Pålitliga IT-system i Försvarsmakten

– en behovsinventering

NINA LEWAU OCH JACOB LÖFVENBERG

FOI-R--3799--SE
ISSN 1650-1942 December 2013

Nina Lewau och Jacob Löfvenberg

Pålitliga IT-system i Försvarsmakten

– en behovsinventering

Bild/Cover: (Bildbyrå och namn på fotograf)

Titel	Pålitliga IT-system i Försvarsmakten - En behovsinventering
Title	Trustworthy IT systems in the Swedish Armed Forces - A needs inventory
Rapportnr/Report no	FOI-R--3799--SE
Månad/Month	December
Utgivningsår/Year	2013
Antal sidor/Pages	28 p
ISSN	1650-1942
Kund/Customer	Försvarsmakten
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	Ledning och MSI
Projektnr/Project no	E36047
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Informations- och aerosystem

Detta verk är skyddat enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk.
All form av kopiering, översättning eller bearbetning utan medgivande är förbjuden

This work is protected under the Act on Copyright in Literary and Artistic Works (SFS 1960:729).
Any form of reproduction, translation or modification without permission is prohibited.

Sammanfattning

IT-systemen blir allt viktigare och mer omfattande, både till antal och i komplexitet. I verksamheter med höga krav på IT-säkerhet är behovet av pålitliga IT-system extra angeläget eftersom sådana är en förutsättning för att skapa en säker helhetslösning.

I denna rapport presenteras resultatet av en behovsinventering med syftet att identifiera de behov som finns relaterat till pålitliga IT-system inom Försvarsmakten. Arbetet genomfördes i fyra steg: (1) insamling av data med hjälp av sju djupintervjuer, (2) identifiering av utsagor, (3) identifiering av behov och (4) strukturering av behov.

Resultatet visar på stor bredd både i synsätt på pålitlighet och i vad som bidrar till ökad pålitlighet. Bland annat visar resultatet att för att nå pålitlighet räcker det inte med att ha pålitlighet bara i själva IT-systemet. Det måste också finnas pålitlighet i IT-systemets omgivning och kringliggande funktioner. Exempel på saker som bidrar till ökad pålitlighet i IT-systemen är att ha kontinuitet i IT-säkerhetsarbetet samt en tydlig verksamhetsarkitektur.

Nyckelord: pålitlighet, säkerhet, assurans, behov

Summary

IT systems are growing, both in numbers and in complexity. In organisations with high demands on IT security, the need for trustworthy IT systems are even more important since trustworthiness is necessary in order to create a secure overall solution.

This report presents the result of a needs inventory with the purpose of identifying the needs related to trustworthy IT systems within the Swedish Armed Forces. The inventory was performed in four steps: (1) data collection using seven in-depth interviews, (2) identification of statements, (3) identification of needs and (4) structuring of needs.

The result shows a substantial variation, both regarding the concept of trustworthiness and in what contributes to a higher degree of trustworthiness. One of the results is that to achieve trustworthiness it is not enough with trustworthiness in the IT system. There also has to be trustworthiness in the context of IT systems and neighbouring functions. Examples of what contributes to trustworthy IT system are continuity in the IT security work and a clear business architecture.

Keywords: trustworthiness, security, assurance, needs

Innehåll

1 Inledning 7

2 Bakgrund 8

2.1 Säkerhetskedja för pålitliga IT-system 8

2.2 Behovsanalys 8

2.3 Quality Function Deployment 9

2.4 Kvalitetsdriven kravhantering 9

2.4.1 Insamling av data 9
2.4.2 Identifiering av utsagor 10
2.4.3 Identifiering av behov 10
2.4.4 Analys och strukturering av behov 10

3 Metod 11

3.1 Insamling av data 11

3.2 Identifiering av utsagor 11

3.3 Identifiering av behov 12

3.4 Strukturering av behov 12

4 Resultat 13

4.1 Pålitliga IT-system 14

4.2 Heltäckande IT-säkerhetslösning 14

4.3 Säkerhetskedjan 16

4.4 Kravställning i utvecklingsarbetet 17

4.4.1 Stöd för att ta reda på vilka säkerhetsegenskaper som krävs för ett specifikt IT-system 17
4.4.2 Stöd för hur krav ska ställas för att få önskade säkerhetsegenskaper för ett specifikt IT-system 18
4.4.3 Stöd för att veta vilka lösningar som motsvarar uppställda krav på säkerhetsegenskaper 18
4.4.4 Användbarhet 18

4.5 Effektiva utvecklingsprojekt 19

4.6 Roller och ansvar i verksamheten 20

4.7 Kompetens 21
4.8 Kommersiella programvaror 22
4.9 Hantering av risker 22
4.10 Arkitektur 23
4.10.1 Utformning av arkitekturen 23
4.10.2 Komponenter 24
4.10.3 Komplexitet 24
4.10.4 Separation 24
4.11 Drift 25

5 Diskussion 26

Referenser 28

1 Inledning

De senaste decennierna har uppvisat en enorm ökning i antalet IT-system i samhället och det sker fortfarande en tilltagande digitalisering av allt fler tekniska och administrativa system. IT-systemen växer inte bara till antalet, utan även i storlek och i mängden integrationer och beroenden till varandra. Denna ökande komplexitet är ett problem ur ett IT-säkerhetsperspektiv då IT-systemen och lösningarna blir allt svårare att överblicka och förstå. Detta leder i sin tur till en ökad risk att IT-systemen inte beter sig på det sätt det är tänkt – det vill säga att de inte är pålitliga. I verksamheter med höga krav på IT-säkerhet, i form av sekretess, riktighet och tillgänglighet, är behovet av pålitliga IT-system extra angeläget. Detta eftersom sådana är en förutsättning för att kunna säkerställa att IT-säkerheten är på en tillräcklig nivå.

I denna rapport presenteras resultatet av en behovsinventering med syfte att identifiera de behov som finns relaterat till pålitliga IT-system inom Försvarsmakten. Detta område, pålitliga IT-system, betyder olika saker för olika personer. Behovsinventeringen har därför även haft ett fokus på att försöka fånga dessa olika betydelser av begreppet pålitliga IT-system.

För att fånga vissa skillnader i synsätt används i denna rapport begreppen system och IT-system medvetet med olika innebörd. När begreppet IT-system används åsyftas det tekniska systemet. När begreppet system används åsyftas hela MTO[1]-perspektivet, det vill säga mjukvaran tillsammans med kringliggande rutiner, användning, organisation etc.

