Metodbeskrivning för framtagning av
Användningsfall

Användningsfall

2016-06-30

Revisionshistorik

Version	Datum	Beskrivning	Ansvar
2.3	2016-06-30	Mindre uppdateringar med avseende på begrepp och förtydliganden baserat på erfarenhetsåterkoppling. Version 2.2 är bokformatet.	DAOLO
1.2	2014-05-30	Mindre uppdateringar med avseende på begrepp och förtydliganden samt byte av namn på dokumentet	DAOLO
1.0	2013-02-15	Leverans	DAOLO

Innehåll

1 Inledning

1.1 Syfte

Syftet med detta metodstöd är att få fram verksamhetens behov ur ett IT-säkerhetsperspektiv för att kunna utveckla säkra system på rätt grunder och på ett effektivt sätt och med rätt resurser. Stödet ges i form av genomförande, arbetssätt, förslag på deltagande resurser och kompetens, omfattning och dokumentation.

1.2 Omfattning

Metodstödet för arbetet omfattar:

- Denna metodbeskrivning.
- Flödesscheman för arbetet , se *bild 2:1*. Syftet med dessa är att ge en övergripande bild av arbetsflödet.

Mallar för att ta fram verksamhetsbeskrivning, säkerhetsanalys och säkerhetsmål återfinns i den digitala utgåvan. Syftet med mallarna är att när de är ifyllda ska färdig dokumentation finnas framme.

1.3 Referenser

Ref.	Dokumentnamn	Dok. id.
[1]	Instruktion verifiering system av system	
[2]	HKV Försvarsmaktens IT-styrmodell	
[3]	H Säk Skydd	M7739-352005
[4]	H Säk IT	M7745-734062
[5]	Riktlinjer för klassificering	HKV 2008-06-25 10 812.72264
[6]	KSF 3	

2 Principer för genomförande

2.1 Syfte

Denna metodbeskrivning omfattar framtagning av användningsfall med fokus på att få fram verksamhetsbeskrivning, säkerhetsanalys och risk- och sårbarhetsanalys. Inom dessa områden så är resultatet av verksamhetsbeskrivningen, informationsklassificeringen samt identifiering av verksamhetens sårbarheter vitala för det fortsatta IT-säkerhetsarbetet. Resultatet blir styrande för projektets utveckling av krav och design.

Även om ovanstående områden ses som separata resultat behöver inte genomförandet av arbetet ske del för del. Denna metodbeskrivning ska ge stöd till hur ett genomförande kan göras för att resurser mm ska kunna användas på ett effektivt sätt.

Metodstödet ska vara oberoende av vilken FM handbok som används.

