**Systemnamn**Mall för VerksamhetsbeskrivningMED användningSfall

***Så här används denna mall:***

* *Verksamhetsbeskrivning ska skrivas på FM mall*
* *Instruktionen om vad som ska stå under varje rubrik anges i en punktlista under respektive rubrik. Denna text ska raderas innan dokumentet färdigställs.*
* *Text som är skriven utan punktlista är text som kan användas också i det färdigställda dokumentet.*
* *Ersätt Systemnamn med systemets namn.*
* *Redigera dokumentets metadata genom att fylla i relevant information under ”Egenskaper” (eng. ”Properties”) så som namn på systemet och version på dokumentet. Uppdatera därefter fältkoder.*
* *Ta bort rubriker som inte är relevanta och lägg till egna rubriker där så behövs.*
* *Radera denna sida, inklusive punktlistan nedan.*

***Denna mall för verksamhetsbeskrivning innehåller bl.a. instruktioner om följande:***

* *Information som är viktig att få fram i verksamhetsbeskrivningen är information om verksamheten som kan bli dimensionerande för säkerhetsaspekterna. För att göra detta tar man fram användningsfall (scenariobeskrivning av IT-systemets tilltänka användning) som sedan används för att ta fram:*
  + *Beskrivning av stödprocesser*
  + *Avgränsning*
  + *Externa gränsytor och gränsytor till andra verksamheter*
  + *Internationella aspekter*
  + *Roller i systemet*
  + *Krav på sekretess*
* *Krav på tillgänglighet*
* *Krav på riktighet*
* *Scenariobeskrivning av hot*
* *Etc.*
* *Input till verksamhetsbeskrivning kan t.ex. hämtas från TTEM eller intervjuer/gruppövningar med verksamheten.*
* *Viktiga deltagare i verksamhetsbeskrivningen har kompetens om hur verksamheten bedrivs och hur det nya IT-systemet är tänkt att användas. I vissa delar av verksamhetsbeskrivningen krävs även att personer med mandat att fatta beslut deltar. Vilka personer som deltar i arbetet är avgörande för kvalitén på slutresultatet.*
* *Systembeskrivning (endast i de fall då användningsfall ej kunnat identifieras)*
  + *Exempel på vilken nivå*
  + *Funktionalitet*
  + *Systemidé*
* *Användningsfallsanalysen av TTEM:*
  + *Typ av användningsfall (hur man gör användningsfall)*
  + *Typ av stödprocesser (aktiviteter som inte har direkt koppling till verksamheten eller IT-systemet men som ändå har inverkan och som kan generera IT-säkerhetskrav)*
  + *Informationsflödet*
* *Information för att möta KSF 3*
  + *Exponeringsnivå*
* *Ytterligare förklarande text finns under respektive kapitel nedan. Information om hur verksamhetsbeskrivningen genomförs finns även komplett beskrivning i Metodbeskrivning Användningsfall[ref 6].*

**Innehållsförteckning**

[1 Sammanfattning 5](#_Toc476309488)

[2 Inledning 6](#_Toc476309489)

[**2.1** **Syfte** 6](#_Toc476309490)

[**2.2** **Omfattning och avgränsning** 6](#_Toc476309491)

[3 Basfakta 7](#_Toc476309492)

[**3.1** **Versionshistorik** 7](#_Toc476309493)

[**3.2** **Granskat av** 7](#_Toc476309494)

[**3.3** **Referenser** 7](#_Toc476309495)

[**3.4** **Begrepp och förkortningar** 7](#_Toc476309496)

[4 Verksamhetsöversikt 8](#_Toc476309497)

[5 Användningsfall och stödprocesser 9](#_Toc476309498)

[**5.1** **Användningsfall** 9](#_Toc476309499)

[**5.2** **Stödprocesser** 10](#_Toc476309500)

[**5.3** **Roller i systemet** 10](#_Toc476309501)

