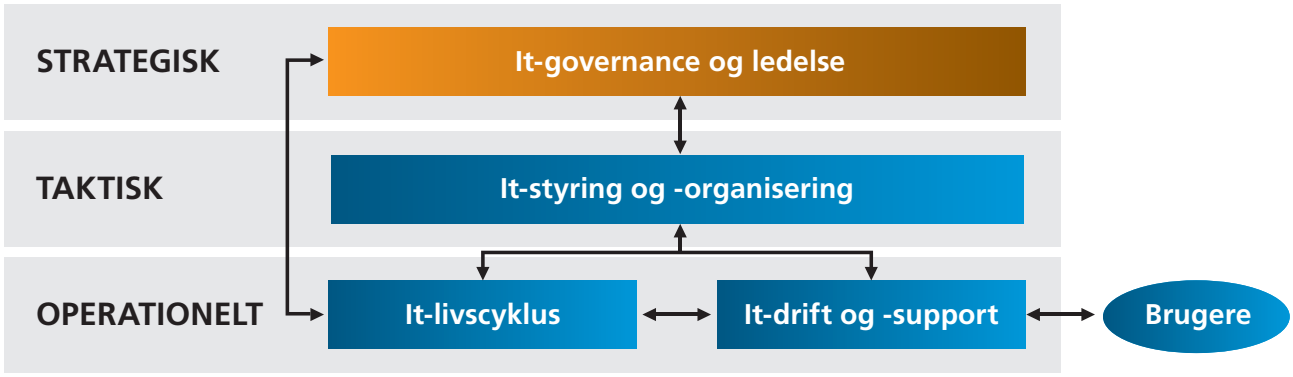
INTERAKTION MELLEM FORRETNING OG IT-AFDELING



Der bør være defineret klare processer for, hvordan der sikres et tæt samspil mellem de forretningsmæssige mål og it-understøttelsen, herunder realistiske tidsintervaller, rolle- og ansvarsfordeling og beslutnings-kompetenceniveauer. Selvom topledelsen har ansvar for it-governance, vil det normalt være it-organisationen, der har ansvaret for at facilitere processerne for området, og det må forventes, at it-organisationen har kompetencer, der kan se it-disciplinen ud fra en forretningsmæssig synsvinkel og forstå processen og interaktionen mellem forretning og it-afdeling.

5. It-governance og ledelse

Procesbeskrivelserne i dette og de efterfølgende afsnit er på et overordnet niveau og er af relevans for de fleste virksomheder. Processerne tilrettelægges i den enkelte virksomhed i henhold til virksomhedens vision, mål, kultur og kapacitet.



Formål
At sikre at virksomhedens it-anvendelse understøtter virksomhedens forretningsstrategi og -politikker. God it-skik indebærer et tæt samspil mellem virksomhedens øverste ledelse og ledelsen af it-aktiviteterne for at sikre, at virksomhedens it-anvendelse udvikler sig i overensstemmelse med forretningen, og at it anvendes strategisk og til at udvikle forretningen.

It-organisationen skal tilføre forretningen viden om it-anvendelse, og forretningen skal tilføre it-organisationen viden om forretningen.

5.1 It-strategisk planlægning

It-strategisk planlægning handler om fastsættelse af mål for it-anvendelsen, der bidrager optimalt til virksomhedens forretningsmæssige og organisatoriske udvikling. Dette kan kun ske, hvis der er tæt samklang mellem virksomhedens vision og de aktiviteter, som it-organisationen iværksætter for at understøtte denne.

Den øverste ledelse bør sikre sig, at:

- der er fastsat klare mål for it-anvendelsen
- der er sammenhæng mellem forretningsstrategien og it-strategien
- ledelsesansvaret er adresseret, når det gælder it-strategiske beslutninger
- målene i it-strategien er kendte og accepterede i hele organisationen
- der er fastlagt retningslinjer for, hvordan ressourcerne tilvejebringes, så målene kan realiseres
- sammenhængen mellem it-organisation og forretning tilrettelægges på en måde, der sikrer, at målsætningerne kan realiseres
- der er etableret processer til evaluering af og opfølgning på fremdrift vedrørende målopfyldelsen
- der er etableret besluttende organer til sikring af forankring, fremdrift, korrektioner og prioritering.

Modenhed

Som en del af den strategiske planlægning bør topledelsen skabe sig et overblik over it-anvendelsens modenhed, herunder den nuværende situation og fremadrettede forventninger inkl. tiltag, der kan sikre nødvendig vækst.

Dette forudsætter bl.a.:

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

Når ovenstående elementer håndteres for et it-område, forventes det, at der tages stilling til, om der kan opnås yderligere fordele gennem outsourcing til en eller flere samarbejdspartnere med større kapacitet og kompetence. En outsourcing skal løbende ledes, og der må derfor afsættes interne ressourcer med de rette kompetencer til løbende opfølgning og ændringshåndtering.

Strategiske indfaldsvinkler
It-strategisk planlægning vil have forskellige indfaldsvinkler og fokus efter hvilken type forretning, it-anvendelsen skal understøtte. Som hovedregel er betydningen af it-anvendelsen afhængig af branche, ydre faktorer og virksomhedens it-teknologiske udviklingsstade.

Virksomhedsledelsen bør sammen med it-ledelsen have gjort sig klart, hvordan balancen mellem sikkerhed omkring it-drift og innovativ it-udvikling skal være. Virksomheder vil have forskellige behov alt efter den forretning, der skal drives, og der vil være en række langsigtede it-organisatoriske og økonomiske aspekter forbundet med de strategiske valg, der tages.

Virksomhedens ledelse bør være bevidst om den strategiske rolle, it-anvendelsen skal spille i virksomheden, ligesom it-ledelsen skal organisere sig i forhold dertil.

5.2 Analyse af muligheder og risici

Virksomhedens interessenter har forventninger og stiller en række krav til virksomheden. På den ene side forventninger om at virksomheden skal være innovativ, skabe værdi og være effektiv. På den anden side stilles der krav om styring af risici og overholdelse af lovgivning, myndighedskrav og god virksomhedsledelse. Virksomheden bør vurdere disse forventninger og krav, afbalancere dem og afspejle dem i strategiske styrings-, compliance- og sikkerhedsmæssige tiltag, hvor virksomheden anvender it til realiseringen.

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

5.3 Beslutning og planlægning

Beslutning om og planlægning af it-aktiviteter er – for de dele, der har betydning for den øvrige forretning – et fælles anliggende mellem it-organisationen og den øvrige virksomhed. Opgaverne, udfordringerne, fremdriften og de beslutninger, der er taget på virksomhedens vegne, bør derfor være synlige.

It-ledelsen og den øverste ledelse bør derfor forholde sig til:

1. I hvilket regi forskellige typer af beslutninger bør tages.
2. Hvordan der skabes ejerskab til besluttede it-aktiviteter i den del af organisationen, hvor ændringen vil få betydning.
3. Hvilken beslutningsproces der er nødvendig for de forskellige typer af beslutninger.
4. Hvordan beslutningerne gradueres i en beslutningsstruktur.
5. Hvilken it-service der skal være til stede for at opnå virksomhedens mål.
6. Hvordan der sikres fornuftig balance mellem økonomi og betydning for forretningen.