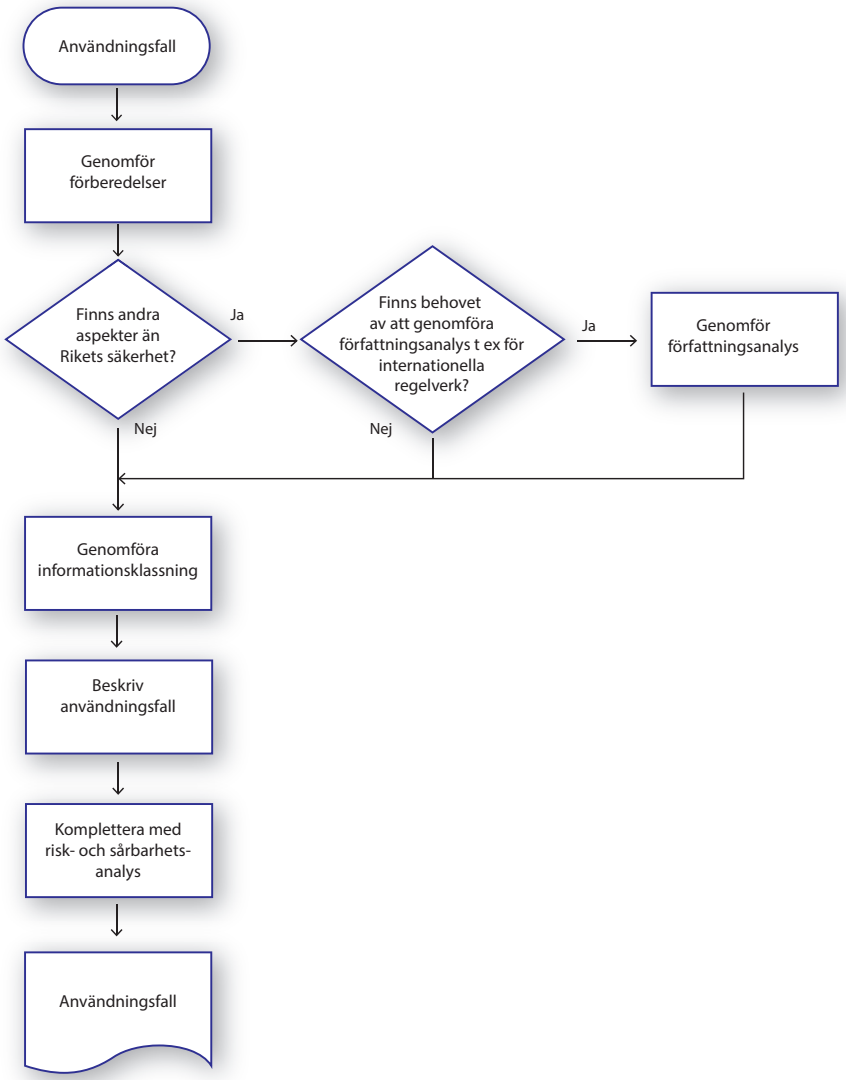

Bild 2:1 Översikt och flöde över framtagning av verksamhetens krav med utgångspunkt från användningsfall

I denna metodbeskrivning finns följande beskrivet

- Förberedelse beskrivs i *kapitel 3*
- Informationsklassning beskrivs i *avsnitt 4.3*
- Användningsfall beskrivs i *avsnitt 4.4*.
- Risk- och sårbarhetsanalys beskrivs i *avsnitt 4.5*.

Metodbeskrivningen är upplagd på följande sätt:

- Först ges en generell beskrivning som rör arbetet i sin helhet med förberedelser, genomförande och resultat.
- Andra delen beskriver arbetssätt i form av genomförande av workshops.
- Tredje delen är en metodbeskrivning för att få fram resultatet för varje del som ska ingå i resultatet. Avsnittet för Verksamhetsbeskrivning fokuserar på framtagning av användningsfall och informationsflöden medan avsnittet för säkerhetsanalys fokuserar på genomförande av informationsklassning eftersom de delmomenten är centrala för resultatet och arbetet. Till sist beskrivs metodbeskrivning för Risk- och sårbarhetsanalys.

3 FÖRBEREDELSER

Ett väl genomfört förberedelsearbetet lägger grunden till kvalitén på resultatet. Förberedelsearbetet är också till för att skapa en uppfattning om det aktuella systemet.

3.1 KRAVDEFINITION

I fasen kravdefinition genomförs arbeten för att klargöra viktiga aspekter som kan påverka det fortsatta arbetet. Följande aspekter är viktiga att klargöra:

- Finns TTEM och beslut från Försvarsmakten med innehåll som beskriver hur verksamheten har tänkt använda systemet? Uppgifter som kan inhämtas från dessa underlag är
  - internationell samverkan
  - avgränsningar
  - användare och roller inom verksamheten
  - krav
  - återbruk av tidigare genomförda säkerhetsmålsättningar
  - samverkan med andra system.
- Finns en version av systemet sedan tidigare?
  Återbrukbarhet av befintlig säkerhetsmålsättning bedöms efter genomförd deltaanalys som visar på eventuella skillnader mellan versioner bland annat i form av
  - kontext
  - användningsområde
  - informationssäkerhetsklass
  - integration med system
  - ingående personal
  - m m.

Nödvändiga uppdateringar görs i det fall den befintliga säkerhetsmålsättningen är återbrukbar, i annat fall tas nödvändig information fram enligt denna metodbeskrivning.

En mer detaljerad instruktion för deltaanalys finns i dokumentet Instruktion verifiering system av system *[1]*.

Är det aktuella systemet är ett så kallat *system av system*? Exempel på det kan vara Säkerhetsmålsättning för BMS där säkerhetsmålsättningen omfattar BMS i sin helhet och inte säkerhetsmål för varje delsystem.

Tillvägagångssätt se övergripande flöde i bilaga 1 – Förberedelser.

3.2 Planering av arbete

Efter analys av indata finns också tillräcklig information för att planera själva arbetet med resurser och tidplaner m m. I planeringen bestäms också på vilket sätt arbetet ska genomföras.

