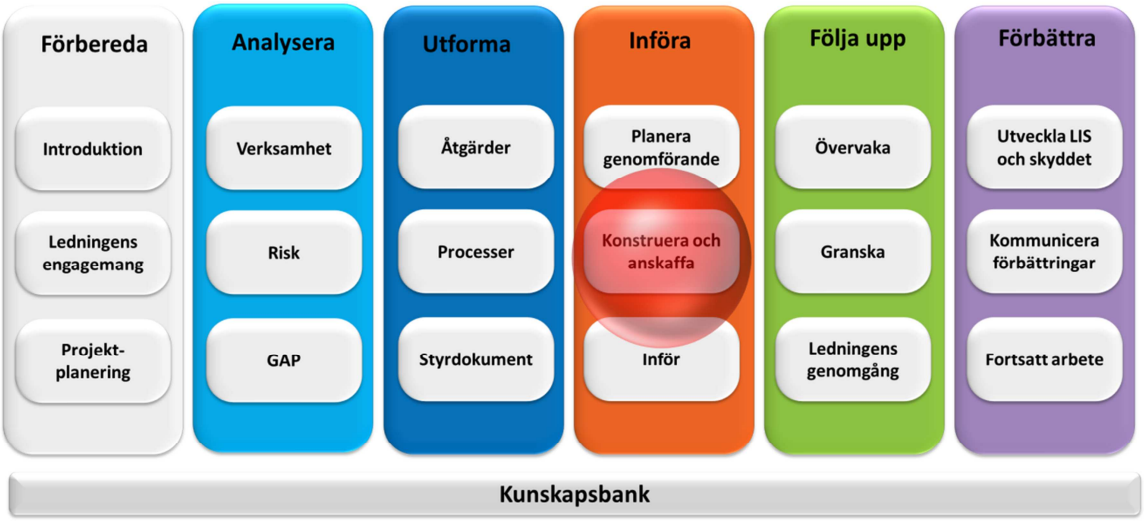
Myndigheten för samhällsskydd och beredskap

Konstruera och anskaffa



Det här dokumentet är en del av metodstödet som finns att tillgå på www.informationssäkerhet.se

Författare
Helena Andersson, MSB
Jan-Olof Andersson, RPS
Fredrik Björck, MSB konsult (Visente)
Martin Eriksson, MSB
Rebecca Eriksson, RPS
Robert Lundberg, MSB
Michael Patrickson, MSB
Kristina Starkerud, FRA

Publicering
Denna utgåva publicerades 2011-12-15

Innehållsförteckning

1. Inledning

Flera av de inplanerade leveransobjekten behöver antingen konstrueras eller anskaffas. Med konstruktion menas det som organisationen utvecklar själv, och anskaffning gäller sådant som köps in utifrån. Vad som ska konstrueras och vad som ska anskaffas framgår av den dokumenterade tidplanen (se delprocessteget planera genomförande) som visar vilka aktiviteter som måste genomföras för varje leveransobjekt. Det kan gälla ett beslutat intrångsdetekteringssystem som ska köpas in, installeras, konfigureras och införas. Det kan också handla om att ta fram en utbildning till medarbetarna. Tidsplanen visar dessutom vem som är ansvarig för att ta fram objektet.

I det här steget, konstruera och anskaffa, ingår alla delaktiviteter som krävs för att ta fram leveransobjektet så att det är klart att införa.

Det finns många generella metoder och principer för att utveckla verksamheter och system, och det gäller även anskaffning av tjänster och produkter. Många av metoderna kan med fördel användas även i det här sammanhanget och de flesta innehåller vissa generella steg. Generella steg i de flesta vanliga metoder är följande:

Generella steg i metoder för konstruktion och anskaffning:

- Specificera kraven
- Konstruera eller anskaffa säkerhetsåtgärden
- Överlämna säkerhetsåtgärden till införande

Den som ansvarar för leveransobjektet har också ansvar för samtliga arbetsuppgifter, även om själva utvecklingsarbetet (eller upphandlingsarbetet) delegeras till andra.