En række praktiske ledelsesdiscipliner skal anvendes for at sikre succes med ovenstående punkter, f.eks. etablering af en it-komité eller et fagudvalg, der har et relevant kommissorium, en repræsentation og en beslutningskraft og er sammensat tværorganisatorisk, med fokus på procesoptimering og standardisering.

Styring af udviklingsprojekter
Det er vigtigt, at virksomhedsledelsen har overblik over og løbende prioriterer porteføljen af udviklingsprojekter. Det er ved gennemførelse af de rette udviklingsprojekter, at målopfyldelsen sikres på et område.

For virksomheder der løbende gennemfører udviklingsprojekter, bør der etableres processer, procedurer og standarder til sikring af ensartet og sammenlignelig projekthåndtering. Discipliner som overblik over sponsoreret ressourcetildeling, økonomi, fremdrift, risici og realisering af de benefits/forbedringer, som projektet muliggør, bør indgå. Rådgivning, kontrol, kvalitetssikring og vedligeholdelse af disse discipliner bør varetages af en funktion med spidskompetencer på området, f.eks. et projektkontor.

Ved større forandringer bør der etableres et program. Et program består af den række projekter, der skal til for at nå en overordnet vision og et mål. Programmet sikrer, at projekternes størrelse og kompleksitet bliver mindre, at projekterne bliver mere håndterbare, og at de gennemføres til rette tid og inden for de aftalte økonomiske rammer. Som en del af programmet bør opfølgning på indfrielse af aftalte forandringer og rationaler indgå, og forandringsagenterne i forretningen spiller en central rolle.

Ved planlægning af konkrete udviklingsaktiviteter bør der indgå overvejelser om:
1. Sponsor- og ejerskab
2. Samspil mellem forretning, projektorganisation og it-organisation
3. Involvering af relevante interessenter
4. Forandringsparathed og forankring
5. Ændringshåndtering
6. Afhængigheder til andre aktiviteter eller omstændigheder
7. Milepæle og risici
8. Styringsbehov, roller og ansvar

Beslutningsprocessen
Beslutningerne bør tages ud fra en klart defineret ansvarsfordeling, således at alle interessenter kender deres beslutningskompetence på de forskellige områder. Den øverste ledelse kan påtage sig dette ansvar på områder af vital betydning for virksomheden, men normalt vil ansvaret være placeret hos den, der er ansvarlig for, at fordelene realiseres, og det vil også være her, procesejerskab og sponsorering er placeret.

Ejerskaberne bør være klart definerede:
Procesejer – hvormed menes ansvar for forretningens processer og arbejdsgange.
Systemejer – som er et mere teknisk ejerskab af den konkrete løsning, der skal understøtte de ønskede forretningsprocesser.
Dataejer – som har ansvar for datakvalitet, fortrolighed, integritet og tilgængelighed.

It-ledelsen bør til enhver tid kunne fremvise den dokumentation, der kan give den øverste ledelse og de øvrige ansvarlige den nødvendige indsigt i initiativerne, fremdriften og de realiserede effekter. It-organisationen har kompetencerne til at facilitere beslutningsprocesserne, forventningsafstemme og være bindeled mellem forretningen (f.eks. repræsenteret ved procesejeren) og it-organisationen.

5.4 Implementering

Ved implementeringen af løsningerne sikrer ledelsen, bl.a. gennem udarbejdelse af handlingsplaner, at:
1) beslutningerne kommer til organisationens kendskab i fornødent omfang
2) beslutningerne er klare og overskuelige for dem, der skal føre dem ud i livet
3) processerne sikrer, at relevante krav til overholdelse af lovgivningen efterleves
4) der er den fornødne viden og andre menneskelige ressourcer til rådighed
5) der er de fornødne økonomiske ressourcer
6) der foretages den fornødne detaljerede planlægning i forhold til opgavernes art og karakter
7) implementeringen er underlagt fornøden styring og rapportering
8) de forretningsmæssige mål, der ligger til grund, er kendte.

5.5 Overvågning og opfølgning

Ledelsens overvågning og opfølgning omfatter en række forhold, f.eks. compliance, performance, risici og opfyldelse af forretningsmæssige krav mv. Overvågning og opfølgning er ledelsens mulighed for at sikre (eventuelt ved anvendelse af uafhængige undersøgelser og objektive vurderinger), at de vedtagne beslutninger føres ud i livet, og at de forventede resultater opnås.

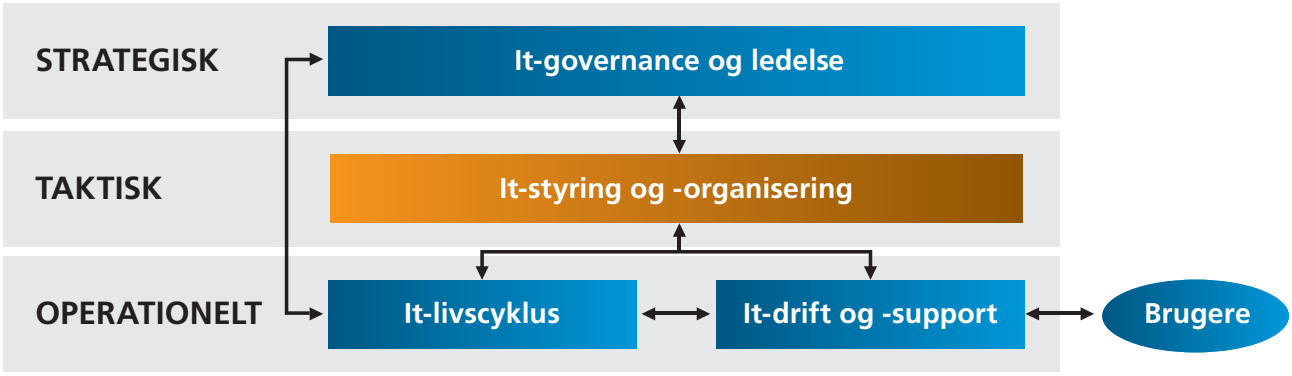
Ledelsen prioriterer, hvad der skal foretages opfølgning på, og tilrettelægger opfølgningen med udgangspunkt heri. Herved fastlægges en frekvens for opfølgning, ressourcer hertil, samt hvilket ledelsesniveau der skal være involveret i opfølgningen og/eller bedømmelsen af resultatet af opfølgningen.

Den praktiske overvågning og opfølgning sker ved, at:

1) ledelsen i fornødent omfang deltager i planlægningen og gennemførelsen, herunder opfølgning på Key Performance Indicators
2) ledelsen regelmæssigt får forelagt planer og budgetter
3) ledelsen på passende valgte tidspunkter får forelagt statusrapporter
4) der gennemføres målinger af, om de planlagte resultater opnås og potentielle gevinster realiseres
5) der foretages en passende kvalitetsvurdering af de gennemførte opgaver
6) ledelsen følger op på investerings- og omkostningsbudgetterne i forhold til den aktuelle udvikling i virksomheden.

