UPTEC STS 11 007
Examensarbete 30 hp
Mars 2011

Auktorisation och ackreditering inom Försvarsmakten

En studie i nyttan av en standardiserad process för att hantera informationssäkerhet

Susanne Fredriksson

UPPSALA
UNIVERSITET

Teknisk- naturvetenskaplig fakultet
UTH-enheten

Besöksadress:
Ångströmlaboratoriet
Lägerhyddsvägen 1
Hus 4, Plan 0

Postadress:
Box 536
751 21 Uppsala

Telefon:
018 – 471 30 03

Telefax:
018 – 471 30 00

Hemsida:
http://www.teknat.uu.se/student

Abstract

Authorisation and accreditation in the Swedish Armed Forces

Susanne Fredriksson

Information Technology is an essential part of the society today, not least in large organisations dealing with sensitive information. An example of such an organisation is the Swedish Armed Forces which indeed is in the need of ways to ensure information security in their Information Technology systems. The means which is used is an authorisation and accreditation process.
All Information Technology systems go through a life cycle which includes realisation, usage, development and liquidation. In the Swedish Armed Forces the lifecycle is an authorisation process. Each step in the process is followed by an authorisation decision and one of these steps is accreditation. Accreditation is a formal approval to put the system in operation.
The aim of the thesis is to study how large organisations may ensure information security when developing IT and the importance of a standardised process to handle information security. The study has been carried out by comparing the process of the Swedish Armed Forces with other methods to run projects and theories concerning development of IT.
Interviews with Information Security Consultants at Combitech AB along with a study of documentation have been carried out in order to study the process. The theoretical framework has been formed through a literature study of project models and methods for development of IT.
The main result of the thesis is that a standardised processes which manage quality, communication, traceability, complexity, aim, operation and liquidation plan, risk assessment as well as use cases increases the chance of a successful project and the achievement of information security in development of new IT. High quality in the formation of the security aim and the specification of requirements, along with tests to establish that all requirements are fulfilled, are crucial when it comes to information security.

Handledare: Therése Bergengren
Ämnesgranskare: Aletta Nylén
Examinator: Elísabet Andrésdóttir
ISSN: 1650-8319, UPTEC STS11 007
Sponsor: Combitech AB

Sammanfattning

IT-system har kommit att bli en allt större del av vår vardag, så även inom stora organisationer som behandlar känslig information. Ett exempel på en sådan organisation är Försvarsmakten som därmed har ett stort behov av att säkerställa informationssäkerheten inom sina IT-system, vilket sker genom auktorisation och ackreditering.

Varje IT-system genomgår en livscykel i form av realisering, användning, utveckling och avveckling. För Försvarsmaktens IT-system hanteras detta genom en auktorisationsprocess där varje del i livscykeln omfattas av ett auktorisationsbeslut. Ackreditering är ett av dessa auktorisationsbeslut och innebär ett formellt driftgodkännande som ska ges innan ett IT-system inom Försvarsmakten tas i bruk.

Detta examensarbete syftar till att studera hur stora organisationer kan hantera informationssäkerhet i utveckling av nya IT-system samt varför det ska finnas en standardiserad process för detta. Studien har utförts genom att jämföra Försvarsmaktens auktorisations- och ackrediteringsprocess med andra modeller för projektstyrning och IT-utveckling.

Auktorisations- och ackrediteringsprocessen har studerats genom intervjuer med konsulter på Combitech AB samt genom att studera deras auktorisations- och ackrediteringsunderlag. Det teoretiska ramverket har satts upp genom litteraturstudier av projektmodeller och modeller för IT-utveckling.

Studien har visat att genom att ha en standardiserad process som behandlar kvalité, kommunikation, komplexitet, riskhantering, målsättning, plan för drift och avveckling, spårbarhet samt användarfall ökar chansen att ett projekt lyckas och för att uppnå informationssäkerhet vid IT-utveckling. En bra säkerhetsmålsättning och kravspecifikation i början av processen är avgörande när det gäller informationssäkerhet och testning är viktig för att säkerställa att IT-systemet uppfyller alla krav innan det sätts i drift.

Förord

Jag vill rikta ett stort tack till Combitech AB och de experter inom informationssäkerhet där som gjort detta examensarbete möjligt genom bidrag med kunskap och inspiration. Ett speciellt tack vill jag rikta till min handledare, Therése Bergengren, vars hjälpsamhet och stöd varit oumbärligt.

Jag vill även tacka min ämnesgranskare på Institutionen för informationsteknologi vid Uppsala Universitet, Aletta Nylén, för vägledning under arbetets gång.

Linköping, December 2010

Susanne Fredriksson

Innehållsförteckning

1 Inledning

Över allt i samhället finns de, i våra hem, på våra arbetsplatser, uppe i luften och nere i vattnet. IT-system har kommit att omge vår vardag och vara ett stöd inom alla tänkbara områden. Men på samma sätt som de är ett stöd bringar de även nya hot, risker och sårbarheter. Försvarsmakten är en organisation där IT-systemen har en stor inverkan på hela verksamheten och där informationssäkerhet därför får en central roll. I yttersta fall kan IT-systemen till och med spela en livsavgörande roll.

För att säkerställa att de IT-system som tas i bruk inom Försvarsmakten hanterar information på ett säkert sätt ska samtliga IT-system ackrediteras. Ackreditering innebär ett godkännande av ett IT-system ur säkerhetssynpunkt. Genom ackreditering säkerställs att det IT-system som utvecklas håller rätt nivå på säkerhet. IT-systemet granskas utifrån de säkerhetskrav som satts upp för det. IT-systemet måste bland annat uppfylla en rad förordningar som består av såväl svensk lag som Försvarsmaktens regler. Ackreditering föregås av en auktorisationsprocess. Auktorisation ger Försvarsmakten, som är en mycket stor organisation, samordning av verksamhetens IT-system vilket innebär en möjlighet att fatta beslut om utveckling av ett nytt IT-system eller om en redan befintlig lösning kan nyttjas. Genom auktorisation bedöms möjligheten att realisera ett IT-system med informationssäkerhet i fokus. IT-säkerhet innebär att ett IT-system ska skyddas med avseende på sekretess, tillgänglighet, riktighet och spårbarhet. Processen drivs fram genom ett antal beslutspunkter och huvudmomenten går ut på att ta fram en kravbild, beskriva IT-systemet utifrån informationssäkerhetssynpunkt och att slutligen granska det färdiga IT-systemet utifrån den ställda kravbilden med systembeskrivningen som underlag. Alla IT-system inom Försvarsmakten måste genomgå auktorisation men det är endast de som behandlar sekretessbelagda uppgifter som måste ackrediteras.

Försvarsmaktens arbete med auktorisation och ackreditering utgår från en livscykelprocess med sju beslutspunkter. I det första beslutssteget utreds behovet och i det andra beslutssteget sätts en målbild upp som sedan utvecklas till en kravbild i det tredje beslutssteget. I fjärde beslutssteget tas en lösning fram som granskas ur säkerhetssynpunkt i det fjärde och femte beslutssteget. Resterande två beslutsstег handlar om driftsättning, beslut under drift samt avveckling. Arbete i form av livscykler och olika beslutsstег återfinns i många traditionella projektstyrningsmetoder och IT-utvecklingsformer. Därför är det intressant att jämföra auktorisation och ackreditering med andra metoder för att se vilka likheter och olikheter det finns samt vilka lärdomar som kan dras utifrån detta.

I den här uppsatsen undersöks hur Försvarsmakten arbetar med auktorisation och ackreditering av sina IT-system. Försvarsmakten är unik då det inte finns någon annan liknande verksamhet i Sverige. Organisationen kan ändå jämföras med andra stora institutioner i samhället till exempel landstinget, polisen och banker som också har ett stort behov av att skydda sina IT-system med avseende på informationssäkerhet och på så sätt får uppsatsen ett bredare syfte.

Examensarbetet har gjorts hos Combitech AB som stödjer Försvarsmakten i auktorisations- och ackrediteringsprocessen vid framtagandet av underlag till beslutspunkterna. Arbetet har möjliggjorts genom studier av dessa underlag samt intervjuer med experter inom informationssäkerhet på Combitech AB.

1.1 Syfte

Syftet med denna uppsats är att studera hur stora organisationer som behandlar information med stort skyddsvärde kan hantera informationssäkerhet i utvecklingen av nya IT-system samt varför det ska finnas en standardiserad process för detta. Detta görs genom att jämföra Försvarsmaktens auktorisations- och ackrediteringsprocess med andra modeller för projektstyrning och IT-utveckling för att påvisa eventuell förbättringspotential hos processen.

1.1.1 Frågeställning

- Hur ser projektmodellen ut i Försvarsmaktens auktorisations- och ackrediteringsprocess?
- Hur bör en standardiserad process för att hantera informationssäkerhet i utveckling av nya IT-system i stora organisationer med höga krav på informationssäkerhet se ut och varför bör den se ut just så?
- Vilka är nyckelfaktorerna i en sådan modell?

1.2 Avgränsning

Auktorisation och ackreditering förekommer i många sammanhang. I den här uppsatsen är det Försvarsmaktens auktorisation och ackreditering som undersöks. Ett IT-systems livscykel sträcker sig från det att ett behov uppkommer till dess att ett IT-system ska avvecklas. I denna uppsats har jag dock valt att koncentrera mig på processen fram till dess att IT-systemet är ackrediterat, det vill säga inte drift och avveckling.

1.3 Definitioner

Nedan definieras ett antal begrepp som tas upp i uppsatsen. För mer utförlig begrepps- och ordlista se bilaga 1.

Ett *system* är ett antal delar som samverkar med varandra och därmed bildar en helhet. (Nationalencyklopedin, 2010e)

Ett *informationssystem* är ett system som hanterar information och såväl fysisk utrustning som processer kring systemet innefattas i termen. (Nationalencyklopedin, 2010a) I denna uppsats används begreppet *IT-system* som här syftar till datorstödda informationssystem.

IT-säkerhet är ett begrepp för all säkerhet rörandes data som hanteras i ett IT-system. I den här uppsatsen används begreppet *informationssäkerhet* som har samma betydelse som IT-säkerhet men med fokus på den information som datan representerar. Genom informationssäkerhet ska sårbarhet motverkas, det vill säga information ska skyddas med avseende på sekretess, tillgänglighet, riktighet och spårbarhet. (Nationalencyklopedin, 2010b)

Med *systemsäkerhet* menas i denna uppsats att systemet inte ska orsaka skada på person, egendom, eller miljö. (Försvarsmakten, 2004)

En allmän definition på *sekretess* är förbud att röja en uppgift muntlig eller genom utlämning av handling. (Nationalencyklopedin, 2010d) Inom Försvarsmakten delas information in enligt öppna uppgifter, hemliga uppgifter, utrikeshemliga uppgifter samt

uppgifter som berörs av övrig sekretess. Övrig sekretess är till exempel personlig sekretess. Utifrån informationens skyddsvärde bedöms vilka säkerhetsfunktioner ett IT-system behöver.

Tillgänglighet anger ett systems tillförlitlighet, det vill säga driftsäkerhet. Tillgänglighet innebär således den tid som systemet är funktionsdugligt. (Nationalencyklopedin, 2010f)

Riktighet definierar att något, i det här fallet informationen, inte innehåller några fel men även att den inte har ändrats eller manipulerats. (Nationalencyklopedin, 2010c)

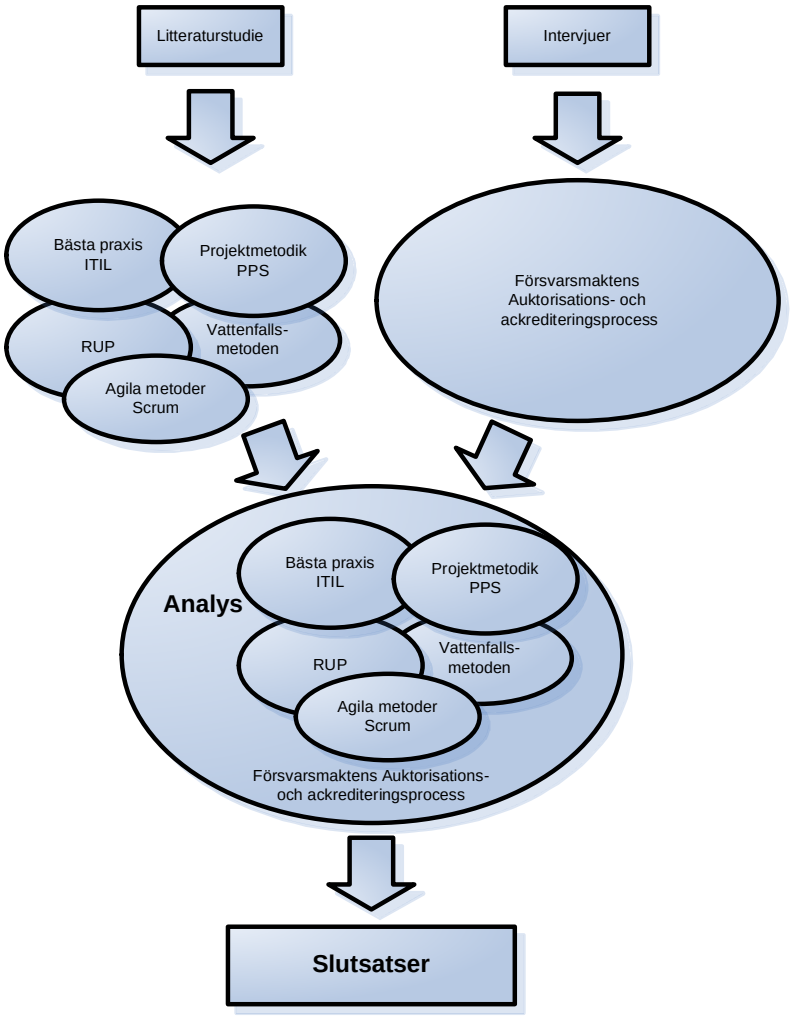
I uppsatsen används fler definitioner av *spårbarhet.* En aspekt är spårbarhet i IT-system i syfte att uppnå informationssäkerhet. Spårbarhet innebär då att det ska gå att se avsiktliga såväl som oavsiktliga ändringar i information, var dessa ändringar har skett, när de skedde och vem som gjorde dem. En annan aspekt är spårbarhet i dokumentation i auktorisations- och ackrediteringsprocessen. Då handlar det om att det ska framgå vilken version ett dokument har, vilka ändringar som har gjorts sedan föregående version, vem som gjort ändringarna och när. Även vilket underlag dokumentet tillhör samt vilka bilagor som finns måste framgå. En tredje aspekt är spårbarhet när själva granskningen av IT-systemet ska utföras. Då ska det tydligt framgå från vilket krav vart och ett av säkerhetsmålen härrör. Även kvarstående åtgärder och krav på användning måste tydligt kunna spåras till vilket krav de kommer ifrån. När beslut fattas måste det vara tydligt på vilka grunder det görs.

2. Metod

2.1 Tillvägagångssätt

För att möjliggöra denna studie har Combitech AB haft en stor betydelse genom att låta mig studera deras arbete med auktorisation och ackreditering. Detta har dels skett genom att jag tagit del av deras auktorisations- och ackrediteringsmaterial, men även fått möjlighet att intervjua deras experter på området. För att sätta upp det teoretiska ramverket har en litteraturstudie utförts.

I teoriavsnittet presenteras teorier om projektmetodik, bästa praxis och metoder för IT-utveckling. Empiriavsnittet är en fallstudie där Försvarsmaktens auktorisations- och ackrediteringsprocess är objektet som studeras genom en fördjupning i hur Combitech som extern konsult bistår i processen. Därefter görs en analys på empirin utifrån det teoretiska ramverket, se figur 1. Där undersöks vilka likheter och skillnader som finns mellan auktorisations- och ackrediteringsprocessen jämfört med traditionell projektmetodik och IT-utveckling. En studie av vad som följs och inte följs görs för att kunna utröna vad som är viktigt i utveckling av nya IT-system med avseende på informationssäkerhet.



Figur 1: Arbetsprocessen i rapporten.

2.2 Litteraturstudie

För att läsa in mig på auktorisation och ackreditering har jag tagit del av materiel från såväl Försvarsmakten som Combitech. Försvarsmaktens auktorisations- och ackrediteringsarbete utgår från *Direktiv för försvarsmaktens informationsteknikverksamhet, DIT 04* som jag har använt för att läsa in mig på processen. Även andra dokument från Försvarsmakten har använts som underlag. Från Combitech har jag tagit del av exempel på utförda ackrediteringar samt deras utbildningsmaterial. Att få ta del av konkreta exempel har varit till stor hjälp i fallstudien. Det finns svårigheter i att ta del av Försvarsmaktens materiel för den oinvigde och därmed har kunskap från Combitech varit ett stort stöd.

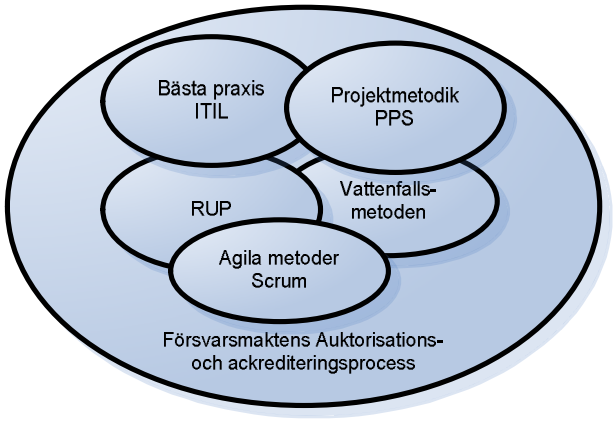
För att skapa det teoretiska ramverket har jag studerat ett antal olika projektmodeller. Dessa inkluderar så väl generella metoder för att driva projekt som specifika metoder för IT-utveckling och då speciellt mjukvaruutveckling. Försvarsmaktens auktorisations- och ackrediteringsprocess är en stödprocess vid utveckling av IT-system med fokus på informationssäkerhet, och projektmodellerna har således applicerat på stödprocessen det vill säga utveckling av dokument och så vidare.