Den här metodbeskrivningen kommer att fokusera på det som är specifikt för arbetet med att konstruera och anskaffa komponenter som är avsedda för informationssäkerhet. Dokumentet innehåller alltså inga detaljer kring olika utvecklingsmetodiker.

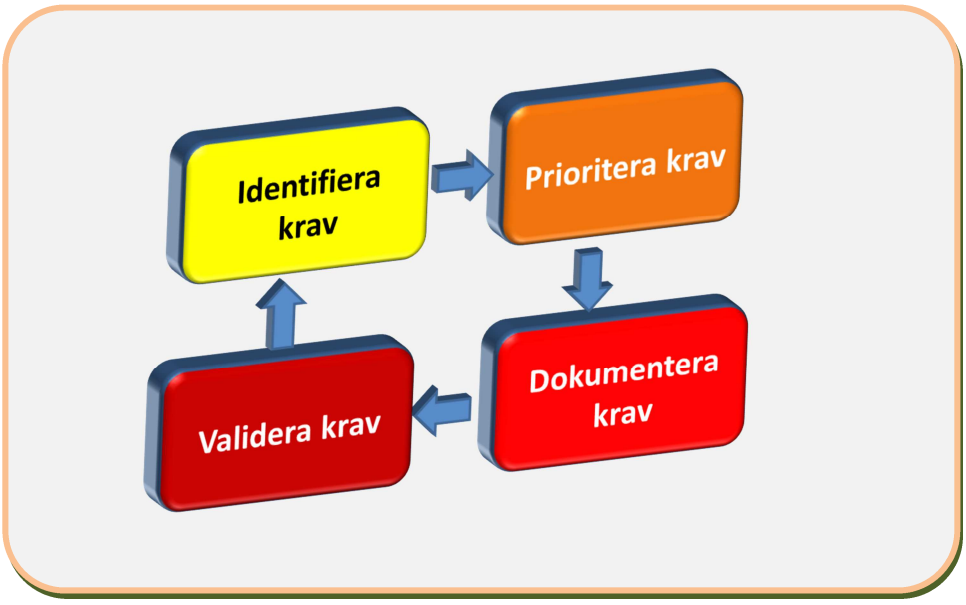
2. Arbetsuppgifter

2.1 Specificera krav

”Som man frågar får man svar” är ett känt talesätt, och det gäller i högsta grad när man ställer krav på en säkerhetsåtgärd eller en säkerhetsprocess. När ett utvecklingsprojekt går snett beror det ofta på brister i kravställningen, till exempel att ett krav blir feltolkat eller rentav helt glöms bort. Misstaget blir dock väldigt kostsamma om det upptäcks först när systemet är färdigt, eller ännu värre – när det är satt i drift.

Det är en fördel att arbeta iterativt, det vill säga kontinuerligt, med att specificera kraven. Den ansvarige kravställaren lyckas knappast pricka in en komplett kravlista från början, utan man får i stället utgå från att kraven måste ses över under hela utvecklingsarbetet. Mot slutet bör dock förändringarna vara ganska små. Varje iteration, det vill säga upprepning av kravspecificeringen, består av ett antal steg som varierar beroende på vilken metodik man använder. Den metodik som illustreras här består av de fyra grundläggande stegen som visas i figur 1. Om leveransobjektet ska köpas in (anskaffas) är det viktigt att komma överens med leverantören om kontinuerliga uppföljningsmöten för att se över kraven.

Figur 1. Viktiga moment för att iterativt specificera kraven på en säkerhetsåtgärd eller säkerhetsprocess.



2.1.1 Identifiera och gruppera krav

Beställaren av en säkerhetsåtgärd eller en säkerhetsprocess har ofta en bild av hur lösningen ska se ut. Kravlistan är en exakt beskrivning av den bilden och ett *kontrakt* mellan beställaren och leverantören. Detta ska gälla även om verksamheten är sin egen leverantör. Notera att diskussionen om krav här inte avser endast krav på säkerhetsåtgärden eller säkerhetsprocessens säkerhet, utan även andra krav på påverkar dess utformning.