Denna rapport är framtagen inom FoT-projektet Pålitliga IT-plattformar. Projektet startades 2013-01-01 och dess slutdatum är 2015-12-31. Tidigare under 2013 har en litteraturstudie genomförts inom ramen för FoT-projektet (Löfvenberg och Rodhe, 2013). Litteraturstudien har studerat vilka metoder och tekniker som finns för att påvisa att mjukvara som körs på en IT-plattform är pålitlig, i betydelsen att den beter sig som den ska.

[1] Människa, teknik, organisation – alla tre delarna sedda som en sammanhängande enhet.

2 Bakgrund

I följande avsnitt beskrivs säkerhetskedjan för pålitliga IT-system, systemutvecklingsaktiviteten behovsanalys, kvalitetsramverket Quality Function Deployment (QFD) samt ansatsen kvalitetsdriven kravhantering.

2.1 Säkerhetskedja för pålitliga IT-system

I tidigare arbeten på FOI kring pålitliga plattformar har det tagits fram en modell över en mjukvaras livscykel från specifikation till körande program (Löfvenberg och Lundholm, 2010). Denna modell benämns *säkerhetskedja* (Figur 1). Syftet med säkerhetskedjan är att beskriva de länkar som alla måste vara starka när det byggs ett IT-system med höga säkerhetskrav. Modellen är gjord på en relativt hög nivå för att påvisa de mest påtagliga aktiviteterna i säkerhetskedjan.

Figur 1 Säkerhetskedja för IT-system

Säkerhetskedjan skulle kunna förlängas åt båda håll och därigenom fånga en större del av mjukvarans livscykel, men dessa tidigare och senare faser har inte varit fokus i denna behovsinventering. Det innebär dock inte att de är mindre viktiga eller intressanta.

2.2 Behovsanalys

Behovsanalys är den aktivitet som utgör grunden för denna studie. Behovsanalyser syftar till att identifiera och analysera behov. Ofta ses behovsanalys som en del i aktiviteten kravhantering (Davis, 2005). Många skiljer inte heller på begreppen behov och krav, och lite slarvigt kallas ibland behov för användarkrav eller verksamhetskrav. Även om det i utvecklingsarbete kan vara lätt att blanda ihop vad som är behov och vad som är krav så har begreppen två skilda betydelser. Krav ställs på det som ska anskaffas, medan behov finns hos dem som ska nyttja produkten, det vill säga hos intressenter eller verksamhet.

Behov kan vara antingen medvetna eller omedvetna samt verkliga eller upplevda. Uttalade behov är ofta relaterade till någon form av inneboende krav på åtgärd. Behov kan också vara tillfredsställda, vilket oftast gör dem svårare att identifiera. Detta är fallet eftersom ett tillfredsställt behov ofta är ett omedvetet behov vars uppfyllelse känns självklar. Tillfredsställa behov kan dock bli väldigt tydliga efter en förändring, då det som tidigare tillfredsställde vissa behov inte längre gör

det; exempelvis kan detta inträffa efter införande av nya IT-system. Trots att uppfyllda behov inte uttrycks explicit så väcker förändringar som leder till att de inte längre uppfylls ofta till stort missnöje.

2.3 Quality Function Deployment

Quality Function Deployment (QFD) är ett kvalitetsramverk som syftar till att stödja utvecklingen av produkter och tjänster så att dessa ger en hög grad av kundtillfredsställelse (Cohen, 1995). Denna ansats ligger till grund för den behovsinventering som genomförts i denna studie. QFD började utvecklas i Japan under senare delen av 1960-talet. Grunden i QFD är att erhålla förståelse för vilka kunderna är, deras behov och därefter omvandla dessa till egenskaper hos produkter och tjänster. På så vis skapas produkter och tjänster med hög grad av nytta för kunderna. Kundens behov sätts i centrum och inga funktioner eller egenskaper som inte bidrar till kundnyttan utvecklas. Utvecklingsprojekt som drivs enligt QFD kan genomföras på ett flertal olika sätt. Aktiviteterna genomförs med stöd av kvalitetsverktyg som till exempel relationsdiagram, tabeller och matriser.

Ett av många kvalitetsverktyg som har utvecklats inom QFD är kundrösttabeller[2] (Shillto, 2001). I kundrösttabellen skrivs kundens uttalanden in som utsagor. Dessa utsagor analyseras därefter utifrån (1) vem som anses behöva det, (2) vad de anser sig behöva, (3) när de behöver det, (4) var det behöver användas, (5) varför behovet finns och (6) hur de vill att det ska fungera. Analys med stöd av kundrösttabell har som mål att kunna formulera faktiska behov. Kundrösttabellens primära funktion är att underlätta analysen av vad kunden egentligen behöver.

2.4 Kvalitetsdriven kravhantering

Kvalitetsdriven kravhantering baseras på några av de verktyg som finns i QFD, och genomförs i sex steg: (1) insamling av data, (2) identifiering av utsagor, (3) identifiering av behov,(4) analys och strukturering av behov, (5) identifiering av krav och (6) analys av krav (Hallberg, Andersson & Westerdahl, 2005). I denna behovsinventering var de första fyra stegen aktuella, varför de beskrivs närmare nedan.

2.4.1 Insamling av data

Under den första aktiviteten samlas data in som är av intresse för studien. Insamling av data kan ske med flera olika metoder och tekniker, exempelvis

[2] Eng: voice of the customer table

intervjuer, observationer, workshops eller enkäter. Ett effektivt sätt att samla in relevant information är att efterfråga upplevda problem, något som indikerar situationer som upplevs otillfredsställande i något avseende. Otillfredsställande situationer avviker från det förväntade eller det önskade. Problem kan vara existerande eller tänkbara i framtida situationer. Utdata från detta steg ska vara i textformat.

2.4.2 Identifiering av utsagor

Under den andra aktiviteten analyseras texten för att identifiera utsagor. En utsaga är en text som innehåller information som sedan kan nyttjas för att bestämma behov. En utsaga ska inte vara för omfattande eller innehållsrik utan bör bestå av en eller ett par meningar, men ändå ge en förståelse för vad texten beskriver.

2.4.3 Identifiering av behov

Under den tredje aktiviteten genomförs en analys av utsagorna med syftet att identifiera behov. För detta ändamål används kundrösttabeller. Varje utsaga kan innehålla ett eller flera behov, men kan också vara så innehållsfattig att inget behov alls kan extraheras. Resultatet av denna aktivitet utgörs av ett antal behovsformuleringar.