6. It-styring og organisering

Procesbeskrivelserne i dette og de efterfølgende afsnit er på et overordnet niveau og er af relevans for de fleste virksomheder. Processerne tilrettelægges i den enkelte virksomhed i henhold til virksomhedens vision, mål, kultur og kapacitet.



6.1 Styringsprincipper og -modeller

Formål
At sikre at virksomhedens it-ressourcer og it-udvikling styres, så de anvendes optimalt i forhold til virksomhedens strategi. Dette sker ved anvendelse af metoder og værktøjer, der er afpasset efter virksomhedens forhold.

6.1.1 Styring af udviklingsprojekter

Virksomheden bør lægge sig fast på en projektstyringsmodel, der kan dække behovet for styring af de forskellige typer af projekter, som virksomheden over tid skal have håndteret, f.eks. anskaffelser, systemudvikling, organisationsudvikling, vedligeholdelse af driftsmiljø og sourcing.

Modellen skal bl.a. sikre, at:

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

6.1.2 Styring af drift og vedligeholdelse

Der bør anvendes standardiserede drifts-, vedligeholdelses- og afviklingsmetoder, således at it-anvendelsen er velstruktureret og dokumenteret.

Der bør udvikles eller anskaffes værktøjer til effektivisering og understøttelse af metoder og standarder. It-arkitekturen bør fastlægges efter behov til sikring af effektivt genbrug og udnyttelse af it-løsningerne.

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

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

Der bør anvendes en struktureret metode til versionsstyring og -kontrol til at sikre, at:
1) den gældende version svarer til den, som ledelsen og systemejeren har godkendt
2) der er overensstemmelse mellem den gældende version og den tilhørende dokumentation
3) der til stadighed kan redegøres for og genfindes tidligere versioner i fornødent omfang.

Der bør anvendes ændringsprocedurer for at sikre, at alle ændringer i eksisterende systemer kvalitetssikres, godkendes (af proces-, system- og dataejer) og dokumenteres, samt at der etableres fallback-planer i tilstrækkeligt omfang, inden de sættes i drift.

Det anbefales, at der anvendes strukturerede og dokumenterede test for at sikre, at ændringerne lever op til de forretningsmæssige mål, og for at sikre at forretningsgangene kan gennemføres efter ændringerne. Testindsatsen tilpasses den forretningsmæssige risiko.

6.2 Organisering

Formål
At sikre optimale organisatoriske rammer til varetagelse af it-relaterede aktiviteter med klare roller og ansvar for rådgivende forsamlinger blandt beslutningstagere, medarbejdere, leverandører og andre interessenter.

6.2.1 It-organisering

Der bør etableres en gennemskuelig organisationsstruktur med klare kommandoveje, en informationsstruktur og en klar definition af mandat, rolle og ansvar for alle, der medvirker. Gennem den rette organisering skal det sikres, at it-ressourcerne kan anvendes optimalt og koordineret, således at suboptimering og afhængighed af enkeltpersoner undgås.

Organisationsstrukturen bør endvidere sikre ledelsens og brugernes indflydelse på it-anvendelsen, når it-anliggender kommer på dagsordenen

Der bør sikres en høj grad af koordinering og kommunikation mellem it-organisationen og dens interessenter.

Ansvar og beføjelser i it-organisationen bør være klart beskrevet og kommunikeret og skal efterleves i praksis.

En organisatorisk adskillelse af brugerfunktioner, udviklings-/vedligeholdelsesfunktioner, driftsfunktioner og sikkerhedsfunktioner bør etableres og overvåges, således at ingen enkeltperson har eller kan få kontrol over alle faser i it-anvendelsen.

Hvis virksomheden har valgt at outsource it-aktiviteter, bør det sikres, at en organisatorisk funktion forhandler, optimerer, overvåger og styrer indgåede aftaler med hensyn til serviceniveau, forretningsmæssigt udbytte, ændringshåndtering og risici.

6.2.2 Kvalificerede medarbejdere

De nødvendige medarbejderressourcer bør sikres, såvel kvantitativt som kvalitativt.

De enkelte medarbejdere bør kvalificeres til deres arbejdsfunktion gennem oplæring, efteruddannelse og træning.

Medarbejderne bør sikres et forsvarligt arbejdsmiljø, såvel psykisk som fysisk.

Er der ikke kritisk masse til opretholdelse af et kompetenceområde, bør det overvejes at tilføre nye kompetencer, at kompetenceudvikle eller om det er bedre, at en ekstern konsulent eller leverandør varetager opgaven.

6.2.3 Kommunikation af it-relateret information

Rapportering og opfølgning bør tilrettelægges, så den er målrettet de behov, som de enkelte it-ansvarlige og interessenter har for at kunne holde sig tilstrækkeligt orienteret, beslutte rettidigt samt styre aktiviteter og initiativer.

Det anbefales, at der etableres et performanceopfølgningssystem indeholdende:

- Bruger-/kundeundersøgelse
- Opfølgning på strategien: Er strategi, teknologi og arkitektur i overensstemmelse med markedets udvikling, følger applikationsstrategien virksomhedens udvikling, og implementeres it-strategien som besluttet?
- Produktivitet og effektivitet
- Opfølgning på projekter
- Opfølgning på serviceydelser.

Medarbejderne bør have den fornødne forståelse af ledelsens holdninger, mål, strategier, politikker og øvrige retningslinjer, herunder forventninger til performance, kvalitet og sikkerhed.

Målsætninger, strategier, politikker og al øvrig nødvendig information bør være let tilgængelig for medarbejderne i virksomheden.

6.2.4 Fastlæggelse af ejerskab af it-aktiver

Systemer, udstyr, netværksressourcer og faciliteter bør have en organisatorisk ejer, der er ansvarlig for anskaffelse, vedligeholdelse og anvendelse af disse. For outsourcede aktiviteter bør ejerskab af aktiviteten stadig forankres internt i virksomheden.

6.3 Styring af risici og eksterne krav

Formål
At afdække eksterne krav, vurdere risici i forbindelse med virksomhedens it-anvendelse og etablere de vedtagne forholdsregler til sikring af virksomhedens it-anvendelse som et væsentligt element i virksomhedens generelle risikostyring.

6.3.1 Risikovurdering af it-anvendelsen

Analyse, vurdering og håndtering af risici ved den samlede it-anvendelse bør gennemføres regelmæssigt i henhold til en valgt metode.

