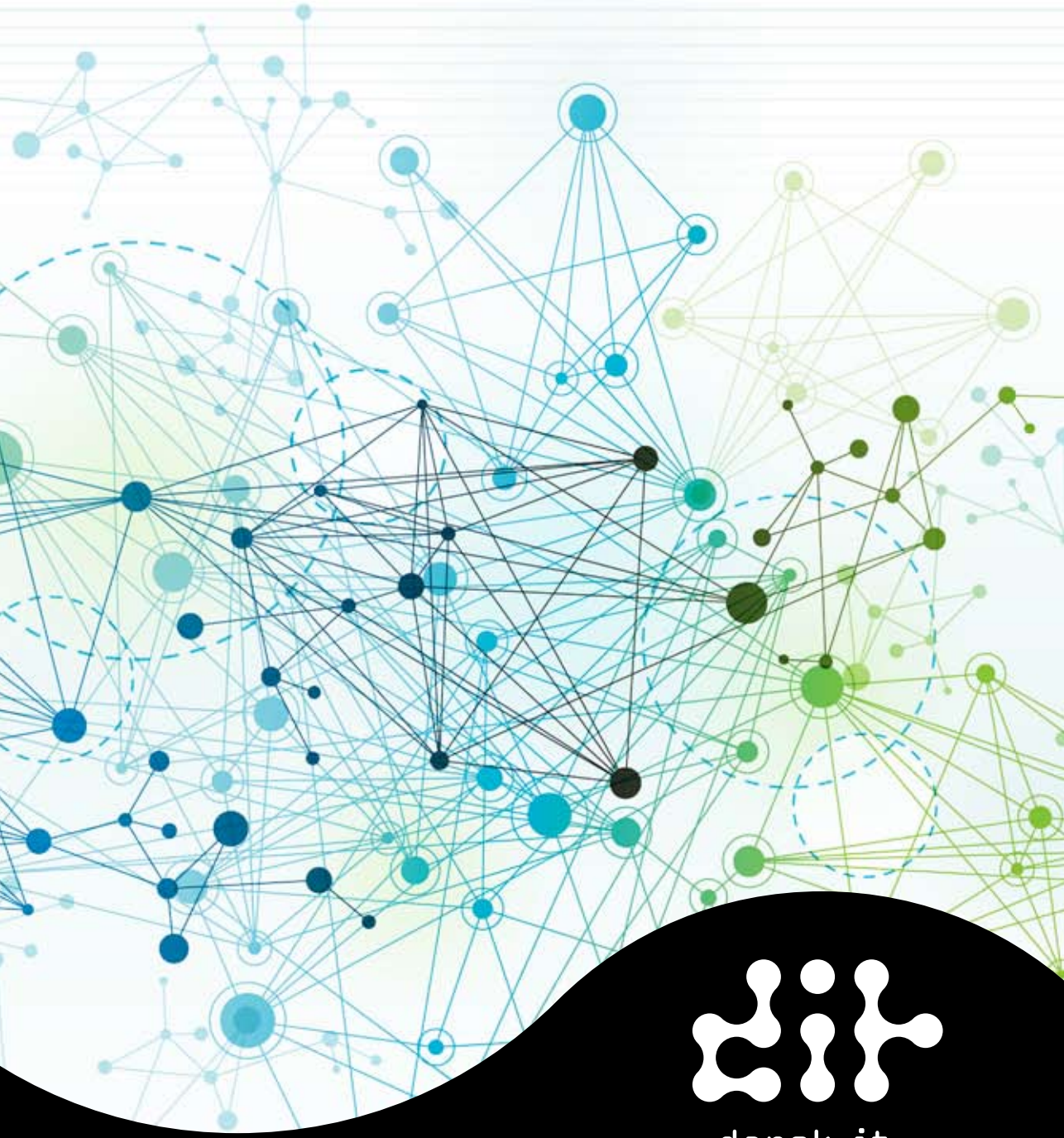
Sikkerhed ved it-outsourcing

Quickguide



dansk·it

Quickguide:
Sikkerhed ved it-outsourcing

1. udgave, 1. oplag 2012

Oplag: 1000 stk
Udgivelse: november 2012

Forfattere:
DANSK IT's it-sikkerhedschefkreds

Tryk:
Jannerup Offset a/s

Layout:
DANSK IT

Bredgade 25a
DK 1260 København K
Tlf: +45 3311 1560
dit@dit.dk
www.dit.dk

Quick-guide

Sikkerhed ved it-outsourcing

Udarbejdet af
DANSK IT's It-sikkerhedschefkreds

dansk•it

Indhold

Indledning

Denne guide er tiltænkt de it-sikkerhedsmæssige aspekter ved It-outsourcing, og omhandler ikke den forretningsmæssige vinkel ved outsourcing, da det forudsættes, at selve beslutningen om outsourcing er vurderet. Endvidere vendes elementer omkring revision, jura og CSR i korte træk.

It-sikkerhedschefkredsen har valgt at skrive denne quick-guide, fordi vi har erfaring for, at sikkerhed og andre risikofaktorer ofte bliver overset eller tænkt på i en fase, hvor virksomheden allerede har truffet beslutningen – måske endda underskrevet kontrakten. Manglende fokus på sikkerhed og andre risikofaktorer, vi beskriver i denne guide vil ofte betyde, at omkostningen i forhold til den oprindelige business case vil øges, når disse faktorer senere kommer til at indgå.

Disse faktorer skal derfor afdækkes i en tidlig analysefase, og være en del af beregningsgrundlaget for en realistisk business case.

Informationssikkerhed og risiko ved elementerne hemmeligholdelse, integritet og tilgængelighed er omdrejningspunkter i guiden.

Formål

Målet med denne guide er at give et hurtigt overblik over de væsentligste risikofaktorer, man bør tage med i sine overvejelser allerede i en analysefase, og dermed et enkelt værktøj til at vurdere disse faktorer. Samtidig er guiden et medvirkende redskab til at få beskrevet en business case, så der ikke kommer for mange ”hovsaer” senere.

It-sikkerhedschefkredsen, der står som forfatter til guiden, tæller ca. 35 sikkerhedschefer eller it-sikkerhedschefer fra store virksomheder i Danmark, og guidens punkter er bygget op på basis af medlemmernes samlede erfaringer. Med hensyn til de juridiske overvejelser har vi fået bistand af koncernjurist og Compliance Officer i Tryg, Bettina Drejer Clausen. De revisionsmæssige vinkler er beskrevet med bistand fra IT-revisorer.

Opbygning

Guiden indeholder et antal punkter i en struktur, som afspejler faserne i en outsourcing situation.

- Forberedelse
- Samarbejdsfasen
- Afslutning af samarbejdet

Under de enkelte punkter er med få linjer beskrevet, hvad det går ud på. Dette skal betragtes som selve tjeklisten, som kan anvende selvstændigt. Guiden er i sin natur ikke dybdegående, men den skulle gerne vække opmærksomheden hos læseren, der efter behov må fordybe sig grundigere i de enkelte elementer.

De enkelte punkter er beskrevet mere uddybende senere i guiden, men igen må det understreges, at der ikke er tale om detaljerede svar på alt. Det kræver læserens egen fordybning i de enkelte risikopunkter.

Definitioner på outsourcing og offshoring

Der findes flere forskellige definitioner på outsourcing. Vi har valgt at holde os til en simpel fortolkning. Outsourcing er i sin enkelthed at overføre varetagelse af en opgave/dele af en opgave til et andet firma. Det omfatter således ikke indkøb af varer eller tjenester.

Begrebet offshoring dækker i princippet over det samme – her er blot tale om at opgaverne outsources til en virksomhed i et andet land.

Vi håber at denne kortfattede guide kan være med til at højne sikkerheden, når en virksomhed påtænker at outsource.

På vegne af It-sikkerhedschefkredsen,
Tom Engly, koncernsikkerhedschef, Tryg Forsikring A/S.

