Myndigheten för samhällsskydd och beredskap

Vägledning – informationssäkerhet i upphandling

Informationssäkerhet i upphandling av system, outsourcing och molntjänster

Vägledning – informationssäkerhet i upphandling

Informationssäkerhet i upphandling av system, outsourcing och molntjänster

Vägledning – informationssäkerhet i upphandling

Myndigheten för samhällsskydd och beredskap (MSB)

Layout: Advant Produktionsbyrå AB
Tryckeri: DanagårdLiTHO

Publ.nr MSB555 - april 2013
ISBN 978-91-7383-338-7

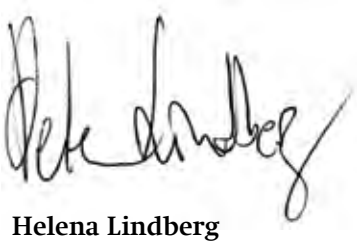
Förord

Företag, myndigheter, kommuner och landsting bygger i allt högre grad sin verksamhet på informationshantering. Det är inte bara betydelsen av informationshanteringen som ökat utan också kostnaderna. I E-delegationens förstudie Effektiv it-drift beräknades den offentliga sektorns kostnader för it 2012 till 46,5 miljarder kronor[1]. I Riksrevisionens rapport ”IT i statsförvaltningen” sägs att it-kostnaderna är den tredje största utgiftsposten i myndigheternas förvaltningsanslag efter löner och lokalkostnader[2]. Sammantaget innebär detta att en effektiv styrning av informationshanteringen både kan utveckla verksamheten och ge möjlighet till betydande kostnadsreduktioner.

Tidigare har organisationerna huvudsakligen själva ägt både system, hårdvara och kommunikation. Idag har landskapet förändrats. Tjänster som outsourcing och molntjänster är ett allt mer använt alternativ till egen drift och egna system. Både E-delegationens förstudie och Riksrevisionens rapport pekar på att det finns stora vinster i en ökad användning av denna typ av tjänster. Det poängteras också att det alltid måste ske en analys av vilken aktör som är bäst lämpad att leverera det it-stöd som myndigheten behöver. I detta ligger också att det inte endast är kommersiella alternativ som kan vara aktuella utan även olika typer av partnersamarbeten. Rekommendationen att göra en analys av vilket alternativ som är mest gynnsamt får anses som lika giltig för myndigheter, kommuner, landsting och företag.

För att kunna genomföra fungerande upphandlingar av it-relaterade tjänster är det av avgörande betydelse att kraven ur informationssäkerhetssynpunkt är en del i processen. Om så inte är fallet riskerar den upphandlande organisationen inte bara att få en levererans med säkerhetsproblem utan också en bristande ekonomisk styrning där stora oväntade kostnader kan tillkomma.

Denna vägledning är avsedd att ge ett övergripande stöd till olika typer av organisationer för att genomföra sina upphandlingar av it-relaterade tjänster så att även informationssäkerhetsaspekterna beaktas. På så sätt förbättras även samhällets säkerhet.



Helena Lindberg
Generaldirektör
Myndigheten för samhällsskydd och beredskap

1. Effektiv IT-drift, förstudie från E-delegationen i juni 2013 - Bilaga 1 - Kostnadsberäkningar för nuläge, sid. 9
2. Riksrevisionens rapport 2011:4 IT inom statsförvaltningen - har myndigheterna på ett rimligt sätt prövat frågan om outsourcing bidrar till ökad effektivitet?, sid. 9

Innehåll

Inledning

1. Inledning

1.1 Syfte

Syftet med denna vägledning är att ge olika typer av organisationer, både offentliga och privata, ett stöd för att föra in informationssäkerhetsaspekter på effektivt sätt i sina upphandlingsprocesser.

Målgruppen är informations- och it-säkerhetsansvariga, it-ansvariga, upphandlare samt projektledare för projekt där varor och tjänster som påverkar informationssäkerheten ska upphandlas eller utvecklas.

1.2 Bakgrund

En förändring som skett under de senaste decennierna är att organisationer, både privata och offentliga väljer att i allt högre grad fokusera på sin kärnverksamhet. Istället för att till exempel sköta lokalvård och it-drift i den egna organisationen anlitas externa leverantörer av dessa tjänster. I vissa fall väljer man även att lägga ut delar av sin kärnverksamhet på externa leverantörer som till exempel då ett privat vårdföretag får i uppdrag att driva en vårdcentral.

Mängden av tjänster som en organisation kan upphandla som stöd för den egna verksamheten ökar ständigt. I allt högre grad bygger tjänsterna på någon typ av informationshantering. Spannet är stort där vissa av tjänsterna innebär övertagande av merparten av kundens informationshantering medan det i andra ytterkanten kan handla om att köpa en tjänst som fyller en mycket begränsad funktion hos kunden. Utvecklingen mot att allt mer av den tidigare interna verksamheten nu sker via köp av tjänster gäller i hög grad för it-drift och övriga it-tjänster.

Samtidigt har kraven på informationssäkerhet ökat eftersom både offentliga och privata verksamheter blivit mer medvetna om beroendet av sin informationshantering.

Informationssäkerhet syftar, som begreppet antyder, till att skydda information. Med skydd avses att kunna upprätthålla rätt nivå av

- konfidentialitet
- riktighet
- tillgänglighet
- spårbarhet

Informationssäkerhet vid upphandling av it-relaterade tjänster handlar därmed om att styra upphandlingsprocessen så att den levererade tjänsten kan upprätthålla de krav på att informationen ska vara skyddad hos leverantören som har definierats i avtalet. Det innebär till exempel att informationen ska vara skyddad från obehörig insyn och förändring hos leverantören samt att informationen och möjligheten att hantera den finns hos kunden på den nivå som överenskommits. Kunden ska också ha möjlighet att granska hur informationen har hanterats hos leverantören.

I tjänstesamhället är upphandling ett centralt moment för att styra verksamheten. Detta gäller även för styrningen av informationssäkerhet och för att säkerställa att organisationens säkerhetsregler följs i alla de aktiviteter som man har ansvar för, även om dessa utförs av utomstående parter. Grundläggande för samtliga fall då informationshanteringen helt eller i delar läggs ut på en annan part är att ansvaret för informationen och dess säkerhet alltid ligger kvar hos informationsägaren. För myndigheter, kommuner och landsting är denna princip också lagstadgad.

Att upphandla stöd i form av ett nytt system eller annan teknisk lösning för den interna verksamheten är kanske den aktivitet som ligger närmast till hands då begreppen ”upphandling” och ”informationssäkerhet” sammanförs. Upphandling av hela system är dock inte den enda situation då informationssäkerheten blir en viktig faktor. Det finns många tjänster som i sig inte innebär att en leverantör får i uppdrag att sköta delar av kundens informationshantering men som ändå kan påverka informationssäkerheten. Exempel på detta är lokalvård och olika typer av konsulttjänster där anställda hos de anlitade leverantörerna får möjlighet att ta del av eller på annat sätt påverka kundens informationsresurser. Denna vägledning kommer inte närmare att beskriva hur informationssäkerhetskrav kan ställas i sådana situationer men resonemang och metoder kan tillämpas vid alla upphandlingar där det kan antas att kundens informationssäkerhet kan påverkas.

Syftet med vägledningen är att ge stöd för säkerhet i upphandling av:

- It-system
- Outsourcing av it-relaterade tjänster
- Molntjänster

I fortsättningen kommer dessa tre typer av tjänster att kallas it-relaterade tjänster. Observera att med begreppet outsourcing täcks även situationer när leverantörer i kundens lokaler utför tjänster av denna typ.

Vägledningen har ett livscykelperspektiv på informationshanteringen, det vill säga visa på att en upphandling inte är en enskild aktivitet begränsad i tid. Istället bör upphandlingen ses som startpunkten i en längre relation som innehåller bland annat en lång förvaltningsfas och en avveckling alternativt arkivering av information. Informationssäkerhet ingår som en viktig del i hela förloppet och kommer att påverka de ekonomiska förutsättningarna för relationen. Att inte integrera säkerhetsaspekterna i upphandlingen redan från början kan leda till mycket negativa konsekvenser under lång tid både för säkerheten och för ekonomin.

1.2.1 Samverkan kring it-relaterade tjänster

Det har blivit allt vanligare att organisationer istället för att upphandla eller utveckla själva går samman och skapar exempelvis ”partnermoln”. En annan variant är då myndigheter erbjuder varandra tjänster i form av till exempel servicecenter eller att hela myndigheter skapas för att tillhandahålla tjänster till andra myndigheter.


CARL XVI GUSTAF · SVERIGE

Denna typ av lösningar innebär inte upphandling i vanlig bemärkelse men ur säkerhetssynpunkt är grundförhållandet detsamma; en organisation överlåter åt en annan part att sköta delar av organisationens informationshantering. Därmed kan principer i denna vägledning tillämpas även i denna typ av lösningar.

Av särskild betydelse är att klarlägga ansvar och roller samt fastställa processer för hur säkerhetskrav ska hanteras och hur uppföljning ska ske. Grundpremissen är att kundorganisationen, oavsett om denna är en partner eller inte, ska formulera sina säkerhetskrav genom informationsklassning. Kraven ska kunna matchas mot leverantörens utbud som måste finnas på säkerhetnivåer som motsvarar kundorganisationens krav.

1.2.2 Offentlig upphandling och LOU

För offentlig sektor finns särskild lagstiftning, lagen (2007:1091) om offentlig upphandling (LOU) som styr hur upphandling ska ske. LOU omfattar både upphandling via enstaka avtal och så kallade ramavtal då leveransen kan avropas under en bestämd tid. Denna vägledningen går inte närmare in på hur LOU ska tillämpas, mer information går att inhämta bland annat på Konkurrensverkets webbplats[3].

1.2.3 Säkerhetsskyddad upphandling

Innan en myndighet påbörjar en upphandling ska myndigheten pröva om upphandlingen helt eller delvis ska säkerhetsskyddas, dvs. att det ska genomföras en så kallad upphandling med säkerhetsskyddade avtal (SUA). Det som avgör om en upphandling ska säkerhetsskyddas eller inte är om företaget kan få del av hemliga uppgifter i förfrågningsunderlaget eller under uppdragets utförande. Hemliga uppgifter avser uppgifter som är hemliga enligt säkerhetsskyddslagen (1996:627).

Med säkerhetsskydd avses:

- skydd mot brott som kan hota rikets säkerhet
- skydd av hemliga uppgifter som rör rikets säkerhet
- skydd mot terrorism.

Om tjänsten som myndigheten ska upphandla innebär att hemliga uppgifter blir tillgängliga för leverantörer ska myndigheten enligt 8 § säkerhetsskyddslagen träffa ett skriftligt säkerhetsskyddsavtal med anbudsgivaren eller leverantören om det säkerhetsskydd som behövs i det särskilda fallet. I denna vägledning kommer inte säkerhetsskyddade upphandlingar att vidare beröras, istället rekommenderas den vägledning som har tagits fram av Säkerhetspolisen (SÄPO) i denna fråga[4].

