Myndigheten för
samhällsskydd
och beredskap

Upphandla informationssäkert – en vägledning

Upphandla informationssäkert – en vägledning

Upphandla informationssäkert – en vägledning

Myndigheten för samhällsskydd och beredskap (MSB)

Foto: Johan Eklund

Produktion: Advant Produktionsbyrå

Publikationsnummer: MSB1177 - november 2018
ISBN: 978-91-7383-802-3

Förord

Varje år genomför statliga myndigheter, kommuner och landsting tusentals upphandlingar runt om i Sverige. Upphandlingarna rör många olika typer av varor och tjänster såsom inköp av kontorsmaterial, medicinsk utrustning, byggtjänster, rådgivningstjänster och it-tjänster. Gemensamt för upphandlade varor och tjänster är att de är beroende av att information hanteras på ett tillräckligt säkert sätt.

Information finns överallt – på papper, på servrar, i molnet, i mobiltelefoner och på whiteboards. Informationssäkerhet handlar om att skydda er information efter behov och se till att endast behöriga personer får ta del av den, att den är korrekt och går att lita på och att den finns när ni behöver den.

Det är därför av stor vikt att ni har ett fungerande arbetssätt för att tidigt i upphandlingen beskriva vilka behov av skydd er information har och utifrån dessa ställa tydliga informationssäkerhetskrav. Ni behöver också säkerställa att ni har ett arbetssätt för att följa upp att leverantörerna svarar mot era informationssäkerhetskrav under hela avtalstiden.

Den här vägledningen ska vara ett stöd för er organisation att arbeta med informationssäkerhet på ett strukturerat sätt inför, under och efter en upphandling. En framgångsfaktor är att informationssäkerhetsfrågorna integreras i och blir en naturlig del av er upphandlingsprocess.

Vi tackar Upphandlingsmyndigheten för det stöd vi har fått i arbetet med den här vägledningen.

Åke Holmgren

Avdelningschef
Avdelningen för cybersäkerhet och skydd av samhällsviktig verksamhet

Innehåll

Sammanfattning

Sammanfattning

I inledningen beskrivs vägledningens syfte, målgrupp och avgränsningar. Vad informationssäkerhet är samt vad ni behöver tänka på vid bland annat upphandling enligt ramavtal beskrivs i kapitel 2. Kapitel 3 beskriver hur ni får tillräcklig förståelse för organisationens behov. Kapitel 4 redogör för vad ni behöver tänka på gällande informationssäkerhet vid alla typer av upphandlingar och vad ni bör göra för att ställa bra krav i avtalet. I kapitel 5 beskrivs kortfattat hur ni förvaltar och avslutar en leverantörsrelationen. Kapitel 6 tar upp vad ni som organisation speciellt bör tänka på när ni upphandlar it-system, verktyg och program samt utveckling av it-system. Avslutningsvis beskrivs det som är särskilt relevant för informationssäkerheten när det gäller upphandling av it-system.

Vägledningen följer de tre steg som Upphandlingsmyndighetens inköpsprocess är indelad i, förbereda, upphandla och realisera. De aktiviteter som behöver genomföras i varje steg sammanfattas i en ”snabbguide” i tabell 1.

Tabell 1. Aktiviteter för att uppnå informationssäkerhet kopplade till upphandlingens tre steg

FÖRBEREDA →	UPPHANDLA →	REALISERA →
• **Genomföra förstudie**	• **Identifiera behov och krav** • **Utvärdera och tilldela**	• **Kontrollera leverans** • **Förvalta** • **Avsluta**
• Identifiera behov	• Besluta att behovet ska realiseras med upphandling	• Säkerställa att leveransen uppfyller ställda krav
• Identifiera information	• Identifiera ansvar	• Godkänna leverans
• Genomföra initial klassning av informationen	• Genomföra fördjupad informationsklassning	• Följa upp att säkerhetskraven uppfylls över tid
• Bedöma relevansen av krisberedskap och samhällsviktig verksamhet	• Genomföra fördjupad riskbedömning	• Identifiera behov av förändringar
• Identifiera interna krav och behov	• Identifiera säkerhetskrav	• Förbereda avslut av leverantörsrelationen
• Identifiera externa krav och behov	• Definiera utvärderingsmodell för säkerhetskrav	• Ta hem informationen
• Genomföra initial riskbedömning	• Färdigställa upphandlingsunderlag	• Säkerställa att ingen information finns kvar hos leverantören
• Besluta om hur behovet ska realiseras	• Godkänna upphandlingsunderlag	
	• Utvärdera leverantörer	
	• Utvärdera kravuppfyllnad	
	• Fatta tilldelningsbeslut	
	• Skriva avtal	

Källa: MSB utifrån Upphandlingsmyndighetens inköpsprocess

Inledning

1. Inledning

Informationssäkerhet vid upphandling handlar om att identifiera och ställa de krav som ni anser nödvändiga för att er information ska hanteras säkert hos den externa leverantören. Ni behöver också se till att er leverans uppfyller de krav på säkerhet som ni har ställt. Det kan både handla om krav som ni själva eller leverantören måste uppfylla.

För att kunna ställa bra krav behöver ni kartlägga den information som ingår i upphandlingen och leveransen. Genom att arbeta systematiskt med informationsklassning och riskbedömningar identifierar ni vilket värde informationen har för er organisation och vilka risker som ni måste hantera under upphandlingen och avtalsperioden.

Genom att hantera identifierade risker tidigt i upphandlingsarbetet undviker ni att krav på säkerhet identifieras senare i upphandlingen eller till och med efter att organisationen ingått avtal, något som är både dyrt och tidskrävande.

1.1 Syftet med vägledningen

Vägledningen är till för att underlätta för er att uppnå en säker informationshantering vid upphandlingen och under avtalsperioden. Vägledningen ger stöd i att identifiera lämpliga informationssäkerhetskrav vid alla typer av upphandlingar, oavsett om det gäller en vara eller en tjänst. Har er organisation processer för upphandling och kravställning vid upphandling bör arbetet med att få in informationssäkerhet i upphandlingen integreras med dessa processer.

1.2 Målgrupp

Vägledningen riktar sig till CISO (informationssäkerhetsansvariga och dylika funktioner), it-säkerhetsansvariga, it-ansvariga, beställare, upphandlare och projektledare för projekt där varor och tjänster ska upphandlas.

Alla typer av organisationer kan dra nytta av denna vägledning.

1.3 Avgränsning

Fokus i denna vägledning ligger på hur informationssäkerhetskrav kan identifieras så att informationen hanteras på ett säkert sätt under upphandlingsarbetet och så att informationen som hanteras av den vara eller tjänst som upphandlas får lämpligt och bibehållet skydd.

Vägledningen beskriver inte arbetssättet för upphandling som del av en inköpsprocess[1] men vi visar hur arbetet med informationssäkerhetskrav passar in i ett sådant arbetssätt.

Vi berör endast ytligt upphandling med säkerhetsskyddsavtal[2] och de särskilda överväganden man behöver göra vid upphandling av samhällsviktig verksamhet.[3]

Vi presenterar inte några detaljerade krav på säkerhetsåtgärder för specifika upphandlingsbehov.

1. Upphandlingsmyndigheten ger stöd i form av kunskap, verktyg och metoder för offentligt upphandling, www.upphandlingsmyndigheten.se
2. Säkerhetspolisen och Försvarsmakten ger stöd för att genomföra säkerhetsskyddad upphandling med säkerhetsskyddsavtal.
3. *Upphandling till samhällsviktig verksamhet – en vägledning.* Publikationsnummer: MSB840 - september 2018

Upphandling och informationssäkerhet

2. Upphandling och informationssäkerhet

I dagens digitaliserade samhälle ställs allt högre krav på att hantera information säkert. Det är inte ovanligt att hela eller delar av en verksamhet och dess information hanteras av en extern leverantör genom varor eller tjänster. Det medför ett behov av säkerhetskrav som behöver inkluderas vid upphandling.

Som organisation behöver ni förstå vilka risker det medför att en extern aktör får åtkomst till och kontroll över er information och ni behöver ha klart för er vilka säkerhetsåtgärder leverantören behöver vidta för att hantera informationen på ett säkert sätt.

2.1 Vad är informationssäkerhet?

Informationssäkerhet innebär att hantera information så att:

- endast behöriga personer får ta del av den (konfidentialitet)
- den alltid går att lita på, att den är korrekt och inte är manipulerad eller förstörd (riktighet)
- den alltid finns åtkomlig och användbar när den behövs (tillgänglighet)

För att uppnå informationssäkerhet, det vill säga bevara informationens konfidentialitet, riktighet och tillgänglighet, behöver man oftast införa olika säkerhetsåtgärder. Säkerhetsåtgärder kan vara av administrativ, teknisk eller fysisk karaktär eller en kombination av dessa.

Informationssäkerhet vid upphandling innebär både att:

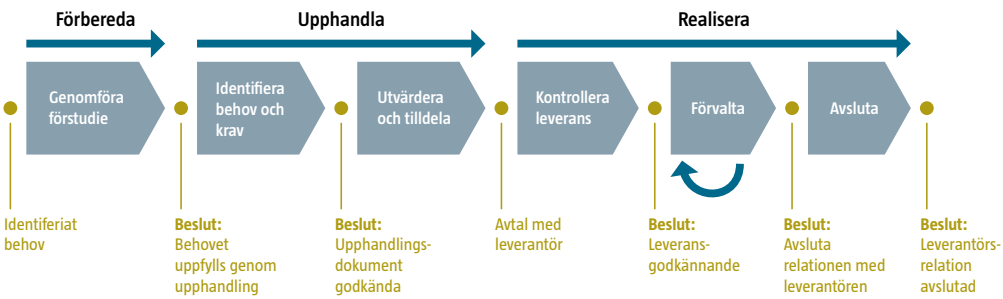
1. den information som hanteras under upphandlingsarbetet behandlas på ett säkert sätt både inom er egna organisation och hos intresserade leverantörer (informationssäker process).
2. varan eller tjänsten uppfyller de krav på informationssäkerhet som ni identifierat som nödvändiga under hela avtalsperioden (informationssäker leverans).

2.2 Upphandling som ett arbetsflöde

För att förtydliga när olika aktiviteter för att uppnå säker informationshantering ska genomföras relaterar vi aktiviteterna till ett arbetsflöde med tre steg.