Guidens punkter som tjekliste

Forberedelse

- ☐ **Hvilken form for outsourcing** *(uddybning side 11)*
  Outsourcing betyder i bund og grund bare, at lade en opgave udføre af andre. Det betyder, at IT-outsourcing som begreb, dækker over et væld af forskellige ydelser.

- ☐ **Business case** *(uddybning side 12)*
  Alle større forandringer i en virksomhed bør besluttes på baggrund af en positiv business case. Beslutning om outsourcing er ingen undtagelse.

- ☐ **Etablering af scope** *(uddybning side 13)*
  Ud over at få business casen på plads er det vigtigste ved outsourcing naturligvis at få fastlagt/etableret scopet.

- ☐ **Outsourcing vs. Offshoring** *(uddybning side 14)*
  Fremfor at outsource kunne offshoring - med egne ressourcer - være et alternativ. Men selvom business casen kan se rigtig fin ud er der dog potentielt mange faldgruber.

- ☐ **Modenhed** *(uddybning side 15)*
  For at opnå den optimale outsourcing/offshoring er det vigtigt at virksomheden har et tilstrækkeligt modenhedsniveau.

- ☐ **Krav til leverandørens infrastruktur** *(uddybning side 16)*
  Design, opbygning og vedligeholdelse af leverandørens infrastruktur er essentiel fx til sikring af adskillelse mellem leverandørens kunder.

- ☐ **Definer SLAer** *(uddybning side 17)*
  Gennem en SLA - Service Level Agreement - stiller virksomheden konkrete, målbare og entydige krav til den leverance, som leverandøren skal yde.

- ☐ **Risikoanalyse** *(uddybning side 18)*
  En sourcing-leverandør er basalt set eksponeret for de samme risici, som en in-house it-funktion. Virksomheden må derfor sikre sig, at disse risici bliver imødegået i henhold til virksomhedens forretningsbehov og risikoappetit.

☐ **Vurdering af regulative og juridiske krav** *(uddybning side 19)*
I forbindelse med outsourcing er der en række juridiske forhold, som man skal tage stilling til, og som bør beskrives i en skriftlig aftale mellem parterne evt. med involvering af juridisk bistand.

☐ **Leverandørvurdering (CSR)** *(uddybning side 21)*
Én af de vigtige milepæle i et outsourcing-projekt er at vælge leverandør. Men hvilken leverandør skal man vælge i et stærkt konkurrencepræget marked, hvor både pris og de tilbudte ydelser stort set er sammenlignelige?

☐ **Aftale om revision/audit** *(uddybning side 22)*
Overvej hvorledes det sikres, at aftalen overholdes eller hvordan virksomhedens revisorer får overbevisning om, at kontrolmiljøet fungerer betryggende hos den outsourcede leverandør. Involver virksomhedens revisorer tidligst muligt

☐ **Fastlæg exit strategi** *(uddybning side 23)*
Overvej hvordan du gennem en exit strategi eller exit plan sikrer virksomhedens data i en situation, hvor du skal forlade din outsourcing leverandør eller hvor samarbejdet på anden måde er ophørt.

☐ **Etablering af kontrakten - til og med underskrivelse** *(uddybning side 24)*
Det er vigtigt at give den forudgående behovsafdækning tilstrækkelig fokus i processen omkring etablering af kontrakten for at sikre et forløb, hvor der er tilstrækkelig klarhed hos parterne om, hvad der skal leveres og dermed hvilke vilkår, der er relevante.

☐ **Etabler organisation** *(uddybning side 25)*
Et outsourcing-projekts success er i høj grad afhængig af, at der etableres den ”rigtige” organisation omkring projektet. Den ”rigtige” organisation er imidlertid ikke nødvendigvis den samme gennem alle projektets faser.

☐ **Roller og ansvar** *(uddybning side 26)*
Den investering der gøres, i at få etableret den tilbageværende organisation, som skal fungere efter outsourcing, kommer mangefold igen, når først outsourcingen kører i normal drift.

☐ **Håndtering af tilbageblivende interne ressourcer/ kompetencer** *(uddybning side 27)*
Navigering af en it-organisation midt i en outsourcing proces kræver stor bevågenhed. Slutmålet for virksomheden er at sikre, at der findes de rigtige kompetencer til forvaltning af de tilbageblivende opgaver.

Samarbejdsfasen

☐ **Løbende kontrol af leverancer – får vi det vi har købt?** *(uddybning side 29)*
Virksomheden bør ved indgåelse af kontrakt fastlægge et passende niveau for kontrol af leverancerne.

☐ **Håndtering af incidents** *(uddybning side 30)*
Når der opstår incidents, er det vigtigt, at de bliver håndteret som aftalt i kontrakt, evt. i den tilhørende SLA - Service Level Agreement.

☐ **Business Continuity** *(uddybning side 32)*
Business Continuity er en disciplin, som med udgangspunkt i en prioritering af forretningsprocesser og -services, skal sikre forretningens videreførelse i tilfælde af alvorlige hændelser eller katastrofe.

☐ **Løbende ændringer – Change Management** *(uddybning side 33)*
Aftaler om outsourcing kan ofte løbe over flere år og i denne periode vil både de forretningsmæssige vilkår og tekniske muligheder formentlig udvikle sig. Derfor er man selvfølgelig nødt til, i en outsourcing kontrakt, at tage højde for, at der vil opstå behov for at lave ændringer undervejs.

☐ **Test af beredskab** *(uddybning side 33)*
Beskrivelse af hvordan test af it-beredskabet er etableret hos outsourcing partneren, og hvordan ansvaret for de enkelte områder er fordelt.

☐ **Sikkerhedstest** *(uddybning side 33)*
Sikkerhedstest kan udgøre en del af egenkontrollen af den outsourcede ydelse, hvorfor mulighed for anvendelse af dette bør inkluderes som en del af kontraktgrundlaget.

☐ **Gennemføre audits / opfølgning på revisionsrapporter** *(uddybning side 34)*
Tilse, at den aftalte erklæring er modtaget og har tilstrækkelig kvalitet til at kunne basere sin ledelses- og revisionsopfølgning herpå.

Afslutning af samarbejde

☐ **Eksekvering af exit strategi** *(uddybning side 36)*
Overvej, hvordan du gennem en exit strategi eller exit plan sikrer virksomhedens data i en situation, hvor du skal forlade din outsourcing leverandør, eller hvor samarbejdet på anden måde er ophørt.

Uddybning af punkter fra tjeklisten

Forberedelse

Hvilken form for outsourcing

It-outsourcing eksisterer i mange varianter, lige fra outsourcing af it-drift, over outsourcing af softwareudvikling, til nutidens cloud computing. Og selvom der vil være nogle fælles træk, vil hver form også have særlige karakteristika - et eget sæt af risici, som man er nødt til at forholde sig til.

Den traditionelle outsourcingform, outsourcing af it-driften, omfatter en række scenarier, som adskiller sig ved ansvarsfordelingen mellem virksomhed og leverandør. Ved fuld outsourcing ligger ejerskab af både datacenter, udstyr, software og driftspersonale hos leverandøren, og ydelsen er - set fra virksomhedens side - en ren service. Men mange andre varianter forekommer, f.eks. drift af virksomhedens egen platform i leverandørens datacenter osv.. Oftest vil der dog med traditionel outsourcing være en direkte sammenhæng mellem den leverede service og det udstyr, som servicen leveres fra, og den pågældende virksomhed. Og virksomhedens data vil kunne lokaliseres til bestemte fysiske enheder.

Cloud computing er et nyere outsourcingbegreb og dækker over services på flere abstraktionsniveauer. Fælles for cloudløsninger er, at det er virtuelle services, og at de oftest understøtter mange kunder på én gang - kun adskilt i det virtuelle lag. Der er således ingen sammenhæng mellem fysisk udstyr og den leverede service, og data kan ikke allokeres til bestemte fysiske enheder.