3.2.1 Vem och vilka ska genomföra arbetet?

Arbetet behöver följande roller enligt *[2]* Beställare, Koordinator, Utförare och Användare som deltagare i workshopen. Vid genomförandet av workshops bör personer med verksamhetskunskap men även av IT-tekniska personer delta. Arbetet kräver dessutom att en person agerar moderator.

I arbetet är det vitalt att resurser med god verksamhetskunskap deltar då det är verksamhet som ska beskrivas, informationssäkerhetsklass avgöras samt risker ska bedömas. Resultatet och tidplanen är helt beroende på tillgång till kompetenta deltagare med mandat från den verksamhet som IT-systemet ska stödja.

3.2.2 Vad ska göras?

Beställaren svarar för:

- Beställaren beställer arbetet med framtagning av användningsfall.
- Planera in arbetet i tiden. Kompetens och verksamhetsinsikt borgar för kvalitet och riktighet i den kravställning som systemet ska dimensioneras för.
- Utse deltagare enligt *avsnitt 3.2.1* ovan.
- Planering och kallelser till workshops som bör tilldelas deltagare i tidigt skede.

Koordinatorn av arbetet svarar för att:

- Stödja beställaren
- Klara ut omfattning och avgränsningar för arbetet.
- Leda och förbereda workshops.
- Driva, genomföra och leverera resultatet.

3.2.3 Hur ska arbetet genomföras?

En del av förberedelsearbetet i ett helhetsperspektiv är att bestämma hur arbetet ska bedrivas i sin helhet över tiden.

Informationsklassning, användningsfall samt Risk- och sårbarhetsanalys, förordas genomföras via workshops. En workshop ger en bra möjlighet för leverantören av arbetet att fånga denna information vilken på plats kan diskuteras och bedömas. Fördelen med workshop är att det går snabbt att genomföras och begränsar tid och kostnader. Nackdelen är att det kan bli en ögonblicksbild som, efter en tid, blir inaktuell eller behöver uppdateras. Genomförs arbetet via flera workshops hinner deltagarna tänka till och fler uppdateringar hinner göras och kvalitén ökar på materialet.

Hur många workshops som behövs bör bestämmas likaså vilka delar som ska beröras på vilka workshops. En workshop kan mycket väl hantera flera av områdena Säkerhetsanalys, Verksamhetsbeskrivning samt Risk- och sårbarhetsanalys beroende på hur arbetet bestäms läggas upp.

En mer detaljerad beskrivning av genomförande av workshop ges i *avsnitt 4.2*.

Exempel på disponering av tid för arbetet.

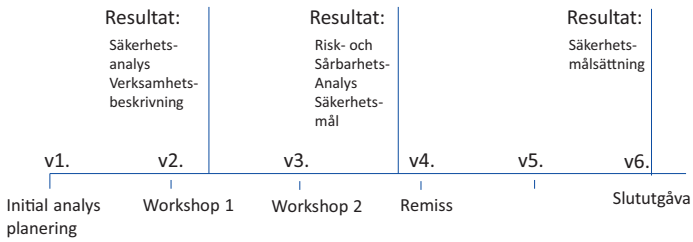

Bild 3:1 Exempel på disponering av tid för arbetet

Beställaren måste trycka på att uppgiften är viktig och svara för att rätt resurser finns att tillgå och därmed göra en bedömning av när kallelser måste skickas ut för att rätt kompetens ska finnas på plats.

4 Genomförande

4.1 Inledning

Nedan ges dels en beskrivning av ett arbetssätt för att ta fram användningsfall och dels en metodbeskrivning för framtagning av resultat för respektive del i det arbetet.

4.2 Arbetssätt

Flera delmoment i framtagning av användningsfall sker med fördel i form av workshops som anges i *avsnitt 3.2.3*.

4.2.1 Workshop 1

4.2.1.1 Inför workshop

1. Den initiala analysen ska vara genomförd för att deltagare ska ha en bra uppfattning av det aktuella systemet. Arbetet ska planeras enligt *avsnitt 3.1*.
2. Bestäm vilka deltagare som ska delta.
3. Skicka kallelser minst 3 veckor innan första workshop. I detta moment skickas kallelser till både workshop 1 och 2 så att resurser är inplanerade hela vägen. I kallelsen kan, med fördel, information från den initiala analysen bifogas, samt tidplan för hur resterande arbetet med användningsfallen kommer att ske i tiden.