[6 Informationsflöde och informationsklassning 11](#_Toc476309502)

[**6.1** **Informationsflöde inom systemet** 11](#_Toc476309503)

[**6.2** **Gränsytor till andra verksamheter eller system** 12](#_Toc476309504)

[7 Hotanalys 13](#_Toc476309505)

[**7.1** **Hot kopplat till användningsfall 1** 13](#_Toc476309506)

[**7.2** **Hot kopplat till användningsfall 2** 14](#_Toc476309507)

[**7.3** **Hot kopplat till stödprocess 1** 14](#_Toc476309508)

[8 Kompletterande systembeskrivning 15](#_Toc476309509)

[**8.1** **Nivåbeskrivning** 15](#_Toc476309510)

[**8.2** **Funktionsbeskrivning** 15](#_Toc476309511)

[**8.3** **Systemidé** 15](#_Toc476309512)

[9 Exponeringsnivå 16](#_Toc476309513)

[**9.1** **Exponering från personer** 16](#_Toc476309514)

[**9.2** **Exponering från informationsutbyte** 16](#_Toc476309515)

[10 Verksamhetskrav 17](#_Toc476309516)

1. **Sammanfattning**

* *Under denna rubrik görs en kort summering (max 1 A4-sida) av verksamhetsbeskrivningen inkluderat det primära resultatet och de slutsatser som kan dras.*

1. **Inledning**

Verksamhetsbeskrivningen är central och beskriver användningsfall, informationsflöde samt en sammanställning av verksamhetskrav.

* 1. **Syfte**

Syftet med detta dokument är primärt att utgöra en verksamhetsbeskrivning där användningsfall, stödprocesser och informationsflöden samt en sammanställning av säkerhets­relevanta verksamhetskrav återges för *Systemnamn*.

* 1. **Omfattning och avgränsning**
* *Ange omfattning och eventuella avgränsningar för verksamhetsbeskrivningen.*
* *Verksamhetsbeskrivningen ska omfatta användningsfall, identifiering av informationsflöden och informationsklassificering i samband med informationsflödet. Även exponering (i vilken utsträckning ett system är exponerat för intern respektive externa parter, intern respektive externa system etc.) samt assuransnivå (identifiera de kritiska punkterna exempelvis var information med olika klassificeringar möts).*
* *Exempel på omfattning är vilka delsystem och gränsytor som avses ingå.*
* *Exempel på avgränsning är angränsande system som inte ingår, delkomponenter som inte anses vara IT-system/relevanta ur IT-säkerhetspunkt osv.*
* *Var noggrann med avgränsningen så att verksamhetsbeskrivningen inte blir för omfattande. TTEM kan eventuellt ge input till avgränsning.*

1. **Basfakta**
   1. **Versionshistorik**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ver** | **Datum** | **Status** | **Beskrivning** | **Fastställt av** |
|  |  |  |  |  |

* 1. **Granskat av**

|  |  |  |
| --- | --- | --- |
| **Namn** | **Organisation** | **Kompetensområde** |
|  |  |  |

* 1. **Referenser**
* I tabellen nedan listas exempel på referenser.

|  |  |  |
| --- | --- | --- |
| **Ref. nr.** | **Dokument** | **Dok. Nr.** |
|  | *Försvarsmaktens interna bestämmelser om IT-säkerhet* | *FIB 2006:2* |
|  | *Instruktion Verifiering system av system* | *13FMV5921-12:1* |
|  | *TTEM Systemnamn* |  |
|  | *Metodbeskrivning för Användningsfall* | *13FMV5921-8:2* |
|  | *KSF Krav på IT-säkerhetsförmågor hos IT-system v3.1* | *FM2014-5302:1* |

* 1. **Begrepp och förkortningar**

*Se Säkerhetsmålsättning <Systemnamn> eller användningsfall.*

1. **Verksamhetsöversikt**

*Övergripande beskrivning av verksamheten och dess operativa verksamhet. Exempel på information som ska ingå i detta kapitel är:*