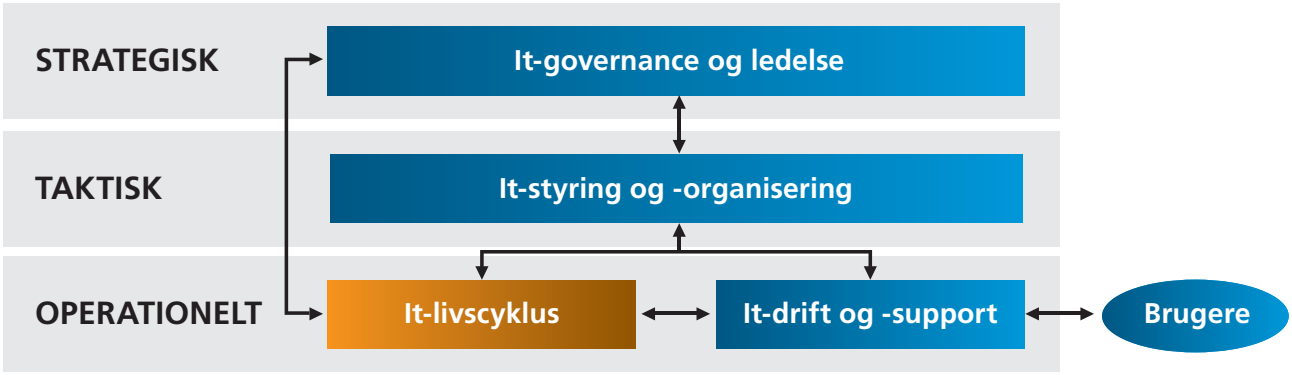
6.3.2 Overholdelse af regulativer og aftalte rammer

Virksomheden bør etablere og vedligeholde interne regelsæt og procedurer, der kan sikre overholdelse af lovgivning, aftaler, branchestandarder og lignende regulering, som virksomheden er underkastet.

Reguleringens betydning for virksomheden bør vurderes, og der bør etableres foranstaltninger, der gør virksomheden i stand til at følge op på overholdelsen af disse regelsæt og procedurer.

Kendskabet til interne regelsæt og procedurer bør udbredes og forankres i organisationen.

7. It-livscyklus



7.1 Behovsanalyse og afdækning af løsningsmuligheder

Formål
Der gennemføres en analyse af de forretningsmæssige behov for it-understøttelse samt de mulige teknologiske løsninger til dækning heraf som grundlag for at træffe beslutninger om eventuel anskaffelse, udvikling, implementering og udfasning af løsninger.

7.1.1 Gennemførelse af behovsanalyser

Anskaffelse og implementering af it-løsninger bør besluttes ved, at der forud for investeringen gennemføres analyser af forretningsområdets behov og krav.

Det er forretningens fagområder, der med deres forretningsviden skal sikre, at alle relevante behov er kortlagt, og at der er udarbejdet en business case.

Som en del af behovsanalysen bør der foretages en prioritering og et fagligt skøn af, om et behov har tilstrækkelig transaktionsmængde til at skulle understøttes af den nye teknologi.

It-organisationen har ansvaret for styringen af behovsanalyseprocessen og skal sikre, at behovsanalysen og opstillingen af krav bliver gennemført på en måde, der gør implementering af ny teknologi mulig. Ved opstillingen af krav skal det tilstræbes, at disse er udformet på en måde, der giver mulighed for at udnytte den nye teknologis logik optimalt og dermed nedbringe behov for specialtilpasning til et minimum.

It-organisationen skal tilegne sig en vis forretningsindsigt, men primært have kompetencer der kan facilitere it-rettede dele af en behovsanalyse og i den forbindelse inddrage faglig spidskompetence fra forretningen eller gennem ekstern assistance.

I behovsanalysen er det væsentligt at vurdere de behov og muligheder, der er for information (intern og ekstern), samt hvorledes informationen vil kunne anvendes.

7.1.2 Afdækning af teknologiske muligheder og leverandører

Afsøgning af markedet anvendes dels til at identificere relevante løsninger på de beskrevne forretningsmæssige behov og dels til at identificere løsninger, som kan supplere de erkendte behov med mere visionære løsninger.

It-løsninger har ofte lang levetid fra anskaffelsesbeslutning til udfasning, og det er vigtigt, at man i afsøgningsfasen bevidst vurderer den teknologiske levetid for potentielle løsninger.

Ved vurderingen af leverandørerne er det vigtigt at være opmærksom på, både hvem der leverer basisteknologien, og hvem der tænkes at skulle levere den konkrete løsning. Det er ofte vigtigere, at basisteknologien er relativt standardiseret, end at løsningsleverandøren forventes at blive i markedet.

7.2 Anskaffelse af brugersystemer

Formål
At sikre en forsvarlig og styret anskaffelse (enten i form af teknologi, rammesystemer eller som udviklingsprojekt) af det valgte system under anvendelse af de fastlagte metoder og standarder.

7.2.1 Anskaffelse af brugersystem

Ved anskaffelse af it-løsninger af en vis størrelse, kompleksitet og økonomi bør valg af løsning og leverandør ske gennem en udbudsproces.

Der findes forskellige modeller for gennemførelse af udbud, ligesom der er lovgivning, virksomheds- og branchenormer for dette. It-ledelsen bør derfor sætte sig grundigt ind i dette felt, således at den undgår at blive beskyldt for pligtforsømmelse og lovbrud.

Fælles for god udbudshåndtering er, at:
- udbudsbetingelserne skal være klare, entydige og overholde lovgivning og branchenormer
- udbudsmaterialet skal udformes således, at tilbuddene bliver sammenlignelige
- tilbudsgiverne skal gøres bekendt med udbudsbetingelser, proces og tidsfrister
- tilbudsgiverne skal have lige vilkår
- ingen tilbudsgivere må forfordeles med information og dialog
- valget af leverandør sker alene efter de opstillede udvælgelseskriterier
- der skal gives begrundet afslag på tilbud.

7.3 Etablering og vedligeholdelse af it-infrastruktur

Formål
At sikre en forsvarlig og styret etablering, vedligeholdelse og ændring af it-infrastrukturen ved brug af fastlagte metoder og standarder. It-infrastrukturen skal vedligeholdes, så den understøtter de forretningsmæssige behov, it-strategien og de forretningskritiske applikationer.

7.3.1 Fastlæggelse og vedligeholdelse af it-infrastruktur

It-infrastrukturen skal understøtte etablering, brug og deling af information i virksomheden på en måde, der på optimal vis sikrer integritet, fleksibilitet, funktionalitet, rettidighed, tilgængelighed og sikkerhed. It-organisationen bør sikre etablering og vedligeholdelse af en it-infrastruktur, der understøtter forretningens ønsker og behov. Dette indebærer, at:

1) it-organisationen bør foretage en regelmæssig revurdering af arkitekturen i forhold til nye teknologier, ændrede organisatoriske forhold samt ændringer i virksomhedens omverden – eksempelvis kundekrav eller lovmæssige krav
2) der bør fastlægges en kontrolstruktur i it-infrastrukturen
3) systemarkitektur (it-systemer), informationsarkitektur (databaser m.v.) og teknologiarkitektur (netværk, udstyr og basissystemer) bør fastlægges
4) it-organisationen bør etablere en beskrivelse af systemsammenhænge samt evt. datamodel og dataklassifikation
5) de teknologiske forudsætninger for effektiv udvikling, drift og vedligeholdelse, herunder ændringer, bør etableres gennem adskilte udviklings-, test- og driftsmiljøer
6) der er etableret en struktureret ændringshåndtering med klare roller, ansvar og beslutningsprocesser
7) der bør etableres en samlet oversigt over anvendt it-udstyr, basissystemer, databaser med videre.

7.4 Projektforløb

Formål
At sikre det rette mandat og forsvarlig gennemførelse af alle former for it-projekter til aftalt tid, økonomi og opnåede effektmål.

7.4.1 Etablering af projektramme

Der bør foretages en ansvarsplacering, der sikrer en hensigtsmæssig organisatorisk forankring af ansvaret for projektets gennemførelse og økonomi.