2.3 Intervjuer

Den främsta källan till information i denna uppsats är intervjuer. Totalt har 16 intervjuer genomförts varav fem skedde via telefon och en var en gruppintervju. Att majoriteten av intervjuerna skedde genom fysiska möten var för att underlätta skapandet av en diskussion. Intervjuerna var semistrukturerade, det vill säga de följde en struktur men respondenten gavs utrymme för att uttrycka egna åsikter och tankar. Gruppintervjun fördes i diskussionsform men med struktur utifrån en erfaren informationssäkerhetskonsult som ledde diskussionen. Att en andra part ledde diskussionen innebar att jag kunde koncentrera mig på att ta in vad som sades och ställa följdfrågor på detta. Respondenterna har varit informationssäkerhetskonsulter, projektledare samt en affärsutvecklare på Combitech. De specialister på informationssäkerhet som intervjuats arbetar främst med framtagande av underlag till auktorisation och ackreditering. Två av respondenterna har dock varit i den roll på Försvarsmakten där de granskar innehållet i underlaget. Att få en bild från båda sidorna har varit fördelaktigt för att öka förståelsen för processen. Några av informationssäkerhetsspecialisterna har mycket stor erfarenhet av auktorisation och ackreditering vilket har varit till stor hjälp vid informationsinsamlingen. De som är mindre erfarna har dock haft stor betydelse även de då de i större utsträckning har kunnat påpeka vilka svårigheter som finns i arbetet. Många av respondenterna har en bakgrund inom Försvarsmakten och dessa har bidragit med kunskap i hur Försvarsmaktens verksamhet fungerar. Projektledarna som intervjuats har främst bidragit med kunskap om hur auktorisation och ackreditering kan stödja utvecklingen av IT-system. Att samtliga respondenter är anställda på Combitech innebär att den bild av auktorisations- och ackrediteringsprocessen som presenteras i den här studien är något vinklad till hur externa konsulter ser på den.

3. Utveckling av IT-system i projektform

Auktorisation och ackreditering bedrivs i projektform och kan ses som en stödprocess vid utveckling av IT-system. Därför följer nedan beskrivningar av olika projektformer, dels en generell metod men även mer specifikt i form av Information Technology Infrastructure, Vattenfallsmetoden, Rational Unified Process samt Scrum. Dessa beskriver främst utveckling av mjukvara, men går även att applicera allmänt på utveckling av IT-system. Detta ramverk har valts eftersom det beskriver såväl traditionella som nya, agila, metoder. I den här uppsatsen appliceras de på dokumentutveckling i arbetet med informationssäkerhet då ett IT-system utvecklas. Detta används sedan i analyskapitlet för att se vilken eller vilka av dessa projektformer som används i auktorisation och ackreditering och vilka för- och nackdelar det har, se figur 2. Där analyseras även vilka fördelar en standardiserad process har och nyckelfaktorer som finns i en bästa praxis för IT-utveckling.



Figur 2: Analys av auktorisation och ackreditering utifrån olika projektformer.

3.1 Projektledningsmetodik

Det finns en rad olika modeller framtagna för att styra projekt av olika slag. Många av dessa metoder följer en liknande struktur. Nedan presenteras först en allmän struktur för projektledning som sedan följs av en specifik metod framtagen av Tieto som benämner den Praktisk projektstyrning, PPS.

3.1.1 Affärsbeslut

Alla projekt drivs framåt genom olika beslut. Dessa beslut rör syfte, inriktning, mål och ramar. Jansson och Ljung (2004) benämner dem affärsbeslut och menar att varje affärsbeslut är en tydlig markering för att ett projekt går in i en ny fas. Det finns fyra affärsbeslut som är relevanta i alla projekt och det första av dessa är när projektet går från *om* projektet ska genomföras till hur det ska genomföras, se figur 3.

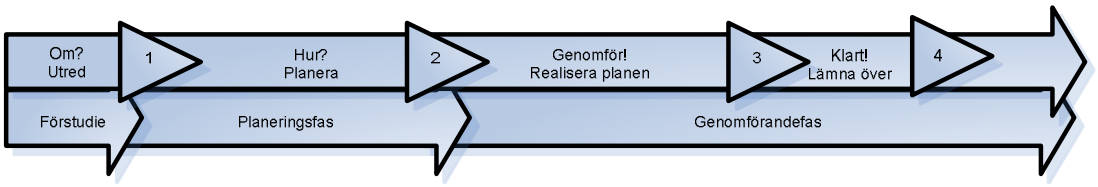
Figur 3: Affärsbeslut i ett projekt.

(Modifierad figur, Jansson och Ljung, 2004, s.79)

Det går ofta fort att fatta beslutet att projektet ska genomföras. Det innebär oftast bara att olika alternativ utreds. I det andra affärsbeslutet handlar det om att gå från att planera till att realisera. Planeringsarbetet fortsätter ofta även i realiseringsfasen och redigering av den ursprungliga planen måste ofta göras. I det tredje affärsbeslutet handlar det om att överlämna projektet till den slutliga nyttjaren. Det här steget kräver ofta ett aktivt beslut. Det fjärde affärssteget innebär att överlämningen är avklarad och att det är dags att städa upp. Nu är det de interna mottagarna som har ansvaret för projektet. Det här affärsbeslutet utförs även om projektet måste avbrytas i förtid. (Jansson och Ljung, 2004, s. 75-79)

3.1.2 Projektfaser

Affärsbesluten kan kompletteras med olika faser, förstudie, planeringsfas samt genomförande fas, se figur 4.



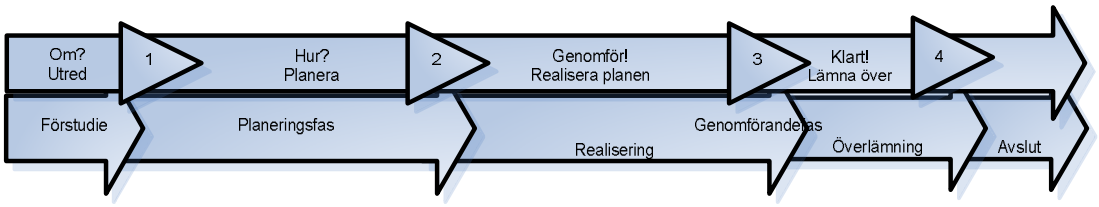
Figur 4: Affärsbeslut och faser i ett projekt.

(Modifierad figur, Jansson och Ljung, 2004, s. 83)

I fasen för *förstudie* skapas underlag för beslut om huruvida systemet ska realiseras eller inte. Storleken på förstudien är mycket varierande, ibland rör det sig om omfattande arbete och ibland är den av mer informell och otydlig karaktär. Arbetet består av utvärdering av projektidén, analys av genomförandeplan för projektet samt sammanställning av beslutsunderlag. Förstudien bör svara på frågor om organisationen ska syssla med det här, vilka krav som ska uppfyllas, om lönsamheten är tillräcklig i jämförelse med kostnaderna, om det finns tekniska och praktiska möjligheter att uppfylla kraven samt hur projektet ska gå till i stora drag. (Jansson och Ljung, 2004, s. 85-86)

Planeringsfasen inleds med det första affärsbeslutet och syftet är att planera genomförandet. Beroende på hur organisationen ser ut kan beslutsfattandet vara formellt med tydliga regler för dokumentation et cetera eller så sker det spontant med avsaknad av formella krav. Arbetet handlar främst om att analysera förutsättningar, avgränsa projektet, bedöma olika alternativ samt att organisera projektet. Planeringsfasen blir sällan en renodlad planeringsfas, genomförandet av arbetet startar nästan alltid parallellt. Detta är ofta nödvändigt för att klara en snabb leverans. Det innebär dock en risk eftersom det kan innebära att arbetet är på fel spår och måste göras om då en annan strategi än den som det jobbas efter väljs. Viktiga aktiviteter i den här fasen är beslut om krav och avgränsningar samt bedömningar av resursbehov, teknik- och strategival och så vidare. Även uppskattning av ledtid och resursåtgång, planering av tid och budgetering är viktiga inslag. Fasen avslutas genom att projektbeställaren tar affärsbeslut två och därmed inleds genomförandefasen. (Jansson och Ljung, 2004, s. 87-91)

Genomförandefasen består enligt Jansson och Ljung (2004) av tre etapper; realisering, överföring och avslut och startas genom att affärsbeslut två tas, se figur 5. Denna gräns passeras inte automatiskt, ett aktivt beslut måste fattas.



Figur 5: Affärsbeslut, projektfaser och etapper i ett projekt.

(Modifierad figur, Jansson och Ljung, 2004, s.83)

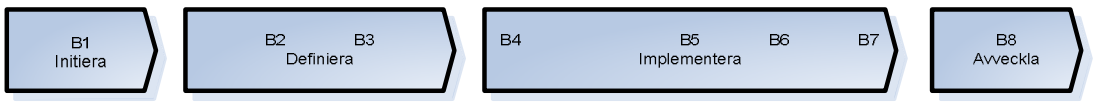
Realiseringsetappens syfte är att skapa det avsedda projektresultatet så att det kan föras över till interna mottagare och eventuell kund. Kommunikation inom organisationen är viktigt i denna fas. Beslut ska fattas angående ändringar i krav eller förutsättningar. I *överlämningsetappen* ska ansvaret för projektet överlämnas till den interna mottagaren och den eventuella kunden. Etappen initieras genom att affärsbeslut tre tas. Även denna övergång är ofta inte självklar, utan ett beslut måste tas när resultatet anses vara tillräckligt bra. I den här etappen måste även beslut fattas om hur kvarstående brister ska hanteras. Om ett projekt måste avslutas i förtid behandlas också det här. Att ett projekt måste avslutas i förtid kan bero på att resurserna behövs någon annanstans i organisationen eller att det inte längre finns någon möjlighet att nå målet. Då är det ändå viktigt att ta tillvara på delresultat som kanske kan användas i andra delar av organisationen. Den sista etappen, *avslut*, syftar till att ta tillvara de erfarenheter som gjorts under projektets gång. Etappen påbörjas genom att det fjärde affärsbeslutet fattas. Det kan vara bra att sammanställa erfarenheter från projektet i en rapport där samtliga som deltagit i projektet deltar. Detta medför att personer i liknande projekt kan dra nytta av tidigare erfarenheter men även att deltagarna får reflektera över sitt eget arbete. (Jansson och Ljung, 2004, s. 91-99)

3.1.3 Styrgrupp

I en styrgrupp förs en dialog mellan chefer angående de viktigaste besluten som fattas i ett projekt. En av cheferna är ledare för styrgruppen och stödjer projektledaren för projektet. Styrgruppen fungerar som verksamhetsledning och är således beslutsfattande inom projektet. (Jansson och Ljung, 2004, s. 59, 63)

3.1.4 Praktisk projektstyrning

Praktisk projektstyrning, PPS, är en modell för stöd i projekt. PPS definierar åtta beslutssteg som styrgruppen ansvarar för, se figur 6. Syftet med beslutspunkterna är att skapa kontroll över projektet, få kontroll över fördelar för organisationen samt status för resultat, tid och kostnad. (Tieto, 2010)



Figur 6: Projektstyrning enligt PPS.

Vid varje beslutspunkt har styrgruppen möjlighet att besluta om projektet ska fortlöpa. Dessutom ska styrgruppen i varje beslutspunkt ge direktiv inför kommande beslutspunkt. Det ger således en möjlighet för styrgruppen att bemyndiga projektdelar steg för steg. Beslutspunkt ett är projektägarens beslut att initiera ett projekt och forma ramverket för hur definieringsarbetet ska gå till. Den andra beslutspunkten innebär ett beslut om att projektarbetet i förberedelsefasen är på rätt väg och detta fastställs genom beslutspunkt tre. Beslutspunkt fyra startar genomförandet av projektet. Det innebär att arbetsmetoder, kostnads-/ och nyttouppskattning, tidsplan och risknivåer för hela projektet ska vara fastställt. För delar som redan godkänts kan genomförandefasen inledas innan förberedelsefasen är helt avslutad om det till exempel råder tidsbrist. Beslutspunkt fyra till och med sju utgör genomförandefasen. Beslutspunkt fem är en återkommande beslutspunkt som rör styrnings-, produktions- och affärsmodeller. Beslut om leverans av projektresultatet fattas i beslutspunkt sex medan det i beslutspunkt sju beslutas om ansvarsöverlämning. Den sista beslutspunkten, åtta, innebär avslut och en sammanfattning av erfarenheter. Projektledaren är ansvarig för att ta fram underlag till respektive beslut medan styrgruppen är ansvarig för att fatta besluten. (Tieto, 2010)

3.2 Bästa praxis

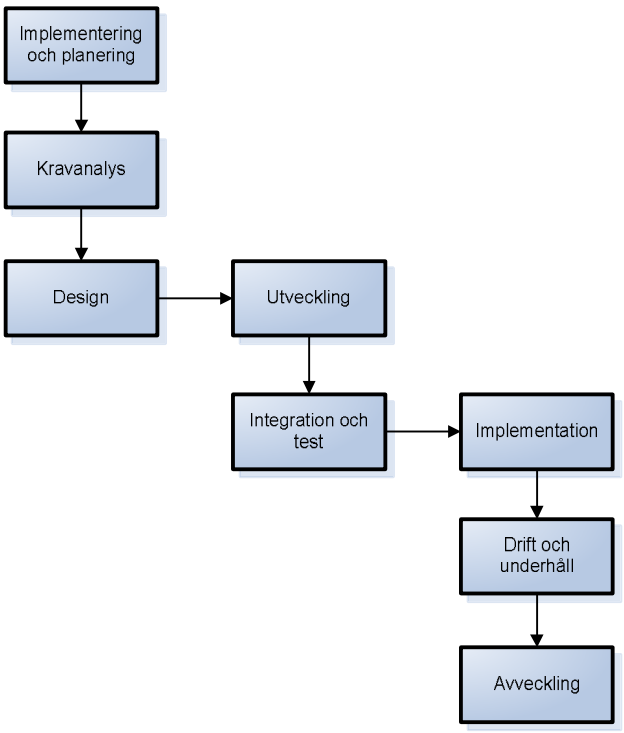
Grady Booch (2004) menar i *Software Development Best Practises* att det finns några generella faktorer som gör att projekt misslyckas. En av dessa är tvetydiga budskap och brister i kommunikation. En annan är för hög grad av komplexitet samt oupptäckt inkonsekvens i design och implementering. Slutligen är brister i riskhantering en omständighet som bidrar till att projekt misslyckas. Om det finns en plan för hur dessa problem ska hanteras så har projektet större sannolikhet att lyckas. Problem med mjukvara är mycket billigare att åtgärda i början av utvecklingen än efter att den spridits. Därför är det viktigt att kontinuerligt fastställa ett systems kvalité med tanke på till exempel funktionalitet och tillgänglighet. Att verifiera ett systems funktionalitet innebär testning för samtliga huvudscenarion. Genom testning uppnås kunskap om vilka scenarier som inte uppfyllde kraven. Detta är en iterativ process i samband med utvecklingen. Att testa systemet på det här sättet innebär att en rad av vanliga utvecklingsproblem elimineras, till exempel så blir projektets status tydligt eftersom det är själva systemet som testas, inte dokumentation kring det. Det blir även en objektiv bedömning av krav och design. Brister identifieras tidigt och innebär därmed minskade kostnader. (Booch, 2004, s. 3-16)

Vidare anger Booch ett antal specifika problem med mjukvaruutveckling. Dessa går att applicera generellt på utveckling av IT-system. Booch menar att olika utvecklingsprojekt misslyckas av olika anledningar men att det finns några faktorer som ofta ligger till grund för misslyckande:

- Felaktig uppfattning av behovet hos slutanvändaren
- Oförmåga att handskas med förändringar av behovet
- Mjukvara som är svår att upprätthålla eller vidareutveckla
- Brister i projekt upptäcks sent
- Dålig kvalité
- Mjukvaran beter sig inte som det är tänkt
- Användare gör spårbarheten omöjlig, det vill säga det går inte att se vem som ändrade vad, när, var och varför (Booch, 2004, s. 3-16)

3.2.1 En IT-tjänsts livscykel

Angelica Haverblad (2004) beskriver en IT-tjänst livscykel i *IT Service Management i praktiken*, se figur 7. Hon menar att en IT-tjänst består av steg som sträcker sig från initiering och planering till och med avveckling. Redan vid initiering av ett projekt måste det planeras för drift och förvaltning. Genom att IT-tjänsten håller en hög kvalité redan vid driftsättning så hålls driftkostnader nere. Ur ett IT Service Management-perspektiv finns det ett antal steg som ska gås igenom i livscykeln. Först kommer ett *initierings- och planeringssteg* där behovet identifieras. En nyttovärdering utförs och utifrån den tas beslut om huruvida realisering ska ske eller inte och redan i det här steget är det viktigt att beakta driften för att kunna beräkna kostnader för till exempel tillgänglighet och tillförlitlighet. Nästa steg är *kravanalys och design* där funktionella, icke funktionella och tekniska krav ska identifieras. I det här steget ska beaktas hur IT-systemet ska integreras med redan befintliga IT-system. Därefter följer *utveckling, integration och test* då IT-systemet ska testas med avseende på kvalitet innan det driftsätts. Steget som följer därpå är *implementation* där en pilotdrift av IT-systemet görs innan det sätts i drift i verkligheten. IT-systemet testas då för att säkerställa stabilitet och tillförlitlighet. Driftrutiner och dokumentation kring IT-systemet och drift utformas. Efter implementation följer *drift och underhåll*. Det är viktigt att roller, ansvar och befogenheter är tydligt definierat i form av exempelvis systemägare och systemansvariga. Det sista steget är *avveckling* som sker antingen på grund av att IT-systemet inte längre används, att det är för höga driftkostnader eller för att det ska ersättas med ett nytt. (Haverblad, 2004, s.60-62)



Figur 7: En IT-tjänst livscykel enligt IT Service Management.
(Modifierad figur, Haverblad 2004)