- **Steg 1:** Förbereda. Här genomför ni en förstudie för att identifiera vilka grundförutsättningar ni har för att fatta beslut om det är aktuellt med upphandling eller om ni ska lösa behovet på ett annat sätt.
- **Steg 2:** Upphandla. Här tar ni fram och dokumenterar era informationssäkerhetskrav, för in dem bland övriga krav som ställs i upphandlingen och ni utvärderar inkomna anbud mot ställda säkerhetskrav.
- **Steg 3:** Realisera. Här inleder ni med att säkerställa att leveransen har de säkerhetsåtgärder som ni avtalat om. Därefter förvaltar ni relationen med den externa aktören och genomför regelbundna uppföljningar av att leveransen över tid uppfyller avtalet. Slutligen avslutar ni relationen med den externa aktören så att er information inte längre finns kvar hos leverantören.

Figur 1. Upphandlingens steg och faser



Källa: MSB utifrån Upphandlingsmyndighetens inköpsprocess

2.3 Att tänka på när organisationer delar tjänster

Organisationer kan gå samman och dela tjänster i stället för att varje organisation själv upphandlar, utvecklar eller driftar it-system. Det kan röra sig om ett gemensamt mindre projekt mellan två parter eller, som i fallet Statens servicecenter, en för ändamålet bildad myndighet som tillhandahåller ekonomi- och personalrelaterade tjänster till flertalet statliga myndigheter.

Arbetssättet för denna typ av lösningar liknar upphandling där en organisation överlåter åt en annan part att sköta vissa delar av sin informationshantering. Därmed kan man också i denna form av samverkan tillämpa principerna i den här vägledningen.

Om ni delar tjänster med en annan organisation är det viktigt att ni klarlägger ansvar och roller, fastställer arbetssätt för hur säkerhetskraven ska hanteras samt hur kraven ska följas upp. Grundprincipen är att den eller de organisationer vars information ska hanteras formulerar sina säkerhetskrav utifrån genomförd informationsklassning och riskbedömning. Därefter jämförs identifierade säkerhetskrav mot hur uppfyllnad av kraven ser ut för den lösning och den organisation som hanterar informationen. Detta måste ske innan ni påbörjar samverkan, skriver samverkansavtal och delar information.

2.4 Att tänka på vid offentlig upphandling

För offentlig sektor finns särskild lagstiftning, fyra lagar, som styr hur upphandlingarna ska ske:

- LOU – lag (2016:1145) om offentlig upphandling.
- LUF – lag (2016:1146) om upphandling inom försörjningssektorerna.
- LUK – lag (2016:1147) om upphandling av koncessioner.
- LUFS – lag (2011:1029) om upphandling på försvars- och säkerhetsområdet.

Målet med regelverken kring offentlig upphandling är att säkerställa dels likabehandling av leverantörer, dels ett kostnadseffektivt arbetssätt för offentlig verksamhet. Dessa regler ger inte stöd i hur nödvändiga informationssäkerhetskrav kan ställas. De sätter ramarna för hur upphandling ska gå till.

2.5 Att tänka på vid ramavtal

Ramavtal är ett avtal för en viss vara eller tjänst som en eller flera myndigheter, landsting, kommuner eller motsvarande ingår med en eller flera leverantörer i syfte att senare avropa, det vill säga göra beställningar, utifrån det som specificeras i avtalet. Att använda ramavtal underlättar och effektiviserar offentlig förvaltning.

Ibland erbjuder ramavtalen fördefinierade valmöjligheter, där avtalet specificerar olika nivåer av funktionalitet och säkerhetsåtgärder till ett förhandlat pris.

Det är sällsynt att samtliga nödvändiga krav gällande informationssäkerhet finns med i ramavtalen. Ni ska därför identifiera och komplettera de krav som behöver ställas vid avropet, så länge kraven är inom ramen för avtalet och att avtalet är öppet för kompletteringar. Ett exempel på formulering i ett ramavtal som är öppet för komplettering är: Utöver ovanstående kan kund precisera andra säkerhetskrav som gäller verksamheten.

Vissa säkerhetskrav som är formulerade i ramavtalen kan specificeras ytterligare, exempelvis när säkerhetskraven finns under rubriken ”Allmänna villkor” eller motsvarande. Då kan ni vid avrop göra preciseringar av dessa villkor. Det framgår av varje ramavtals kravkatalog vilka krav och preciseringar som får göras.[4]

Vissa ramavtal kan redan från början innehålla specifika informationssäkerhetskrav och inte vara öppna för er att påverka vid ett avrop varken gällande kravens utformning eller innehåll.

Uppfyller inte ramavtalet era krav i sitt grundutförande och det saknas möjlighet att komplettera eller specificera kraven så att era behov tillgodoses ska ni inte använda ramavtalet. Ni behöver istället göra en egen upphandling där ni kan ställa tillräckliga säkerhetskrav.

Innan ni går vidare och gör en egen upphandling bör ni först undersöka om ni behöver anmäla detta till berörd upphandlingsfunktion, inköpscentral eller motsvarande. Till exempel, om er organisation är en statlig myndighet och befintliga ramavtal från Kammarkollegiet inte motsvarar era behov behöver ni göra en avstegsanmälan till Kammarkollegiet.

---

4. Lagen om offentlig upphandling (LOU 2016:1145) 7 kap Ramavtal, inköpscentraler och annan samordnad upphandling.

I avstegsanmälan ska anledningen till beslutet att genomföra egen upphandling anges. Skälen kan vara att egen upphandling ger bättre pris, högre kvalitet, lägre administrativa kostnader, en produkt som på bättre sätt tillgodoser myndighetens behov eller annat skäl[5]. Om er organisation har tecknat ramavtal via SKL Kommentus Inköpscentral och inte anser att de ramavtalen uppfyller ert försörjningsbehov väljer ni själva hur behovet ska täckas[6].

2.6 Att tänka på vid säkerhetsskyddad upphandling

Innan ni påbörjar upphandlingen behöver ni identifiera om den information som leverantören kommer att få åtkomst till faller in under säkerhetsskyddslagstiftningen.

Om ni i er säkerhetsskyddsanalys[7] eller i den klassning av information som ni gör inför upphandlingen kommer fram till att informationen är säkerhetsskyddsklassificerad ska ni genomföra upphandlingen med så kallade säkerhetsskyddsavtal (SUA).

För organisationer som ska genomföra en upphandling som kräver säkerhetsskyddsavtal ska i vissa fall samråd[8] genomföras med berörd tillsynsmyndighet, det vill säga Försvarsmakten eller Säkerhetspolisen. Ta stöd av er organisations säkerhetsskyddschef vid den här typen av upphandling. Säkerhetspolisen och Försvarsmakten har vägledning för säkerhetsskyddad upphandling.[9]

5. Kammarkollegiet underrättelse om avsteg. Underrättelse om avsteg kan och ska lämnas av myndigheter under regeringen enligt 4 § förordningen (1998:796) om statlig inköpssamordning.
6. SKL Kommentus Inköpscentral. – verkstad för samordnade nationella och regionala upphandlingar.
7. Begrepp från den nya säkerhetsskyddslagen Säkerhetsskyddslag (2018:585).
8. Säkerhetsskyddsförordningen (1996:633) § 16 a.
9. http://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/handbocker/h-sak-sua-2010.pdf och http://www.sakerhetspolisen.se/sakerhetsskydd/sakerhetsskyddad-upphandling.html

Förbereda upphandlingen

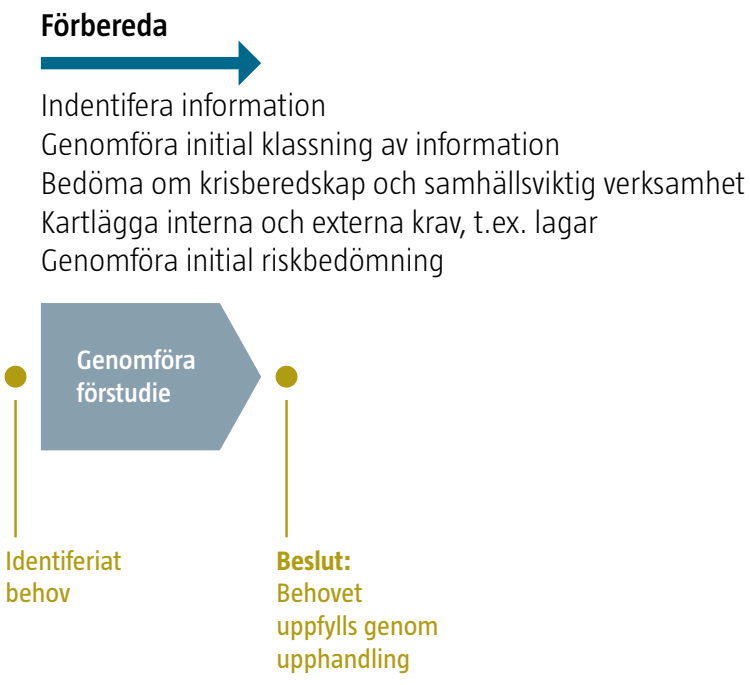
3. Förbereda upphandlingen

3.1 Identifiera behov

När ett behov av en vara eller tjänst uppstår i er verksamhet behöver ni först bestämma hur ni ska tillgodose behovet. I vissa fall är upphandling en given lösning, till exempel vid inköp av kontorsmaterial. I andra fall är det mer osäkert om upphandling verkligen är det bästa sättet att hantera det behov som uppkommit.

Innan ni beslutar hur ert behov ska tillgodoses bör ni genomföra en förstudie för att tydliggöra förutsättningarna för och de krav ni har på varan eller tjänsten. Genomför ni inte en förstudie behöver ni ändå genomföra samtliga punkter i nästa avsnitt (avsnitt 2.2 Genomför en förstudie).

Figur 2. Upphandlingens förberedelsefas



Källa: MSB utifrån Upphandlingsmyndighetens inköpsprocess

3.2 Genomföra en förstudie

Har er organisation ett arbetssätt för att genomföra en förstudie så använd i första hand det och komplettera arbetssättet med de aktiveter nedan som saknas.

3.2.1 Identifiera information

Identifiera vilken information som ni kommer att hantera under själva upphandlingen och vilken information som den externa aktören kommer att få tillgång till under avtalstiden.

Några exempel på olika tjänster och den information som externa aktörer kan få tillgång till:

- Ett städuppdrag kan innebära åtkomst till en detaljerad beskrivning av organisationens byggnader och larmrutiner.
- Ett uppdrag där en extern part ska förvalta er it-utrustning kan medföra att leverantören tar del av detaljerade uppgifter om er it miljö och dess skydd.
- En taxitjänst kan resultera i att olika taxibolag får del av ett register över era anställda och deras hemadresser.

