“Det är en tuff bedömning, men den behöver ju göras”

- En explorativ fallstudie på svenska Försvarsmakten om bedömningar av uppdateringar på säkerhetsklassade IT-system.

Författare:
Carl-Fredrik Enerholm (901201)
Mats Nilsson (870329)

HT20
Informatik med systemvetenskaplig inriktning, kandidatkurs, 30 hp
Ämne: Informatik
Handelshögskolan vid Örebro universitet
Handledare: Ella Kolkowska
Examinator: Hannu Larsson

Förord

Vi vill rikta ett stort tack till de representanter för Försvarsmakten och Combitech som deltagit i vår fallstudie. Ert tålamod och engagemang har varit ett stort bidrag till denna uppsats. Vi vill också tacka vår handledare Ella Kolkowska och vår kontaktbibliotekarie Gitta Harder för all den hjälp vi fått.

Sammanfattning

Godkännande av IT-system ur ett säkerhetsperspektiv görs inom flertalet olika organisationer som hanterar information som de anser behöver skyddas. När ett godkännande görs tas det hänsyn till hur det specifika IT-systemet uppfyller olika säkerhetskrav vid tillfället för godkännandet. Detta godkännande kallas av Försvarsmakten för ackreditering. Men hur påverkas en ackreditering av system- och säkerhetsuppdateringar? Detta har visat sig svårt att ge ett svar på och varje enskild uppdatering måste bedömas utifrån aktuell kravbild. I denna studie ställs därför frågan "*Vilka faktorer är viktiga vid en bedömning av om en ackreditering måste omprövas vid system- och säkerhetsuppdateringar på ett ackrediterat IT- system som hanterar säkerhetsklassad information?*" För att undersöka detta genomförs en explorativ fallstudie på Försvarsmakten och deras leverantör Combitech. Slutsatsen visar på att kompetens hos de som utför bedömningarna samt stöd i form av stöddokument och kommunikation är viktiga faktorer.

Nyckelord:
Ackreditering, Försvarsmakten, IT-system, system- och säkerhetsuppdateringar.

Centrala begrepp/Förkortningar

Ackreditering:	"*Godkännande av IT-system ur säkerhetssynpunkt*" (Fredriksson, 2014, s. 60)
Assuranskrav	"*De krav i KSF på åtgärder och underlag som ska säkerställa att säkerhetsmålen uppfyllts på ett tillräckligt och effektivt sätt.*" (Försvarsmakten, 2014e, s. 4)
CIO	Chief Information Officer, den del av Försvarsmaktens ledningsstab som ansvarar för frågor rörande informationssäkerhet.
DoD:	Department of Defense, den amerikanska motsvarigheten till Försvarsmakten.
Evaluerare	Den som genomför en evaluering.
Evaluering	"*Verifiering av ett IT-systems IT-säkerhetsegenskaper genom aktiviteter såsom granskning av dokumentation, källkod och konfiguration, testning av IT-systemets IT- säkerhetsfunktionalitet och granskning av miljön där utveckling av IT-systemet äger rum.*" (Försvarsmakten, 2014e, s. 5)
ISO:27001	Standard för att kvalitetssäkra processer och arbete med Informationssäkerhet (Svenska Institutet för Standarder, u.å.)
IT-system:	"*Ett system med teknik som utbyter och hanterar information med omgivningen.*" (Försvarsmakten, 2014e, s. 7)
IT-säkerhet	All typ av säkerhet som berör data i IT-system.
Livscykel:	"*Tiden från och med det att ett behov av en it-tjänst eller ett it-system har identifierats till den tidpunkt när it-tjänsten eller systemet har avvecklats*" (Försvarsmakten, 2017b, s. 2)
Om-ackreditering:	En ackreditering som sker på ett IT-system som är i drift i organisationen och därför redan har ackrediterats.
Sekretess	"*Avsikten att innehållet i ett informationsobjekt (eller ibland även dess existens) inte får göras tillgängligt eller avslöjas för obehöriga.*" (Försvarsmakten, 2014e, s. 9)
Säkerhetsklassad information	Information som bedöms skyddsvärd

Innehållsförteckning

1 Introduktion

I detta avsnitt introduceras det fenomen som denna uppsats är ämnad att beröra. Vidare redogörs kortfattat för tidigare litteratur på ämnesområdet och en problemformulering presenteras. Studiens syfte och forskningsfråga presenteras, problematiseras och avgränsas. Avslutningsvis ges även läsaren en kortfattad beskrivning av den process som genomgående berörs under studien.

1.1 Bakgrund

I början av vårt uppsatsarbete tog vi kontakt med Combitech som är en av flera leverantörer av IT-system till den svenska Försvarsmakten. Under sitt arbete med att underhålla och uppdatera IT-system åt Försvarsmakten lyfte Combitech (personlig kommunikation, 26 november 2020) en problematik kring frågan när en uppdatering ska bedömas ha en påverkan på befintlig ackreditering. Det vill säga att uppdateringens påverkan på systemet är i den omfattning att en ny säkerhetsbedömning behöver göras och godkännas, härefter kallat om-ackreditering. Det framkom att en om-ackrediteringsprocess är kostsam ur både ett tids- och kostnadsperspektiv och eventuellt skulle kunna undvikas om man redan i ett initialt skede i uppdateringsarbetet har en klar förståelse över vad som påverkar ackrediteringen.

Combitech (personlig kommunikation, 26 november 2020) menade att många företag, myndigheter och andra organisationer som hanterar information som omgärdas av sekretess eller som bedöms som säkerhetsklassad använder någon form av process för godkännande av sina IT-system innan de får användas. Detta görs inte minst utifrån ett säkerhetsperspektiv för att kontrollera att säkerhetsnivån på det tilltänkta IT-systemet är fullgott och lever upp till de krav som ställs av organisationen. Vidare menar Combitech att ett IT-system under sin livscykel näst intill alltid har mer eller mindre behov av uppdateringar, det kan gälla både funktionella och säkerhetsrelaterade uppdateringar, som förändrar IT-systemet över tid. Deras kund Försvarsmakten är ett exempel på en organisation som hanterar information som omgärdas av sekretess eller som bedöms som säkerhetsklassad.

För att se om Försvarsmakten delade Combitechs syn på problematiken kring frågan om när en uppdatering ska bedömas ha en påverkan på befintlig ackreditering så togs en initial kontakt med Försvarsmakten. Försvarsmakten (personlig kommunikation, 3 december 2020) bekräftade att det är en komplex process och instämde i problematiken. Vidare beskrev de att uppdateringar som görs på ackrediterade IT-system inom Försvarsmakten inte får försämra den säkerhetsnivå som IT-systemet ursprungligen ackrediterats för. Om det finns risk för att så är fallet behöver en om-ackreditering göras. Detta medför att alla uppdateringar på IT-system måste ställas mot den ursprungliga kravbilden och en bedömning av dess inverkan göras.

Att utreda problematiken kring bedömningar av om uppdatering bidrar till att den befintliga ackrediteringen påverkas till den grad att en om-ackreditering behöver göras kan därför bli av stor vikt, inte bara för Försvarsmakten och dess underleverantörer utan för samtliga myndigheter som har som skyldighet att följa vad som tydliggörs i 12§ av säkerhetsskyddsförordningen (SFS 1996:633) "*Systemet får inte tas i drift förrän det har godkänts från säkerhetssynpunkt av den för vars verksamhet systemet inrättas."*

För att klarlägga om hantering av uppdateringar upplevdes som problematiskt även utanför Försvarsmakten valde vi att kontakta en rad olika myndigheter via mail. I mailet beskrev vi Försvarsmaktens process kortfattat och frågade om de tillfrågade hade en liknande process och om de i så fall upplevde samma problematik. Det som framkom var att Polisen, Luftfartsverket, Domstolsverket, Skatteverket (SKV), Försvarets Radioanstalt (FRA) och Kronofogdemyndigheten hade liknande processer. Säkerhetspolisen valde att inte besvara frågan utan hänvisade till sekretess. SKV och FRA beskrev vidare att de håller på att se över sina processer för att underlätta arbetet och bekräftar att de upplever en liknande problematik.

Tidigare litteratur gällande godkännande av IT-system inom organisationer som hanterar säkerhetsklassad information utgår nästintill uteslutande ifrån att ett nytt IT- system utvecklas och sedan implementeras. Dock lyfter Nemr (2008) godkännande ur perspektiv av redan befintliga IT-system som har behov av godkännande innan implementering. Det är svårare att hitta information i befintlig litteratur om hur man hanterar detta när det kommer till drift och underhåll och eventuella behov av att förnya godkännande efter att ett IT-system förändrats så pass mycket att det kan påverka IT-säkerheten.

Tysenn (2006) pekar på att man inom branscher som inte har lika högt säkerhetsbehov framgångsrikt har använt sig av ett tillvägagångssätt där förnyanden av godkännanden sker med ett påförhand angivet tidsintervall. Loughry (2013) menar däremot att om en signifikant uppdatering görs kan ett nytt godkännande behöva göras av det redan implementerade IT-systemet. Denna skrivning ger utrymme för tolkning av vilka uppdateringar som påverkar när en ny process om godkännande bör genomföras. Shilling (2016) menar också att om-ackrediteringar behöver göras vid förändringar, men skulle inte detta ske bör man ändå om-ackreditera vart tredje år om en om-ackreditering inte skett.

Gemensamt för litteraturen är att de talar om ackrediteringsprocessen vid ett införande av IT- system i en organisation. Enbart kortfattat nämns det att om-ackrediteringar behöver göras om större eller signifikanta ändringar görs som nämnt tidigare. Detta visar på att det idag finns ett kunskapsgap när det gäller om-ackrediteringar i befintlig litteratur.

Fredriksson (2011) angriper ackrediteringsprocessen från ett svenskt perspektiv när hen kartlägger hur Försvarsmakten och tidigare nämnda Combitech hanterar befintlig process fram till dess att en ackreditering är på plats. Hen exkluderar således en djupare analys av de delar av processen som berör en eventuell om-ackreditering. Hen lyfter vidare i sitt avslutade stycke att "*intressant vore att studera beslut som tas under drift för att knyta samman hela livscykelperspektivet*" (Fredriksson, 2011, s. 56).

1.2 Problemformulering

I befintlig litteratur lämnas frågan om vad som krävs för att en uppdatering från en leverantör ska påverka den befintliga ackrediteringen utan svar. Denna fråga blir dock omöjlig att svara på då olika system bygger på olika kravbilder och bedömningar behöver därför göras utifrån det specifika IT-systemet. Dessa bedömningar görs löpande av leverantörer och beställare från det att en uppdatering initieras till dess att den införs. Bedömningarna ligger till grund för det underlag som beställare fattar sitt beslut på gällande om en uppdatering ryms inom befintlig ackreditering eller ej. Ett problem som uppstår i denna process är att det är svårt för leverantören att veta om de bedömningar som görs stämmer överens med vad beställaren anser ligga inom ramen för gällande ackreditering. Bedömningarna blir således viktiga, men vi lämnas med frågan om vad som blir viktiga faktorer för att göra dessa bedömningar.

I denna uppsats kommer en fallstudie av svenska Försvarsmakten genomföras som ett exempel på en organisation som med hjälp av IT-system hanterar information som omgärdas av sekretess eller som bedöms som säkerhetsklassad och hur de arbetar med deras leverantör Combitech kring uppdateringar av dessa IT-system. Genom denna fallstudie hoppas vi kunna identifiera vilka faktorer som är viktiga i bedömningsarbete och komma med förslag på hur detta arbete kan underlättas. Vidare hoppas vi genom att identifiera problematiken kring bedömningar av uppdateringar kunna ge ett underlag för fortsatt forskning på ämnet.