Uddybende information:

Cloud Security Alliance:
"Security Guidance for Critical Areas of Focus in Cloud Computing v. 3.0"

ENISA:
"Cloud Computing, Benefits, Risks and Recommendations for Information Security"

Business case

Business casen beskriver, som beslutningsgrundlag, de forretningsmæssige fordele et outsourcingprojekt vil medføre. Disse fordele kan både være af økonomisk karakter samt andet - f.eks. kvalitet, agilitet mv.. For at kunne lave en reel sammenligning, kvantificeres alle fordele dog typisk til økonomi. Business casen er som udgangspunkt et "levende" dokument, som bør opdateres, hvis der sker ændringer i de opstillede forudsætninger.

Business casen bør - som hovedregel - indeholde en tids- og aktivitetsplan for projektet, en ressouceplan, en oversigt over projektøkonomien, en strategi for høst af fordele, en plan for organisering af projektet samt en vurdering af relevante risici.

Som grundlag for business casen defineres et præcist scope for projektet. Af hensyn til sammenligningen er det nødvendigt at kende den nuværende tilstand for dette scope i detaljer. Det gælder både de økonomiske forhold (investeringsbehov, driftsomkostninger, personaleomkostninger), de mere kvalitative forhold (SLA'er, tilgængelighed, support mv.) samt sikkerhedsmæssige krav (compliance, fortrolighed, integritet). Denne opgørelse bliver udgangspunktet (base line) for business casen.

Outsourcing-kontrakter indgås normalt for en længere periode. Business casen bør afspejle hele perioden samt medtage evt. forhold ved udtrædelse af kontrakten.

Uddybende information:

ISACA:
"The Business Case Guide: Using Val IT 2.0"

OGC:
"Managing Successful Projects with PRINCE2"

Etablering af scope

I forbindelse med etableringen af scopet er det vigtigt at overveje baggrunden for virksomhedens ønske om at outsource, men her er de typiske bevæggrunde:

- Gør virksomheden i stand til at fokusere på "kerneforrretningen"
- Kan reducere virksomhedens investeringer
- Kan reducere virksomhedens ricisi
- Gør virksomheden mere fleksibel overfor forandringer
- Kan være med til at give virksomheden international erfaring og netværk

Outsourcingen kan altså være en proaktiv stragegisk beslutning om at blive mere lønsom, eller der kan være eksterne omstændigheder - som eksempelvis adgangen til kvalificeret arbejdskraft - der påvirker beslutningen. Under alle omstændigheder skal virksomheden gøre sig det klart, at beslutningen om outsourcing forudsætter ledelsesmæssige ressourcer, og at det kræver en helt anden organisering set i forhold til at holde it-driften, it-supporten eller it-udviklingen inden for egne døre

Derfor bør man ved etableringen af scopet at analysere følgende:

- Hvor meget sparer man i virkeligheden på at outsource?
- Hvad er omkostningen i tid og penge ved at genneføre processen?
- Er lavere it-omkostninger det mest kritiske for virksomheden og dens kunder?
- Hvilke processer kan det bedst betale sig at bevare in-house?
- Er der andre forhold end pris/omkostninger, der reelt har større betydning?

Uddybende information:

Erran Carmel, Paul Tjia:
"Offshoring Information Technology to a Global Workforce"
ISBN: 978-0-521-84355-3

Outsourcing vs. Offshoring

Specielt virksomheder, der i dag har egne produktionsfaciliteter i Østeuropa eller Asien, vil ifm. udfærdigelsen af business casen erfare, at offshoring af it-opgaver (hvor der benyttes egne medarbejdere) rent faktisk vil give en endnu mere positiv business case i forhold til at outsource opgaverne til en ekstern leverandør.

Man skal dog være opmærksom på, at der er et antal risici, som let overses, når business casen laves, men som skal håndteres.

F.eks. opleves det ofte, at kulturforskellen indebærer, at der typisk skal medregnes et langt større ledelsesoverhead, end man er vant til, idet varetagelse af opgaverne kræver kontinuerlig opfølgning. Der må derfor forventes, at der skal investeres både ekstra tid og ressourcer i et sådant samarbejde.

Man skal også være opmærksom på, hvilke sprogegenskaber, der er i det område, man offshorer til. For hvad hjælper det, at arbejdskraften er langt billigere, hvis det er mere eller mindre umuligt at tale med medarbejderne? Her kan det derfor være en fordel at offshore til et område (eks. i eller omkring en storby), hvor der er bedre engelskkundskaber - men omvendt gør dette så også, at timelønnen stiger.

Endeligt er det vigtigt at være opmærksom på, at en offshoring typisk vil kræve, at der er en dansk medarbejder udstationeret i en kortere eller længere periode for at være "fødselshjælper", og afhængigt af familieforhold kan omkostningen til dette blive meget stor, idet der evt. vil skulle betales for international skole til børn, tabt lønindkomst for ægtefælle osv.

Uddybende information:

Erran Carmel, Paul Tjia:
"Offshoring Information Technology to a Global Workforce"
ISBN: 978-0-521-84355-3

DANSKT IT's fagråd for IT & Jura:
" Persondatabeskyttelse er ikke en hindring for offshoring af it"

Modenhed

Mange virksomheder har desværre først for sent fundet ud af, at det kræver et meget højt procesmæssigt modenhedsniveau for at kunne lave en ordentlig outsourcing/offshoring.

Dette bevirker, at de enten helt må droppe projektet, eller i det mindste bliver nødt til at at rekapitulere og få procesmodenheden højnet, før der kan køres videre med projektet. Dette gør jo ikke kun, at projektet bliver forsinket, men også at dette bliver langt dyrere end forventet.

For som nævnt under "Etablering af scope" vil det jo typisk ikke være virksomhedens kernekompetencer der outsources/offshores, men derimod opgaver/områder, hvor man måske har mindre styr på tingene, og hvor procesmodenheden dermed også er lavere.

Dette er naturligvis specielt et problem ved offshoring, hvor man jo reelt blot flytter nuværende arbejdsopgaver til et lavlønsområde. Så her opnår man så bare at få samme "kvalitet" blot til en lavere omkostning.

Ved outsourcing derimod kan et af incitamenterne for at bruge en ekstern leverandør jo netop være at få adgang til kvalificeret arbejdskraft og/eller processer, således at man er fri for at opbygge kompetencerne selv. Stadigt er der dog et behov for, at virksomhedens procesmodenhed er på et tilstrækkeligt niveau, idet det jo ikke hjælper, at de outsourcede arbejdsopgaver kører fuldt ud optimalt hos en ekstern leverandør, hvis de interne processer, der relaterer til disse, ikke også er optimerede/modne.

Uddybende information:

Erran Carmel, Paul Tjia:
"Offshoring Information Technology to a Global Workforce"
ISBN: 978-0-521-84355-3

Krav til leverandørens infrastruktur

Ved outsourcing bliver ens egen infrastruktur en del af en større infrastruktur. Dette betyder en række nye risici af forskellig karakter som f.eks., at en virus i en anden del af leverandørens netværk kan sprede sig til ens eget netværk, eller at ens data kan blive lækket f.eks. ved brug af shared services. Designet af driftleverandørens netværk har derfor betydning for sikkerheden i ens eget netværk.

Krav til infrastrukturen kan groft deles i tre områder:

1. Krav om stærk adskillelse mellem andre kunder og leverandørens eget administrative netværk
2. Krav om mulighed for at overholde egen miljøstrategi og intern segmentering
3. Krav om mulighed for proaktive kontroller i forbindelse med anvendelse af shared services

Ad 1.
Det skal sikres, at leverandørens administrative netværk er tilstrækkeligt sikret og adskilt fra deres kunders netværk. En vigtig komponent er det administrationspunkt (jumphost), som leverandøren anvender til at administrere de forskellige kunders netværk fra. Her bør det være et krav at kun et fåtal af administratorerne har administrativ adgang til selve hosten, og at kunderne selv ikke har adgang.