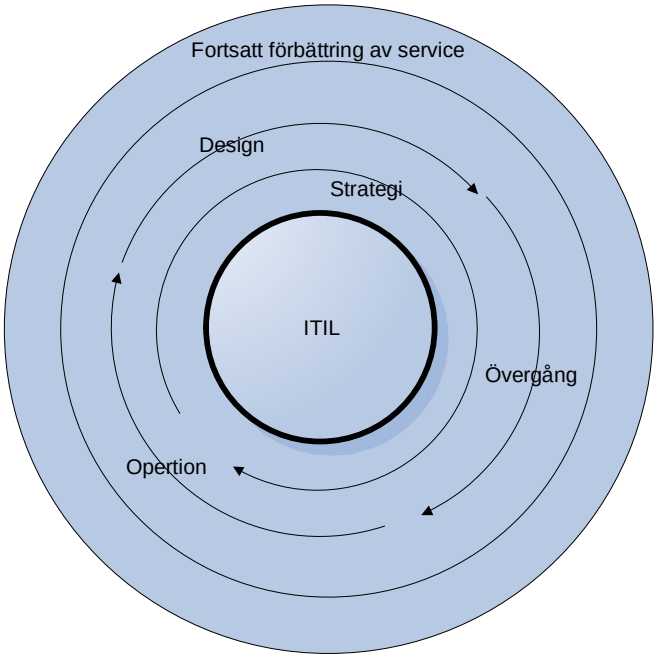
3.2.2 Förändringsprocessen

I *IT ur ett affärsperspektiv* pekar Haverblad (2006) på elva huvudorsaker till att förändringsprocesser misslyckas. Den första orsaken är att *projektet blir ett teknikprojekt*, det vill säga fokus ligger på IT-systemet som ska utvecklas istället för organisatoriska förändringar som utvecklingen medför. En annan orsak är *otydliga mål och otydlig avgränsning*. Stora ändringar under processens gång bör hanteras som nya projekt annars upplevs ursprungsprojektet som ett evighetsprojekt. *Kortsiktiga mål* motverkas genom att skapa en helhetsbild och ha långsiktiga mål. Ett annat problem är att m*ålen inte mäts*. Att skapa mätbara mål för att veta vad som är, respektive inte är uppnått är av stor vikt. Att det *inte finns definierat vad som krävs för en fungerande process* hör ihop med vikten av en tydlig målsättning. För att få en fungerande processen krävs till exempel att roller, ansvar, rutiner, mål och mätvärden definieras. Dessa punkter har dock ingen verkan om *processen inte följs*. Det är viktigt att projektet är förankrat hos alla som berörs av det för att det inte ska uppstå motstånd mot projektet. Även *avsaknad av förvaltning av processen* är en orsak till misslyckande. En processägare ska utses tidigt och ansvaret ska vara tydligt. Problem med förankring kan också uppstå om *projektet till stora delar har utförts av externa resurser*. Det finns risk att intern kompetens saknas om projektet till stor del utförts av externa konsulter vilket i sin tur leder till att processen inte följs. Detta kan förhindras genom att förankra processen i verksamheten vilket kan ske genom kommunikation och information. Det är viktigt att de som påverkas av förändringen får vara delaktiga i designen under processen. Också *brist på kompetensöverföring mellan extern och intern resurs* kan orsaka problem. Genom hela projektet måste en kompetensöverföring ske så att det i fortsättningen inte krävs en extern resurs för förvaltning. Det kan också vara *för stort fokus på en modell eller ett ramverk*. Det måste först definieras vad som ska uppnås och vilken strategi som ska användas. Modeller och ramverk måste sedan anpassas efter detta. Slutligen kan förändringen vara för *överambitiös*. Det går inte att genomföra för mycket på en gång. Istället ska projektet delas upp i väldefinierade steg. (Haverblad, 2006, 58-61)

3.2.3 Information Technology Infrastructure Library

Information Technology Infrastructure Library, ITIL, är principer och riktlinjer för IT-utveckling och ger en omfattande beskrivning av hur verksamhet kring ett IT-system kan gå till. ITIL utgår från en bästa praxis-ansats där expertis tillsammans med input från användare driver utvecklingen av både teknik och organisation kring IT-system. En av fördelarna med ITIL är att organisationen får bättre kontroll över sina IT-system vilket leder till minskade kostnader, samordning och stabilitet. Därmed bidrar den även till ökad säkerhet för verksamheten. Genom att ha en utstakad process med rutiner som används kontinuerligt är det lättare att möta behov från verksamheten. Tydliga processer och tydligt ansvar hjälper till att öka effektiviteten, dessutom bidrar ITIL till ett gemensamt språk där termer definieras. Vanlig kritik är att den upplevs som byråkratisk men dess förespråkare hävdar att det handlar om att förankra dess fördelar för dem som ska använda den. Metoden passar bäst för stora företag eftersom behovet av samordning och formella arbetssätt då är störst. (Arraj, 2010) (ITIL, 2010)

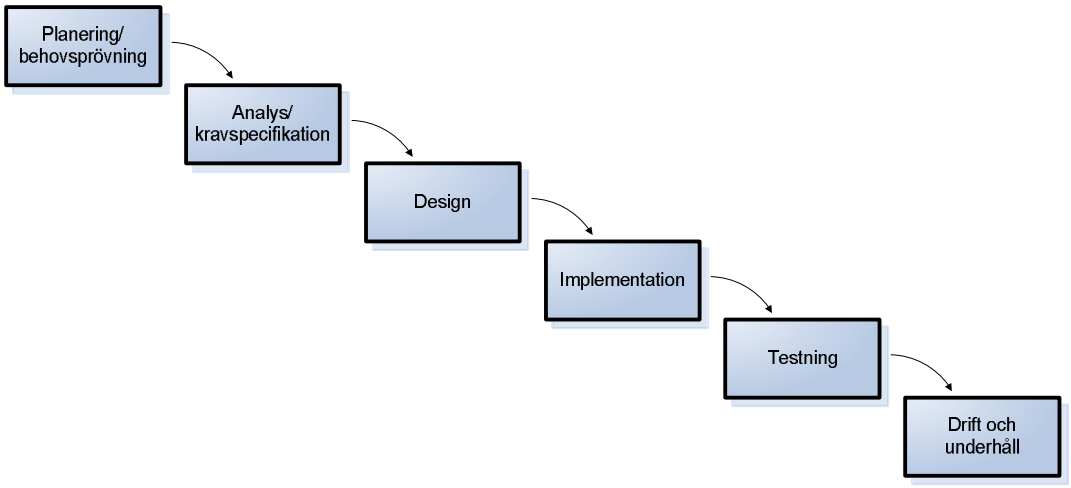
Enligt ITIL ska IT-tjänster vara inriktade på ett sådant sätt att de stödjer och är till nytta för ett företags verksamhet. ITIL är en livcykelprocess som börjar med att ett behov identifieras som kan stödjas med hjälp av en IT-tjänst, se figur 8. Därefter kommer design och implementering av tjänsten i verksamheten som följs av en övervaknings- och förbättringsfas. (ITIL, 2010) Livscykelns första fas är *strategi* där kunden för IT-tjänsten ska identifieras samt vilka tjänster som behövs för att möta kundens behov. Därefter följer *designfasen* där en teknologi och arkitektur som möter kundens behov ska skapas. I livscykelns *överföringsfas* byggs, testas och valideras designen för att säkerställa att den uppfyller samtliga ställda krav och en kontroll av komponenter i form av såväl hårdvara som mjukvara sker. Därpå följande fas handlar om *drift* och omhändertagande av problem som uppstår under systemets livstid. Kring hela livscykeln finns en kontinuerlig kontroll av IT-tjänsten för att förbättra och effektivisera såväl tekniken som processen. (Arraj, 2010)



Figur 8: Livscykel enligt ITIL.
(Modifierad figur, Arraj, 2010)

3.3 Vattenfallsmodellen

Vattenfallsmodellen är en linjär process där varje steg avslutas helt innan nästa steg tas. På samma sätt som ett vattenfall inte rinner uppåt så går det inte att backa i processen. Systemutveckling, kravspecifikation, analys, design och testning är steg som bearbetas ett i taget, se figur 9. (Computer Sweden, 2010c) Kritik har framförts mot modellen då den inte hanterar förändringar av behov och det är svårt att senare i processen rätta till fel som uppkommit i början av den. (SoftDevTeam, 2011)



Figur 9: De vanligaste faserna enligt Vattenfallsmodellen.

Vattenfallsmodellen skapades på 1970-talet av Winston W. Royce som menade att all mjukvaruutveckling innebär två huvudsakliga steg, analys och kodning. För att få ett lyckat resultat krävs det dock ytterligare processteg men dessa leder inte lika explicit fram till slutprodukten och de kommer dessutom att öka utvecklingskostnaderna. Därför är det viktigt att organisationens ledning förankrar dessa processteg hos såväl de som utvecklar systemet som hos dem som ska betala för det. En fara med modellen är att testningen sker först när processen är långt gången. Om systemet inte klarar testningen innebär det antingen att mycket behöver göras om till stora kostnader eller att kravställningen måste ändras. (Royce, 1970)

Royce menar att utöver de definierade stegen i processen finns det även viktiga kringprocesser av vilken en är dokumentation. Utan en omfattande dokumentation med hög standard är det omöjligt att styra utvecklingen av systemet. Dokumentation är viktigt för kommunikation i projektet samt att moment och processer blir mer definitiva genom att föras ner på papper. Dessutom specificeras systemets design genom dokumentation. Det verkliga värdet i dokumentationen kommer mot slutet av processen då det är dags för testning av systemet. Utan dokumentation blir det svårt för någon annan än den som skapat systemet att förstå det och det är inte acceptabelt varken då systemet ska testas eller då det ska användas. Ytterligare en kringprocess är planering och kontroll kring tester. Testningsfasen är utan tvekan den mest resurskrävande enligt Royce. Testningen sker sent i processen då back up alternativ är få eller till och med obefintliga och det finns några särskilda faktorer som bör beaktas. Helst ska någon oberoende testa systemet, det vill säga det är inte samma person som skapat systemet som ska testa det. Många fel går ofta att se med blotta ögat så att alltid ha en andra part som granskar materialet är viktigt. En viktig kringprocess hos Vattenfallsmodellen rör användaren och dennes delaktighet i utvecklingen av systemet. Kunden måste

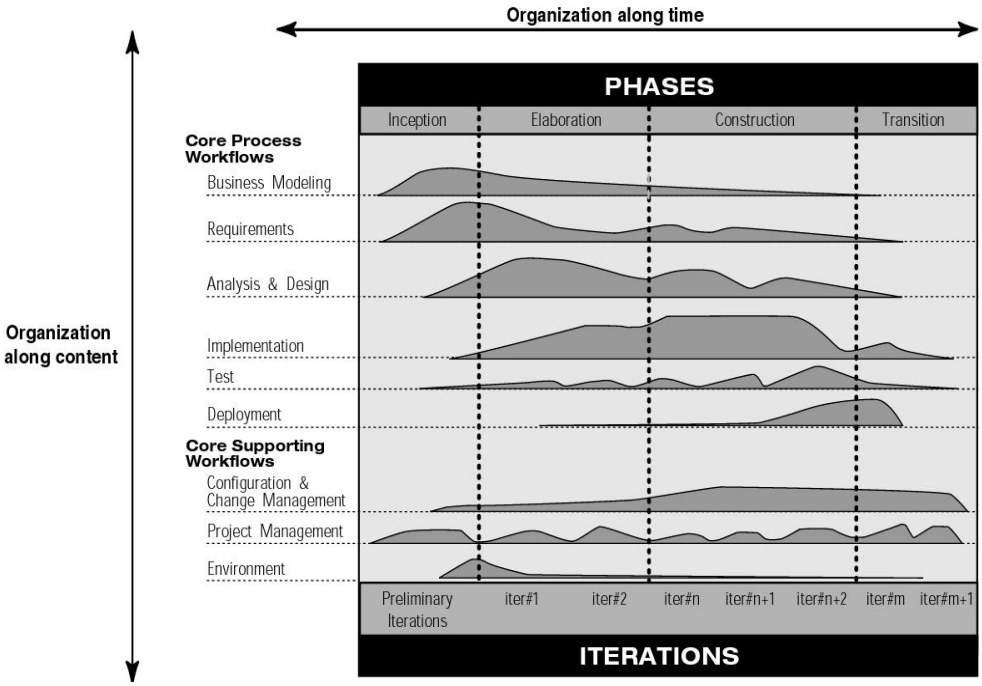
involveras på ett formellt sätt så att denne anknyts till systemet innan det levereras. (Royce, 1970)

3.4 Rational Unified Process

Rational Unified Process, RUP, riktar sig till utveckling av mjukvara och behandlar många av ovannämnda punkter för bästa praxis inom utveckling av system. (Kruchten, 2004, s. 18) Processen bygger på tidigare metoder och processer som sedan har flätats samman till RUP. I *Fyra rundor med RUP* ger Hans Lunell (2003) en introduktion till RUP. Lunell menar att det finns sex utpekade metoder som RUP står för. Den första av dessa är *iterativ utveckling*, det vill säga programvara ska utvecklas iterativt. En annan är *kravhantering* eftersom krav oundvikligen förändras under utveckling, och därför måste det finnas en metod för att hantera det. *Arkitekturcentrerad utveckling* är viktigt eftersom en bra arkitektur är avgörande för huruvida ett projekt lyckas. Detta gäller framför allt när utvecklingen sker iterativt, då måste arkitekturen kunna anpassas så att systemet kan växa successivt. *Visuell modellering* har fördelen att olika perspektiv av systemet kan analyseras var för sig men ändå jämföras. *Upprepad kvalitetsverifiering* är betydelsefullt eftersom processen är iterativ och då måste även verifiering ske iterativt för att inte gå miste om iterativ utvecklings fördelar. Slutligen krävs *konfigurations- och ändringshantering* för att hantera de olika versioner som uppstår genom iterativ utvecklig. (Lunell, 2003, s. 23-24)

Lunell identifierar även fyra nyckelegenskaper för RUP där den första är användningsfallsdriven utveckling. Användningsfall kan ses som den drivande kraften i processen omkring vilken andra aktiviteter kretsar. Den andra är featurebaserad utveckling som innebär att användningsfall och iterationer delas in efter funktioner. Riskfokusering är ytterligare en nyckelegenskap, RUP fokuserar tidigt på risker för att reducera dessa och riskhantering är ett av målen med processen. Slutligen menar Lunell att RUP är en konfigurerbar process, det vill säga en generell process som ger utrymme för anpassning efter olika utvecklingsprojekts unika egenskaper. (Lunell, 2003, s.25)

RUP kan beskrivas i två dimensioner där den horisontella axeln representerar tiden och därmed cykler, faser, iterationer och milstolpar, se figur 10. Den vertikala axeln visar en statisk aspekt som beskriver aktiviteter, artefakter, arbetare och arbetsprocesser. Utvecklingsmodellen är uppdelad i fyra faser; förberedelse, etablering, konstruktion samt överlämning. I likhet med de flesta andra projektstyrningsmodeller består det första steget av en förstudie där en analys av behovet utförs. I etableringsfasen tas designen för systemet fram och i konstruktionsfasen skapas själva systemet. Den sista fasen innebär överlämning av systemet. Var och en av milstolparna som avslutar respektive fas är en kritisk beslutspunkt. Det som skiljer RUP från många gängse projektmetoder är att varje fas är en iterativ cykel och behandlar på så sätt förändringar som uppstår under utvecklingen av systemet. En iterativ process innebär att risker dämpas tidigare, förändringar är enklare, återanvändning av idéer underlättas och projektet kan lära under tiden. (Rational Software, 1998)



Figur 10: Tvådimensionell modell av RUP.
(Rational Software, 1998)

3.4.1 Faser

Under *förberedelsefasen* avgränsas och definieras projektet. Externa enheter som systemet ska samverka med måste identifieras på ett övergripande plan och hur samverkan sker måste beskrivas i form av användarfall. Även målsättning, riskanalys, kostnadsanalys samt en övergripande tidsplan ska sättas upp för de kommande milstolparna. Fasen resulterar i ett dokument som behandlar ovanstående. I *etableringsfasen* ska problemet som föranlett projektet analyseras och arkitekturen för systemet ska etableras. Projektplanen ska utvecklas vidare och de största riskerna för projektet ska elimineras. Av de fyra faserna är denna den mest kritiska. En prototyp tas fram i en eller flera iterationer beroende på projektets komplexitet och denna ska användas för att undersöka de användarfall som identifierats i förberedelsefasen och som därmed visar på projektets största risker. Utöver en prototyp ska fasen även resultera i en beskrivning av mjukvaruarkitekturen. Om projektet inte klarar att passera den här milstolpen är det läge att tänka om ordenligt eller avveckla projektet. I *konstruktionsfasen* utvecklas alla återstående komponenter och integreras i produkten. Allting testas. Konstruktionsfasen kan ses som tillverkningsfasen. Produkten som kommer ut ur fasen ska vara redo för användning. Milstolpen är en början till möjlighet att använda produkten. Genom att milstolpen passeras beslutas det att produkten är redo för att användas utan att det innebär några stora risker. *Överlämningsfasen* syftar till att överlämna produkten till användarna. Detta medför ofta att nya, oupptäckta problem uppstår vilket innebär att nya versioner eller korrigeringar av produkten måste göras och kvarstående åtgärder att ta itu med. Fasen innebär utbildning och stöd till användare. (Rational Software, 1998)

3.4.2 Arbetsprocesser

En arbetsprocess är en rad aktiviteter som leder fram till ett observerbart värde. RUP definierar sex huvudsakliga arbetsprocesser: affärsmodellering, krav, analys och design, implementation, test samt spridning. I många projekt uppstår en lucka mellan produktutvecklare och affärsutvecklare. RUP överbryggar denna lucka genom ett gemensamt språk och en gemensam process för de båda. Kravprocessen syftar till att fastställa vad systemet ska göra så att utvecklare och kunder är överens. För att uppnå detta är dokumentation och spårbarheten mellan dokumentation viktigt. Aktörer, som representerar användarna, och användarfall identifieras. Varje användarfall beskrivs i detalj. Målet med analys- och designprocessen är att visa hur systemet ska realiseras i implementeringsprocessen och resulterar i en designmodell. I implementeringsprocessen testas komponenter och hur flera komponenter fungerar som enheter. RUP beskriver även hur komponenter ska kunna återanvändas. Syftet med testprocessen är att verifiera att interaktionen mellan komponenter fungerar, att alla krav är uppfyllda och att alla brister tas om hand innan mjukvaran sprids. Testningen sker iterativt genom hela utvecklingsprocessen för att så fort som möjligt upptäcka eventuella brister. I spridningsprocessen ska produkten ut till användaren. Denna aktivitet sker främst i överlämningsfasen men den måste planeras för tidigare i processen. (Rational Software, 1998)

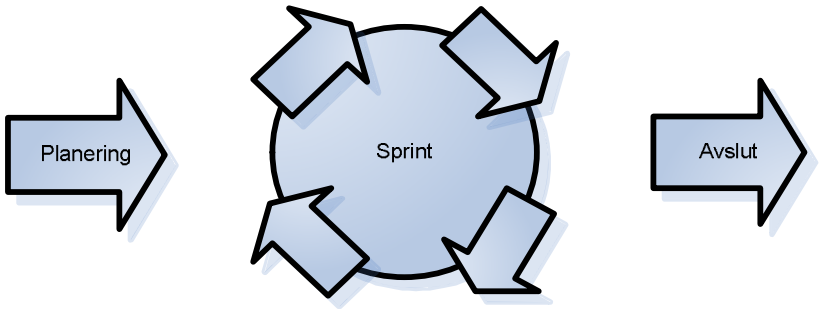
3.4.3 Roller, aktiviteter och artefakter

Enlig RUP definierar en roll vem som ska göra något i ett projekt, det vill säga det ansvar en individ har. Eftersom en person kan ha olika roller och ansvar inom ett och samma projekt så definieras en roll som ett ansvar snarare än individ. Aktiviteter definierar hur något ska göras och är det som en viss roll förväntas göra. Artefakt syftar till vad som ska göras och är den information som produceras, modifieras eller används i en process. Artefakten används som input av rollen då en aktivitet utförs. (Rational Software, 1998)