3.2.2 Genomföra initial klassning av information

Utifrån den information ni identifierat genomförs en initial informationsklassning. Detta gör ni genom att besvara följande:

1. Vilka krav på ***konfidentialitet*** gäller för informationen ni identifierat?
   - Kommer själva upphandlingsunderlaget innehålla sekretessbelagda uppgifter eller uppgifter som är känsliga för organisationen?
   - Kommer aktören hantera sekretessbelagda uppgifter eller uppgifter som är känsliga för organisationen vid själva utförandet av tjänsten?
   - Kommer aktören hantera känsliga personuppgifter eller andra personuppgifter?
2. Vilka krav på ***riktighet*** gäller för informationen i fråga?
   - Vilka konsekvenser får det om informationen förvanskas?
3. Hur ser ***tillgänglighetsbehoven*** för informationen ut?
   - Hur lång tid kan ni vara utan informationen?
   - Finns situationer eller tidpunkter när informationen måste vara tillgänglig?

För att kunna genomföra en initial informationsklassning behöver ni kunskap om vilket värde informationen har för er organisation. Ni kan med fördel använda en redan genomförd informationsklassning, om det finns att tillgå.

3.2.3 Identifiera samhällsviktig verksamhet

En viktig del av förstudien är att identifiera om ni behöver ställa särskilda krav på den externa leverantören för att denna kommer att leverera något till den samhällsviktiga verksamheten som ni ansvarar för. Genom att identifiera vilken samhällsviktig verksamhet som den externa aktören ska leverera och vilken information gällande samhällsviktig verksamhet som denna får kännedom om kan ni identifiera tydligare krav. Det är också viktigt att förstå i vilka situationer som den samhällsviktiga verksamheten behöver fungera under, till exempel olika typer av kriser, vid höjd beredskap eller krig.

För er som ska upphandla varor eller tjänster som stödjer samhällsviktig verksamhet finns mer detaljerad information i MBS:s Upphandling till samhällsviktig verksamhet – en vägledning.[10]

3.2.4 Identifiera interna och externa krav

Interna krav

Ni behöver identifiera om ni har några regler eller övriga interna behov som berör upphandling. Några exempel på regler är:

- Policyer – avsiktsförklaringar för er organisation.
- Anvisningar, riktlinjer, strategier eller motsvarande – mer detaljerade styrningar kring hur er organisation kan, bör eller ska agera.
- Rekommendationer av olika slag.

Vissa regler är generella, till exempel arbets- och delegationsordning, arbetsmiljö- och miljöpolicy eller upphandlingspolicy. Andra regler är viktiga för en viss typ av upphandling. Exempel på detta är om organisationen har regelverk för hur säkerhetsskyddad upphandling ska genomföras eller under vilka förutsättningar organisationen bör utkontraktera it-drift.

10. *Upphandling till samhällsviktig verksamhet – en vägledning.* Publikationsnummer MSB840 – september 2018.

En del regler är mer specifika i sin kravställning på informationssäkerhet. Där kan det framgå exakt vilka krypteringslösningar som accepteras vid informationsöverföring mellan två parter beroende på resultatet av informationsklassningen.

Externa krav

Ni behöver även identifiera vilka rättsliga krav eller övriga externa behov och krav som finns för den vara eller tjänst som ni ska upphandla. Några exempel på sådana är:

- EU-förordningar, EU direktiv och internationella konventioner
- Svenska lagar och förordningar
- Myndighetsföreskrifter
- Kundförväntningar

De externa kraven kan utesluta upphandling av vissa varor eller tjänster beroende på vilken typ av information som kommer att omfattas.

Andra intressenter så som ingångna avtal eller överenskommelser och vissa branschpraxis kan vid upphandling påverka vilka krav du behöver ställa.

3.2.5 Genomföra initial riskbedömning

Det är viktigt att göra en riskbedömning för att förstå de risker som är förknippade med att hantera informationen[11]. I en sådan bedömning identifierar ni vilka risker som kan drabba er organisation som en följd av att ni väljer att upphandla eller inte. Har er organisation en etablerad process för riskbedömning så bör ni använda den processen.

Gör en initial riskbedömning genom att reflektera kring och besvara följande tre frågor:

1. ***Vad*** kan hända?

- Specificera vad det är som ni ska upphandla – är det ett system som ska driftas i egen miljö, någon form av utkontraktering (inklusive molntjänst) eller en kombination där tjänsten är uppdelad så att vissa delar hanteras internt och vissa externt.
- Fundera ut händelser (hot) som kan påverka informationen, er organisation och era kunder.

11. Gällande riskbedömning inom informationssäkerhet: ta del av det som står i I SS ISO/IEC 27005:2013, *Informationsteknik – Säkerhetstekniker – Riskhantering för informationssäkerhet.*

2. Vad blir ***konsekvenserna*** om det inträffar?
   - Tänk på hur er organisation, era kunder, allmänheten och andra kan drabbas.

3. Hur ***sannolikt*** är det att det inträffar?
   - Bedöm hur sannolikt det är att händelsen (hotet) realiseras. Till stöd för sannolikhetsbedömningen kan statistik, om sådan finns användas. Annars är en generell bedömning bra nog.

Om ni kan uppskatta eller har kunskap om hur ofta en händelse inträffar ger det tillsammans med kunskap om konsekvensen en god bild av hur stor risken är. I den initiala riskbedömningen bör minst de som kommer att få ansvar för att förvalta en eventuell leverantörsrelation delta.

Riskbedömningen ska dokumenteras och riskägaren ska ges chans att komplettera om denna inte deltagit själv. Har ni genomfört en riskbedömning gällande att hantera informationen eller utkontraktera verksamheten tidigare kan den med fördel användas som underlag.

3.3 Bestäm hur ni ska hantera ert behov

Baserat på den genomförda förstudien (eller motsvarande underlag) kan ni nu fatta beslut om att gå vidare med en upphandling eller att möta behovet genom andra åtgärder.

Om ni beslutar er för att upphandla måste ni identifiera vilka förfaranden[12] som är möjliga och önskvärda eftersom det påverkar hela upphandlingens upplägg. Detta arbete kan ni få stöd av från er upphandlingsfunktion utifrån det underlag ni tagit fram.

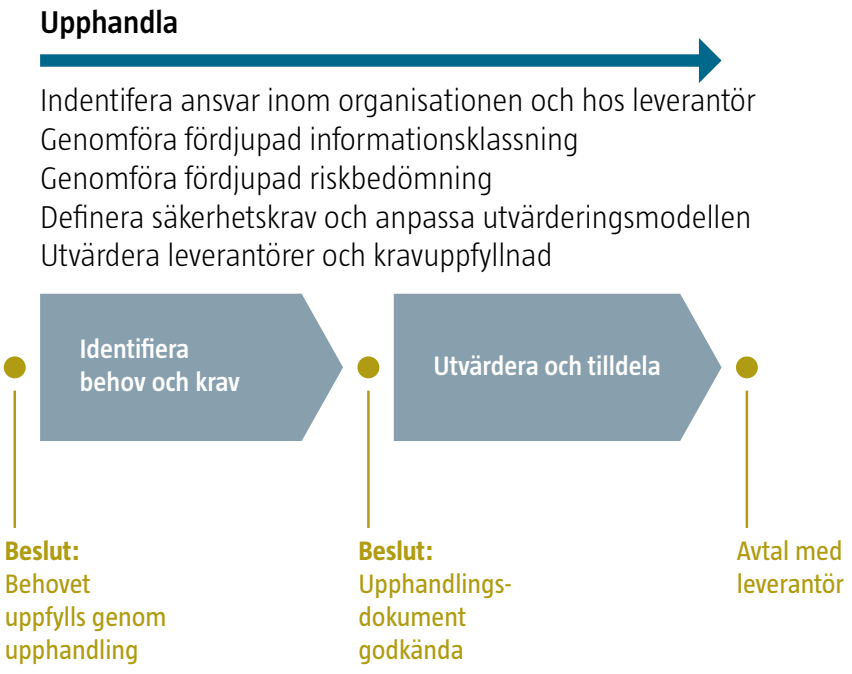
12. För utförlig information om olika förfaranden, se Upphandlingsmyndighetens webbplats, www.upphandlingsmyndigheten.se.

Informationssäker upphandling

4. Informationssäker upphandling

Nu har ni beslutat er för att genomföra en upphandling. Det här kapitlet tar upp de delar av upphandlingen som handlar om identifieringen av krav på informationssäkerhet och framtagandet av upphandlingsdokument. Avslutningsvis beskrivs det ni behöver tänka på när ni skriver avtal för att säkerställa att ni får en säker leverans. Avsnitten i det här kapitlet är relevanta för upphandling av alla typer av varor och tjänster. Kapitel 6 tar upp det som är av särskild betydelse för informationssäkerheten vid upphandling av it-system.

Figur 3. Upphandlingsfasen



Källa: MSB utifrån Upphandlingsmyndighetens inköpsprocess

4.1 Upphandlingsdokumenten

Upphandlingsdokument[13] är de underlag där ni fastställer innehållet i upphandlingen och som ni tillhandahåller intresserade leverantörer.

Bland de handlingar som ingår behöver ni noga överväga vilka krav[14] (ska-krav) ni ska ställa på leverantören och vilka krav (ska-krav) ni ska ställa på varan eller tjänsten. Ni ska också tänka igenom vilka tilldelningskriterier[15] (bör-krav) som ni vill ställa på varan eller tjänsten.

Huruvida ni ska ställa krav eller tilldelningskriterier beror på om ni verkligen behöver till exempel en funktion eller om den inte är nödvändig men ni är villiga att betala mer för varan eller tjänsten om kriteriet uppfylls.

Det är också viktigt att i upphandlingsdokumenten ange hur anbudsgivarna ska bevisa att de uppfyller ställda krav och tilldelningskriterier.

4.2 Kompetenser i upphandlingen

För att uppnå ett bra resultat behöver olika kompetenser delta vid upphandlingen. Bredden av kompetenser behövs tidigt i upphandlingsarbetet, med fördel redan i förstudien. Beroende på vad ni ska upphandla kan ni behöva följande kompetenser:

- **Förvaltning** för att ställa krav på hur samarbetet med leverantören ska fungera under avtalstiden och när avtalet upphör samt verifiera att kraven uppfylls.
- **Informationshantering** för att vägleda i att ställa krav på hur information delas, bearbetas och lagras samt verifiera att dessa uppfylls.
- **Informationssäkerhet** för att formulera informationssäkerhetskrav och verifiera att dessa uppfylls.
- **Informationsägarskap** eller **verksamhetsansvar** för att identifiera krav och behov.
- **It** för att bedöma hur tjänsten kan kunna integreras på lämpligt sätt i befintlig infrastruktur.
- **It-säkerhet** för att formulera it-säkerhetskrav och verifiera att dessa uppfylls.