1.3 Syfte och forskningsfråga

Syftet med denna studie är att undersöka om det går att underlätta arbetet med bedömningar om en system- och säkerhetsuppdatering påverkar befintlig ackreditering av ett IT-system som hanterar säkerhetsklassad information.

Huvudfråga:

- Vilka faktorer är viktiga vid en bedömning av om en ackreditering måste omprövas vid system- och säkerhetsuppdateringar på ett ackrediterat IT- system som hanterar säkerhetsklassad information?

Underfrågor för att besvara huvudfråga:

- Vad säger befintliga styrdokument om system- och säkerhetsuppdateringar på ett ackrediterat IT-system?

- Hur arbetar Försvarsmakten med att göra bedömningar om vilka förändringar som bidrar till att den befintliga ackrediteringen måste omprövas vid system- och säkerhetsuppdateringar på ett ackrediterat IT-system?

- Hur arbetar Combitech med att göra bedömningar om vilka förändringar som bidrar till att den befintliga ackrediteringen måste omprövas vid system- och säkerhetsuppdateringar på ett ackrediterat IT-system?

1.4 Problematisering och avgränsning

Studien kommer att använda sig av Försvarsmaktens definiering av IT-system vilket är "*Ett system med teknik som utbyter och hanterar information med omgivningen.*" (Försvarsmakten, 2014e, s. 7). Ackreditering avser den typ av godkännande som görs på ett IT-system för att säkerställa att det uppfyller de säkerhetskrav som finns. Med system- och säkerhetsuppdateringar avses alla förändringar som sker från det att IT-systemet blivit ackrediterat till dess att det avvecklas. Styrdokument är de dokument som har till uppgift att reglera vilka regler som gäller för en viss verksamhet.

Huvudfrågan ställs då det kommit till vår kännedom att det är svårt att veta vad som bidrar till att en system- och säkerhetsuppdatering påverkar om en om-ackreditering behöver göras och att mycket grundar sig i bedömningar. Det är därför intressant att titta på vilka faktorer som är viktiga för en bra bedömning. För att göra detta behöver vi först undersöka vad befintliga styrdokument säger om uppdateringar, dels för att se om svar finns där men framförallt för att skapa en god förståelse för aktuella styrdokument. Vidare blir det även viktigt att se till hur de olika parterna i studien arbetar med styrdokumenten och vad de upplever som problematiskt med bedömningar av uppdateringar. Utifrån den identifierade problematiken borde det framgå vilka faktorer som blir viktiga i bedömning av uppdateringar.

Avgränsningen görs till att bara se till hur arbetet med bedömningar av om en system- och säkerhetsuppdateringar leder till en om-ackreditering på ett IT-system är aktuell eller inte. Vidare görs en avgränsning mot att se till förhållandet mellan myndigheter som behöver förhålla sig till säkerhetsskyddsförordningen (SFS 1996:633) och dess leverantörer och deras processer för att hantera system- och säkerhetsuppdateringar.

1.5 Försvarsmaktens ackrediteringsprocess

I Försvarsmaktens Handbok Säkerhetstjänst Informationssäkerhet beskriver de att "*En myndighet som avser driftsätta ett IT-system som är avsett för behandling av hemliga uppgifter ska innan driftsättningen ha ackrediterat IT-systemet (godkänt systemet ur säkerhetssynpunkt*)" (Försvarsmakten, 2013, s. 329). Fredriksson (2011) beskriver utförligt i sitt arbete hur ackrediteringsprocessen inom Försvarsmakten går till och menar att syftet med processen är att säkerställa att IT-systemet är säkert. Försvarsmakten tittar dels på vilken typ av information systemet ska behandla och på vilket sätt denna kommer att

behandlas. Utifrån detta gör man sedan en bedömning för hur informationen ska skyddas. Frediksson (2011, s. 27) menar att "*genom ackreditering säkerställs att det IT-system som utvecklas verkligen håller en tillräckligt hög nivå vad gäller informationssäkerhet*". Fredriksson (2011) menar vidare att innan en ackrediteringsprocess påbörjas genomförs något som kallas auktorisation. I denna fas beskrivs behovet av IT-systemet och man motiverar varför det behövs och vad det ska användas till. Vidare görs en rad olika analyser av vilket säkerhetsbehov som finns för systemet och riskanalyser m.m. genomförs. Dessa analyser ligger sedan till grund för att säkerhetsklassa systemet vilket kommer få betydelse för vilka krav som kommer att ställas på systemet. Efter detta skapas de krav som systemet måste uppfylla ur en säkerhetssynpunkt. Kraven kommer sedan att gälla genom hela IT-systemets livscykel. De ligger även till grund för att ta fram en preliminär teknisk kravspecifikation som har till uppgift att omvandla säkerhetsmålen till tekniska krav på IT-systemet. Dessa tekniska krav ligger sedan till grund för att ta fram IT-systemet som testas och granskas innan det lämnas över för ackreditering.

Fredriksson (2011) skriver att när IT-systemet ska ackrediteras så övergår beslutsunderlaget till ackrediteringsunderlag där en del har till uppgift att beskriva hur kraven är uppfyllda. Underlaget ska också innehålla en rad dokument så som, systemöversikt, installationshänvisningar, handböcker, leveransbeskrivningar, säkerhetsfunktioner, testplan och testfall, testrapport och en säkerhetsgranskning. Utifrån ackrediteringsunderlaget fattas sedan ett beslut av Försvarsmaktens Chef Information Officer (CIO) om IT-systemet ska bli ackrediterat och därmed godkänt att använda inom försvarsmakten eller ej.

Vidare skriver Fredriksson (2011) att när IT-systemet är i drift så tas det fortlöpande olika beslut under dess livscykel. Ändringar som ryms inom ackrediteringen, alltså inte påverkar systemsäkerheten negativt kan göras. Om det inte ryms inom befintlig ackreditering så måste ackrediteringsbeslutet revideras, det vill säga systemet utsätts för en om-ackreditering.

2 Teoretisk bakgrund

I detta avsnitt ges en teoretisk bakgrund av ämnesområdet i form av en redovisning av vad tidigare forskning säger om ämnesområdet.

2.1 Tidigare forskning

Utifrån de artiklar som blev utvalda i vår litteratursökning som beskrivs i metodavsnittet var det få som berörde fenomenet med hur uppdateringar påverkar befintlig ackreditering. En betydande del av litteraturen riktar sig mot den amerikanska motsvarigheten till svenska Försvarsmakten, Department of Defense (DoD), och deras styrdokument och riktlinjer. Litteraturen riktar sig mot den typ av godkännanden som berör ett system som ännu ej är i drift i den aktuella organisationen. Det finns därmed en avsaknad av hur man bedömer om det finns ett behov av att göra om processen för godkännande efter en uppdatering på ett system i drift.

Loughry (2013) lyfter vikten av att varje IT- system som används av statliga myndigheter måste genomgå en ackrediteringsprocess för att kunna användas, men även att IT- systemet behöver om-ackrediteras om det skulle genomgå "signifikanta" uppdateringar. Vidare menar artikelförfattaren att ackrediteringsprocessen ofta är att betrakta som tidskrävande för de parter som deltar i den och att den ofta drar ut på tiden. En anledning till detta som lyfts fram är att de personer som gör bedömningar och fattar beslut kopplade till processen ofta känner ett personligt ansvar för att ta korrekta beslut och att detta leder till långa handläggningstider. Författarna lyfter även att det finns indikationer på att informell kommunikation mellan berörda parter som deltar i ackrediteringsprocessen är en bidragande faktor till en lyckad process.

Capitan (2008) menar att utformningen av en ackrediteringsprocess och hur den hanterar informationssäkerhet är den enskilt viktigaste faktorn för att bibehålla god kvalitet och säkerhet inom de IT- system som används av DoD. Hen menar att arbetet med en ackrediteringsprocess dock är komplex oavsett utformningen och att det därför blir viktigt att denna process fungerar och att man lyfter problematiken som en ledarskapsfråga snarare än en ren implementeringsfråga.

Enligt Tysenn (2006) är det viktigt att ha ett säkerhetstänk genom ett IT-systems hela livscykel. Extra viktigt blir detta när man ser till de IT-system som används inom DoD. Hen menar att om fokus ligger på detta kan man öka både säkerheten men även göra kostnadsbesparingar. Vidare menar författaren att många privata företag kan dra nytta av det arbete som görs av DoD då det med lätthet skulle gå att applicera även deras processer.

Även Dawson, Burell, Rahim och Brewster (2010) lyfter vikten av att tidigt i IT- systemets livcykel inkludera ett tydligt säkerhetstänk. De är även eniga med Tysenn (2006) om att detta blir extra viktigt när det gäller IT-system inom DoD eller andra länders försvarsmakter. Detta då de menar att man som utvecklare av ett IT- system som ska användas inom försvarsindustrin har ett anvar gentemot de liv som IT- systemet ska vara med att försvara.

Dawson m.fl. (2010) menar att kompetent personal därför blir en lika viktig faktor som de policies och processer som tas fram i samband med skapandet av ett IT- system.

Buszta (2008) menar att det framförallt finns två viktiga faktorer för att en ackrediteringsprocess ska bli lyckad. Dels gäller det att alla berörda parter i utvecklingen och driften av ett IT- system förstår de olika krav som ställs på IT- systemet. Något som i vissa fall kan bli problematiskt om kraven lämnar utrymme för tolkning då olika personer kan tolka saker på olika vis. Utöver detta gäller det att man har mät- och nyckeltal som är rättvisa och kan användas på ett konsekvent sätt i IT-systemet.

En betydande del av den litteratur som finns på ämnet ackrediteringar berör som tidigare nämnt DoD. Salmans (2014) skriver om att fram till 2014 använde DoD sig av den interna processen "*Department of Defense Information Assurance Certification and Accreditation Process*" (DIACAP), men bytte till "*Risk Management Framework" (RMF).* Båda dessa processers mål beskrivs av författaren som att mildra eventuella sårbarheter i IT- system till en acceptabel nivå. Dessa eventuella sårbarheter uppstår oftast av svaga säkerhetsrutiner och dålig intern kontroll och kan leda till oönskade följder vid systemfel, männskliga misstag, störningar i driftmiljö och inte enbart av målmedvetna attacker mot IT-systemet vilket tycks vara den vanligaste farhågan.

3 Metod

Inledningsvis i detta avsnitt beskrivs hur den litteratursammanställning som redovisats i föregående avsnitt genomförts. Vidare beskrivs de metodavsnitt som studien består av i form av en fallstudiebeskrivning, ett metodavsnitt för hantering av styrdokument och ett metodavsnitt för intervjuer. Avsnittet innehåller även en diskussion om de etiska överväganden som behövts göras i samband med vald metod. Avslutningsvis förs även en metoddiskussion där kritik mot den valda metoden lyfts fram.

3.1 Litteratursammanställning

Vid sammanställning av tidigare forskning har vi valt att utgå ifrån Web of Science och Scopus. Detta då dessa två har ett erkänt gott rykte och allmänt betraktas som trovärdiga. Även en sökning i DiVA gjordes för att se om det fanns tidigare uppsatser som berörde ämnet.