Der bør etableres en kompetent projektorganisation, herunder styre- og arbejdsgrupper, der sikrer de fornødne ressourcer såvel kvalitativt som kvantitativt.

Der bør fastlægges realistiske mål, succeskriterier og tidsterminer.

Der bør etableres en begrebsramme for den økonomiske vurdering og prioritering af it-investeringer og -service. Denne bør forankres i en portefølje af projekter, der er underbygget af business cases, kalkuler og budgetter.

7.4.2 Fastlæggelse af fornødne aftaler

Der bør etableres kontrakter for alle væsentlige eksterne leverancer på it-området (anskaffelse af udstyr, konsulentassistance, vedligeholdelsesaftaler og outsourcing-aftaler). Kontrakterne bør fastlægge begge parters juridiske ansvar, pligter og rettigheder i forbindelse med den aftalte leverance.

I kontrakter med eksterne leverandører bør kontrol af de modtagne ydelser (tid og kvalitet) være defineret i kontrakten, evt. som tillæg. Endvidere bør der være mulighed for at vurdere designet og effektiviteten af kontrollen, hvilket eventuelt kan foretages af en uafhængig tredjepart.

For interne ydelser indgås de fornødne serviceniveauaftaler, som fastlægger ansvaret for it-komponenternes drift og vedligeholdelse samt ydelsernes målbare kvalitet.

7.4.3 Plan for implementering

Der bør udarbejdes en plan for implementeringsforløbet med klare rolle- og ansvarsfordelinger, ressourcetræk og succeskriterier for gennemførelsen.

Der bør fastlægges et testforløb, der giver organisationen tilstrækkelig mulighed for at kunne overbevise sig om it-teknologiens virkemåde, og som kan afdække eventuelle væsentlige fejl eller uhensigtsmæssigheder.

Den reelle mulighed for at videreføre forretningsprocesserne i tilfælde af, at it-grundlaget ikke lever op til forventningerne, eller at den forsinkes, bør sikres ved udarbejdelse af fallback-planer.

Den nødvendige uddannelse af brugere, teknisk personale, drift- og supportpersonale bør sikres forud for ibrugtagning af it-teknologien (eller dele heraf).

I de tilfælde hvor det drejer sig om implementering af nye it-brugersystemer, skal der tillige udarbejdes en plan for konvertering af data fra gammelt til nyt system, og der bør træffes beslutning om indsamling af intern og ekstern information til brug for løsningen.

7.4.4 Igangsætning/transition

Til sikring af en effektiv og kontrolleret igangsætning og transition skal en række forhold adresseres.

Betydelige interessenter bør deltage i planlægningen af igangsætningen og give input ud fra brugernes krav, herunder gennemgå anmodninger om ændringer, ændringsforslag, ændringsplaner og business cases, før ændringer godkendes. De betydelige interessenters grundlag for vurdering, prioritering og godkendelse af ændringer bør klarlægges, og der bør udarbejdes en analyse af konsekvenserne, herunder de tekniske, økonomiske, personalemæssige og organisatoriske konsekvenser.

Idriftsætning bør være forberedt og kontrolleret, før nye eller ændrede services/applikationer sættes i drift. Samtidig bør det påses, at planer og aktiviteter i løbet af transitionsprocessen sker i forhold til fastlagte kriterier.

Testplaner bør udarbejdes i overensstemmelse med risikoprofilen, og test bør udover funktionalitet omfatte installations-, integrations-, belastnings-, performance- og penetreringstest. Herudover bør det testes, hvorvidt ændringen giver den forventede effekt og de forventede fordele. Muligheder for utilsigtede resultater bør vurderes med betydelige interessenter. Resultaterne heraf bør indgå i risikovurderingen og i beslutningen om at afvise/acceptere ændringen eller gennemføre eventuelle risikobegrænsende tiltag.

Der skal sikres behørig ændringsdokumentation til at vurdere effektiviteten af ændringer, virkningen af ændringer og indhentede erfaringer. Et ændringsstyringsteam i virksomheden bør deltage i eller overvåge samt godkende hasteændringer, herunder informere brugerne om eventuelle risici ved ændringen og indhente deres accept af implementeringen af ændringen.

Efter implementeringen bør det sikres, at kontrolaktiviteterne er i overensstemmelse med forretnings-områdets behov og aftaler.

7.4.5 Effektmåling

Både under projektet og efter projektet er overdraget til drift, og it-løsningen er taget i anvendelse, skal der følges op på, om de effektmål, der er en del af business casen, realiseres. Dette gælder både for en ny infrastruktur og ved et nyt brugersystem.

Styregruppen vil normalt have aftalt nogle forandringsagenter (fra forretningen eller it-afdelingen), der skal sørge for, at effektiviseringstiltag igangsættes, så effekten opnås.

7.5 Udfasning

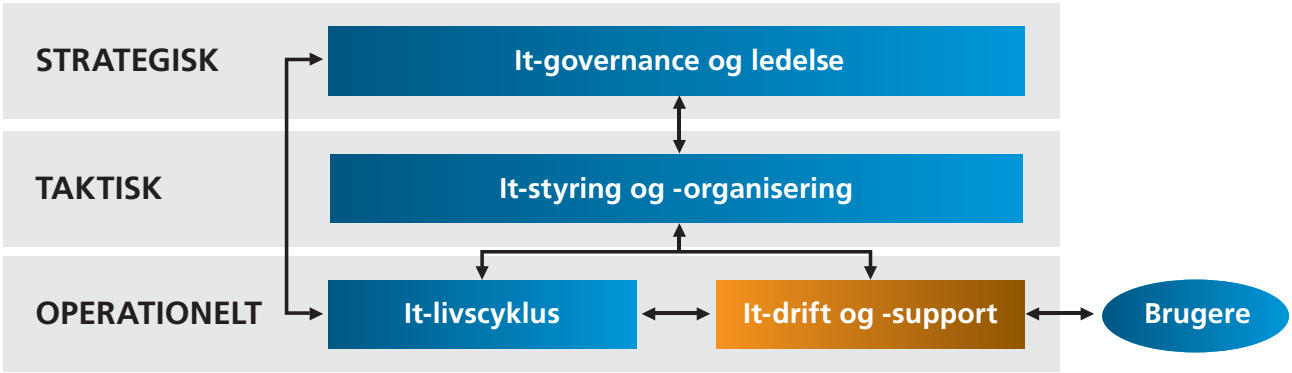
Ligesom der er fokus på udvikling af it-området, bør it-ledelsen i tæt samarbejde med forretningen løbende vurdere rentabiliteten af de it-løsninger, der er i drift. It-ledelsen bør sikre, at der løbende foretages vurderinger af it-driftsmiljøet med henblik på at finde potentiale for driftsoptimering (teknologisk, kontraktligt og organisatorisk).

Som en del af den samlede projektportefølje bør de udfasningsprojekter indgå, der med de rette og netop tilstrækkelige kompetencer sikrer et optimalt driftsmiljø, rentable it-systemer og en rentabel it-organisation (i forhold til de opgaver, der skal varetages).

