VEILEDNING FOR OUTSOURCING AV IT

SPESIELT RETTET MOT SMÅ OG MELLOMSTORE BEDRIFTER

SEPTEMBER 2010

INNHOLD

SAMMENDRAG

Sammendrag
Outsourcing av IT innebærer å sette ut én eller flere IT-funksjoner eller IT-tjenester til eksterne leverandører. Det er viktig å ha orden og oversikt i egen virksomhet og gjennomføre nødvendig planleggings- og forberedelsesarbeid som et ledd i en outsourcingsprosess. Vær oppmerksom på at outsourcing ikke endrer det ansvar virksomhetsledelsen har for å følge lover og forskrifter.

Ha orden i egen virksomhet

Gjør en begrenset forundersøkelse og skaff deg oversikt over status og framtidige behov som virksomheten har. Hold beslutningen om outsourcing av IT åpen til forundersøkelsen er ferdig. Sørg for god forankring både hos ansatte og ledelse. Hva vil du oppnå med outsourcing? Har du fokus mot kostnads- eller mulighetssiden, eller kanskje begge? Hvilke forretningsprosesser og informasjon er kritiske for din virksomhet?

Vurder spesielt om noen av dine IT-tjenester er kritisk for kjernekompetansen i din virksomhet. Vurder også hvor sårbar virksomheten er hvis kritisk informasjon blir kjent for uvedkommende. Hva er styrke og svakheter i dine nå værende IT-tjenester? Bruk sjekklistene i veiledningen og lag en foreløpig beskrivelse av dine krav, et kravdokument.

Hvordan finner du riktig leverandør?

Det er mange måter å gjennomføre anskaffelser på. Er din virksomhet en del av offentlig sektor eller petroleumsvirksomhet, så foreligger det omfattende krav om hvordan anskaffelsesprosesser skal gjennomføres.

For de virksomheter som ikke er underlagt spesielle innkjøpsreglement anbefales en prekvalifisering Finn 3- 5 mulige leverandører og vurder anbudsprosess eller kjøp etter forhandlinger.

For mange små- og mellomstore virksomheter (SMB) vil det å gå i tett dialog med 2–3 leverandører gi bedre resultater enn anbudsprosess. Du vil da også hindre at detaljerte spesifikasjoner og ferdig definerte løsninger fra din side fører til at leverandørene skrur opp prisen for å ta høyde for risiko

Velger du en slik framgangsmåte er det nå du trenger kravdokumentet fra forundersøkelsen. En dialog

Bruk sjekklisten i veiledningen og sørg for at din virksomhet styrer unna fallgruvene i oppstartsfasen.

med flere leverandører vil gi deg en mulighet til å lære mest mulig om innholdet i leverandørenes standard-leveranser for de IT-tjenestene du ønsker å outsource. Leverandørene får anledning til å sette seg inn i dine forretningsbehov og krav. Du får mulighet til å utfordre leverandørene for å gi din virksomhet nye muligheter og lavere IT-kostnader.

Bruk anledningen sammen med leverandørene til også å se på hva som kan gå galt – vurdering av risiko. Drøft med leverandørene de verst tenkelige scenariene, se spesielt på områder som driftsstans og gjenoppretting, sikkerhetskopiering og beskyttelse av virksomhetskritisk informasjon.

Basert på denne dialogen med flere leverandører, oppdater dine krav, bruk sjekklisten i veiledningen og fokuser på det som er relevant for deg.

Hvordan få en god og balansert avtale?

Basert på samtaler med flere leverandører bør du nå kunne velge ut 1 eller 2 leverandører for avtale-forhandlinger. Det er viktig å finne leverandører som forstår dine behov og din forretning. Sett av nok tid til kontraktsarbeidet. Bruk en av standardkontraktene på markedet, evt. en bransjeavtale.

En viktig del av avtalen skal sikre deg som kunde mot uforutsette hendelser. Avtalen må sikre prosesser for det som er uforutsett og for endringer som blir nødvendige. Arbeid med de verst tenkelige scenerier og vurder behovet for å avtale rett til erstatning. Hvor mye av din omsetning taper du hvis datasystemene er ute av drift i en dag eller lengre?

Bruk sjekklisten fra veiledning og sørg for at avtalen som et minimum dekker:

- Beskrivelse av tjenestene i en servicehåndbok med avtalte servicenivåer.

- Beskrivelse av alle tre faser i et oursourcingsoppdrag:
  - Oppstartsfasen og overføring til ny leverandør: planlegging, testing og overføring av IT-tjenester, evt. infrastruktur, personell og programvare til leverandøren, testing og godkjenning
  - Driftsfasen med detaljerte krav for de løpende-tjenesteleveransene samt mekanismer for styring av endringer og forbedringer samt evaluering av leveransene i form av revisjoner og/ eller

Avtalen må sikre prosesser for det som er uforutsett og for endringer som blir nødvendige.

kundetilfredshets målinger
- Avslutning av avtalen, retningslinjer for hva som skjer om en av partene vil ut av avtalen.

Oppstartsfasen og overføring til outsourcingsleverandør

Outsourcing innebærer ofte endringer av IT-systemer, arbeidsprosesser og rapporteringsrutiner. Det er viktig å sørge for at rutiner for support og brukerhjelp er klare og at brukerne får nødvendig opplæring.

Hva kan gå galt i oppstartsfasen? Det er spesielt tre områder som er gjengangere:

- Informasjon og kommunikasjon til ansatte og mellom kunde og leverandør
- Teknologi og teknisk kontroll
- Motivasjon og opplæring av brukere

Bruk sjekklisten i veiledningen og sørg for at din virksomhet styrer unna fallgruvene i oppstartsfasen.

Hvordan følger virksomheten opp avtalen?

Det finnes flere rammeverk for styring og oppfølging av driftstjenester. Hvis outsourcingsleverandøren benytter et slikt rammeverk, avklar med leverandør hvilke prosesser som din virksomhet bør involveres i.

Sørg for å ha fokus på forhold som er viktige for din virksomhet, og spesielt for at disse områdene følges opp:

- Utpek kontaktpersoner og avklar tydelige roller i egen virksomhet og hos leverandøren
- Behold noe IT-kompetanse i egen virksomhet, om mulig
- Sørg for et endringsregime med klare plikter for kunde og leverandør – få leverandøren til å logge endringer
- Sørg for at større endringer risikovurderes av leverandør og at tiltak for å redusere risiko skal framlegges
- Sørg for å etablere standarder for hvordan kvaliteten på tjenestene og servicenivå (SLA) skal måles
- Sørg for dialog om virksomhetskritiske IT-tjenester gjennom driftsmøter minst hver måned

1. OM DENNE VEILEDNINGEN

Outsourcing av IT omfatter hel eller delvis tjenesteutsetting av IT-tjenester og /eller IT-drift til eksterne leverandører. Målgruppen for veiledningen er små- og mellomstore virksomheter (SMB). Veiledningen kan også være til nytte for større virksomheter, selv om vi ikke kan gå god for at alle spørsmål som er relevante for større virksomheter er grundig nok behandlet.

Mange virksomheter ønsker å redusere kostnader og effektivisere arbeidsprosesser. Samtidig øker kravet til tilgjengelighet og oppetid for IT-systemer og IT- infrastruktur. For noen kan outsourcing av IT-tjenester være et ledd i å redusere kostnadene eller øke effektiviteten. Denne veiledningen inneholder sjekklister og vurderingspunkter som skal bidra til å rettlede din virksomhet gjennom outsourcingsprosessen og forbedre din mulighet til å lykkes med prosessen, uansett hensikt.

Uttrykket Cloud Computing blir nevnt i mange IT-sammenhenger, men hva er egentlig dette, og hvordan kan en leder i en norsk virksomhet forholde seg til utviklingen av nye leveranseformer for IT?