3.5 Scrum

Agil betyder lättrörlig och agila metoder är således ett gemensamt namn för olika lättrörliga metoder. Scrum är en agil metod med fokus på projektstyrning. (Agile Sweden, 2004) Ken Schwaber, en av Scrums skapare, menar att desto komplexare ett system är desto större är risken att den centrala styrningen kollapsar och att det är då Scrum kommer till sin rätt. (Schwaber, 2004) Det största problemet med Vattenfallsmetoden är att den är linjär och därmed kan den inte hantera oförutsedda händelser längs processen. För att avhjälpa detta konstruerades sprialmetoden där varje fas i Vattenfallsmetoden avslutas med en riskanalys och framtagande av en prototyp. Processen är dock fortfarande linjär. Scrum är en utveckling av iterativa metoder för att driva projekt. Metoden är tänkt att användas för utveckling av redan befintliga system. (Schwaber, 1995) Typiskt för Scrum är dagliga möten, korta iterationer och fortlöpande uppskattning av återstående tid för projektet. (Agile Sweden, 2004)

Scrum går ut på att den första fasen, planering, och den sista fasen, avslut, består av definierade processer med linjärt flöde förutom några iterativa steg i planeringsfasen. Däremellan liggande process kallas sprint som är en cykel som itereras och denna är mindre preciserad, se figur 11. Varje iteration innehåller därför kontroller och riskanalyser och sprintarna är således inte linjära. (Schwaber, 1995)



Figur 11: Projektprocess enligt Scrum.
(Modifierad figur från Schwaber, 1995)

Faserna delas in i tre grupper; pregame, game och postgame. I pregame ingår planering och systemarkitektur. Planeringsfasen går ut på att planera datum då produkten ska vara klar och uppskatta vilken kostnad projektet förväntas få. Det innebär även en riskanalys och bekräftelse från organisationens styre att utveckla produkten. Arkitektursteget innebär att förändringar som behövs ska identifieras men även vilka problem det finns med dessa förändringar. I game ingår utvecklingssprints som är iterativa cykler för utveckling. Ledtid, konkurrens, kvalitet och funktionalitet är nyckelbegrepp som itereras fram tills avslutningsfasen inträder. Gruppmöten är viktiga inslag. En sprint varar vanligtvis mellan en och fyra veckor beroende på produktens komplexitet och riskanalys. Postgame består av avslutningsfasen som inleds genom att ledningen anser att ovanstående nyckelbegrepp är redo. Integration, systemtest, användardokumentation och förberedelse av utbildningsmaterial är de huvudsakliga inslagen i avslutningsfasen. (Schwaber, 1995)

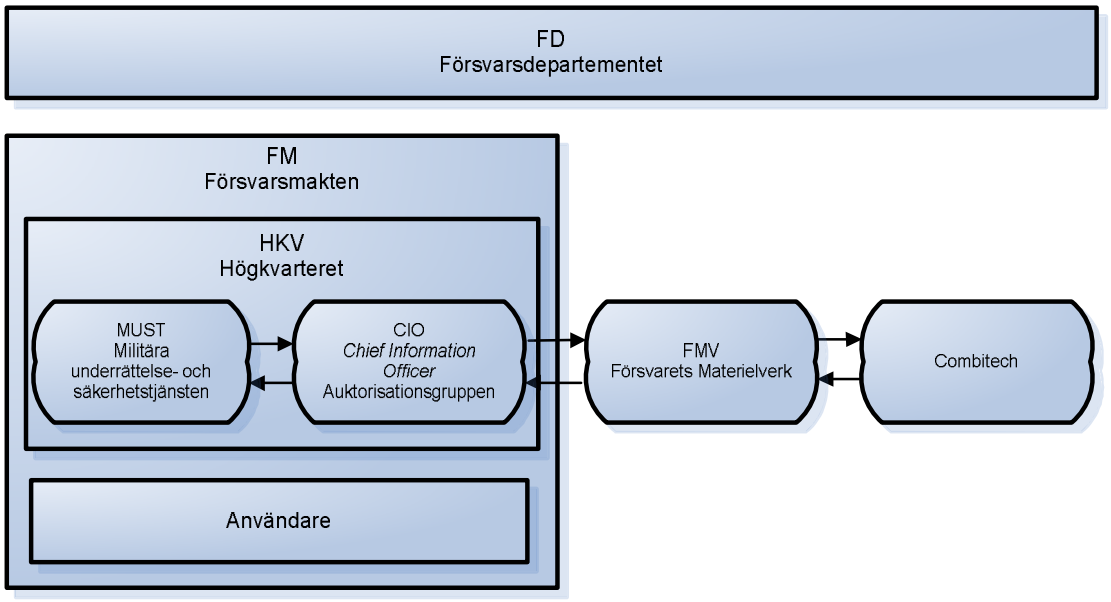
Metoden har tydliga riktlinjer vad gäller gruppstorlek, iterationslängd och samarbete i samma lokal, vilket innebär svårigheter för stora projekt. Därför har Scrum kritiserats för att vara olämplig för stora system där stora organisationer och outsourcing är inblandade. Scrum kritiseras även för problem med spårbarhet, det går att se vad som gjorts i de olika sprinterna men inte hur det har gjorts. (Computer Sweden, 2010a)

4. Försvarets organisation

I följande kapitel presenteras aktörer och roller inom Försvarsmakten för att underlätta förståelsen till auktorisations- och ackrediteringsprocessen.

4.1 Aktörer

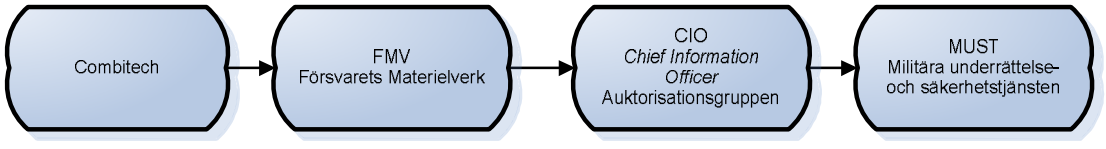
Nedan beskrivs de huvudaktörer som är verksamma i arbetet med auktorisation och ackreditering, se figur 12.



Figur 12: Försvarets organisation.

4.1.1 Försvarets materielverk

Försvarets materielverk, FMV, är fristående från Försvarsmakten och kan ses som en konsultfirma som stödjer Försvarsmakten vid upphandlingar av materiel av olika slag. När ett IT-system ska auktoriseras och ackrediteras är det FMV som tar kontakt med IT-konsulter för stöd. Ackrediteringsmaterialet skickas till CIO. Därefter skickas det vidare militära underrättelse- och säkerhetstjänsten, MUST, se figur 13. (Törnkvist, 2010)



Figur 13: Ackrediteringsärendets gång.

4.1.2 Chief Information Officer och auktorisationsgruppen

Chief Information Officer, CIO, är ansvarig för Försvarsmaktens informationssäkerhet. Dennes uppgift är att leda, utveckla samt kontrollera Försvarsmaktens informationssystem och informationsinfrastruktur. (Försvarsmakten, 2007a) CIO handlägger auktorisationsärenden och fattar auktorisationsbeslut. (Försvarsmakten, 2007b) CIO kontrollerar formalia i auktorisationsunderlaget, det vill säga att alla delar

som enligt DIT04 ska finnas med gör det. Om det blir godkänt skickas det vidare till MUST annars skickas det tillbaks till den som gjort ackrediteringsunderlaget för komplettering. (Törnkvist, 2010) CIO är chef för auktorisationsgruppen som bereder underlag till denne. I auktorisationsgruppen ingår även en ordförande. Små ärenden kan delegeras av CIO till ordföranden att fatta beslut i. Auktorisationsgruppen granskar underlag i beslutspunkterna B1-B4 i Försvarsmaktens livscykelanalys. (Nützman, 2010)

4.1.3 Militära underrättelse- och säkerhetstjänsten

Militära underrättelse- och säkerhetstjänsten, MUST, ska avge yttrande om IT-säkerheten till CIO. Efter att CIO har lämnat sakfrågan till MUST ska MUST tillsätta en handläggare och sedan lämna yttrande till CIO som bereder beslut. (Sunnegårdh, 2010) Det är MUST som ställer kraven och står för regelverket, till exempel MUST:s krav på säkerhetsfunktioner som har en central roll inom ackreditering. (Törnkvist, 2010) Efter att ett ärende beretts hos MUST undertecknas det av chef på MUST och därmed är systemet godkänt ur säkerhetssynpunkt och således ackrediterat. (Roswall, 2010)

4.2 Roller

Det finns några roller i processen som har stor betydelse när det gäller att fatta beslut och ta fram underlag. Dessa roller besitts av personer på Försvarsmakten och beskrivs nedan.

4.2.1 Produktägare

Produktägaren, som tillhör Högkvarteret, utses av CIO och är ansvarig för verksamheten kring IT-systemet. (Försvarsmakten, 2007b) Utvecklingsarbetet i livscykelmodellen beställs ofta av någon organisation utanför Försvarsmakten men det är produktägaren som är ansvarig och denne fattar beslut inom ramen för auktorisationsbeslut. Produktägaren ska se till att det finns resurser för att bereda beslut. När det är dags för avveckling är det produktägaren som fattar det beslutet. (Försvarsmakten, 2004, s. 52-53)

4.2.2 Produktansvarig

Produktansvarig utses av produktägaren och handlägger ärenden och tar fram beslutsunderlag åt denne. Många uppgifter som är den produktansvariges utförs i praktiken av någon annan, till exempel utvecklaren av IT-systemet. Produktansvarig ska se till att auktorisationsansökan sker och följa upp fattade beslut bland annat genom att se till att det finns ett auktorisationsbeslut innan fortsatt utveckling eller upphandlig sker. Rollen innebär även ansvar för framtagning av auktorisations- och ackrediteringsunderlag. (Försvarsmakten, 2004, s. 54-56)

4.2.3 Systemägare

Systemägaren är lokalt ansvarig för systemet, det vill säga chef för en organisationsenhet där IT-systemet ska användas. Lokalt ackrediteringsbeslut fattas av systemägaren. (Försvarsmakten, 2004, s. 58-59)

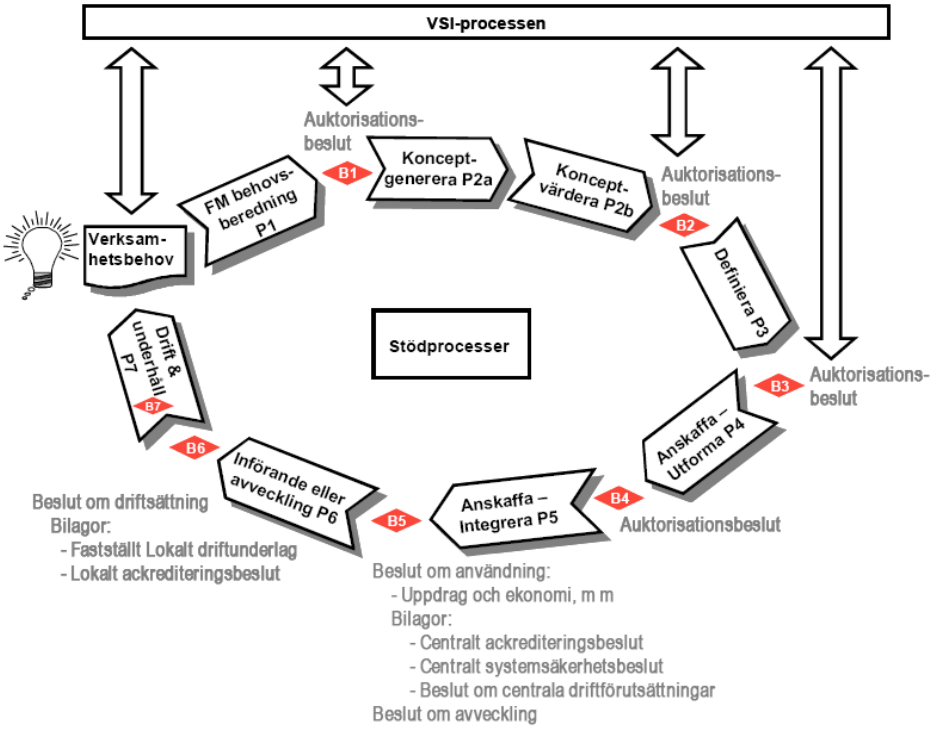
5. Auktorisation och ackreditering – en fallstudie

I följande kapitel redovisas auktorisations- och ackrediteringsprocessen utifrån Combitechs perspektiv. Combitech har kompetens att driva processen från början till slut, men kan även bistå genom att ta fram dokumentation i enstaka delar. Det är personer inom Försvarsmakten som fattar alla beslut medan Combitech bistår med metodkunnande, stöd och framtagande av underlag. I detta kapitel sker först en introduktion till begreppen auktorisation och ackreditering, därefter följer en beskrivning av processen utifrån dess olika beslutssteg.

5.1 Introduktion till processen

Varje IT-system genomgår en livscykel i form av realisering, användning, utveckling och avveckling. För Försvarsmaktens IT-system hanteras detta genom en auktorisationsprocess där varje del i livscykeln omfattas av ett auktorisationsbeslut. Ackreditering är ett av dessa auktorisationsbeslut och innebär ett formellt driftgodkännande som ska ges innan ett IT-system inom Försvarsmakten tas i bruk.

Combitechs arbete med ackreditering och auktorisation utgår från ”Direktiv för Försvarsmaktens IT-verksamhet”, DIT04, som beskriver såväl ackrediterings- som auktorisationsprocessen utifrån en så kallad livscykelmodell, se figur 14.

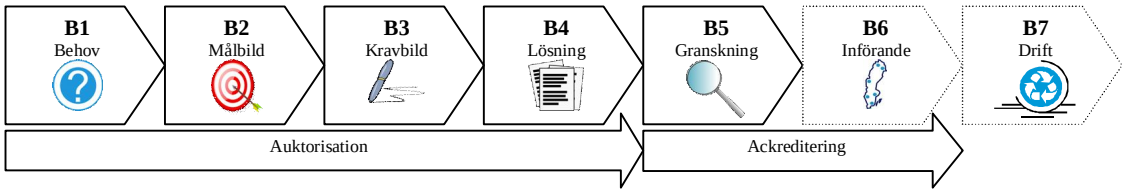


Figur 14: Försvarsmaktens livscykel för IT-system.

(Försvarsmakten, 2004, s.36)

Auktorisationsprocessen består av sju beslutspunkter, B1-B7. I det första beslutssteget, B1, är det behovet som är det centrala. Inför det andra beslutssteget, B2, sätts en säkerhetsmålsättning upp. Till det tredje beslutssteget, B3, tas en preliminär teknisk

specifikation fram. I B3 utformas även en preliminär systembeskrivning som sedan fastställs i det fjärde beslutssteget, B4. Det femte beslutssteget, B5, innebär en granskning av IT-systemet. Denna granskning utförs utifrån säkerhetsmålsättningen som tagits fram i B2 samt MUST:s krav på säkerhetsfunktioner med systembeskrivningen i B4 som underlag. Det är således viktigt att systembeskrivningen är utförligt skriven i fråga om informationssäkerhet så att det går att säkerställa vilka mål och krav som är uppfyllda. Ett godkännande innebär att IT-systemet är centralt ackrediterat och att beslut om användning kan fattas. (Bergengren, 2010)



Figur 15: Beslutspunkter i auktorisations- och ackrediteringsprocessen.

Beslut B1-B4 fattas av auktorisationsgruppen medan B5 fattas av produktägaren. (Andersson, 2010) Försvarsmaktens livscykel för IT-system behandlar även B6, som rör lokal ackreditering och B7 som rör beslut under drift. I B6 och B7 deltar Combitech vanligtvis inte. (Sunnegårdh, 2010) Således kan Combitechs deltagande i auktorisation och ackreditering ses som en linjär process, till skillnad från Försvarsmaktens process som är en livscykel, se figur 15. Då det är Combitechs arbete som studeras koncentrerar jag mig i denna uppsats på beslutspunkt B1-B5.

Processen följs inte alltid som det är tänkt, ibland är det ett redan befintligt IT-system som ska ackrediteras och ibland är det ett nytt IT-system som kommit en bit in i processen som ska ackrediteras. Auktorisationsgruppen har beslutat att det inte får gå mer än 18 månader mellan varje auktorisationsbeslut. Det innebär att underlaget från föregående beslutssteg måste göras om om det gått längre tid än så. (Andersson, 2010)

5.1.1 Auktorisation

Auktorisation är ett beslut under en utvecklingsfas, i detta fall ackrediteringsprocessen. (Försvarsmakten, 2004) Det är ett bemyndigande som ansöks om i fyra beslutspunkter, B1-B4. (Sunnegårdh, 2010) Auktorisation innebär samordning av IT-utveckling men det ger även en möjlighet för Försvarsmakten att centralt stödja, inrikta och kontrollera sina IT-system. (Försvarsmakten, 2004)

Även avveckling faller in under auktorisation. (Nützman, 2010) Utöver den tekniska prövningen fyller auktorisation även en ekonomisk funktion. Genom att se beslutsprocessen som *gater* som inte får passeras om inte vissa krav är uppfyllda så ökar möjligheten för Försvarsmakten att stoppa projekt som annars bara kommer att kosta pengar utan att de går att använda i slutändan. På samma sätt ges indikationer på när ett projekt är lönsamt att släppa vidare i projektprocessen. (Törnkvist, 2010) En mellanväg är att styra om inriktningen för ett projekt. (Bergman, 2010)

Ett auktorisationsbeslut måste fattas kring all verksamhet som rör ett IT-system inom Försvarsmakten och beslutet fattas av CIO. Underlagen till beslutspunkterna kommer in från produktägaren eller dennes handläggare, produktansvarig. Underlagen skickas till auktorisationsgruppen som gör en övergripande kontroll av innehållet och försäkrar sig om att allt som ska finnas med gör det. Chef för auktorisationsgruppen är CIO.