Det finns ett antal vanliga metoder för att *identifiera krav*:

- **Gruppdiskussioner**. En representativ grupp samlas under en halv- eller heldag för att på ett strukturerat sätt diskutera fram kraven.
- **Intervjuer**. Kraven kan samlas in med hjälp av strukturerade intervjuer med förberedda och standardiserade frågor. Alternativet är ostrukturerade intervjuer, där man går lite på känsla och anpassar frågorna efter svaren.
- **Enkäter**. Väl utformade enkäter till olika roller inom organisationen kan ge en övergripande kravbild.
- **Användarstudier**. Identifiering av kraven genom att följa ett antal personer under en arbetsdag och se hur de jobbar.

Inledningsvis bör man använda den första metoden – en gruppdiskussion för att både identifiera kraven och gruppera dem. En gruppdiskussion för kravidentifiering kan till exempel gå till så att alla deltagare får skriva upp förslag på krav på post-it-lappar som fästs på väggen. Därefter får varje deltagare förklara sina lappar för de övriga och när alla har förstått varandras krav ska kraven grupperas. För att täcka in så många aspekter som möjligt bör diskussionsgruppen inkludera

- IT-driftsansvariga (om det är en teknisk åtgärd)
- chefer från de berörda avdelningarna
- medarbetare från de berörda avdelningarna
- jurister
- supportpersonal.

Under arbetet kommer man troligen att notera två olika typer av krav: *funktionella* krav och *icke-funktionella* krav. Något förenklat kan man säga att funktionella krav beskriver *vad* åtgärden/processen ska göra medan de icke-funktionella kraven beskriver *hur* åtgärden/processen ska göra det. Tabell 1 nedan visar som exempel typiska kategorier för icke-funktionella krav vid utveckling/anskaffning av en teknisk säkerhetsåtgärd.

Tabell 1. Exempel på kategorier för icke-funktionella krav för teknisk säkerhetsåtgärd.

Kategori	Beskrivning
Effektivitet	Detta är krav som beskriver hur ”snabbt” systemet är och hur stora resurser det kräver. Hit hör också krav på skalbarhet (vad händer till exempel när antalet användare växer?).
Tillförlitlighet	Kraven beskriver till exempel hur långt ett driftuppehåll får vara i samband med fel eller underhåll.
Användbarhet	Dessa krav beskriver hur ”lätt” systemet ska vara att lära sig och hur dokumentationen ska vara utformad. Det kan också vara krav på ergonomi och gränssnitt.
Underhållbarhet	Här beskrivs kraven på hur systemet till exempel ska kunna uppgraderas, konfigureras och analyseras samt förändras under drift.
Flyttbarhet	Kategorin gäller till exempel installationskrav.
Designkrav	Kraven rör till exempel utvecklingsmiljön (Microsoft Visual Studio) eller programmeringsspråket (C++, Java eller liknande). Det kan också gälla krav på utvecklingsmetodik (som RUP eller SCRUM). När det gäller en extern leverantör är det viktigt att tänka igenom om det finns särskilda krav som berör hanteringen av känslig information under utvecklingsfasen.

Användbarheten är särskilt viktig när det handlar om åtgärder för informationssäkerhet. Då minskar risken att de nya säkerhetsåtgärderna uppfattas som ”jobbiga” och de tas emot bättre av medarbetarna i verksamheten.

Ett generellt tips är att sträva efter krav som är *mätbara* eftersom det då blir lättare att införa åtgärden i nästa steg. Ett krav som ”lösningen ska vara lättanvänd” är väldigt subjektivt och svårt att verifiera. Formulera det i stället på ett konkret sätt: *”Den som använder lösningen för första gången ska inom två minuter kunna rapportera in en ny incident”.* Då går det att testa om kravet är uppfyllt.