Veiledningen dekker ikke alle de spesielle vurderinger som må gjøres av virksomheter som er underlagt helsepersonelloven, helseregisterloven eller lov om forebyggende sikkerhet (sikkerhetsloven) uansett størrelse på virksomheten. Veiledningen dekker heller ikke alle krav for virksomheter som er underlagt Finanstilsynets IKT-forskrift.

Veiledningen vil likevel kunne brukes av virksomhetene nevnt ovenfor. Det er da nødvendig å gjøre særskilte vurderinger i tillegg for de krav som følger av lover og forskrifter som den enkelte virksomhet er underlagt.

1.1 IT er virksomhetskritisk

IT er virksomhetskritisk i de fleste virksomheter i dag. SMB-er har begrenset IT-kompetanse og mange har ikke dedikerte IT-ansatte. Det er likevel viktig å ha orden og oversikt i egen virksomhet og gjennomføre nødvendig planleggings- og forberedelsesarbeid som et ledd i en outsourcingsprosess. Det kan i verste fall føre til svært dårlige avtaler dersom dette ikke tas vare på.

1.2 Outsourcing av IT endrer ikke virksomhetens ansvar

Outsourcing av IT-drift endrer ikke det ansvaret som leder i den enkelte virksomhet har i henhold til lover og forskrifter. Ansvar kan ikke delegeres eller avtales bort, kun arbeidsoppgaver. Dette gjelder f. eks. ved elektronisk behandling av personopplysninger. Ifølge personopplysningsloven med forskrifter så er det virksomhetens leder som er ansvarlig selv om det er en ekstern leverandør som gjør databehandlingen. Kravene er spesielt omfattende for virksomheter som behandler sensitive personopplysninger. Det er imidlertid fullt mulig å planlegge for at outsourcingsleverandøren i forbindelse med avtaleforhandlinger påtar seg å gjennomføre grunnlagsarbeidet for en del av de pliktene som virksomhetens ledelse har.

1.3 Outsourcing av IT gir forsterket behovet verdivurdering og beskyttelse

Det må vurderes hvilken informasjon og forretningsprosesser som er kritisk for virksomheten og som derfor må beskyttes. Det kan være forhold knyttet til produkter, produksjon, kunderegister, sikkerhetstiltak, herunder fysiske sikringstiltak, osv. Virksomheten må sørge for at kritisk informasjon og kunnskap ikke tilfeldig kan ødelegges eller blir tilgjengelig for uvedkommende. Virksomheter som ikke allerede har gjennomført en verdivurdering bør gjøre det. For mer informasjon om verdivurdering,

NSM: www.nsm.stat.no/Arbeidsomrader/Verdivurdering

2. HVA ER IT-OUTSOURCING

IT-outsourcing innebærer å sette ut en eller flere IT-funksjoner og/eller tjenester i en virksomhet til en eller flere eksterne leverandører isteden for å drive disse selv. Leverandørene kan være selskaper i nærmiljøet, nasjonale aktører, eller leverandører som leverer disse tjenestene fra land utenfor Norge, eller kombinasjoner av dette. Utstyr og systemer kan være plassert hos kunden, hos leverandør, eller en kombinasjon av dette.

2.1 Rimelige forventninger til outsourcing av IT-tjenester?

Det er gjort noen undersøkelser blant norske virksomheter som sier noe om hvilke forventninger virksomhetene har. Handelshøyskolen BI har gjennomført en outsourcingsundersøkelse i 2007 og 2009. BI-undersøkelsen har hentet data fra virksomheter med omsetning større enn 500 mill NOK, og resultatene er derfor ikke direkte overførbare på SMB-er. De viktigste forventningene er:

- Kostnadsreduksjoner
- Bedre tilgang til IT-ressurser og IT-kompetanse,
- Større fleksibilitet og skalérbarhet i forhold til behovene i egen virksomhet
- Forbedret kvalitet på IT-tjenester og brukerhjelp
- Mulighet for større fokus mot egen kjernekompetanse

Det påpekes som en viktig grunn til IT-outsourcing at virksomhetene vil fokusere på det de er best til, kjernekompetansen. BI-undersøkelsen fra 2009 viser at fokuset på kostnadsreduksjoner er økt i forhold til 2007. I 2007-undersøkelsen var forventet besparelse i gjennomsnitt for alle funksjoner ca 21 %, mens oppnådd besparelse var ca 18 %. For områdene helpdesk/brukerstøtte og IT-systemer og infrastruktur ligger oppnådd besparelse på mellom 15 % og 17 %.

Mange virksomheter tar ikke med i regnestykket at det kommer til kostnader ved outsourcing som kommer til fradrag fra disse besparelsene. Dette gjelder både kontraktskostnader og kostnader for å følge opp at leverandøren faktisk leverer etter avtalen (forvaltningskostnader) samt styring av framtidige endringer.

Siden de erfarte kostnadsbesparelser i mange tilfeller ikke er større enn 15 %, er det god grunn til å se på også andre forbedringsområder enn kostnadsbes-

parelser når IT-outsourcing vurderes, f. eks mulighetene for endringer og effektivisering i egen virksomhet gjennom tilgang til nye teknologimuligheter, bedre IT-tilgjengelighet, bedre brukerhjelp og mer standardiserte løsninger.

2.2 Hva kan gå galt ved IT outsourcing?

BI-undersøkelsen har kartlagt kundenes oppfatning av trusler og risiko ved outsourcing av IT. Høringsinstansene har også bidratt med synspunkter på hva som kan gå galt ved outsourcing. De viktigste risikoområder som er pekt på er:

- Utilstrekkelig kvalitet på IT-tjenestene
- Mangelfull kontrakt og uklare ansvarsforhold mellom partene
- Mangelfullt samarbeid og samhandling mellom kunde og leverandør, f. eks. vedrørende endringer, teknologistyring, rapportering og kontroll
- At kundens virksomhet mister kompetanse, og:
  - reduserer evnen til å kunne vurdere kvalitet på leveransen
  - reduserer evnen til styring og kontroll med IT-virksomheten, f. eks. leverandørens sikkerhetsregime og sikkerhetsdokumentasjon
  - Mangel på kompetanse hos kunden fører til at lover og regler ikke følges, f. eks. personopplysningsloven
  - Utfordringer med tilkobling av IT-drift som kunden selv fortsatt har ansvar for

Erfaringer fra mange virksomheter tilsier at mangler innenfor områdene samhandling kunde – leverandør, samt mangelfull kontrakt, er nok til å hindre en vellykket outsourcing av IT-tjenester.

Det påpekes som en viktig grunn til IT-outsourcing at virksomhetene vil fokusere på det de er best til, kjernekompetansen.

3. HVORDAN VELGE RIKTIG STRATEGI?

Å velge strategi for outsourcing av IT handler i første omgang om valg av leveransemodell – og det er flere leveransemodeller å velge blant.

Virksomheten kan få alle tjenester levert fra én leverandør, eller fra flere (multisourcing). IT-leverandøren kan fjerndrifte serverne som fortsatt er plassert i dine lokaler (onsite outsourcing), eller du kan leie serverkapasitet og evt. systemer hos leverandøren (hosting). Det vil forenkle prosessen videre hvis du velger leveranseform i forkant av vurdering av mulige leverandører.