13. Lagen om offentlig upphandling (LOU 2016:1145) 1 kap. 23 §.
14. Lagen om offentlig upphandling (LOU 2016:1145) 14 kap Kvalificering.
15. Lagen om offentlig upphandling (LOU 2016:1145) 16 kap Utvärdering av anbud och tilldelning av kontrakt.

- **Upphandling** för att välja rätt förfarande, kvalitetssäkra upphandlingdsokumenten och säkerställa att upphandlingen resulterar i ett affärsmässigt och verksamhetsmässigt fungerande avtal.

4.3 Roller i upphandlingen

Under upphandlingsarbetet behövs någon eller några i er organisation som ansvarar för att bevaka alla informationssäkerhetsfrågor. Detta görs dels genom

- att kravställa,
- att utvärdera olika leverantörers anbud avseende säkerhetsåtgärder och
- att kontrollera att införda säkerhetsåtgärder omhändertagit informationsägarens intressen samt
- att kontrollera att leverantören och de avtalade säkerhetsåtgärderna svarar upp mot ställda krav.

Redan under upphandlingen bör den funktion som ska ansvara för att förvalta leveransen vara utpekad.

Säkerställ också att er organisation

- kan ta emot till exempel incident- eller statusrapporter avseende tjänsten,
- har resurser och kompetens för att säkerställa leverans och
- kan genomföra uppföljningar om ni ska ansvara för dessa.

Relationen mellan kund och leverantör måste bygga på en gemensamt accepterad ansvarsfördelning. I kravställningen ska det framgå vilka roller och ansvar som leverantören måste ha för att möta ställda krav.

När avtal sluts ska det också framgå vilken av parterna som har ansvar för att uppfylla de säkerhetskrav som ställts samt om det behövs ytterligare avtal, till exempel där leverantören hanterar er organisations personuppgifter[16].

Att fastställa ansvar och roller för informationssäkerhet är lika viktigt i affärsmässiga relationer, som exempelvis partnermoln, som där myndigheter samverkar till exempel i gemensamma servicecenter.

16. Aktuell information kring kraven på hantering av personuppgifter finns på Datainspektionens webbplats, www.datainspektionen.se

4.4 Säkerhetskrav vid upphandling

Nu vet ni vad ni ska upphandla samt vilken information som ska hanteras och de risker det medför på ett övergripande plan. För att identifiera bra informationssäkerhetskrav behöver ni fördjupa er kunskap om vilken information som kommer att ingå i upphandlingsarbetet och efterföljande avtal och hur riskerna ser ut. Den fördjupade informationsklassningen och riskbedömningen ger de underlag som krävs.

4.4.1 Genomföra fördjupad informationsklassning

Har ni redan klassat den information som ingår i upphandlingen så återanvänd den. Annars använd er informationsklassningsmodell för att genomföra den fördjupade[17] klassningen. Om ni inte har någon klassningsmodell finns stöd för hur man klassar information på informationssäkerhet.se. Kommuner och landsting kan få stöd med klassning och kravställning av det verktyg som Sveriges Kommuner och Landsting (SKL) har tagit fram (KLASSA[18]). Informationsklassning inför upphandlingen görs för att identifiera värdet av den information som anbudsgivare och leverantören kommer att hantera. Detta gäller både

- information som ingår i själva upphandlingen och som anbudsgivarna behöver få kännedom om för att kunna lämna anbud och
- information som ni överlåter till leverantören att hantera som en del av leveransen.

Den initiala informationsklassningen i förstudien ger ett bra ingångsvärde för denna aktivitet. I detta steg ska ni dock göra en djupare analys.

Informationen klassas utifrån de konsekvenser som ni bedömer att en oönskad händelse kan leda till. Det innebär att klassningen kan skilja sig åt mellan organisationer trots att informationen är densamma. När ni analyserar informationstillgångarna kan ni använda MBS:s Vägledning för processorienterad informationskartläggning[19] som underlag.

17. Fördjupad informationsklassning i detta dokument motsvarar den informationsklassning ni normalt genomför i er organisation för att identifiera vilken konsekvens avseende konfidentialitet, riktighet och tillgänglighet otillräckligt skydd kan få för er organisation och era intressenter.
18. https://klassa-info.skl.se/
19. Publikationsnummer MSB493 – utgiven november 2012.

Använd klassningens resultat för att identifiera vilka säkerhetsåtgärder leveransen ska uppfylla. Om ni redan har ett systematiskt informationssäkerhetsarbete så ska det finnas definierade säkerhetsåtgärder kopplade till informationsklassningsmodellens nivåer eller definierade på annat sätt.

4.4.2 Genomföra en fördjupad riskbedömning

Syftet med den fördjupade riskbedömningen är att identifiera om de säkerhetsåtgärder som ni identifierat är tillräckliga eller om ytterligare säkerhetsåtgärder behöver ställas på

- leverantören,
- varan eller tjänsten,
- den egna organisationen.

När ni under upphandlingsarbetet får ny kunskap om hur skyddet för er information kommer att se ut bör ni komplettera riskbedömningen utifrån de nya förutsättningarna. Ett exempel på en ny förutsättning är om den tänkta tekniska lösning som framkommer av anbuden är en annan än den ni riskbedömt. En annan ny förutsättning är om den information som leverantören måste få tillgång till för att kunna genomföra leveransen skiljer sig åt från den som ni initialt planerat för.

Dokumentera de risker som ni identifierar och särskilt de konsekvenser ni har identifierat. Dokumentera också vilken eller vilka säkerhetsåtgärder som minskar dessa risker.

Riskbedömningen och föreslagna säkerhetsåtgärder överlämnas till informationsägaren som fattar beslut om hur riskerna ska hanteras. Eftersom skadeverkningarna av bristande säkerhet uppstår hos informationsägaren så är det denna som måste bedöma resultatet av såväl informationsklassningen som av den genomförda riskbedömningen.

4.4.3 Definiera informationssäkerhetskrav

När ni ska formulera krav utifrån de säkerhetsåtgärder ni identifierat genom informationsklassning och riskbedömning tänk på att uttrycka era behov utifrån det ni vill uppnå. Att identifiera vad er verksamhet behöver och vill ha är ett bra sätt att öppna upp för olika möjliga lösningar så att ni inte låser leveransen eller utförandet till en särskild teknik, arbetsmetod eller produkt utan möjliggör för leverantörerna att komma med alternativa lösningar som ni själva inte har identifierat. Ni ställer helt enkelt säkerhetskraven för att uppnå det skydd som man bedömt att informationen behöver ha.

För att kunna avgöra *vilka krav* som möter *vilka risker* samt kunna göra medvetna val om ni beslutar er för att ta bort vissa krav behöver ni ha spårbarhet även för säkerhetskraven i er kravsammanställning. Ni kan stryka alla krav som inte möter någon risk. Alla risker behöver omhändertas på något sätt. Det är informationssägaren som ytterst ansvarar för hur en risk omhändertas.

Det förekommer att externa aktörer erbjuder sina utbud i olika nivåer där säkerhetsåtgärder grupperats. Detta gör det möjligt för er att göra en avvägning mellan *nivån av skydd* och *kostnaden* utifrån de specifika säkerhetskrav ni identifierat. Om ni behöver avstå från att få vissa krav uppfyllda när ni väljer nivå behöver ni göra en riskbedömning för att ge informationsägaren ett underlag att ta ställning till – är detta en risk denna är beredd att acceptera?

Att externa aktörer erbjuder olika nivåer på säkerhetsåtgärder kan vara till nytta för dig som kund eftersom ditt behov och hoten mot den upphandlade varan eller tjänsten kan förändras över tid. Nivån på skyddet kan därmed behöva höjas eller sänkas under avtalstiden. Om er leverantör endast tillhandahåller en bestämd säkerhetsnivå, alternativt gör unika kundlösningar, finns en risk för att ni antingen kommer att bli tvungna att byta leverantör eller behöva betala för ytterligare anpassning av tjänsten.

4.4.4 Använd informationssäkerhetsstandarder som krav

Vi rekommenderar att ni använder standarder som stöd i arbetet med att identifiera säkerhetskrav. Vilka standarder som är lämpliga att använda beror på vilken vara eller tjänst ni ska upphandla. Att inför en upphandling undersöka vilka relevanta standarder och andra accepterade specifikationer som kan ge er stöd är väl investerad tid.

Standarden för ledningssystem för informationssäkerhet SS-EN ISO/IEC 27001, eller motsvarande, kan användas på två sätt:

- dels kan ni ställa krav på att er leverantör ska vara certifierad eller arbeta utifrån relevanta delar av standarden,
- dels är den en bra utgångspunkt för att identifiera möjliga säkerhetskrav på varan eller tjänsten. Dessa krav behöver specificeras utifrån vad ni ska upphandla, utifrån er informationsklassning och riskbedömning.

Om leverantören redovisar att de är certifierade enligt SS-EN ISO/IEC 27001 så ska de bifoga sitt Uttalande om Tillämplighet, UoT (på engelska *Statement of Applicability, SoA*). Detta för att ni ska veta mer specifikt vilka delar av leverantörens verksamhet och vilka delar av standarden som ingått i certifieringen. När det gäller att ställa krav på varan eller tjänsten utifrån standarder kan det i vissa fall räcka med att leverantören svarar att de uppfyller ställda krav och inkommer med bevis som styrker det. I andra fall behöver leverantören redovisa *hur* de uppfyller ett krav.

4.4.5 Exempel på frågor som ni som upphandlar kan behöva besvara

Nedan listas ett antal frågor som ofta behöver besvaras av den som upphandlar. Listan är inte uttömmande och beroende på vad som ska upphandlas är inte alla frågor relevanta. I slutet på kapitel 6 finns fler frågor som rör it-miljö och är särskilt relevanta vid upphandling av it-system.