4.2.1.2 Genomförande

Workshop 1 omfattar en dags arbete, vilket kan uppdelas på två halvdagar beroende på förutsättningar. Fördelen med två halvdagar är att det kan vara lättare att boka upp personer samt att det kan bli arbetsamt med en kompakt arbetsdag. Syfte till att genomföra stegen:

1. Informera om syftet med workshopen, presentera vad som hittills är känt om IT-systemet (eventuell systembild) samt förväntad utgång/ resultat av dagen.
2. Identifiera skyddsvärda tillgångar enligt *avsnitt 4.3*.
3. Bedöma konsekvensen avseende oönskad spridning av sekretess, tillgänglighetsförlust och oönskad förändring för respektive tillgång enligt *avsnitt 4.3.1*.
4. Prioritera de viktigaste tillgångarna.
5. Identifiera dimensionerande användningsfall och stödprocessen, enligt *avsnitt 4.4.1*.
6. Identifiera informationsflödet i användningsfallen, se *avsnitt 4.4.2*.
7. Genomför informationsklassificering enligt *avsnitt 4.4.4*.

Dokumentera löpande enligt mallar i bilaga 2.

4.2.1.3 Tidsåtgång

Omfattning:

- Punkt 1 uppskattas till 30 min
- Punkt 2 och 3 uppskattas till 2 timmar
- Punkt 4 uppskattas till 30 min
- Punkt 5, 6 och 7 uppskattas till 4 timmar.

Observera att tidsuppskattningen kräver ett förberedelsearbete från beställare, koordinator och användare enligt avsnittet Inför workshop.

4.2.1.4 Efterarbete

Renskriv och uppdatera dokumentationen.

Skicka resultat till deltagare för synpunkter.

4.2.2 Workshop 2

4.2.2.1 Inför workshop

- Inför workshop 2 ska deltagaren ha kunnat få tillgång till resultatet från workshop 1.
- Förbered en kortare presentation av föregående resultat.
- Bestäm deltagare, det kan vara så att det krävs personal med IT-kompetens i denna workshop.
- Skicka en kallelse till deltagare.
- Boka lämpliga lokaler för ändamålet med rätt verktyg.

4.2.2.2 Genomförande

Omfattar en dags arbete

1. Startar med att presentera resultatet från föregående workshop. Beskriv deltagare i analysen samt vilket kompetensområde dessa representerar.
2. Identifiera exponeringsnivå se *avsnitt 4.4.5*.
3. Genomför sårbarhetsanalys med utgångspunkt användningsfall och stödprocesser identifierade informationsflöden enligt *avsnitt 4.5*.
   - Förklara syftet med risk- och sårbarheten och de begrepp som kommer att användas i arbetet såsom hot, scenario, skada, konsekvenser. Denna analys är till för att ta fram verksamhetens sårbarheter.
   - Hitta hoten i användningsfallen från workshop 1.
   - Hitta riskerna i användningsfallen.
4. Presentation av användningsfallet (avgränsning, definition av gränsytor etc).
5. Identifiera hotbild.
   - Beskriv hot
   - Indelning av hot efter kategorierna sekretess, riktighet, tillgänglighet samt generella hot.
   - Gör en scenariobeskrivning för hur hotet inträffar, se exempel *avsnitt 4.5.1*.
   - Beskriv skadeverkningar.

Punkterna 1, 2 och 3 görs av personer med verksamhetskunskap.

Punkterna 3, 4 och 5 kan dels göras av personer med verksamhetskunskap men även av IT-tekniska personer.

4.2.2.3 Efterarbete

Sammanställning av säkerhetsmål. Omfattning:

- Punkt 1 uppskattas till 30 min.
- Punkt 2 uppskattas till 1 timme.
- Punkt 3 uppskattas till 5,5 timmar.

4.3 Informationsklassning

Fokus i informationsklassningsarbetet är att identifiera de skyddsvärda tillgångarna samt deras informationsklassificering. De skyddsvärda tillgångarna kan sedan vara ett hjälpmedel i att ta fram de, ur ett säkerhetsperspektiv dimensionerande användningsfallen.

För skyddsvärda tillgångar görs en bedömning av konsekvensnivå och därefter informationsklassificering för de skyddsvärda tillgångarna.

För varje tillgång anges vilket informationssäkerhetsområde som berör tillgången, det vill säga om det berörs av sekretess, riktighet eller tillgänglighet.