2.1.2 Prioritera krav

När kraven är identifierade ger man dem ett prioritetsvärde. Det finns ett antal olika värdeskalor som används för att ange hur viktigt ett krav är, men en vanlig och enkel metod är att använda tre nivåer: *”ska-krav”, ”bör-krav” och ”bra-att-ha-krav”.* Om det finns tid över vid gruppdiskussionen kan gruppen prioritera de olika kraven men i annat fall kan den som ansvarar för leveransobjektet göra det efteråt på egen hand. Då är det viktigt att

prioriteringen skickas på remiss till dem som var med vid diskussionen (om någon sådan hölls) eller på något annat sätt har varit med i arbetet att ta fram kraven.

2.1.3 Dokumentera kraven

En kravspecifikation kan se ut på lite olika sätt och följa ett antal standarder. Många organisationer har egna rutiner för detta. En generell kravspecifikation kan exempelvis innehålla rubrikerna i tabell 2.

Tabell 2. Exempel på rubriker för kravspecifikation

Bakgrund	Beskriv den säkerhetsåtgärd eller säkerhetsprocess som ska tas fram och vad den ska syfta till. Ange också formalia som ansvariga, kontaktpersoner och så vidare. Beskriv också termer och begrepp som kommer att användas i dokumentet.
Funktionella krav	Lista de krav som beskriver *vad* åtgärden/processen ska utföra. Var specifik och lämna så lite tolkningsutrymme som möjligt. Kraven ska i möjligaste mån vara mätbara.
Icke-funktionella krav	Lista de krav som beskriver *hur* åtgärden/processen ska utföra uppgiften. Kom ihåg att sträva efter mätbarhet. Dela gärna upp denna del på de kategorier som angavs tidigare.
Krav på utvecklingsmiljö eller metodik	Ange kraven på hård- och mjukvara (om tillämpligt). Det kanske finns krav på att en speciell metodik ska användas.
Dokumentation	Ange de krav som finns på dokumentation. Ska det finnas online-hjälp? Ska manualerna vara skrivna på flera språk?

Varje kravspecifikation bör minst innehålla

- benämning
- nummer (id)
- beskrivning av kravet
- beroenden (andra krav som det här kravet är beroende av)
- prioritering.

Det kan också vara bra att dokumentera varför kravet kom till och av vem. Ibland måste man också ange referenser till bakgrundsmaterialet för att förstå kravet.

2.1.4 Validera kraven

Nya säkerhetsåtgärder blir ofta en inskränkning eller ett hinder för de som jobbar i verksamheten. Åtgärderna införs alltid för att förbättra verksamheten (eller över huvud taget göra den möjlig) men ändå kan åtgärderna uppfattas som nya och ”jobbiga” krav på medarbetarna. Därför bör man redan i kravställningen förankra kraven bland dem som berörs och på så sätt få förståelse och acceptans för det nödvändiga i säkerhetsåtgärderna.

Tips för att förankra kraven bland medarbetarna:

- Tillsätt en referensgrupp som får kommentera kraven och föreslå förbättringar. Se till att de övriga medarbetarna känner till referensgruppen så deltagarna känner ett personligt ansvar för uppgiften.
- Be referensgruppen att fokusera på de ”mjuka” kraven. Tekniska detaljer hanteras troligtvis bäst av just tekniker.
- Försök att hitta metoder för att testa hur negativt påverkande en åtgärd är och hur ”jobbig” den uppfattas av den som påverkas av den, till exempel enkäter eller enkla beteendestudier där man studerar och mäter hur mycket längre tid en arbetsuppgift tar.
- Den som ansvarar för en säkerhetsåtgärd ska vara tillgänglig för frågor och ta sig tid att bemöta eventuell kritik redan i detta stadium.

2.2 Konstruera och anskaffa säkerhetsåtgärder

När kraven är fastställda och förankrade är det dags att skrida till verket, antingen genom att beställa leveransobjektet utifrån eller utveckla det internt i verksamheten. Det beslutet togs tidigare under planeringen men kravspecifikationen kan innebära att man vill ändra sig. En del krav kan till exempel innebära att kompetensen inte finns i den egna verksamheten.

2.2.1 Konstruera

Exakt hur en åtgärd ska konstrueras beror på vilken utvecklingsmetodik som organisationen normalt använder. Oftast använder man den ordinarie system- eller verksamhetsutvecklingsmetodiken även när det handlar om att utveckla säkerhetsåtgärder och säkerhetsprocesser, men även här är det bra att tänka på de som kommer att påverkas (medarbetarna). Den som använder en iterativ utvecklingsmetodik kan gärna låta användarna följa och kommentera utvecklingen.