Auktorisationsgruppen berörs av beslutspunkterna B1-B4. Indata till respektive beslutsunderlag är alltid föregående auktorisationsbeslut, det vill säga föregående auktorisationsbeslut innehåller synpunkter på vad nästkommande underlag ska innehålla. Beslutspunkterna slås ibland samman, vanligast är då att B2 och B3 slås samman, men alla fyra beslutstegen kan slås samman till ett. (Nützman, 2010) Auktorisationsprocessen har en lång handläggningstid vilket innebär svårigheter med kontinuiteten. Enligt DIT04 ska underlag till B1 lämnas in och sedan ska beslut från CIO inväntas innan arbetet med B2 tar vid. För att uppnå kontinuitet och för att minska kostnader fortsätter arbetet ofta med efterföljande beslutssteg innan auktorisationsbeslutet kommer. Om arbetet är på rätt spår innebär detta att tid och pengar sparas. Är arbetet istället på fel spår blir det mycket dyrt och tidsödande. (Sunnegårdh, 2010)

En stor nytta med auktorisation är samordning. Det finns ett stort antal IT-system som ska nyutvecklas eller vidareutvecklas och lösningen till ett av dem kan vara lösningen till fler och därmed uppnås effektivisering. (Sunnegårdh, 2010) Genom auktorisation undviks en situation där hjulet uppfinns flera gånger, lösningar går att återanvända och olika enheter kan dra nytta av varandras erfarenheter. Därmed sparas även pengar. (Lindskog, 2010) Auktorisationsprocessen börjar med att ett behov uppstår och detta kan uppstå vart som helst i organisationen, till exempel på ett förband. Genom att framföra detta behov till auktorisationsgruppen kan då den tala om huruvida det redan finns ett IT-system som stödjer behovet eller inte. Det innebär även att de IT-system som utvecklas är kompatibla med varandra så att ett förbands IT-system inte är oförenliga med IT-system som används någon annanstans i organisationen. (Nützman, 2010) Om auktorisationsprocessen påbörjas i tid och följs som den är tänkt så utgör den även ett stöd för verksamheten genom riktlinjer och direktiv för när och hur olika moment ska utföras. (Eklöf, 2010) För Försvarsmakten som organisation innebär det att de får kontroll över sin IT-verksamhet. (Nützman, 2010) Nackdelen är att det är tidskrävande och att det inte alltid är anpassat till hur IT-system utvecklas och anskaffas i verkligheten. (Sunnegårdh, 2010)

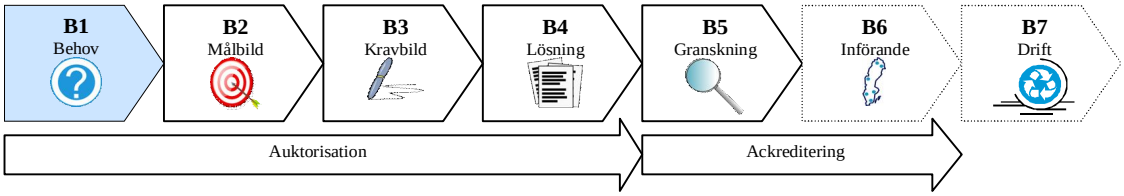
5.1.2 Ackreditering

Ett IT-system i Försvarsmakten måste uppfylla en rad förordningar, till exempel svensk lag och Försvarsmaktens regler. Ackrediteringsprocessen säkerställer att IT-systemet uppfyller dessa. Ackreditering innebär en stor nytta för produktägaren som därmed vet att det är ett säkert IT-system som han eller hon överlämnar för drift. (Sunnegårdh, 2010) I ackrediteringsprocessen reder man ut vilken typ av information som ska finnas i IT-systemet, hur den ska användas och hur den behöver skyddas utan att det byggs in för mycket säkerhetsfunktioner med avseende på informationssäkerhet i IT-systemet. Mer säkerhetsfunktioner leder till ett komplexare IT-system som kan leda till sämre systemsäkerhet och försvåra användning och därför bör inte en orimligt hög nivå hållas på skyddet av informationen. Genom ackreditering säkerställs att det IT-system som utvecklas verkligen håller en tillräckligt hög nivå vad gäller informationssäkerhet. (Lindskog, 2010)

Auktorisationsbeslut B5 är ett driftgodkännande ur IT-säkerhetssynpunkt och en del i B5 är centralt ackrediteringsbeslut. (Sunnegårdh, 2010) Ackreditering bygger på att det finns en kravbild och sedan mäts objektet, det vill säga IT-systemet, efter hur väl det uppfyller kravbilden. (Gruppintervju, 2010) Informationssäkerheten ska säkerställas främst för sekretessbelagda uppgifter men det finns även andra uppgifter som ska

skyddas. Alla IT-system måste gå igenom auktorisation men det är endast de som är sekretessbelagda som måste ackrediteras. Det är dock väldigt sällan som IT-system inte berörs av sekretess. Det är inte bara rikets säkerhet utan även personlig sekretess som ska beaktas. Om MUST i B4 beslutar att IT-systemet måste ackrediteras går det vidare till B5, annars driftsätts det efter B4. (Roswall, 2010) Ett exempel på ett IT-system som måste gå igenom auktorisationsprocessen men inte behöver ackrediteras är en pulsklocka. Den är ett IT-system, om än litet, men berörs inte av sekretess eller känsliga uppgifter. (Nützman, 2010) Spårbarheten i IT-systemet är viktigt för att kunna påvisa vem, när och hur eventuellt intrång har skett. (Försvarsmakten, 2006a, s. 157-159)

5.2 B1 – Behovet



Figur 16: I B1 är det behovet som är det centrala.

I beslutsunderlaget till B1 är det behovet som är det centrala, se figur 16. (Andersson, 2010) Det är viktigt att motivera problem, behov och nytta med införandet av ett nytt IT-system och vilken verksamhet det ska stödja. Underlaget till B1 bör innehålla vilken typ av IT-system det rör sig om, en övergripande systemlösning samt avgränsningar. Det ska dessutom finnas förslag på hur IT-systemet ska finansieras, initial kostnads-, och nyttoanalys, samt tidsaspekter, det vill säga planerad driftsättning och så vidare. I det här steget fastställs roller så som produktägare och vilken avdelning IT-systemet ska tillhöra. (Eklöf, 2010) Det är långt ifrån alltid som det finns en idé på hur ett behov ska lösas redan i det här stadiet. Det är inte heller meningen att fokus ska ligga på förslag till lösning. Om ett lösningsförslag lämnas är det på konceptnivå och utan detaljer. B1 fokuserar på informationssäkerhet i förstahand, någon form av skattning av IT-systemets informationsklassning måste finnas med, åtminstone en uppfattning om huruvida det är öppet eller hemligt. Vilken klassning ett IT-system får har stor inverkan på dess kostnad. Auktorisationsgruppen tar beslut om huruvida IT-systemet ska genomgå fullständig ackreditering eller om processen endast ska följas fram till att ett tekniskt ackrediteringsunderlag tas fram. En del IT-system behöver inte ackrediteras, endast auktoriseras och det beslutet fattas här. Även detta innebär en stor skillnad i kostnad för Försvarsmakten. (Gruppintervju, 2010)

Finansieringen är en viktig del av beslutsunderlaget till B1. Tanken är att auktorisationsgruppen ska ha kontroll över när det går att återanvända gamla lösningar. Den som kommer med en idé är inte alltid insatt i helheten. I detta steg kan auktorisationsgruppen upptäcka om det finns något liknande IT-system som kan nyttjas. Med hjälp av detta uppnås kostnadseffektivitet. Det fungerar dock inte alltid i verkligheten eftersom det finns så många IT-system att det inte går att ha kontroll över alla. Auktorisationsgruppen har förutom egna erfarenheter en databas till stöd för detta. (Gruppintervju, 2010)

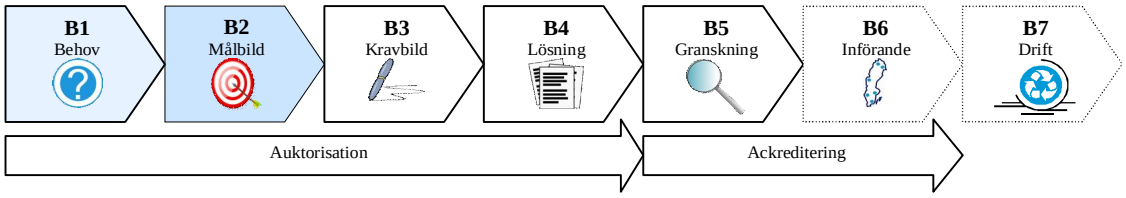
Auktorisationsgruppen bestämmer i det här steget vilka underlag de vill ha in för kommande beslutspunkter. Detta beror på vilken typ av IT-system det rör sig om. (Nützman, 2010) Det är mycket ovanligt att ett IT-system inte går vidare från den här

punkten, det händer i stort sett bara om det redan finns ett annat IT-system som är likvärdigt. Ofta går B1-ansökan igenom men med särkskilda direktiv av olika slag. (Roswall, 2010)

Metoden som används i ett initialt skede är små möten där intressenter samlas. (Andersson, 2010) Arbetet går ut på att samla information och sammanställa i en rapport. (Eklöf, 2010) Det underlättar om alla involverade är medvetna om DIT04:s livscykelmodell. Att människor slutar och kommer till i projektet har också inverkan på hur smidigt processen fortlöper. (Andersson, 2010)

5.3 B2 – Målbild

Inför den andra beslutspunkten är det målen som är det viktiga, IT-systemet finns fortfarande bara i teorin, se figur 17. (Andersson, 2010) Nedan följer en beskrivning av de dokument som ingår i underlaget.



Figur 17: I B2 är det målbilden som är det centrala.

5.3.1 Utkast taktisk-teknisk-ekonomisk målsättning

UTTEM är utkastet till taktisk-teknisk-ekonomisk målsättning, TTEM. UTTEM beskriver behovet som föranlett utvecklingen av ett nytt IT-system. Det är Försvarsmaktens målsättningsdokument, en kravbild från Försvarsmakten som beställare till FMV som uppköpare. (Yngvesson, 2010)

Det viktigaste momentet är att reda ut vilka intressenter som finns i form av myndigheter och organisationer. Utkastet ska innehålla grunderna i vad som behövs, hur mycket det får kosta och hur det stöttar verksamheten. Utkastet utvecklas i B3 till en preliminär taktisk-teknisk-ekonomisk målsättning, PTTEM, och i B5 slutlig taktisk-teknsik-ekonomisk målsättning, STTEM, det vill säga det är en utveckling av samma dokument. (Lindskog, 2010)

5.3.2 Säkerhetsmålsättning

Säkerhetsmålsättningen innehåller analyser, krav, bedömningar och säkerhetsmål för IT-systemet och ligger således till grund för säkerheten i och kring IT-systemet. Syftet är att identifiera kravbilden ur säkerhetssynpunkt. (Yngvesson, 2010) IT-systemet måste skyddas ur två perspektiv. Dels behöver det skyddas så att det alltid finns tillgängligt för verksamheten, och dels behöver informationen i IT-systemet skyddas. (Försvarsmakten, 2006a, s.65) Säkerhetsmålsättningen kan liknas vid en husgrund. Utan den är det svårt att bygga ett hus och en bra husgrund är förutsättningen för att få ett bra hus. På samma sätt är en bra säkerhetsmålsättning av yttersta vikt för att det fortsatta auktorisations- och ackrediteringsarbetet ska lyckas. (Sunnegårdh, 2010) Säkerhetsmålsättningen är viktig både säkerhetsmässigt och kostnadsmässigt. (Gruppintervju, 2010)

Säkerhetsmålen ska beskrivas utifrån kraven avseende sekretess, tillgänglighet, riktighet samt spårbarhet. (Lindskog, 2010) Allting måste brytas ner till specifika fall för att det ska gå att använda vid granskning. (Andersson, 2010) Säkerhetsmålsättningen ska även innefatta en övergripande systembeskrivning som beskriver vilka delar IT-systemet består av, de externa gränsytorna, gränsytor mot användaren samt vilken miljö IT-systemet är tänkt att användas i. (Andersson, 2010) För ett komplext IT-system kan analyserna behöva arbetas om några gånger. (Försvarsmakten, 2006a, s. 67, 77)

Ytterligare en nytta med säkerhetsmålsättningen är att krav som är i konflikt med varandra kan upptäckas. Det är såväl informationssäkerhet som kostnad och systemsäkerhet som ska beaktas och dessa strider ibland mot varandra. Informationssäkerhetskrav tillgodoses ofta enklast genom att göra IT-systemet så låst som möjligt medan systemsäkerhet innebär att IT-systemet ska vara så lättåtkomligt som möjligt. Ett exempel på det är inloggning. Ur informationssäkerhetssynpunkt är det bra att ha ett så låst IT-system som möjligt, där det ställs krav på att det ska vara lösenord i kombination med nyckel för systemåtkomst och där det dessutom ställs specifika krav på lösenordet. För att garantera systemsäkerhet och därmed tillgång till IT-systemet är det mer fördelaktigt att varken ha lösenord eller nyckel för åtkomst. (Andersson, 2010)

Till grund för säkerhetsmålsättningen ligger fyra olika analyser; verksamhetsanalys, säkerhetsanalys, författningsanalys samt hot-, risk- och sårbarhetsanalys. (Bergengren, 2010) Dessa analyser renderar krav som omsätts till säkerhetsmål och förs in i säkerhetsmålsättningen. Underlag till samtliga analyser förutom författningsanalysen är gruppövningar tillsammans med representanter från olika delar av organisationen, till exempel användare, systemkunniga, verksamhetskunniga men även beslutsfattare. En svårighet med dessa möten är att samla alla människor fysiskt. Analyserna ska alltid verifieras av de personer som deltagit vid dess skapande. (Andersson, 2010) (Yngvesson, 2010)

5.3.2.1 Verksamhetsanalys

Verksamhetsanalysen är en nulägesanalys av befintlig eller nyplanerad verksamhet, inom en organisation och mellan olika organisationer. Eftersom den ligger till grund för säkerhetsmålsättningen är den av stor vikt då även dessa blir fel om verksamhetsanalysen skulle bli fel. Allt som görs i efterkommande steg grundas på denna. (Roswall, 2010) Kraven som analysen renderar ska vara relevanta för övriga säkerhetsmål, men syftet med verksamhetsanalysen är också att auktorisationsgruppen ska förstå vilken verksamhet det rör sig om. (Eklöf, 2010) Det är viktigt att användarna och förbanden är delaktiga i utvecklingen av det nya IT-systemet så att en situation där förbanden inte kan ta det nya IT-systemet i drift uppstår. Driften behandlas annars inte förrän i B6 då IT-systemet redan är utvecklat. (Gruppintervju, 2010)

Användarfall är en aktivitet som utövas för att uppfylla ett mål. Genom att arbeta med användarfall kontrolleras till exempel att ett IT-system inte blir för stort fysiskt så att det inte får plats där det är tänkt att det ska stå. Kringprocesser är aktiviteter som inte har direkt koppling till verksamheten eller IT-systemet men som ändå har inverkan och det är därför lämpligt att utforma analysen efter användarfall och kringprocesser. Organisation, roller och ansvar för verksamheten och hur dessa kommer i kontakt med information ska definieras. Därefter ska informationsflödet i IT-systemet beskrivas. Denna beskrivning ska inkludera hur information rör sig mellan olika gränssnitt, vem

som tar del av den samt vilka andra verksamheter som information utbyts med och vad dessa verksamheter ställer för krav respektive vilka krav som ska ställas på dessa verksamheter. (Försvarsmakten, 2006c)

5.3.2.2 Säkerhetsanalys

Syftet med säkerhetsanalysen är att identifiera öppna uppgifter, hemliga uppgifter, utrikes hemliga uppgifter samt uppgifter som berörs av övrig sekretess, till exempel personlig sekretess. Hemliga uppgifter ska även informationsklassas, det vill säga delas in ytterligare enligt Hemlig/Restricted, Hemlig/Confidential, Hemlig/Secret eller Hemlig/Top Secret. En helhetssyn av IT-systemets klassificering ska också redovisas. (Försvarsmakten, 2006b) (Försvarsmakten, 2010) Om ett IT-system innehåller information av olika klassning måste den alltid klassas till den högsta klassen om det inte går att särskilja de olika delarna. Ökade krav ger ökade utvecklingskostnader så onödigt hög klassning bör undvikas. (Andersson, 2010) Hemliga och utrikesklassificerade uppgifter får bara användas i IT-system som är ackrediterade enligt den högsta informationssäkerhetsklassen som uppgifterna är placerade i. (Försvarsmakten, 2010) Informationsklassningen syftar även till att klargöra vilken av MUST:s kravmängd som informationen ska underordnas, det vill säga vilket krav på skydd som finns. (Andersson, 2010)

Säkerhetsanalysen syftar dessutom till att möjliggöra en identifiering av vilka lagar som informationen måste underställas och ligger således till grund för författningsanalysen. (Yngvesson, 2010) Säkerhetsanalysen avgränsas till den verksamhet och de IT-system som är upptagna i verksamhetsanalysen och ska omfatta såväl informationen i IT-systemet som de fysiska anläggningar som utgör IT-systemet. (Försvarsmakten 2006b) Det är viktigt att utröna informationsflödet inom, till och från IT-systemet för att kunna informationsklassa informationen. (Eklöf, 2010)

5.3.2.3 Författningsanalys

Syftet med författningsanalysen är att identifiera lagrum och hur dessa uppfylls och ska således innehålla lagar och förordningar. Viktiga indata är därför Sveriges lagar, Försvarets författningssamling och Försvarets interna bestämmelser. (Sunnegårdh, 2010)

Författningsanalysen finns inte specifikt upptagen i beslutsunderlaget som DIT04 behandlar eftersom lagar och regler alltid ska uppfyllas oavsett vad det är för IT-system. Det underlättar dock att skriva en författningsanalys för att skapa specifika krav att föra in i säkerhetsmålsättningen. Det underlättar även spårbarheten då det ska vara tydligt var alla krav kommer ifrån. (Bergman, 2010)

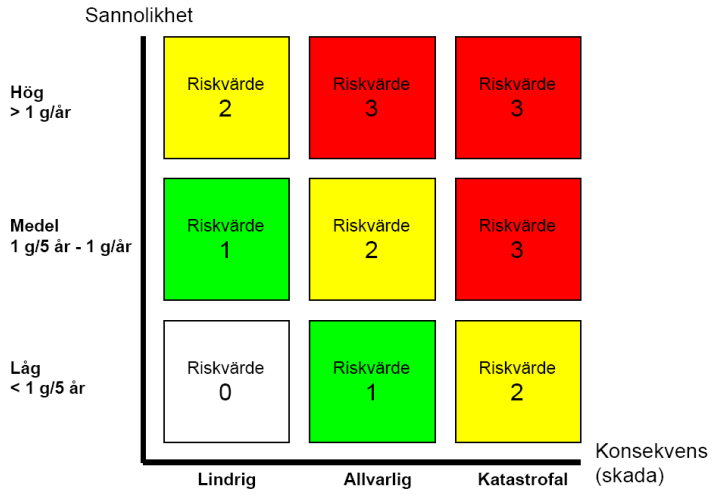
5.3.2.4 Hot-, risk- och sårbarhetsanalys

Hot-, risk- och sårbarhetsanalysen syftar till att ta fram ett antal hot mot verksamheten och IT-systemet och analysera dessa utifrån sannolikhet, konsekvens samt förslag till krav. (Försvarsmakten, 2006d)

Under analysens gång är det bra att ha följande frågor i åtanke (Andersson, 2010):

- Vilken exponering av gränsytor är det?
- Vilken spridning har IT-systemet?
- Är det i enlighet med säkerhetsanalysen?
- Om en incident inträffar, kan IT-systemet överleva ändå?
- Finns det fara för liv?