3. http://www.konkurrensverket.se/upload/Filer/Trycksaker/Infomaterial/Upphandlingsreglerna.pdf
4. http://www.sakerhetspolisen.se/download/18.34ffc68f1235b740c0680001063/Sakerhetsskyddadupphandlingen-vagledning.pdf

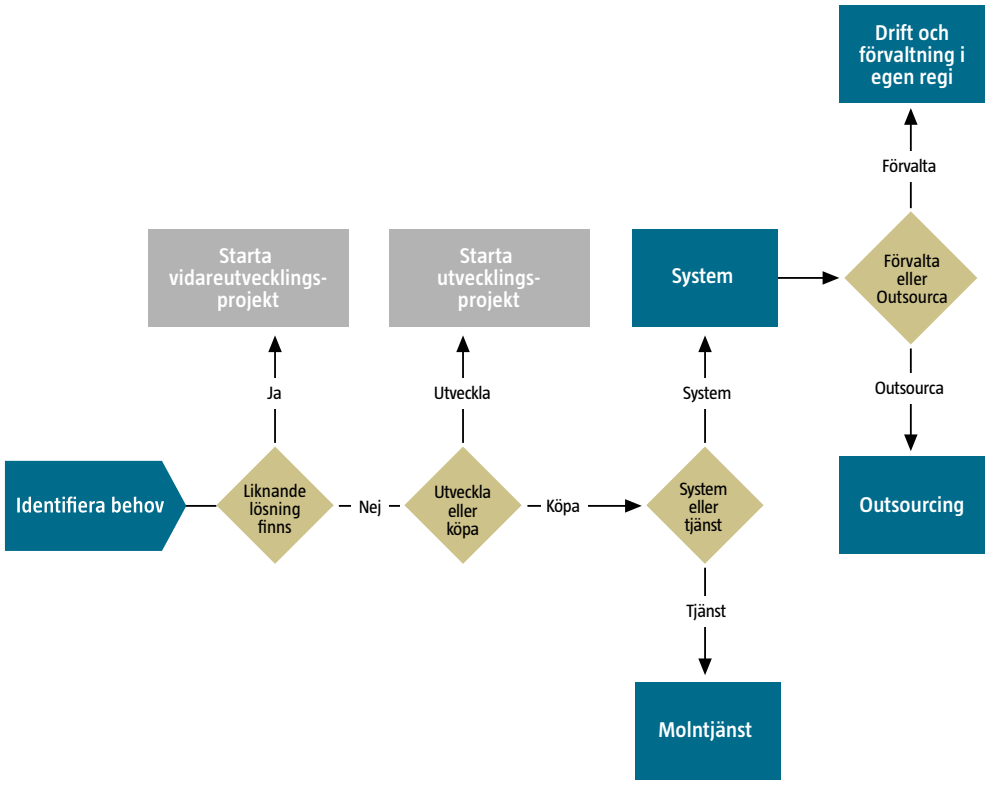
1.3 Avgränsning

Nedanstående bild visar på olika vägval när det gäller att tillgodose behovet av ytterligare it-stöd inom en organisation.

Allting utgår självfallet från det behov som har identifierats och som bör vara så väl beskrivet och förankrat i organsationen som möjligt. Om man därefter konstaterar att befintligt stöd inte täcker behovet uppstår frågan om det nya stödet ska utvecklas inom den egna organisationen eller köpas upp av en extern leverantör.

Denna vägledning kommer inte närmare att beröra utvecklingsprojekt även om många av de generella råd som ges fortsättningsvis kan användas som stöd i denna typ av projekt.

Vägledningen kommer däremot att beröra de ytterligare vägval i som visas figuren. Det gäller upphandling av molntjänster eller system, det senare då antingen i egen regi eller i outsourcad drift.



Figur 1: *Process för alternativa lösning för att tillgodose behov av ytterligare it-stöd.*

Att upphandla it-stöd – fördelar och risker

2. Att upphandla it-stöd – fördelar och risker

Länge kunde upphandling av it-stöd delas upp i kategorierna hård- respektive mjukvara. Numera täcker inte dessa begrepp de alternativ som finns då en organisation vill upphandla ett it-stöd. En långsiktig trend är att alltmer av it-stödet tillhandahålls av utomstående leverantörer medan kunden kan köpa olika typer av tjänster som i varierande grad innebär att hårdvara och mjukvara ägs av kunden. Många kunder är idag osäkra på vad de egentligen ska upphandla och vad det innebär ur säkerhetssynpunkt.

Att klargöra vad upphandlingen gäller är viktigt ur säkerhetssynpunkt eftersom det avgör hur bland annat ansvarsfördelningen ser ut mellan kund och leverantör.

Nedan följer en schematisk bild av vad leveransen i en upphandling kan vara. I kolumnen Form visas de tre alternativen som kan upphandlas ”System”, ”Molntjänst” och ”Outsourcing”. Genom att peka ut var information, system och hårdvara befinner sig fysiskt samt av vem de ägs klargörs skillnaderna mellan de olika formerna för it-leverans.

För t.ex. köp av system för egen drift gäller att såväl information, hårdvara som system finns fysiskt hos kunden. Kunden äger även samtliga tillgångar i detta avseende.

I fallet med outsourcing gäller att hårdvara och system fysiskt finns hos leverantören, medan informationen finns såväl hos leverantören som hos kunden, i alla fall under den tid då kunden hämtar och bearbetar informationen. Som kund gäller det att säkerställa att lösningar för kommunikation och åtkomst är motsvarar de klassning av informationen som har gjorts, se avsnittet 3.5 om informationsklassning.

FORM	FYSISKT HOS KUNDEN	FYSISKT HOS LEVERANTÖREN	ÄGANDE HOS KUNDEN	ÄGANDE HOS LEVERANTÖREN
Köpa och sköta driften av system	I H S		I H S	
Molntjänst	I	I H S	I	H S
Outsourcing	I	I H S	I S	H

I *Information* S *System* H *Hårdvara*

Tabell 1: *Ansvar och fysisk åtkomst i förhållande olika lösningar i olika former av it-leverans.*

Bilden på föregående sida är generell och det finns ett mycket stort antal variationer och mellanformer mellan att köpa system, en molntjänst och outsourcing. Särskilt bör understrykas att bilden inte endast kan användas då det gäller kommersiella alternativ utan i lika hög grad då det gäller andra typer av samverkan. Exempel på detta kan vara då myndigheter skapar gemensamma servicecenter eller på annat sätt samverkar kring sin informationshantering. Oavsett vilken lösning som väljs är det viktigt att redan från inledningsfasen utgå från informationshanteringens hela livscykel, det vill säga även förvaltning och avveckling.

Här följer en översiktlig genomgång av säkerhetsaspekter i de olika alternativen. Allmänt kan sägas att en genomarbetad och välförankrad it-strategi är ett mycket bra stöd både för att göra ett initialt val av typ av lösning och för den fortsatta upphandlingsprocessen. It-strategin bör bygga på en övergripande riskanalys som har lett fram till generella ställningstaganden i säkerhetsfrågor. Inför mer omfattande upphandlingar av it-relaterade tjänster är det ofta lämpligt att knyta en sourcingstrategi till it-strategin.

2.1 Drift och förvaltning av system i egen regi

Under detta kapitel behandlas fallet då en organisation väljer att köpa en färdig lösning som ett system och därefter sköta drift och förvaltning av detta i egen regi. Inför valet att köpa färdigt system är det självfallet viktigt att man, förutom de rent säkerhetsmässiga kraven, även tar med de krav som relaterar till den egna driftmiljön, att systemet ”passar in” i den befintliga arkitekturen.

Det finns naturligtvis många typer av system, från mer avancerade system för t.ex. att hantera vårdinformation till mindre, körbar programkod för att lösa enstaka uppgifter (som till exempel brevmallar eller makron till kontorsprogramvaror). Motiven för valet att sköta driften själv kan variera. I en del fall handlar det om att skaffa sig bättre kontroll över systemet och få en bättre kontakt mellan verksamheten och systemdriften. I andra fall handlar det om en säkerhetsmässig bedömning, där man ser fördelar med att slippa kommunicera över öppna nätverk för att nå tjänsten. Säkerhetsmässigt kan det också vara enklare att integrera ett system i sin egen befintliga miljö med de administrativa och tekniska säkerhetslösningar som redan finns implementerade än att ställa krav på till exempel en molntjänst.

Krav på gallring och arkivering är, inte minst för myndigheter, kommuner och landsting som lyder under arkivlagen, viktiga frågor som ofta blir bortglömda vid upphandlingar. För den organisation som har merparten av resurserna för sin informationshantering i egen drift och förvaltning kan det vara enklare att införa ett livscykelperspektiv där även behovet av gallring och arkivering formuleras för samtliga system. Möjligheten att införa någon typ av e-arkiv kan också underlättas.

Det kan också gå snabbare att genomföra ett systembyte i den egna miljön än att avsluta ett ingånget avtal för outsourcing eller för en molntjänst.

Att upphandla ett system för drift i egen regi kan alltså innebära tydliga fördelar ur säkerhetssynpunkt men också risker. Ett problem som ofta dyker upp är att

en intern rollfördelning kring kravställning inte är etablerad. Det innebär att det inte finns tydliga roller, processer och rutiner för att verksamheten ska kunna ställa säkerhetskrav på den interna it-funktionen eller systemägare. I en sådan situation finns en uppenbar risk att säkerhet blir en fråga långt ner på prioriteringslistan.

God informationssäkerhet förutsätter inte bara kompetens inom säkerhetsområdet utan också att de medarbetare som har ansvar för vitala resurser som till exempel för verksamheten centrala system har mycket god kompetens inom relevanta tekniska områden. Tillräcklig kompetens kan vara svår att upprätthålla i en liten eller medelstor verksamhet vilket kan leda till säkerhetsbrister och nyckelpersonsberoende. När det inte går att genom egna medarbetare tillgodose behovet av kompetens kan dessutom ett alltför omfattande konsultberoende bli följden.

Brist på aktuell kompetens kan också göra att utvecklingsinsatser kring systemet avstannar och att kunden nöjer sig med de uppdateringar som kommer från leverantören.

En aspekt som ofta framhålls som en fördel med molntjänster är möjligheten till snabba förändringar i kapacitetsutnyttjande, vilket kan vara betydligt svårare om informationshanteringen sker i egna system. Detsamma gäller redundans där det kan vara mycket mer resurskrävande att i en enskild organisation skapa alternativa lösningar för att kunna upprätthålla driften än vad det är för en stor it-leverantör.

2.1.1 Fördelar och nackdelar

Nedan följer ett antal fördelar och nackdelar som kan finnas då system driftas och förvaltas i egen regi. Beskrivningen bör ses som ett försök att identifiera förhållanden som kan uppstå i denna situation och som bör analyseras vid ett vägval.

FÖRDELAR	NACKDELAR
Bättre möjlighet till kontroll	Svårt att upprätthålla rätt kompetens över systemets livscykel
Organisationen kan själv styra utvecklingen	Svårt att skapa en tydlig rollfördelning med kravställning mellan verksamhet och intern it-organisation
Nära kontakt med verksamheten, kan ge möjlighet till snabbare anpassning	Svårt att snabbt förändra kapacitetsutnyttjandet
Bättre support och kompetens i verksamhetsfrågor	Låg potential för utveckling
Krav på arkivering och gallring är enklare att genomföra	Innebär inte samma möjlighet till stordriftfördelar som i sin tur kan led till ekonomiska fördelar
Möjlighet att lägga till ytterligare säkerhetsåtgärder utifrån egna behov	

FÖRDELAR	NACKDELAR
Möjlighet att lägga till ytterligare säkerhetsåtgärder utifrån egna behov	Svårt att uppnå höga krav på redundans
Säkerhet genom kommunikation via interna nätverk	Sämre utbud av möjliga säkerhetslösningar
Matcha egna skyddsnivåer mot organisationens modell för informationsklassning	Svårt att byta ut föråldrade system vilket kan leda till inlåsningseffekter
Enklare att genomföra systembyte	
Större lojalitet mot organisationens intressen hos systemägare och systemförvaltare	

2.2 Outsourcing och molntjänster

Outsourcing och molntjänster har många likheter och det går inte alltid att dra en exakt gräns mellan dessa typer av tjänster. I inledningen av kapitel 2 finns en bild som ger stöd för hur en uppdelning skulle kunna se utifrån uppdelning av ägande och fysisk åtkomst till information, system och hårdvara. En närmare beskrivning av vad som avses med de olika begreppen följer här.

2.2.1 Outsourcing

Outsourcing brukar definieras som det förhållande att en organisation låter en annan organisation sköta en eller flera av deras processer. I vårt fall handlar det om it-relaterade tjänster som annars skulle ha producerats inom organisationen men som genom avtal sköts av någon annan.