3.1 Onsite outsourcing

Onsite outsourcing innebærer at leverandøren fjerndrifter dine systemer og infrastruktur som fortsatt er plassert i dine lokaler. Det finnes ulike alternativer når det gjelder kontinuitet, beredskap og backup. Det kan være aktuelt at mulig katastrofedrift legges på leverandørens infrastruktur og systemer. Den viktigste fordelen med denne modellen er enkel integrasjon med de outsourcede IT-tjenester og tjenester som fortsatt skal gjennomføres i egen bedrift, f. eks. systemer som er knyttet til bedriftens kjernekompetanse innenfor produksjon, analyse, problemløsning, etc. Gjennomføringsrisikoen vil trolig bli noe mindre enn for andre alternativer fordi det er mindre omfattende endringer som skal gjennomføres

3.2 Application Service Provider

Bruk av Application Service Provider (ASP) betyr at du som kunde leier tilgang til programvaren din virksomhet har behov for, systemer, lisenser, server/lagringskapasitet og backup og recovery løsninger. Tilgang til tjenestene får du via leid linje, over internett, eller evt. via mobiltelefon.

Fordeler for din virksomhet er at du ikke har investeringer i lisenser, oppgraderinger, servere etc. og får forutsigbare faste kostnader pr. bruker pr. mnd. I tillegg får du backup/restore håndtert utenfor dine lokaler – noe som er verdifullt i tilfelle f. eks. brann i egne lokaler. Typiske løsninger som tilbys er Microsoft kontorstøtte, e-post med sikkerhetsløsninger for virusvask og håndtering av søppelpost, felles fillagring, økonomisystemer, etc.

De viktigste fordelene med denne løsningen er små investeringer i forkant og god skalérbarhet. Bygger du opp eller ned din virksomhet, så følger IT-kostnadene med. I tillegg får din virksomhet ofte tilgang til løsninger for mobile arbeidstakere som hadde vært kostnadskrevende å bygge opp selv. Har din virksomhet mange ansatte som bare sporadisk bruker IT, kan dette være en god modell.

ASP løsningen har flere risikoområder.
Hvis tilkoblingen til ASP-leverandøren faller bort grunnet linjebrudd, etc, og du ikke har reservelinje, så står din virksomhet uten de fleste IT-tjenester, kanskje for en dag eller to til linjebruddet er ordnet. I tillegg vil du kunne få utfordringer med integrasjon mellom ASP-tjenestene og IT-tjenester som fortsatt skal kjøres i egen regi, f. eks systemer som er knyttet til bedriftens kjernekompetanse innenfor produksjon, analyse, problemløsning. Hvis din virksomhet er avhengig av mange slike systemer som støtter kjernekompetanse i din virksomhet, er neppe en 100 % ASP-løsning et godt valg.

3.3 Cloud computing

Cloud Computing er en betegnelse for IT-tjenester levert over internett. Dette leveres oftest med dataprosessering og datalagring på servere som står i store, eksterne serverparker tilknyttet internett og hvor du kan leie tilgang til systemapplikasjoner og øvrige IT-tjenester.

Cloud Computing leveres "on demand" – når du trenger dem. Slike tjenester er elastiske og skalérbare – du får så mye eller så lite du trenger målt etter flere kriterier enn bare pr mnd eller pr bruker. Målet

med Cloud Computing å tilby enkle, sikre, skalérbare IT-tjenester til kundene. Det eneste brukerne trenger lokalt er en nettleser på arbeidsstasjonen, enten det er en PC, en Mac eller andre typer enheter.

Fordelene med Cloud Computing er at driften er svært standardisert, gjøres på svært store serverparker, ofte plassert utenfor Norge. Dette gir mulighet for stordriftsfordeler og store reduksjoner i driftskostnader. På kjøpet kan din virksomhet få høy tilgjengelighet, backup/restore utenfor egne lokaler og tilgang til en profesjonell og sikker drift/kompetanse. Cloud Computing kan gjøre det økonomisk mulig å tilby bedrifts e-post og intranett til ansatte som ikke bruker PC til daglig, også for virksomheter med mange ansatte.

Cloud Computing vil også gjøre det mulig å tilby nettbaserte IT-tjenester over hele verden til en svært lav kostnad. De fleste av oss bruker Cloud Computing allerede i dag i det minste i privat sammenheng til e-post, til internett, telefoni, sosiale medier, etc.

Risikoområder ved Cloud Computing er som for ASP-løsningen – virksomheten blir svært avhengig av tilkoblingen til Internett. Hvis tilkoblingen faller bort grunnet linjebrudd, etc, og du ikke har reservelinje, så står din virksomhet uten de fleste IT-tjenester, kanskje for en dag eller to til linjebruddet er ordnet. Som for ASP kan du ha utfordringer med integrasjon mellom Cloud-tjenestene og IT-systemer du velgere å kjøre lokalt i eget hus, f. eks. systemer tilknyttet produksjonen. I tillegg vil du kunne miste en del valgfrihet i forhold til hvilke versjoner av programvare du skal bruke, når du skal oppgradere etc.

I tillegg kommer det forhold at med nettleser mot Internett som eneste brukergrensesnitt må virksomheten forholde seg til at nettleserprogramvare er utsatt for stadige forsøk på infeksjoner fra Internett. Denne risikoen bør håndteres i avtaler med outsourcingsleverandør slik at nødvendig sikkerhet for din virksomhet blir ivaretatt.

Dersom de eksterne serverparkene står utenfor Norge vil din virksomhet i tillegg måtte passe på at kontrakten reguleres av norsk lov og følger norske krav til personvern. Du må være sikker på at persondata kan overføres til og lagres i det landet som serverparken liggere. Det er mange og komplekse regler knyttet til overføring av personopplysninger ut av Norge. Sørg for at outsourcingsleverandøren

De viktigste fordelene med denne løsningen er små investeringer i forkant og god skalérbarhet. Bygger du opp eller ned din virksomhet, så følger IT-kostnadene med.

tar ansvaret for tilfredsstillende rutiner, prosedyrer og teknologi slik at det er mulig for kunden å følge Personopplysningsloven. Sørg for at outsourcingsleverandøren dokumenterer for deg hvordan dette sikres. Hvis din virksomhet lagrer sensitive personopplysninger så søk råd hos Datatilsynet før du beslutter strategi for outsourcing.

3.4 Offshoring

Offshoring kalles det når IT-tjenester leveres fra leverandører i andre land. Dette er ofte en del av Cloud Computing-konseptet og det henvises til fordeler og risiko presentert under Cloud Computing.

For offshoring tilkommer det ytterligere risikomomenter:

- Svikt i kritisk infrastruktur/strømforsyning i vertslandet - ikke bare i internettilknytningen kan gi redusert tilgjengelighet
- Ustabilitet i regimer (avhengig av land) og andre reguleringsregimer
- Kulturforskjeller og språkutfordringer
- Egen kompetanse innen internasjonal kontraktsrett og IT er ofte mangelfull i små bedrifter. Har virksomheten bestillerkompetanse til å sikre egne rettigheter?

For SMB-er anbefales det, dersom offshoring skulle være aktuelt, å inngå avtale gjennom en leverandør som har kontor i Norge og sørge for at avtalen forholder seg til norsk lov.

3.5 Kjenn din leverandør

Vit hvor dataene dine er. Velg en leverandør som oppgir hvor i verden dine data lagres/sikkerhetskopieres, slik at du som kunde evt. kan få dem slettet eller overført hvis kundeforholdet opphører. Ved en Cloud Computing leveranseform er det spesielt viktig å sørge for at avtalen har tydelige bestemmelser om avvikling og tilbakeføring av datagrunnlag til din virksomhet når avtalen avvikles.

Vit hvem som kan få tilgang til dataene dine. Virksomheten bør vite hvem som kan få tilgang til dataene dine, særlig når det gjelder informasjon som har stor verdi for virksomheten, samt sensitive personopplysninger.

Er din virksomhet underlagt krav om å følge standarder innenfor informasjonssikkerhet? Dette omfatter standarder ditt selskap er underlagt gjennom egne beslutninger, krav til børsnoterte selskap, bransjekrav etc. Som eksempel kan nevnes SOX, PCI, SAS70, ISO 27001 og Finanstilsynets IKT-forskrift, bare for å nevne noen. Sørg for at outsourcingsleverandøren dokumenterer for deg i avtalen hvordan oppfyllelse av kravene sikres. Få alle krav inn i avtalen og avtal rett til test av sikkerhet og årlige revisjonserklæringer fra uavhengig tredjepart i forhold til oppfyllelse av standardene. Sørg for at dette er en del av de avtalte leveransene.