2.4.4 Analys och strukturering av behov

Under den fjärde aktiviteten genomförs en analys av behovsformuleringarna. I ett första steg genomförs detta med relationsdiagram, där likartade behov grupperas så att kategorier skapas för att skapa ordning bland behoven. Dessa kategorier grupperas i sin tur med liknande kategorier.

Identifierade behov kan vara enkla eller sammansatta. Enkla behov kan inte delas upp ytterligare, medan sammansatta är möjliga att dela upp i flera olika behov. I det senare fallet kan behovet ses som en kategori innehållande andra kategorier och behov. Under analysen sorteras även dubbletter av behov bort och formuleringar ensas.

Det andra steget i denna aktivitet inleds med att överföra relationsdiagrammen till hierarkiska diagram. Dessa diagram analyseras sedan vidare i syfte att upptäcka om behov saknas, och om strukturen med behov i så fall behöver kompletteras.

3 Metod

Detta kapitel beskriver hur metoden *Kvalitetdriven kravhantering* i delar tillämpats i denna behovsinventering. Arbetet genomfördes i fyra steg: (1) insamling av data, (2) identifiering av utsagor, (3) identifiering av behov och (4) strukturering av behov. Det fjärde steget, analys och strukturering av behov modifierades något vid genomförandet av denna studie då det snarare genomförts en behovsinventering än en behovsanalys. Närmare beskrivning ges i avsnitt 3.4 Strukturering av behov.

3.1 Insamling av data

Under den första aktiviteten samlades data in, som direkt eller indirekt innehöll information om relevanta behov. Insamlingen gjordes genom sju stycken djupintervjuer med respondenter från olika verksamheter inom Försvarsmakten. Respondenterna hade IT-systemrelaterade arbetsuppgifter bland annat bestående av beställning, metodutveckling, drift, IT-säkerhetsgranskning, systemdesign och projektledning. Varje intervju tog cirka två timmar.

Då det område som detta FoT-projekt hanterar är något svårdefinierat och tolkas på många olika sätt valdes ett öppet angrepssätt vid formulering av intervju-frågorna. Inledningen av intervjuerna hölls korta och begrepp från litteratur-studien undveks för att inte styra respondenten utan istället fånga upp de begrepp respondenten själv använde. Därefter ägnades en stor del av intervjun till att diskutera respondentens syn på området, vad denne anser viktigt gällande pålitliga IT-system och behov som respondenten ser i området. En stund in i intervjun visades figuren av säkerhetskedjan upp för respondenten och användes för reflexion och diskussion kring begreppet pålitlighet.

Vid varje intervjutillfälle deltog en respondent och två intervjuare. En av intervjuarna ansvarade för att ställa frågorna och den andra för att föra anteckningar och komma med kompletterande frågor. Tre av intervjuerna spelades in, och inspelningarna nyttjades för komplettering av intervju-dokumentationen. Efter renskrivning skickades dokumentationen till respektive respondent för att ge dem möjlighet att kontrollera att inget missats eller missuppfattats, samt för att ge dem möjlighet att tillföra ytterligare information.

3.2 Identifiering av utsagor

Under den andra aktiviteten analyserades dokumentationen för att identifiera utsagor. Under genomläsningen markerades utsagor som var relevanta för problemställningen. Utsagorna tilläts vara delvis överlappande för att säkerställa

att så många aspekter som möjligt av utsagorna fångades. De identifierade utsagorna dokumenterades i en tabell.

3.3 Identifiering av behov

Under den tredje aktiviteten skedde en analys av utsagorna med syfte att identifiera behov som relaterar till pålitliga IT-system. För detta ändamål användes kundrösttabeller (se avsnitt 2.3). Både behov som var tillfredsställda och behov som var otillfredsställda identifierades. Aktiviteten resulterade i en ifylld kundrösttabell med bland annat ett antal behovsformuleringar, vilket allt dokumenterades i anslutning till de identifierade utsagorna. En anpassning av kundrösttabellen gjordes i form av borttagning av kolumnen ”Var” då denna inte bedömdes vara relevant i studien.

3.4 Strukturering av behov

Under den fjärde aktiviteten genomfördes en strukturering av behoven genom att gruppera likartade behov så att kategorier skapades. Dessa kategorier grupperades i sin tur med liknande kategorier. Under detta arbete togs dubbletter bort, sammansatta behov delades upp i flera behov och formuleringar ensades. Resultatet av denna aktivitet dokumenterades i en behovslista med spårbarhet till utsagorna. Studien inte är en behovsanalys utan en behovsinventering med syftet illustrera bredden av behov. Därför har resultatet inte bearbetats för att identifiera saknade behov, justera överlappande kategorier eller prioritera behov.

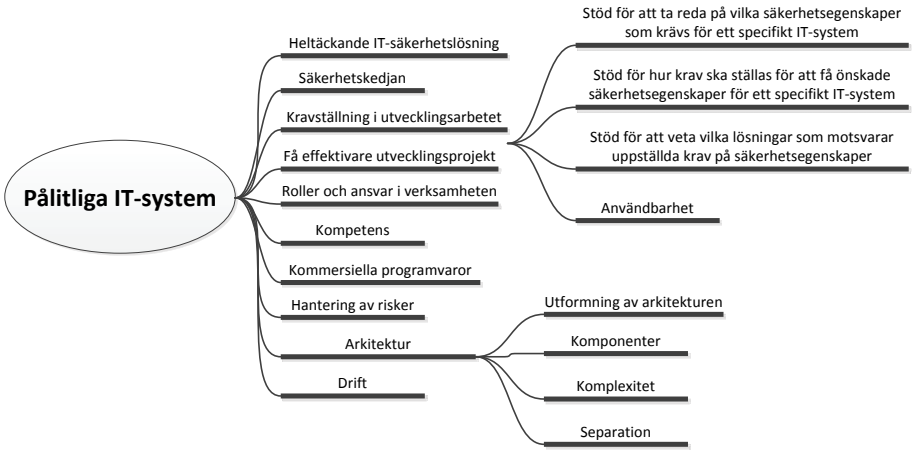
4 Resultat

I detta kapitel presenteras en sammantagen bild av de behov som har framkommit under behovsinventeringen. En del beskrivna behov har uttryckts vara tillfredsställda, andra är mer eller mindre otillfredsställda.