Outsourcing kan vara mer eller mindre omfattande. Det kan handla om allt från utläggning av enstaka tjänster till outsourcing av hela driftmiljöer.

2.2.2 Molntjänster

Det finns inte någon allmänt accepterad definition av molntjänster och molntjänster kan även ta sig olika former. Vi kommer här att utgå från Sveriges IT-arkitekters definition:

Termen Cloud Computing relaterar både till applikationer som levereras som tjänster över Internet och till den hårdvara och systemmjukvara som tillhandahåller dessa tjänster[5].

Molntjänster kan skapas och levereras på olika sätt. Det som i dagligt tal avses är kommersiella molntjänster som kan ses som en typ av outsourcingtjänst där kunden köper datorkraft och system via internet. Tjänsterna levereras på ett lättillgängligt sätt av leverantörer och där kunden har möjlighet att skala upp användning utifrån sitt behov. Kundens kostnad för tjänsten blir också relaterad

5. IASA – Sveriges IT arkitekter 2009

till den faktiska användningen vilket också kan vara förmånligt jämfört med att ha samma tjänst i egen miljö.

Men molntjänster kan också finnas i form av icke-kommersiell samverkan mellan exempelvis kommuner. Det grundläggande är att det är en tjänst som levereras via internet eller annat publikt nät och att kundens/användarens information inte hanteras/lagras i en fysiskt avgränsad server.

Det som kallas molntjänster är egentligen inte en ny teknisk lösning utan ett nytt sätt att leverera datorkraft och tjänster. Molnen kan organiseras på olika sätt där tre huvudtyper kan urskiljas:

- **Privata moln**– tjänster uppbyggda enligt molnprinciper men endast tillgängliga inom ett privat nätverk
- **Partnermoln** – tjänster som erbjuds till en begränsad och väldefinierad grupp av intressenter
- **Publika moln** – tillgängliga för alla organisationer som så önskar

2.2.3 Informationssäkerhet vid outsourcing och användandet av molntjänster

När det gäller informationssäkerhet är också likheterna många mellan outsourcing och användandet av molntjänster, eftersom det i båda fallen handlar om att överlämna sin informationshantering till en utomstående part. Det är dock vara svårare att kontrollera fysiskt skydd och andra säkerhetsåtgärder som omger de resurser som hanterar den aktuella informationen än vid traditionell outsourcing.

Nedanstående är skrivet ur perspektivet att det är en kommersiell molntjänst som är aktuell. Flertalet av riskerna är dock relevanta även då avsikten är att använda tjänster i ett partnermoln.

Sourcing-strategi

Ett första steg för en säkrare upphandling av outsourcing och molntjänster är att ta fram och besluta en sourcing-strategi i anslutning till den it-strategi som organisationen förhoppningsvis redan har. I sourcingstrategin beskrivs i vilka delar de långsiktiga behoven och målen för verksamheten kan uppnås med hjälp av outsourcing alternativt molntjänster. I strategin ska även en övergripande inriktning för informationssäkerheten i de tjänster som ska upphandlas anges. Även ansvar och roller i både upphandlingen och den långsiktiga förvaltningen av de upphandlade tjänsterna bör framgå. Som andra liknande strategier måste även en sourcing-strategi fastställas av ledningen för att fungera som ett verktyg för styrning.

Redundans och flexibelt kapacitetsutnyttjande

Fördelarna med outsourcing och molntjänster är många och det finns en tydligt ökad användning av kommersiella tjänster, liksom för olika typer av partnersamverkan. Inte minst finns stora ekonomiska vinster i de stordriftsfördelar och i den internationella integrering som framför allt molntjänster leder till. I vissa fall kan dessa tjänster innebära en möjlighet att förbättra säkerheten för en organisation. Fördelarna ur säkerhetssynpunkt är bland annat knutna till möjligheten till redundans, dvs. leverantören kan styra om leveransen mellan olika leveransställen så att kunden/partnern inte behöver riskera avbrott i tillgängligheten. I detta ligger

naturligtvis också att kunden/partnern har möjlighet att snabbt utöka sitt utnyttjande av tjänsten, något som kan varar betydligt svårare om man har driften i sin egen verksamhet.

Effektiva och uppdaterade säkerhetslösningar
En annan typ av fördelar är att en leverantör av molntjänster eller outsourcing har möjlighet att installera säkerhetslösningar samt rutiner för att administrera dessa på ett sätt som är svårt att klara för en enskild organisation. Det kan t.ex. gälla upptäckt av skadlig kod, härdning och hanteringen då incidenter har inträffat. Inte minst är det så att uppdateringar som förbättrar säkerheten betydligt snabbare kan distribueras i denna typ av lösningar. Detta gäller även i nät som inte drivs i kommersiell regi, dvs. som partnermoln, där det finns en stor potential i att flera separata aktörer kan bidra med sin säkerhetskompetens i en gemensam säkerhetslösning.

Otydliga ansvarsförhållanden
Det finns också ett antal gemensamma riskområden. Ett centralt sådant är ansvarsfördelning. En säker informationshantering bygger på att det finns uttalade och tydliga ansvarsförhållanden. När en organisation använder molntjänster eller outsourcingtjänster finns det ett stort antal förhållanden där ansvaret måste regleras mellan kund och leverantör. En fälla som kunden lätt kan gå i är att man gör underförstådda antaganden att leverantören genomför olika typer av säkerhetsaktiviteter, som exempelvis regelbundna tester med återläsning av kopior, penetrationstester och skydd mot skadlig kod, utan att detta behöver avtalas. Riskerna är naturligtvis mycket olikartade beroende på vilken typ av molntjänst eller outsourcing alternativt samarbete som är aktuellt. För att ta ett exempel gällande molntjänster är det med stor sannolikhet så att publika moln kan erbjuda betydligt större tillgänglighet och redundans än ett privat nät. Å andra sidan är den egna organisationens möjlighet att kontrollera åtkomst och efterlevnad på en helt annan nivå i ett privat nät. För att ytterligare komplicera frågan kan det finnas en tendens att negligera säkerhetsfrågorna i ett partnermoln utifrån den underförstådda föreställningen att de andra ingående parterna redan har genomfört analyser och säkerhetsåtgärder. Det går alltså inte att värdera risker utifrån en specifik teknisk eller organisatorisk lösning. Istället måste kunden se till helheten av sina egna behov och vad den aktuella lösningen kan erbjuda.

Om avtalsprocessen inte leder fram till ett klarläggande av vilka säkerhetsåtgärder som ska vidtas och vem som är ansvarig för dem kan det också leda till andra problem. Ett sådant är att kunden och leverantörens säkerhetsåtgärder interagerar på ett negativt sätt, t.ex. att kundens brandväggar förhindrar leverantörens sårbarhetsanalyser.

Användande av underleverantörer
Av särskild betydelse för kunden är att skaffa sig kontroll över situationer där leverantören kan tänkas använda underleverantörer. Detta kan påverka även ansvarsförhållanden och t.o.m. av legala skäl omöjliggöra användandet av molntjänster. Enligt personuppgiftslagen (SFS 1998:204) ska den personuppgiftsansvarige ha en mycket god kontroll över personuppgiftsbiträdet, dvs. leverantören av en molntjänst eller en outsourcingleverantör. Denna kontroll kan vara i princip omöjlig att upprätthålla om leverantören använder underleverantörer och

ansvarsförhållandena är oklara. Detta är särskilt kritiskt för molntjänster som bygger på att informationen kan förvaras i princip var som helst på jorden.

Risken att hamna i ”dåligt sällskap”
Som kund hos en leverantör är det svårt att välja sina medkunder, vilket kan leda till vissa risker då dessa kan ägna sig åt aktiviteter som påverkar leverantörens övriga kunder. Kriminell verksamhet hos en kund kan exempelvis leda till att servar beslagtas av polisen, vilket kan drabba samtliga kunder som har information på den aktuella servern. Vissa organisationer kan också vara utsatta för olika typer av attacker som t.ex. överbelastningsattacker. Attackerna kan då drabba även andra kunder hos leverantören. Slutligen kan en organisation som väljer ”fel” leverantör hamna i dåligt sällskap som påverkar den egna organisationens rykte.

Inlåsning och överföring av avtalsvillkor till annan part
En av de stora fördelarna med molntjänster och outsourcing som ofta lyfts fram är den flexibilitet som kan erbjudas kunden. Denna sanning bör dock modifieras med tanke på den risk för inlåsning som kan finnas, dvs. att kunden inte på ett enkelt sätt kan flytta sin information eller sitt tjänsteutnyttjande till en annan leverantör eller tillbaka till sin egen driftmiljö. För närvarande finns inte etablerade verktyg eller standarder för hur migrering ska kunna ske mellan olika tjänsteleverantörer. Detta leder till en inlåsning där det blir svårt för kunden att ha en sund affärsmässig relation med leverantören där t.ex. säkerhetskrav kan vara svåra att genomdriva. För den som ämnar upphandla molntjänster eller outsourcing är det lämpligt att utgå ifrån att det inte hos leverantörer finns ett starkt naturligt intresse för att underlätta för kunden att byta leverantör. Kunden måste därför räkna med att ensam analysera på vilket sätt en eventuell migrering ska ske och ställa krav på leverantören utifrån detta.

En risk relaterad till inlåsning är då leverantörens förhållanden kraftigt förändras, i ytterlighetsfallet att leverantören går i konkurs eller blir uppköpt av ett annat företag. I en sådan situation kan kunden bli tvungen att ta hand om information och tjänster i ett akut läge vilket i sig utgör en stor risk t.ex. i form av allvarliga avbrott eller informationsförluster.

När en avtalspart upphör att existera förflyttas i de flesta fall avtalet över till en annan part. Här kan dock inte den andra parten räkna med att de delar av relationen som inte är bindande och nedskrivna i avtal följer med. Precis som vid en längre outsourcing kan ett längre utnyttjande av en molntjänst tendera till att allt fler icke-bindande överenskommelser och även outtalade förväntningar kommer att ingå i relationen. Om denna relation hastigt avbryts eller förändras starkt kan kunden alltså helt plötsligt stå i en helt annan situation än tidigare, en situation som det kan vara svår att snabbt få överblick över.

Kontinuitetshantering
För de tjänster där det finns höga krav på tillgänglighet är det viktigt att kunden förbereder sig på denna typ av situationer med utarbetade reservrutiner och kontinuitetsplanering. Likaså bör kunden fortlöpande dokumentera även mer informella överenskommelser samt bedöma i vilken mån dessa bör ingå i ett förnyat avtal.

Arkivering och gallring

En viktig aspekt av informationshantering som tidigare påpekats och som ofta underskattas eller glöms bort är hur arkivering och gallring ska ske. Krav finns, särskilt för myndigheter, landsting och kommuner, i allmänhet i båda riktningarna, det vill säga både på att arkivera och på att gallra. Både lagstiftning och organisationens egna behov gör det ofta nödvändigt att lagra information i oförändrat skick under kortare eller längre tid. Å andra sidan kan det finnas lika starka krav, inte minst av integritetsskäl, på att information ska gallras efter en bestämd tid. Tidigare har lagringen av digital information betraktats som en stor potentiell kostnad eftersom lagringsmedia har varit relativt kostsamma. Idag är förhållandet snarare det omvända; det dyrare att gallra än att lagra information. Om det finns lagkrav eller specifika överenskommelser kring arkivering och gallring finns det därmed en betydande risk att information som av olika anledningar borde gallras ändå finns kvar hos leverantören. Det finns därför ofta skäl att föra in krav på gallring och arkivering i avtalet med leverantören.