Ad 2.
Internt skal infrastrukturen understøtte ens egne krav til en miljøstrategi som f.eks., at produktion og ikke-produktion samt internt og eksternt eksponerede områder skal være adskilte. Et andet fokusområde bør være tværgående systemer, som har adgang til alle andre systemer (Antivirus, Backup, etc.). Disse services bør være placeret korrekt i service-in/-out net. Samtidigt bør der være tale om fysisk adskilte systemer, der håndterer hhv. interne og eksternt eksponerede systemer.

Ad 3.
Endeligt bør der være krav om særskilt risk management fokus i forbindelse med leverandørens shared-services. Disse udgør en potentiel kilde til datalækage og virusspredning. Eventuelt fundne svagheder bør håndteres - primært ved implementering af proaktive kontroller. Løsningen på ovenstående kan være at gennemføre egenkontrol på design og implementering af leverandørens kontroller. Dette kan man enten gennemføre selv, eller få en tredjepart til at vurdere. Enten som en del af de generelle revisionserklæringer eller som separate analyser af udvalgte områder.

Definer SLA'er

Sørg for at SLA'en er en del af kontraktgrundlaget, og som leverandøren med sin underskrift har anerkendt som de krav, der stilles til leverancen. Det er svært efterfølgende at komme med leverancekrav i en SLA, når kontrakten er godkendt og underskrevet af parterne. SLA'en kan være udformet som en del af kontrakten eller som et tillæg dertil. Er det sidste tilfældet, skal den være skrevet ind i kontrakten som en del af leverandørens forpligtelser. Konsekvenser ved mislighold af SLA'en skal være dokumenteret enten i kontrakten eller SLA'en.

Der kan sagtens være krav til leverandøren, der er afhængige af ydelser eller opfyldelse af visse betingelser fra virksomhedens side, før leverandøren kan opfylde sine krav. Fx nytter det ikke at stille krav til leverandøren om at alarmere ved incidents, hvis virksomheden ikke har ressourcer, der kan modtage og agere på alarmerne.

I SLA'en kan der stilles alle de konkrete krav til leverandørens ydelse, fx oppetid, planlagt nedetid, sikkerhed, svartider, responsetider ved incidents, alarmering m.m. Det er vigtigt, at man gør sig klart, hvilke krav man som virksomhed har til den ydelse, som man køber. Det fortæller samtidig også om leverandørens modenhed og evne til at levere, hvis han fx ikke vil eller kan levere 99,5 % men kun 94 % oppetid, og kun support mellem kl. 09 - 15, hvis man har brug for 24/7 support.

Det er også her, at man som virksomhed stiller de eventuelle krav til backup og adgang til sine data, som er nødvendige, hvis samarbejdet ophører (som beskrevet i afsnittet Exit strategi).

Sørg for, at kravene i SLA'en er konkrete, entydige og målbare, og regn på, hvad det reelt betyder i tid og omkostninger. Hvad betyder fx 95 % oppetid mod 99,999 % oppetid? Er det inklusive eller eksklusive planlagte service-vinduer? Og hvad er leverandørens pris? 24/7 support er dyrere end 08 - 16 support mandag til fredag. Så her er en cost/benefit analyse tilrådelig, så man ikke betaler for en service, virksomheden reelt ikke har brug for.

Risikoanalyse

Alle virksomheder er udsat for risici, som kan skade deres forretnings lønsomhed eller endda virksomhedens eksistens. Risikoanalyse er en struktureret disciplin, som sætter virksomheden i stand til at vurdere og imødegå disse risici - evt. dele risikoen med andre, f.eks. gennem forsikring - eller på et oplyst grundlag acceptere en risiko.

Virksomhedens overordnede risikoanalyse sætter således rammen for det niveau af risici, som virksomheden er villig til at acceptere. Og det er inden for denne ramme, at forretningsprocesserne skal understøttes med it - hvad enten it håndteres internt eller er outsourcet.

I et outsourcet miljø har virksomheden imidlertid ikke længere direkte kontrol over it-funktionen. Så målet er her at sikre, at sourcing-leverandøren implementerer de nødvendige modforanstaltninger, procedurer og kontroller, som sikrer virksomhedens behov. Og her kommer standarder og "best practices" til hjælp. Certificeringer efter anerkendte standarder, som ISO 20000 og ISO 27001 sandsynliggør, at leverandøren har fornuftige drifts- og sikkerhedsprocesser på plads. Implementering af "best-practice" driftsprocedurer, f.eks. ITIL, giver gennemskuelighed og målbarhed. Og en solid governancemodel, som COBIT, sikrer, at grænsefladerne mellem leverandør og kunde kan fungere effektivt. Endelig vil eksterne assessments, som f.eks. uvildige ISAE 3402 eller SSAE 16 erklæringer og sikkerhedsscanninger sandsynliggøre, at levarandøren lever op til virksomhedens krav.

Men hvis alt dette skal have værdi, er det vigtigt, at virksomheden forstår det miljø, som outsources, til bunds. En risikovurdering skal være gennemført inden outsourcing, data skal være klassificerede og evt. compliance-krav skal være identificerede. Denne "baseline" danner grundlag for kravene til sourcingleverandøren, samt til de kontroller, som skal vise leverandørens performance.

Uddybende information:

IT Governance Institute:
"Control Objectives for Information and Related Technology" (COBIT)

ISACA:
"The Risk IT Framework"

Cloud Security Alliance:
"Security Guidance for Critical Areas of Focus in Cloud Computing v. 3.0"

ENISA:
"Cloud Computing, Benefits, Risks and Recommendations for Information Security"

Vurdering af regulative og juridiske krav

Når en virksomhed outsourcer ydelser, som hidtil har været varetaget af virksomheden selv, kan det give anledning til juridiske problemstillinger, der stort set altid kræver, at man involverer juridisk ekspertise.

Hvis der i forbindelse med outsourcing indgår persondata, skal outsourcingaftalen indeholde en særlig databehandleraftale. Inspiration til formulering af denne kan findes på Datatilsynets hjemmeside. Der gælder særlige regler om godkendelse i Datatilsynet, hvis outsourcing sker til leverandører i lande udenfor EU/EØS. Ved outsourcing til tredjelande kan særlige EU standardkontrakter anvendes.

Den daværende IT- og Telestyrelse har udgivet en vejledning om "Cloud computing og de juridiske rammer", der kan være relevant at læse såfremt cloud computing indgår i løsningen.

Et andet forhold, man skal være opmærksom på, er, at medarbejdere, der har været beskæftiget med de aktiviteter, der nu outsources, kan være beskyttet af regler i lov om virksomhedsoverdragelse og har ret til at følge den outsourcede aktivitet. Kontrakten med outsourcingpartneren bør adressere dette forhold.

Ved outsourcing kan regler i Bogføringsloven og Regnskabsloven endvidere være relevante - herunder reglerne om, hvor materialet skal opbevares, hvis outsourcing partnerens server er beliggende udenfor Danmark.

Når en virksomhed foretager outsourcing, bør der ligeledes tages stilling til, hvordan rettigheder til hardware, software og data skal være i aftalens løbetid samt ved aftaleophør.

For finansielle virksomheder, der outsourcer væsentlige aktivitetsområder, stiller Finanstilsynet særlige krav til aftalens indhold, herunder at Finanstilsynet skal have adgang til leverandørens lokaler mv..

Uddybende information:

www.datatilsynet.dk

www.finanstilsynet.dk

www.itst.dk

Leverandørvurdering (CSR)

I kort perspektiv er prisen næsten altid i fokus. Mange outsourcing-projekter har som et højt prioriteret mål at spare penge - som oftest sandsynliggjort i en økonomisk business case. Et andet vigtigt forhold er den tekniske løsning. Men hvad med den lidt længere horisont?

I dag bliver virksomheder i stigende grad målt på andre parametre end varens pris og kvalitet. Såkaldte bløde værdier som socialt ansvar, bæredygtig produktion, ordentlige arbejdsforhold for medarbejderne m.m. er pludselig også i spil og prioriteret lige så højt. Og disse krav til social ansvarlighed stilles, uanset om virksomheden producerer selv eller benytter sig af underleverandører. Derfor bør man tage nøje udgangspunkt i, hvordan ens virksomhed profilerer sig på CSR-området (Corporate Social Responsibility) og bringe disse værdier i spil over for potentielle underleverandører.