Et viktig område å regulere i avtalen er kontraktsfestede rettigheter til kundens egenutviklede programvare. Hvis dette ikke er i orden kan du oppleve at outsourcingspartner videreutvikler programvaren i selskaper utenfor Norge og bruker den til egne formål, evt. selger lisensrettigheter til andre kunder.
Vær spesielt nøye med kontraktskrav og servicenivå for tjenestene siden det ofte er vanskelig og arbeidskrevende å følge opp rettslig overfor selskaper, evt. deres underleverandører i utlandet. Sørg for sanksjoner hvis det er mulig.

4. HA OVERSIKT I EGEN VIRKSOMHET – GJØR EN FORUNDERSØKELSE

Outsourcing av IT-tjenester vil kunne innebære en krevende endringsprosess til en ny IT-hverdag. Denne endringen krever forberedelse og god planlegging. Som ved alle endringer bør den enkelte virksomhet gjøre en grundig vurdering av hvorfor virksomheten skal endre IT-leveransene og hva organisasjonen vil oppnå med dette.

Men arbeidet er ikke over når avtalen er undertegnet. Outsourcing er en kontinuerlig prosess. Det er viktig å følge opp at avtalt servicenivå leveres, samt styre leveransen og gjennomføre nødvendige endringer. Det er også nødvendig å forberede en eventuell avvikling av avtalen og overgang til en ny leverandør eller egen drift av hele eller deler av de IT-tjenestene som avtalen dekker. Det er viktig at bedriftssensitiv informasjon ikke gjøres tilgjengelig for uvedkommende. Gjør en nøye vurdering av hvordan slik informasjon og kunnskap kan beskyttes og hvem som skal ha tilgang til den (verdivurdering).

For å kunne gjøre riktige valg på alle disse områdene er det behov for å skaffe seg oversikt i egen virksomhet, samt vurdering av framtidige forretningsbehov, dvs. gjøre en begrenset forundersøkelse. Det er også behov for å utarbeide en begrenset spesifikasjon basert på det du vet etter denne forundersøkelsen, og prioritere dine egne krav i absolutte krav, viktige krav og ønskelig. Denne begrensede forundersøkelsen bør være godt forankret både hos ledelse og ansatte, slik at en evt. outsourcing av IT-tjenester blir forstått og akseptert.

Alle alternativ bør stå åpne til du er ferdig med denne forundersøkelsen, også det alternativet å beslutte at outsourcing ikke er det beste alternativet, evt. ikke aktuelt for enkelte IT-tjenester.

4.1 Ha orden i egen virksomhet - stikkord for sjekkliste

- Før du overlater driften av IT-miljøet til en outsourcingspartner, vær sikker på hva som foregår i din egen IT-avdeling
- Skaff deg oversikt over hva slags bedriftssensitiv informasjon du behandler og lagrer og hvor kritisk den er for virksomheten om uvedkommende får tilgang
- Behandler du personopplysninger så dokumentér dette – husk å vurdere risiko i henhold til Personopplysningsforskriften
- Skaff deg oversikt over utstyr, systemer og graden av viktighet for virksomheten

Outsourcing er en kontinuerlig prosess. Det er viktig å følge opp at avtalt servicenivå leveres, samt styre leveransen og gjennomføre nødvendige endringer.

- Kartlegg styrker og svakheter i dagens IT-tjenester f. eks. (tilgjengelighet, kvalitet, sikkerhetsrisiko vedrørende f. eks. informasjonslekkasjer, informasjonsspionasje, osv)
- Dekker dagens IT-tjenester forretningens behov på kort og lengre sikt?
- Kartlegg egne rutiner, systemer, infrastruktur
- Finnes ikke skriftlige rutinebeskrivelser er dét noe som må på plass
- Problemer må spesielt kartlegges – mange har brent seg på å outsource en intern IT-tjeneste som man ikke har kontroll over
- Skaff deg oversikt over skjulte IT-kostnader slik at de faktiske kostnadene fremkommer
- Skaff deg også oversikt over IT-behandling som gjennomføres av miljøer utenfor IT- avdelingen og evt. krav til integrasjon med IT-avdelingens systemer
- Har du omfattende IT-systemer som støtter kjernekompetanse for forretningen, så vurder spesielt nøye hvor forretningskritisk dette er og hva slags kompetanse som kreves i din virksomhet.
- Skaff deg oversikt over egenutviklet programvare og om denne programvaren er en kritisk faktor i forretningens kjernekompetanse
- Skaff deg oversikt over kostnadsbildet for dine IT-tjenester, har du ikke oversikt, vil det kunne være vanskelig å vurdere kostnadene i en outsourcing-savtale

4.2 Hva er kritisk informasjon for virksomheten?

- Skaff deg oversikt over informasjon om virksomhetens produkter, produksjon, kunderegister, sikkerhetstiltak, herunder fysiske sikringstiltak osv.
- Hvordan kan denne informasjonen misbrukes?
- Hvem kan misbruke denne informasjonen?
- Hva vil være konsekvensen om denne informasjonen blir kjent?

4.3 Hva vil din virksomhet oppnå med outsourcing?

Stikkord for sjekkliste:

- Lavere kostnader
- Høyere kvalitet
- Forbedret oppetid
- Tilgang til ressurser og høyt kvalifisert arbeidskraft, nye tjenester og evt. bruk av ny teknologi
- Bedre sikkerhet i form av økt tilgjengelighet, bedre katastrofeløsninger, bedre sikkerhet mot trusler fra internett
- Andre forretningsforhold som er viktige i din virksomhet

NB! Pass på forankring i ledelsen.

4.4 Framtidige forretningsbehov – stikkord for sjekkliste

- Vurdér virksomhetens behov for fleksibilitet og skalérbarhet i forhold til mulig vekst eller nedskjæringer - forretningsbehov om 5 år, endret forretningsdrift?
- Har du mobile medarbeidere som er mye på farten?
- Trenger du IT-støtte bare til hovedkontoret, eller har du virksomhet andre steder i Norge eller utlandet?
- Kan ny teknologi og kommunikasjonsløsninger gjøre noe for forretningen?
- Hva med oppetid 24/7 – kan det endre grunnlaget for din virksomhet?
- Vurdér bruk av mer standardiserte løsninger, systemer og evt. ny teknologi. Det kan være mye å spare i IT-drift ved outsourcing hvis du kan bruke standard løsninger.

4.5 Omfanget av outsourcing – en sjekkliste

Hvilke IT-tjenester skal settes ut? Det er vanlig å dele opp IT-tjenestene i noen hovedområder:

- Outsourcing av infrastruktur og drift
- Outsourcing av drift/forvaltning av applikasjoner/systemer
- Outsourcing av forretningsprosesser (f. eks lønn, regnskap)
- Outsourcing av IT-ledelsesfunksjonen, ofte også inkludert styring av framtidig teknologiutvikling

4.6 Hvordan velge riktig omfang og retning?

Hva du skal velge avhenger av mange forhold:

- Hvilke behov din virksomhet har nå og på lengre sikt
- Hvilken IT-kompetanse din virksomhet har, og hvordan dette evt. bør endres
- Behovet for kompetanse og rådgivning fra outsourcingsleverandør
- Hvor skal driften gjennomføres, i dine lokaler eller hos outsourcingsleverandør
- Hva med printere, kopimaskiner, mobiltelefoner og annet bærbart utstyr?
- Må ansatte skifte jobb eller miste den?
- Hvordan vil du sørge for å sitte igjen med tilstrekkelig kompetanse til oppfølging av outsourcing-savtalen, leveranser og sikkerhet?
- Omfang av egen IT-kompetanse: Kan det være aktuelt å kjøpe en IT-ledelsesfunksjon på deltid?
- Hva vil konsekvensen av outsourcing være mht bemanning, kompetanse og sårbarhet?