I analysen undersöks scenariofall. (Andersson, 2010) Deltagare i analysgruppen får ange värde på sannolikhet och konsekvens för olika hot som sedan viktas samman till ett riskvärde, se figur 18. (Försvarsmakten, 2006d)



Figur 18: Viktning av sannolikhet och konsekvens till riskvärde.
(Försvarsmakten, 2006d)

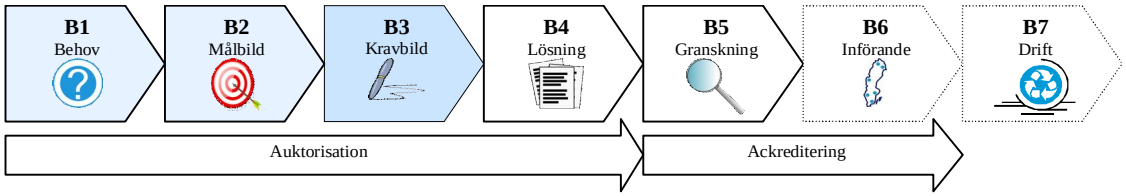
Hot med lågt riskvärde kan ignoreras medan hot med högt riskvärde tas med i säkerhetsmålsättningen. (Yngvesson, 2010) Dubbletter sorteras bort och hoten sorteras i prioritetsordning. Hoten klassas även med en kod utifrån sekretess, tillgänglighet, riktighet, spårbarhet och hot av allmän karaktär. (Bergengren, 2010)

5.3.3 Eventuellt förslag på realiseringslösning

Förslag på realiseringslösning är en beskrivning av IT-systemet. Detta kan finnas redan i behovsstadiet, och då kan det underlaget användas för vidareutveckling. (Yngvesson, 2010) Även offerter som skickas in från tillverkare används som underlag till förslag på realiseringslösning. (Lindskog, 2010) I dokumentet föreslås en lösning sett till behovet. Det kan till exempel vara förslag på komponenter eller hur de ska integrera. Ibland handlar det om designprinciper som förslag på vilket operativsystem som önskas användas. Om det inte finns några önskemål på hur IT-systemet ska se ut behöver förslag på realiseringslösning inte skrivas. Förslag på realiseringslösning kan även skrivas för att IT-systemet ska skapas på ett sätt så att vissa säkerhetsmål ska kunna tas bort. Det är en iterativprocess och det händer att den utformas i samarbete med industrin. (Andersson, 2010)

5.4 B3 – Kravbild

I beslutsunderlag till B3 ska IT-systemet beskrivas och lösningen ska bedömas, kravbilden ska tas fram, se figur 19. (Andersson, 2010) Beslutspunktens viktigaste dokument är den preliminära systembeskrivningen. (Sunnegårdh, 2010) Beslutsunderlaget består även av en preliminär teknisk kravspecifikation samt en redovisning av ändringar av inlämnat B2-underlag. Den taktisk-teknsika-ekonomiska målsättningen utvecklas i det här stadiet och dessutom ges en möjlighet att utveckla verksamhetsanalysen. (Försvarsmakten, 2004, s. 79)



Figur 19: I B3 är det kravbilden som är det centrala.

Då B3 inleds ska säkerhetsmålsättningen redan vara godkänd. I praktiken är det ovanligt att det sker utan restpunkter. (Gruppintervju, 2010) B3-beslutet ska tas innan upphandling sker och innebär ett beslut om att utveckling ska genomföras, en upphandlingsspecifikation tas fram. (Gruppintervju, 2010) Det viktigaste momentet är nätverks- och kommunikationslösningar, då dessa är svårast att skydda. Resultatet som ska komma ur det här steget är en beskrivning över hur IT-systemet ska se ut. Det ska finnas en lista över programvaror, licenser et cetera. (Nützman, 2010) Indata till B3 är också B2-beslutet. I verkligheten påbörjas detta steg ibland utan inväntat B2-beslut på grund av tidsbrist. (Sunnegårdh, 2010) Det är också vanligt att B2 och B3 slås samman för att inte dra ut på processen i onödan, speciellt då det är en redan färdig produkt som ska inhandlas. (Gruppintervju, 2010)

5.4.1 Preliminär teknisk kravspecifikation

Den preliminära tekniska kravspecifikationen syftar till att omsätta säkerhetsmålen till tekniska krav. (Yngvesson, 2010) Genom den preliminära tekniska kravspecifikationen börjar IT-systemet växa fram. Säkerhetsmålen bryts ner i bitar och även MUST:s krav på säkerhetsfunktioner inbegrips. Dessa ska alltid vara täckta. Kravspecifikationen är inriktad på informationssäkerhet. Det är en mappning från mål till funktioner. (Andersson, 2010) Kraven måste vara mätbara, konkreta och verifierbara, de måste gå att testa. (Yngvesson, 2010) En bra metod att använda är gruppövningar där den tekniska kravspecifikationen successivt växer fram. Användargrupperna kan användas till att skissa upp användarfall. Hänsyn måste tas till huruvida IT-systemet är autonomt eller inte, det vill säga om det kommunicerar med andra IT-system. För IT-system som inte är autonoma måste krav ställda av ansvariga för de IT-system som systemet kommunicerar med inkluderas. (Sunnegårdh, 2010)

5.4.2 Preliminär systembeskrivning

I en preliminär systembeskrivning ska IT-systemet beskrivas så långt det går. Det finns fortfarande inte i realiteten och det finns inte heller en utvald leverantör. Systembeskrivningen är den centrala dokumentationen av IT-systemet. Denna kompletteras med manualer, drivrutiner et cetera. (Lindskog, 2010) Produktägaren behöver en systembeskrivning men den används även för samordning med andra IT-

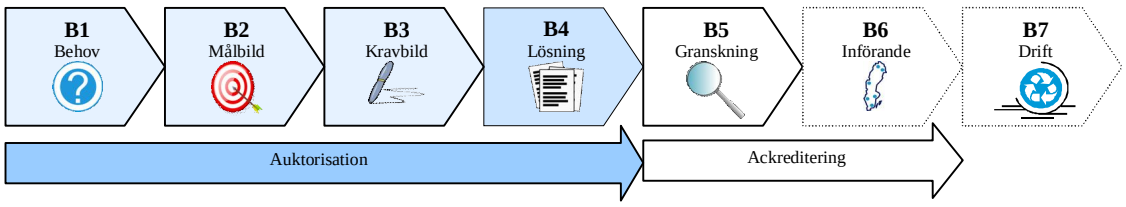
system. Genom systembeskrivningen kan det utrönas om det finns delsystem eller komponenter som ingår i systemet som redan är godkända. I sådana fall behöver de inte godkännas igen. Är komponenterna inte godkända kan det hända att de inte får användas och istället ska bytas ut mot redan godkända komponenter. (Eklöf, 2010) Auktorisationsgruppen ansvarar för detta. (Andersson, 2010) Systembeskrivningen används även för granskning av IT-systemet senare i processen. (Sunnegårdh, 2010)

Den preliminära systembeskrivningen ska spegla den preliminära tekniska kravspecifikationen. (Andersson, 2010) Vikten läggs på säkerhetsmekanismer och säkerhetsfunktioner. (Gruppintervju, 2010) Systembeskrivningen delas upp enligt funktionell design, lågnivådesign och implementation. (Andersson, 2010) Domäner, operativsystem, hårdvara och gränssnitt är exempel på sådant som ska definieras. (Jönson, 2010)

5.4.3 Redovisa ändringar av inlämnat B2-underlag med versionshantering

I detta dokument redovisas hur direktiv från auktorisationsgruppen i föregående beslut har följts. Ett exempel på direktiv kan vara att det ska samordnas med något annat projekt och då ska det redovisas i detta dokument hur detta har gått till. Även andra ändringar som gjorts sedan föregående beslutssteg redovisas i detta dokument, exempelvis om förutsättningar ändrats. Ändringarna kan gälla allt från hänvisningar till hela avsnitt. Versionshantering innebär att det ska framgå vilka tidigare versioner som finns av ett dokument, till exempel säkerhetsmålsättningen, och att ändringar i de olika versionerna kan spåras. Redovisning av ändringar med versionshantering gäller för alla beslutsunderlag. (Nützman, 2010)

5.5 B4 – Lösning



Figur 20: I B4 är det lösningen som är det centrala.

I beslutsunderlag till B4 finns IT-systemet i realiteten och ska testas och granskas. Det är lösningen som är det viktiga, se figur 20. Den preliminära systembeskrivningen blir definitiv i det här steget. Utöver systembeskrivningen är granskningsrapporten central i underlaget. Granskningsrapporten är en avstämning mellan kraven från säkerhetsmålsättningen och MUST:s krav på säkerhetsfunktioner utifrån systembeskrivningen. (Försvarsmakten, 2004, s.79) Till grund för denna ligger verifierings- och valideringsrapporten. Vid verifiering visas hur kraven är uppfyllda och validering innebär att IT-systemet inte bara uppfyller kraven utan att kraven varit tillräckliga. Även en integrationsplan som är en plan för hur IT-systemet ska integreras med andra IT-system är en del av underlaget. (Yngvesson, 2010) Liksom i underlaget till B3 ska en redovisning av inlämnat B3-underlag med versionshantering göras. (Försvarsmakten, 2004, s.79)

I B4 levereras IT-systemet till FMV tillsammans med en systembeskrivning. (Sunnegårdh, 2010) Därefter testas IT-systemet och det är sista steget i

auktorisationsprocessen innan går det över till ackreditering. (Gruppintervju, 2010) Det är sista chansen att testa om IT-systemet har förutsättning att fungera i verkligheten. CIO kräver till exempel en kontroll av att de som ska sätta IT-systemet i drift verkligen klarar av det. Det är mycket sällsynt att IT-system misslyckas i det här skedet, auktorisationsgruppen ger istället restpunkter om det behövs, men IT-systemet får ändå gå vidare i processen. Det kan falla på att vissa krav inte är uppfyllda. (Nützman, 2010) Indata till B4 är B3-beslut, preliminär systembeskrivning samt information om vad som är upphandlat. (Sunnegårdh, 2010)

5.5.1 Systembeskrivning

Systembeskrivningen är en vidareutveckling av den preliminära systembeskrivningen från B3, skillnaden är att den är slutgiltig i det här steget. Dessutom har nu upphandlingen skett så leverantören är känd och denne får betydelse för systembeskrivningen eftersom det nu finns en lösning, det är känt hur IT-systemet verkligen ser ut. Leverantören kan vara med och specificera systembeskrivningen. (Sunnegårdh, 2010) (Yngvesson, 2010) Synpunkter som auktorisationsgruppen lämnat på den preliminära systembeskrivningen från B3 beaktas. (Eklöf, 2010) Det är oerhört viktigt att en ordentlig kravspecifikation är gjord för att det ska bli en bra systembeskrivning. (Sunnegårdh, 2010)

5.5.2 Granskningsrapport

Granskningrapport benämns ibland även evalueringsrapport. Evaluering är granskning mot givet kriteria, i det här fallet är det en granskning av hur kravbilden uppfylls. (Andersson, 2010) Granskningsrapporten är en avstämning mellan kraven från säkerhetsmålsättningen och MUST:s krav på säkerhetsfunktioner mot systembeskrivningen. Därför är det viktigt att systembeskrivningen behandlar säkerhetsaspekterna av IT-systemet, inte bara de tekniska funktionerna. Om det inte finns beskrivet i systembeskrivningen hur ett visst krav är uppfyllt innebär det problem med spårbarheten. (Yngvesson, 2010)

Kopplingen mellan systembeskrivningen och säkerhetsmålsättningen respektive MUST:s krav på säkerhetsfunktioner är central. Det reds ut vilka krav som är uppfyllda och vilka som inte är uppfyllda. (Lindskog, 2010) Samtliga krav från säkerhetsmålsättningen ska hanteras. (Yngvesson, 2010) Den som utför granskningen måste sätta sig in i det IT-system som ska granskas och det görs med hjälp av systembeskrivningen. Sedan ska kravbilden hanteras. Det händer, men är ovanligt, att IT-system uppfyller samtliga krav. Då det kvarstår icke uppfyllda krav är det upp till produktägaren att fatta beslut om hur detta ska hanteras. Det är upp till denne att bestämma huruvida IT-systemet med kvarstående åtgärder ska driftsättas eller inte och om driftsättningen i sådana fall ska ske med eller utan restriktioner. En restriktion kan till exempel vara att IT-systemet får tas i drift under förutsättning att kravet åtgärdas inom en viss tid. En annan restriktion kan vara att IT-systemet får tas i drift men endast under vissa förutsättningar. (Bergman, 2010) Granskningen ska vara oberoende och därför ska det helst inte vara den person som har gjort systembeskrivningen som utför granskningen. (Lindskog, 2010)

I granskningen mot MUST:s krav på säkerhetsfunktioner kontrolleras leverantörens processer, exempelvis undersöks loggningsfunktioner, säkerhetslogg såväl som vanlig teknisk logg. Säkerhetsloggen är mest intressant ur informationssäkerhetssynpunkt och

utreds utifrån vem som har tillgång till den. Ett exempel på krav på säkerhetsfunktion är att systemadministratören inte ska ha tillgång till säkerhetsloggen eftersom denne då kan gå in och ändra i den. I granskningen säkerställs att detta verkligen är uppfyllt. (Dzaferagic, 2010)

Det är den faktiska lösningen som ska granskas, det vill säga det faktiska IT-systemet och dess dokumentation. Det går inte att granska mot kravspecifikation och helst ska det vara en helt färdig lösning annars ändras förutsättningarna. Man kan ibland göra en förgranskning på hur IT-systemet uppfyller kraven på säkerhetsfunktioner i ett preventivt syfte. (Andersson, 2010)

5.5.2.1 Kvarstående åtgärder

Kvarstående åtgärder är de åtgärder som måste vidtas för att kravbilden från MUST:s krav på säkerhetsfunktioner samt säkerhetsmålsättningen ska anses uppfylld. De krav som fått utlåtande ”ej uppfyllt” flyttas till detta dokument som identifierade brister. Till varje identifierad brist ges ett åtgärdsförslag. Krav på åtgärd innebär att det endast krävs en engångsinsats för att kravet ska anses uppfyllt. (Bergengren, 2010) (Eklöf, 2010)

5.5.2.2 Krav på användning

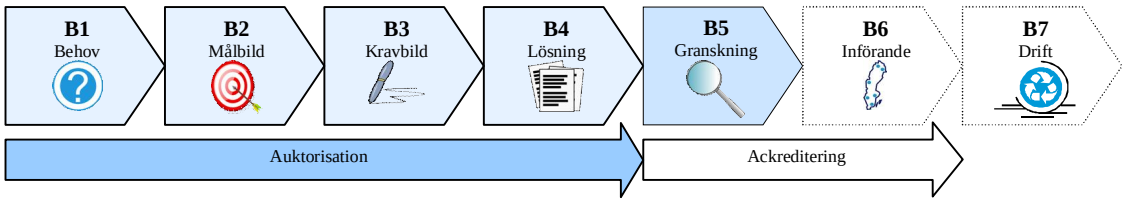
De krav som fått utlåtandet Krav på användning i granskningsrapporten och verifieringsrapporten listas i dokumentet Krav på användning som kan ses som en checklista bestående av restriktioner som måste uppfyllas för att kravbilden från MUST:s krav på säkerhetsfunktioner samt säkerhetsmålsättningen ska anses uppfylld. Krav på användning är ett levande dokument som måste följa IT-systemet genom hela dess livslängd, till skillnad från de krav som listas i Kvarstående åtgärder där det endast krävs en engångsåtgärd för att kravet ska vara uppfyllt. Krav på användning kan till exempel vara att driftjournal måste föras. Detta är ingen engångsåtgärd, utan måste ske kontinuerligt. (Bergengren, 2010) (Eklöf, 2010)

5.5.3 Verifierings- och valideringsrapport

Verifiering och validering innebär att IT-systemet testas och granskas ur säkerhetssynpunkt. Informationen ska skyddas såväl inom den egna verksamheten som mot utomstående. (Roswall, 2010) Det krävs en uppsättning av IT-systemet för att kunna verifiera och validera det. Även tillgång till systembeskrivningen och tillhörande dokumentation, till exempel handhavandedokument, designdokument och testdokument krävs. (Eklöf, 2010) En provmiljö med simulering sätts upp. Alla specificerade krav måste ha testfall och det ska vara ett fall för varje krav för att det ska godkännas. (Yngvesson, 2010)

Vid verifiering visas hur kraven är tillgodosedda. Systembeskrivningen ställs mot den tekniska kravspecifikationen. Vid validering testas att IT-systemet verkligen blev det önskade, det vill säga inte bara att IT-systemet uppfyller kraven, utan också att kraven varit tillräckliga. Validering går således ut på att se om IT-systemet gör det som var tänkt. (Eklöf, 2010) (Sunnegårdh, 2010) (Yngvesson, 2010) Verifiering och validering är viktigt ur informationssäkerhetssynpunkt men eftersom det är auktorisations- och ackrediteringsprocessen i stort, och inte några moment i detalj, som är det huvudsakliga studieobjektet i den här uppsatsen sker ingen vidare fördjupning i verifiering och validering här.

5.6 B5 – Granska

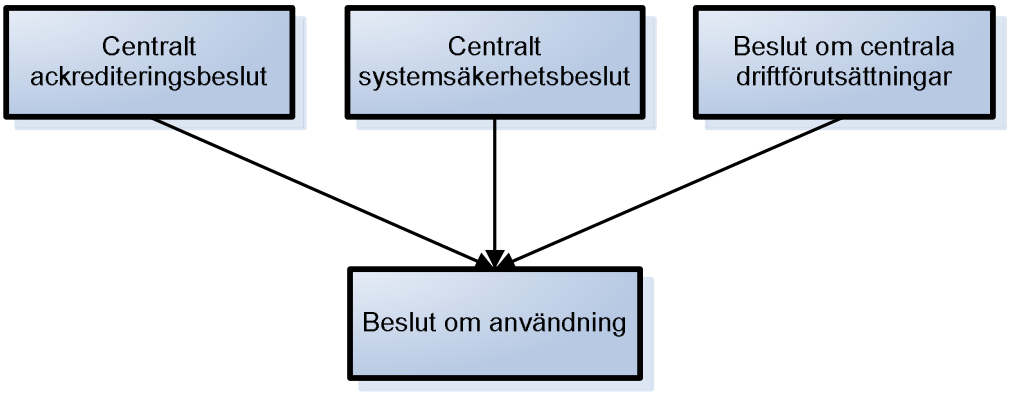


Figur 21: I och med att beslut B5 tas så är IT-systemet ackrediterat.

I B5 ska IT-systemet ackrediteras och beslutsunderlaget blir således ackrediteringsunderlag, se figur 21. (Andersson, 2010) Det viktigaste i B5-underlaget är det centrala och tekniska ackrediteringsunderlaget. Den taktisk-teknisk-ekonomiska målsättningen blir slutlig och verifieringsrapporten kan revideras i det här steget. (Försvarsmakten, 2004, s.79)

B5 är beslut om användning. (Gruppintervju, 2010) Det ska beslutas om IT-systemet ska användas, om det räcker att rätta till eventuella fel, eller om det ska läggas ned. (Dzaferagic, 2010) Då det har tagits ett beslut med hjälp av beslutsunderlaget så är IT-systemet ackrediterat och därmed godkänt att använda i Försvarsmakten. Med detta är IT-systemet ackrediterat centralt men måste även genomgå en lokal ackreditering på varje förband utifrån lokala förhållanden. (Roswall, 2010) B5 är central driftöverlämning medan B6 innebär lokal driftöverlämning. (Sunnegårdh, 2010)

För att beslut om användning ska kunna fattas vägs informationssäkerheten samman med systemsäkerhet samt centrala driftförutsättningar och förvaltning, se figur 22. (Andersson, 2010)



Figur 22: Förutsättningar för beslut om användning.