Område: organisation

- Ska ni specificera vilka lagar leverantören behöver följa gällande leveransen? Hur ska en eventuell tvist lösas? Ska ni specificera att minst svensk lag (utom i vissa särskilda undantagsfall) ska gälla?
- I vilken omfattning får leverantören anlita underleverantörer? Vilka krav ska ni ställa på leverantören att i sin tur ställa på sina underleverantörer? Vill ni bli informerade om vilka underleverantörer som används?
- I vilken omfattning ska leverantören informera om ett eventuellt byte av arbetssätt (till exempel under avtalstiden går från licenser för er it-miljö till en molntjänst)? Vill ni kunna bryta avtalet om leverantören byter leveranssätt?
- Ska leverantören redovisa sin säkerhetsorganisation samt sin planering för att undvika nyckelpersonberoende? Arbetar leverantören utifrån SS-EN ISO/IEC 27001 eller motsvarande standard? Behöver ni kunna verifiera att leverantören har ett väl fungerande arbetssätt för de delar som är relevanta för er?
- Ska leverantören utse en särskilt utpekad kontaktperson för informationssäkerhetsfrågor?

- Vilka möjligheter till olika former av granskningar av leverantörens säkerhetsarbete behöver ni? Några exempel:
  - » rätten att genomföra granskningar
  - » krav på åtkomst till resultatet av leverantörens egenkontroller eller externa granskningar initierade av leverantören själv
  - » stöd från leverantören vid granskningar ni initierar enligt granskningsplan eller utifrån händelser/incidenter. Till exempel att kunnig personal från leverantören bidrar, att ni får tillgång till information, att ni har rätt att vistas i lokaler vid granskningar
  - » stöd från leverantören vid granskningar där en tillsynsmyndighet initierar granskningen av informationshanteringen
- Behöver ni utifrån rättsliga krav och behov kravställa på hur informationen lagras, rutiner för gallring och metoder för arkivering?[20]
- Behöver ni leverantörens stöd för att kunna hantera utlämnandeärenden? (offentliga verksamheter[21])
- Behöver ni kravställa på leverantören hur information eller utrustning som hanterat er information ska förstöras när avtalstiden gått ut eller utrustning sänds för destruktion? Vad gäller om leverantören avser använda utrustning igen för andra kunder? Behöver lagringsmedia raderas på särskilt sätt?
- Vad behöver ni reglera i avtalet för att avsluta relationen med leverantören på ett sätt så ni kan fortsätta arbetet med en annan leverantör eller själva ta över arbetet? Hur ska information och it-utrustning som hanterat er information raderas eller förstöras?
- Har leverantören en kontinuitetsplanering? Om ja: uppfyller denna era behov?
- Kan leverantören säkerställa leveransen under kris, krisberedskap, höjd beredskap eller krig, om så behövs?

20. Ni bör beakta Riksarkivets föreskrifter och allmänna råd (RA-FS 2013:1) om gallring och återlämnande av handlingar i detta sammanhang.
21. Offentlighets- och sekretesslagen gäller även för ekonomiska föreningar och stiftelser där kommuner eller landsting utövar ett rättsligt bestämmande inflytande jämställas med myndigheter. Offentlighets- och sekretesslag (2009:400) 2 kap. 3 §.

Område: Personsäkerhet

- Vilka anställningskontroller ska leverantören genomföra för den personal (anställda av leverantören) som får tillgång till er information? Vilket ansvar för underleverantörens personal ska leverantören ha?
- Hur ska utbildning av leverantörens personal och eventuella underleverantörer genomföras så att de har tillräcklig kunskap om säkerhet, informationssäkerhet och för uppdraget relevant lagstiftning?

Område: Fysisk miljö

- Om leverantören hanterar er information hos sig.
  - » Har leverantören riskbedömt sin fysiska miljö (inklusive omliggande miljö)? Har leverantören genomfört alla åtgärder som är nödvändiga för att skydda er information tillräckligt?
  - » Behöver ni säkerställa att lokalerna och omgivningen uppfyller behovet av skydd? Behöver ni ställa krav på speciella säkerhetsåtgärder inne i leverantörens lokaler, där informationen hanteras eller lagras?
  - » Hur begränsar leverantören den fysiska åtkomsten till informationen (till exempel genom krav på förvaring i säkerhetsskåp eller genom särskild avskild datormiljö)?

I de flesta fall är leverantörens ekonomiska stabilitet, arbetsmiljö, miljö och andra faktorer viktiga.[22] Krav på dessa områden berörs inte ytterligare i denna vägledning men är viktiga för att över tid ha tillit till att leverantören har möjlighet att upprätthålla den nivå av säkerhet som ni avtalat.

När ni har tagit fram era behov behöver de anpassas så de passar in i upphandlingsdokumenten. Vissa behov ställs lämpligen som krav (ska-krav) och andra som tilldelningskriterier (bör-krav).

22. Exempel på ytterligare stöd vid upphandling finns bland annat i Ekobrottsmyndighetens skrift *Att tänka på när du upphandlar eller avropar tjänster – rutiner och tips som försvårar användningen av svart arbetskraft inom offentlig sektor*, mars 2013.

4.5 Avtalets omfattning

Det avtal som ni upprättar ska beskriva vilka delar som ni tycker är viktiga dels för leveransen, dels för att följa upp och säkerställa att leveransen sker enligt vad ni avtalat. Avtalet bör vara tillräckligt flexibelt för att fungera över den tid som avtalet omfattar.

4.5.1 Beskriv samtliga överenskommelser

Det är viktigt att avtalet beskriver just de säkerhetsåtgärder som ni kommit överens om med den externa aktören. Ni kan inte förutsätta att leverantören kommer att uppfylla säkerhetskrav som ni tycker är underförstådda. Ett exempel: Om det inte står i avtalet att ”leverantören ska rapportera incidenter i dokumenterad form en gång i månaden” så kan ni inte heller kräva detta, åtminstone inte utan extra kostnad.

Om ni inte har kommit överens i avtalet att ni ska få verifiera att uppgivna säkerhetsåtgärder verkligen finns eller initiera olika typer av granskningar som ni (kunden) anser er behöva genomföra så kan leverantören motsätta sig detta utan att ni har någon större möjlighet att påverka deras beslut.

För att undvika konflikter och oväntade kostnader bör således avtalet så tydligt som möjligt beskriva samtliga överenskommelser, för hela leveransens livscykel, som ni har med leverantören.

4.5.2 Beskriv hur uppföljning och kontroll ska göras

Avtalet bör innehålla både *vilka* säkerhetsåtgärder som ska följas upp, *hur* detta ska ske och *av vem* samt med *vilken frekvens*.

Kontrollerna av säkerhetsåtgärder kan genomföras på följande sätt:

- genom att leverantören genomför egenkontroller och rapporterar resultaten till er,
- genom att ni själva genomför revisioner eller
- genom att ni tar in en oberoende tredje part som kontrollerar avtalade säkerhetskrav.

I avtalet ska det även ingå

- att ni ska få tillgång till leverantörens genomförda kontroller, granskningar och revisionsrapporter samt de åtgärdsplaner som följer av att brister uppmärksammats,
- hur granskningarna ska genomföras samt
- hur ofta leverantören ska genomföra egenkontroller och granskningar eller revisioner.

Om ni själva genomför uppföljning av hur leverantören uppfyller säkerhetsåtgärderna i avtalet behöver ni avtala att ni har tillträde till lokalerna och rätt att få tillgång till det material ni behöver för att kunna verifiera att säkerhetsåtgärderna är tillräckliga. Det kan också vara nödvändigt att säkerställa att leverantören avsätter resurser med rätt kompetens för att er granskning ska bli meningsfull.

Ifall ni och leverantören har avtalat om att revisonen ska ske av oberoende tredje part så behöver ni säkerställa att det finns kompetens hos er som kan bedöma om omfattning och utförande sker på ett tillfredsställande sätt.

Berörs ni av att en eller flera myndigheter har rätt att genomföra tillsyn av er informationshantering behöver det framgå av avtalet på vilket sätt leverantören behöver vara behjälplig om tillsynsmyndighet begär underlag och genomför besök.

4.5.3 Särskilda villkor vid samverkan

Även vid samverkan måste det finnas någon form av överenskommelse som beskriver förutsättningarna för användningen av den information som utbyts eller delas samt tillhörande ansvar för att skydda informationen. Vägledning för digital samverkan finns bland annat på eSams webbplats[23].

4.5.4 Var uppmärksamma vid standardavtal

Vid direktupphandling är det vanligt att leverantörer erbjuder standardavtal. Om dessa inte överensstämmer med er organisations krav på leveransen behöver ni förhandla fram ett avtal där era krav tillgodoses.

4.5.5 Att tänka på när avtal avslutas

Ni bör specificera i vilka situationer ni har rätt att avsluta relationen med leverantören innan avtalet har löpt ut. Det ska också framgå vilket stöd leverantören ska ge er vid en sådan situation. Exempel på när ni bör avtala om rätt att avsluta avtalet är brister i leverantörens säkerhetsåtgärder. Med brister menas här inte mindre säkerhetsproblem som leverantören kommunicerar till er och åtgärdar inom rimlig tid.

23. E-samverkansprogrammet, eSam, är ett medlemsdrivet program för samverkan mellan 25 myndigheter och SKL. Samarbetet syftar till att underlätta och påskynda digitaliseringen av det offentliga Sverige, www.esamverka.se

Avtalet ska också reglera hur leverantören ska säkerställa att er information inte finns kvar i form av backup eller i olika it-system vid avtalets avslut.

4.5.6 Uppköp av leverantör

Det kan hända att leverantörer, av någon anledning, lägger ner sin verksamhet eller blir uppköpta under avtalsperioden och därmed få andra ägare än när avtalets ingicks. Ni behöver i förväg tänka igenom vilka konsekvenser detta kan medföra. Det kan handla om hur er information blir åtkomligt för leverantörer eller underleverantörer i tredje land.

Ni kan i avtalet särskilt begära att få information om ägarbyten och att ni ska få tillräckligt med tid för att kunna kontrollera de nya ägarna och deras säkerhetsåtgärder innan de tar över avtalet. Möjligheten att avbryta avtalet om de nya ägarna inte uppfyller ställda krav bör också framgå av avtalet.

4.5.7 Förändrade förutsättningar – förändrade villkor

Ni bör avtala om att kunna förändra vissa villkor ifall omvärlden eller hur tjänsten används förändras. Man kan givetvis endast förändra villkor under vissa förutsättningar[24], men ni behöver ta höjd för till exempel nya hot mot informationen, nya rättsliga krav eller att förändringar i användningen av tjänsten gör att överenskomna krav står i konflikt med varandra.

4.5.8 När leverantören har säkerhetskrav på er organisation

I vissa fall kan även leverantören ställa säkerhetskrav på er, eftersom en kunds bristande säkerhet kan äventyra säkerheten såväl för leverantören som hos deras övriga kunder.