2.2.2 Anskaffa

De flesta organisationer brukar följa sina normala procedurer för anskaffning även när det gäller säkerhetsåtgärder. För offentliga organisationen styrs upphandlingsprocessen delvis av lagen om offentlig upphandling. Upphandlingen kommer att gå lättare om kravspecifikationen är väl utformad med tydliga och mätbara krav. Först måste dock organisationen undersöka om uppdraget innebär att den externa leverantören och uppdragstagaren får eller kan få del av uppgifter som är kritiska för organisationens verksamhet. Med *kritiska* menas här att uppgifterna är konfidentiella (se informationsklassificering). De tre frågorna nedan kan användas som guide för att hitta rätt nivå på säkerhetsavtalet.

Nivåguide för säkerhetsavtalet

- **Nivå 1.** Leverantören ska hantera och förvara sekretessbelagd information i sina egna lokaler.
- **Nivå 2**. Leverantören ska hantera sekretessbelagd information i organisationens lokaler.
- **Nivå 3**. Leverantören kan råka få del av sekretessbelagd information i organisationens lokaler eller på någon annan plats.

För nivå 1 bör leverantören beskriva sina säkerhetsåtgärder och -rutiner i en säkerhetsinstruktion som organisationen måste godkänna. Vid nivå 2 och 3 bör leverantören eller organisationen ta fram en sådan säkerhetsinstruktion om det behövs.

När uppdraget är klart finns det ytterligare några viktiga saker att tänka på:

- **Inlämning av passerkort**. Externa konsulter som har haft tillgång till organisationens lokaler måste lämna tillbaka nycklar och passerkort.
- **Ändra behörighet till IT-system**. Alla tillfälliga användare ska tas bort ur systemet.
- **Kunskapsöverföring.** Se till att få en kompetensöverföring innan ett uppdrag avslutas för att inte vara beroende av den externa leverantören. Detta bör vara ett avtalskrav och ske löpande under uppdragets gång.

Organisationen bör ha rutiner för det som ska göras när en person avslutar sitt uppdrag. Det gäller oavsett om uppdraget fortsätter med andra uppdragstagare från samma leverantör, eller om det avslutas helt.

2.3 Överlämna till införande

När alla komponenter är framtagna eller införskaffade ska de lämnas över till den som ansvarar för att införa dem i verksamheten. I den bästa av världar är alla komponenter testade och väldokumenterade, och åtgärden kan införas enligt organisationens normala rutiner. I praktiken går överlämnandet sällan helt smärtfritt och det kan vara bra om de som lett utvecklingen eller inköpet är beredda att ge stöd även efter överlämnandet.

Exakt vad som ska ingå i leveransen beror givetvis på typen av leveransobjekt. Det är dock viktigt att få med så mycket ”kringdokumentation” som möjligt, till exempel

- kravspecifikation
- testprotokoll
- manualer
- avtal kring införskaffade produkter
    - avtal om tjänstenivåer (SLA)
    - garantier
- dokumentation av referensgruppens kommentarer och förslag.

Rent praktiskt är det bra att lämna över åtgärden under ett seminarium med utvecklaren eller den ansvariga upphandlaren och dem som ansvarar för att införa åtgärden. Parterna kan då komma överens om hur de ska samarbeta kring införandet. Även efter överlämnandet är det ofta nödvändigt att ha upprepade kontakter med utvecklingsavdelningen. Utvecklarna kan också snappa upp åsikter från medarbetare vars arbetssituation kommer att förändras av införandet, och det är bra om de för ”informell” information vidare in i eventuella framtida förbättringar.

3. Nästa steg

När alla komponenter är färdiga och införskaffade är det dags att låta införandeorganisationen sätta dem i verket. Nästa dokument, som går igenom steget ”Införa” visar att det innebär både tekniska, administrativa och pedagogiska utmaningar.