För sekretess finns stöd i konsekvensbedömning och informationsklassificering i *[4]* och *[5]*. Informationsklassificering för sekretess ligger sedan till grund för att göra en bedömning av konsekvensnivåer enligt *[6]*. Principen för relationen mellan säkerhetsmålsättning och KSF 3 visas nedan. Den informationsklassificering som genomförs i arbetet är input till den konsekvensbedömning och därefter kravnivå som beskrivs i KSF 3. Finns inte säkerhetsmålsättning tas informationen fram via användningsfall enligt denna metodbeskrivning.

Bild 4:1 Relation mellan säkerhetsmålsättning och KSF 3 för konsekvensbedömning

När de skyddsvärda tillgångarna är identifierade kan man passa på att redan här ta fram en hotbild kring dessa. Denna information kan sedan användas i Risk- och sårbarhetsanalysen, se *avsnitt 4.5*.

4.3.1 Konsekvensbedömning

Konsekvensen är ett mått på hur mycket verksamheten skadas om hotet blir verklighet. När de skyddsvärda tillgångarna är identifierade görs en bedömning av konsekvenser avseende oönskad spridning av sekretess, tillgänglighetsförlust och oönskad förändring för respektive tillgång.

Vilka nivåer som ska finnas på konsekvensbedömningen samt dess betydelser görs på workshop. En rekommendation är att använda jämt antal nivåer för att få fram ett ställningstagande om konsekvensen är under medel eller över medel. För många nivåer ökar komplexiteten och bedömningen upplevs som svår.

När det gäller sekretess så finns stöd för konsekvensbedömning i *[4]* och *[5]*. För verksamheten är tillgänglighet och riktighet viktig därför bedöms även dessa områden. Nedan ges exempel på 4-gradiga skalor för dessa nedan.

4.3.1.1 Tillgänglighet

I tabellen nedan anges vilka beteckningar som används i mallen för säkerhetsanalys för konsekvensbedömning med avseende på tillgänglighet.

Beskrivning	Benämning	Betydelse
Kritisk	K	Kommunikations-/informationsbortfall där informationen ej går att återskapa inom längsta tillåtna avbrottstid. Kommunikations-/informationsbortfall i kritisk situation.

Beskrivning	Benämning	Betydelse
Allvarlig	A	Lång tids kommunikations-/informationsbortfall. Kommunikations-/informationsbortfall i allvarlig situation.
Betydlig	B	Kortare tids kommunikations-/informationsbortfall l i mindre kritisk situation.
Lindrig	L	Tillfälligt kommunikations-/informationsbortfall i icke kritisk situation.

4.3.1.2 Riktighet

I tabellen nedan anges vilka beteckningar som används i kapitel 4 i mallen för säkerhetsanalys bilaga 2 för konsekvensbedömning med avseende på riktighet.

Beskrivning	Benämning	Betydelse
Kritisk	K	Kritisk data förändras utan upptäckt. Förändring av konfigurationer utan upptäckt inom den tid som verksamheten måste upptäcka det.
Allvarlig	A	Data förändras utan upptäckt. Förändring av konfigurationer utan upptäckt inom den tid som verksamheten måste upptäcka det.
Betydlig	B	Försök till förändring som upptäcks inom den tid som verksamheten måste upptäcka det.
Lindrig	L	Försök till förändring som misslyckas och upptäcks inom den tid som verksamheten måste upptäcka det.

4.3.2 Informationsklassificering

Efter konsekvensbedömningen görs en informationsklassificering av de skyddsvärda tillgångarna.

Med utgångspunkt från konsekvensbedömningen görs en prioritering av de skyddsvärda tillgångarna.

När det gäller sekretess så finns stöd för det i *[4]* och *[5]*.

I övrigt görs på samma sätt som *avsnitt 4.3.1*.

4.4 Användningsfall

Information som är viktig att få fram i användningsfall är information om verksamheten som kan bli dimensionerande för IT-säkerhetsaspekterna. För att göra detta tar man fram användningsfall (beskrivning av IT-systemets tilltänkta 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
- sårbarheter för verksamheten

Viktiga deltagare i användningsfall har kompetens om hur verksamheten bedrivs och hur det nya IT-systemet är tänkt att användas. Vilka personer som deltar i arbetet är avgörande för kvalitén på slutresultatet.