De krav som leverantören ställer på er organisation kan till exempel omfatta krav på visst skydd mot skadlig kod, viss brandväggskonfiguration eller viss behörighetshantering. Om leverantören har denna typ av krav ska det framgå i avtalet.

---

24. Lagen om offentlig upphandling (LOU 2016:1145) 17 kap Fullgörande av kontrakt.

4.5.9 Arkivering och gallring

Utifrån rättsliga krav och verksamhetens egna behov ska viss information gallras medan annan måste bevaras under kortare eller längre tid. Det kan därför finnas skäl att ställa särskilda krav i avtalet med externa aktörer på hur gallring och arkivering ska ske.

4.5.10 Kontinuitetsplanering och robusthet

För tjänster där ni har höga krav på tillgänglighet (åtkomst) är det viktigt att ni förbereder er på situationer där det kan uppstå avbrott i tjänsten. Ni behöver utarbetade kontinuitetsplaner så att er verksamhet kan fungera om tjänsten inte är åtkomlig under en kortare eller längre tid. Detta gäller oavsett vad ni avtalat om med leverantören gällande hur tjänsten ska fungera eller om avbrott i tjänsten är förknippat med vite.

4.5.11 Vite

Avtalet behöver reglera möjligheten att kräva vite om säkerhetsåtgärder inte uppfylls. Vitesbeloppen bör sättas på en nivå så att risken minimeras för att leverantören hellre tar ett vitesföreläggande än den ekonomiska kostnad som ett fullföljande av avtalet kan innebära.

4.5.12 Tilldelning av kontrakt

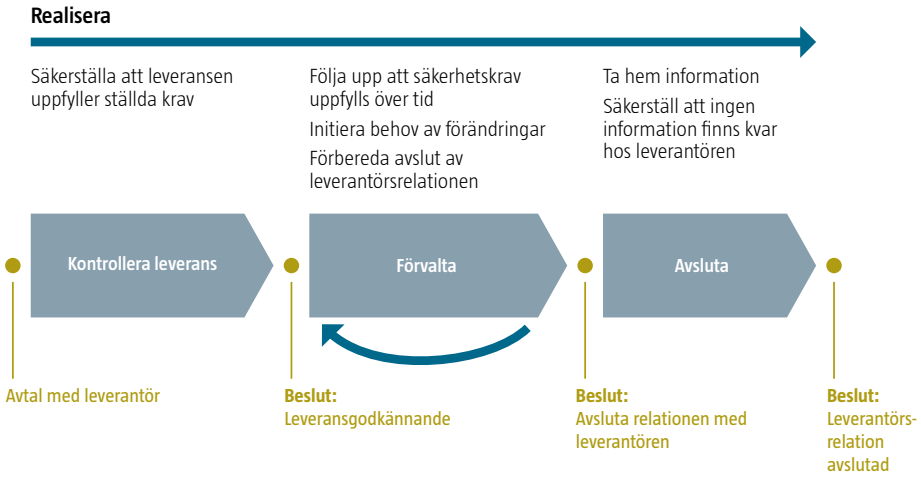
Innan ni fattar ett tilldelningsbeslut och undertecknar avtalet bör ni genomföra en fördjupning av befintlig riskanalys. Denna ska inbegripa den leverantör som ni nu valt samt eventuella underleverantörer. Utgå från den lösning ni valt och de säkerhetsåtgärder som leveransen innehåller och avtalets löptid när ni gör riskbedömningen.

Realisera, förvalta och avsluta upphandlingen

5. Realisera, förvalta och avsluta upphandlingen

Er organisation måste följa upp att leverantören uppfyller det ni avtalat om. Relationen till leverantören kan vara kort, till exempel en enstaka leverans av en vara eller tjänst. Men relationen kan även sträcka sig över en längre tid som när drift av ett it-system upphandlas.

Figur 4. Realiseringsfasen



Källa: MSB utifrån Upphandlingsmyndighetens inköpsprocess.

5.1 Leveransgodkännande

Kontrollera att alla leveranser uppfyller de krav som ni ställt. Detta görs genom att dokumentera resultatet av de verifieringar som ni genomför, oavsett om leveransen gäller en vara eller en tjänst. Hur ett leveransgodkännande ska gå till ska framgå av avtalet.

Vissa leveranser har en period där er organisation och den externa aktören samverkar för att garantera att leveransen går att genomföra. Ni behöver få tid, till exempel för att acceptanstesta ett nytt it-system, och leverantören behöver tid för att rätta till eventuella buggar, fel och funktioner som inte uppfyller de krav och tilldelningskriterier ni avtalat.

Om driften är extern behöver ni och den externa aktören säkerställa att alla viktiga säkerhetsåtgärder fungerar. Ni kanske har avtalat om att ni har rätt att själva kontrollera att er information skyddas i enlighet med avtalet och den externa leverantören kanske behöver åtgärda eventuella brister innan ni accepterar leveransen.

5.2 Uppföljning, kontroll och kvalitetssäkring

Uppföljning och kontroll är viktigt för att kunna bibehålla bland annat säkerheten i den upphandlade produkten eller tjänsten under avtalstiden.

Ni bör regelbundet följa upp de säkerhetsåtgärder som ni i avtalet kommit överens om med er leverantör. Problem som ni eller leverantören identifierar under avtalstiden kan också ge upphov till extra uppföljning.

Under hela avtalstiden bör ni fortlöpande dokumentera överenskommelser av informell karaktär och sådant som kommuniceras muntligt. En strukturerad avtalsförvaltning visar att ni är professionella upphandlare som följer det som har överenskommits och som verkar för en affärsmässig relation med leverantören.[25]

5.3 Förbereda slutet på en avtalsrelation

En avtalsrelation kan avslutas på två sätt:

- genom att avtalstiden tar slut eller
- genom att antingen ni eller leverantören avslutar relationen i förtid.

Det är viktigt att ni säkerställer att ni får tillbaka all information från leverantören oavsett hur relationen avslutas. Dessutom behöver ni se till så att leverantören överlämnar informationen i ett format som såväl ni som andra externa aktörer kan använda.

25. Upphandlingsmyndigheten *Avtalsförvaltning, vägledning nr 2* (2016).

Att upphandla it-system

6. Att upphandla it-system

Detta kapitel lyfter fram det som en organisation speciellt behöver ha i åtanke när den upphandlar it system. Med it-system avser vi här alla informationsbehandlande tekniska system, från fristående produkter till hela it-miljöer som driftas hos den egna organisationen eller externt. Även tjänster som utveckling och anpassning av produkter och miljöer samt olika drifttjänster ingår.

6.1 Klargör var informationen finns

Vid upphandling av it-system behöver ni utgå från er informationsklassning och klargöra var informationen, mjukvaran respektive hårdvaran befinner sig fysiskt. Det påverkar vilka och mot vem kraven ska ställas. Oavsett driftform är det viktigt att ni beaktar ett livscykelperspektiv för informationshanteringen, det vill säga var informationen befinner sig när den delas, bearbetas och lagras och hur den slutligen arkiveras eller förstörs. Det kan underlätta att rita ett flödesschema för att åskådliggöra informationsflödet i den tilltänkta lösningen.

Figur 5 visar schematiskt vem som har åtkomst till information, mjukvara och hårdvara genom att visa var dessa finns fysiskt samt hur ägandeförhållandena ser ut. Figuren är generell, därmed finns även andra varianter och kombinationer av var informationen hanteras. Exempelvis när organisationer samverkar kring informationshantering.

Figur 5. Var informationen och ägandet finns vid olika driftsituationer

FORM	FYSISKT HOS ORGANISATION	FYSISKT HOS LEVERANTÖR	ÄGANDE HOS ORGANISATION	ÄGANDE HOS LEVERANTÖR
Egen drift av system	i m h		i m h	
Utkontraktering	i	i m h	i	m h
Molntjänst	i	i m h	i m	h

i *Information* m *Mjukvara* h *Hårdvara*

Källa: MSB

Om ni ska köpa it-system för egen drift, översta raden i figur 5, så finns information, mjukvara och hårdvara fysiskt hos er. Ni hanterar uppdateringar av systemen utan att leverantören behöver ha åtkomst till dem.

I fallet med utkontraktering, mellersta raden i figur 5, så kommer både hårdvara och mjukvara finnas fysiskt hos leverantören, medan informationen är åtkomlig för både er och leverantören – åtminstone under den tid ni bearbetar informationen. Som kund gäller det att säkerställa att de säkerhetsåtgärder som ni använder i samband med åtkomst motsvarar det skyddsbehov som er klassning av informationen ledde fram till (se avsnitt 3.4.1 om fördjupad informationsklassning) samt att leverantören skyddar er information i sin it-miljö. Molntjänster är en typ av utkontraktering. I figur 5 tillhandahåller leverantören mjukvara för behandling av information.

6.2 Upphandling av it-system för drift och förvaltning i egen regi

När ni som organisation väljer att köpa en färdig produkt (som till exempel it-system, verktyg, körbar programkod eller program för behandling av information) och därefter sköter drift och förvaltning i egen regi behöver minst följande uppmärksammas.

6.2.1 Systemet ska kunna integreras i befintlig driftmiljö

Inför valet att köpa en eller flera produkter är det viktigt att ni, förutom de rent säkerhetsmässiga kraven, även tar med de krav som krävs för att den nya produkten ska passa ihop med er egen it-miljö till exempel krav på interoperabilitet.

6.2.2 Leasing – att hyra it-utrustning

I stället för att äga it-utrustningen, såsom datorer, telefoner, skrivare eller scanner kan ni välja att hyra (eller *leasa*) den. Det innebär att själva ägandet är kvar hos leverantören, medan ni har en nyttjanderätt.

Om ni väljer att leasa it-utrustning så behöver ni ställa krav på hur leverantören får hantera informationen i utrustningen. Det kan exempelvis handla om att hårddiskar och skrivartrummor där er information hanteras ska förstöras eller raderas på ett säkert sätt och att ni har rätt att närvara när utrustningen förstörs. Står utrustningen hos er kan kravet vara att den inte får lämna era lokaler innan ni själva raderat informationen.

6.3 Upphandling av utkontraktering och molntjänster

Vid utkontraktering låter en organisation en extern aktör sköta en eller flera delar av organisationens it-stöd som annars skulle ha utförts i en egen regi. Sådan ukontraktering kallas ibland i dagligt tal för outsourcing. Utkontraktering kan exempelvis ske genom molntjänster.