* *Uppgift*
* *Antal användare*
* *Operativ miljö*
* *etc*

1. **Användningsfall och stödprocesser**

* *Övergripande syfte med verksamheten (kan hämtas från TTEM).*
* *Verksamheten bryts ned i ett antal scenarier: användningsfall och stödprocesser.*
* *Effektivisering och positiva effekter pga. det nya IT-systemet (kan hämtas från TTEM).*
* *Ur användningsfallen kan sedan informationsflöde och gränsytor extraheras.*
  1. **Användningsfall**
* *Här identifieras de dimensionerande användningsfallen.*
* *Beskriver kortfattat olika fall för hur IT-systemet ska användas/nyttjas och vilka IT-säkerhetskrav det genererar.*
* *Syftet med dessa användarfall är att ge en rimlig uppfattning om:*
* *Vilken typ av information som systemet kan komma hantera.*
* *Vilka driftmiljöer som kan tänkas bli aktuella.*
* *Vilka hot och risker som bör belysas i en separat analys.*
* *Vilka regelverksområden som kan komma att påverkas i och med behovet av en viss informationsstruktur.*
* *Vilka säkerhetsdomäner som passeras, identifiera om det finns en risk att information med olika informationssäkerhetsklass möts…*
* *Användningsfallen utgörs av en aktivitet eller en sekvens av aktiviteter som en aktör utför inom en verksamhet/ett system för att uppfylla en specifik förmåga, exempelvis IT-stöd för underhåll.*
* *Ur användningsfallen extraheras verksamhetskrav som förs in i kravtabellen i kapitel 9.*
* *Kan hämtas ur TTEM eller tas fram genom intervjuer/workshop med verksamhetspersonal. Rätt verksamhetspersonal i framtagning av användningsfall är en framgångsfaktor.*
* *Exempel på vad som ska kontrolleras i användningsfallen:*
* *Om endast ett fåtal personer ska nyttja IT-systemet och man ställer krav på olika roller och att en individ inte får inneha flera roller så kan man inte ha flera roller än antal användare i IT-systemet.*

***Exempel på användningsfall:***

* *Detta är ett exempel på ett användningsfall. Ersätt med användningsfall för IT-systemet i fråga.*
* *Användare använder IGR för att prata med annan användare. Extern utrustning i form av kryptonyckel och autentiseringsparametrar behövs. Dataöverföring för anslutna informationssystem ska kunna ske samtidigt som radiokanal används. Kvaliteten på det överförda talet skall vara så bra att det medger röstigenkänning.*
* *Krav som kan extraheras ur användarfallet (skrivs i kapitel 9 med hänvisning till detta avsnitt, ej här):*
* *Systemnamn ska vara försett med av Försvarsmakten godkänt krypto. (Sekretess)*
* *Användare ska autentiseras vid användning av Systemnamn. (Sekretess)*
* *Dataöverföring för anslutna informationssystem och/eller sensorer skall kunna fortsätta samtidigt som radiokanal används. (Tillgänglighet)*
* *Kvaliteten på det överförda talet skall vara så bra att det medger röstigenkänning och sinnesstämning/nyanser i röst ska förmedlas. (Riktighet)*
  1. **Stödprocesser**

*Stödprocesser är aktiviteter som inte har direkt koppling till verksamheten eller IT-systemet men som ändå har inverkan och som kan generera IT-säkerhetskrav. Ur stödprocesserna extraheras verksamhetskrav som förs in i kravtabellen i kapitel 9. Dessa kan även hämtas ur TTEM eller tas fram genom intervjuer/workshop med verksamhetspersonal.*