I detta FoT-projekt används begreppet pålitlighet i betydelsen att IT-system ska göra det som de ska göra, enligt specifikation, och ingenting annat. Detta resonemang har olika innebörd för de olika respondenterna sett till vad som bidrar till och påverkas av strävan att nå pålitliga IT-system. För att kunna lita på att information hanteras korrekt krävs en viss nivå av IT-säkerhet, vilket ger att en del behov som respondenterna uttalat och som presenteras i denna rapport berör IT-säkerhet.

Även om en del synsätt har en teknisk inriktning präglas behovsinventeringen av ett stort antal icke-tekniska aspekter. Alla respondenter var dock eniga om att pålitlighet handlar om en kombination av teknik, människa och organisation. Detta är skälet till att göra den tydliga skillnaden mellan system och IT-system, så som beskrevs i kapitel 1.

Behoven har delats in i ett antal kategorier, tio på första nivån direkt under behovet pålitliga IT-system och ytterligare åtta på en andra nivå under två av behoven på den första nivån (Figur 2). Notera att avsnitt 4.1 ligger på en behovshierarkisk nivå ovanför de resterande avsnitten i kapitlet.



Figur 2 Behovsstruktur

4.1 Pålitliga IT-system

Eftersom det finns aktörer som vill komma åt Försvarsmaktens information är kraven på IT-säkerhet höga. Dels är kraven på säkerhetsfunktionalitet mer omfattande, dels är Försvarsmaktens tillit till att ett IT-system har de önskade säkerhetsegenskaperna mer långtgående. Det finns därmed behov av att kunna lita på alla IT-system inom Försvarsmakten, i betydelsen att de gör det de ska och ingenting annat genom att uppfylla sina krav och säkerhetsprofiler. I detta behov ligger både tillit till IT-säkerheten och till att de levererar verksamhets-kraft (förmåga). Exempelvis finns behov av pålitlighet för IT-system som inte nödvändigtvis hanterar sekretessklassad information, men som hanterar information med skyddsvärde, exempelvis väderinformation. Behovet av pålitlighet är extra högt gällande säkerhetsfunktioner.

4.2 Heltäckande IT-säkerhetslösning

För att uppnå pålitliga IT-system finns det behov av att få en heltäckande IT-säkerhetslösning, utifrån resonemanget att ingen kedja är starkare än sin svagaste länk.

Bedöm IT-säkerhet ur en samlad bild utifrån samtliga delområden

I syfte att få en heltäckande, pålitlig IT-säkerhetslösning finns det behov av att ta hänsyn till samtliga delområden vid bedömning av vilken IT-säkerhetslösning som krävs. De områden som då omfattas är bland annat sekretess, spårbarhet, integritet, tillgänglighet och användbarhet.

Få med alla relevanta tillkommande funktionella IT-säkerhetskrav

Det finns behov av att i säkerhetsanalysen noggrant analysera det specifika IT-systemets kontext och därigenom säkerställa att alla relevanta tillkommande funktionella IT-säkerhetskrav kommer med i arbetet.

Se till lösningen på en högre nivå

För att uppnå pålitlighet finns det behov av att bedöma IT-säkerheten mer än per komponent eller per lösning, utan att istället hantera systemen i sin helhet. De behov som uttryckts gäller att säkerställa pålitligheten dels vad gäller interaktionen mellan verifierade komponenter, dels ur ett system-av-system-perspektiv. Detta medför även behov av att minska detaljfokuseringen och istället öka förståelsen för att komponentunika krav ibland får stå tillbaka till

förmån för lösningen på en högre nivå. Det finns även behov av att IT-system granskas på denna högre nivå.

Ha god metodmässig hantering under systemets hela livscykel

Det finns behov av att under hela systemets livscykel metodmässigt hantera systemet på ett effektivt sätt som bidrar till tillit, såsom exempelvis patch-hantering.

Säkerställ en känd användningssituation

För att säkerställa pålitlighet genom en heltäckande IT-säkerhetslösning finns behov av en balans mellan IT-säkerhet och användbarhet, så att användarna kan sköta sitt jobb, för då är användningssituationen känd. Om användarna inte kan utföra sina uppgifter tillfredsställande tenderar de att ta genvägar, vilket ger en okänd användningssituation och därmed minskad pålitlighet. Ett exempel kan vara användare som lyfter information in och ut ur IT-system från olika sekretessnivåer. Då sänks säkerheten i IT-systemet eftersom det inte är designat för regelbunden in- och utmatning.

Ta hänsyn till den mänskliga faktorn

Det finns behov av att ta hänsyn till frågor relaterade till människan under hela utvecklings- och produktionskedjan, där exempel på frågeställningar är hur tillverkningsprocessen har gått till, vem eller vilka som har haft tillgång till utvecklingsmiljön samt bedömning av företag. Med hänsyn till den mänskliga faktorn och som skydd mot insiderhot finns det behov av att ha säkra rutiner för att hantera systemadministratörer och deras höga behörigheter i IT-systemen.

Genomför säkerhetsgranskning väl och vid önskad tidpunkt

Då Försvarsmakten har tillit till de godkända IT-system och komponenter som används finns behov av väl genomförda säkerhetsgranskningar av oberoende part, som tar hänsyn till IT-systemets kontext och som säkerhetsställer att IT-systemets säkerhetsegenskaper motsvarar kraven. Det finns även behov av att granskningarna ska kunna genomföras i takt med projektens granskningsbehov, för att undvika fördröjningar.

Ha hög kvalitet i arbetet

För att nå pålitliga IT-system krävs det hög kvalitet i säkerhetsarbetet, vilket omfattar alla utförda uppgifter, alla resultat som produceras, i alla faser och från alla involverade aktörer.

4.3 Säkerhetskedjan

Det finns behov av att undvika påverkan av antagonister under varje fas i säkerhetskedjan, det vill säga från det att programmeringen startar till att det körande programmet har laddats i datorn. Behoven är främst i form av administrativa regler, som sedan förstärks med IT-säkerhetsskydd.

I dessa behov ingår även att gentemot ansvariga för och involverade i utvecklingsarbetet, både sett till egenutveckling och leverantörer, vara tydlig i att påvisa var i utvecklingsfaserna verifiering är viktigt. För egenutvecklade IT-system ligger behoven främst i de första faserna i säkerhetskedjan, exempelvis verifiering mellan specifikation och källkod.