5.6.1 Centralt ackrediteringsunderlag

Syftet med centralt ackrediteringsunderlag är att produktägaren ska kunna fatta beslut om användning. (Sunnegårdh, 2010) Det centrala ackrediteringsunderlaget kan ses som en checklista för förbanden och i de fall då det är problem med driftsättningen på förbanden har det brustit i det centrala ackrediteringsunderlaget. (Bergman, 2010) Det är en sammanställning av information där helheten beaktas för ett IT-system. Det kan baseras på en eller flera tekniska ackrediteringsunderlag. I centralt ackrediteringsunderlag testas hur de olika tekniska ackrediteringsunderlagen fungerar

ihop. Dokumentet innehåller referenser till andra dokument som ligger till grund för ackrediteringsunderlaget. (Lindskog, 2010)

Ett centralt ackrediteringsunderlag gäller för IT-systemet oavsett vart det används. Hur kraven uppfylls på respektive förband är sedan systemägarens ansvar. Produktägaren bör i det centrala ackrediteringsunderlaget ange krav på lokala åtgärder som systemägaren måste hantera i det lokala ackrediteringsarbetet, eventuellt tillsammans med driftansvariga. (Lindskog, 2010)

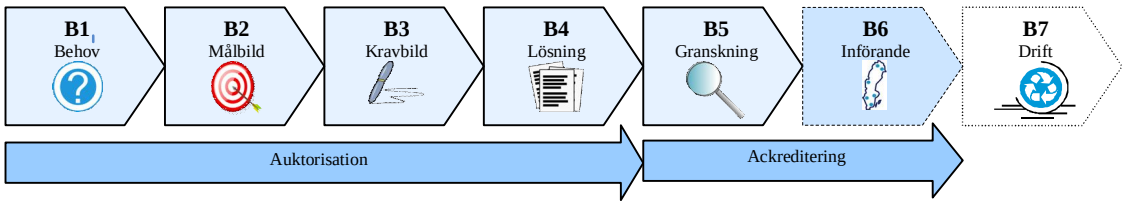
5.6.2 Tekniskt ackrediteringsunderlag

Tekniskt ackrediteringsunderlag är tekniskt inriktad och beskriver hur kraven är uppfyllda. (Sunnegårdh, 2010) Det är en sammanställning av ett antal informationsbitar och ska innehålla utfall från säkerhetsgranskningen och krav på åtgärder. (Andersson, 2010)

En del i underlaget är kravnedbrytning som pekar direkt på den preliminära tekniska kravspecifikationen. Utöver denna ska även systemöversikt, säkerhetsfunktioner, installationsanvisningar, handböcker, leveransbeskrivning, testplan och testfall, testrapport, säkerhetsgranskning samt kvarstående åtgärder ingå. (Andersson, 2010)

I en del fall behöver inte underlag tas fram längre än till tekniskt ackrediteringsunderlag. Detta gäller då en komponent ska integreras i ett IT-system. Då behöver påvisas att den specifika komponenten inte påverkar miljön och ett centralt ackrediteringsunderlag behövs inte. (Sunnegårdh, 2010) (Yngvesson, 2010)

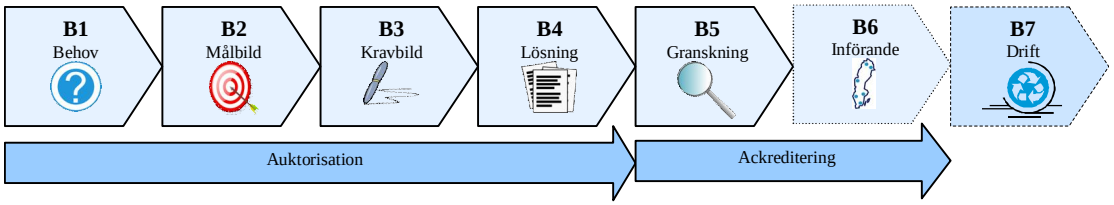
5.7 B6 – Införande



Figur 23: I B6 är det driftsättningen på lokala förband som är det centrala.

I beslutsunderlaget till B6 handlar det om driftsättning ute på lokala förband, se figur 23. (Eklöf, 2010) Beslutsunderlaget ska innehålla lokalt ackrediteringsbeslut, lokalt driftunderlag samt budget för drift. (Försvarsmakten, 2004, s. 79) I lokalt ackrediteringsunderlag tar den lokala chefen ställning till att godkänna det nya IT-systemet. Det är viktigt med ett lokalt godkännande eftersom miljön och förutsättningarna är olika på olika förband. (Gruppintervju, 2010) Beslut om driftsättning fattas efter att beslut om lokal ackreditering och lokalt driftunderlag fattats. Efter beslut om driftsättning får IT-systemet användas. (Försvarsmakten, 2004)

5.8 B7 – Drift

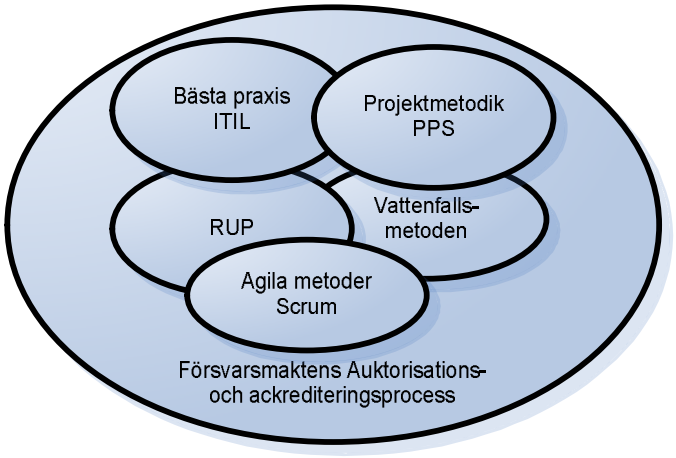


Figur 24: I B7 tas fortlöpande beslut om IT-systemet

I B7 tas fortlöpande beslut om IT-systemet, se figur 24. Produktägaren fattar beslut som ligger inom ramen för beslut om användning som bygger på ackrediteringen för IT-systemet. Om det inte ligger inom ramen för beslut om användning måste det genomgå en ny auktorisations- och ackrediteringsprocess. Systemägaren ansvarar för användningen av IT-systemet, driftägaren ansvarar för driften och designansvarig för åtgärder som produktägaren beslutat inom ramen för beslut om användning. (Försvarsmakten, 2004, s.39-40) Även avveckling av IT-systemet faller in under B7. Att planera för avveckling är viktigt eftersom det kan kosta mycket pengar och innebära mycket arbete. (Gruppintervju, 2010)

6. Informationssäkerhet i IT-utveckling – en standardiserad process

I följande kapitel analyseras Försvarsmaktens auktorisations- och ackrediteringsprocess utifrån de olika projekt- och IT-utvecklingsmetoder som redovisades i kapitlet *Utveckling av IT-system i projektform* för att utröna vilka likheter som finns samt vilken nytta som kan dras genom att ha en standardiserad process för IT-utveckling när det gäller informationssäkerhet, se figur 25.



Figur 25: Analys av auktorisation och ackreditering utifrån olika projektformer.

6.1 Projektledningsmetodik och praktisk projektstyrning

Försvarsmaktens auktorisations- och ackrediteringsprocess har många likheter med klassiskt projektstyrning där auktorisationsgruppen kan ses som en styrgrupp. Syftet med ett projekts affärsbeslut enligt Jansson och Ljung är att skapa kontroll över projektet, få kontroll över fördelar för organisationen samt status för resultat, tid och kostnad. Auktorisationsprocessens beslutssteg kan ses som just affärsbeslut eller *gater* som inte får passeras om inte vissa krav är uppfyllda. På det sättet kontrollerar Försvarsmakten när det är dags att stoppa ett projekt som inte går att använda i slutändan utan endast kostar pengar att utveckla. På samma sätt kan de avgöra vilka projekt som är lönsamma att släppa vidare i processen. Liksom en traditionell styrgrupp ger auktorisationsgruppen i varje beslutspunkt direktiv inför kommande beslutspunkter.

6.1.1 Projektets faser

Den första affärsbeslutet enligt Jansson och Ljung är projektägarens beslut att initiera ett projekt och forma ett ramverk för hur projektet ska gå till. Beslutet föregås av en *förstudie*. Detta gäller också för auktorisationsprocessens första beslutspunkt. Efter den första beslutspunkten skiljer det sig lite då det enligt Jansson och Ljung kommer en *planeringsfas* medan auktorisationsprocessen fokuserar på att skapa en målsättning genom ett antal analyser som renderar i krav. Att ställa krav är endast en del i planeringsfasen som även inkluderar resursbehov som i auktorisationsprocessen ska ske redan innan beslutspunkt ett fattas. Jansson och Ljung menar att det handlar om att analysera förutsättningar vilket även sker i auktorisationsprocessen då analyserna som renderar i krav samt ligger till grund för säkerhetsmålsättningen utförs. Författarna menar att det sällan blir en renodlad planeringsfas utan *genomförandefasen* påbörjas

innan planeringsfasen är avslutad, vilket ofta är nödvändigt för att klara en snabb leverans. Så ser det ofta ut även i auktorisationsprocessen där beslutssteg ibland slås ihop för att tidseffektivisera. Då tas risken att arbetet inleds på ett felaktigt spår och att det som var tänkt att spara pengar istället blir kostsamt. Att det inte finns någon tydlig tidpunkt när ett projekt går från planeringsfas till genomförandefas blir även tydligt då de flesta dokument görs i flera versioner. Ett exempel på det är taktisk-teknisk-ekonomisk målsättningen som i B2 skapas i form av ett utkast, i B3 är preliminär för att sedan bli slutgiltig i B5. Även teknisk kravspecifikationen och systembeskrivningen är dokument som i tidiga skeden är preliminära för att sedan fastställas vart efter förutsättningar ändras. Samtliga dokument tas fram genom iteration och därför är det viktigt att ett aktivt beslut tas för att projektet ska gå vidare till en ny fas. Övergången mellan *realisering* och *överlämning* är enligt Jansson och Ljung inte självklar, ett beslut måste tas när resultatet anses vara tillräckligt bra, det vill säga ett beslut måste fattas om huruvida eventuella brister ska omhändertas eller inte. Det samma gäller när ett IT-system ska ackrediteras, då produktägaren måste fatta beslut om hur kvarstående åtgärder ska behandlas. Då realiseringsetappen går över i överlämningsetapp kan liknas vid det moment då produktägaren lämnar över ansvaret för ett IT-system till systemägaren. Det är inte ovanligt att det finns kvarstående åtgärder och produktägaren måste besluta huruvida ett beslut om användning kan tas trots att det finns brister. Antingen kan produktägaren besluta att dessa måste åtgärdas innan IT-systemet tas i drift eller så kan IT-systemet tas i drift med restriktioner kring de kvarstående åtgärderna. I den sista etappen, *avslut*, där erfarenheter ska tas om hand finns potential för utveckling i auktorisations- och ackrediteringsprocessen. Processen innehåller ingen uttalad plan för återkoppling vilket innebär att personer som deltagit i processen inte får veta om IT-systemet klarade ackrediteringen, och om det inte gjorde det vad det i sådana fall berodde på. På det viset går erfarenheter förlorade. De personer som deltagit i projektet bär med sig lärdomar från tidigare projekt men de förs inte vidare till andra inom organisationen på ett strukturerat sätt. Delvis hanteras detta genom att nya personer får arbeta med mer erfarna personer, men det faktum att det inte finns några rutiner kring erfarenhetsöverföring kvarstår.

6.1.2 Praktisk projektstyrning

Tietos modell för projektstyrning följer i stora drag Jansson och Ljungs modell. Varje beslutspunkt ger styrgruppen möjlighet att ge direktiv inför kommande beslutspunkt på samma sätt som auktorisationsgruppen i varje beslut ger direktiv i auktorisationsprocessen. PPS skiljer sig lite genom att definiera fler beslutspunkter än Jansson och Ljung. Till exempel så är den andra beslutspunkten mitt i förberedelsefasen till för att fastställa att arbetet är på rätt väg. I auktorisationsprocessen kan B3 liknas vid ett sådant beslut eftersom en preliminär teknisk kravspecifikation och preliminär systembeskrivning tas fram i underlaget till B3 för att sedan fastställas i B4. Detta skulle kunna ses som en kontroll för auktorisationsgruppen att arbetet är inne på rätt spår. Om det råder tidsbrist ger PPS utrymme för att påbörja genomförandefasen innan förberedelsefasen är avslutad för de delar som redan är godkända. Något sådant utrymme ger inte auktorisationsprocessen rent teoretiskt men i praktiken förekommer det ändå att underlaget till nästa beslutssteg påbörjas utan att beslut från auktorisationsgruppen och CIO inväntas. Beslutspunkt sex enligt PPS är ett beslut om leverans vilket kan liknas vid auktorisationsprocessens B4 då IT-systemet levereras till Försvarsmakten från industrin eller FMV. Nästkommande beslutspunkt i PPS är ansvarsöverlämning vilket motsvaras av B5 i auktorisationsprocessen då IT-systemet

ackrediteras och produktägaren fattar beslut om användning och överlämnar ansvaret till systemägaren. Den sista beslutspunkten enligt PPS betyder avslut och erfarenhetsöverföring vilket det enligt ovan råder brist på i auktorisations- och ackrediteringsprocessen. Auktorisations- och ackrediteringsprocessen slutar inte heller efter ansvarsöverlämning eftersom den är en livscykel som följer IT-systemet under hela dess livslängd. Dock har jag i denna uppsats inte närmare studerat den del som sker efter ansvarsöverlämningen och därmed stämmer PPS relativt väl in med de steg som finns i auktorisations- och ackrediteringsprocessen, med skillnaden att PPS definierar fler beslutspunkter. Att införa fler beslutspunkter i auktorisations- och ackrediteringsprocessen skulle innebära att auktorisationsgruppen fick mer insikt i processen. Några indikationer på att det skulle vara nödvändigt eller efterfrågat har inte uppkommit under studien. Underlagen i sig itereras fram och därmed skapas en ständig översikt över att arbetet är adekvat.

6.2 Bästa praxis

6.2.1 Hantering av IT-utveckling genom bästa praxis

Många delar av Boochs modell, som främst beskriver utveckling av mjukvara, är även tillämpbara på generell utveckling av IT-system och därför har jag här valt att applicera dem på Försvarsmaktens auktorisations- och ackrediteringsprocess.

6.2.1.1 Tvetydiga budskap och brister i kommunikation

Booch menar att det bör finnas en bästa praxis för att hantera utveckling av mjukvara då det finns några generella faktorer som ofta bidrar till att projekt misslyckas. En av dessa är tvetydiga budskap och brister i kommunikation. Genom tydliga direktiv från auktorisationsgruppen och MUST stävjas detta problem. Brister i kommunikation bearbetas genom att arbeta med tydlig dokumentation och versionshantering. I DIT04 ges tydliga riktlinjer för vilken dokumentation som ska skapas för varje beslutssteg och auktorisationsgruppen ger även tydliga direktiv i varje beslutspunkt för vad som gäller för varje enskilt IT-system som utvecklas. Ett problem i kommunikationen är att underlag som kommer in till auktorisationsgruppen och MUST ibland är mycket omfattande. I de fall då det saknas tydliga referenser till var de delar som är intressanta står att finna bidrar det till att handläggningstiden blir fördröjd som i sin tur innebär att hela auktorisations- och ackrediteringsprocessen drar ut på tiden. För att säkerställa att alla menar samma sak och därmed eliminera missförstånd används gemensamma begrepp. Det finns till exempel tydligt beskrivet vad som ska ingå i en säkerhetsmålsättning och vad den fyller för funktion så att uppdragsgivaren menar samma sak med säkerhetsmålsättning som den som ges uppdraget att ta fram den.

6.2.1.2 Komplexitet

En annan faktor som ofta bidrar till att projekt misslyckas är enligt Booch för stor komplexitet. I Försvarsmakten rör det sig ofta om stora projekt med hög grad av komplexitet. Detta hanteras genom att dela upp stora system i delsystem. Ett flygplan kan till exempelvis ses som ett enda stort IT-system. Men det består av många små IT-system som visserligen integrerar med varandra men som ändå går att bryta ner i delsystem som kan genomgå auktorisation och ackreditering var för sig. I verksamhetsanalysen som ligger till grund för säkerhetsmålsättningen analyseras beroende och informationsflöde till andra IT-system. Verksamhetsanalysen ligger sedan

till grund för säkerhetsanalysen där informationens skyddsvärde bestäms utifrån såväl information som finns i det IT-system som ska ackrediteras som information i IT-system som IT-systemet under granskning kommunicerar med. På så vis går det att dela upp IT-systemet i delsystem utan att informationssäkerhetsaspekten går förlorad. Det är inte heller ovanligt att det är komponenter som ska integreras med redan ackrediterade IT-system som genomgår auktorisation och ackreditering. Då stannar processen vid att tekniskt ackrediteringsunderlag tas fram, det vill säga inget centralt ackrediteringsunderlag tas fram, ett beslut som fattas av auktorisationsgruppen. Att dela upp IT-systemet i delsystem kan också ske mer informellt genom att dela upp analyserna i underlaget till B2 eller att utforma systembeskrivningen utifrån delsystem.

6.2.1.3 Inkonsekvens i design och implementering

Vidare menar Booch att oupptäckt inkonsekvens i design och implementering bidrar till misslyckande. För att förhindra detta ska stor vikt läggs i början av auktorisations- och ackrediteringsprocessen då säkerhetsmålsättningen och den tekniska kravspecifikationen utformas. Säkerhetsmålsättningen är grunden på vilken hela processen står och därför brister det i slutet om säkerhetsmålsättningen är undermålig. Det som inte tas upp i säkerhetsmålsättningen och den tekniska kravspecifikationen kommer inte att finnas med i lösningen som tas fram av leverantören och därför är det centralt att dessa är grundligt utförda. Det är även viktigt att systembeskrivningen utformas med informationssäkerhet som utgångspunkt så att samtliga informationssäkerhetsbitar tas om hand och att det inte lämnas utrymme för missuppfattningar. Eftersom ackreditering innebär granskning där det färdiga IT-systemet granskas gentemot säkerhetsmålsättningen och MUST:s krav på säkerhetsfunktioner med systembeskrivningen som underlag så stärker processen möjligheterna för att upptäcka just brister i design och implementering.