En rad sökord användes och dessa redovisas i tabell 1 nedan. Sökorden har kombinerats på en rad olika sätt samt delats in i tre olika kategorier, vad, var och hur. Kategorin “vad” har bestått av sökord kopplade till vad som ska göras. Kategorin “var” har bestått av sökord för att definiera i vilket sammanhang detta ska ha skett. Kategorin “hur” har bestått av förstärkande sökord som i de fall de har använts har använts för att smalna av sökningen. Även ett professionellt stöd användes i sökprocessen i form av en kontaktbibliotekarie för informatikområdet på Örebro Universitet.

Vi har även gjort valet att på en rad sökord använda oss av asterix för att inte avgränsa oss till en ändelse på ord vars olika ändelser vi vill ha med. Ett exempel på detta är sökordet “updat*” som innefattar sökord som “update”, “updates”, “updating” med mera som alla anses relevanta för resultatet av sökningen. Vidare har även de sökord som har vedertagna förkortningar slagits ihop då det har varit innebörden av sökordet som varit det viktiga snarare än om det förkortats eller inte. Ett exempel på detta är sökordet “("department of defense" OR dod)” där målet har varit att få med artiklar som berör det amerikanska försvarsdepartementet oavsett om det har förkortats eller inte.

Under pågående sökning har vi valt att inte på förhand låsa oss vid sökord utan varit öppna för att inkludera nya sökord som vi inte hade kännedom om vid sökningens start, något som lyfts fram som viktigt av Oates (2006) för att få fram relevanta söksträngar. Två exempel på detta är “("risk management framework" OR rmf)” och “diacap“ som är exempel på DoD:s riktlinjer för ackreditering som dök upp under sökningen gång. Vidare har vi under pågående sökning inte haft några krav på att söksträngar måste innehålla sökord från varje kategori utan vikt har lagts vi att skapa sökningar som ger ett överskådligt antal sökträffar.

Vad	Var	Hur
"accred* of system*"	"armed forces"	"best practice"
"security accred*"	"high security"	("risk management framework" OR rmf)
“risk management”	"information system*"	Diacap
accred*	"life cycle"	
ackreditering	"systems security engineering"	
maintenance	“security systems”	
patching	("department of defense" OR dod)	
re-accreditation	("ministry of defense" OR mod)	
updat*	("system development life cycle" OR sdlc)	
	försvarsmakten	
	military	

Tabell 1: Redovisning av sökord.

Vid varje sökning har artiklarna genomgått två stycken gallringar. I ett första skede har artiklarnas “abstract” lästs igenom och om den lyft fram något av intresse inom området har artikeln markerats som intressant. I nästa steg har artiklarna lästs igenom i sin helhet och de som fortfarande ansågs intressanta markerades som utvalda och lästes sedan igenom grundligt. Bedömningen om artikeln är intressant eller blir utvald har gjorts i förstahand utifrån om den tar upp fenomenet med hur bedömningar bör göras av uppdateringar, i andrahand utifrån om artikeln berör problematik gällande ackrediteringar och till sist om artikeln var behjälplig att tydliggöra de två tidigare beröringspunkterna. Utöver innehåll gjordes även en avgränsning att inte ha med artiklar äldre än 20 år.

Antalet unika sökträffar och antalet utvalda artiklar kan ge en bild av att det skett en mer snäv gallring än vad som påvisas ovan men så är inte fallet. De flesta artiklar gallrades bort då de berörde ackrediteringar av olika arbetssätt t.ex. inom vården som bedömdes ointressanta för denna studie. I realiteten fanns en mycket begränsad mängd artiklar som berörde ämnet.

Totalt gjordes 33 sökningar som gav mer än en träff och mindre än 100 träffar. Dessa gav totalt 450 artiklar, vilket ger ett genomsnitt på 13,64 artiklar per söksträng. I tabell 2 nedan redovisas det totala antalet artiklar samt det unika antalet efter att de dubbletter som dykt upp i sökningar med olika söksträngar tagits bort.

	Sökträffar	Intressanta	Utvalda
Totalt antal	450	58	32
Antal unika	317	22	9

Tabell 2: Redovisning av sökträffar.

3.2 Fallstudiebeskrivning

Syftet med denna studie är att undersöka om det går att underlätta arbetet med bedömningar om en system- och säkerhetsuppdatering påverkar befintlig ackreditering av ett IT-system som hanterar säkerhetsklassad information. För att undersöka detta har vi valt att genomföra en explorativ fallstudie av hur dessa bedömningar går till när dom görs på IT-system som hanteras av Försvarsmakten och en av deras leverantörer, Combitech. Oates (2006) menar att en explorativ fallstudie är en bra metod i de fall där det inte finns så mycket litteratur eller då litteratur saknas helt.

Valet av Försvarsmakten är gjort dels då den litteratur som finns på ämnet om ackrediteringar lyfter den stora mängd säkerhetsklassad information som hanteras inom just olika länders försvar. Detta tyder på att det är en bransch som kommit långt i sitt arbete kring problematiken i hur man hanterar bedömningar och har arbetat med det under en lång tid. Vidare har Försvarsmakten som främsta uppgift "*att ansvara för Sveriges militära försvar och att värna om Sverige*" (Försvarsmakten, u.å.). Detta gör att den IT-säkerhet man har i förlängningen är den IT-säkerhet som berör hela riket vilket gör det till en intressant myndighet att utgå ifrån. Problematiken finns hos andra myndigheter och om ett tydligt förhållningssätt kan klargöras skulle det eventuellt gå att applicera på andra myndigheter och företag som behöver göra samma typ av bedömningar.

Valet av Combitech som leverantör av IT-system till Försvarsmakten gjordes då de har ca 1000 konsulter som arbetar med försvarsrelaterade frågor vilket gör dom till Sveriges största IT-konsultbolag inom försvarsindustrin (Combitech, u.å.). Detta bör leda till en mycket god insyn i frågan utifrån en leverantörssynpunkt.

I fallet kan man kortfattat beskriva att Försvarsmakten har en roll som beställare och användare av IT- system som tas fram och underhålls av Combitech. Combitech har med andra ord en roll som systemutvecklare och leverantör, men även evaluerare. Behovet av en uppdatering kommer ofta från beställaren, men kan i vissa fall även komma från leverantören eller dennes leverantörer. I det fall en uppdatering initieras från en underleverantör ligger ansvaret fortfarande hos leverantören som har systemintegrationsansvar.

När en uppdatering väl sker behöver ett beslut tas utifall den påverkar den befintliga ackrediteringen. Om man bedömer att detta sker ska en om-ackrediteringen genomföras. Det formella beslutet tas av Försvarsmaktens CIO. För att kunna ta detta beslut görs bedömningar av uppdateringens påverkan av ackrediteringen av systemutvecklare och evaluerare under processens gång innan uppdateringen är klar. Bedömningar görs gentemot om dom krav som finns på IT-systemet har påverkats. Kraven återfinns i den ackreditering som är gjord och som utgår ifrån Försvarsmaktens dokument Krav på IT-säkerhetsförmågor hos IT-system v3.1 (KSF 3.1). Dessa krav kan i vissa fall vara svårtolkade och i andra fall kan det finnas olika krav som kan motsäga varandra. Efter att bedömningarna har gjorts blir de till beslutsunderlag för det beslut som ska tas av Försvarsmakten. Det är i denna bedömningsprocess som man idag upplever ett problem och det blir därför där denna studie kommer att ha sitt fokus.

Initialt i vår fallstudie så hölls möten med representanter från Försvarsmakten och Combitech. Under dessa möten hade vi möjlighet att ställa frågor gällande hur processen med uppdateringar på ackrediterade IT-system går till, om båda parter upplevde någon problematik och vad den i så fall var och vilka styrdokument och hjälpmedel som var aktuella. Detta gav oss en djupare förståelse för processen och gav oss de förutsättningar vi behövde för att genomföra vår fallstudie.

Fallstudien är uppdelad i två delar, vars metod beskrivs i de två efterföljande avsnitten, styrdokument och intervjuer. Granskningen av styrdokument har skett för att undersöka vad Försvarsmaktens egen dokumentation säger om processen och om problematiken går att identifiera här. Detta har gjorts dels för att ge en teoretisk förståelse för själva processen som vi anser nödvändig för att kunna genomföra tillfredställande intervjuer, men även för att undersöka om frågeställningen kan besvaras utifrån de dokument som finns idag. Intervjuerna har sedan gjorts för att få en mer verklighetsbaserad bild av processen och problematiken samt att förankra hur detta tolkas av de olika parterna.

3.3 Styrdokument

För att besvara den första underfrågan har vi valt att samla in och analysera de av Försvarsmakten uppsatta styrdokument med tillhörande stöddokument för att tydliggöra vad de uttryckligen säger gällande system- och säkerhetsuppdateringar och deras roll när det gäller om-ackrediteringar.

Underfråga 1:
"*Vad säger befintliga styrdokument om system- och säkerhetsuppdateringar på ett ackrediterat IT-system?*"

3.3.1 Insamling av styrdokument

För att göra en korrekt insamling av styrdokument har vi kontaktat Försvarsmakten som står som ansvariga för att ta fram, underhålla och tillhandahålla dessa dokument, och även Combitech som bedriver verksamhet med system- och säkerhetsuppdateringar som omfattas av ackrediteringar. Efter etablerad kontakt har ett initialt möte skett med, av de olika organisationerna, utpekad person som arbetar med och har god insyn i vilka styrdokument som berör det aktuella ämnet. I de fall dokumenten hänvisat till tidigare icke nämnda styrdokument eller riktlinjer har dessa inkluderats i analysen. Insamling av dokumenten har sedan skett från den myndighet som står som ägare av dokumentet.

Denna insamlingsmetod har valts för att i ett tidigt stadie smalna av insamlingen av styrdokument till att bara gälla dokument som används i praktiken och som erkänts som relevanta av de som arbetar med frågor rörande ackrediteringar och om-ackrediteringar. Valet av att kontakta både beställare/användare av IT- systemet (Försvarsmakten) och leverantör/utvecklare/evaluerare (Combitech) menar vi har uteslutit risken för att få en entydig bild och tar bort risken för att dokument som av den ena parten beskrivs som irrelevanta inte kommer med i studien. Valet att inkludera nya styrdokument och riktlinjer

under analysen av redan införskaffade har gjorts för att utesluta att relevanta dokument som berör ämnet inte har missats av båda tidigare nämnda parter.

3.3.2 Analys av styrdokument

Vi har genomfört vad Oates (2006) beskriver som en temaanalys med ett induktivt förhållningssätt i vår analys av styrdokument. Ett induktivt förhållningssätt användes för att inte låsa upp sig vid på förhand bestämda teman då det skulle kunna lett till att vi exkluderade segment som inte passade in. Relevansen i segmenten har bedömts utifrån hur de relaterar till bedömningar av uppdateringar under IT-systemets livscykel.