CSR-regnskabet har en stigende betydning i de fleste virksomheder - både for virksomhedens image, men så sandelig også for bundlinjen. Derfor bør principperne i FN's Global Compact være en vigtig del af overvejelserne i business casen og vægtes passende i forbindelse med valget af sourcingleverandør.

Uddybende information:

Udenrigsministeriet og FN:
"Global Compact: Små og mellemstore virksomheder på vej til global ansvarlighed"

ISBN: 978-87-7087-174-7 (trykt)
ISBN: 978-87-7087-175-4 (elektronisk)

(FN-initiativ, der opstiller 10 generelle principper for virksomheders arbejde med samfundsansvar.

Disse er grupperet inden for hovedområderne: menneskerettigheder, arbejdstagerrettigheder, miljø og antikorruption)

Aftale om revision/audit

Ved outsourcing sker en del af virksomhedens aktiviteter uden for virksomhedens umiddelbare egenkontrol. Det er derfor vigtigt at overveje, hvorledes ledelsen sikrer, at kontrolmiljøet i virksomheden, der outsources til, fungerer betryggende. Det kan gøres på flere forskellige måder eller som en kombination af disse, eksempelvis:

1. der føres egenkontrol med outsourcingleverandørens overholdelse af aftalegrundlaget
2. der indhentes en revisionserklæring på, at aftalegrundlaget er overholdt i erklæringsperioden

Kravet omkring kontrolomfang kan være afledt af lovgivning, som det bl.a. kendes fra finansielle virksomheder.

Virksomhedens ledelse bør indgå i en dialog med virksomhedens revisorer så tidligt i forløbet som muligt. Hvis der er tale om væsentlige aktiviteter eller aktiviteter, som kan have regnskabsmæssig påvirkning, skal revisorerne overveje deres revisionsstrategi i forhold til dette, hvilket betyder at de enten skal: foretage revisionen hos leverandøren selv (Dette skal der som udgangspunkt altid være mulighed for i aftalen), eller modtage en erklæring fra et revisionsselskab om aftalegrundlagets overholdelse (Det er vigtigt, at de kontroller som er væsentlige, og som virksomhedens revisorer baserer deres revision på, er medtaget i aftalegrundlaget)

Virksomhedens revisorer vurderer typisk i forhold til deres revision, om de kan benytte erklæringen i deres revision. Herunder om afgiven revision opfattes som uafhængig, har tilstrækkelig faglige kompetencer m. m. Det er en fordel allerede at drøfte revisorvalg i forbindelse med indgåelse af aftalen. De nævnte erklæringer vil typisk være de samme. Således kan brugen koordineres mellem virksomhedens ledelse og revisorerne.

Der findes forskellige typer af erklæringer, men der arbejdes med internationale revisionsstandarder på området, hvilket gør rapporteringen mere gennemsigtig for modtageren og den afgivende part. Vurder sammen med virksomhedens revisorer, hvilken standarderklæring, der skal anvendes.

Der findes flere niveauer for dybden af erklæringen, som skal fastsættes ved aftaleindgåelsen - herunder erklæring om kontrollerne er tilstede og tilstrækkelige (designet korrekt), samt om de er implementeret og fungerer effektivt i hele erklæringsperioden. Typisk vil revisor ønske en revisionserklæring, som dækker test af design, implementering og effektivitet.

Vær opmærksom på, at ordet audit i en kontrakt ofte tolkes som, at det er revisorer, der kan udføre den. Det bør specifikt fremgå, hvis man også selv som it-sikkerhedsafdeling ønsker at kunne udføre audits.

Uddybende information:

Finanstilsynet:
"Bekendtgørelse om outsourcing af væsentlige aktivitetsområder"

ISACA:
"G4 Outsourcing of IS Activities to Other Organisations"

IAA:
"GTAG 7 - Information Technology Outsourcing"

Fastlæg exit strategi

I forbindelse med forberedelserne til outsourcing skal der foretages en risiko- og konsekvensvurdering, der bl.a. vurderer hvor kritiske data er for virksomheden, som nu overlades til outsourcing leverandøren at håndtere, men hvor der er ønske om eller krav til, at virksomheden kontrollerer behandlingen.

Ud fra dette skal det vurderes, om virksomheden kan tåle data tab, og eventuelt hvor meget data tab virksomheden kan acceptere, fx 24 timers data tab, og hvorvidt virksomheden er i stand til at rekonstruere de tabte data ud fra fx input materiale.

Dokumentér i kontrakten, hvem der ejer de data, som leverandøren behandler på vegne af virksomheden, og at leverandøren ved samarbejdets ophør skal være behjælpelig med at udlevere data.

Indgå via kontraktens SLA (Service Level Agreement) en backupaftale med leverandøren, således at virksomheden enten selv kan foretage en regelmæssig online backup eller bede om at få en backup tilsendt med aftalt tidsrum. Husk at få data tilsendt i et format, som gør virksomheden i stand til at genskabe data. Virksomheden bør - alt efter risiko – teste, om system og/eller data kan genskabes ud fra backup'en.

Der bør endvidere udtænkes og - om muligt - efterprøves alternativer til, hvordan man optimalt flytter sine outsourcede aktiviteter til anden leverandør – eller i værste fald insourcer igen.

Etablering af kontrakten - til og med underskrivelse

Kontraktetableringen bør opstartes med en indledende behovsafklaring samt evt. en udbudsproces, hvor der i udbudsmaterialet bør indgå kravspecifikation, konkrete betingelser og tidsplan for selve udbuddet, samt kontraktbetingelser, som outsourcing leverandøren skal forholde sig til. For offentlige udbud gælder særlige regler. Efterfølgende vil leverandøren typisk afgive tilbud med forbehold for udfald af due diligence - særligt vedrørende medarbejderforhold.

Outsourcing har de specielle karakteristika, at der indgås en længerevarende aftale med en leverandør om nogle ydelser, der med stor sandsynlighed ændrer sig over tid, og som er af en sådan karakter, at det ofte vil være svært at overføre aftalen til en anden leverandør med kort varsel. Det betyder blandt andet, at kontrakten skal regulere, hvordan ændringer i ydelsen håndteres governancemæssigt, og hvordan prisstrukturen påvirkes af ændringer i ydelserne samt af ændringer i andre ydre forhold - herunder mulighed for benchmarking.

Selve ydelsen bør beskrives indgående i en SLA med konkret fastsatte mål for f.eks. oppe / nedetid, effektivitet, bod og bonusstruktur, rapporteringskrav og øvrige krav til leverandøren, f.eks. til dokumentation, beredskab mv. Af øvrige forhold, der bør reguleres, kan nævnes garantier, misligholdelse, force

majeure, rettigheder, tavshedspligt, samt punkterne nævnt under ”vurdering af regulative og juridiske krav”. Opsigelse -herunder hjemtagelse eller overførsel af leverancen til tredjemand - bør ligeledes reguleres indgående. Her bør leverandøren forpligtes til at medvirke. Ved overførsel til tredjemand er der en risiko for, at medarbejdere skal medfølge fra leverandøren til tredjemand.

Blandt andet fordi outsourcingaftaler kan være besværlige og ressourcekrævende at opsige, er det vigtigt med en beskrivelse af konfliktløsningsprocessen, som kan eskalere fra involvering af styregrupper, til udpegelse af teknisk sagkyndig, eventuel mægling og voldgiftsbestemmelser.

Etabler organisation

Et outsourcing projekt gennemlever normalt en række faser: En indledende fase, hvor kravene formuleres og leverandøren udvælges, en transitionsfase, hvor services og evt. personale overflyttes, en driftsfase, hvorunder de aftalte services leveres og endelig en exitfase, hvor services tages hjem eller flyttes til en anden leverandør. Disse faser har store forskelligheder, og man bør derfor tage højde herfor, når de enkelte faser organiseres.

