UMEÅ UNIVERSITET

VÄGLEDNING

ATT UPPHANDLA PÅ ETT SÄKERT SÄTT

Innehåll

1. Att upphandla på ett säkert sätt

Denna vägledning bygger på Myndigheten för samhällsskydd och beredskap (MSB) vägledning – Upphandla informationssäkert - MSB1177 - november 2018.

I en upphandling av IT-relaterade tjänster måste utgångspunkten vara att identifiera vilken funktion Umeå universitet 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 vi inte känner till utesluts ur upphandlingen.

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.*

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. Bild 1 beskriver en generisk upphandling i processform där aktiviteter där informationssäkerhetsaspekter och lagkrav särskilt måste beaktas är markerade.

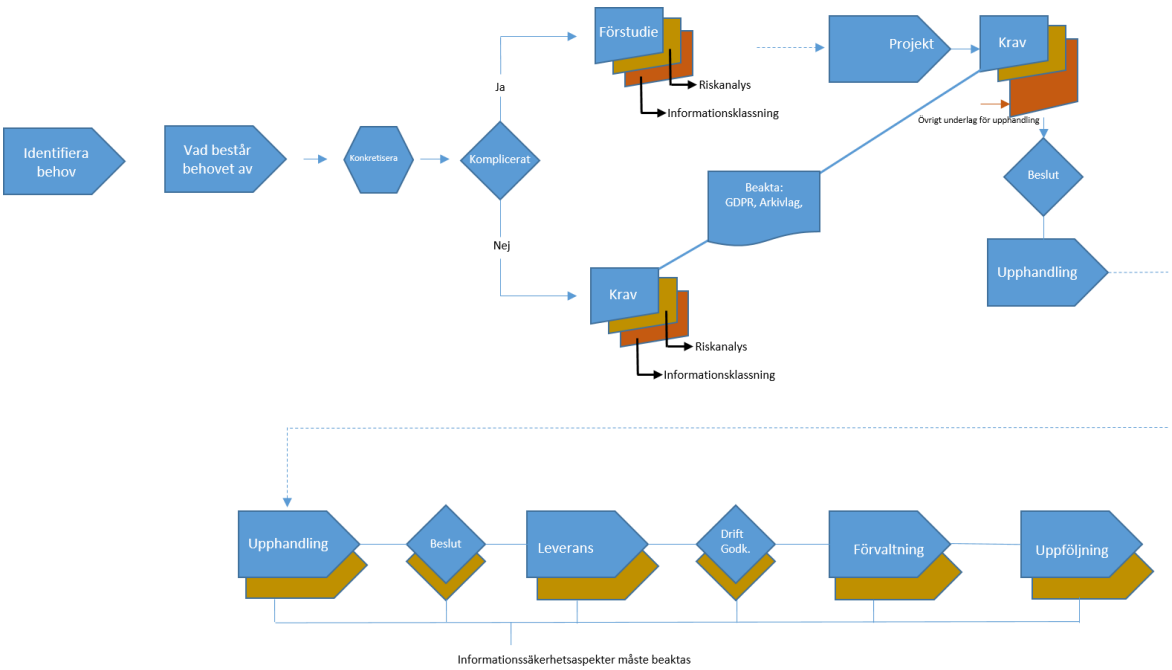

Bild 1. Generisk process (MSB1177 - november 2018)

För att kunna genomföra en upphandling av IT-tjänster finns stöd att få inför själva upphandlingen utöver er egen verksamhetskompetens och universitetets upphandlingskompetens för att identifiera krav och behov:

- Säkerhetskompetens för att bedöma risker och kunna ställa rätt säkerhetskrav utifrån genomför klassning av aktuell informationshantering och riskanalys

- IT-kompetens för att göra bedömningen hur tjänsterna ska kunna integreras på lämpligt sätt i befintlig infrastruktur

- Juridisk kompetens för att fastställa de rättsliga förutsättningarna och kraven och se till att dessa uppfylls

- Arkiv- och informationshanteringsinriktad kompetens för att kunna beskriva krav på gallring och arkivering utifrån den dokumenthanteringsplan som finns på Umeå universitet och som i sin tur bygger på Riksarkivets föreskrifter.

Det är viktigt att betona att ovan nämnda kompetenser behövs redan på ett tidigt stadium i processen. Bland annat kraven på informationssäkerhet och de legala kraven kan påverka de grundläggande förutsättningarna för upphandlingen. **Under arbetet med kravställning ska därför ITS rådfrågas angående tekniska krav och jurister rådfrågas beträffande legala krav**.

2. Identifiera krav

För att fastställa säkerhetskraven inför en upphandling bör inventering göras av vilka informationstillgångar det upphandlade IT-systemet eller IT-tjänst kommer att hantera. Informationstillgångarna klassificeras sedan enligt universitetets modell för informationsklassning. Klassningen ligger till för att precisera den säkerhetsprofil som aktuell upphandling ska uppfylla och för att kunna avgöra vilka krav som kan uteslutas. I universitetets modell för informationsklassning finns en referenstabell med ett antal inom universitetet förekommande informationstyper och dess säkerhetsprofil som kan omvandlas till en kravbild för externa leverantörer.