Vurdér spesielt om noen av dine IT-tjenester støtter kjernekompetansen. Har din virksomhet systemer eller teknologi som er et nødvendig forretningsfortrinn, f. eks. i form av egenutviklet programvare, IT-systemer eller IT-tjenester som krever omfattende inngripen fra fagspesialister i din virksomhet? Erfaring fra mange virkelige outsourcingstilfeller viser at outsourcing av slike systemer og tjenester sjelden blir vellykket.

Vurdere nøye hvor sårbar virksomheten er hvis forretningskritisk informasjon blir kjent for uvedkommende.

Det er også viktig å vurdere IT-kompetansen i egen organisasjon og virksomhetens strategi for å videreutvikle eller endre denne. Hvis din strategi er å ha minst mulig egen IT-kompetanse, vil det være viktig å vurdere outsourcingsleverandører som er geografisk plassert i nærmiljøet, slik at det er enkelt å hente kompetanse. Dette er spesielt viktig hvis du også planlegger å outsource IT- ledelses funksjonen til outsourcingsleverandør.

Blir ansatte berørt av outsourcingsprosessen så sørg for å følge lovverk og inngåtte avtaler. Involvér de ansatte og deres tillitsvalgte tidlig nok.

5. HVORDAN ARBEIDE MED LEVERANDØRVALG OG REFERANSER

Å outsource IT-tjenester er for mange virksomheter en svært omfattende beslutning. En outsourcing-savtale for IT-tjenester innebærer ofte betydelige kostnader både ved inngåelse og evt. ved avslutning. Langsiktighet er derfor viktig og din virksomhet bør i utgangspunktet planlegge for en periode på 3 – 5 år. Det er derfor en langsiktig samarbeidspartner din virksomhet nå skal lete etter.

Det er mange måter å gjennomføre anskaffelser på. Er din virksomhet en del av offentlig sektor eller petroleumsvirksomhet, så foreligger det omfattende krav om hvordan anskaffelsesprosesser skal gjennomføres. Det henvises der til offentlige innkjøpsreglement samt veiledninger fra Direktoratet for forvaltning og IKT (Difi):
http://www.anskaffelser.no/tema/2009/10/ikt-anskaffelser

5.1 Prekvalifisering – 3 til 5 mulige leverandører

Hvordan finne ut hvilke leverandører som kan være aktuelle? Ta kontakt med ASP Norge eller IKT-Norge for oversikter, http://www.aspnorge.no/, http://www.ikt-norge.no/. Ta kontakt med et bredt utvalg av mulige leverandører og beskriv kort hva din virksomhet ønsker å gjennomføre. Basert på forundersøkelsen vet du nå mye om styrke og svakheter i dine nåværende IT-tjenester, du vet en del om langsiktige forretningsbehov og viktige prioriteringer. Be om referanser fra tilsvarende kunder.

Svarene du får er en god indikator på hvor attraktiv du er som kunde. Du bør sørge for å snakke med flest mulig referanser som likner mest mulig på din egen virksomhet og med tilsvarende IT-systemer og infrastruktur.

5.2 Anbudsprosess eller forberedende samtaler med flere leverandører?

For store og mellomstore virksomheter er anbudsrunde ofte neste skritt. Her gjelder det å beskrive så tydelig som mulig hva jobben går ut på. Sett opp kriterier som gjør det mulig å sammenlikne tilbud. Kravene til f. eks offentlige anbudsprosesser gjennomgås ikke i denne veiledningen, det henvises til **http://www.difi.no/anskaffelser**

5.3 Forberedende samtaler med flere leverandører

En tradisjonell anbudsprosess er ikke alltid den beste løsningen. For mange SMB-er vil det å gå i en tett dialog med 2 – 3 leverandører gi bedre resultater. Du vil da også hindre at detaljerte spesifikasjoner og ferdig definerte løsninger fra din side fører til at leverandørene skrur opp prisen for å ta høyde for risiko. Bruk denne prosessen til å bygge opp personer i din virksomhet for å kunne ivareta styring og kontroll av IT-tjenestene etter at de er satt ut til ekstern leverandør. Etabler allerede nå god kommunikasjon med leverandørene og faste kontaktpunkter i din organisasjon.

Velger du en slik framgangsmåte er det nå du trenger kravdokumentet fra forundersøkelsen. En dialog med flere leverandører vil gi deg en mulighet til å lære mest mulig om innholdet i leverandørenes standardleveranser for de IT-tjenestene du ønsker å outsource. Leverandørene får anledning til å sette seg inn i dine forretningsbehov. Du får mulighet til å utfordre leverandørene på bruk av ny teknologi og standardiserte IT-tjenester for å gi din virksomhet nye muligheter og lavere IT-kostnader. Du får også en mulighet til å drøfte hvordan leverandøren vil samarbeide med din virksomhet, servicenivå, kontaktpunkter og ansvarsdeling.

Bruk anledningen sammen med leverandørene til også å se på hva som kan gå galt – de verst tenkelige scenarioene, se spesielt på driftsstans og beskyttelse av virksomhetskritisk informasjon.

Basert på samtaler med flere leverandører bør du nå kunne velge ut én eller to leverandører for avtaleforhandlinger. Sørg for at valg av leverandører harmonerer med dine langsiktige målsetninger. Hvis din virksomhet har en nasjonal eller nordisk ambisjon, bør du sørge for at leverandøren har en mulighet for å være med å støtte deg videre.

5.4 Oppdater dine krav

Basert på forundersøkelsen og dialogen med flere leverandører bør det nå være mulig å oppdatere ditt kravdokument, og ta inn mer detaljerte krav til servicenivå og responstider, oppetider, brukerhjelptjenester, osv.

Bruk sjekklisten nedenfor og plukk det som er relevant for deg:

- Ditt kravdokument må være en presis og nøyaktig beskrivelse slik at tilbyder skal kunne gi et riktigst mulig tilbud, og slippe å ta seg unødig betalt for risiko vedrørende arbeidsomfang.
- Krav til brukerhjelp.
- Krav til opplæring av nyansatte.
- Krav til regelmessig opplæring av ansatte.
- Hvordan arbeidsdeling skal være når det gjelder styring og kontroll av endringer, IT-sikkerhet, teknologioppdateringer og krav til beredskap, backup og dokumentasjon
- Hvordan lovkrav skal håndteres, f. eks personopplysningsloven med forskrifter
- Presiser hva som skal leveres og la leverandøren få muligheten til å si hvordan.
- Kravspesifikasjonen må inneholde elementer av katastrofeberedskap. Hva skal skje når det f. eks. brenner i din virksomhet eller hos leverandøren?
- Krav til katastrofe og beredskapsløsninger:
  - Hvor lenge kan din virksomhet være uten systemer/informasjon?
  - For hvor lang periode kan din virksomhet akseptere å tape data?
  - Hva er leverandørens standard sikkerhetsløsninger?
- Ønsket kontraktstid og muligheter for utvidelser må fremgå.
- Fleksibilitet fra leverandøren må være et krav når forretningsbehovet endrer seg. Avtalen må ikke være et statisk dokument i avtaleperioden.
- Vurder krav til servicenivå.
- Aktuelle og til dels overlappende mål for servicenivå kan være:
  - Oppetider for eksempelvis brukerhjelp
  - Tilgjengelighet for tjenester for hele eller deler av døgnet.
  - Svartider for brukerhjelp og systemer
  - Leveringstid fra f. eks. brukerhjelp, tid det tar å få en løsning, en endring etc.
  - Feilutbedringstid
  - Kundetilfredshet
  - Evt. sanksjoner hvis minimum servicenivå ikke holdes.
- Be leverandør beskrive hvordan denne vil måle servicenivået på leverte tjenester, og hvordan og hvor ofte dette skal rapporteres.
- Be gjerne tilbydere om pris på alternative servicenivåer for å kunne drøfte dette nærmere.
- Eventuelle krav og vilkår for at leverandør skal overta ansvar for bedriftens personale etter en eventuell kontraktsinngåelse må være nøye presisert.
- Hvilken type kontrakt som skal brukes eller om virksomheten ønsker å bruke standardkontrakt.
- Det må gå klart frem på hvilket grunnlag tilbud velges ut og forkastes, hvilken rett til begrunnelse tilbydere skal ha ved forkasting m.v.
- Ved outsourcing/drifting av lisenser som eies av andre, må alle rettigheter og plikter være klart definert.
- Det samme gjelder for programvare utviklet av din virksomhet
- Det må kreves at leverandøren har inkludert i avtalen avslutning av leveransen med påfølgende tilbakelevering eller overlevering til annen leverandør. Pris for dette må etterspørres.