6.3.1 Sourcingstrategi – för säkrare upphandling

Om er organisation har en sourcingstrategi utgör den ett viktigt underlag i upphandlingsarbetet. En sourcingstategi är ett ställningstagande rörande styrningen av det strategiska arbetet med organisationens informationshantering. Den beskriver vilka delar av er verksamhets långsiktiga behov och mål som bör uppnås med hjälp av utkontraktering av något slag (inklusive molntjänster). Sourcingstrategin bör även beskriva ansvar och roller i såväl upphandling som i långsiktig förvaltning av upphandlade it-tjänster. Sourcingstrategi är riskbaserad och behöver därför uppdateras när hot, risker och rättsliga krav förändras. Den ska relatera till organisationens it-strategi.

6.3.2 Molntjänster är en form av utkontraktering

Molntjänster definieras av Pensionsmyndigheten som tjänster som tillhandahålls med nätverksåtkomst och med möjlighet till resursdelning, snabb skalbarhet, självbetjäning och betalning efter användning eller volym. Begreppet inkluderar infrastrukturella tjänster, plattformstjänster och mjukvarutjänster som kan tillhandahållas på olika sätt: från publika tjänster med okänd global lagring till tjänster som dedikeras åt endast en användare och där infrastrukturen kan hanteras av användaren själv eller av annan aktör på en bestämd plats. Molntjänster kan ses som en form av utkontraktering med de särskilda kännetecken som ryms inom definitionen. Molntjänster skiljer sig dock åt från traditionell utkontraktering i bland annat affärsmodell och hur de organiseras[26].

6.4 Upphandling av it-utveckling

Behov av it-utveckling kan uppstå både när organisationen väljer att ta fram ett it system från grunden och när organisationen behöver anpassa ett inköpt it-system för att uppfylla sina behov.

---

26. *Molntjänster i staten – En ny generation av utkontraktering*, Pensionsmyndigheten 2016.

Har er organisation ett väldefinierat arbetssätt för att styra it utveckling inklusive att kontrollera att leveranser sker på ett strukturerat sätt underlättar det vid upphandling. Det är då lättare att ställa krav på vilken kompetens och vilka resurser som behövs samt att bedöma om tidsplanen är rimlig.

Tänk på att när ni har gjort ett leveransgodkännande behöver ni troligtvis fortsatt utveckling, till exempel i form av support för rättning av buggar eller fel som upptäcks eller anpassning mot era andra tjänster och programvaror som utvecklas över tid. Detta är specifika och viktiga krav som måste regleras i avtalet.

6.4.1 Ställ specifika krav för att säkerställa dataintegritet

Man kan genomföra ett it-utvecklingsprojekt på olika sätt. Beroende på om ni väljer att bedriva utvecklingsarbetet inklusive olika typer av tester med konsulter i er egen utvecklingsmiljö eller om utveckling och test sker helt hos leverantören behöver kravställningen se olika ut.

Sker utvecklingen hos extern leverantör behöver ni, till exempel ställa krav på hur de ska säkerställa dataintegriteten i den framtagna mjukvaran (koden) och att endast behöriga har åtkomst till den. Samma sak gäller för testdata, testresultat och hårdvara.

Det finns också olika kombinationer av hur organisationer kan samarbeta med sina leverantörer under it utveckling. Ibland kan konsulter, av utrymmesskäl hos organisationen, behöva sitta i sina lokaler men ha fjärråtkomst till er utvecklingsmiljö där allt arbete sker. I dessa fall behöver ni komma överens om hur åtkomsten ska ske för att vara säker.

6.4.2 Reglera licenser och ägandeskap för kod

Oavsett hur ni beslutar att själva it-utvecklingen ska ske behöver ni reglera användandet av licenser och ägandeskapet för den programkod som ska utvecklas. Licenser kan behövas både under utvecklingen av programkoden och för att den kod leverantören tar fram senare ska fungera i er driftmiljö. Beroende på vad ni avtalat kring ägandeskapet av programkod kan ni behöva säkerställa tillgång till källkoden, för att kunna få en kontinuitet i leveransen om leverantören får problem, vid exempelvis uppköp, flytt eller konkurs.

6.5 Särskilt om informationssäkerhetskrav vid upphandling av it-system

Utöver de informationssäkerhetskrav som beskrivs i kapitel 4 tar det här avsnittet upp det som är av särskilt vikt vid upphandling av it-system. Beskrivningarna utgår från att en kommersiell tjänst ska upphandlas. Flertalet av avsnitten är också relevanta även om tjänsten inte behöver upphandlas för att den är gratis eller är ett samarbete mellan olika offentliga aktörer.

6.5.1 Fler frågor som ofta behöver besvaras av den som upphandlar

I kapitel 4 listas ett antal frågor som den som upphandlar kan behöva svara på avseende organisation, personsäkerhet och den fysiska miljön. Här nedan finns ytterligare frågor om it-miljön som kan behöva besvaras vid upphandling av it-system.

Område: It-miljö

- Hur styrs åtkomsten till er information? Vad kan ni styra gällande åtkomst till exempel er driftmiljö (tid när leverantören kan komma åt, beställning av öppning och stängning av åtkomst till er miljö)? Hur bör behörighetshanteringen se ut? Vilka olika åtkomstgrupper behövs inklusive behörigheter för att genomföra support samt teknisk administration av it miljön?
- Vilken typ av spårbarhet (loggning) ska finnas för användaraktiviteter och teknisk administration? Hur ska ni granska dessa loggar?
- Ska produkten vara certifierad av någon tredjepart enligt t.ex. Common Criteria?
- Hur ska ni ge åtkomst till och/eller överföra information mellan er organisation och leverantören?
- Hur ska ni skydda informationen under lagring och överföring? Vilka krypteringslösningar ska användas?
- Vilken tillgänglighet i tjänsten (inklusive återställelsetider) måste leverantören uppfylla?
- Ska leverantören ansvara för att det finns strukturerad ändringshantering och testmiljöer för att prova uppdateringar?
- Vilka krav ställer ni på leverantörens rutiner för hantering av sårbarheter i it-miljön?
- Hur är leverantörens it-arkitektur uppsatt och konfigurerad, och vilka säkerhetsåtgärder är införda? Ger detta sammantaget informationen tillräckligt skydd?

- Skiljer leverantören driftmiljö och testmiljö från varandra? Har de några rutiner för vilken information som de får hantera i olika it-miljöer? Hur sker godkännandet av att flytta information från test till drift?
- Vem ansvarar för licenser och för att uppfylla immateriella rättigheter? Vilket skydd mot skadlig kod har leverantören? Finns skydd för att upptäcka försök till och förhindra obehörig åtkomst?
- Vilka krav har ni på säkerhetskopiering av informationen? Hur ska leverantören testa säkerhetskopior? I vilket format ska leverantören lagra informationen? Vad är maximal tid för att återläsa informationen?
- Hur vill ni att leverantören ska rapportera de eventuella incidenter (hos leverantören) som kan orsaka konsekvenser för er? Har leverantören något arbetssätt för hur de ska upptäcka, hantera och utreda incidenter?
- Vilken support vill ni att leverantören ska tillhandahålla?
- Behöver ni reglera åtkomst till källkod på något sätt?
- Hur ser flexibiliteten ut, det vill säga er möjlighet att skala upp användningen av tjänsten på ett ekonomiskt fördelaktigt sätt?
- Om leveransen är att utveckla programvara, har leverantören:
  - » Rutiner och miljöer för att hantera kod på säkert sätt?
  - » Rutiner för säker programmering?
  - » Testmiljöer och testdata som säkerställer slutproduktens kvalitet och uppfyller rättsliga krav till exempel avseende behandling av personuppgifter?

6.5.2 Reglering mellan organisation och leverantör samt avtalsförvaltning

När en organisation använder molntjänster eller annan utkontrakterad tjänst är det ett stort antal förhållanden som behöver regleras. Precis som vid alla typer av upphandling är dokumenterade och tydliga ansvarsförhållanden av stor vikt. Det är också viktigt att avtala exakt vilka typer av säkerhetsåtgärder som ingår, exempelvis regelbundna tester av återläsning av backuper, skydd mot skadlig kod, nivån på skydd mot så kallade DDoS-attacker, övningar att hantera incidenter tillsammans med organisationen och så vidare.

Innan ni väljer leverantör behöver ni identifiera vilken information leverantören kommer att ha åtkomst till samt vilka skyddsåtgärder som ni behöver avtala om (se kap 4.4.5). Detta arbete utgör ert underlag för att kunna verifiera exempelvis vilka säkerhetsåtgärder hos

leverantören som ni kan acceptera som de är, godkänna, eller vilka kompletterande åtgärder som behövs samt vilka brister i säkerheten som inte går att åtgärda inom rimlig tid eller för rimlig kostnad.

Avtalet ska tydligt beskriva vilka säkerhetsåtgärder leverantören ska vidta. Dessa ska omfatta hela avtalstiden och det ska vara tydligt dokumenterat vem som är ansvarig för respektive åtgärd. (se kap 3.5).

Vissa säkerhetsåtgärder kan behöva aktivt deltagande från båda parter samt från underleverantörer, men det är bara en av parterna som kan ha huvudansvar för att en åtgärd införs och är effektiv.

6.5.3 Krisberedskap, force majeure och dylikt

Om ni upphandlar för att säkerställa behovet av kontinuitet och driftsäkerhet vid kriser behöver ni tydliggöra leverantörens ansvar genom att ta in en klausul avseende hur force majeure i avtalet inte gäller under vissa förutsättningar. På detta sätt har ni kontroll över vilka händelser som enligt avtalet ska utgöra force majeure.

Force majeure är ett begrepp som förekommer inom avtalsrätten. Den beskriver under vilka onormala eller oförutsedda händelser som en avtalspart inte är bunden av överenskommelserna i avtalet. Force majeure kan bland annat omfatta naturkatastrofer, statliga ingripanden, krig, arbetskonflikt och liknande[27].

Precis som vid alla annan typ av upphandling bör avtalet reglera möjligheten att kräva vite om säkerhetsåtgärder inte uppfylls.

6.5.4 Användande av underleverantörer

Av särskild betydelse för informationssäkerheten vid utkontraktering är att skaffa sig kontroll över situationer där leverantören använder underleverantörer. Användandet av underleverantörer påverkar ansvarsförhållandena och kan därför av rättsliga skäl omöjliggöra användandet av en viss leverantör eller vissa molntjänster.

Den som är personuppgiftsansvarig behöver kunna försäkra sig om att personuppgiftsbiträdet skyddar informationen tillräckligt då den personuppgiftsansvariga alltid har ansvar för uppgifterna.