Den indledende fase er en projektfase, hvor de forretningsmæssige krav skal omsættes til en leveranceaftale. Det vil typisk kræve deltagelse af forretningsansvarlige med dyb forståelse for it’s be-tydning for forretningen, it-ansvarlige, kontraktspecialister, jurister, samt evt. personalejuridiske kompetencer. Det er vigtigt at kravene til sikkerhed medtages i leveranceaftalen.

Transitionsfasen er ligeledes en projektfase, som skal sikre, at services implementeres i overensstemmelse med det aftalte, samt at evt. personale overflyttes. Der er i denne fase i højere grad brug for projektstyrings- og løsningsorienterede tekniske kompetencer. Her skal det sikres, at sikkerheden opretholdes i en periode med store forandringer.

I selve driftsfasen er der behov for en tæt governance af aftalen. Organisationen må omfatte både forretnings- og tekniske kompetencer samt kontraktspecialister, som kan sikre, at kontraktforholdet udvikles i overensstemmelse med forretningens behov, samt at den aftalte leverance (også på sikkerheds-

området) også rent faktisk leveres.

Sluttelig vil exitfasen være en projektorienteret fase, hvor der er behov for stærkere projektstyrings- og tekniske kompetencer. Her er det primære fokus på servicekontinuitet.

Outsourcing projektets faser er således forskellige, og projektets succes er afhængig af, at organiseringen af disse sker i overensstemmelse med de opgaver, som den enkelte fase skal løse.

Uddybende information:

ISACA - IT Governance Institute:
"Governance of Outsourcing"
ISBN: 1-933284-13-7

ISACA:
"Control Objectives for Information and Related Technology" (COBIT)

Roller og ansvar

Det er vigtigt, at virksomheden selv foretager en analyse af roller, og hvordan ansvaret skal fordeles mellem egen virksomhed og den virksomhed, der outsources til. Transitionsfasen indeholder en række definitioner og afgørelse, og hvis man som virksomhed har en klar opfattelse af de fremtidige roller og ansvar, vil man komme igennem transitionen langt nemmere og med et bedre resultat. Den efterfølgende drift vil også forløbe mere optimalt.

For at kunne definere de fremtidige roller og ansvar er man nød til at beskrive, hvordan det ser ud før outsourcingen. Det vil sige i detaljer beskrive hvilke ydelser, der bliver leveret og i hvilken form. Den beskrivelse er fundamentet for de efterfølgende processer, man skal igennem.

Næste skridt er at gå tilbage til outsourcing strategien og business casen og med det afsæt at udvikle den nye organisation. I den udviklingsproces indgår følgende:

1. Udvælg de relevante processer
2. Definer de nye organisationsfunktioner og størrelse
3. Detaljering af de processer, der skal være tilbage
4. Roller mappes over i funktioner
5. Etablering af RACI skema, hvor der findes sammenhænge mellem ansvar, kommunikation og processer

Nu kan den nye organisation detaljeres og beskrives.

Derefter skal der ske en planlægning af implementering og etablering af en kommunikationsplan. Det skal nøje beskrives, hvilken rolle it-sikkerhed skal have efter en outsourcing. Ansvaret kan som bekendt ikke outsources kun opgaverne – så it-sikkerhed får en central rolle som controller.

Håndtering af tilbageblivende interne ressourcer/ kompetencer

Forandringsledelse er nøgleordet i de processer der findes i outsourcing-opgaven. Der vil naturligt være meget usikkerhed omkring den fremtid, som er ”ukendt” for medarbejdere og i nogen grad for ledelse i it-afdelingen.

Ledelsen har en særlig forpligtigelse til at sikre et højt kommunikationsniveau til medarbejdere. Det, der skal kommunikeres om (helst så åbent som muligt), er f.eks.:

1. Hvorfor outsourcing - hvad er visionen og strategien bag beslutningen
2. Hvordan skal det foregå, hvilke projekt bliver der etableret
3. Hvad sker der undervejs, hvad kan det betyde for dig som medarbejder
4. Hvordan og hvor ofte bliver du som medarbejder fortsat informeret i processen

Når man har fået de første designs af den tilbagværende organisation etableret , er det vigtigt at få skrevet de jobbeskrivelser, der skal være de blivende i den tilbageværende organisation. Disse jobbeskrivelser er et godt grundlag til at få en dialog om, hvilke opgaver der vil være fremover.

Det kan igen føre til overvejelser hos medarbejdere og ledelse om, hvorvidt det er den rette position for den enkelte, om der skal ske et kompetenceløft, eller om man skal flytte med til outsourcingsfirmaet. Der er en forpligtigelse hos virksomheden overfor outsourcingsfirmaet, at der i outsourcingen følger kompetence med til at sikre en fuldstændig dokumentation af overdragelse af systemer/applikationer. Disse forpligtigelser skal også tilgodeses.

I denne planlægning skal risikoen for utilfredse medarbejdere vurderes. Det kan være nødvendigt, at øge overvågning.

Samarbejdsfasen

Løbende kontrol af leverancer - får vi det, vi har købt?

Virksomheden bør ud fra type af leverancer fastlægge hvilket niveau af opfølgning der er nødvendigt.

Virksomheden kan vælge 2 overordnede strategier for opfølgning som tager udgangspunkt i den kontrakt, der er indgået med leverandøren:

1. Kontrakten udgør den overordnede ramme, som i brede termer stiller krav til leverandøren som eksempelvis, at leverandøren skal overholde relevante dele af ISO 27001. Overholdelse af krav dokumenteres som en certificering af leverandøren eller en revisionserklæring om det interne kontrol miljø hos leverandøren.

2. Kontrakten kan være specificeret i de enkelte kontroller, som virksomheden stiller krav til at leverandøren implementerer, eller der kan i kontrakten være stillet krav om, at kontrolrammeværket skal udarbejdes i samarbejde med virksomheden ved påbegyndelse af samarbejdet. Kontrolrammen skal indeholde beskrivelse af den enkelte kontrol, frekvens for gennemførelse samt aftalt rapportering af samme.

Håndtering af incidents

I SLA'en bør det være konkretiseret, hvad man som virksomhed forstår ved en incident, og hvorledes man prioriterer og klassificerer incidents - lige fra uvæsentlige incidents til kritiske/uacceptable incidents.

For hver enkelt kategori af incidents skal det være aftalt i SLA'en hvem hos leverandøren, der kontakter hvem hos virksomhed, og herunder hvor hurtigt, at det skal ske. Der skal altså være en opdateret og aktuel alarmeringsliste med krav til alarmeringstider, når det er besluttet, at der skal alarmeres. I nogle tilfælde kan en mail som advisering være nok, hvis der er tale om et uvæsentligt incident, blot det er aftalt.

I SLA'en bør det ligeledes fremgå, hvor lang tid leverandøren har til at få løst et incident, herunder om den skal eskaleres til Problem Management (ITIL). Der kan være aftalt bod i tilfælde af, at en incident ikke håndteres hurtigt nok. Ligesom der kan være tale om så kritiske incidents, at det er væsentlig kontraktmisligeholdelse.

Hvis der foreligger aftale om periodiske rapporter og/eller statusmøder, skal incidenthåndteringen behandles som fast punkt i rapporten eller på mødets dagsorden.

Business Continuity

Business continuity - eller forretningsberedskab - har til formål at sikre videreførelsen af forretningskritiske processer eller services, såfremt der indtræffer en alvorlig hændelse, som helt eller delvist påvirker den måde disse normalt udføres på. Et eksempel på en sådan hændelse er et it-nedbrud, der påvirker it-understøttelsen af de kritiske forretningsprocesser i en sådan grad, at disse må udføres på manuel eller anden vis.

En mulig proces for at få udarbejdet forretningsberedskabet er:

1. Analysér og fastlæg de kritiske forretningsprocesser
2. Fastlæg overordnet beredskabsstrategi
3. Etablér selve det praktiske forretnings¬beredskab
4. Test beredskabet.