*Exempel på vad som ska kontrolleras i stödprocesserna:*

* *IT-systemet måste kunna avhemligas inför att transport.*

*Exempel stödprocess – Installation av programvara*

* *Detta är ett exempel på en stödprocess. Ersätt med stödprocesser för IT-systemet i fråga.*
* *Installation av ny programvara ska utföras av administratör. Installation får ej ske under skarpt uppdrag.*
* *Krav som kan extraheras ur stödprocessen (skrivs i kapitel 9 med hänvisning till detta avsnitt, ej här):*
  + *Installation av ny programvara ska utföras av administratör. (Riktighet)*
  + *Installation får ej ske under skarpt uppdrag. (Tillgänglighet)*
  1. **Roller i systemet**
* *Kan finnas beskrivet i TTEM eller i annan verksamhetsdokumentation (processer, rutiner, organisationsscheman etc.)*
* *Rollerna kan identifieras utifrån framtagna användningsfall alternativt bli identifieras först och sedan användas som input till framtagningen av användningsfall.*
* *Fyll i tabellen nedan med roll, beskrivning av rollens rättigheter, samt vilken/vilka aktör(er) som innehar rollen. Ta bort de roller som inte är relevanta för just detta IT-system och komplettera med ytterligare roller om så är relevant. Det kan t.ex. finnas olika typer av rollen ”Användare” i IT-systemet. Ange i sådana fall samtliga användarroller samt beskriv skillnaden i rättigheter. I tabellen finns för vissa roller även angivet exempel på rättigheter. Justera detta efter aktuellt IT-system.*

Tabellen nedan anger olika roller i *Systemnamn.*

|  |  |  |
| --- | --- | --- |
| **Roll** | **Rättigheter** | **Aktör** |
| *Användare* | *Skriv- och läsrättigheter, brukare av systemet. Hanterar Systemnamn och informationen. Analyserar, importerar och exporterar information ur Systemnamn.* |  |
| *Systemadministratör* | *Installerar/grundkonfigurerar och uppdaterar systemet.* |  |
| *Säkerhetsadministratör* | *Skapar operatörskonto/inloggningsbehörighet.* |  |
| *Loggadministratör* | *Läsrättigheter säkerhetsloggar.* |  |
| *Drifttekniker/underhåll* | *Systemtester och läsrättigheter av loggar för verifieringar och underhållsanalys samt driftsjournallogg.* |  |

1. **Informationsflöde och informationsklassning**

* *I detta kapitel beskrivs och illustreras av informationsflödet.*
* *I samband med beskrivning av informationsflöde och gränsytor till andra verksamheter/system placeras även värden för informationsklassning ut.*
* *Input till detta informationsflöde kan erhållas ur användningsfallen i kapitel 3 ovan.*
* *Input till informationsklassningen kan erhållas ur en säkerhetsanalys framtagen av Försvarsmakten, se separat bilaga till säkerhetsmålsättningen.*
* *I verksamhetsbeskrivningen realiseras det teoretiska och generella resultatet från säkerhetsanalysen, man konkretiserar det utifrån respektive användningsfall i kapitel 3 ovan samt informationsflöde. I verksamheten kan resultatet av informationsklassningen ändras utifrån den verksamhet som bedrivs just där. Konkretiseringen kan ske utifrån aspekter som t.ex. tid och rum.*
* *Konkretiseringen av informationsklassningen är viktig att göra i workshopform, det är deltagarna som är avgörande.*
* *Informationsklassningen i verksamhetsbeskrivningen blir sedan stöd för designfasen.*
* *För bakgrundsbeskrivning till informationsklassningen, se Metodbeskrivning Användningsfall [ref 6].*
  1. **Informationsflöde inom systemet**
* *Beskrivning av informationsflödet.*
* *Input till informationsklassningen erhålls ur säkerhetsanalysen, se separat bilaga till säkerhetsmålsättningen.*
* *Input till informationsflöde inom systemet kan erhållas ur från användningsfallen i kapitel 3 ovan.*
* *Interna gränssnitt ska beskrivas.*
* *Illustration eller tabell över informationsflöde.*
* *Det ska framgå vem som tar del av informationen.*
* *I tabellen nedan anges exempel på interna gränsytor och informationsflöde. Radera dessa och ersätt med hur det ser ut i verkligheten för systemet i fråga.*