Ved beslutning af nye it-udviklingstiltag bør der indgå overvejelser om udfasning af de it-systemer og den it-service, som bliver overflødig ved implementeringen af de nye tiltag. Det er it-ledelsens ansvar at sikre dette.

På områder hvor it-drift og vedligeholdelse er udliciteret (outsourcet) til anden it-driftsleverandør, bør it-ledelsen sikre, at der løbende foregår en ændringshåndtering og aftalestyring, således at virksomheden kun får løst de opgaver, der giver værdi og effektivitet.

8 It-drift og -support



8.1 It-drift og service management

Formål
At sikre at it-drift og service management er styret og kontrolleret på en sådan måde, at it-opgaverne afvikles rettidigt og effektivt.

8.1.1 Gennemførelsen af it-drift og service management

Planlægningen af it-drift og service management bør være med til at understøtte virksomhedens forretningsprocesser og funktioner. Det bør ske på en sådan måde, at eventuelle hændelser eller afbrydelser minimeres og håndteres, uden at it-brugerne bliver unødigt genereret af dette.

Virksomheden kan vælge at outsource dele af it-driften eller service management til tredjepart. Ledelsen har dog fortsat det overordnede ansvar for drift og service management.

It-ledelsen bør sikre en styret og kontrolleret it-drift og service management, der sker ved efterlevelse af de fastlagte metoder og standarder, herunder at it-driften gennemføres i henhold til det aftalte kvalitets- og serviceniveau. It-drift bør således:

- baseres på forretningens behov og brugernes krav
- være i overensstemmelse med interne retningslinjer, lovgivning og kontraktuelle forpligtelser
- være effektivt og sparsommeligt (virkningsfuldt) sourcet og leveret
- integreres med anden service
- ske i samarbejde med leverandører og underleverandører
- overvåges og forbedres løbende.

Følgende er nøglefaktorer, der påvirker it-drift og service management

Leveringen af it-service bør være baseret på klare strategiske mål, som er afstemt med nuværende og fremtidige forretningsplaner. Styringen af it-service bør i særlig grad:

- underbygge it-strategien (og virksomhedens vision og strategi)
- skabe et stabilt og pålideligt it-driftsmiljø
- skabe opmærksomhed, indsigt og forståelse gennem klar kommunikation
- formalisere, standardisere og optimere it-processer, så de er effektive og lette at følge
- opbygge kendskab til anerkendte standarder og certificeringer, og inddrage disse hvor det giver værdi
- støtte og handle for at sikre overholdelse af politikker, standarder og kontroller for at overholde interne og eksterne regulatoriske og retslige krav (f.eks. bogføringsloven selskabslovgivning, persondataloven, markedsføringsloven, EU-direktiver og Basel II for finansielle virksomheder)
- sikre et positivt og optimalt afkast af investeringer i it-understøttede initiativer.

8.1.2 Overvågning

It-ledelsen bør fastlægge, hvilke begivenheder der skal overvåges og styres i forhold til den it-service, der leveres til virksomhedens kunder – såvel interne som eksterne. Som følge heraf bør begivenheder, der påvirker it-service, overvåges, og der bør gribes ind, når begivenhederne påvirker it-servicen negativt. Efter en overtrædelse af en aftale evalueres hændelsesforløbet, årsagerne hertil identificeres, og der træffes de nødvendige korrigerende foranstaltninger.

It-driften bør overvåge og sikre, at løsninger af udfald af it-service iværksættes hurtigst muligt og i prioriteret rækkefølge.

Der bør udføres regelmæssig rapportering i forbindelse med problemhåndtering, og der bør defineres en politik og regler for overvågning og rapportering. Der bør ligeledes udarbejdes rapporter til at måle it-serviceniveauet og svartiderne og for at identificere tendenser eller tilbagevendende problemer.

8.1.3 Drifts- og servicerutiner

Som en del af beredskabet bør begivenheder og hændelser, der kan medføre forstyrrelser, identificeres, og det bør fastlægges, hvilken reaktion der er nødvendig (f.eks. hændelse, manuel reaktion, service desk-alarm).

Der bør løbende ske en måling af forventninger og servicetilfredshed ved at indhente tilbagemelding fra brugere og forretningsområder samt ved rapportering om serviceniveau, succeser og fiaskoer, baseret på en prioritering, der er aftalt med forretningsområderne, af hændelser pr. service/ydelse. Hændelsernes forretningsmæssige betydning indgår i prioriteringen. Dette indebærer, at definerede niveauer og tidsplaner for funktionel og hierarkisk eskalering baseres på aftalte mål med kunderne. Serviceniveauet skal være aftalt og dokumenteret i aftalen, og der foretages regelmæssig gennemgang af aftalerne for at sikre, at servicen opfylder brugernes behov.

Brugerne bør være bekendt med servicen, dens tilgængelighed og procedurerne for service-anmodning samt give feedback med meningsfuld og detaljeret kategorisering af hændelser og problemer. Brugerne bør ligeledes være involveret i og støtte op om undersøgelser i at diagnosticere årsager til serviceproblemer. Herunder sikre at et passende niveau af ressourcer og ekspertise anvendes.

Indhentet viden om problemer medtages i et service-review med den forretningsansvarlige kunde. Dette skal sikre, at kunden er bekendt med de iværksatte tiltag og planer for at forhindre, at fremtidige større hændelser indtræffer.

Driftsplanerne skal gennemgås for at sikre, at kundernes krav er opfyldt, og at kunderne får den rigtige information sikkert og rettidigt.

It-drift bør løbende arbejde med forretnings- og serviceteamet med henblik på løbende forbedringer af servicen. Forbedringerne bør være drevet af forretningsmæssige mål og ønsker.

8.2 It-support og brugeradministration

Formål
At sikre brugerne en kontrolleret adgang til informationer og data, der er begrænset på baggrund af et forretningsmæssigt behov. Og at sikre at brugerne har adgang til den nødvendige information, der kan understøtte og hjælpe brugerne i anvendelsen af it.

8.2.1 Vejledning og støtte af brugerne i anvendelse af systemer

Det bør sikres, at slutbrugere af it-systemer får den nødvendige støtte til at kunne anvende disse. Det skal være med til at sikre en god og sikker anvendelse af it-systemerne. Det vil endvidere minimere risikoen for, at fejl opstår under anvendelse af it-applikationerne. Støtte til brugerne bør omfatte:

- Daglig support af brugerne, herunder vejledning og instruktion i anvendelse af systemerne
- Prioritering og afhjælpning af hændelser
- Information til brugerne om opståede hændelser eller utilgængelighed i systemerne (hvis muligt varsel i god tid i form af servicevinduer)
- Formel uddannelse af brugerne i anvendelse af it-systemer

8.2.2 Administration af logiske og fysiske brugeradgange

Det bør sikres, at administrationen af logiske og fysiske brugeradgange sker på betryggende vis efter klart definerede rutiner. Dette skal være med til at sikre styring af adgang til relevant funktionalitet, samtidig med at den nødvendige funktionsadskillelse opretholdes.