4.4.1 Dimensionerande användningsfall och stödprocesser

Användningsfall ska visa på användningsområde av IT-systemet som kan vara dimensionerande för IT-säkerhetsarbetet och i förlängningen påverka krav och design. Mycket av grundarbetet förväntas att hämtas från verksamhetskrav och verksamhetsnyttobeskrivningen. Det ska ha en fast ram och avgränsning är avgörande vid utformandet av användningsfall.

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.

Exempel på användningsfall: En soldat ska skicka lägesinformation till ledningsplats, se förenklad figur nedan.

Exempel på frågor som uppstår och där svaren kan beskrivas i användningsfallet är:

- Är soldaten mobil?
- Hur är det fysiska skyddet?
- Vad är det för typ av information som soldaten ska skicka?
- Vad händer med informationen på ledningsplatsen?
- Hur hanteras informationen lokalt i soldatens enhet för data?
- Internationella resurser och samverkan på plats?
- Vad händer efter fusion?
- Sekretessnivå? Var finns H/S information t ex? Kan den hanteras ute hos soldat?
- Tillgänglighetskrav?
- Riktighetskrav?

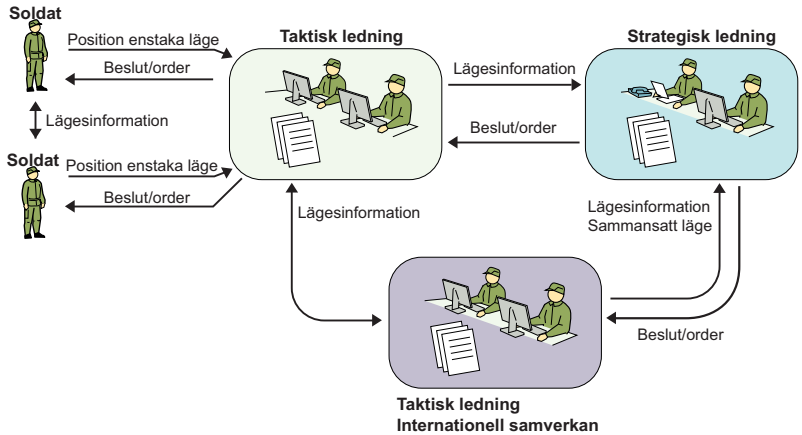

Bild 4:2 Förenklat användningsfall

4.4.2 Informationsflöde

Informationsflödesbeskrivning ska inkludera hur information rör sig mellan olika gränssnitt i användningsfallen, vem som tar del av den samt vilka andra verksamheter som information utbyts med och vad dessa verksamheter ställer för krav respektive vilka krav som ska ställas på dessa verksamheter. Informationsflödet kan beskrivas i en tabell eller grafiskt.

Exemplet ovan är informationsflödet enligt ovan:

- Lägesinformation från soldat till ledningsplats.
- Beslut och order från ledningsplats till soldat.
- Lägesinformationsutbyte mellan enskilda soldater.
- Fusionerad lägesinformation från taktisk till strategisk ledningsplats.

4.4.3 Konsekvensbedömning

Med utgångspunkt från användningsfallet så görs en konsekvensbedömning av informationsflödet.

Exempel på konsekvensbedömning: Baserat på användningsfallet i *avsnitt 4.4.1* skickas från enstaka soldat.

Område	Beskrivning	Benämning
Sekretess	Lindrig	Endast ringa men om informationen kommer obehöriga till del.
Riktighet	Allvarlig	Betydligt om informationen ändras utan upptäckt
Tillgänglighet	Allvarlig	Betydligt om informationen vid tillslag inte finns tillgängligt.

Med utgångspunkt från konsekvensbedömningen görs informationsklassificering.

4.4.4 Informationsklassificering

I beskrivningen av informationsflöde och gränsytor till andra verksamheter/system görs även en informationsklassificering. Input till informationsklassificeringen fås av avsnitt 4.3, Informationsklassning och konsekvensbedömning, se *avsnitt 4.3.1*.

I säkerhetsanalysen har information i systemet klassats och denna klassning kan användas som en input till informationsklassificeringen för användningsfallen. Dock ska informationen i användningsfallet genomgå en separat informationsklassificering i de fall någon aspekt har tillkommit som förändrar förutsättningarna.

4.4.5 Identifiering av exponeringsnivå

Med *exponering* menas t ex i vilken utsträckning ett system är exponerat för intern respektive externa parter, intern respektive externa system etc. Bedömd exponeringsnivå är input till att avgör systemets säkerhetsnivå som i sin tur bestämmer applicerbara KSF-krav se *[6]*.