Var för sig gick vi igenom styrdokumenten och delade in dem i tre olika nyckelteman som Oates (2006) beskriver som det första steget i en temaanalys. I den första nyckelteman placerades segment utan relevans som lämnades omarkerat. I de andra två nyckeltemana placerades segment med en viss relevans och markerades med en färg och segment som ansågs ha klar relevans med en annan. Detta ledde sammanlagt till 143 segment fördelat över sju dokument. Efter detta gick vi igenom alla markerade segment gemensamt för att plocka ut kärnan i det som var relevant i segmentet. Dessa segment sammanställdes senare och de som var snarlika och berörde liknande saker slogs ihop för att skapa kategorier till exempel alla segment som tryckte på en fördelning av ansvar skapade kategorin Ansvarsfördelning. Sammanlagt resulterade detta i fem kategorier:

- Ansvarsfördelning
- Dokumentation
- Förtroende
- Planer och rutiner
- Systemgradering

Sammanlagt var 30 segment vid en närmare tolkning ej intressanta för forskningsfrågan och valdes således bort vilket resulterade i att 113 segment återstod för analys. Detta i sin tur ledde till att även ett utav dokumenten valdes bort då det inte längre bidrog med några segment av relevans. Utav de återstående segmenten var det även tolv stycken segment som var på ett övergripande plan och således inte placerades i någon kategori men behölls i dokumentationen då de ändå bedömdes ha betydelse för förståelse för forskningsfrågan på ett övergripande plan. Ett exempel genom citatet nedan från 13 kap. 6§ i Försvarsmaktens interna bestämmelser om IT-säkerhet (Försvarsmakten, 2017a).

“Ett it-system som är avsett för behandling av hemliga uppgifter och som har ackrediterats ska ackrediteras på nytt om det sker förändringar i eller kring systemet som kan påverka dess säkerhet.”

3.4 Intervjuer

För att besvara den andra och tredje underfrågan har vi valt att intervjua personer från både Försvarsmakten och Combitech. Detta för att få en syn hur samtliga tre berörda parter (beställare, leverantör och evaluerare) arbetar med bedömningar av uppdateringar.

Underfråga 2:
"Hur arbetar Försvarsmakten med att göra bedömningar om vilka förändringar som bidrar till att den befintliga ackrediteringen måste omprövas vid system- och säkerhetsuppdateringar på ett ackrediterat IT-system?"

Underfråga 3:
"Hur arbetar Combitech med att göra bedömningar om vilka förändringar som bidrar till att den befintliga ackrediteringen måste omprövas vid system- och säkerhetsuppdateringar på ett ackrediterat IT-system?"

3.4.1 Genomförande intervjuer

Intervjufrågor har konstruerats i syfte att ge informanterna möjlighet att ge sin bild av hur de anser att processen rörande uppdateringar av ackrediterade IT- system ska tolkas. För att ge möjlighet till mer utforskande intervjuer har vi valt att använda oss av vad Oates (2006) beskriver som semistrukturerade intervjuer. Med hjälp av detta tillvägagångssätt ges möjligheten att byta ordning på frågor och addera ytterligare frågor under intervjuns gång.

Valet av intervjupersoner gjordes utifrån målet att få olika infallsvinklar i frågan. Detta då styrdokumenten i praktiken tolkas av olika parter som berörs av dem. Försvarsmakten står som ägare av styrdokumenten och kan liknas med beställare eller användare av IT- systemet. Combitech har i denna process en roll som kan liknas vid leverantör eller utvecklare av systemet men även en roll som evaluerare. Båda parter har med andra ord ett behov av att göra tolkningar av de styrande dokumenten men ifrån olika perspektiv. Vi menar att vi med detta tillvägagångssätt skapar en bredare förståelse för hur tolkningar görs. Vi har valt att kalla våra intervjudeltagare för informanter då de delger information om faktiska förhållanden som berör fallstudien. Valet av informanter går även att härleda till Oates (2006) som beskriver det som en vanligt förekommande benämning på deltagare i fallstudier.

I urvalet av informanter hos Combitech har vi i samråd med dem valt ut två personer med olika roller. En informant som arbetar med kravställning och evaluering (fortsättningsvis benämnd som Evalueraren) samt en person som arbetar i en ledande roll med systemutveckling (fortsättningsvis benämnd som Leverantören). Dessa två informanter besitter mångårig erfarenhet inom området. I urvalet av informant hos Försvarsmakten blev vi efter en förfrågan till dem tilldelade en kontaktperson på Försvarsmaktens CIO avdelning. Personen i fråga arbetar med verksamhetsutveckling (fortsättningsvis benämnd som Beställaren) på CIO avdelningen som är den avdelning på Försvarsmakten som hanterar ackrediteringar.

Inför intervjun mailades de frågorna som skulle ställas till informanterna. Detta valde vi att göra för att ge informanterna en möjlighet att sätta sig in i frågorna och komma så förberedda som möjligt till intervjun. Då frågorna berör hur man arbetar med bedömning av uppdateringar och hur tolkning av styrdokument görs såg vi inget behov av spontana svar eller reaktioner på frågorna. Spontana svar och reaktioner är något som Oates (2006) lyfter fram att man går miste om när man skickar frågorna på förhand. Detta tillvägagångssätt gav informanterna en möjlighet att ge bättre och utförligare svar och skapade en bättre grund för dem att svara på följdfrågor från oss, vilket också var målet med intervjuerna.

Intervjuerna har skett i konferenssamtal i Teams efter önskemål från informanterna. Den huvudsakliga målsättningen var att träffa informanterna ansikte mot ansikte men på grund av det rådande läget med en pandemi under hösten/vintern 2020 valde vi att genomföra intervjuerna digitalt. Oates (2006) lyfter fördelar med att genomföra en personlig intervju som vi ville ta tillvara på. En av dessa är att vi ges möjlighet att tolka känslor och tonlägen på ett sätt som inte är möjligt vid till exempel mailkontakt. Vikten av att höra informanternas tonläge ser vi även som viktigt för att våra följdfrågor och diskussioner kring de givna svaren ska bli relevanta. Det ges även möjlighet att få svar på eventuella följdfrågor eller förtydliganden direkt om det skulle behövas.

Vidare har intervjuerna genomförts av en av uppsatsförfattarna som styrt intervjun och samtalet medan en person har haft en mer avvaktande roll, men har varit behjälplig att inflika med olika följdfrågor. Detta har bidragit till en större träffsäkerhet i det samtal som förts och i följdfrågorna samtidigt som det inte blivit allt för rörigt för informanten under intervjun. Detta då den som genomfört intervjun har kunnat fokusera på samtalet och förlita sig på att den andra personen plockar upp eventuella oklarheter för förtydligande eller ställer relevanta följdfrågor som missats. Intervjuerna pågick i snitt en timme vilket även var målsättningen innan.

Intervjuerna har vidare spelats in ljudmässigt för att kunna transkriberas och analyseras i efterhand. I transkriberingen har disfluenser som “öh” och “eh” utelämnats. Även upprepning av ord har utelämnats i de fall de förekommit av annan anledning än i förstärkande syfte. Detta har gjorts för att få en mer lättolkad transkribering och vi menar att de inte tillfört något om de stått med.

3.4.2 Analys av intervjuer

Vi har i vår analys av intervjuerna genomfört vad Oates (2006) beskriver som en temaanalys med ett induktivt förhållningssätt. Ett induktivt förhållningssätt användes för att det inte finns någon tidigare teori från litteraturen att analysera utifrån. De kategorier som framkom i analysen av styrdokumenten användes inte då intervjuerna till stor del handlade om vad som fattades i den befintliga styrdokumentationen. Att använda kategorierna som framkom av analysen av styrdokumenten skulle kunna lett till att vi misstolkade vad informanterna egentligen menade för att få det att passa in i kategorierna.

Efter att vi transkriberat intervjuerna så lästes de igenom flertalet gånger. Detta gjordes för att få en känsla och förståelse för intervjuernas helhet. Efter detta markerades det som vi

ansåg var intressant med vår forskningsfråga i åtanke. Detta gjordes var för sig av uppsatsförfattarna för att sedan diskuteras gemensamt. Detta angreppssätt valdes för att med ett så öppet sinne som möjligt enskilt välja ut allt som kunde tänkas vara av intresse för att sedan genom gemensam diskussion välja ut det som faktiskt var intressant. Genom att göra på det här sättet anser vi att vi minimerade risken att missa något relevant.

De intressanta delarna kopierades och klistrades in till ett nytt dokument, ett för varje informant, där de olika dokumentens text hade egen färgmarkering. Det kondenserade materialet lästes igenom flertalet gånger. Material som var återkommande i alla tre dokumenten klipptes ut och klistrades in i ett nytt dokument och bildade då en kategori. Ett tillfälligt beskrivande kategorinamn valdes för att få en bra struktur i dokumentet. Färgmarkeringarna från de olika informanterna behölls för att se vem som uttryckt vad. När allt material som var återkommande i de tre intervjuerna delats in i olika kategorier så summerades vad varje informant uttryckt i ett nytt dokument. De olika informanternas åsikter i varje kategori bildade ett eget stycke med sin ursprungliga färgmarkering. Det gjorde att det i varje kategori på ett överskådligt sätt gick att se vad varje informant uttryckte i frågan. Kategorinamnen byttes sedan ut för att bättre beskriva dess innehåll och kategorier som var "besläktade" bildade teman. De teman och kategorier som återfanns redovisas i tabell 3 nedan.

Under analysen sparades en kopia på varje dokument inför varje nytt analysmoment och en konsekvent färgkodning för de olika informanterna användes. Detta gjordes för de tillfällen då det uppstod frågor om vad som menades och det skulle då gå att läsa texten i sitt sammanhang.

Svagheter	**Krav**
Kompetens	Initiala kravformuleringens påverkan
Dyrt och tidskrävande med om-ackreditering	Omfattning
Bristande dialog	Frångå krav
	Kravuppfyllnad
Ansvarsfördelning	**Stöd**
Underlag och beslutsordning	Stöddokumentation
Gränsytor	Kommunikation

Tabell 3: Redovisning av teman och kategorier från intervjuer.

Utifrån de fyra teman (svagheter, krav, ansvarsfördelning och stöd) gjordes en jämförelse mellan de olika informanternas syn på ämnet. Denna jämförelse gjordes för att kunna lokalisera huruvida leverantör och beställare hade en samsyn, förståelse för den andres problem eller om olika syn på ämnet fanns.

3.5 Etiska överväganden

Flertalet etiska överväganden har gjorts under studiens gång. Majoriteten av dessa har berört hanteringen av personuppgifter och insamlat material som uppstått i samband med

intervjuerna. Samtliga informanter är anonyma till den grad att de enbart nämns med en beskrivning av sina arbetsuppgifter samt en bokstavsförkortning i transkriberingen. Vidare har informanterna fått tagit del av den nedskrivna transkriberingen för att ges möjlighet att gå igenom denna. Beslutet att låta informanterna vara anonyma har gjorts med åtanke på deras integritet medan valet att låta dem granska transkriberingen har skett för att säkerställa att ingenting som kan vara aktuellt för sekretess ska finnas med i transkriberingen. I det fall detta har uppstått har informationen korrigerats. Vidare har vi även valt att inte dela med oss av inspelningar från intervjuerna och beslutat att dessa ska raderas efter publicering av denna studie. Även detta har gjorts för att värna integriteten på informanterna då vi bedömer att anonymiteten skulle kunna röjas utifrån inspelningarna.

3.6 Metodkritik

Valet att använda sig av en fallstudie kan ifrågasättas. Enligt Oates (2006) är risken att resultatet av en fallstudie enbart kommer till nytta för den som fallstudien berör och med andra ord blir svår att generalisera mot andra. Vidare lyfter Oates kritik mot att det kan vara svårt att få tillgång till nödvändiga dokument och kontaktpersoner. Detta har underlättats av att fallstudien varit inriktad mot en myndighet som tillämpar offentlighetsprincipen och hanterar dokument som är att betrakta som allmän handling (Försvarsmakten 2011). Det har därför inte upplevts som någon större problematik att få tillgång till dokument.