Ved tilrettelæggelsen af brugeradministrationen bør der tages hensyn til nedenstående:

- Forestå vedligeholdelse af brugerautorisationer i henhold til gældende politikker.
- Sikre at tildeling af logisk og fysisk brugeradgang sker ud fra et forretningsmæssigt behov.
- Identificere kritiske brugeradgange eller autorisation og sikre størst mulig begrænsning af adgange til disse.
- Sikre funktionsadskillelse mellem it-udvikling, it-drift og forretning.
- Sikre en passende adskillelse mellem forretningskritiske funktioner.
- Sikre adskillelse mellem forretningsanvendelse og teknisk systemadministration
- Begrænse leverandørers adgang til det netop nødvendige.
- Sikre at styresystemer, netværk, kommunikationsudstyr, databasesystemer m.v. er opsat i overensstemmelse med it-sikkerhedspolitikken.
- Regelmæssig gennemgang og vurdering af de rette adgangsforhold, både fysiske og logiske.
- Overvågningsprocedurer der sikrer registrering af it-mæssige hændelser, herunder alle former for tilsigtet og utilsigtet ændring af data.
- Rapporteringsprocedurer der sikrer, at systemejeren og ledelsen informeres om sikkerhedsbrud.
- Etablering af fysisk beskyttelse af it-komponenter, herunder fysisk adgangskontrol i henhold til gældende politikker.

9. Ledelsens it-værktøjskasse

9.1 Den øverste ledelses opmærksomhedspunkter

Det følger af selskabslovgivningen, at selskabets øverste ledelse skal sørge for en forsvarlig organisering af selskabets regnskabsfunktion, intern kontrol, it-organisering, budgettering og særlige risici.

I de fleste virksomheder har it en sådan væsentlighed, at det er naturligt, at den øverste ledelse forholder sig til virksomhedens it-anvendelse, it-organisation og it-sikkerhed.

Bestyrelsen bør derfor ved enhver væsentlig ændring og som minimum en gang årlig forholde sig til følgende forhold i relation til it:

- It-strategi og politik
- It-risikovurdering
- Virksomhedens informationssikkerhedspolitik

9.2 It-strategi og -politik

En it-strategi er den samlede beskrivelse af den øverste ledelses strategiske beslutninger om it-anvendelse. It-strategien bør være i overensstemmelse med virksomhedens forretningsstrategi.

Virksomheden kan vælge at inkludere it-strategien i forretningens samlede strategi. Her vil it-organisationen på linje med de øvrige forretningsområder arbejde efter en understøttende forretningsplan. Alternativt kan it-strategien være udarbejdet som særskilt disciplin af it-ledelsen.

It-strategien bør ikke stå alene, men skal være fulgt af dokumenterede, underbyggende aktiviteter og rammer på de næste ledelsesniveauer (taktisk og operationelt niveau). Kun herved godtgøres at it-strategien efterleves i praksis.

Ved udarbejdelsen af en it-strategi vil følgende områder fra it-strategien blive behandlet på strategisk niveau:

- Visioner og pejlemærker
- Serviceniveau
- Arkitektur og forretningsunderstøttelse
- Styring, organisering og politikker
- Kompetencer
- Risikostyring og informationssikkerhed
- Økonomi

På taktisk niveau bør der udarbejdes handlingsplaner til sikring af, at grupper og teams kan prioritere opgaver. Formulerede politikker sikrer den adfærd og kultur, der bedst sikrer strategiens opfyldelse. Dokumenterne bør udarbejdes på gruppeleder- og teamchefniveau på baggrund af anbefalinger og beslutninger fra etablerede beslutningsfora.

På operationelt niveau bør der defineres processer, procedurer, instrukser og manualer for at effektivisere, synliggøre og ensarte daglige rutiner. Der bør foretages en løbende afvejning og prioritering, så der ikke skabes et overflødigt administrativt eller arbejdsmæssigt bureaukrati. Der bør udpeges ansvarlige for løbende vedligeholdelse af de udarbejdede materialer.

Processen med tilblivelsen af en it-strategi er vigtig, idet den bør være forankret i de dele af virksomheden, der skal bidrage til sikring af, at strategien bliver realiseret. Derfor bør forretning, it-ledelse og andre relevante interessenter inddrages i processen. Det samme gør sig gældende ved justeringer af it-strategien.

It-strategiens udformning og gennemgående tema vil være styret af, hvor it-anvendelsen er i sin modenhed, og hvad virksomheden har fokus på. Det kunne f.eks. være:

- Vækst
- Konsolidering
- Sourcing (herunder licitering)
- Fusion eller spaltning
- Stabilisering
- Procesoptimering (effektivisering)

I relation til it-strategien bør der som minimum være en politik for, hvordan der prioriteres mellem opgavebehov, økonomi og ressourcer, således at it-anvendelse og intentionerne for it-strategien overholdes.

9.3 It-risikovurdering

Risikovurderingen er en proces, der tager udgangspunkt i en analyse af de it-mæssige risici, der eksisterer for de forskellige forretningsmæssige processer. Ved gennemførelse af risikovurderingen bør det overvejes, hvilke begivenheder (såvel interne som eksterne forhold) der kan påvirke opfyldelsen af virksomhedens strategier i form af forhold knyttet til:

- It-driften
- Systemudviklingen
- It-leverandører
- Datasikkerheden
- Medarbejdere
- Regeloverholdelse

En effektiv risikovurderingsproces bør sikre, at:

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

Ledelsen bør i risikoanalysen forholde sig til fortrolighed, integritet og tilgængelighed ved vurdering af relevante trusler og sårbarhed. Dette kan ske ved at opliste relevante sikkerhedstruende hændelser i f.eks. 8-10 grupper og for disse vurdere sandsynlighed og konsekvens for at få et reelt trusselsbillede i forhold til virksomhedens kritiske forretningsprocesser.

Sikkerhedstruende hændelser kan f.eks. være:

- menneskelige fejl
- systemfejl
- driftsproblemer
- manglende efterlevelse af procedurer
- personafhængighed
- uautoriserede eller kriminelle interne aktiviteter
- eksterne angreb
- organisatoriske problemer
- uforudsete konsekvenser af ændringer.

Virkningen af eksisterende sikringsforanstaltninger bør vurderes for at bedømme deres tilstrækkelighed i forhold til virksomhedens risikovillighed. På baggrund af vurderingen kan der suppleres med yderligere sikringsforanstaltninger for at begrænse nettorisikoen.

9.4 Virksomhedens informationssikkerhedspolitik

Virus-angreb, spam-mails, manglende backup, hacking, misbrug af systemadgange, manglende beskyttelse af oplysninger, tyveri af it-udstyr og lignende it-sikkerhedsbrud er konkrete trusler mod mange virksomheders drift, økonomi og omdømme.

Informationssikkerhed bør i dag tages for givet som en virksomhedsdisciplin og skal derfor være integreret i forretningsprocesserne, udviklingen og teknologianvendelsen samt i ledelsens og medarbejdernes kultur på arbejdspladsen.

Til sikring af at virksomhedens ledelses generelle holdning til sikkerhed er kendt og defineret, bør der udarbejdes en informationssikkerhedspolitik. Risikoanalysen i afsnit 9.3 er meget konkret og et vigtigt element i fastlæggelsen af politikken. Risikoanalysen kan dog ikke tage højde for alle forhold, hvorfor fastlæggelse af nogle grundlæggende principper er relevant.