Legala risker

Slutligen finns det legala risker. När det gäller molntjänster och outsourcing kan de grovt delas in i två dimensioner: vissa risker är kopplade till sakfrågor i det rättsliga regelverk som är tillämpligt, andra handlar om osäkerheten kring vilket rättsligt regelverk som de facto ska tillämpas.[6] Till den första kategorin hör exempelvis ett otydligt avtal som reglerar hur skyddet för personuppgifter eller immateriella rättigheter ska upprätthållas. Kan inte ett adekvat skydd ges innebär detta i förlängningen risk för påföljd och skadestånd om brott mot nämnda lagar konstateras. Till den andra kategorin kan räknas de fall där man visserligen har utrett och i avtalet tydligt hanterat den lagstiftning som man ser som primärt tillämplig, men man har missat att annan lagstiftning kan bli tillämplig pga. att informationen hanteras i andra länder.

6. Inom ramen för arbetet inom sammanslutningen Cloud Sweden, initierat av Dataföreningen, har en juridisk checklista tagits fram av en juridikgrupp. Juridikgruppen har representanter från en rad olika advokatbyråer, Stockholms universitet samt Myndigheten för samhällsskydd och beredskap. Checklistan ger en övergripande vägledning inför den rättsliga analysen. http://cloudsweden.files.wordpress.com/2011/12/juridisk_checklista_fc3b6r_molnavtal_version_10.pdf

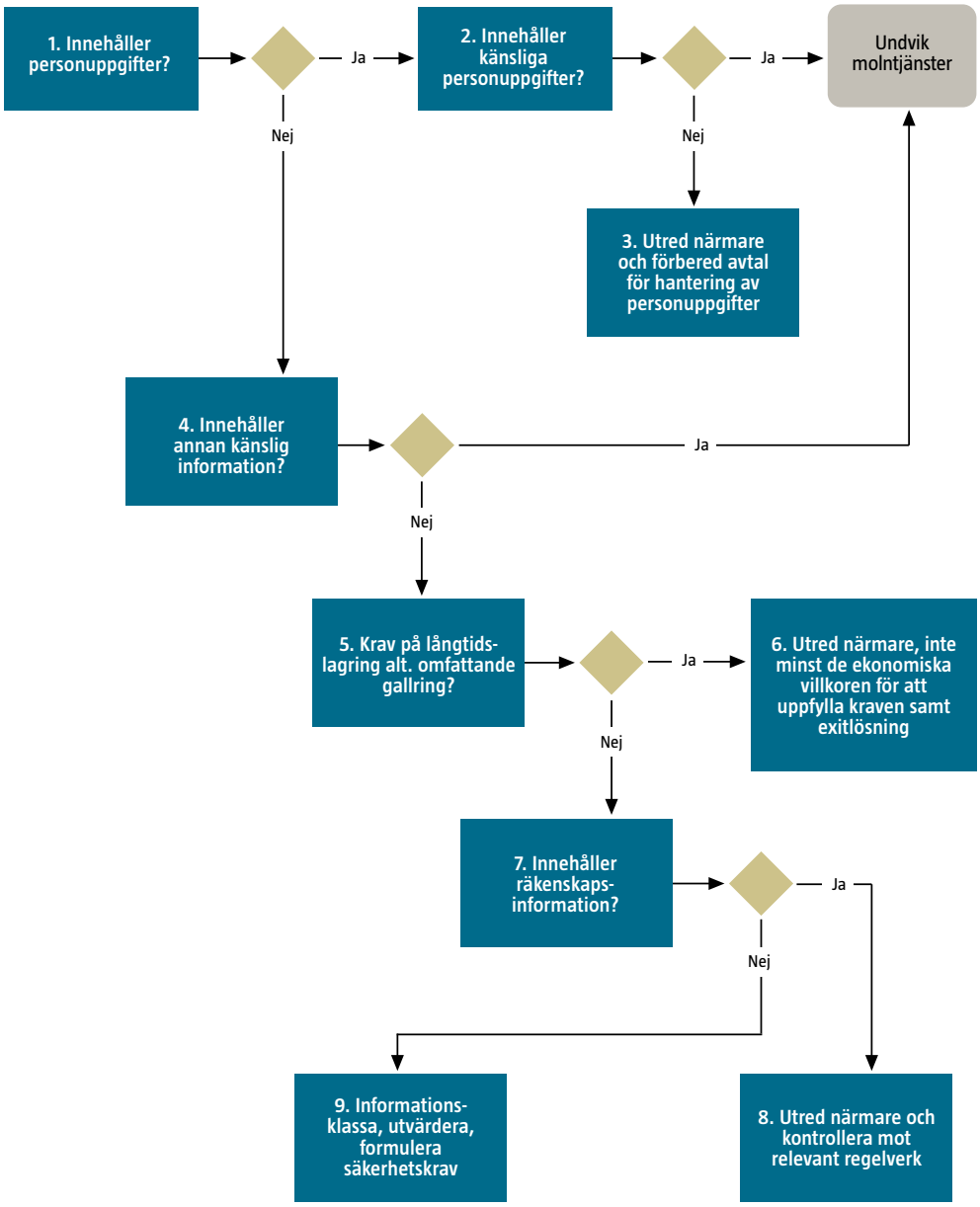
2.2.4 Fördelar och nackdelar

Liksom med uppräkningen av för- och nackdelar med drift och förvaltning i egen regi ska denna matris endast se som utgångspunkt för en djupare analys.

FÖRDELAR	NACKDELAR
Möjlighet till redundans	Beroende av internet vilket kan öka risken för obehörig åtkomst och avbrott
Ekonomi genom stordriftsfördelar	Delad miljö med okända medkunder vilket kan leda till olika hot
Hög kompetens inom säkerhetsområdet hos leverantören	Hanteras ofta internationellt vilket kan leda till bland annat oklara rättsliga förhållanden och att personuppgifter hanteras på ett olagligt sätt
Flexibelt kapacitetsutnyttjande	Kundens egen kompetens sjunker vilket kan leda till att man blir sämre beställare
Starka kravställare på underleverantörer	Risk för svårigheter att byta leverantör
Kompententa leverantörer av it-tjänster	Finns risk för otydliga ansvar och roller för säkerhet samt oklara avtalsvillkor
Förbättrad säkerhet, till exempel genom snabbare uppdateringar och bättre härdning	Sämre möjligheter för kunden att kontrollera åtkomst och efterlevnad inte minst hos leverantörens eventuella underleverantörer
	Kunden och leverantörens säkerhetslösningar kan interagera på ett negativt sätt eller vara inkompatibla
	Risk för att leverantören köps upp eller upphör vilket kan leda till att avtalsvillkor inte längre gäller eller ett akut återtagande av information/tjänst till kunden

2.2.5 Liten lathund för riskanalys av molntjänster

Molntjänster är fortfarande en relativt ny typ av tjänst för många organisationer. Med tanke på detta har denna enkla lathund tagits fram för att ge ett stöd för att inleda en riskanalys inför en upphandling där molntjänster är ett alternativ.



Figur 2: *Översiktlig lathund kring säkerhet i molntjänster.*

Sammanfattningsvis kan sägas att molntjänster kan vara ett bra alternativ för en organisation med höga krav på tillgänglighet men där informationen inte är känslig när det gäller konfidentialitet, riktighet och spårbarhet. För en organisation i snabb tillväxt och därmed snabbt ökande behov av it-kapacitet kan användningen av publika molntjänster framstå som den mest fördelaktiga lösningen. Rekommendationen är dock att göra en noggrann riskanalys innan beslut tas om att inleda upphandling av molntjänster.

Att upphandla på ett säkert sätt

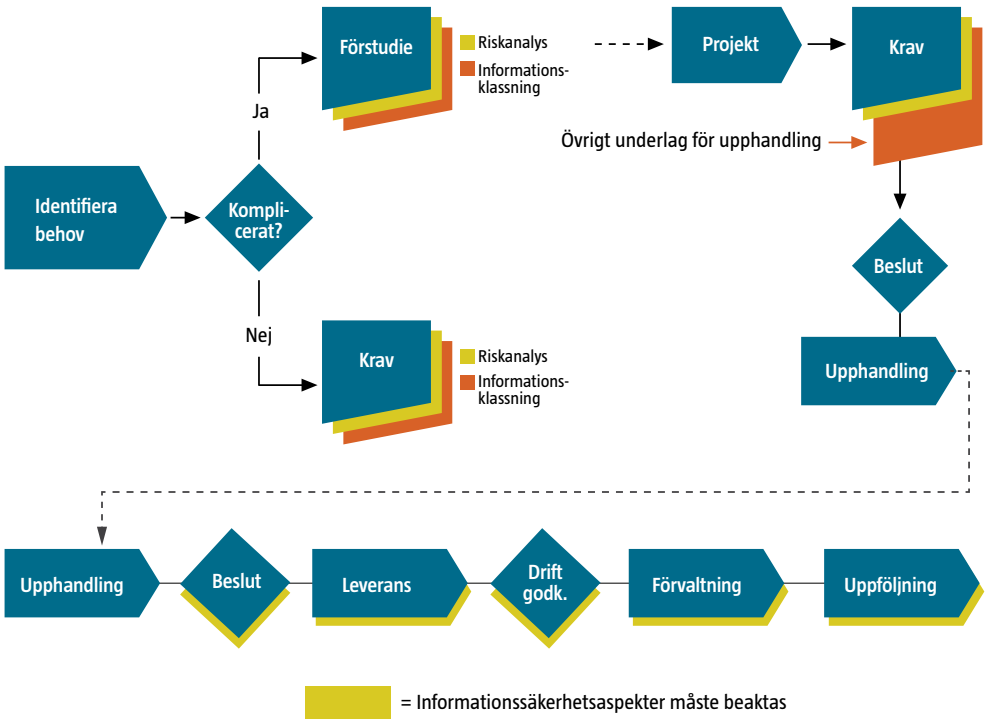
3. Att upphandla på ett säkert sätt

I en upphandling av it-relaterade tjänster måste utgångspunkten vara att identifiera vilken funktion kunden vill ha, det vill säga en insikt om att upphandlingen inte automatiskt innebär att köpa ett visst system eller en viss tjänst. Det innebär också att den funktion som behovsanalysen pekar på noggrant måste definieras. Däremot bör funktionen inte beskrivas i tekniska detaljer eftersom det kan leda till att bra lösningar som kunden inte känner till utesluts ur upphandlingen. Öppenhet måste också råda om att en outsourcing inte innebär att funktionen kommer att fungera på exakt samma sätt som tidigare. Kunden måste alltså styra processen för upphandlingen så att man får den funktionalitet som efterfrågas, men vara öppen för att detta sker med en annan lösning än den som kunden hade då t.ex. driften sköttes i egen regi. Detta resonemang gäller i hög grad också då kraven på informationssäkerhet ska formuleras. Kraven på informationssäkerhet ska vara mycket tydliga gällande vilken nivå av säkerhet som ska levereras men behöver inte gå in på exakt hur detta ska uppnås av leverantören.

En inledande diskussion måste också föras kring vad det är som ska upphandlas; är det ett system som ska driftas i kundens egen miljö, en molntjänst eller är det någon form av outsourcing? I vissa fall kan olika lösningar accepteras, till exempel kan en kund vara öppen för att den nya funktionen för registrering av frånvaro antingen sköts via ett system i den egna miljön eller som en tjänst. Vilka alternativ som är både möjliga och önskvärda måste klarläggas redan från början eftersom det påverkar hela upphandlingens upplägg.

Det är ofta en god idé att vid större upphandlingar göra en initial marknadsanalys för att få en uppfattning om vilka tjänster och leverantörer som verkar inom det aktuella området. Den som är ansvarig för att bevaka informationssäkerhetsfrågorna vid upphandlingen har all anledning att sätta sig in i hur olika leverantörer presenterar sitt utbud även ur denna aspekt. En väl genomförd marknadsanalys ger upphandlingen rätt inriktning och innebär att upphandlingen snabbare kan slutföras utan att avkall görs på kvaliteten.