Att samla in styrdokumenten utifrån vad de blivande informanterna bedömer som relevant kan anses problematiskt då det kan ge en ensidig bild. Vi vill dock hävda att när detta sker av flera av varandra oberoende personer minimeras den risken. Valet av ett induktivt förhållningssätt i analysen av styrdokumenten motiveras i metoden. Dock kan man ifrågasätta om det varit möjligt att göra på något annat vis överhuvudtaget med tanke på den tidigare litteratur som finns på ämnet.

Antalet intervjuer i studien uppgår till sammanlagt tre stycken. Detta kan anses vara ett för litet antal och det hade stärkt studien om fler intervjuer hade genomförts. Att bara en representant för respektive del, beställare, leverantör och evaluerare, har intervjuats skulle kunna leda till att en personlig bild av verkligheten förmedlats gällande just den rollen. Vi valde även att skicka intervjuernas innehåll i förväg för att ge informanterna möjlighet att se över och förbereda sig för att besvara våra frågor under intervjun. Detta skulle kunna medföra en problematik i att informanterna försöker att påverka sitt svar på olika sätt och att vi går miste om spontana tankar som dyker upp. Vidare valde vi även att som Oates (2006) rekommenderar skicka över transkriberingen av intervjuerna till informanterna. Detta skulle kunna leda till att informanterna ber om att få ändra sina svar i syfte att snygga till dem.

Analysen av intervjuerna skedde som tidigare nämnt med ett induktivt förhållningssätt. Alternativet hade varit att försöka ha fastställda teman att utgå ifrån. Dock ställer vi oss även här, precis som när det kommer till analysen av styrdokument, kritiska till om detta ens hade varit möjligt. Ett förhållningssätt hade kunnat varit att försöka utgå från de kategorier som framkom från analysen av styrdokument.

4 Analys och resultat

I detta avsnitt kommer vi att presentera data som framkommit från styrdokumenten och intervjuerna.

4.1 Analys och resultat av styrdokument

I tabell 4 nedan redovisas de styrdokument som lyftes fram i våra inledande samtal med Försvarsmakten och Combitech. Båda parterna betonade vikten av KSF 3.1 med tillhörande underbilagor som behjälpliga i processen. Extra vikt lades vid den underrubrik som hanterar assuranskraven. Utöver KSF 3.1 lyfte båda parter Fib 2017:11 och Fib 2017:8. Försvarsmakten lyfte även fram den designregel som Försvarets Materielverk (FMV) har för programvaror med underhåll.

Dokument	Fullständigt namn på dokument
18FMV3960-2:1	Designregel Programvaror med underhåll, utgåva 1.0
Fib 2017:11	Försvarsmakten interna bestämmelser om IT-verksamhet
Fib 2017:8	Försvarsmakten interna bestämmelser om IT-säkerhet
KSF 3.1	Krav på IT-säkerhetsförmågor hos IT-system v3.1 (Bilaga 1)
KSF 3.1 - ITSS	Krav på IT-säkerhetsförmågor hos IT-system v3.1 - IT-systemets säkerhetsspecifikation (Underbilaga 2)
KSF 3.1 - SF	Krav på IT-säkerhetsförmågor hos IT-system v3.1 - Funktionella säkerhetskrav (Underbilaga 3)
KSF 3.1 - SA	Krav på IT-säkerhetsförmågor hos IT-system v3.1 - Assuranskrav (Underbilaga 4)

Tabell 4: Redovisning av analyserade styrdokument.

I de olika styrdokumenten framkom sammanlagt 113 stycken olika segment som kan anses vara behjälpliga när det kommer till hanteringen av uppdateringar. Dessa kan placeras in i sex stycken olika kategorier som redovisas i tabell 5 nedan.

Kategorinamn	Antal	Beskrivning
Ansvarsfördelning	20	Segment som berör hur ansvarsfördelning bör ske mellan IT-systemets intressenter gällande uppdateringar
Dokumentation	38	Segment som berör olika typer av dokumentation av utförda uppdateringar
Förtroende	2	Segment som berör vikten av förtroende mellan beställare och leverantör
Planer och rutiner	36	Segment som berör olika typer av planer och rutiner som finns innan en uppdatering börjar utvecklas eller implementeras
Systemgradering	5	Segment som berör skillnader mellan olika typer av IT- system när det gäller uppdateringar
Övergripande	12	Segment som berör forskningsfrågan men på ett så övergripande plan att de inte kan sorteras in

Tabell 5: Redovisning av kategorier.

För att ge en övergripande bild av vilka dokument som bidrog med segment och vilken kategori dessa segment tillhör har en sammanställning av detta gjorts i tabell 6 nedan. Här framkommer det tydligt att det framförallt är i KSF 3.1 - assuranssäkerhetskrav som de flesta segment som berör uppdateringar finns, vilket även var det dokument som lyftes fram av både Försvarsmakten och Combitech som ett av de dokumenten av störst vikt. I tabellen nedan har även de 30 borttagna segmenten tagits med för att visa på att dokumentet KSF 3.1 - funktionella säkerhetskrav föll bort helt.

	Ansvarsfördelning	Borttagen	Dokumentation	Förtroende	Planer och rutiner	Systemgradering	Övergripande	Totalt
18FMV3960-2:1	0	0	0	0	2	2	2	6
Fib 2017:11	0	0	2	0	1	0	1	4
Fib 2017:8	0	0	0	0	0	1	1	2
KSF 3.1	0	3	0	2	2	2	2	11
KSF 3.1 - ITSS	0	1	5	0	0	0	0	6
KSF 3.1 - Assurans säkerhetskrav	20	21	31	0	31	0	6	109
KSF 3.1 - Funktionella säkerhetskrav	0	5	0	0	0	0	0	5
Totalt	20	30	38	2	36	5	12	143

Tabell 6: Förekomst av kategorier redovisat tillsammans med dokument.

Ansvarsfördelning - 20 av de 113 segmenten (18%) berörde hur ansvarsfördelning bör ske när det gäller olika uppgifter. Utav dessa segment är 17 stycken inriktade mot att tydliggöra systemutvecklarens ansvarsområden. Detta gäller framförallt när det kommer till beskrivningar av IT- systemet och dess olika delar. De går bland annat att utläsa att "*Systemutvecklaren ska tillhandahålla en Sammanställning av säkerhetskrav*" (Försvarsmakten, 2014b, s. 9) och att "*Systemutvecklaren ska upprätta en livscykelmodell som ska användas vid utveckling av systemet och systemutvecklarens förvaltning av systemet*" (Försvarsmakten, 2014b, s. 22).

Dokumentation - 38 av de 113 segmenten (34%) berörde något typ av dokumentation av vad som gjorts vid IT- systemets skapande eller vid uppdateringar och som ligger till grund för de bedömningar som ska göras i samband med uppdateringar. Bland annat ska dokumentation om IT- systemets gränsytor beskrivas samt IT- systemets arkitektur. Vidare lyfts även att dokumentation gällande kravtolkning ska finnas med i form av ett dokument vid namn Tolkning av säkerhetskrav. *"Syftet med Tolkning av säkerhetskrav är att beskriva en sammanställd kravbild för systemet och att genomföra och dokumentera kravtolkning utifrån de säkerhetskrav som identifierades i kapitlet Samanställning av säkerhetskrav. Kraven i KSF formuleras på en allmän nivå som resulterar i att varje system behöver precisera dessa krav med en tolkning av hur kravet appliceras på systemet" (*Försvarsmakten, 2014d, s. 9). Gemensamt för dessa segment är att de i sig inte ger något svar på hur uppdateringar ska dokumenteras utan snarare att de ska dokumenteras.

Förtroende - 2 av de 113 segmenten (2%) berörde på ett direkt sätt vikten av förtroende. Båda dessa segment riktar sig mot förtroende för IT- systemets ursprung med den skillnaden att det ena hänvisar till den miljö IT- systemet utvecklats i rent fysiskt och det andra hänvisar till den personal som IT- systemet utvecklats av.

Planer och rutiner - 36 av de 113 segmenten (32%) berörde olika typer av planer eller rutiner för hur man hanterar olika processer under ett IT- systems livscykel. Bland annat går att utläsa att "*Livscykelmodellen ska innehålla rutiner för att bedöma om en åtgärdad brist i en komponent är säkerhetsrelevant och ska införas och hur den ska accepteras*" (Försvarsmakten, 2014b, s. 38). Denna rutin bör vara av stor vikt när det kommer till hur bedömningar bör göras. Det lyfts vidare fram att "*Rutinerna ska innehålla detaljerade instruktioner för hantering av säkerhetsuppdateringar för samtlig mjukvara i systemet*" (Försvarsmakten, 2014b, s. 44). Detta är ett segment som även det ger utrymme för att skapa rutiner för hur man bör bedöma olika uppdateringars påverkan på befintlig ackreditering. Dock är det även här, precis som under dokumentation, snarare segment som klargör vad som ska dokumenteras i form av planer och rutiner snarare än faktiska rutiner på hur uppdateringar ska bedömas.

Systemgradering - 5 av de 113 segmenten (4%) förtydligar det faktum att det är skillnad på IT- system och IT- system och att detta bör finnas i åtanke när man gör bedömningar om ett IT- system ska om-ackrediteras. Ett av de tydligaste exemplen på detta återfinns i Försvarets materielverks designregel som säger att "*Olika programvaror påverkar i olika stor grad ett IT-systems möjligheter att kunna godkännas ur ett IT-säkerhetsperspektiv (ackrediteras) över tiden och det är därför viktigt att programvarornas livscykel hanteras korrekt*" (Försvarets materielverk, 2018).

Övergripande - 12 av de 113 segmenten (11%) har berört ämnet med uppdateringar på ett så pass övergripande plan att de inte kunnat gå att placera in i någon av tidigare nämnd kategorier. Ett exempel på detta är förtydligandet om att "Ä*ven förändringar av it-system och it-tjänster ska vara godkända. Ett beslut om godkännande av ett it-system eller en it-tjänst förutsätter att beslut om ackreditering har fattats eller att beslut om att ackreditering inte krävs*" (Försvarsmakten 2017b, s. 3) som förtydligar att även förändringar, alltså uppdateringar, ska godkännas utan att närmare gå in på hur eller varför.

4.2 Analys och resultat av intervjuer

Resultatet baseras på de tre intervjuer som genomfördes i december 2020 med en representant från Försvarsmakten fortsatt benämnd som Beställaren. Vidare med två representanter från Combitech fortsatt benämnda som Leverantören och Evalueraren. I resultatet framkom det 4 teman och 11 kategorier.

Svagheter	Krav
Kompetens	Initiala kravformuleringens påverkan
Dyrt och tidskrävande med om-ackreditering	Omfattning
Bristande dialog	Frångå krav
	Kravuppfyllnad
Ansvarsfördelning	**Stöd**
Underlag och beslutsordning	Stöddokumentation
Gränsytor	Kommunikation

Tabell 3: Redovisning av teman och kategorier från intervjuer.

4.2.1 Svagheter

Kompetens – Under intervjuerna framkom det att underhåll av IT-system inom Försvarsmakten, där ändringar ställs mot den kravbild som finns, handlar mycket om bedömningar. Att kunna genomföra korrekta bedömningar bygger på att man har kompetent personal med erfarenhet av att göra bedömningar och att man som Evalueraren utryckte det har en känsla för problematiken. Beställaren beskrev "*jag tror att det är väldigt svårt att kunna, om man inte har hållit på med detta tidigare bara egentligen läsa sig till detta. Det tror inte jag kommer funka*."