Arbeta enligt beskrivna regler

Det finns behov av att ha administrativa regler för att undvika påverkan från antagonister under utveckling. Bland dessa regler ingår bland annat rutiner för hur ändringar i program hanteras, från beslut till genomförande, samt tvåsamhet i arbetet som ett skydd mot insiderhot i utvecklingen. Det finns dessutom behov av att få bevis för att utveckling har skett enligt dessa regler.

Kostnadseffektivt hantera stor mängd kod

Då IT-system oftast involverar komplexa förhållanden, beroenden och stor mängd kod ger det behov av att kunna hantera detta resurskrävande arbete vid verifieringar i säkerhetskedjan. Detta innebär bland annat behov av att kostnads-effektivt kunna granska stor mängd kod, samt behov av att ha IT-system med god insynsmöjlighet, då det förenklar granskningarna.

Skapa en säker utvecklingsmiljö

Det finns behov av att hantera utvecklingsmiljöer som hemliga IT-system sett till deras krav på säkerhet. Det gäller specifikt för utvecklingsmiljöer där hemliga IT-system utvecklas. Behovet innefattar bland annat bra källkodshantering och change management.

Bevisa ett IT-systems funktioner och IT-säkerhet

Då dagens IT-system är så komplexa finns det behov av att bevisa ett IT-systems funktioner och IT-säkerhet, möjligen genom formella metoder genom säkerhetskedjan, med avsikt att få IT-system som är tillräckligt säkra men med hög användbarhet (dvs. komplexa funktioner och strukturer). Behovet innefattar även att få effektivare granskningsförfarande och ökad pålitlighet hos lösningar, vilket i sin tur skulle kunna medge högre grad av logisk separation i IT-system och därmed ökad användbarhet i vissa sammanhang.

4.4 Kravställning i utvecklingsarbetet

Det finns ett stort antal behov som relaterar till att säkerställa att de system som tas fram både har tillräckligt IT-säkerhet och är användbara. Samverkan mellan verksamhet och teknik visar sig även i behov gällande att ta fram verksamhetsregler i samspel mellan verksamhetens behov och teknikens möjligheter. Då känsligheten i den information som hanteras i Försvarsmaktens system är så hög ställs det höga IT-säkerhetskrav, något som ibland upplevs begränsande hos användarna, och det finns behov av att säkerställa att användarna har förståelse för varför de olika IT-säkerhetskraven ställs.

Försvarsmakten har även ett behov av möjlighet att påverka informationshanteringen genom att få ställa kraven.

4.4.1 Stöd för att ta reda på vilka säkerhetsegenskaper som krävs för ett specifikt IT-system

Det finns behov av att få stöd för att utifrån ett specifikt IT-system i en specifik kontext kunna avgöra vilka IT-säkerhetsegenskaper som krävs för att kunna få ett pålitligt IT-system. (Notera att endast IT-säkerhetsegenskaper inte ger pålitligt system enligt övriga behov i analysen)

Designprinciper för IT-system

Det finns behov av att få stöd och riktlinjer för hur ett tillräckligt säkert IT-system bör byggas arkitektuellt i form av designprinciper. Bland annat utifrån infra-strukturella aspekter såsom separation, men även utifrån andra arkitekturella val som kan göras.

Beskrivning av det önskvärda resultatet och hur man kommer dit

Det finns behov av metodstöd för IT-säkerhet som beskriver det önskvärda resultatet och även hur man kommer dit, inte enbart checklistor. Detta stöd kan

då bidra till att analyser, såsom säkerhetsanalyser görs ordentligt genomarbetade med hänsyn till vad som ska skyddas och vad det ska skyddas mot. Metodstödet behöver vara ständigt aktuellt och uppdaterat utifrån kunskaper och erfarenheter samt innehålla beskrivningar av hur bra ordning och reda både i utveckling och under drift bidrar till högre IT-säkerhet och hur ordning och reda kan uppnås.

Säkerställ att tänkt lösning uppfyller kraven

Det finns behov av att kunna säkerställa att det man vill är det man tror man vill, bland annat genom att säkerhetsexpertis kommer in redan från början i projekten, så att behov av IT-säkerhet och motsvarande krav identifieras från start, jämfört med att uppkommer vid slutet.

4.4.2 Stöd för hur krav ska ställas för att få önskade säkerhets-egenskaper för ett specifikt IT-system

Det finns behov av stöd för att veta hur och vilka krav som ska ställas för att få önskade IT-säkerhetsegenskaper, det vill säga eliminering av tolkningsutrymmet i regelverket för IT-säkerhetskrav. Detta arbete behöver resultera i en vederhäftig säkerhetsmålsättning.

4.4.3 Stöd för att veta vilka lösningar som motsvarar uppställda krav på säkerhetsegenskaper

Det finns behov av att vid framtagning av IT-system ha stöd för att veta vilka lösningar (i form av produkter, designval etc.) som motsvarar uppställda krav på IT-säkerhetsegenskaper och därmed ger en godkänd säkerhetslösning. Detta både för att undvika omarbetningar i projekten på grund av ej godkända säkerhets-lösningar, men även för att undvika att antaganden görs om att mer komplexa säkerhetslösningar krävs med överarbetade lösningar som följd.

4.4.4 Användbarhet

För att ett system ska ge önskad effekt måste det användas på tänkt sätt i verksamheten, vilket ger behov av att systemen inte bara måste vara säkra utan även användbara. Användarna måste även kunna lita på systemet. Risken är annars att de inte använder systemet, vilket kan resultera i en mindre säker totallösning.

Ha en samlad bild av krav och behov innan lösningen tas fram

Det finns behov av att identifiera funktionella krav och IT-säkerhetskrav samtidigt, för att säkerställa kunskap om systemets användning och syfte i verksamheten. Även drift- och förvaltningsrelaterade behov, såsom driftövervakning, behöver omhändertas innan lösningen tas fram.

Ha kunskap om systemets användning och syfte i verksamheten

Det finns behov av att under systemets användningsfas ha kunskap om hur systemet ska användas, och dess syfte i verksamheten. Detta för att säkerställa användbarhet och uppnådd systemeffekt och därmed undvika att systemet inte används eller används fel.

4.5 Effektiva utvecklingsprojekt

Det finns ett antal behov som relaterar till utvecklingsprocessen avseende att få den så effektiv som möjligt.

Väl fungerande rutiner för förbättringshantering för IT-säkerhetsarbetet

Det finns behov av att ha väl fungerande rutiner för att ständigt förbättra IT-säkerhetsarbetet och omhänderta förbättringsförslag.