Oavsett vad som ska upphandlas finns det ett antal aktiviteter som bör genomföras. Omfattningen av aktiviteterna styrs av omfattningen på upphandlingen; är det ett mindre, alternativt mindre känsligt, system eller tjänst som ska upphandlas kan aktiviteterna genomföras på ett enklare sätt. Varje organisation bör dock ha en beslutad upphandlingsprocess där det ingår säkerhetsåtgärder som alltid till genomförs. På nästa sida finns en bild som beskriver en generisk upphandling i processform där aktiviteter där informationssäkerhetsaspekter särskilt måste beaktas är markerade.



Figur 3: *Gör rätt - hela processen*

De interna rollerna i upphandlingsprocessen bör också vara tydligt definierade med sina respektive ansvar.

I fortsättningen av detta kapitel kommer ett antal centrala aspekter vid upphandling av it-relaterade tjänster att diskuteras.

3.1 Ansvar och roller

En outsourcing eller upphandling av molntjänster innehåller ett antal roller och ansvar som ska definieras i ett tidigt skede. För det första är det relationerna inom den upphandlande organisationen, och för det andra är det relationen mellan kunden och leverantören samt dennes underleverantörer.

De interna relationerna bör, när det gäller informationssäkerhet, utgå från informationsägaren. Informationsägare är den funktion som har ansvar för den verksamhet vars information ska hanteras. Eftersom skadeverkningarna av bristande säkerhet uppstår hos informationsägaren är det informationsägaren som måste bedöma risker och ställa krav bland annat genom informationsklassning.

Det måste också i fallet molntjänst eller liknande lösning klarläggas vem i organisationen som ska agera som beställarfunktion i förhållande till leverantören, dvs. systemägaren. Inom organisationen bör det finnas en tydlig beskrivning hur dessa roller ska samverka under hela den tid som upphandling, leverans, förvaltning och avveckling varar.

Grundläggande för en affärsrelation är att kunden har ett antal krav som ska tillgodoses genom leverantörens utbud. När det gäller it-relaterade tjänster blir ansvarfördelningen för informationssäkerhet en central fråga. Relationen mellan kund och leverantör måste bygga på både en gemensamt accepterad ansvarsmodell av typen som den ovan beskrivna med informationsägare och systemägare och på ansvaret för konkreta säkerhetsåtgärder. Exempel på sådana säkerhetsåtgärder kan vara loggning, behörighetshantering, incidenthantering och kontinuitetshantering. När avtal sluts ska det också klart framgå vilken av parterna som har ansvar för arkivering och gallring samt att leverantören är personuppgiftsbiträde om lösningen hanterar personuppgifter. Aktuell information kring kraven på hantering av personuppgifter finns på Datainspektionens webbplats[7].

Slutligen är en viktig aspekt de förväntningar som kunden har på rapportering i säkerhetsfrågor, inklusive incidentrapportering, och vem eller vilken funktion som är kontaktpunkten för frågor rörande informationssäkerhet. Även detta ska dokumenteras i avtalet.

Att utreda ansvar och roller för informationssäkerhet är lika viktigt att göra också i de relationer som inte är av kommersiell karaktär, som till exempel i partnermoln eller i myndigheters gemensamma servicecenter.

3.2 Beställarkompetens

För att kunna genomföra en upphandling av de tjänster som är aktuella här krävs i de flesta fall en komplex beställarkompetens inför själva upphandlingen som omfattar bland annat följande kompetensområden:

- Verksamhetskompetens för att identifiera krav och behov
- Säkerhetskompetens för att bedöma risker och kunna ställa rätt säkerhetskrav
- It-kompetens för att göra bedömningen hur tjänsterna ska kunna integreras på lämpligt sätt i befintlig infrastruktur
- Upphandlingskompetens för att upphandlingen ska avslutas med ett affärsmässigt och verksamhetsmässigt fungerande avtal
- Juridisk kompetens för att fastställa de rättsliga förutsättningarna och kraven och se till att dessa uppfylls
- Arkiv- och informationshanteringsinriktad kompetens för att kunna beskriva informationshanteringsprocesser, krav på gallring och arkivering med mera.

Det är viktigt att betona att ovan nämnda kompetens behövs redan på ett tidigt stadium i processen. Bland annat kraven på informationssäkerhet och de legala kraven kan påverka de grundläggande förutsättningarna för upphandlingen.

Beroende på upphandlingens inriktning kan det behövas kompetens även i ett internationellt perspektiv. Många av de större leverantörer som verkar på den svenska marknaden är multinationella och därför gäller det att tidigt utreda om detta kan få någon inverkan på upphandlingen. Om en molntjänst används är det inte alls säkert att informationen kommer att hanteras inom Sveriges eller

7. http://www.datainspektionen.se/

EU:s gränser, vilket kan ha avgörande betydelse då det gäller exempelvis hantering av personuppgifter.

Som tidigare påpekats upphör inte behovet av beställarkompetens då själva upphandlingen har avslutats. Eftersom det är kontinuerligt levererade tjänster kommer det att behövas en fast funktion hos kunden som har ansvar för relationen med leverantören. Detta innebär bland annat att utgöra en kontaktpunkt i informationssäkerhetsfrågor och säkerställa att kraven inom detta område uppfylls.

3.3 Säkerhetsaktiviteter i projektmodell

De flesta större upphandlingar sker idag i projektform. Det är därför viktigt att se till att väsentliga säkerhetsaktiviteter ingår i den projektmodell som används av kundens organisation. Grundläggande här är att definiera ansvar och roller, genomföra riskanalys och informationsklassning samt säkerställa att tillräcklig säkerhetskompetens finns i projektet. När det gäller riskanalys kan det vara bra att poängtera att det är en riskanalys inriktad på informationssäkerhetsaspekter, inte den riskanalys som ofta sker för projektets genomförande.

I projektmodellen är det viktigt att ta med när leveransgodkännande ska ske och vilken instans som får besluta om avvikelser från bland annat säkerhetskrav.

3.4 Riskanalys

För att få en första uppfattning om vilka krav som ska ställas på den funktion som ska upphandlas är det viktigt att göra en riskanalys. Riskanalysen bör inledas med att kartlägga vilken roll systemet eller tjänsten ska ha i organisationen samt vilka interna och externa intressenter som finns till lösningen när den är i drift. För att kunna göra riskanalysen krävs därför att man översiktligt beskriver vilken information som ska hanteras och på vilket sätt[8]. Vissa aspekter bör säkerställas initialt eftersom de är avgörande för vilka lösningar som är möjliga, som till exempel:

- Innehåller informationen personuppgifter? Om ja, är dessa uppgifter att betrakta som känsliga personuppgifter?
- Kan lösningen komma att hantera information som påverkar rikets säkerhet?

Om lösningen är tänkt att hantera denna typ av information kommer det att finnas särskilda säkerhetskrav i lagstiftning som redan från början kan utesluta vissa typer av lösningar som exempelvis molntjänster. Detta leder till att upphandlingen får en tydligare inriktning och att kommunikationen både internt och externt blir bättre.

Därefter identifieras de hot som tjänsten eller systemet kan utsättas för och vilka konsekvenser dessa hot kan få om de förverkligas. Slutligen bedöms sannolikheten för att hoten förverkligas. För att få ett bra beslutsunderlag bör riskanalysen genomföras av riskägaren (informationsägaren), dvs. den funktion som äger verksamheten och informationen som ska hanteras i den potentiella lösningen. Om det är flera informationsägare som ska använda lösningen bör samtliga delta

8. Se MSB:s vägledning Processorienterad informationskartläggning, https://www.msb.se/sv/Start1/Nyheter-fran-MSB/Nyheter/Vagledning-for-processorienterad-informationskartlaggning/

i riskanalysen. Riskanalysen ska genomförs innan en eventuell projektstart så att den kan ingå som underlag för ett projektdirektiv eller motsvarande beställningsdokument.

Ytterligare ett skäl att lägga riskanalysen utanför projektfasen är att det då är lättare att bibehålla analysens inriktning på informationssäkerhetsrisker i den planerade lösningen. Om riskanalysen istället genomförs efter projektstart finns det en tendens till sammanblandning mellan risker i den tänkta lösningen och risker för projektets genomförande. Det kan även vara svårt att få engagemang från riskägaren när projektet startat och beställningen är gjord.

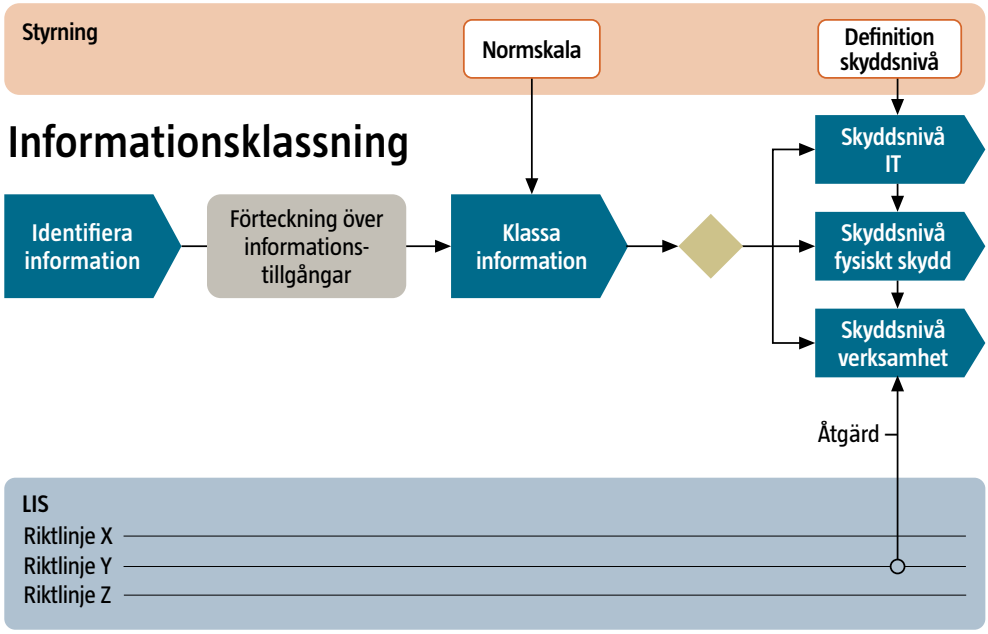
En deltagare som bör vara med i riskanalysen är den funktion som är ansvarig för förvaltningsfasen eftersom även långsiktiga risker måste kunna identifieras.

För att riskanalysen ska kunna fungera som ett bra beslutsunderlag krävs kompetens både i metod och inom informationssäkerhetsområdet. Därför bör organisationens säkerhetsfunktion stödja riskanalyser både med metoder och med kompetens rörande hot, risker och säkerhetsåtgärder. På så sätt får organisationen ett mer systematiskt informationssäkerhetsarbete med samordnade riskbedömningar och god kommunikation mellan verksamhet och säkerhetsorganisationen.

När avslut börjar närma sig för upphandlingen och aktuella leverantörer finns bör riskanalys även genomföras för varje leverantör. Ett särskilt riskområde är då leverantören använder underleverantörer. Detta förhållande kan vara svårt att kontrollera för kunden och därmed blir det svårt att försäkra sig om att de säkerhetskrav som har ställts i det kommande avtalet verkligen kommer att överföras till underleverantörer. Som presumtiv kund bör man skaffa sig en bild av den kedja av aktörer/aktiviteter som leder fram till den slutgiltiga leveransen av tjänsten för att kunna göra en relevant riskbedömning. Om något led i kedjan verkar oklart bör man begära in ytterligare information, t.ex. avtalsvillkor mellan leverantör och underleverantör som kan påverka säkerheten. Det kan även gälla om exempelvis lagring av information sker inom annan jurisdiktion.