På frågan om Leverantören upplever problem med bedömningar gällande om en ändring behöver om-ackrediteras eller ej svara hen att det inte upplevt så mycket problem och fortsätter "*Och jag vet inte vad det beror på om vi bara har haft tur att ha bra projektmedarbetare som kan dra en bra slutsats liksom eller.*"

Bristande dialog - Under intervjuerna framkom det att ändringar är av en väldigt skiftande art och avsaknaden av fungerande processtöd gör det svårt att veta vad Försvarsmakten anser om de tolkningar leverantören gjort. Leverantören utrycker att de försöker motivera varför de anser att en ändring ryms inom befintlig ackreditering. Beställaren menar att dialogen ofta kommer sent, när man är i driftsättning vilket fördröjer tiden och därmed höjer risken.

Dyrt och tidskrävande med om-ackreditering - På frågan varför en om-ackreditering vill undvikas svarade alla informanterna att det handlar om att spara tid och pengar då det är väldigt tidskrävande att gå in i en ny ackreditering. Beställaren svarade dock först att en om-ackreditering ska undvikas för att det i många fall betyder att vi har påverkat säkerheten negativt. Vidare sade hen "*Eftersom vi har ju satt lägsta nivån genom ackrediteringsbeslutet, och höjer vi säkerheten så gör vi ingen om-ackreditering på det.*"

4.2.2 Krav

Initiala kravformuleringens påverkan - Samtliga informanter betonade vikten av att tydliga krav skrivs i den initiala kravspecifikationen. En av informanterna utryckte att "*ju bättre arbete man gjort initialt ju lättare blir det egentligen att hantera uppdateringar också*." Leverantören menar också att man inte ska bryta ner kraven allt för mycket långt ner i kedjan utan att om man håller kraven "*på en relativt hög nivå så att, ja man har lite flexibilitet där under om man säger.*"

Omfattning – Kravspecifikationen som krävs för att ett IT- system ska bli ackrediterat är väldigt omfattande vilket samtliga informanter tydligt lyfte fram under intervjuerna t.ex. sade en av informanterna "*det är ju inte ovanligt att det är hyllmeter med dokumentation*." En annan av informanterna uttryckte "*så blir det sjukt många krav att realisera och ha koll på.*" Evalueraren uttryckte att trots sin omfattning så är kraven nödvändiga.

Beställaren lyfte också problematiken kring "*att hitta ett bra sätt att faktiskt fokusera på det som är dom viktigaste bitarna. Alltså dom mest kritiska säkerhetsfunktionerna och beskriva dom väldigt djup och i detalj.*" Vidare menade hen att det ibland läggs för stort fokus på att uppfylla enskilda krav istället för se till vilken skyddsförmåga som ska uppnås. Att man till exempel stirrar sig blind på hur man uppfyller ett enskilt assuranskrav. Leverantören uttryckte att det kanske inte är de tekniska delarna som är den största utmaningen utan att det många gånger är assuranskraven - "*man kravställer ju i princip en organisation för att sköta allt det här*."

Frångå krav - När kravtolkningen görs inför den initiala ackrediteringen så kan krav frångås om väldigt bra motiv finns och det går att uppvisa att samma skydd uppfylls på annat sätt. Detta är något som samtliga informanter uttryckte i sina intervjuer. Ett exempel som lyftes i två av intervjuerna var kravet på att inloggningskontroll i vissa fall är ett mycket bra krav men att det i t.ex. ett stridsflygplan kanske inte är så lämpligt om piloten blir utloggad ur IT-systemet, som en informant uttryckte "*det kan bli stört jobbigt liksom.*" Beställaren klargjorde att när ett IT- systemet väl är ackrediterat så är kraven bindande, "*Ja för då har man ju satt den här, alltså den lägsta nivån.*" och frångår man ett krav efter det så är risken stor att man hamnar under den lägst godkända nivån.

Evalueraren lyfte att det kan finnas olika kravbehov på olika IT- system och att KSF 3.1 är hårt knuten till sekretess. Medan insatsledningsssytem i vissa lägen kan behöva titta mer på tillgänglighet och riktighet. Att det helt enkelt kan vara viktigare att systemet fungerar ur ett driftperspektiv än att bibehålla sekretessen fullt ut. Vidare menade Evalueraren att avvägningen är svår men kravställningen påverkas av hur man ser på aspekterna kring sekretess kontra tillgänglighet och riktighet. Vill man frångå ett krav idag så måste någon fatta det beslutet och redovisa att det skyddet uppnås på annat sätt. Det borde finnas andra aspekter hur man hanterar skillnader eller synsätt på. "*Det hade varit bra med en modeleringsmöjlighet beroende på det tänkta systemets driftsprofiler".*

Kravuppfyllnad - Samtliga informanter betonade vikten av att testa ändringar mot den ursprungliga kravbilden. Testet visar på förändringens påverkan och ligger till grund för det underlag man skapar åt Försvarsmakten gällande om en om-ackreditering behövs eller ej.

Leverantören menade att de inte haft några större bekymmer med att bedöma sina ändringar och att det beror på att de testar allt väldigt noga. Vidare menade hen att "*jag tror att om man verkligen kan definiera vilka krav som respektive förändring påverkar och att man verkligen testar systemet utifrån dom kraven. Så kan man nog göra en ganska bra bedömning.*"

4.2.3 Ansvarsfördelning

Underlag och beslutsordning - Under intervjuerna framkom det från samtliga informanter att det är leverantören som skapar underlag och Försvarsmakten som fattar besluten gällande alla ändringar. Det framkom även att bedömningen sker i flera steg, först görs det en bedömning inom projektet av leverantören. Sedan skapar leverantören ett underlag som evauleraren granskar och lämnar sedan ett utlåtande till Försvarsmakten. En informant utryckte "*Så att då blir det egentligen tre parter. Dels gör ju leverantörerna en bedömning, sen gör ju den här Evalueraren en bedömning sen gör ju den som granskar en bedömning också*."

Beställaren menar när det gäller säkerhetsuppdateringar att "*det finns ju ett syfte med att göra det snabbt.*" Leverantören uttryckte under intervjun ett missnöje över att det ofta tar väldigt lång tid att få ändringar godkända, även små ändringar som inte är aktuella för en om-ackreditering. Vidare lyfte hen att "*det ligger mycket liksom på försvarsmaktssidan att deras granskningstider är väldigt långa*."

Gränsytor - Inom Försvarsmakten har man i vissa fall stora IT- system som består av flera delsystem där Försvarsmakten i vissa fall är systemintergratörer med helhetsansvaret medan det i andra fall är leverantören som är det. Samtliga informanter menade att dessa IT- system är kritiska i att man i varje delsystem måste ta hänsyn till de gränsytor man har mot andra delsystem. Leverantören sade att det i hans projekt inte är ett stort problem men menade att det mycket väl kan vara det för andra.

Både Beställaren och Evalueraren menade att det är väldigt viktigt att vara noga med beskrivningen på de förändringar som görs mot gränsytorna då det handlar om komplexa IT-system som utvecklas över tid. Beställaren tryckte på att det blir riskfyllt om det görs många ändringar och man blir efter i dokumentationen och att "*Det är ju ett mått på att egentligen risken ökar med tiden.*"

4.2.4 Stöd

Stöddokumentation - I intervjuerna framkom det att visst metodstöd i form av en Informationssäkerhetsdeklaration (ISD) finns men att det är väldigt omfattande och generellt skrivet och inget som används i någon större utsträckning. Evalueraren menade att det dokumenteras någon form av konsekvensanalys som skulle kunna generaliseras och användas som "lessons learned" på en högre nivå.

Samtliga informanter såg behovet av ett processtöd för hur kraven ska tolkas vid ändringar och att ett sådant stöd måste vara systemspecifikt. Leverantören sade i intervjun "*ett förslag vore kanske att låta Försvarsmakten, när dom ändå gör en säkerhetsmålsättning för systemet, att också inkludera nån typ av bedömningshjälp.*" och syftade på bedömningshjälp vid uppdateringar. Vidare sa hen "*får man nån typ av i alla fall bedömningsmatris kanske så. Vore det väldigt, ja det vore önskvärt skulle jag säga.*". Evalueraren utryckte "*Ja det hade varit önskvärt. Ja, nått sånt stöd. Så att man i samband med ackrediteringen redan där tänker klargöra hur vi ska upprätthåll säkerheten över tiden.*"

Beställaren lyfte utöver processtöd även vikten av att utbilda leverantören på plats i hur de ska tänka kopplat till kravbilden, "j*ag tror att båda dom här bitarna är jätteviktiga. Och jag tror att speciellt utbildning eftersom man kan ställa frågor också.*" Vidare lyfter hen även ett metodstöd i systematiskt arbete inom informationssäkerhetsfrågan som bygger på ISO:27001 och ges ut av MSB på informationsäkert.se

Kommunikation – Under intervjun med Beställaren framkom det att Försvarsmaktens CIO har ett forum där de lyfter större eller kritiska ändringar. I forumet deltar olika experter inom som skapar underlag för beslut. Denna process inom Försvarsmakten fungerar bra men är inget som leverantören normalt är en del av. Vidare lyfter hen "*att det viktiga där är den här dialogen man behöver få till. För en osäkerhet jag tror att det finns det är hur känner dom sig trygga i att dom åtgärder dom vidtar bedöms som tillräckliga från vår sida.*" Hen menar att en fungerande dialog kan minska ovissheten kring vad som förväntas och på det viset även korta ner tiderna för ändringar.

Samtliga informanter tror att ett forum dit leverantörer enkelt vänder sig för att diskutera olika problem med Försvarsmaktens experter och med kollegor ute i landet kan vara till hjälp. Beställaren menade att "*det är en intressant tanke men det är inte så vi har hanterat det just nu.*" Evalueraren sade att "*Det hade varit bra tror jag. Åtminstone ur ett systemutvecklingsperspektiv"* och fortsätter med att det nog hade underlättat mycket för systemutvecklaren och hjälpt denna att undvika att gå på minor och hamna i fallgropar om man enkelt kunnat diskutera produkter och lösningar som ej är önskvärda eller att föredra.

De påtalades dock att vissa frågor kan vara av känslig natur och varför ett forum inte alltid passar. Vid sådana tillfällen menade Beställaren att man har något som heter Teknik och Vidmakthållandekontor (TVK) som är de som har ansvar för IT- systemen under dess livscykel. De ska både sköta samordning av liknande uppdateringar på olika IT- system men också sitta på expertiskunskaper och kunna vara behjälpliga. Det är också dem som har kontakten med leverantören. Evalueraren sade att hen samverkar med TVK men saknar ett stöd i evalueringsarbetet. Vidare sa hen att det genom åren funnits olika former av stöd bland annat kataloger med produkter, hård och mjukvara som på något vis varit att föredra inom Försvarsmakten. Det har försvunnit de sista åren och hade varit önskvärt att få tillbaka. Leverantören sa sig inte sprungit på TVK i sitt arbete men ser att en lättillgänglig samordnande funktion inom Försvarsmakten skulle vara bra. Att kunna vända sig dit utan att det är någon hierarkisk ordning som fördröjer och försvårar kontakten, menar hen skulle vara intressant.

5 Diskussion

I detta avsnitt förs en diskussion om den analys som har gjorts och det resultat som framkommit från styrdokument och intervjuer. Avslutningsvis för en sammanfattande diskussion.