Ensad begreppsflora inom Försvarsmakten gällande IT-säkerhet

Det finns behov av att ensa begreppsfloran inom IT-säkerhetsområdet i Försvarsmakten med syfte att minska antalet missförstånd på grund av olika användning av samma begrepp.

Bara behöva granska en gång

Det finns behov av att effektivisera utvecklingsprocessen genom att bara behöva genomföra granskning en gång för att sedan kunna återanvända utan omgranskning. Detta behov appliceras på såväl enskilda komponenter och produkter som på hela plattformar. I de fall det handlar om att en tidigare granskad plattform ska kompletteras med en ny produkt är behovet att enbart behöva granska gränssnittet mellan IT-systemen (förutsatt de var för sig granskats tidigare). Behovet är även att enkelt kunna se vilka produkter alternativt IT-system som granskats och godkänts, och under vilka förutsättningar.

En effektiv auktorisationsprocess

Det finns behov av att förkorta auktorisationsprocessen genom att korta tiden för att ta beslut. Detta för att bland annat minska risken att information hinner bli inaktuell eller tappas bort i personalbyten samt för att minska kostnader för bland annat konsulter som inväntar beslut för att kunna fortsätta sitt arbete.

Granska direkt gentemot leverantörs produktbeskrivning

Det finns behov av beskrivning, riktad till tillverkare, av vad som krävs för att en programvara eller produkt ska bli godkänd, exempelvis att den måste ha en viss kontrollmekanism. Det skulle då kunna ge att en programvara eller produkt var direkt användbar, utan att behöva genomgå en hel granskningsprocess, så länge den är utvecklad enligt specifikationen.

Ha långsiktiga strategier

Det finns behov av långsiktiga strategier både för IT och IT-säkerhet, med avseende på att kunna ta beslut om IT-system som bedöms vara pålitliga både i kortare och längre perspektiv.

Värdera pålitlighet vid upphandling

Det finns behov av att vid upphandling kunna värdera pålitlighetsfaktorer och få med dem i beslutsbilden av upphandlingsalternativ.

4.6 Roller och ansvar i verksamheten

Det finns behov av tydlighet i ansvar och befogenheter för de roller som innehas av de som är involverade i IT-säkerhetsarbetet. De involverade kan i detta fall vara både enskilda personer och organisationsenheter. Bland annat behöver det vara tydligt var ansvaret för en lösning finns.

Samarbeta mot en gemensam IT-säkerhetslösning

Det finns behov av att förändra uppgifter och ansvar hos organisationsenheterna involverade i IT-säkerhetsarbetet för att tydliggöra ansvar och uppgifter, och undvika polarisering, internt och externt.

Ha kontinuitet i IT-säkerhetsarbetet

Det finns behov av kontinuitet i IT-säkerhetsarbetet i utvecklingsprocessen och förvaltningen. Då officerarna relativt ofta byter tjänst ger det ofta ett tapp i kunskap och erfarenhet, vilket ger ojämn nivå och ökar risken att uppgifter faller mellan stolarna. Behovet av kontinuitet applicerar även på det stora antal konsulter som idag arbetar i utvecklingsprojekten vilket gör Försvarsmakten sårbart gällande att tappa kunskap och kontinuitet när konsulterna slutar.

Genomför uppgifter samvetsgrant

Det finns behov av att säkerhetsanalyser, ackrediteringar och andra uppgifter inom anskaffning genomförs samvetsgrant, bland annat genom att inte se metodstöd enbart som checklistor utan ta hänsyn till systemets kontext och göra noggranna analyser och förstå syftet med uppgiften.

4.7 Kompetens

Det finns behov av att ha jämn och bra kunskapsnivå för att arbeta med IT-säkerhetsfrågor, men även av att ha tillgång till tillräckligt antal personer med relevant kompetens.

Förståelse för hur IT-system fungerar i praktiken

Det finns behov av förståelse för hur IT-system fungerar i praktiken bland de personer som arbetar med säkerhetsmålsättningen. Detta gäller inte minst de som genomför säkerhetsanalyser där det kan vara svårt att inse och identifiera potentiella problem utan praktisk erfarenhet av IT-system.

Erforderlig kompetens hos de som granskar lösningar

Det finns behov av att de som granskar IT-säkerhetslösningar har erforderlig kompetens för att göra rätt bedömning och förstå de komplexa systemen.

Utnyttja erfarenheter och tidigare arbete och beslut

Det finns behov av att inom Försvarsmakten samla och utnyttja erfarenheter från tidigare anskaffningar, lösningar och beslut.

4.8 Kommersiella programvaror

Då kommersiella programvaror, COTS[3] (kan även vara MOTS[4]), används inom Försvarsmakten finns det behov av att kunna hantera riskerna med kommersiella programvaror, där de risker som har påtalats främst relaterar till komplexitet, ständiga uppdateringar, stor andel nätverkstrafik samt svårigheterna med att verifiera startat program mot källkod. Det har uttryckts behov gällande säkerhetsrelaterade programvaror, såsom dataslussar. Det finns även behov av att bedömningen av pålitligheten i en programvara inte enbart ska ligga i relationen till ett företag utan mer utifrån assuransunderlag och produkt, då det ger sårbarhet om programvaran eller företaget skulle säljas till ett företag som Försvarsmakten inte har detta förtroende till. Behoven handlar således om att hantera bristen på pålitlighet hos kommersiella programvaror.

Kostnadseffektiv evalueringsmetod

Det finns behov av kostnadseffektiva och bra evalueringsmetoder. Det har även uttryckts behov av uppmärksamhet vid utvärdering av kommersiella programvaror som marknadsförs som evaluerade, där evalueringen kan gälla enbart en specifik version eller del av programvaran.

Modularisera kommersiella programvaror

Då många kommersiella programvaror är omfattande och komplexa och Försvarsmakten ibland får sitt behov tillgodosett av endast en del av programvaran finns det behov av att få möjlighet att enbart anskaffa den del av programvaran som avses användas. Detta behov är dock inte av karaktären att det direkt ligger inom Försvarsmaktens påverkansområde.

4.9 Hantering av risker

Det finns behov av att kunna balansera IT-säkerhetskraven gentemot systemets kontext och att ibland kunna acceptera vissa risker.