3.5 Informationsklassning

I anslutning till den övergripande riskanalysen bör en informationsklassning genomföras. Klassningen kan ses som en mer detaljerad riskanalys där det också bör ingå fördefinierade skyddsåtgärder beroende på vilka konsekvenser som kan bli en följd av att ett hot förverkligas. I en klassning ingår ett antal aktiviteter som att identifiera information, klassa den och besluta vilken skyddsnivå informationen ska hanteras i. Klassningen ska bedöma konsekvenser vid bristande konfidentialitet, tillgänglighet, riktighet och spårbarhet.

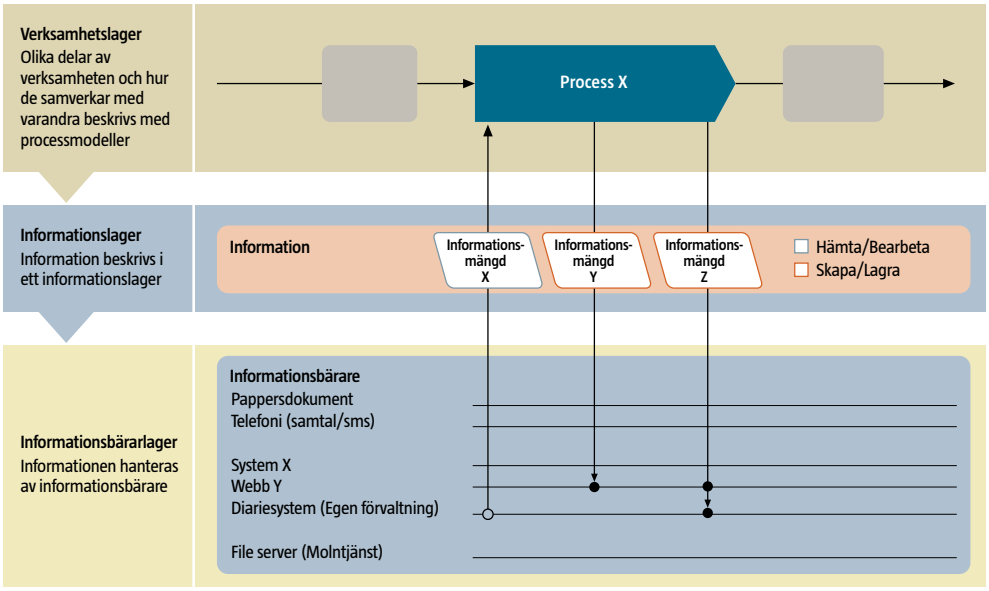


Figur 4: *Informationsklassning*

Lämpligen görs informationsklassningen i form av en processkartläggning för att också få informationen i den tänkta lösningen i sitt rätta sammanhang för att se vilka resurser som används för olika aktiviteter i processen. I bilden beskrivs hur verksamhetens processer är beroende av information och bärare som it-system och it-tjänster. I processbilden går det att identifiera vilka informationsmängder som är aktuella och vilka resurser som krävs för att hantera dem[9].

På en övergripande nivå kan man se förhållandet mellan verksamhet, information och bärare enligt figur 5 på nästa sida.

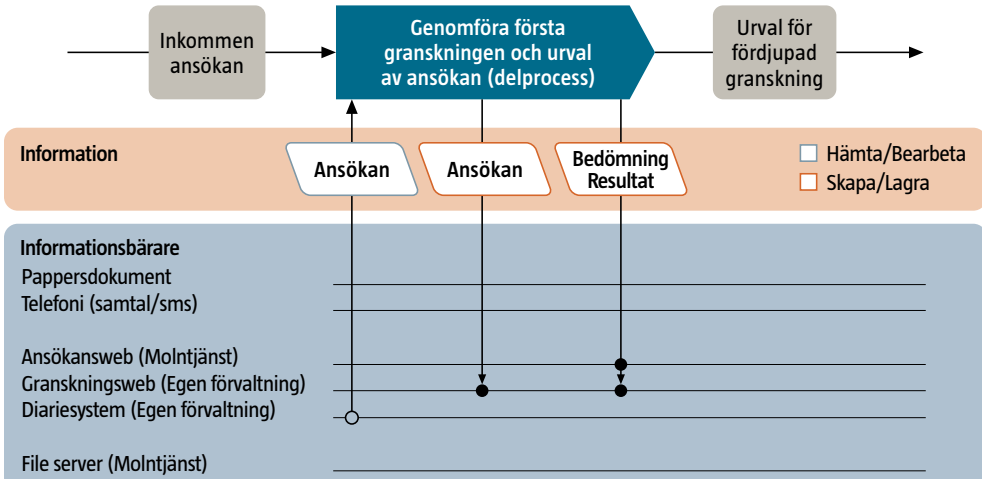
9. Se MSB:s vägledning Processorienterad informationskartläggning, https://www.msb.se/sv/Start1/Nyheter-fran-MSB/Nyheter/Vagledning-for-processorienterad-informationskartlaggning



Figur 5: *Verksamhetsprocesser och informationshantering*

Det är alltså i verksamhetslagret som det går kartlägga kravställningen och den information som används i processen vilket i sin tur skapar kraven för den it-relaterade tjänst som ska upphandlas.

Ett mer konkret exempel kan se ut som i figur 6 nedan.



Figur 6: *Utlysa och tilldela forskningsmedel (process)*

Var i processen en viss aktivitet utförs påverkar också möjligheten till att outsourca alternativt använda en molntjänst för resurser som används för aktiviteten. Om ett system eller tjänst är mycket komplext integrerat i organisationens egen infrastruktur kan det vara svårt att lyfta ut den till en extern leverantör.

Informationsklassning, rätt genomförd, ger också ett underlag för att specificera vilka åtgärder kundens organisation behöver vidta i både kortare och längre perspektiv. Beställarorganisationen måste finnas på plats inte bara för den initiala beställningen utan under hela tiden som relationen med den utomstående parten varar. Se mer om detta under avsnitt 3.9 om förvaltningsfasen. Riskanalys tillsammans med informationsklassning ger också en uppfattning om behovet av kontinuitetsplanering.

Den organisation som har infört en informationsklassningsmodell med definierade skyddsnivåer kommer att ha en stor del av kravspecifikationen ordnad när klassningen är genomförd. De definierade skyddsnivåerna ger också underlag för en enhetlig säkerhetsarkitektur där egna system och externa tjänster kan integreras på ett väl fungerande sätt.

3.6 Kontinuitetshantering

Oavsett vilken variant av upphandling av it-stöd som genomförs är den beställsande organisationen alltid ansvarig för att upprätthålla sin egen verksamhet även då avbrott eller störningar sker. Metoden för att klara detta brukar kallas kontinuitetshantering.

Kontinuitetshantering handlar om en organisations förmåga att kunna upprätthålla sina centrala processer även under svåra förhållanden. För att klara det behövs framförallt en god kännedom om vilka de viktigaste processerna är och vilka resurser som är nödvändiga för att upprätthålla dem. Informationshantering är en avgörande resurs för de flesta verksamhetsprocesser. Av den anledningen förutsätter en fungerande kontinuitetshantering en beskriven koppling mellan verksamhetsprocesser och informationshantering. Tidigare har en organisation i hög grad kunnat skapa sin egen it-infrastruktur. Nu skapas en organisations infrastruktur förutom av de egna systemen och tjänsterna även av resurser som tillhandahålls av utomstående parter. Därmed måste en kontinuitetshantering byggas upp kring en förståelse av hur de egna resurserna samverkar med utomstående tjänster.

Förståelsen skapas enklast genom att göra processorienterade informationskartläggningar för processer som en aktuell upphandling påverkar. Ur denna kartläggning kan sedan krav på återställning tas fram som både påverkar upphandlingen men även den egna organisationens interna planering.

Kraven på leverantören är till exempel väl definierade återställelsetider (dvs. hur snabbt tjänsten eller systemet ska fungera normalt igen efter avbrott), deltagande i kundens egna övningar och att leverantören visar upp sina egna dokumenterade kontinuitetsplaner.

Hur väl kraven på upprätthållande av kontinuitet än ställs måste kunden ändå vara medveten om att det kan uppstå längre avbrott i leveransen. Det kan gälla vid större naturolyckor som översvämning eller storm som påverkar leverantörens möjlighet att leverera, men också genom att leverantören vid en större incident gör en prioritering av kunder. Oavsett orsak måste den beställande organisationen ändå ha en plan för hur ett längre avbrott ska hanteras.

Om en verksamhet har sådana krav på t.ex. tillgänglighet att längre avbrott inte kan accepteras bör man noga överväga om outsourcing alls är möjligt. För myndigheter kan samverkan med andra myndigheter vara ett alternativ.

3.7 Kravställning

De centrala verktygen för att fastställa kraven för it-relaterade tjänster är riskanalys och informationsklassning eftersom tjänsterna måste uppfylla organisationens allmänna säkerhetskrav. Den upphandlande organisation som har definierade skyddsnivåer i sin modell för informationsklassning har en klar fördel eftersom innehållet i aktuella skyddsnivåer då kan omvandlas till en kravbild för externa leverantörer.

Ett generellt krav är att leverantören ska kunna erbjuda sitt utbud på olika skyddsnivåer. Det innebär en möjlighet för kunden att göra en bedömning mellan risk och kostnad. Att leverantörerna kan erbjuda olika skyddsnivåer är också betydelsefullt eftersom kundens användning av tjänsten kan förändras över tid och vid en förnyad informationsklassning kan kraven höjas eller sänkas. Om leverantören endast kan tillhandahålla en skyddsnivå alternativt göra unika lösningar för en kund finns en överhängande risk för att kunden antingen blir tvungen att byta leverantör eller behöva betala för en egen anpassning av tjänsten.

Villkor som att leverantören ska följa ISO-standarden för informationssäkerhet, ISO/IEC 27001 och 27002, bör ingå i kravställningen. Att leverantören följer ISO-standarden (eller eventuellt någon annan standard) ska dock inte överskattas som säkerhetshöjande effekt. Standarderna beskriver inte exakta skyddsnivåer utan snarare arbetssätt och metoder, vilket däremot kan ge ett underlag för en bra kommunikation mellan kund och leverantör. När en leverantör använder standarder för styrning av sitt arbete med informationssäkerhet ger det en tydlig indikation om att man har prioriterat frågan. En certifiering kan ytterligare stärka intrycket av en säkerhetsmedveten leverantör som har inkluderat informationssäkerhet i sin affärsmodell.

Kunden bör också ställa krav på andra organisatoriska förutsättningar som rapportering, en särskilt utpekad kontaktperson för informationssäkerhetsfrågor och möjlighet till olika former av granskningar av leverantörens säkerhetsarbete. Av särskild betydelse är att reglera rapportering av incidenter.

Utöver detta finns ett antal konkreta säkerhetskrav som bör ha genererats via informationsklassning som till exempel:

- Hur åtkomst ska styras till informationen
- Vilken typ av spårbarhet som ska finnas

- Hur loggning ska ske och hur loggar ska granskas
- Åtkomst till relevant dokumentation hos leverantören som påverkar leveransen
- Krav på tillgänglighet i tjänsten
- Vilka återställelsetider som leverantören måste uppfylla vid avbrott
- Krav på säkerhetskopiering
- Hur incidenter ska rapporteras och hanteras
- Vilken support leverantören ska kunna tillhandahålla
- Vilka anställningskontroller som leverantören ska genomföra för de anställda som får tillgång till kundens information
- I vilken omfattning leverantören får anlita underleverantörer och vilka krav som ska ställas på dessa
- Hur överföring av information ska ske mellan leverantör och kund
- Krav på att leverantören ska redovisa sin säkerhetsorganisation och sin kontinuitetshantering samt planering för att undvika nyckelpersonberoende
- Vid behov, rutiner för gallring och metoder för arkivering
- Möjlighet för kunden att initiera externa revisioner av leverantören

Ett moment som ofta underskattas är kvalificeringen av den kravlista som har kommit fram. De krav som har formulerats måste prioriteras men också analyseras närmare. Vilka krav kan ställas som skall-krav och vilka är bör-krav? Vilka krav kan anges exakt och vilka krav bör lämna öppet för anbudsgivare att presentera egna lösningar? Inom it-området liksom inom informationssäkerhetsområdet finns en fälla i att alltför snävt ange exakta tekniska lösningar som krav. Att vara alltför precis är en nackdel eftersom det dels förhindrar att leverantörer erbjuder andra likvärdiga eller bättre lösningar, dels skapar en kravbild som snabbt blir föråldrad.