5.1 Styrdokumenten

Syftet med analysen av styrdokumenten var att besvara frågan "*Vad säger befintliga styrdokument om system- och säkerhetsuppdateringar på ett ackrediterat IT-system?*"

Stort fokus läggs vid dokumentation om vad som har gjorts tidigare men även dokumentation i form av planer och rutiner. Sammanlagt 65% av segmenten från analysen placeras in i dessa två kategorier och vikten av en god dokumentation är något som även Capitan (2008) talar om i tidigare litteratur. Det framkommer dock inte exakt hur dessa planer och rutiner samt dokumentation ska utformas och om de kan vara behjälpliga när det kommer till hur man ska gå tillväga med bedömningar av uppdateringar. För att ta reda på detta lyfte vi frågan under intervjun för att se hur man arbetade med detta idag. Det framkom då att dessa typer av dokument ger en viss grund till hur man ska arbeta med uppdateringar men de lämna en del att önska.

Utöver olika typer av dokumentation läggs även stor vikt vid ansvarsfördelning i styrdokumenten. Denna ansvarsfördelning tar sig form i att beskriva vem som ska göra vad när det kommer till den tidigare nämnda dokumentationen. Detta i sig ger inte så mycket information om själva bedömningarna av uppdateringarna då detta inte berörs direkt.

Det två kategorier som förekom minst under analysen var Systemgradering och Förtroende. De segment som på ett direkt sätt berörde förtroende lyfte vikten av att Försvarsmakten har förtroende för de som utvecklar IT- systemet och blir således inte relevanta för att besvara frågan. Dock lyfter de en intressant aspekt om att vikt läggs vid just förtroende för leverantör, något som även gjorts av Dawson m.fl. (2010). Det skulle även kunna gå att argumentera för att de segment som framkommit från det stöddokument som berör assuranskrav går att kategorisera i förtroende då de finns till för att kravställa leverantörers arbetssätt och processer. Dock har vi ansett att de kunnat kopplats tydligare till andra kategorier men värt att notera är att förtroende är en viktig aspekt.

De segment som berörde Systemgradering pekade på att man i bedömningarna om ett IT-system måste om-ackrediteras måste ta hänsyn till det specifika IT- systemet och hur det är utformat, hur det används m.m. Detta i sig ger ingen nytta åt att förstå hur uppdateringar ska hanteras.

I inledningen påpekade vi att Loughry (2013) menar att det är signifikanta uppdateringar som borde leda till om-ackreditering. Vad som är signifikanta uppdateringar nämns inte närmare. Denna problematik med vaga beskrivningar återfinns även i styrdokumenten, närmare bestämt i Försvarsmaktens interna bestämelser som säger att "*Ett it-system som är*

avsett för behandling av hemliga uppgifter och som har ackrediterats ska ackrediteras på nytt om det sker förändringar i eller kring systemet som kan påverka dess säkerhet" (FIB 2017:8). Sammanfattningsvis kan sägas att det inte ges någon klar bild av hanteringen av uppdateringar. Det som framkommer är att styrdokumenten har ett fokus på vad som ska göras och utav vem, medan de lämnar frågan om hur det ska göras obesvarad när det kommer till bedömningar om en uppdatering påverkar befintliga ackreditering eller ej vilket exemplifieras i citatet ovan.

5.2 Intervjuerna

Syftet med analysen av intervjuerna var att besvara frågorna *"Hur arbetar Försvarsmakten med att göra bedömningar om vilka förändringar som bidrar till att den befintliga ackrediteringen måste omprövas vid system- och säkerhetsuppdateringar på ett ackrediterat IT-system?" och "Hur arbetar Combitech med att göra bedömningar om vilka förändringar som bidrar till att den befintliga ackrediteringen måste omprövas vid system- och säkerhetsuppdateringar på ett ackrediterat IT-system?"* Dessa arbetssätt ställs här mot varandra för att se vad man har samsyn i och vad man ser olika på.

Resultatet visar på en samsyn hos informanterna i vikten av att skriva tydliga krav i den initiala kravspecifikationen. Buszta (2008) lyfter också vikten av att kraven ska vara tydliga och menar på att om de inte är tydliga så finns det en risk för att olika personer gör olika bedömningar. Detta skulle i studiens fall kunna leda till att leverantören gör en bedömning av att en om-ackreditering inte behövs medans Försvarsmakten gör en annan bedömning. Vidare lyfter informanterna att hur dessa krav är skrivna påverkar hur svårt eller lätt det är att visa att en ändring ryms inom ramen för det kravet. Även om processen kring bedömningar på sina håll är problematiskt så fungerar den idag. Det gör den mycket på grund av att man har kompetent och erfaren personal som testar sina ändringar mycket och därmed kan lämna ifrån sig bra underlag för beslut. Skulle denna kompetens gå förlorad finns därför en risk för att bedömningarna blir svårare att göra vilket i sin tur medför att risken för att en om-ackreditering behöver göras ökar.

Resultatet visar att aktuella styrdokumenten generar en stor mängd med krav som man sedan måste förhålla sig till under IT- systemets livscykel. Tysenn (2006) lyfter som tidigare nämnt vikten av att ha ett säkerhetstänk genom ett IT-systems hela livscykel och det framgår från informanterna att det finns en förståelse för att det behöver vara många krav för att hålla en hög säkerhet. Leverantören lyfter att det är assuranskraven, där man i princip kravställer en hel organisation, som är svårast att hantera. Beställaren menade att det ibland läggs för stort fokus på att uppfylla enskilda krav istället för se till vilken skyddsförmåga som ska uppnås. När en kravspecifikation initialt upprättas så är det möjligt, om det finns särskilda skäl till det, att frångå krav. Men man behöver då visa på att man uppnår samma skyddsvärde på annat sätt. Evalueraren lyfter att det finns olika kravbehov för olika IT-system och de aktuella styrdokumenten har ett stort sekretessfokus vilket kan vara problematiskt när man skriver en kravspecifikation där fokus behöver ligga på tillgänglighet och riktighet. Det gör att man måste frångå en del krav och när man gör det måste det rättfärdigas och någon måste besluta om det. En önskan om ett mer modellerbart styrdokument gällande kravspecifikationen lyftes. Det aktuella styrdokument som reglerar

kravspecifikationen gäller för alla IT-system inom Försvarsmakten och att göra det mer modellerbart skulle innebära två fördelar. Det skulle som Evalueraren uttryckte det ge en mer specifik kravspecifikation där man slipper frångå krav och det arbete som det innebär. Det skulle förmodligen också generera något färre krav då man inte skulle behöva täcka upp för alla typer av system i samma kravspecifikation.

Utifrån resultatet kan vi se att det finns en tydlig gränsdragning gällande att skapa underlag och fatta beslut. Det är Försvarsmakten som fattar alla beslut medan det oftast är leverantören som skapar underlag för hur deras ändringar påverkar aktuell ackreditering. Vissa ändringar t.ex. säkerhetspatchar kan beslutas långt ner i kedjan då Försvarsmakten ser ett behov av att kunna göra ändringar snabbt. Leverantörsidan lyfter att alla ändringar de vill göra tar väldigt lång tid att få godkända av Försvarsmakten. Det är intressant att Försvarsmakten trycker på behovet av att kunna utföra snabba ändringar medan Leverantören lyfter väldigt långa granskningstider på även mindre ändringar som önskas genomföras.

Resultatet visar även att gränsytor mellan IT- system är en kritisk punkt där det är väldigt viktigt att man redogör och dokumenterar de ändringar man gör på eller emot gränsytorna. Det är den som är systemintegratör som ansvarar för att detta görs. Risken med en bristande dokumentation på de ändringar som gjorts i gränsytorna är att man tappar spårbarheten och att framtida ändringar inte ställs mot aktuella förutsättningar. Gränsytorna är lätta att missa för oerfaren personal och är ett mått på att i stora IT- system med många gränsytor ökar risken med tiden. Återigen ser vi här att kompetens blir en viktig faktor när det kommer till de bedömningar som ska göras.

Capitan (2008) lyfter som tidigare nämt vikten av fungerande processer när det kommer till hur en ackrediteringsprocess ska genomföras. I studiens fall så finns det processer för ackrediteringsprocessen och det lyfts inte som något problem med hur en sådan process ska genomföras. Det framkommer ett önskemål från leverantörsidan om ett processtöd i hur aktuella krav ska bedömas. Även Försvarsmakten kunde se fördelar med ett sådant stöd. Ett bedömnings stöd i form av stöddokument måste skrivas specifikt för varje IT- system då varje kravspecifikation är unik. Ett sådant stöd skulle behöva innehålla någon form av guidning om vad Försvarsmakten anser tillåtet. Det skulle kunna vara en checklista så att man tydligt ser att man håller sig inom ramen för vad som är godkänt eller liknande. Det finns ett behov av att utveckla ackrediteringsprocessen för att ge stöd för hur man ska hantera frågor kring uppdateringar under den fas i IT- systemets livscykel då det är i drift.

Försvarsmakten ser ett behov i att på plats utbilda leverantörer i hur de ska tolka krav. Resultatet visar även att kommunikation är väldigt viktigt för att underlätta arbetet med att bedöma ändringar. Man ser fördelar i att det skulle finnas ett forum där leverantörer enkelt kan lyfta frågor både med andra leverantörer och med experter på Försvarsmakten. Många IT- system har komponenter av liknande art och därför ställs olika IT- system inför samma problem till exempel hur en Windows-uppdatering påverkar ens system. Som det ser ut idag behöver alla funderingar gå genom den inom Försvarsmakten systemansvarige i projektet vilket kan vara tidskrävande och omständligt. För att tillmötesgå dessa behov och korta ner kommunikationsvägarna behöver Försvarsmakten tillhandahålla ett forum för leverantörer

förslagsvis webbaserat. Vissa frågor man ställs inför kan vara av en känsligare art och skulle därför inte passar att ställa i ett öppet forum och här finns en önskan om att enklare kunna lyfta dessa frågor med experter på Försvarsmakten.

5.3 Sammanfattande diskussion

För att knyta an vår diskussion till vår huvudfråga "*Vilka faktorer är viktiga vid en bedömning av om en ackreditering måste omprövas vid system- och säkerhetsuppdateringar på ett ackrediterat IT- system som hanterar säkerhetsklassad information?*" kommer vi här att presentera en sammanfattande diskussion.

Utifrån det samlade resultatet framgår det att underhållet av ett IT- system under dess livscykel bygger på bedömningar och för att lyckas göra korrekta bedömningar krävs det att man har kompetent och erfaren personal något som även styrks i teorin av Dawson m.fl (2010). I studiens fall framgår det vid flera tillfällen att det inte går att läsa sig till hur bedömningar ska göras och bristen på ett processtöd för dessa bedömningar gör det näst intill omöjligt att klara detta utan erfarenhet. Långa kommunikationsvägar som ofta kommer sent i processen bidrar också till svårigheter att veta om man gjort rätt vilket i sin tur leder till otydligheter som i sin tur leder till en långsammare process och därmed en ökad risk.