Virksomhedens ledelse bør derfor deltage i fastsættelsen af et passende niveau for informationssikkerhed. Niveauet fastlægges og prioriteres under hensyntagen til relevante trusler, konsekvenser, ressourcer, de forretningsmæssige mål, relevant lovgivning og aftalemæssige forpligtelser.

Virksomhedens informationssikkerhedspolitik bør indeholde virksomhedens:

- Målsætning for informationssikkerhed
- Organisering af informationssikkerhedsarbejdet
- Generelle procedurer for risikovurdering
- Identifikation af relevant lovgivning og aftalemæssige forpligtelser
- Samlede risikoappetit
- Basale sikkerhedsregler og sikringsforanstaltninger.

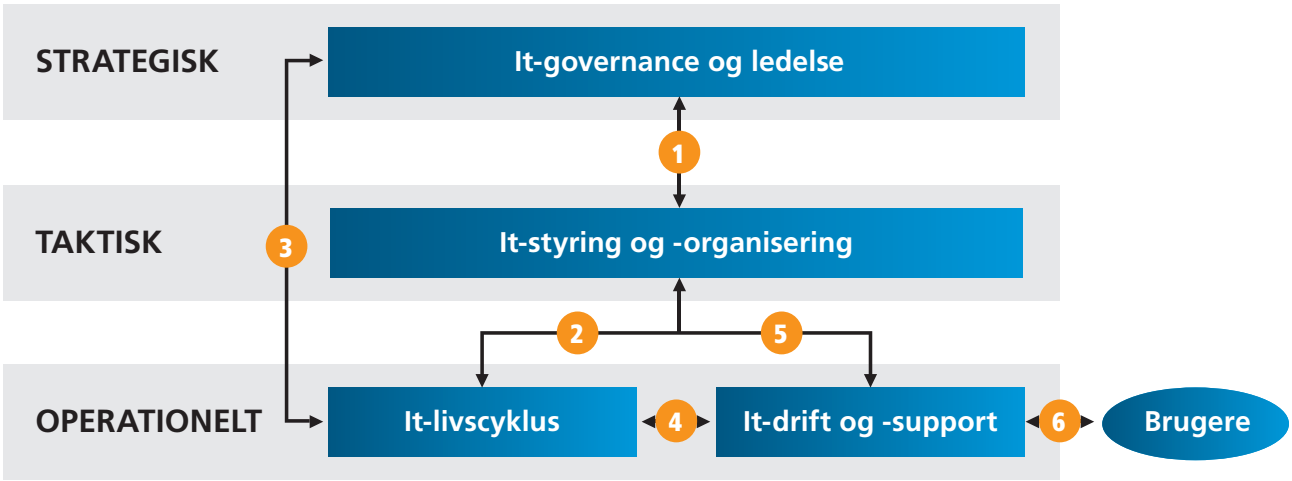
Undertiden adresserer informationssikkerhedspolitikken ligeledes de værdier og principper, som skal forankre det besluttede informationssikkerhedsniveau blandt virksomhedens ansatte.

It-risikoanalyse og -vurdering bør gentages i henhold til en besluttet frekvens, f.eks. én gang årligt. Væsentlige interne eller eksterne ændringer, som påvirker virksomhedens trusselsbillede, bør adresseres som led i den løbende vedligeholdelse af informationssikkerhedspolitikken.

I selskaber bør bestyrelsen årligt forelægges virksomhedens informationssikkerhedspolitik med henblik på godkendelse. Det vil ofte være hensigtsmæssigt at basere virksomhedens informationssikkerhedspolitik på et eksisterende framework, jf. **afsnit 4**, idet man herved får adgang til en eksisterende struktur, hjælpeværktøjer o. lign.

9.5 Styringsinformation for it-området

I det følgende beskrives væsentlige informationer (dokumenter) til sikring af forventningsafstemning og styring mellem de beskrevne hovedprocesser. Informationerne bruges på forskellige ledelsesniveauer, hvilket er illustreret i nedenstående figur.



Nedenfor er angivet en liste over de væsentlige nøgledokumenter, der ofte bruges som styringsdokumenter.

Spilleregler for information:

- En information (et dokument) bruges til at forventningsafstemme eller afrapportere mellem to hovedprocesområder.
- Normalt udarbejder det nederste niveau dokumentet efter aftalte rammer, og niveauet over godkender dokumentets rigtighed og indhold.
- De dokumenter, der er godkendt på et overordnet niveau, vil altid være ramme for underliggende hovedprocesområder og gentages derfor ikke i tabellen nedenfor.
- Tabellen forholder sig ikke til, hvordan de enkelte informationer er registreret og formidlet, men det er oplagt at håndtere og formidle informationerne i elektroniske medier.
- Listen af informationer i tabellen nedenfor er opstillet i vilkårlig rækkefølge, og det skal understreges, at tabellen ikke er fuldkommen, men et eksempel på information der kan indgå.
- Den enkelte virksomhed skal forholde sig til, hvilken styringsinformation der skal være til stede, for at forretningen og it-understøttelsen heraf drives på forsvarlig vis.

Snitflade	Information	Regi hvori informationen behandles
1	• Forretningsstrategi og politikker • It-vision og -mål • It-strategi og -handlingsplan • It-ressourcestrategi • It-budget og -regnskab • It-sourcingstrategi • It-kompetencestrategi • It-serviceniveauaftale (SLA) • It-projektprioriteringsstrategi • It-sikkerhedspolitik og -beredskabsplaner	• Øverste ledelse • Forretningsansvarlige • It-chef • It-sikkerhedschef • It-ændringsråd
2	• It-udviklingsplaner • It-projektstyringsmodel • It-projektportefølje • It-programledelse • Erfaringsopsamling • It-udviklingsmetoder og -standarder	• It-ledelse • It-projektledelse • It-udviklingschef • It-programchef
3	• It-kundeudviklingsplaner • It-projektkommissorium • It-projektplan (projektinitieringsdokument) • It-business case • It-ændringsanmodninger • It-risikovurdering • It-kommunikationsplan • It-projektfremdriftrapport • It-projektøkonomi	• It-kundekonsulenter (KAM'er) • Forretningens forandringsagenter • Styregrupper • Seniorsponsor • It-projektchef • It-projektledere • It-projektkontor
4	• It-driftsoverdragelse • It-versionsstyring • It-problemhåndtering • It-arkitektur	• It-udviklingschef • It-driftsleder • It-transitionsprojektteam • It-arkitekt
5	• It-driftsmetoder og -standarder • It-driftshåndbog • It-produktions- og kapacitetsplan • SLA-monitorering og -rapportering • It-problem- og hændelsesrapporter	• It-ledelse • It-driftsledelse
6	• It-procedurer for fejlhåndtering • It-vejledninger og -hjælperutiner • Status og statistikker på it-fejlsager • It-forbedringsforslag	• It-servicedesk / it-helpdesk • It-supportchef • It-brugere og superbrugere • It-brugergrupper

DANSKE REVISORER FSR

ISACA Trust in, and value from, information systems Denmark Chapter

Foreningen af Interne Revisorer The Institute of Internal Auditors - Denmark

dansk•it