I vissa fall bör dock kraven vara mer preciserade. Ett sådant exempel är loggning där det bör beskrivas vilka loggar och vilken statistik som kunden ska ha tillgång till. Ett annat är hur incidentrapportering ska ske. Ytterligare en punkt där konflikter kan uppstå är kundens åtkomst till relevant dokumentation hos leverantör. I detta sammanhang bör det beskrivas hur kunden ska få tillgång till information om loggar, incidenter och dokumentation. Det kan t.ex. gälla att kunden ska få kopior av dokumentation och inte endast ha möjlighet att ta del av information hos leverantören.

Generellt gäller att då molntjänster eller outsourcinglösningar ska inhandlas kan det leda till större förändringar i informationshanteringen eftersom vinsten med dessa tjänster bygger på större, hårt standardiserade lösningar. De krav som ställs ur informationssäkerhetssynpunkt måste ta hänsyn till detta och utformas så att de kan tillämpas i ett stort spann av tänkbara lösningar.

3.8 Utformning av avtal

Ett väl utformat avtal är förutsättningen för att få en fungerande relation mellan kund och leverantör. Avtalet ska i detta sammanhang ses som befästandet av att leverantören förbinder sig att uppfylla de säkerhetskrav kunden har. En självklarhet som alltför många kunder inom det här området bortser ifrån är att avtalet beskriver det man har kommit överens om och att kunden inte kan förutsätta att det finns underförstådda leveranser. Står det inte i avtalet att incidenter ska rapporteras i dokumenterad form en gång i månaden kan inte kunden kräva detta utan extra kostnad. Har inte parterna i avtal kommit överens om vilka typer av granskningar som kunden får initiera så kan leverantören motsätta sig detta utan att kunden har någon större chans att påverka beslutet. Avtalet bör därför så tydligt som möjligt beskriva överenskommelser som har ingåtts för hela leveransens livscykel för att konflikter och oväntade kostnader inte ska uppstå.

Även i partnermoln och i privata moln måste det finnas dokumenterade överenskommelser som beskriver olika förutsättningarn för användningen av tjänsterna.

Utöver rena säkerhetskrav bör följande områden regleras i avtal:

- Klarläggande av ansvar och roller med krav på leverantörens ansvarstagande.
- Krav på hantering av personuppgifter, bl .a. att hantering av personuppgifter inte får ske utanför EES-området. Kräver också att ett skriftligt avtal upprättas med såväl molnleverantören som eventuella underleverantörer innehållande instruktioner om hur personuppgiftshanteringen ska gå till.
- Krav på hur leverantören i sin tur kan använda underleverantörer.
- Krav på arkivering, avveckling, migrering och exitlösning.
- Krav på beställningsformer, exempelvis utifrån avropsförfarande.
- Krav på flexibilitet, dvs. möjlighet för kunden att skala upp sin användning av tjänsten på ett ekonomiskt fördelaktigt sätt.
- Krav på användning av licenser och immateriella rättigheter.
- Krav på hur en eventuell tvistelösning ska ske, inte minst vilket lands lagstiftning som ska gälla.

Kunden bör se till att samtliga relevanta avtalsfrågor klargörs i avtalet och inte skjuts på framtiden då detta kan skapa osäkerhet kring vad som egentligen gäller. Leverantören ska inte heller ha rätt att ensidigt ändra i tjänstespecifikationen.

Leverantören erbjuder ofta standardavtal, något som kan förefalla bekvämt för kunden. Dessutom finns det av naturliga skäl i de allra flesta fall en större erfarenhet hos leverantören än hos kunden när det gäller att paketera tjänster till fungerande helheter. Trots detta bör kunden vara ytterst restriktiv med att anta en leverantörs standardavtal eller avtalsmallar som underlag för det gemensamma avtalet. Leverantörens avtalsformer är utformade för att gynna leverantörens affär och affärsmodell vilket inte alltid överensstämmer med kunden intresse.

Avtalet bör även innehålla villkor för vad som kan leda till att det kan brytas i förtid av kunden. Ur informationssäkerhetssynpunkt är det viktigt att öppna för möjligheten att bristande uppfyllnad av kraven på informationssäkerhet kan

leda till uppsägning i förtid. I detta sammanhang är det också centralt att beskriva hur leveransgodkännande ska ske, dvs. vilka krav som måste vara uppfyllda för att leveransen ska anses som genomförd.

Även om kunden lyckas upprätta ett bra avtal så ska risken för att leverantören av någon anledning lägger ner sin verksamhet eller blir uppköpt beaktas. Likaså är det en lämplig säkerhetsåtgärd att sondera till vilka målgrupper olika leverantörer vänder sig och om möjligt även vilka kunder som redan använder aktuella leverantörer. Detta kan ge en uppfattning om i vilket sällskap man som kund kan hamna och vilka eventuella risker detta skulle kunna innebära.

I vissa fall kan leverantören ställa krav ur säkerhetssynpunkt på kunden eftersom en kunds bristande säkerhet skulle kunna äventyra säkerheten för andra kunder. Det kan omfatta krav på visst skydd mot skadlig kod, viss brandväggskonfiguration eller viss behörighetshantering. Har leverantören denna typ av krav ska det framgå i avtalet.

3.9 Överlämnande till förvaltning

Redan tidigt under upphandlingen bör det beskrivas hur den upphandlade lösningen ska överlämnas till förvaltning. Som tidigare påpekats krävs en beställarorganisation i förvaltningsfasen som ska utgöra kontaktpunkt i relationen mellan kund och leverantör.

Molntjänster och outsourcing handlar ofta om längre åtaganden från leverantörens sida som inte heller är enkla att snabbt lämna för kunden. Det innebär att det kommer att ske ett stort antal förändringar som påverkar relationen. Teknisk utveckling erbjuder nya möjliga lösningar och förändringar i kundens verksamhet och information leder till nya kravbilder till exempel. Dessa förändringar ska hanteras på ett långsiktigt sätt, vilket ställer krav på en kontinuerlig organisation för förvaltningsfrågor hos kunden. Denna organisation bör vara definierad så tidigt som möjligt i upphandlingsprocessen eftersom det är den som kommer att få hantera leveransen.

Ansvariga för förvaltning är viktiga kravställare på den levererade lösningen och bör därför ha en central roll i leveransgodkännandet.

3.10 Uppföljning

Som tidigare framgått leder upphandlingen fram till en längre relation som ska styras av kunden. Som underlag för styrningen krävs en strukturerad uppföljning som kan bestå av rapportering på olika nivåer, intern och extern efterlevnadskontroll samt gemensam utvärdering. I uppföljningen ska även kontroll av att överenskomna säkerhetsaktiviteter fullföljs ingå. Grundprincipen är att kunden ska säkerställa sin egen möjlighet till administrativa och tekniska kontroller i den omfattning som tjänstens omfattning och/eller känslighet kräver.

Uppföljningen bör sättas i ett större sammanhang enligt modellen plan-do-check-act så att den kan utgöra grund för ständiga förbättringar både hos kund och leverantör.

Definitioner

4. Definitioner

BEGREPP	DEFINITION
Avveckling	Process som syftar till att minska eller avskaffa informationsbehandlingsresurser på ett definierat sätt
Drift	Kontinuerlig verksamhet som innefattar åtgärder vilka syftar till att upprätthålla funktionen hos ett förvaltningsobjekt
Förvaltning	Åtgärder för att säkerställa en regelbunden skötsel av ett objekt, så att förändringar styrs och samordnas
Incident	Oönskad och oplanerad händelse som kan få allvarliga konsekvenser
Information	Innebörd hos data
Informationsklassning	Att genom konsekvensanalys identifiera skyddsbehovet för en viss informationsmängd
Informationsmängd	Mängd information som är avgränsad för ett visst ändamål
Informationssystem	System som behandlar, dvs. insamlar, bearbetar, lagrar och distribuerar information
Informationssäkerhet	Tillstånd som innebär skydd med avseende på konfidentialitet, riktighet, tillgänglighet och spårbarhet hos information
Informationsägare	Person eller enhet som har ansvaret för den information som skapas och hanteras inom den egna verksamheten
It-incident	Oönskad och oplanerad it-relaterad händelse som kan påverka säkerheten i en organisation eller i samhällets informationshantering och som kan innebära en störning av organisationens förmåga att bedriva sin verksamhet
It-relaterad tjänst	I denna vägledning avses upphandling av: It-system Outsourcing av it-relaterade tjänster Molntjänster

It-system	Informationstekniskt system
It-säkerhet	Säkerhet beträffande it-system med förmåga att förhindra obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning vid databehandling samt dator- och telekommunikation
Kontinuitetshantering	Planering för att en verksamhet trots störning ska kunna leverera de tjänster och produkter som anses viktigast
Molntjänst	Molntjänst är en teknik där resurser, som till exempel processorkraft, lagring och funktioner, tillhandahålls som tjänster via internet. Tjänsten kategoriseras oftast som någon av tre olika typer av tjänster: *SaaS (Software as a Service)* Mjukvara som tjänst Denna tjänstetyp kan levereras på flera sätt, t.ex. direkt mot användare eller mot företagets interna nätverk. Leverantören står för underhåll Multitenancy, flera kunder på samma instans av mjukvaran. Kan medföra problem vid uppdateringar *PaaS (Platform as a Service)* Utvecklingsmiljö som tjänst. Denna typ av tjänst liknar IaaS med skillnaden att man använder sig av en typ av ramverk där man kan köra eller utveckla nya systemer. Det kan liknas med en utvecklingsplattform Utöver att PaaS håller OS uppgraderat, så erbjuder det utvecklare att arbeta på projekt i samma plattform även då de kan vara geografiskt utspridda *IaaS (Infrastructure as a Service)* Infrastruktur som tjänst. Här menas fysisk hårdvara såsom servrar, lagringsutrymme, arkitekturiell uppbyggnad, lastbalansering, etc
Outsourcing	Utkontraktering av en it-relaterad tjänst som tidigare utfördes internt, till en extern leverantör
Risk	Kombination av sannolikheten för att en incident ska inträffa och konsekvenserna av en sådan händelse
Riskanalys	Identifiering och värdering (med hjälp av riskvärden) av hot mot en viss verksamhet för att kartlägga vilka risker verksamheten är utsatt för

System	Uppsättning samverkande program för användare, operativsystem, databaser, serverbaserade program samt program för datakommunikation, datasäkerhet och annat som tillsammans kan användas för att utföra arbetsuppgifter. Även maskinvara ingår i datasystemet
Systemägare	Person eller enhet som har det övergripande ansvaret för ett it-system
Utveckling	Systematisk metod för att införa nya funktioner eller förbättra befintliga

Bilaga

Att avropa från Kammarkollegiets ramavtal

Om möjligheterna att vid avrop från vissa ramavtal ställa krav i enlighet med MSB:s Vägledning – informationssäkerhet i upphandling – Informationssäkerhet i upphandling av system, outsourcing och molntjänster. Här ges två exempel på hur detta kan göras: E-förvaltningsstödjande tjänster (EFST) och IT-driftstjänster.

De bägge ramavtalsområdena har sinsemellan olika innehåll och utgångspunkter och även ansatser för att säkra en bra kravställning inom området informationssäkerhet.