Tabellen nedan anger interna gränsytor och informationsflöde för *Systemnamn.* Kolumnerna ”Delsystem/komponent” anger vilken verksamhet/system som information utbyts med. Kolumnen ”Information” anger vilken slags information som utbyts och i kolumnen ”Klassning” anges informationsklassning. För bakgrundsbeskrivning till informationsklassningen se kapitel 3 i bilagan säkerhetsanalys. I kolumnen ”Kommentar” kan övrig relevant information anges, t.ex. om informationen är enkel- eller dubbelriktad.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Delssystem /komponent** | **Delssystem /komponent** | **Information** | **Område** | **Klassning** | **Kommentar** |
| *Central tidsserver* | *Ethernetport* | *Tid* | *Sekretess* | *Ej sekretess* | *Enkelriktad* |
| *Nyckelkort* | *Kryptodel* | *Kryptonycklar* | *Sekretess* | *H/R* | *Enkelriktad* |
| *Komponent A* | *Komponent B* | *Taktiskt tal, ordrar etc.* | *Sekretess* | *H/R* | *Dubbelriktad* |
| *Tillgänglighet* | *A* |

* 1. **Gränsytor till andra verksamheter eller system**
* *Externa gränsytor*
* *Input till externa gränsytor kan erhållas ur användningsfallen i kapitel 3 ovan.*
* *Vilken information utbyts med andra system/verksamheter? (Exempel på information: taktiskt tal, systeminformation, kryptonycklar, loggar etc.)*
* *Vilka andra IT-system/verksamheter kan ställa krav på detta IT- system (funktion, information)?*
* *Vilka krav ställer detta IT-systemsystem på andra IT-system/verksamheter (funktion, information)?*
* *Input till informationsklassningen erhålls ur säkerhetsanalysen, se separat bilaga till säkerhetsmålsättningen.*
* *Gränsytor kan finnas beskrivet i TTEM eller i annan verksamhetsdokumentation (processer, rutiner, organisationsscheman etc.)*
* *I tabellen nedan anges exempel på externa gränsytor och informationsflöde. Radera dessa och ersätt med hur det ser ut i verkligheten för systemet i fråga.*

Tabellen nedan anger externa gränsytor och informationsflöde till andra verksamheter/IT-system. Kolumnen ”Verksamhet/System” anger vilken verksamhet/system som information utbyts med. Kolumnen ”Information” anger vilken slags information som utbyts och i kolumnen ”Klassning” anges informationsklassning. För bakgrundsbeskrivning till informationsklassningen se kapitel 3 i bilagan säkerhetsanalys. I kolumnen ”Kommentar” kan övrig relevant information anges.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Verksamhet/System** | **Information** | **Område** | **Klassning** | **Kommentar** |
| *METOC* | *Väderdata* | *Tillgänglighet* | *L* |  |
|  |  |  |  |  |

1. **Hotanalys**

* *Utgå från tidigare identifierade användningsfall och stödprocesser.*
* *Vid beskrivning av scenario för hotet ska scenariot utgöra en beskrivning av hur hotet kan inträffa. I scenariobeskrivning exemplifieras hotrubriken genom att svara på hur, när var och av vem scenariot utförs. Man ska tänka på vad det är man vill säga när man skriver scenariot.*
* *Indelning av hot efter kategorierna sekretess, riktighet, tillgänglighet samt generella hot.*

*Hoten kan identifieras utifrån användningsfallen och förtecknas nedan ett och ett samt bearbetats enligt följande:*