Anledning att *assuransnivå* finns med i arbetet är att ge verksamheten en möjlighet att ge sitt perspektiv på detta. Verksamheten kan identifiera de kritiska punkterna exempelvis var information med olika klassificeringar möts vilket ger input sedan såväl i kravspecifikations- som i produktionsfasen (ISD-processen) och arkitekturarbetet. Detta är viktigt såväl för sekretess- som för kostnadsaspekterna.

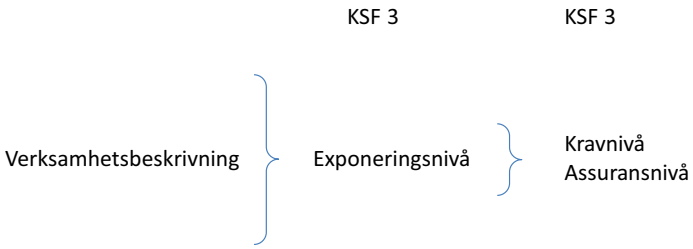

Bild 4:3 Relation mellan användningsfall och KSF 3 för exponeringsnivå

4.4.6 Framtagning av systembeskrivning

Det finns fall där det är svårt att få fram användningsfall ur ett verksamhetsperspektiv där inte det aktuella systemet direkt kan kopplas till en specifik verksamhet till exempel i form av ledningssystem eller något liknande utan är mer av karaktären generella komponenter som ska kunna användas i flera verksamheter. Exempel på sådana komponenter är generella IT-säkerhetskomponenter (ex signalskyddssystem) och kommunikations- och infrastrukturkomponenter. I de fall tas en systembeskrivning fram som beskriver hur komponenten ska fungera.

4.5 Risk – och sårbarhetsanalys

Input hämtas främst från Verksamhetsbeskrivning i form av identifiering av omfattning och avgränsningar, samt användningsfall inklusive informationsflöden och stödprocesser, se *avsnitt 4.4*.

I analysen är det viktigt att fokus ligger på hot som är specifika för verksamheten och aktuellt användningsfall, andra hot har det ofta tagits höjd för i till exempel MUST KSF.

Risk- och sårbarhetsanalysen genomförs med fördel via workshop, se *avsnitt 4.2.2*.

För säkerhetsmålsättningsarbetet ger det liten effekt att gå in i detalj på sannolikhet och åtgärder. Det som är viktigt är att hitta de sårbarheter som verksamheten upplever finns för att därigenom kunna identifiera verksamhetens behov ur ett IT-säkerhetsperspektiv.

4.5.1 Scenariobeskrivning

Ett scenario är en beskrivning av en händelse som har en början och ett slut. Det är något som initierar scenariot, denna initiala händelse medför ett antal ställningstaganden och följdhändelser, som till slut mynnar ut i ett slut.

Scenario ska beskriva frågeställningarna:

- Hur uppstår hotet?
- Vad hände?
- När uppstod det?
- Var uppstod det?
- Vem är upphovsman till hotet?

Exempel på scenario från användningsfallet i *avsnitt 4.4.1* är: En soldat blir av med sin enhet med information.

Hur ser omständigheterna ut när han blev av med informationen, det vill säga vad är det som föranleder att detta kommer med i en risk- och sårbarhetsanalys? Är det en avbrott situation? Visar det sig att en obehörig (vem) har fått tillgång till den utrustning som soldaten har för att sända meddelandet?

En övertagen nod kan mynna ut i många olika följdhändelser:

- Sekret information kommer till kännedom för vår ”fiende”.
- Fienden skickar desinformation till våra styrkor.
- Utrustningen används för att göra en DoS attack.

Slutet på händelsen kan vara att systemets skyddsmekanismer gör att attacken inte förverkligades eller att effekten av attacken blev hanterbar för våra styrkor.

4.5.2 Beskriv skadeverkningarna

Med utgångspunkt från scenariobeskrivningen och dess händelser så ska den skada som drabbar verksamheten beskrivas. Konsekvenser (skada) värderas enligt *avsnitt 4.3.1*.

4.6 Framtagning av säkerhetskrav

TBD

Exempel

Bilaga 1 Mallar

Följande mallar i word-format finns till Metodbeskrivning användningsfall.

- *Mall Verksamhetsbeskrivning*
- *Mall Säkerhetsanalys*
- *Mall Säkerhetsmål*
- *Mall för ITSS 1*