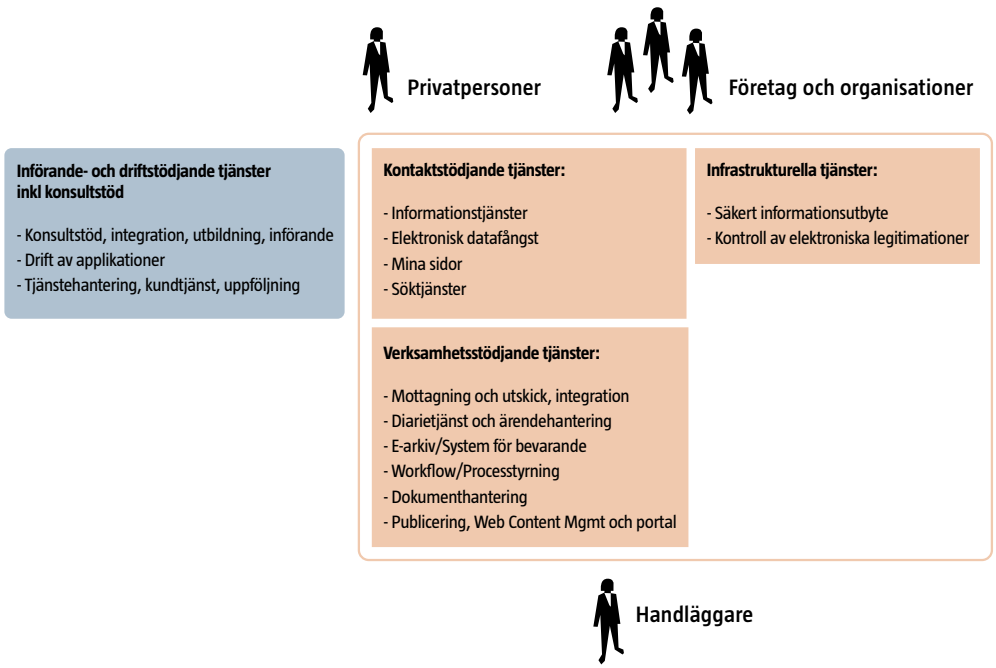
Ramavtalsområdet E-förvaltningsstödjande tjänster

Från ramavtalet kan funktioner avropas

Upphandlingens fokus ligger på funktionell nivå. Krav på tjänsterna ställs på en funktionell generell och övergripande nivå. Krav ställs på säkerhet, användbarhet, interoperabilitet och kostnadseffektivitet. Ramavtalsleverantören får ansvaret att utforma tjänsterna så att avtalade funktioner och tjänstenivåer uppfylls. Leverantören äger i normalfallet och underhåller den bakomliggande tekniska plattformen.

Den avropande organisationen kan utgå från verksamhetens behov och kan lämna utformningen och hantering av den tekniska lösningen och plattformen till vald leverantör. Den avropande organisationen preciserar de i ramavtalsupphandlingen ställda kraven och ramavtalsvillkoren så att de konkreta behoven möts.

Med tjänst menas i sammanhanget en samlad tjänsteleverans. Med det avses möjlighet att avropa e-förvaltningsstödjande funktioner, med tillhörande kundtjänst, support och utbildning samt administration, uppföljning och statistik.



Stöd i Säkerhetsarbete

Ramavtalen inom E-förvaltningsstödjande tjänster omfattar även konsultstöd för säkerhetsarbete samt generella förstudier, planering, utveckling, anpassning, införande och integration inom området.

I ramavtalsupphandlingen har krav ställts på Organisation för informationssäkerhet – Ledningssystem för att skydda den avropande organisationens informationstillgångar och som kan tilldela roller för säkerhetsarbetet och samordna aktiviteter och som omfattar metoder och processer för informationssäkerhet, som riskbedömning och riskhantering.

Krav har ställts på Policy för informationssäkerhet som anger hur stöd utformats för krav enligt MSBFS 2009:10 och som omfattar principer, standarder och krav för säkerhet vid leverans av avropade tjänster.

Riskanalyser bör utgå från organisationens ordinarie informationssäkerhetsarbete. De konkretiseringar som blir aktuella vid ett avrop kan genomföras antingen innan avrop genomförs eller som något som avropas och som genomförs i samverkan med den valda leverantören. Mer övergripande analyser kan också göras innan avrop och med fördjupningar med vald leverantör. Bl a bör hantering av personuppgifter uppmärksammas.

Säkerhetsåtgärder som skydd för personuppgifter

Krav har även ställts på Säkerhetsåtgärder som skydd för personuppgifter. Sådana kan utgöras av tekniska och organisatoriska åtgärder för att säkerställa skydd av personuppgifter i enlighet med krav som personuppgiftsansvarig har att följa. De övergripande krav som ställts preciseras utifrån resultat från riskanalyserna. Inom olika funktionsområden ställs vissa mer konkreta krav. Det bör t ex finnas färdig funktion för användaren att märka personuppgifter och andra känsliga/sekretessbelagda uppgifter på fält/ord/tecken-nivå för att kunna dölja dessa vid presentation, utskrift och publicering av uppgifter (Diarietjänst och ärendehantering). Personuppgifter och andra känsliga/sekretessbelagda uppgifter bör kunna märkas och döljas vid utlämnande av allmänna handlingar (E-arkiv/System för bevarande).

Skydd av den avropande organisationens informationstillgångar

Övergripande krav på skydd av myndighetens register och viktiga informationstillgångar avseende förlust, förstörelse och förfalskning har ställts. Dessa kan preciseras utifrån resultat av genomförda säkerhetsanalyser. Krav har också ställts på hantering av informationstillgångar, att förteckning och skyddsåtgärder skall finnas för tillgångar och system.

Incidentrapportering

Rapportering av IT-incidenter av säkerhetskaraktär skall ske. Leverantören skall för tillhandahållna tjänster ha och tillämpa dokumenterade rutiner för hantering av säkerhetsincidenter som skall omfatta och definiera registrering, rapportering, prioritering, påverkan på kundens verksamhet, klassificering, uppdatering, eskalering, lösning och formell stängning av alla incidenter.

Tjänstekontinuitet och tillgänglighetshantering

Tjänstekontinuitet och tillänglighetshantering är en del av tjänstehanteringen och regleras i allmänna villkor e-förvaltningsstödjande tjänster. Det fastslås att leverantören skall ha en process för tjänstekontinuitet och tillgänglighet. Att kraven identifieras på grundval av kundernas verksamhetsplaner, överenskommelse om tjänstenivå och riskbedömningar. Tillgänglighets- och kontinuitetsplaner för tjänsten skall utvecklas och granskas minst en gång per år för att ge möjlighet att säkerställa att kraven uppfylls enligt avtal under alla omständigheter, från normal drift till långa eller allvarliga avbrott i tjänsten.

Tjänstehantering

Hantering av säkerhet ingår i den generella hanteringen av tjänsternas egenskaper. Verktyg för detta tillhandahålls genom avtalstexten om tjänstehantering. Denna är egentligen en kommunikationsmodell för att styra och hantera tjänsteleveransen från leverantören. Tjänstehanteringen bör användas med försiktighet för att inte skapa en tungrodd kommunikationsmodell som inte används. En överarbetning blir lätt kontraproduktiv. Tjänstehanteringen beskrivs i ramavtalets allmänna villkor avsnitt 3 Tjänstehantering.

Ramavtalsområdena IT-driftstjänster

Syftet med ramavtalen

Syftet med Kammarkollegiets ramavtal av IT-drift är att tillgodose myndigheternas allmänna, breda och gemensamma behov av utkontraktering av IT-drift.

I upphandlingen har krav på tjänsterna ställts på en funktionell, generell och övergripande nivå. Den avropande organisationen preciserar i avropsförfrågan kraven utifrån ramavtalens kravkatalog och de egna specifika behoven. För alla fyra ramavtalsområdena inom IT-driftstjänster finns det två kravområden avseende ”säkerhet” som myndigheten kan anpassa till det egna behoven:

1. Informationssäkerhet, utvärdering av hur leverantören avser att säkerställa konfidentialitet, integritet och tillgänglighet för tillgångar, information, data och IT-tjänster. Utöver den elektroniska hanteringen inkluderar begreppet också ”fysisk” hanteringen av papper, tillträde till byggnader, telefonsamtal etc.
2. IT Säkerhet, utvärdering av säkerhet eller säkerhetsnivåer, t ex för leverantörens datahallar, vid anslutning i myndighetens nätverk, eller kommunikationslösningar

Ramavtalsleverantören får ansvaret att utforma tjänsterna så att avtalade funktioner och tjänstenivåer uppfylls. Leverantören äger i normalfallet och underhåller den bakomliggande tekniska plattformen.

Tjänste- och ramavtalsområden

Tjänster avropas inom följande tjänsteområden (ramavtalsområden):

- Helhetsdrift
- Hosting
- På-platsdrift
- Användarnära funktioner

Helhetsdrift, en leverantör med ramavtal inom detta område ska kunna leverera allt från ett helhetsåtagande för samtliga tjänsteområden till ett delåtagande. Hosting omfattar drift och förvaltning av servers, nätverk, datalagring utanför myndigheten. Påplatsdrift omfattar driftstjänster i form av åtgärder på plats på myndigheten. Användarnära funktioner omfattar drift och förvaltning av arbetsplatser och skrivare.

Ramavtalsområdena inom IT-Drift är helt inriktade på funktionsinriktade tjänster. Med detta avses att funktionella krav ställs på leverantören, som får ansvaret att utforma tjänsterna så att överenskomna servicenivåer uppfylls.

Leveransavtal

Leveransavtalet struktur medger en stor valfrihet att utforma myndighetsspecifika bilagor. Leveransavtalet består av Leveransavtalssidan och de av följande bilagor som myndigheten väljer att inkludera. Bilagorna 3, 13, 16 och 17 är dock obligatoriska:

Bilaga 1 Syfte och mål med avtalet
Bilaga 2 Allmänna begrepp
Bilaga 3 Specifikationen (Leverantörens åtagande såsom tjänstekatalog m.m.)
Bilaga 4 Kundens åtagande samt åtkomst till kundens lokaler, utrustning etc.
Bilaga 5 Införandet (inkl. överföring av utrustning, programvara och personal)
Bilaga 6 Servicenivåavtal (även benämnt Avtal om garanterad servicenivå)
Bilaga 7 Vites- och incitamentsmodell
Bilaga 8 Samverkan och rapportering
Bilaga 9 Säkerhet
Bilaga 10 Förändringshantering
Bilaga 11 Benchmarking
Bilaga 12 Fakturerings- och beställningsrutiner
Bilaga 13 Ersättning, avgifter och betalningsvillkor
Bilaga 14 Avveckling
Bilaga 15 Konsultansvarsförsäkring (om kryss i rutan)
Bilaga 16 Tilläggsvillkor IT drift 2010
Bilaga 17 Allmänna bestämmelser IT-Drift version 2008

På Leveransavtalssidan ska myndigheten ange om säkerhetsskyddsavtal avses tecknas i ett separat avtal. Om så är fallet ska man kryssa i detta på Leveransavtalssidan. I sådana fall är Leveransavtalets giltighet och fortbestånd villkorat av att ett gällande säkerhetsskyddsavtal föreligger mellan parterna. Detta avser situationen att säkerhetsskyddsavtal ligger separat, dvs. inte att det är inkluderat i Leveransavtalet (som bilaga).

I Bilaga 9 kan parterna specificera vilka säkerhetsaspekter som avtalats att gälla under leveransavtalsperioden.

Innan ett beslut att outsourca myndighetens verksamhet rekommenderar Kammarkollegiet att myndigheten specificerar ansvar och roller samt genomför en outsourcingstrategi inkluderande riskanalys med informationsklassning och kontinuitetsplanering utifrån MSBs Vägledning – informationssäkerhet i upphandling.

Myndigheten för samhällsskydd och beredskap (MSB)
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB555 - april 2013 ISBN 978-91-7383-338-7