I del 1 gennemføres en såkaldt Business Impact Assesment (BIA), der har til formål at afdække de mest forretningskritiske processer og services. På baggrund af denne afdækning udvælges en eller flere strategier for hvordan disse processer kan videreføres i tilfælde af alvorlige hændelser eller katastrofer. I denne forbindelse bør målsætningen for forretningsvidereførelsen fastlægges. Det gælder bl.a. en beslutning om, hvor hurtigt en genoptagelse af driften skal ske (Recovery Time Objective (RTO)).

Disse strategier bør dække over:

1. Sikring af personale med tilstrækkelig viden
2. Anvendelse af mulige alternative lokationer
3. Teknik/teknologi strategi
4. Tilstrækkelig adgang til informationer/data
5. Alternative leverandør/leverance muligheder

Alt efter de strategiske valg som træffes, vil det efterfølgende være muligt at udarbejde en plan, der sikrer, at forretningens krav til maksimal tålelig nedetid kan honoreres.

At it leverancen outsources ændrer ikke på nødvendigheden af at gennemføre ovenstående. BIA'en vil endvidere være en central øvelse i forbindelse med designet af de services, der skal købes fra leverandøren, da denne afdækker kritikaliteten af de enkelte services Nogle af de føromtalte strategier vil dog allerede være givet på forhånd, da disse vil være inkluderet i de ydelser, der købes af leverandøren. Test, auditering og leverandørdokumentation bliver derfor endnu mere kritisk, da ydelserne udgør en essentiel del af understøttelsen af forretningsberedskabet (Se mere om test af beredskab senere).

Uddybende information:

British Standard:
"BS 25999"

Business Continuity Institute:
"Good Practice Guidelines"

Løbende ændringer – Change Management

Behovet for ændringer kan falde enten inden for den indgåede outsourcing aftales område, eller udenfor.

Når det gælder ændringer, som ligger inden for aftalens område, f.eks. en udvidelse af kapaciteten eller lignende på eksisterende services, bør den governancestruktur, som er implementeret i forbindelse med aftalen, kunne varetage dette. Disse ændringsønsker kan dog have stor betydning for det samlede engagement og udløse betydelige ekstraomkostninger. Her kan det være en stor fordel, at basere ændringsprocessen på standarder og "best practice", f.eks. ISO 20000 / ITIL. På denne måde sikres det, at både virksomhed og leverandør har samme opfattelse af processen og at ændringsønsker får den rette ledelsesmæssige bevågenhed. Ændringer i sikkerhedsmæssige forhold bør også kunne håndteres via governance strukturen.

Ændringsønsker, som falder uden for aftalens område, er i praksis opstart på et nyt outsourcingprojekt. Derfor bør sådanne ændringer være genstand for en tilsvarende grundig forretningsmæssig vurdering, både mht. løsningsmodel, business case osv.. Ligeledes bør den pågældende leverandør vurderes kritisk i forhold til den nye opgave, så det optimale udkomme af investeringen sikres.

Styring af ændringer er en vigtig disciplin og den organisatoriske ramme herfor bør aftales i en outsourcingkontrakt. Anvendelse af standarder og "best practices" hjælper med til at definere processen og give en fælles forståelse og terminologi, som igen sikrer en glidende drift. Ændringer, som ligger helt uden for aftalens scope, bør imidlertid håndteres særskilt.

Uddybende information:

Dansk Standard:
"DS/ISO/IEC 20000"

OGC:
"ITIL®"

Test af beredskab

Det skal sikres, at beredskabsaftalen lever op til de (overordnede) krav, som fremgår af it-sikkerhedspolitikken. Med udgangspunkt i beslutningen om Recovery Time Objective skal der designes en metode for test af, om leverandøren i samarbejde med virksomheden er i stand til at leve op til beredskabsaftalen. Følgende elementer skal medtages i aftalen:

1. Hvad, der skal testes (fx forsyning, netværk, backup, servere etc.)
2. Hvordan, det skal testes (fx "skrivebordstest", reetableringstest, test af kontakt til relevante personer etc.)
3. Hvilke scenarier der skal testes (ex. katastrofe test, delvis udfald osv.)
4. Testfrekvensen af de enkelte områder (På de områder, der skal testes, skal det angives hvor ofte, det skal testes - ex ½ årlig, helårlig, hvert andet år etc.)
5. Dokumentation af beredskabstestene - herunder form, vurdering og sammenligning med de mål, der er specificeret i outsourcing aftalen
6. Ansvarsplacering.
   - Hvem har ansvaret for at testene bliver udført?
   - Hvem har opgaven med at udføre dem?
   - Hvem dokumenterer?
   - Hvem formidler resultaterne og hvordan?
7. Afholdelse af beredskabsmøder, formidling af testresultater og forbedringstiltag.

Sikkerhedstest

Sikkerhedstest har til formål at teste sikkerhedsniveauet i de af outsourcing-leverandøren leverede ydelser. Alt efter karakteren af de leverede ydelser bør det overvejes, hvordan sikkerhedstest kan anvendes til at vurdere, om leverandøren lever op til de krav, som er aftalt i kontrakten, eller som må anses at være best practice på området.

Hvis den aftalte ydelse f.eks. vedrører applikationsudvikling, så bør der stilles krav om, at der løbende gennemføres sikkerhedstest, der illustrerer, om det udviklede har et tilstrækkeligt sikkerhedsniveau til at kunne blive sat i produktion på det aftalte tidspunkt.

På tilsvarende vis kan sikkerhedstest også anvendes til at kontrollere sikkerhedsniveauet i en outsourcet infrastruktur. Eksterne sikkerhedstests kan anvendes til at teste, hvor sikker et eksternt perimeter er sat op, mens interne sikkerhedstest kan anvendes til at vurdere, hvor god leverandørens baseline for opsætning af sikkerhedsparametre er generelt. Disse to typer af sikkerhedstest giver en idé om, hvor sandsynligt de nuværende kontroller kan omgås og dermed hvilke eventuelle andre kompenserende kontroller, der bør opstilles.

Såfremt sikkerhedstest ønskes anvendt til enten at afdække svagheder i applikationer eller infrastruktur, så er det essentielt, at de overordnede spilleregler for dette aftales i forbindelse med kontraktsindgåelse. Disse spilleregler bør indeholde: hvor, hvordan og hvornår der skal gennemføres sikkerhedstest, hvem der har ansvaret for at initiere disse, hvem der skal udføre dem, samt hvordan varsling af sikkerheds-test skal foregå, og hvem der bærer omkostningerne.

Endeligt skal det også klart aftales, hvordan eventuelle fund fra sikkerhedstesten skal håndteres, herunder hvem der bærer byrden med at udbedre de fundne svagheder samt maksimal tidshorisont for dette.

Gennemføre audits / Opfølgning på revisionsrapporter

Hvis revisionen har valgt at udføre revisionen selv hos leverandøren, sker revisionen af virksomheden som en helhed og behandles ikke yderligere her.

Hvis det er valgt at modtage revisionserklæring kan ledelsen og revisionen i samarbejde gennemgå rapporten for at se om:

- den er afgivet af uafhængig og kompetent revisor (Der findes særlige revisionsstandarder, som sikrer at revisionserklæringen kan bruges og hvordan)
- omfanget er tilstrækkeligt og i henhold til aftale
- konklusionen vedr. kontrolmiljøet er betryggende
- hvorledes eventuelle svagheder hos den outsourcerede virksomhed er afdækket ved kompenserende kontroller, eller om der skal udføres yderligere revision for at afdække svaghederne, som er rapporteret

Revisionen vil lade erklæringen indgå i deres samlede revisionsstrategi og arbejde for afgivelse af erklæring på årsrapporten.