Anpassa IT-säkerhetskraven efter verksamhet och ekonomi

Det finns behov av att anpassa nivån för IT-säkerhetskraven så att de matchar de ekonomiska förutsättningarna och systemets kontext, det vill säga kunna ta beslut gällande IT-säkerhetsegenskaper med hänsyn till användningssituation. Behovet

[3] Commercial off-the-shelf – produkter som finns att tillgå på den kommersiella(civila) marknaden.
[4] Military off-the-shelf – produkter som finns att tillgå på den militära marknaden.

innebär även möjlighet att balansera prioriteringen mellan kostnader, krav och IT-säkerhet.

Ha möjlighet att acceptera risker

Det finns behov av att vid de tillfällen en IT-säkerhetslösning inte får godkänt i granskningen samtidigt få en konsekvensbedömning av användning i verksamheten, för att på så sätt få möjlighet att göra avvägda beslut om huruvida riskerna är accepterbara. Behov har uttryckts av att kunna ta hänsyn till verksamhetens totala informationssäkerhetslösning, där det ibland framkommer att ett delvis osäkert IT-system är totalt sett säkrare än inget IT-system.

4.10 Arkitektur

Den största mängden behov som har identifierats relaterar till systemets eller lösningens arkitektur, avseende teknik, applikation och verksamhetsregler. Behoven bygger på att ha en arkitektur för IT-systemen där IT-säkerhets-lösningen ses som en helhetslösning, inte enbart beroende på en specifik säkerhetsmekanism. Arkitekturen måste även byggas på ett sådant sätt att det som inte kan säkras upp omhändertas genom att minimera effekterna av eventuell påverkan, även konsekvenser i form av omedveten felanvändning. En sådan arkitektur, i form av avgränsning, ger en större tillit till att systemets skada begränsas. Ett exempel är kommersiell programvara som måste stöttas av arkitekturella lösningar för att uppnå en tillräcklig pålitlighet.

4.10.1 Utformning av arkitekturen

För att få pålitliga IT-system behövs tydliga arkitekturer då det ger mindre komplexitet, ökad möjlighet till överblickbarhet och förenklar IT-säkerhets-lösningarna. De arkitekturer som främst åsyftas är verksamhetsarkitektur, applikationsarkitektur och teknisk arkitektur. Tydliga arkitekturer ökar även möjligheterna för logisk separering i IT-säkerhetslösningar, vilket i sin tur ökar användbarheten. I detta sammanhang finns det även behov av att ha bra dokumentation som kan fungera som en karta över lösningen för att effektivt minska de resurser som krävs för att få kunskap om och överblick över lösningen.

Det finns behov av att undvika kompensationsbaserade lösningar genom att lägga skyddet så nära informationen som möjligt, och ha IT-säkerhetsskydd i flera lager.

Det finns behov av att arkitekturerna för IT-systemen ska vara så ensade som möjligt för att på så sätt öka effektiviteten och minska sårbarheten orsakad av de personberoenden som uppstår med många speciallösningar.

4.10.2 Komponenter

Tillgång till granskade och godkända komponenter

Det finns behov av att vid framtagning av arkitekturen ha tillgång till ett tillräckligt antal betrodda säkerhetskomponenter att välja mellan, tillgängliga vid det tillfälle de behövs och väl testade och fungerande redan från början. För att bidra till pålitligheten bör komponenterna vara enkla att infoga i lösningen, och på så sätt minska risken att de används fel eller inte fungerar som det är tänkt.

4.10.3 Komplexitet

Hantera komplexitet

Då många av Försvarsmaktens system och lösningar är mycket komplexa finns det tydliga behov av att kunna hantera denna komplexitet. Komplexiteten består bland annat av en stor mängd verksamhetsregler, infrastruktur, informationsutbyte samt av att IT-säkerhetsbehovet är kontextberoende (leverans av ett par skor till en soldat i ett förband är inte hemligt, men det totala antalet skor i förbandet kan vara hemligt om det aktuella förbandets antal soldater är hemligt). Komplexiteten kan även ligga i enskilda komponenter i form av stor mängd kod och beroenden och att informationen kan finnas på flera olika ställen, till exempel i IT-systemet (databas), på utskrifter och i systemloggar. En del av behovet är att få så låg komplexitet som möjligt.

Det finns även behov av att minska komplexiteten genom att ha ett fåtal, generella, tekniska lösningar att välja mellan vid utformning av system. Då komplexitet är en orsak till att det blir omöjligt att ta ett helhetsgrepp om lösningar vid deras utformning finns det behov av stöd för att på ett effektivt sätt arbeta sig fram stegvis till en bra och tillräckligt säker totallösning.

4.10.4 Separation

Information med olika sekretessklassningar hanteras i fysiskt separerade IT-system. Det finns behov av att få regler och tekniska system som effektivt stödjer användarnas arbete med information, när olika delar av information som bearbetas i samma arbetsmoment har olika sekretessnivå. Problem som kan uppstå är att den lägre klassade informationen kan bli svår att flytta när den förts in i ett system med högre säkerhetsklassning.

Det finns behov av att i större utsträckning kunna lita på loggningsfunktioner, som skulle kunna larma om någon obehörig tar del av information i IT-systemet. Detta skulle då kunna tillåta en lägre grad av separation.

4.11 Drift

Det finns, främst ur ett tillgänglighetsperspektiv, behov av att säkerställa pålitlighet genom väl fungerande drift av IT-system, med möjlighet att kontrollera hur IT-systemen fungerar via övervakning. Det finns även behov av att vid problem ha tillgång till redundanta IT-system för att kunna säkerställa tillgängligheten.

Säkerställ funktionalitet och IT-säkerhet

Det finns behov av att genom test och verifiering av systemen säkerställa att systemen gör sin uppgift som de ska. För att kunna genomföra relevanta tester finns behov av att ha identiska kopior av produktionsmiljön, med i möjligaste mån samma data

Möjlighet att uppgradera system stegvis

Då IT-systemen och lösningarna är komplexa och omfattande finns det behov av att kunna uppgradera delkomponenter utan att behöva byta ut hela lösningen.

Tydlig förvaltningsorganisation

Organisationen runt systemen måste vara tydlig, med tydliga rollbeskrivningar, rolltilldelningar och ansvar. Genom en tydlig förvaltningsorganisation finns det intressenter att kontakta när så behövs, som kan stödja i kravarbete och säkerställa att kravspecifikationen blir korrekt och tillgodoser behoven. I detta behov ingår även behov av att ha en tydlig kostnadsbild för systemen.