Det framgår att kompetens som förvärvas genom erfarenhet är det som krävs för att kunna göra så bra bedömningar som möjligt. Trots innehav av kompetens råder dock en ovisshet kring om dessa bedömningar kommer att bedömas på samma sätt senare i processen. Det blir därför viktigt att den som gör bedömningen har tillgång till stöd oavsett kompetens även om den ökade kompetensen leder till ett minskat behov av stöd. Under analysen av intervjuerna framkom att det efterfrågade stödet går att dela in i två kategorier. Dels förenklade kommunikationsvägar och dels systemspecifikt processtöd för hur bedömningar ska göras. Detta stöd blir viktigt för att ta tillvara på kompetens på ett tillfredställande sätt och distribuera kompetensen till andra personer som ska göra bedömningar av IT- system. Görs inte detta, och kompetensen hos de som gör bedömningarna går förlorad, finns det en övervägande risk för att felaktiga bedömningar görs som leder till att om-ackrediteringar behöver genomföras, alternativt att en överansträngning görs för att undvika en om-ackreditering. Båda dessa scenarion skulle leda till att ökat behov av resurser i form av tid och pengar samt eventuellt äventyra säkerheten i IT-systemet.

Försvarsmakten bör vidareutveckla det resonemang som förs kring något typ av forum för att lyfta frågor som berör bedömningar av uppdateringar. Det finns idag olika typer av kommunikationsvägar men de upplevs som långsamma och krångliga. Om Försvarsmakten lyckas förenkla dessa skulle det kunna bidra till att kompetensen för hur bedömningarna ska göras förbättras. Vidare bör Försvarsmakten även försöka utreda hur man skulle kunna utforma systemspecifika stöddokument för att hjälpa till i processen med bedömningar av uppdateringar.

6 Slutsats och bidrag

Det är två faktorer som spelar en extra viktig roll när det kommer till att göra bedömningar om vilka uppdateringar som påverkar befintlig ackreditering. Det första är att det finns kompetens baserat på erfarenhet hos den person eller grupp som ska göra bedömningarna. Det andra är att det finns ett tydligt stöd i processerna för att göra dessa bedömningar. Ett sådant stöd behöver dels bestå av utökade kommunikationsvägar och dels bestå av ett systemspecifikt processtöd för system- och säkerhetsuppdateringar. För att kunna applicera systemspecifika processtöd i olika myndigheter behövs ett ramverk eller en standard som visar på hur detta processtöd ska tas fram. I studien lyftes att det finns olika generella standarder som inte analyserats i denna studie, ett exempel på detta är ISO:27001.

Denna studie har bidragit med att identifiera de två viktigaste faktorerna när det kommer till att göra bedömningar om vilka uppdateringar som påverkar befintlig ackreditering inom myndigheter som följer säkerhetsskyddsförordningen. Det vore intressant för vidare forskning att utreda om de faktorer som nämns i denna slutsats skiljer sig från vilka faktorer som är viktiga i en privat sektor. Vidare vore det intressant att analysera för ämnet intressanta industristandarder mot det behov av processtöd som identifieras i denna studie. Detta för att undersöka om ett ramverk redan finns och om det inte gör det så bör ett sådant ramverk tas fram.

7 Källförteckning

Buszta, K. (2008). Challenges in Certification and Accreditation. *IT professional. 10*(3), pp.56–59. DOI: 10.1109/MITP.2008.42

Capitan, B. (2008). Assuring Mission Success: Systems Security Engineering and Assurance MILCOM 2008. *MILCOM 2008 - 2008 IEEE Military Communications Conference*, pp.599–605. DOI: 10.1109/MILCOM.2008.4753123

Combitech AB (u.å.). *Försvar*. Hämtad 2020-12-18 från https://combitech.se/branscher/forsvar/

Dawson, M., Burrell, D. N., Rahim, E., & Brewster, S. (2010). Integrating software assurance into the software development life cycle (SDLC). *Journal of Information Systems Technology and Planning, 3*(6), pp.49-53.

Fredriksson, S. (2011). *Auktorisation och ackreditering inom Försvarsmakten : En studie i nyttan av en standardiserad process för att hantera informationssäkerhet* (Examensarbete). Uppsala: Institutionen för informationsteknologi, Uppsala universitet. http://urn.kb.se/resolve?urn=urn:nbn:se:uu:diva-153267

Försvarets materielverk. (2018). *Designregel Programvaror med underhåll, utgåva 1.0*. Hämtad från Försvarsmaktens materielverk: http://isd.fmv.se/Documents/Designregel%20Underhållna%20programvaror%20utgåva%201.0.0.pdf

Försvarsmakten. (2011). *Handbok för Försvarsmaktens säkerhetstjänst, Sekretessbedömning Del A.* Hämtad från Försvarsmakten: https://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/handbocker/handbok-sak-sekrbed-del-a.pdf

Försvarsmakten. (2013). *Handbok Säkerhetstjänst Informationssäkerhet.* Hämtad från Försvarsmakten: https://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/handbocker/handbok-sak-infosak-andring-2.pdf

Försvarsmakten. (2014a). *Krav på IT-säkerhetsförmågor hos IT-system v3.1*. Hämtad från Försvarsmakten: http://isd.fmv.se/Documents/krav-pa-godkanda-sakerhetsfunktioner-version-3-1.pdf

Försvarsmakten. (2014b). *Krav på IT-säkerhetsförmågor hos IT-system v3.1 - Assuranskrav (Underbilaga 4).* Hämtad från Försvarsmakten: http://isd.fmv.se/Documents/krav-pa-godkanda-sakerhetsfunktioner-version-3-1.pdf

Försvarsmakten. (2014c). *Krav på IT-säkerhetsförmågor hos IT-system v3.1 - Funktionella säkerhetskrav (Underbilaga 3).* Hämtad från Försvarsmakten: http://isd.fmv.se/Documents/krav-pa-godkanda-sakerhetsfunktioner-version-3-1.pdf

Försvarsmakten. (2014d). *Krav på IT-säkerhetsförmågor hos IT-system v3.1 - IT-systemets säkerhetsspecifikation (Underbilaga 2)*. Hämtad från Försvarsmakten: http://isd.fmv.se/Documents/krav-pa-godkanda-sakerhetsfunktioner-version-3-1.pdf

Försvarsmakten. (2014e). *Krav på IT-säkerhetsförmågor hos IT-system v3.1 - Ordlista och begrepp (Underbilaga 1).* Hämtad från Försvarsmakten: http://isd.fmv.se/Documents/krav-pa-godkanda-sakerhetsfunktioner-version-3-1.pdf

Försvarsmakten (2017a). *Försvarsmaktens interna bestämmelser om it-säkerhet.* Stockholm: Försvarsmakten. Hämtad från Försvarsmakten: https://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/lagrum/gallande-fib/fib-2017.8--it-sakerhet.pdf

Försvarsmakten (2017b). *Försvarsmaktens interna bestämmelser om it-verksamhet.* Stockholm: Försvarsmakten. Hämtad från Försvarsmakten: https://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/lagrum/gallande-fib/fib-2017.11-it-verksamhet.pdf

Försvarsmakten (u.å.). *Vår verksamhet*. Hämtad 2020-12-20 från https://www.forsvarsmakten.se/sv/var-verksamhet/

Loughry, J. (2013). A Model of Certifier and Accreditor Risk Calculation for Multi-Level Systems. *Technologies for Homeland Security (HST), 2013 IEEE International Conference on,* pp.224-229. DOI: 10.1109/THS.2013.6699004

Nemr, G. (2008). Obtaining Information Assurance (IA) accreditation for systems initially deployed without ia considerations. *MILCOM 2008 - 2008 IEEE Military Communications Conference*, pp.1–7. DOI: 10.1109/MILCOM.2008.4753217

Oates, B. J. (2006). *Reseaching Information Systems and Computing*. London : SAGE publications Ltd

Salmans, M.H.R. (2015). From DIACAP to RMF: A clear path to a new framework. *CrossTalk, 28*(5), pp.20–25.

SFS 1996:633. *Säkerhetsskyddsförordning*. Stockholm: Justitiedepartementet

Shilling, A. (2016). Integrating cybersecurity into NAVAIR OTPS acquisition. *IEEE AUTOTESTCON 2016 : proceedings : Anaheim, California, USA, september 12-15, 2016 /*, 2016-October, pp.1–5. DOI: 10.1109/AUTEST.2016.7589632

Svenska Institutet för Standarder. (u.å). *Detta är ISO 27000 för cyber- och informationssäkerhet*. Hämtad 2021-01-07 från https://www.sis.se/iso27000/dettariso27000/

Tysenn, J. (2006). Certification & Accreditation - The role of security engineering in the Systems Development Life Cycle. *16th Annual International Symposium of the International*

Council on Systems Engineering, INCOSE 2006, 2, pp.1435–1450. DOI: 10.1002/j.2334-5837.2006.tb02824.x

Bilagor

Bilaga 1 – Intervjuunderlag

Bakgrund

Vi har förstått att alla IT-system och IT-tjänster ska vara godkända och de allra flesta även ackrediterade innan de får användas inom Försvarsmakten. Förenklat kan man säga att om ett system är ackrediterat så är det noga kontrollerat att det uppfyller alla de krav som man ställt på systemet i fråga. Dessa krav utgår ifrån styrdokumentet KSF 3.1 även om det kan finnas ytterligare krav.

När man sedan ska göra uppdateringar av systemen, både säkerhetsuppdateringar och funktionella sådana, så måste man säkerställa att dessa uppdateringar ryms inom ramen för aktuell ackreditering. Gör de inte det ska en om-ackreditering genomföras. Det vill säga att man behöver bedöma till vilken grad påverkar en uppdatering systemets funktionella krav och systemets säkerhetskrav. Hur påverkas dess omgivning osv.

Vad som ligger till grund för denna bedömning och hur den ska göras är komplex och kan upplevas som svårtolkad. Det är därför vår avsikt med denna intervju att försöka klarlägga hur informanten ser på detta utifrån sin expertis på området samt utifrån den organisation denna tillhör.

Förtydliganden

Med bedömning menar vi nedan: Den typ av bedömning som görs om ett redan ackrediterat IT-system behöver om-ackrediteras efter utförda system- och/eller säkerhetsuppdateringar.
Med uppdateringar menar vi nedan: System- och/eller säkerhetsuppdateringar

Intervjufrågor

Info om informanten

- Vilken organisation jobbar du i?
- Vad har du för roll?
- På vilket sätt arbetar du med uppdateringar av system inom Försvarsmakten?

Hur görs bedömningen

- Hur går en bedömning till? (Vem beslutar om en om-ackrediteringar är nödvändig)
- Måste alla uppdateringar bedömas? (Om nej, vilka väljs bort och varför?)
- Vilka dokument ligger till grund för bedömning?
- Vilka ursprungliga krav ligger till grund för bedömning?
- Vad finns det för hjälpmedel för bedömningar? (Rutiner, diskussionsforum m.m.)
- Finns det någon sammanställning av tidigare bedömningar?

Var i ligger problemet

- På vilket sätt upplever du att otydligheterna i frågan om när en om-ackreditering behöver göras dyker upp i ditt arbete?

- Vad finns det för nytta i att slippa en om-ackreditering?

Hur kan man lösa detta

- Här lyfts diskussion baserat på tidigare svar om det inte skett

Krav från KSF 3.1 som vi kan komma ställa specifika frågor kring

SALC_LCM.C3 (s.23)
SALC_BRK.C7 (s.25)
SAOP_BRK.C2 (s.37)
SAOP_BRK.C4 (s.38)
SAOP_BRK.C7 (s.38)
SAOP_BRK.C8 (s.38)
SARU_UPD.C1 (s.44)
SARU_UPD.C7 (s.45)
SARU_KFG.C4 (s.46)