Afslutning af samarbejde

Eksekvering af exit strategi

Outsorcing aftaler er tidsbegrænsede. Ved aftale udløb eller ved misligeholdelse kan virksomheden eller leverandøren vælge at opsige samarbejdet. Det er vigtigt, at man som virksomhed snarest får sikret sine data. Forhåbentlig har man i kontrakten forpligtiget leverandøren til at være behjælpelig med at få data ud, herunder kan der foreligge en aftale om, hvorledes det skal ske (fx via dvd eller online) og i hvilket format. Det skal være muligt for virksomheden at kunne genskabe eller overføre data til en ny leverandør eller til sit eget system.

Det er vigtigt, at sikre sig gennem kontrakten, at leverandøren sletter alle virksomhedens data, når de er sendt retur til virksomheden, og der ikke længere er kontraktmæssig begrundelse for, at data er til stede hos leverandøren. Dette er specielt vigtigt, hvis der er behandlet persondata.

Hvis leverandøren er gået konkurs, og kurator har lukket for adgang til leverandørens systemer, kan der være risiko for, at virksomheden ikke kan komme til sine data og få en kopi ud samt efterfølgende får slettet data på leverandørens systemer. Derfor er det vigtigt, at man som virksomhed periodisk får lavet en brugbar backup/sikkerhedskopi. Perioden mellem backup/sikkerhedskopier afhænger af, hvor kritiske de pågældende data er for virksomheden, og hvor stort et data tab man kan tåle.

Lessons Learned / Common Pitfalls

Et af de fællestræk, der gør sig gældende blandt mange medlemmer af forfatterkredsen, handler om ressourceforbrug internt i virksomheden for at få samarbejde og relationer opbygget og funktionsdygtigt. Flere har ligeledes oplevet, at deres egen procesmodenhed er blevet udfordret i forbindelse med outsourcingen, hvilket har betydet, at der har været flere ikke forventede udfordringer i forløbet med outsourcingen.

Nedenfor er konkrete udfordringer oplevet i virksomhederne:

- Det er alfa og omega at forretningen er informeret/oplyst om hvad de kan forvente af leverancer i forbindelse med outsourcingen. Et af vores mål var større fleksibilitet men der gik en rum tid, før det var virkelighed men, forretningen havde en forventning om dette fra dag ét.

- Leverandøren havde stor ekspertise indenfor IT Security, men først for sent gik det op for os, at denne ekspertise blev solgt som en rådgivningsservice - det var ikke en del af leverancen fra driftscentret.

- Samarbejdet med leverandøren stiller store krav til vores procesmodenhed - både på de processer, der outsources, men også tilbageværende processer såsom ledelse og opfølgning. Vi underestimerede de ressourcer, vi skulle bruge internt for at få samarbejdet til at fungere.

- Det ultimative håndtag i samarbejdet er eskalering - men det gør sjældent et problem mindre. Tværtimod har vi oplevet, at samarbejdet får nogle ridser, som er svære senere at udviske.

- Vi har oplevet kulturforskelle virksomhederne imellem som en stor udfordring - og det er ikke mindre i forbindelse med konflikter.

- Vi har oplevet udfordringer med bl.a. terminologi; hvad betyder ”Working Day” eller ”Severity”?

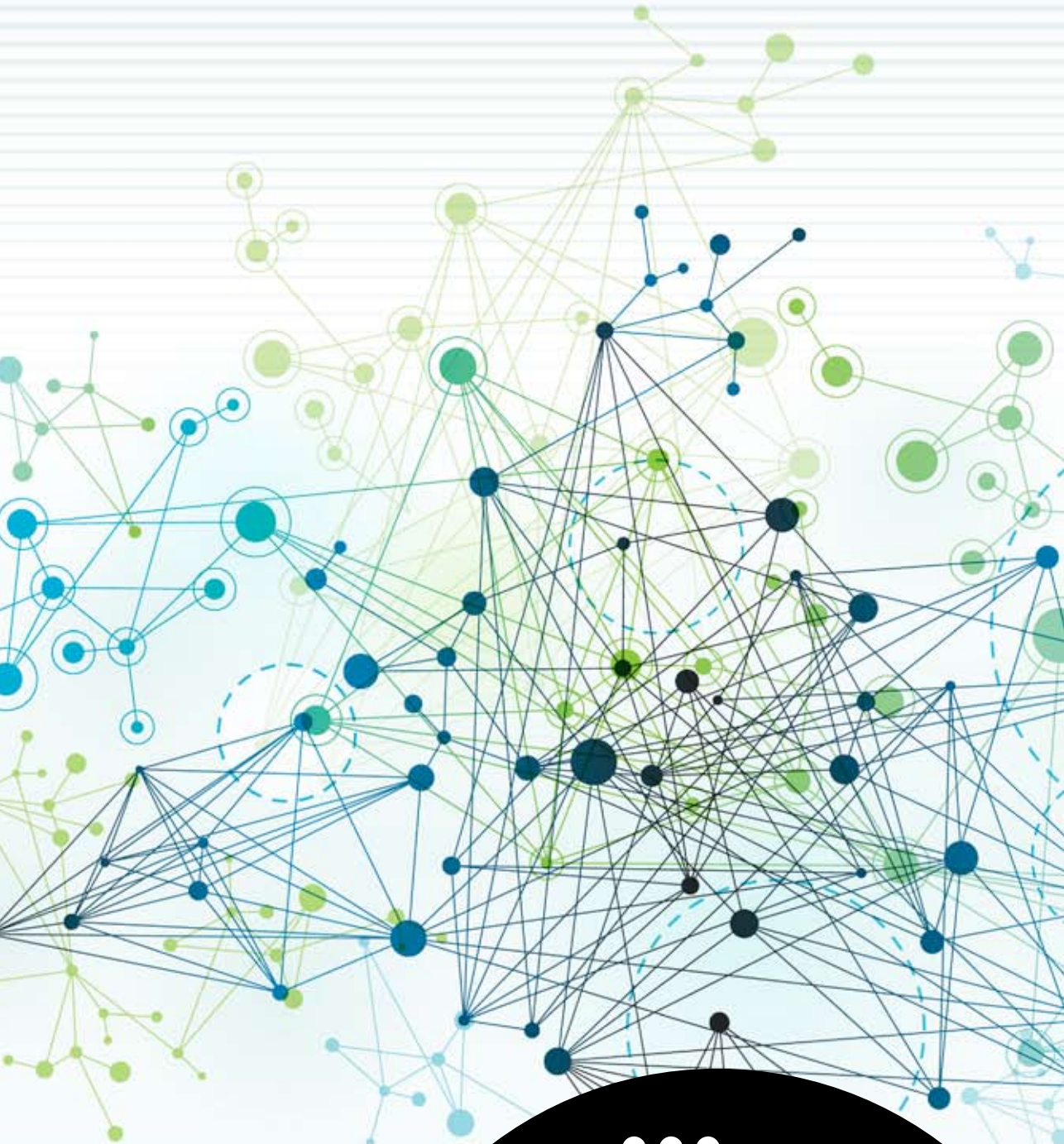
- Man skal ikke underestimere udfordringerne ved videnoverførsel til den nye virksomhed - oven i købet måske et andet land. Vi har lært, at det er vigtigt at have klare KPI’er på læring, vidensniveau og brug af

nye vs. rutinerede medarbejdere - og at KPI'erne bør understøttes af præmiering ved gode resultater.

- Man skal være meget omhyggelig med at få aftalt og formuleret retten til at foretage kontrol af efterlevelsen af aftalte sikkerhedskrav - herunder hvad og hvordan (fysiske eftersyn mv.). Det skal være aftalt, hvorledes evt. afvigelser fundet af revisor eller it-sikkerhedsafdelingen skal rettes, og hvem der skal betale.

- Man kan opleve, at den manglende viden, som leverandøren har om virksomheden i forhold til virksomhedens egne medarbejdere, kan medføre længere eller fejlbehæftede leverancer

- Leverandørens medarbejdere vil ofte være mere specialiserede end virksomhedens egne medarbejdere. Deres generelle kendskab til hele miljøet kan være mindre og have betydning for leverancen.



dansk·it

Bredgade 25 A I DK 1260 København K
Tlf: +45 3311 1560 I dit@dit.dk I www.dit.dk