5 Diskussion

I detta kapitel diskuteras de resultat som framkom under behovsinventeringen. Diskussionen av resultaten utgår från respondenternas synsätt på pålitlighet samt de mest frekvent uttalade behoven. Diskussionen avslutas med förslag på framtida arbete.

Resultaten visar på en stor bredd i synsättet på pålitliga IT-system, såväl vad ett pålitligt IT-system innebär, som vad som krävs för att nå dit. De olika synsätt som har förts fram är inte direkt motsägande, utan snarare formulerade utifrån olika personers perspektiv och därmed med olika prioritering. Det är exempelvis naturligt att en person som arbetar med drift främst beskriver pålitlighet som relaterat till drift av IT-system. Dessa olika perspektiv kompletterar därmed varandra och ger en mer heltäckande bild av behoven avseende pålitliga IT-system.

Utgångspunkten i studien var att fånga behov relaterade till pålitliga IT-system, i betydelsen att de gör det de ska enligt specifikation och ingenting annat. Respondenternas svar visar att problemen inte direkt ligger i att hitta IT-säkerhetslösningar som är tillräckligt säkra för att skapa pålitlighet. De behov som uttalades mest frekvent gäller istället att (1) uppnå pålitlighet med bibehållen verksamhetsnytta, (2) uppnå pålitlighet samtidigt som ackrediterings-processen är effektiv samt (3) nyttja arkitektur som ett medel för att uppnå pålitlighet.

Att få ett system som är tillräckligt säkert för att bli godkänt och samtidigt behålla användbarheten för att därmed ge verksamhetsnytta är en stor utmaning för Försvarsmakten. Kraven på säkerhet är höga och då absolut, bevisad IT-säkerhet inte kan uppnås idag medför det IT-säkerhetsskydd i flera lager för att säkerställa att IT-systemet är tillräckligt säkert. Flera respondenter uttalar behov av att redan i början av projektet arbeta fram funktionella krav och IT-säkerhetskrav samtidigt för att få in säkerheten i systemet så tidigt som möjligt, jämfört med att lägga på IT-säkerhetsskydd vid senare tillfälle då det kan begränsa funktionerna i systemet. Respondenterna beskriver problem med att IT-system är allt för säkra i betydelsen att deras användbarhet begränsas. Att nå pålitlighet menar respondenterna även handlar om hur systemet används – att systemet används som tänkt och att det ger den effekt som behövs i verksamheten. Detta innebär alltså att det inte bara är pålitlighetsfrågor för IT-systemen i sig som är viktiga, utan hänsyn måste tas till pålitligheten för systemen och kontexten som helhet.

Dagens ackrediteringsprocess upplevs av flera respondenter som allt för långdragen och resurskrävande. Behov har därför uttryckts gällande att göra den effektivare, bland annat i form av enklare granskningsförfarande och kortare beslutsprocesser. Effekten av att få dessa behov tillgodosedda skulle bespara

Försvarsmakten resurser och ge en större mängd system som stödjer verksamheten.

En bra arkitektur bidrar till ökad pålitlighet på flera olika sätt. Arkitekturens viktigaste funktion är att hantera den komplexitet som utmärker Försvarsmaktens systemmiljöer, bland annat med avseende på stora mängder kod, verksamhetsregler, systemberoenden och användare. Det finns därmed ett stort behov av att få stöd för att enklare och effektivare kunna förstå och hantera denna komplexitet samt av att se lösningen i ett större sammanhang, både vid integration av tidigare godkända komponenter och på en system-av-system-nivå. Saker som skulle kunna bidra till minskad komplexitet är ensade plattformar, för att minska antalet unika lösningar, och att eftersträva enkla logiska arkitekturer, vilket förenklar de tekniska arkitekturerna. Genom att kunna bevisa olika IT-säkerhetsegenskaper skulle det bli enklare att hantera komplexitet. Minskad systemkomplexitet och stöd för att hantera komplexiteten skulle skapa förutsättningar för enklare IT-säkerhetslösningar och därmed även ökad användbarhet och för Försvarsmakten ökad verksamhetsnytta.

Kommersiella programvaror är svåra att hantera i sammanhanget pålitlighet, då det finns ett stort antal okända parametrar i deras säkerhetskedja. Även om Försvarsmakten får tillgång till källkod kan den vara allt för omfattande för att kunna sätta sig in i, och hur kan det säkerställas att det är just den källkod Försvarsmakten får studera som ligger till grund för programfilerna som är installerade i Försvarsmaktens IT-system? De behov som relaterar till pålitlighet för kommersiella programvaror handlar därför främst om möjligheter att kunna hantera dessa risker och bygga skydd kring programvarorna.

För att sammanfatta vad behovsinventeringen pekar på som nödvändigt för att nå pålitlighet:

En tydlig arkitektur med godkända IT-säkerhetslösningar, gärna via återvinning av befintlig plattform, som stödjer verksamheten på ett effektivt sätt med användbara IT-system, där lösningen är framtagen av kompetent personal, med hjälp av bra och effektivt metodstöd, både i utveckling och i granskning, vilka följs på ett sätt som ger kvalitet där alla involverade aktörer samarbetar på ett effektivt sätt.

Då studien utifrån sju intervjuer visar på en sådan bredd i behoven relaterade till pålitliga IT-system finns det möjligheter att i framtida arbete göra en fördjupad behovsanalys inom prioriterade delområden. Ett sådant arbete kan genomföras genom att dels förankra det i denna rapport presenterade resultatet tillsammans med representanter från Försvarsmakten, dels göra ytterligare djupintervjuer specifikt fokuserade på de prioriterade delområdena. En sådan behovsanalys utgör då grunden för en kravanalys där krav på åtgärder för att skapa pålitliga IT-system tas fram.

Referenser

J. Löfvenberg och K. Lundholm. Pålitliga plattformar. Teknisk rapport FOI-R--3136--SE, 2010.

J. Löfvenberg och I Rhode. Litteraturstudie av tekniker för pålitliga IT-plattformar. FOI-R--3724--SE, 2013.

A. M. Davis. Just Enough Requirements Management: Where Software Developement Meets Marketing. Dorset House, 2005.

L. Cohen. Quality Function Deployment: How to Make QFD Work for You. Addison-Wesley, 1995.

M.L. Shillto. Acquiring, Processing, and Deploying Voice Of The Customer. St Luice Press, 2001.

N. Hallberg, R. Andersson och L. Westerdahl. Quality-driven process for requirement elicitation: the case of architecture driving requirements. Användarrapport FOI-R--1576--SE, 2005.

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se