* *Hotets kod (Se = sekretess, Ri = riktighet, Ti = tillgänglighet, Ge = generellt) samt ett löpnummer*
* *Rubrik/Beskrivning av hotet*
* *Beskrivning av scenario/händelseförloppet där scenariot utgör en beskrivning av hur hotet kan inträffa. I scenariobeskrivning exemplifieras hotrubriken genom att svara på:*
  + *Hur inträffar scenariot?*
  + *När inträffar scenariot?*
  + *Var inträffar scenariot?*
    - *Vilken typ av fysisk miljö inträffar scenariot i?*
  + *Vem utför scenariot?*
* *Beskrivning av skadan som uppstår*
  1. **Hot kopplat till användningsfall 1**

|  |  |
| --- | --- |
| **Hot nr:** |  |
| **Beskrivning:** | *Förlorad enhet med information.* |
| **Scenario:** | *En soldat tappar av misstag sin enhet med information under skarpt uppdrag på internationellt uppdrag.* |
| **Skadeverkning:** | *Allvarlig* |

|  |  |
| --- | --- |
| **Hot nr:** |  |
| **Beskrivning:** |  |
| **Scenario:** |  |
| **Skadeverkning:** |  |

* 1. **Hot kopplat till användningsfall 2**

|  |  |
| --- | --- |
| **Hot nr:** |  |
| **Beskrivning:** |  |
| **Scenario:** |  |
| **Skadeverkning:** |  |

* 1. **Hot kopplat till stödprocess 1**

|  |  |
| --- | --- |
| **Hot nr:** |  |
| **Beskrivning:** |  |
| **Scenario:** |  |
| **Skadeverkning:** |  |

1. **Kompletterande systembeskrivning**

* *I en del fall är tänkta systemet redan känt (t.ex. COTS) eller så är designen så långt kommen med systemet att det kan beskrivas under denna rubrik. I många fall så är endast önskad funktionalitet känd och då lämnas detta avsnitt blankt.*
* *Tänk på att någon utomstående ska kunna förstå beskrivningen.*
* *Redan befintliga verksamhetsbeskrivningar kan användas men var uppmärksam på att dessa kanske inte är på rätt nivå. Här är det informationssäkerheten som ska vara i fokus.*
  1. **Funktionsbeskrivning**
* *Vilka funktioner ska IT-systemet ha?*
* *Beskriv även säkerhetsfunktion (BKS, säkerhetslogg etc.)*
* *Kan finnas beskrivet i TTEM.*
  1. **Systemidé**
* *I en del fall kanske man vet vilket det tänkta systemet är (COTS) eller har kommit långt i designen med systemet och då kan det beskrivas under denna rubrik. Men i många fall så vet man bara vilken funktionalitet som önskas av systemet och då kan man inte skriva något här.*