6. AVTALE OM OUTSOURCING – HVA BØR DEN INNEHOLDE

Sett av nok tid til kontraktsarbeidet. Bruk en av standardkontraktene på markedet. Det foreligger tre utgivere av standardkontrakter for outsourcing: Difi som utgir Statens standardkontrakter, IKT-Norges standardkontrakter og Dataforeningens standardkontrakt. Hvis det foreligger bransjeavtaler som er utarbeidet for din bransje kan det også være et godt utgangspunkt. Uansett valg av avtale, pass på at bestemmelser i bilagene går foran standard avtaletekst.

Dataforeningens avtaler: http://www.dataforeningen.no/it-kontrakter.134108.no.html

IKT-Norges avtaler: http://www.ikt-norge.no/STANDARD-AVTALER/Standardavtaler/

Statens standardavtaler: http://www.difi.no/emne/anskaffelser/statens-standardavtaler-ssa

Av disse avtalene er det bare Difis avtaler som kan benyttes uten avgifter til utgiverne.

Datatilsynet har utarbeidet en egen veileder for hva som må med i en avtale med en outsourcingsleverandør som behandler personopplysninger på vegne av deg som kunde.

Nærmere informasjon om dette, se http://www.datatilsynet.no/templates/article____2742.aspx

Outsourcingsleverandøren blir en viktig partner for din virksomhet. Det er derfor viktig å finne en leverandør som forstår dine behov og din forretning, og som er fleksibel når endringene kommer. Mange konflikter mellom kunde og leverandør skyldes upresise formuleringer om mulige kommende endringer. Det er i utgangspunktet innebygde interessekonflikter mellom kunde og leverandør i en outsourcingsavtale. Kunden ønsker fleksibilitet og å kunne endre IT-tjenestene og avtalen når forholdene endrer seg. Leverandøren ønsker stabilitet for å kunne tjene inn investeringen i oppstartsperioden.

Avtalen må ta høyde for å håndtere framtidige endringer i forretningsbehov, vekst og ekspansjon samt det motsatte. Hvordan skal prisøkninger beregnes på IT-leveransen hvis antall ansatte øker med 50 % i løpet av avtaleperioden eller evt. det motsatte?

En viktig del av avtalen skal sikre deg som kunde mot uforutsette hendelser. Avtalen må sikre prosesser for det som er uforutsett og for endringer som blir nødvendige. Når man skrivere en avtale tror man at man har sett alt, om et par år ser man trolig annerledes på det. Arbeid med de verst tenkelige scenarier og vurder behovet for å avtale rett til erstatning. Hvor mye av din omsetning taper du hvis IT-systemene er ute av drift en dag eller lengre?

Mangel på oversikt over dagens leveranser fra egen IT-avdeling er en risiko i alle outsourcingsavtaler. For å redusere risikoen for deg som kunde, vurder å ta med en bestemmelse om at outsourcingsleverandøren skal erstatte alle de tjenester du selv i dag leverer ved egen intern IT-avdeling. Da får leverandøren et incentiv til nøye å kartlegge interne tjenester som du leverer fra egen IT avdeling.

Sørg for at du har mulighet til i løpet av avtaleperioden å ta ut i det minste et fåtall systemer/funksjoner/tjenester fra avtalen og utføre disse selv eller ved hjelp av tredjepart.

Avtalen må som et minimum inneholde:

- Beskrivelse av tjenestene i en servicehåndbok
  - Løsningene/systemene kan være både kundens og leverandørens eiendom
  - Brukerstøtte og andre tjenester som er en

naturlig del av slike driftstjenester
  - Håndtering av endringer
  - Håndtering av sikkerhet og risiko
- Beskrivelse av alle tre faser i et oursourcingsoppdrag
  - Oppstartsfasen og overgang til ny leverandør, planlegging, testing og over føring av IT-tjenester, evt. infrastruktur, personell og programvare til leverandøren, testing og godkjenning
  - Driftsfasen med detaljerte krav for de løpende tjenesteleveransene samt mekanis mer for styring av endringer og forbedringer samt evaluering av leveransene i form av revisjoner og/ eller kundetilfredshets målinger
  - Avslutning av avtalen, retningslinjer for hva som skjer om en av partene vil ut av avtalen.

6.1 Sjekkliste for avtaleinnhold

Nedenfor finnes en sjekkliste for en del forhold en bør være spesielt oppmerksom på. Listen er ikke komplett og representerer ikke en innholdsfortegnelse. Se spesielt på områder som er viktig for din virksomhet.

- Sørg for at alle tjenester er beskrevet i en service-håndbok
- Planlegging, organisering og gjennomføring av igangsetting/etablering,
- Ansvar og ansvarsbegrensning
  - Hvilken myndighet har leverandør til å ta beslutninger på vegne av kunden
  - Krav til skriftlighet
  - Bestemmelser ved oppkjøp/fusjoner av leverandørens eller kundens virksomhet
- Krav til standarder eller kvalitetssystem som leverandøren skal følge samt dokumentasjon av hvordan dette følges
  – også for underleverandører
- At avtalen tilfredsstiler kravene til databehandler i henhold til veileder fra Datatilsynet - nødvendig dersom leverandør behandler IT-baserte person-opplysninger på vegne av kunde
- Tiltak som følge av personopplysningsloven med forskrift - nødvendig punkt hvis leverandøren behandler personopplysninger på kundens vegne
- Krav til at leverandøren følger anerkjente standarder for informasjonssikkerhet
  - Det bør inngå en beskrivelse av leveran-dørens sikkerhetsregime
  - Risikovurdering – metoder og tidspunkter
  - Rutiner for sikkerhetsoppdatering av programvare for å håndtere f. eks sårbarheter
  - Sikkerhetsløsninger for å beskytte tjenester, servere og brukerutstyr mot Internett kriminalitet og andre risikofaktorer
  - Kontroll med tilgangsstyring og adgangs kontroll til systemer og informasjon
- Eventuelle overføringer av informasjon over landegrenser, spesielt personopplysninger
- Håndtering av endringer
  - Vurdering av forespurte endringer
  - Bestemmelser om versjonsoppgradering – hvem bestemmer når?
  - Varslingstid fra leverandør før endringer gjennomføres
  - Risikovurdering av endringer
  - Godkjenning av endringer
- Avslutning av avtalen
  - Eiendomsrett ved regulær og irregulær avslutning, f. eks. kundens eiendomsrett til egenutviklet programvare, beholde arbeidsbeskrivelser og prosedyrer som er blitt innarbeidet i organisasjonen m.m.
  - Kunden vil normalt ha behov for lengre varslingstid enn leverandøren.
  - Leverandørens plikt til å bistå ved flytting til eventuell annen leverandør eller tilbake til kunden
- Avtalens varighet og evt. opsjoner på forlengelse