För tjänster som bygger på att informationen kan förvaras i princip var som helst i världen[28] behöver ni vara extra noggranna med att identifiera samtliga underleverantörer och vilken information de hanterar och på vilket sätt i den tjänst ni upphandlat.

---

27. MSB har givit ut en vägledning för upphandling av samhällsviktig verksamhet *Upphandling till samhällsviktig verksamhet – en vägledning*. Publikationsnummer MSB840 - september 2018.
28. Överföring av personuppgifter till tredje land, Datainspektionen.se.

6.5.5 Vetskap om de andra kunderna

I en delad it-miljö, så som molntjänster, utnyttjas alla informationsbehandlande resurser av de som upphandlat tjänsten. Det som delas kan till exempel vara internetanslutning, lastbalanserare, processorkraft och minnesutrymme. Det innebär att exempelvis överbelastningsattacker kan drabba samtliga kunder hos en leverantör – även om attacken var ämnad mot en specifik kund.

Det kan också hända att utrustning som ni delar med andra organisationer kan beslagtas av rättsvårdande myndigheter och därför bli otillgängliga för samtliga kunder i den delade miljön. I värsta fall kan detta påverka ert rykte eller varumärke, till exempel ifall ni har råkat välja en leverantör som erbjuder tjänster till misstänkt kriminella.

Att få kännedom om vilka kunder som leverantören har kan vara svårt. Ofta kan man dock få en fingervisning om leverantören säljer sina tjänster till alla eller om de väljer sina kunder utifrån kriterier så som ekonomisk stabilitet, affärsidé eller motsvarande.

6.5.6 Åtkomst till självbetjäningsportal och liknande

Molntjänster har, till skillnad från många andra tjänster som utkontrakteras, ofta ett självbetjäningsgränssnitt där kunden administrerar vilka tjänster leverantören ska tillhandahålla. Självbetjäningsgränssnittet kan ge möjlighet att välja allt från antal servrar, vilka krav kunden ställer på nätverkskonfiguration till generella eller kundanpassade gränssnitt för åtkomst till konto- och behörighetsadministration.

Detta gränssnitt kan antingen vara anpassat mot manuell administration (webbgränssnitt) eller automatiserad via gränssnitt mot kundens administrativa verktyg (API). Då gränssnittet är en central del i förvaltningen av tjänsterna är det av stor vikt att ni kontrollerar att överföringen och behörighetshanteringen för åtkomst till självbetjäningsgränssnittet är tillräckligt skyddad.

6.5.7 Leverantörens åtkomst till informationen

Vid utkontraktering där ni låter en leverantör tekniskt bearbeta er data till exempel en molntjänst eller där leverantören tillhandahåller driftmiljön är det viktigt att reglerar leverantörens personals åtkomst till era it-system och er information. Det handlar såväl om fysisk åtkomst till hårdvara (servrar och lagringsutrustning) som logisk åtkomst (via konsoler, driftövervakning och tjänster) samt hur denna åtkomst kan spåras genom till exempel loggning och övervakningsfilmer.

I de fall en leverantör behöver behörighet och åtkomst till er interna driftmiljö (t.ex. fjärrsupport) bör denna åtkomst ske på ett kontrollerat sätt med krav på till exempel autentisering, loggning, uppföljning och utbildning. Ifall leverantören endast behöver åtkomst till er it-miljö i vissa specifika situationer kan ni överväga att enbart bevilja åtkomst under en viss tid och därefter stänga åtkomstmöjligheten helt. Exempel på hur det kan se ut är att leverantören behöver tillgång fyra timmar en gång i månaden eller när något speciellt hänt och ifall er information är väldigt känslig. Ska leverantören enbart ge support vardagar under kontorstid bör it-miljön inte vara åtkomlig övrig tid utan speciell anledning.

6.5.8 Inlåsningseffekter

En av de fördelar med utkontraktering som ofta lyfts fram är den flexibilitet som kunden erbjuds. Flexibiliteten gäller dock ofta bara inom en viss it-miljö hos den externa leverantören vilket skapar risk för inlåsning. Inlåsning innebär att leverantören hanterar informationen i ett format, eller på en utrustning, som gör det omöjligt, svårt eller kostsamt för er att flytta informationen till annan leverantör eller till er egen driftmiljö om ni anser det nödvändigt för att leverantören inte uppfyller de säkerhetsåtgärder som ni avtalat om.

Vid en utkontraktering behöver ni ställa krav kring hur ett eventuellt byte av leverantör ska gå till. Det är viktigt att ni analyserar på vilket sätt en eventuell framtida migrering ska ske och ni behöver ställa specifika krav dels gällande möjligheten att flytta information, dels gällande informationens format. Ni bör också kräva att leverantören ska vara behjälplig.

Om leverantören går i konkurs kan ni bli tvungna att ta hand om er information och era tjänster i ett akut läge. Med andra ord är det risk för såväl avbrott i leveranser som för informationsförluster – om inte informationen redan är i ett format som ni eller någon annan leverantör kan hantera.

6.5.9 Certifiering och skyddsprofiler

Genom att ställa krav på att använda en certifierad produkt behöver leverantören visa hur de uppfyller krav ställda i en formell kravlista (skyddsprofil, även kallad Protection Profile, PP) samt att produkten genomgått en ackrediterad utvärdering av en tredje part för att visa att kraven i listan uppnås.

Common Criteria (CC)[29] är en internationell standard för kravställning, säkerhetsgranskning och certifiering av säkerhet i it-produkter. CC erkänns internationellt och i flera länder är det obligatoriskt att kravställa utifrån en skyddsprofil när man ska köpa in it-produkter i kritiska infrastrukturer och att leverantören visar att de certifierat produkten innan man köper och installerar produkten.

Skyddsprofiler är it-säkerhetskravspecifikationer för specifika produktkategorier, t.ex. USB-minnen, brandväggar och nätverksprodukter. En skyddsprofil innehåller detaljerade krav på vad produkten behöver uppnå för skydd för specificerade risker. Ni kan använda en redan befintlig kravspecifikation eller ta fram en ny genom att utgå från en befintlig. När ni väljer skyddsprofil behöver ni säkerställa att den är framtagen för den nivå av skydd ni behöver och de risker er organisation har identifierat.

6.5.10 Rättsliga risker

När det gäller utkontraktering inklusive molntjänster kan de risker som är relaterade till rättsliga krav delas in i två kategorier:[30]

- Risker gällande osäkerheten kring vilket lands rättsliga regelverk som ska tillämpas.
- Risker kopplade till sakfrågor i det rättsliga regelverk som är tillämpligt för den information som ska hanteras utanför er organisation.

Om det inte framgår i avtalet vilket lands rättsliga regelverk som ska tillämpas går det inte att bedöma vilket skydd informationen faktiskt har.

När annat lands lagstiftning gäller enligt avtalet finns det ibland förutsättningar att ändå avtala om säkerhetsåtgärder medan det i andra fall finns hinder för detta.

Någon fullständig lista över rättsliga risker går inte att göra, utan man måste utreda riskerna med att hantera informationen utanför Sverige inför varje upphandling där det blir aktuellt. Det kan finnas hinder mot att utkontraktera personuppgifter eller uppgifter som bedömts skyddas av sekretess till annat land om inte särskilda säkerhetsåtgärder vidtas såsom kryptering av informationen.

29. ISO/IEC IS 15408.
30. https://cloudsweden.wordpress.com/2011/05/17/juridisk-checklista-for-kop-av-molntjanster/

Begreppsförklaringar

Begreppsförklaringar

BETECKNING	BETYDELSE
Avropa	Tilldelning av kontrakt från ett ramavtal. Detta görs genom att begära leverans av en vara eller tjänst utifrån ramavtal. [Konkurrensverket[31]]
Avveckling	Process som syftar till att minska eller avskaffa it system eller it-drift på ett definierat sätt.
CISO	Chief information security officer (eng), samlingsnamn för informationssäkerhetsansvarig, informationssäkerhetssamordnare, informationssäkerhetsstrateg m.m.
Drift	Den dagliga driften av en it-tjänst, ett it-system eller en konfigurationsenhet [ITIL ordlista]
Extern aktör	Andra aktörer än den egna organisationen, till exempel leverantörer eller underleverantörer som antigen är privata eller offentlig organisationer. Leverantör eller samverkanspart?
Förvalta	Åtgärder för att säkerställa en regelbunden skötsel av ett it-system, så att förändringar styrs och samordnas.
Information	Innebörden av data. Med data avses representation av fakta, idéer eller liknande i en form lämpad för överföring, tolkning eller bearbetning av människor eller av automatiska hjälpmedel [SS-TR 50:2015]
Informations-säkerhet	Bevarande av konfidentialitet, riktighet och tillgänglighet hos information. [SS-TR 50:2015]
Informa-tionsägare	Den person eller enhet som har ansvaret för den information som skapas och hanteras inom den egna verksamheten. [SS-TR 50:2015]
It-system	Ett system med teknisk utformning som behandlar, det vill säga. en åtgärd eller kombination av åtgärder såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring) information.
Leverantör	Den som på marknaden tillhandahåller varor eller tjänster. [Konkurrensverket]
Mjukvara	Avser exekverbar kod som körs på hårdvara och som är avsedd för datorns inre arbete, och verktygsprogram för datahantering (till exempel filkonvertering) samt tillämpningsprogram (ordbehandling eller verksamhetssystem) och programbibliotek.
Molntjänst	En teknik där resurser, som till exempel processorkraft, lagring och funktioner, tillhandahålls som tjänster via internet eller annat nätverk. Molntjänster kategoriseras oftast som någon av tre olika typer av tjänster: • Infrastruktur som tjänst förkortas **IaaS** *Infrastructure as a Service*. • Utvecklingsmiljö som tjänst förkortas **PaaS** *Platform as a Service.* • Mjukvara som tjänst förkortas **SaaS** *Software as a Service.* [SS-ISO/IEC 17788:2014]
Upphandling	De delar av inköpsarbetet som omfattar arbetet från att planera en specifik upphandling till att ett avtal tecknats. I detta finns anbudsförfrågan, leverantörskvalificering, leverantörsdialog, anbudsvärdering, förhandling, avtalsskrivning m.m. [Upphandlingsmyndigheten]

31. Vanligt förekommande upphandlingstermer Ordlista, konkurrensverket.se/upphandling/fragor-och-svar/ordlista

Myndigheten för samhällsskydd och beredskap (MSB)
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB1177 - november 2018 ISBN 978-91-7383-802-3