För att komma igång med kravställning kan nedanstående sju (7) punkter, enligt MSB, användas till att formulera krav och dessutom utgöra stöd vid informationsklassning och riskanalys.

- En utgångspunkt är att leverantören ska kunna erbjuda sitt utbud på olika skyddsnivåer. Det innebär en möjlighet för universitetet att göra en bedömning mellan risk och kostnad

- Att leverantörerna kan erbjuda olika skyddsnivåer är också betydelsefullt eftersom vår 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 oss finns en överhängande risk för att vi 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, eller någon annan standard bör ingå i kravställningen

- Standarder ger ett underlag för en bra kommunikation mellan universitetet och leverantör

- När en leverantör använder standarder för styrning av sitt arbete med informationssäkerhet ger det en tydlig indikation om att man har prioriterat området

- En certifiering kan ytterligare stärka intrycket av en säkerhetsmedveten leverantör som har inkluderat informationssäkerhet i sin affärsmodell.

Utöver ovanstående sju (7) punkter finns ett antal konkreta säkerhetskrav som MSB anser bör ha genererats via informationsklassning som till exempel:

1. Hur åtkomst styrs till informationen
2. Hur loggning ska ske och hur loggar granskas
3. Åtkomst till relevant dokumentation hos leverantören som påverkar leveransen
4. Krav på tillgänglighet
5. Vilka återställelsetider som leverantören måste uppfylla vid avbrott
6. Krav på säkerhetskopiering
7. Hur incidenter ska rapporteras och hanteras (Både personuppgifter och IT (Hård och mjukvara))
8. Vilken support leverantören ska kunna tillhandahålla vilka anställningskontroller som leverantören ska genomföra för de anställda som får tillgång till kundens information
9. I vilken omfattnings som leverantören får anlita underleverantörer och vilka krav som ska ställas på dessa, t.ex. spårbarhet
10. Hur överföring av information ska ske mellan Umu och leverantör
11. Vid behov, rutiner för gallring och metoder för arkivering samt dataportabilitet
12. Möjlighet för Umu att initiera externa revisioner hos leverantören

Efter detta gäller det att kvalificera kravlistan 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? Och vilka bör-krav värderar Umeå universitet högre än andra bör-krav?

Vilka krav kan anges exakt och vilka krav bör lämnas öppet för anbudsgivare att presentera egna lösningar? 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. Några exempel är:

- Loggning där det bör beskrivas vilka loggar och vilken statistik som universitetet ska ha tillgång till
- Hur incidentrapportering ska ske
- Universitetets åtkomst till relevant dokumentation hos leverantör.

Behovsägaren bör göra riskanalys där kompletterande krav framkommer och där legala krav särskilt klargörs innan upphandling. I de fall behovet rör molntjänster t finns legala risker till exempel, hur skyddet av personuppgifter ska upprätthållas och när informationen hanteras i andra länder utanför EU/ESS. Umeå universitets rekommendation är att inte behandla uppgifter som omfattas av sekretess i molntjänster. Vidare ska känsliga eller integritetskänsliga personuppgifter inte behandlas i molntjänster utan att en mer ingående risk- och sårbarhetsanalys genomförts och att konstaterade nödvändiga säkerhetsåtgärder vidtagits.

3. Samråd vid säkerhetsskyddad upphandling

En statlig myndighet som har för avsikt att göra en säkerhetsskyddad upphandling med säkerhetsskyddsavtal (SUA) ska i vissa fall upprätta en särskild säkerhetsskyddsbedömning och samråda med Säkerhetspolisen innan ett sådant förfarande inleds.

Reglerna gäller statliga myndigheter som har för avsikt att genomföra en upphandling som innebär krav på säkerhetsskyddsavtal på nivå 1, om något av följande krav uppföljs:

- leverantören kan få tillgång till eller möjlighet att förvara säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen hemlig eller högre utanför myndighetens lokaler, eller

- leverantören kan få tillgång till säkerhetskänsliga informationssystem utanför myndighetens lokaler och obehörig åtkomst till systemen kan medföra allvarlig skada för Sveriges säkerhet.

Innan upphandlingsförfarandet inleds ska myndigheten upprätta en särskild säkerhetsskyddsbedömning. Med säkerhetsskydd avses:

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

Myndigheten ska också samråda med sin tillsynsmyndighet, som är Säkerhetspolisen eller Försvarsmakten. Den upphandlande myndigheten ska samråda med Säkerhetspolisen innan upphandlingsprocessen inleds. Normalt sett anses upphandlingsförfarandet vara inlett när den upphandlande myndigheten annonserar upphandlingen. Ansökan om samråd ska alltså göras innan dess.

På Säkerhetspolisens hemsida under fliken säkerhetsskydd ges mer detaljerad information i ämnet.

Referensdokument
Instruktion – informationsklassning, Umu
Instruktion – Risk och sårbarhetsanalys, Umu

Regel – Säker informationshantering, Umu