- Konflikter, mislighold og mangler
  - Lovvalg og konfliktløsning
  - Definisjon av begrepet mislighold f. eks forsinkelser og avvik fra kravspesifikasjon
  - "Force majeure"
  - Konsekvenser ved ulike grader av avvik. Hva skal til for at avtalen skal opphøre? Gir sanksjoner reell kompensasjon? Hvem dekker ekstrakostnader og følgeskader?
- Ansatte, overtallige og vilkår for ansettelse i leverandørens selskap
- Konfidensialitet og krav om taushetsplikt
- Felles utvikling av programvare. Skal begge parter tjene på dette? Eiendomsrett?
- Konsulenttjenester (priser og kvantumsrabatter).
- Brukerservice/Helpdesk inkludert? Åpningstid for denne.
- Opplæring av nyansatte og vedvarende opplæring av fast ansatte.
- Hvordan følges kravene til informasjonssikkerhet opp
- Backup. Katastrofeløsninger, reetablering og testplaner.
  - Definere katastrofe og når katastrofeberedskap iverksettes
  - Leverandørens beskrivelse av gjenoppretting sstrategi og tidsrom til normal drift etter katastrofe
  - Leverandørens beskrivelse av nøddrift og servicenivå ved nøddrift
  - Hvor mye informasjon kan gå tapt
  - Testplaner og tidspunkter for test
  - Rutiner for sikkerhetskopiering (backup)
- Varslingsrutiner ved unntakssituasjoner og sikkerhetshendelser
  - Avtal med leverandøren hvordan avvik og sikkerhetshendelser defineres.
  - Avtal med leverandøren hvordan slike hendelser håndteres og rapporteres til virksomheten.
  - Avtal forebyggende tiltak for å motvirke avvik og sikkerhetshendelser.
  - Se forøvrig NorSIS' veiledning om sikkerhetshendelser
- Kommunikasjon til tredjepart eks. BBS, banker.
- Servicekatalog med beskrivelse av tjenestene. Pass på at du får beskrevet informasjonssikkerhet som en tjeneste
- En serviceleveranseavtale (SLA) må være en del av kontrakten og skal beskrive alle tjenester som overføres med tilhørende servicenivå, det være seg faktisk eller ønsket forbedring. Det må av-

tales regler for hvordan servicenivået endres etter overføring og hvordan det måles og rapporteres til kunde.

- Måleprosedyrer servicenivåer.
  - Avtal automatiske målinger av drifts-stabilitet, oppetider og svartider, for systemer og help desk
  - Avtal månedlige eller kvartalsvise rapporte-ringer av servicenivå for alle tjenester,
- Leverandørens avtaler med tredjepart/underlev-erandører
- Det er viktig å ha klart definerte regler for hvilke deler av kontrakten som har prioritet eller for-rang - det enkleste vil være å gi bilagene forrang framfor avtaleteksten.
- Avtalen bør også regulere prisforhold og tilgang på variable tjenester slik at leverandøren leverer tilleggstjenester til gunstige priser og innenfor gitte tidsrammer.
- Vurder om det er mulig å gjennomføre et pilot-prosjekt for å teste leverandørens faktiske evne til å gjennomføre arbeidet.
- Man må definere etableringskostnader og vilkår, samt avslutningskostnader dersom en evt. pilo-tinstallasjon ikke er vellykket.
- Det må etableres godkjennings- og akseptkriteri-er, som skal oppfylles i godkjenningsperioden.
- Endelig avtale må være inngått før selve imple-menteringsprosjektet starter, gjerne med be-stemmelser om justering etter en 1. driftsfase.
- Leveransesikring og kontroll av leveransen
  - Ved behov, inkluder i avtalen rett til innsyn i leverandørens IT-drift for å ivareta lover/ regler og forskrifter som din virksomhet måtte være underlagt
  - Vurder f. eks halvårlige kontroller med ad gangskontroll til systemer og tilgang til informasjon
  - Mål nivået på sikring, gjennom f. eks gjennomgang av tilganger, tilgangskontroll, sikkerhetsløsninger og kontinuitet og bered-skap regelmessig f. eks halvårlig.
  - Avtal evt. Sikkerhetskontroller med systemer, f. eks i form av årlige penetrasjons-tester for å få vurdert om sikkerheten til systemer er opprettholdt.
  - Sanksjoner basert på måling og rapporte-ring fra IT outsourcing partner. Prisavslag pga. manglende oppfyllelse av servicenivå, time eller dagbot
  - Krav om retting, dekningskjøp fra tredjepart, erstatning, heving

Avtal automatiske målinger av driftsstabilitet, oppetider og svartider, for systemer og help desk

7. IGANGSETTING OG OVERFØRING TIL NY LEVERANDØR – GODKJENNING

Outsourcing innebærer ofte endringer av IT-systemer, arbeidsprosesser og rapporteringsrutiner. Det er viktig å sørge for at rutiner for support og brukerhjelp er klare og at brukerne får nødvendig opplæring.

7.1 Sjekkpunkter for oppstartsfasen

- Bruk god tid til å forberede organisasjonen på endringene som kommer.
- Forberede de ansatte så tidlig som mulig på hva som vil komme
- Husk arbeidsmiljøloven som har bestemmelser om medvirkning for ansatte ved store endringer i arbeidsforhold.
- Ha et ryddig forhold gjennom hele prosessen og sørg for å følge lover og avtaleverk
- Det er bedre om de ansatte får informasjon fra ledelsen enn gjennom ryktebørsen
- Bruk tid på brukeropplæring og nye rutiner.
- Sørg for tett oppfølging av leverandøren under igangkjøring
- Kunden kan tro at jobben er avsluttet etter at kontrakten er signert, men det er jo under igangkjøringen at man er i en kritisk fase.
- Teknologi kan også være en utfordring
- Overlat ansvar for teknologisk overgang til leverandør, men følg opp kontinuerlig
- Planlegg nøye og test ny teknologi
- Ha egne krav til servicenivå, oppetid osv for perioden med igangsetting og overføring til outsourcing leverandør
- Du som kunde må som et minimum ha en prosjektansvarlig
- Utfordre leverandør på styringsmodell for innføringsperioden
- Risikovurdering – plan for informasjon, tester, prøveproduksjon og godkjenning
- En viktig del av innføringsprosjektet er oppdatering og ajourføre dokumentasjon og håndbøker
- Beskrive innholdet i godkjenningsperioden som er en del av innføringsperioden

7.2 Hva kan gå galt i oppstartsfasen?

Det er spesielt tre områder som er gjengangere:

- Informasjon og kommunikasjon til ansatte og mellom kunde og leverandør
- Teknologi og teknisk kontroll
- Motivasjon og opplæring av brukere

Bruk erfaringene fra virkelige caser nedenfor i din virksomhets oppstartfase:

- Tilpasning av egen organisasjon for oppfølging av endret driftssituasjon og outsourcing.
- Kunde er ikke tilgjengelig for beslutninger og formelle avklaringer med outsourcingsleverandør
- Manglende informasjon innad i egen organisasjon og i leverandørens organisasjon
- Manglende brukeropplæring
- Problemer med personal og organisasjonsforhold
- Mislykket teknisk migrering fra din hardware og infrastruktur til leverandørens
- Ofte nytt sted å henvende seg for brukere – brukerhjelp/helpdesk fungerer ikke
- Ofte nye krav til passord og sikkerhet – brukerne er ikke informert

8. STYRING AV AVTALEN OG FREMTIDIGE ENDRINGER

Outsourcing av IT-funksjoner er en kontinuerlig prosess. Det finnes flere rammeverk for styring og oppfølging av driftstjenester. ITIL (IT Infrastructure Library) er det langt mest brukte og er også en ISO Standard. Hvis outsourcingsleverandøren benytter ITIL, avklar med leverandør hvilke prosesser som din virksomhet bør involveres i.