1. **Exponeringsnivå**

* *Med exponeringsnivå avses bedömningen av hur exponerat systemet är avseende någon aktörs möjlighet att påverka systemet. Denna möjlighet kan vara såväl fysisk, d.v.s. att någon kommer åt den tekniska utrustning som utgör systemet, som logisk via systemets olika gränssnitt.*
* *Input till detta kapitel kan erhållas ur ovanstående kapitel (Användningsfall och stödprocesser, Informationsflöde inom systemet, Gränsytor till andra verksamheter eller system samt Roller i systemet).*
* *Informationen i kapitlet ska bl.a. användas för att avgöra exponeringsnivå vid bedömningen av vilka säkerhetskrav som ska tillämpas för IT-systemet utifrån KSF 3.*
* *I kapitlet ska följande beskrivas:*
  + *Fysisk miljö*
  + *Vilka resurser för skydd av verksamhet och IT-systemet och informationen i IT-systemet som finns t.ex. i form av fysiskt skydd*
  + *Om IT-systemet ska användas nationellt eller internationellt*
  + *Om IT-systemet ska användas i fred, kris eller krig*
  + *Exponering från t.ex. personer*
  + *Exponering från t.ex. informationsutbyte*
  + *Exponering från såväl fysiska som logiska aspekter.*
* *Kapitlet ska omfatta en slutsats om exponeringsnivån att som input till KSF 3. Se KSF Krav på IT- säkerhetsförmågor hos IT-system v3, [ref 7] för beskrivning av de olika exponeringsnivåerna.*
  1. **Exponering från personer**
* *Beskriv IT-systemets fysiska miljö.*
* *Beskriv vilka resurser för skydd av verksamhet och IT-systemet och informationen i IT-systemet som finns t.ex. i form av fysiskt skydd.*
* *Beskriv om det sker besök i lokal där IT-systemet finns, hur dessa besök i sådana fall loggas etc.*
* *Beskriv exponering från personer:*
  + *Vilka har tillgång till IT-systemet?*
  + *Hur är rättigheterna för respektive roll i IT-systemet satta?*
  1. **Exponering från informationsutbyte**
* *Med informationsutbyte avses allt utbyte av information med andra IT-system, vare sig det sker över elektroniskt kommunikationsnät eller med flyttbara lagringsmedia. Införande av säkerhetsuppdateringar samt uppdatering av säkerhetsfunktioners kontrollmekanismer och deras styrande data (t.ex. antivirussignaturer) som sker enligt fastställda drift- och säkerhetsinstruktioner, påverkar dock inte exponeringen av IT-systemet.*
* *Beskriv exponering från informationsutbyte*
  + *Elektroniskt kommunikationsnät*
  + *Användning av flyttbart lagringsmedia*
  + *Informationsutbyte med aktörer på samma eller högre konsekvensnivå (ange hur säkerhetsfunktioner skyddar från dessa IT-systems hotaktörer)*

1. **Verksamhetskrav**

* *Verksamhetskraven är en sammanställning utifrån tidigare kapitel i denna verksamhetsbeskrivning (användningsfall, stödprocesser, exponering, hotanalys).*
* *Verksamhetskrav ur IT-säkerhetssynpunkt*
  + *Krav på sekretess*
  + *Krav på riktighet*
  + *Krav på tillgänglighet*
* *Kraven måste kunna vara mätbara, kompletta, relevanta och entydiga.*
* *Kraven som anges i tabellen nedan är exempel på krav. Dessa tas bort och ersätts med verkliga krav för IT-systemet.*

*Verksamhetskraven extraheras ur genomförd verksamhetsbeskrivning samt TTEM.*

*I kolumnen ”Nr” anges löpnummer för respektive verksamhetskrav. Kolumnen ”Krav” anger kravet medan ”Källa” anger referens till var kravet kommer ifrån (verksamhetsbeskrivning eller TTEM). I kolumnen ”Kommentar” kan anges om kravet är tekniskt, administrativt, fysiskt, organisatoriskt eller en kombination av flera. I denna kolumn kan även övrig relevant information anges.*

| **Nr** | **Krav** | **Källa** | **Kommentarer** |
| --- | --- | --- | --- |
|  | *Systemnamn ska vara försett med av Försvarsmakten godkänt krypto.* | *5.1.1* | *Tekniskt krav* |
|  | *Användare ska autentiseras vid användning av Systemnamn.* | *5.1.1* | *Tekniskt krav* |
|  | *Dataöverföring för anslutna informationssystem och/eller sensorer skall kunna fortsätta samtidigt som radiokanal används.* | *5.1.1* | *Tekniskt krav* |
|  | *Kvaliteten på det överförda talet skall vara så bra att det medger röstigenkänning och sinnesstämning/nyanser i röst ska förmedlas.* | *5.1.1* | *Tekniskt krav* |
|  | *Installation av ny programvara ska utföras av administratör.* | *5.2.1* | *Administrativt krav* |
|  | *Installation av ny programvara får ej ske under skarpt uppdrag.* | *5.2.1* | *Administrativt krav* |
|  |  |  |  |