For en gjennomgang av ITIL gå til ITILs norske eller internasjonale hjemmesider http://www.itsmf.no/ og http://www.itilfoundations.com

Vurder hver enkelt av disse punktene og hva som er viktig for din virksomhet:

- Styring og håndtering av drifthendelser og problemer
- Styring av endringer
- Oppfølging av tjenester og servicenivå
- Oppfølging av katastrofesikring og reservedrift
- Sikkerhetsstyring, spesielt i forhold til forretningskritisk informasjon
- Endringer i forretnings behov og nye muligheter
- Styring av ny teknologi, oppgraderinger etc.

Sørg for å ha fokus på:

- Tydelige kontaktpersoner og roller i egen virksomhet og hos leverandøren
- Forsøk å beholde noe IT-kompetanse i egen virksomhet slik at du bedre kan vurdere servicenivå og tjenestetilbud
- Vurder benchmarking mot andre selskaper hvis du ønsker å sammenligne leverandører, tjenester og pris. Slik benchmarking bør være avtalt på forhånd
- Sørg for et endringsregime med klare plikter for kunde og leverandør – få leverandøren til å logge endringer
- Sørg for at større endringer risikovurderes av leverandør og at tiltak for å redusere risiko skal framlegges
- Sørg for å etablere standarder for hvordan kvaliteten på tjenestene og servicenivå (SLA) skal måles
- Vær spesifikk i hva som skal måles og sørg for at begge parter er enige i målemetoder.
- Sørg for dialog om virksomhetskritiske IT-tjenester gjennom driftsmøter minst hver måned.

Kunden kan tro at jobben er avsluttet etter at kontrakten er signert, men det er jo under igangkjøringen at man er i en kritisk fase.

9. BEGREPER

IT-outsourcing
IT-outsourcing innebærer at virksomheten setter ut en eller flere IT-funksjoner/tjenester til en eller flere eksterne leverandører isteden for å drive disse selv.

IT-systemer og IT- infrastruktur
IT-systemer og IT-infrastruktur er i dette dokumentet synonymt med IKT-systemer og IKT infrastruktur. IT står for informasjonsteknologi, IKT står for informasjons og kommunikasjonsteknologi.

IT-systemer og IT infrastruktur omfatter alt av IKT-utstyr, kommunikasjonsløsninger, nettverksutstyr, systemer samt drift og forvaltning av applikasjoner

IT-tjenester, IT- driftstjenester
IT-tjenester omfatter alle tjenester som kan leveres fra en outsourcingsleverandør til en kunde

Brukerhjelp – brukersupport – Help desk
Omfatter vanligvis kontaktpunktet mellom leverandør og brukere hos kunden. Dette består normalt av en eller flere ansatte i kundens eller leverandørens organisasjon som svarer på spørsmål og henvendelser fra brukere pr telefon, e-post e.l. Prinsippet om at brukerhjelp eier problemet til løsning er funnet, er det normale.

ASP
Application Service Provider
En ASP-leverandør innebærer at du som kunde leier en tjeneste som omfatter tilgang til programvaren din virksomhet har behov for, inklusive lisenser, server/lagringskapasitet og backup og recovery løsninger. Tilgang til tjenestene får du via leid linje, over internett, eller evt. via mobiltlf.

Hosting
Outsourcing leverandøren drifter kundens utstyr, og utvalgte systemer installert i leverandørens driftssentral.

Onsite outsourcing
Onsite outsourcing innebærer at leverandøren fjerndrifter dine IT-systemer og IT-infrastruktur som fortsatt er plassert i dine lokaler.

Cloud Computing
er en betegnelse for IT-tjenester levert over Internett. Dette leveres oftest med dataprosessering og datalagring på servere som står i store eksterne serverparker tilknyttet internett og hvor du kan leie tilgang til systemer som f. eks e-post, lagring, intranett.

Offshoring
Innebærer at IT-tjenestene leveres fra et lavkostland Tjenesten kan omfatte de fleste typer IT-tjenester og IT- infrastruktur.

Backup
Kopiering av data for å beskytte mot integritetstap eller tap av originaldata.

Restore
Iverksette handlinger for å gjenopprette en IT-tjeneste /data for brukerne.

Kritisk informasjon
Informasjon eller opplysninger som er kritisk for virksomheten om det blir gjort tilgjengelig for uvedkommende. Det kan være forhold knyttet til produkter, produksjon, kunderegister, sikkerhetstiltak, herunder fysiske sikringstiltak osv.

SLA Service Level Agreement
Avtale om tjenestekvalitet på IT-tjenester, f. eks tilgjengelighetstid for IT-tjenester, svartider for henvendelser, løsningstider for problemer eller endringer, reetableringstid ved driftsstans

ITIL
ITIL. Information Technology Infrastructure Library
Dokumentert god praksis for ledelse av IT-tjenester.

ITIL eies av OGC og består av en serie publikasjoner som gir veiledning til hvordan en kan levere IT-tjenester med et avtalt kvalitetsnivå, samt prosesser og ressurser nødvendige for å understøtte og styre disse.

For mer informasjon se:
http://www.itil.co.uk/

Lov om behandling av personopplysninger (personopplysningsloven):
http://www.lovdata.no/all/nl-20000414-031.html

Databehandleravtaler etter personopplysningsloven og helseregisterloven, veileder, datert 26.5.2009, Datatilsynet
http://www.datatilsynet.no/templates/article____2742.aspx

Forskrift om behandling av personopplysninger (personopplysningsforskriften)
http://www.datatilsynet.no/templates/article____2742.aspx

Sikkerhetsloven (lov om forebyggende sikkerhet)
www.nsm.stat.no

Veiledning i verdivurdering
www.nsm.stat.no / veiledninger

Veiledning i hendelseshåndtering
http://norsis.no/veiledninger/ledelse/Veiledning_i_hendelseshaandtering.pdf

10. REFERANSER

- Dataforeningens kontraktsstandard for IT-drift, sist oppdatert 13.2.2006; Den Norske Dataforening
- IKT Norges standardavtale om IT driftsytelser (outsourcing), sist oppdatert 29.2.2006, IKT Norge
- Avtale om kjøp av driftstjenester knyttet til maskinvare, infrastruktur og programvare. Statens standardavtaler for IT-anskaffelser SSA-D, sist oppdatert mars/april 2009, DIFI
- Dataforeningens sjekkliste for outsourcing, sist oppdatert1997
- Rapport fra Outsourcingsundersøkelsen 2007, Handelshøyskolen BI
- Rapport fra Outsourcingsundersøkelsen 2009, Handelshøyskolen BI
- Lov om behandling av personopplysninger (personopplysningsloven). Forskrift om behandling av personopplysninger (person-opplysningsforskriften) Databehandleravtaler etter personopplysningsloven og helseregister-loven, veileder, datert 26.5.2009, Datatilsynet
- Internkontroll i mindre virksomheter, veileder, datert 15.02.200, Datatilsynet
- En veileder om internkontroll og informasjonssikkerhet, november 2009, Datatilsynet
- Seks steg til outsourcing for SMB, 2007, IDG Magazines Norge AS
- Syv steg til riktig outsourcing, 2005, IDG Magazines Norge AS
- Gartner, Outsourcing Contract terms and Conditions, an understanding of the 19 Articles in a Master Service Agreement, April 2010, Gartner
- Audit of Outsourcing, By S. Anantha Sayana, 2004, ISACA (Information Systems Audit and Control Association)
- Outsourcing Information Security, C. Warren Axelrod, 2006, ISACA

VEILEDEREN UTGIS MED STØTTE FRA