6.2.1.4 Brister i riskhantering

Booch nämner även brister i riskhantering som en omständighet som leder till fallerade projekt. Detta är ytterligare en anledning till varför IT-system bör genomgå ackreditering då stort fokus läggs vid riskanalys i underlaget till B2. I riskanalysen deltar personer från olika delar av verksamheten för att få en så bred kompetens och så olika synsätt som möjligt. Riskanalysen fokuserar på risker som är specifika för IT-systemet eftersom generella risker redan är upptagna i MUST:s krav på säkerhetsfunktioner. Eftersom auktorisations- och ackrediteringsprocessen bidrar till att förhindra dessa problem ökar chanserna för att ett projekt lyckas om auktorisations- och ackrediteringsprocessen tillämpas som den ska.

6.2.1.5 Felaktig uppfattning om behovet

Booch anger felaktig uppfattning av behovet hos slutanvändaren som en faktor till misslyckande inom utvecklingsprojekt. Då ett IT-system ska utvecklas inom Försvarsmakten är det ofta från ett förband som behovet uppkommer och det är detta som föranleder att auktorisationsprocessen startas. Det är sedan auktorisationsgruppens uppgift att se till att det är detta behov som tillgodoses och att det hela tiden är behovet och hur detta på bästa sätt tillfredsställs som är i fokus, inte en speciell lösning. Vidare så deltar verksamhetsnära personal i verksamhetsanalysen i underlaget till B2 där fokus också ligger på användarfall som renderar krav. Dessa krav förs in i säkerhetsmålsättningen och samtliga krav i denna måste vara uppfyllda för att IT-systemet ska bli ackrediterat, det vill säga granskat och godkänt ur säkerhetssynpunkt.

Ytterligare en orsak till misslyckande enligt Booch är oförmåga att handskas med förändringar av behovet. I auktorisations- och ackrediteringsprocessen finns det ingen metod för att handskas med detta. Processen utgår från att det finns ett behov i början och det är utifrån det som utvecklingen sker. I de undersökningar jag gjort har det inte uppkommit några tecken på att förändring av behov skulle vara en anledning till svårigheter eller misslyckande av projekt. När IT-systemet redan är satt i drift, det vill säga i B7, finns dock utrymme för beslut på grund av förändrat behov.

6.2.1.6 Upprätthållning och vidareutveckling

En annan anledning till misslyckande enligt Booch är att det är svårt att upprätthålla och vidareutveckla mjukvara. Eftersom auktorisations- och ackrediteringsprocessen är en livscykelmodell så ingår även drift, det vill säga upprätthållande av IT-systemet, i planeringen. I underlaget för den första beslutspunkten ska driften beaktas där bland annat finansiering och ansvar för driften analyseras. Om ett IT-system inom Försvarsmakten ska vidareutvecklas så finns två alternativ. Om förändringen sker inom ramen för beslut om användning så kan dessa beslut om förändring fattas av produktägaren. Om förändringen inte sker inom ramen för beslut om användning startas en ny auktorisationsprocess.

6.2.1.7 Sent upptäckta brister

Att brister i projekt upptäcks sent är en vanlig faktor som leder till att projekt misslyckas menar Booch. En risk för detta finns i auktorisations- och ackrediteringsprocessen där påvisande av kravuppfyllnad och testning inte sker förrän IT-systemet redan är utvecklat. Ytterligare en risk är att driften inte efterfrågas i underlaget förrän i B6. Det är därför viktigt att ha driften i åtanke tidigare, exempelvis i utförandet av verksamhetsanalysen där användarfall analyseras och verksamhetens, det vill säga de som ska sätta IT-systemet i drift, krav upprättas. Om analyserna som ligger till grund för säkerhetsmålsättningen görs grundligt elimineras risken för att brister upptäcks sent. Dessutom sker framtagandet av underlag genom iterativa processer samt skickas på intern remiss vilket torde bidra till en minskad risk att brister upptäcks sent. Även auktorisationsgruppens och MUST:s granskning i varje beslutssteg bidrar till en kontroll att IT-systemet är på rätt väg.

Booch menar dessutom att desto tidigare brister identifieras och tas om hand desto billigare är de att åtgärda. Att genomföra tester och verifiering enligt auktorisations- och ackrediteringsprocessen bidrar därmed i längden till minskade kostnader. Detta är en viktig anmärkning då auktorisation och ackreditering ibland ses som något onödigt ont av de som arbetar med utvecklingen av IT-systemet. Booch anser också att genom testning fås en bättre bild av projektets status eftersom det är IT-systemet och inte dokumentationen som testas. En av ackrediteringsexperterna som intervjuades betonade också det i en intervju, att det är viktigt att det är det färdiga IT-systemet och inte systembeskrivningen och annan dokumentation, som ska testas i verifierings- och granskningsrapporten. Genom oberoende testning uppnås en objektiv bedömning av krav och design.

6.2.1.8 Dålig kvalité och ej förväntat beteende hos IT-systemet

Auktorisation och ackreditering är en process som stödjer utvecklingen av nya IT-system främst genom säkerhetsmålsättning, kravspecifikation, systembeskrivning och granskning. Samtliga underlag bidrar till att motverka att IT-systemet inte beter sig som det var tänkt samt att öka kvalitén med avseende på informationssäkerhet. Auktorisationsprocessen stödjer även en förbättrad kvalité som inte rör informationssäkerhet även om det inte sker i samma utsträckning. Eftersom auktorisation är en samordning av IT-utvecklingen med central styrning så torde det innebära att IT-system med högre kvalité utvecklas än om varje enskilt förband skulle utveckla sina egna IT-system. Eftersom alla IT-system som ska utvecklas ska passera auktorisationsgruppen uppstår där en erfarenhetsbank som kan dra nytta av kunskaper från olika projekt.

6.2.1.9 Brister i spårbarhet

Slutligen menar Booch att en stor risk som bidrar till misslyckande är att användare gör spårbarheten omöjlig. Spårbarhet kan här tolkas på olika sätt. Den ena är ur ett informationssäkerhetsperspektiv där det är viktigt att kunna se om någon obehörig tagit del av information eller ändrat i den. Den andra aspekten av spårbarhet är att det ska gå att se vem som har ändrat i underlag, när detta skedde samt hur det såg ut innan ändringarna. Den förra av dessa tolkningar ska inte kunna uppstå för ett IT-system som är ackrediterat då just spårbarhet tillsammans med sekretess, riktighet och tillgänglighet är grunden för hur kraven från hot-, risk- och sårbarhetsanalysen, som är ett av underlagen till säkerhetsmålsättningen, ska utformas. Spårbarhet säkerställs exempelvis genom säkerhetsloggning där det går att se vem som gjorde vad och när. Då är det också viktigt att systemadministratören inte har tillgång till säkerhetsloggen så att denne kan ändra i den. Den andra av tolkningarna bearbetas genom till exempel versionshantering av samtliga dokument i underlagen där det är tydligt vilka ändringar som har gjorts, vem som utfört ändringar samt när detta har skett. Det arbetas även med spårbarhet genom att i all dokumentation tydligt tala om vad som kommer varifrån. Ett exempel på detta är att underlagen alltid ska skrivas så att det går att härleda alla säkerhetsmål till specifika krav. De tekniska och centrala ackrediteringsunderlagen kan ses som sammanfattningar av de andra underlagen. Dessa ska gå att läsa för sig men det är även viktigt att det är tydligt var all information kommer ifrån och var fördjupning står att finna.

6.2.2 En IT-tjänsts livscykel

Liksom Försvarsmaktens auktorisations- och ackrediteringsprocessen beskrivs som en livscykel beskriver Haverblad en IT-tjänst ur ett livscykelperspektiv som täcker in såväl initiering och planering som avveckling. Enligt Haverblad är det viktigt att redan i början av processen planera för drift och förvaltning, något som det även uppmanas till i underlaget till den första beslutspunkten i auktorisationsprocessen. Haverblad menar liksom Booch att det är viktigt att IT-systemet håller en hög kvalité från början. Medan Haverblad menar att ett IT-system som håller hög kvalité vid driftsättning minskar driftskostnaderna så menar Booch att brister i kvalitén kan innebära ett helt misslyckat projekt.

Först i IT-tjänstens livscykel kommer enligt Haverblad ett *initierings- och planeringssteg* där en nyttoanalys utförs och behovet identifieras precis som i underlaget till B1 i Försvarsmaktens livscykelmodell. Beslutet som följer i båda

processerna är huruvida realisering ska ske. Enligt IT-tjänstens livscykel kommer sedan *kravanalys och design*, vilket följer Försvarsmakten livscykel, vilkens andra steg även det går ut på att identifiera krav. Hur IT-systemet ska integreras med andra IT-system ska ses över enligt Haverblad och det görs i Försvarsmaktens livscykel i verksamhetsanalysen där informationsflödet analyseras. Därefter följer *utveckling, integration och test* i IT-tjänstens livscykel där IT-systemets ska testas innan det sätts i drift. Detta motsvaras av såväl B3 som B4 eftersom utvecklingen av IT-systemet sker i B3 medan det testas i B4. I *implementationssteget* ska en pilotdrift av IT-systemet göras och driftrutiner samt dokumentation kring detta ska tas fram. I underlaget till B5 finns ingen uttalad pilotdrift av IT-systemet men då verifierings- och valideringsrapporten tas fram i underlaget till B4 så används en uppsättning av IT-systemet för att påvisa kravuppfyllnad vilket innebär att IT-systemet till viss del kan sägas pilotdriftas. Handböcker och liknande tas ofta fram i samband med systembeskrivningen redan i underlaget till B4. Detta faller dock utanför ramen för informationssäkerhet utan rör sig mer om systemsäkerhet. Efter implementationssteget följer *drift och underhåll* där det är viktigt att ansvar och roller är definierat, något som fastställs redan i tidigare beslutssteg. Drift och underhåll motsvaras av B6 och B7 i Försvarsmaktens livscykel. Det sista steget enligt Haverblad är avveckling vilket faller in under B7 i Försvarsmaktens livscykel. IT-tjänstens livscykel saknar på samma sätt som auktorisations- och ackrediteringsprocessen en tydlig rutin för återkoppling vid projektets slut som Jansson och Ljung förespråkar.

6.2.3 Förändringsprocessen

Haverblad pekar liksom Booch ut ett antal huvudorsaker till att projekt misslyckas. I Haverblads fall rör det sig om förändringsprocesser och eftersom utveckling av ett nytt IT-system i högsta grad är en förändringsprocess inom Försvarsmakten anser jag det fullt applicerbart på auktorisations- och ackrediteringsprocessen. Den första orsaken som identifieras är att projektet blir ett *teknikprojekt* istället för koncentration på den organisatoriska förändringen. Liknande problem återfinns i auktorisations- och ackrediteringsprocessen där informationssäkerheten ibland försummas och allt för stort fokus ligger på tekniken i det IT-system som utvecklas. Där fyller auktorisations- och ackrediteringsprocessen en viktig funktion genom att se till att informationssäkerheten beaktas.

Vidare menar Haverblad att *otydliga mål och otydlig avgränsning* är en orsak till att förändringsprocesser misslyckas och att detta ska motverkas genom att stora ändringar ska hanteras som nya projekt. I auktorisations- och ackrediteringsprocessen behandlas detta genom att avgränsa stora system till delsystem. Målet i alla projekt är att IT-systemet ska bli ackrediterat och därmed godkänt ur informationssäkerhetssynpunkt. Auktorisations- och ackrediteringsprocessen fyller även en funktion när det kommer till att motverka *kortsiktiga mål*. Den samordning som uppnås med auktorisation innebär att Försvarsmakten kan se till vad som är bäst för hela organisationen istället för att varje enskilt förband ska utveckla vad som är bäst för dem och för stunden. Att skapa *mätbara mål* är något som arbetas med i yttersta grad då säkerhetsmålsättningen tas fram. Alla mål måste vara mätbara för att de ska kunna användas i granskningen. Mätbara mål skapas även i ett vidare syfte genom att det finns definierat vad som ska vara uppfyllt i varje beslutspunkt för att auktorisationsgruppen ska låta processen fortgå. Detta hör samman med Haverblads nästa punkt, att det *inte finns definierat vad som krävs för en fungerande process,* till exempel i form av roller, ansvar, rutiner, mål och mätvärden. Samtliga av dessa definieras för IT-system som genomgår auktorisation. Att

processen inte följs kan dock vara en bidragande faktor till misslyckade projekt, de som berörs av projektet måste få det förankrat hos sig så att det inte uppstår ett motstånd. Vissa brister när det kommer till att förankra processen inom organisationen finns och många av respondenterna har påtalat vikten av att de som deltar i analyser och så vidare är medvetna om nyttan för att det ska bli ett lyckat projekt. Det finns således anledning att lägga resurser på att förankra auktorisations och ackrediterings nytta. Att det inte finns någon *förvaltning av processen* är också ett problem enligt Haverblad. Detta har också påtalats under intervjuerna, att det är viktigt att det finns någon som driver processen framåt för att projektet ska bli lyckat. Det hör samman med att förankra processen i organisationen, om de som deltar i projektet vill att det ska klara ackreditering så går det ofta bra i slutänden.

Om ett projekt främst har genomförts av *externa resurser* finns en risk för att intern kompetens saknas vilket sedan leder till att processen inte följs enligt Haverblad. Då det är mycket vanligt att just externa konsulter bistår i auktorisation och ackreditering finns en risk för kompetensluckor. Haverblad menar dock att problemet kan motverkas genom att de som sedan ska arbeta med förändringen får vara delaktiga i designen under processen. Detta sker bland annat i verksamhetsanalysen där användarfall är i fokus och användarna får chansen att uttrycka sina synpunkter i såväl verksamhetsanalysen som hot-, risk- och sårbarhetsanalysen. *Avsaknad av kompetensöverföring mellan extern och intern resurs* hör ihop med föregående punkt. Det finns ingen uttalad strategi i processen för hur kompetensöverföring ska ske mellan konsult och Försvarsmakten. Däremot så förs till exempel krav på användning och andra direktiv ut till förbanden genom det lokala ackrediteringsunderlaget. Genom att vid utförandet av underlagen vara noggrann med spårbarhet går det sedan att spåra bakåt i processen bakgrunden till att dessa krav på användning uppkommit.

Haverblad menar också att *för stort fokus på en modell eller ett ramverk* är ett annat problem. Först måste det definieras vad som ska uppnås och vilken strategi som ska användas sedan ska modeller och ramverk anpassas efter detta. I det här fallet är det alltid ackreditering som ska uppnås och målet är att få ett IT-system godkänt ur säkerhetssynpunkt så att det kan driftstättas. Ramverket är liknande för alla auktorisations- och ackrediteringsprocesser eftersom det alltid är samma mål. Det anpassas efter varje specifikt fall genom att auktorisationsgruppen ger direktiv om vilka underlag som måste tas fram och vilka som inte är nödvändiga. Processen är dock inte anpassad till de fall då det är ett redan färdigt IT-system som ska ackrediteras. Den sista anledningen till misslyckade förändringsprocesser enligt Haverblad är att de är för *överambitiösa.* Det är viktigt att dela upp projekt i väldefinierade steg vilket är precis vad som görs i och med auktorisation och är således ett argument för dess nytta.

6.2.4 Information Technology Infrastructure Library

Enligt ITIL är det viktigt att både expertis och användare deltar i utvecklingsarbetet. I analyserna som ligger till grund för säkerhetsmålsättningen tas det fasta på detta genom att såväl användare som beslutsfattare deltar tillsammans med informationssäkerhetskonsulter. Förespråkare av ITIL påpekar vikten av att en organisation har kontroll över sina IT-system eftersom det leder till minskade kostnader, samordning, stabilitet och ökad säkerhet för verksamheten. En utstakad process med rutiner och tydligt ansvar gör det lättare att möta behovet från verksamheten, vilket kan användas som argument för auktorisationsprocessen som ibland möter motstånd då många som berörs av den inte alltid ser dess nytta. Liksom auktorisation kritiseras ITIL

ibland för att vara byråkratisk, vilket enligt ITIL ska bearbetas genom att trycka på dess fördelar, något som det skulle kunna läggas större vikt på när det gäller auktorisation. ITIL, som är en mycket väldefinierad process för att samordna IT passar bäst hos stora företag eftersom de har störst behov av samordning och kontroll. Om samordning saknas finns en risk att olika delar av organisationen tar fram olika lösningar på samma problem vilket skapar onödiga kostnader. Dessutom blir samverkan mellan IT-system svårare om de utvecklas oberoende av varandra. Det är också vanligt att stora organisationer som Försvarsmakten, landsting och banker hanterar känslig information som leder till att de behöver ha kontroll över sina IT-system. Detta är faktorer som kan ses som en indikation på att det är just en mycket väldefinierad process, som auktorisation är, som är lämplig även för Försvarsmakten som i högsta grad är en stor organisation.

ITIL och Försvarsmaktens auktorisationsprocess är i mångt och mycket lika varandra, båda är till exempel livscykelprocesser som initieras med att ett behov som kan stödjas med IT uppstår i vad ITIL benämner *strategifasen*. Enligt ITIL ska kunden, samt vilka tjänster som krävs för att möta dennes behov, identifieras i denna fas. I auktorisationsprocessen är kunden ofta redan identifierad eftersom det många gånger är denne som kommer med idén eller rapporterar ett behov i B1. Detta behov definieras och utreds av auktorisationsgruppen som kan avgöra om det redan finns en lösning som möter behovet eller om ett nytt IT-system ska utvecklas. Strategifasen följs i ITIL av en *designfas* där teknik och arkitektur som möter behovet som definierats i strategifasen ska tas fram. Auktorisationsprocessen är uppdelad i flera steg där krav ställs och tekniken specificeras i detalj innan den designas, vilket är steg som absolut bör finnas med i processen för att säkerställa att det som utvecklas stämmer överens med behovet. Det är viktigt att utgå från behovet, inte lösningen. Designfasen motsvaras således av såväl B2 som B3. Nästa fas i ITIL är *överföringsfasen* där IT-systemet byggs, testas och valideras för att säkerställa att alla krav är uppfyllda innan det sätts i drift. Överföringsfasen motsvaras av B4 och B5 i auktorisationsprocessen där en uppsättning av IT-systemet används för att verifiera och validera IT-systemet för att påvisa kravuppfyllnad i B4. I B4 utförs även en granskning där verifierings- och valideringsrapporten används som underlag tillsammans med säkerhetsmålsättningen och MUST:s krav på säkerhetsfunktioner som stäms av mot systembeskrivningen. Sista steget enligt ITIL är *driften* där kontinuitet och upprepade cykler är viktigt för att fortlöpande förbättra IT-systemet. Även auktorisation utgår från ett livscykelperspektiv, men det har jag valt att inte fokusera på här då jag främst studerat processen fram till ackreditering, det vill säga driften är inte närmare studerad här.

6.3 Vattenfallsmodellen

Den del av auktorisations- och ackrediteringsprocessen som jag har studerat i den här uppsatsen har vissa likheter med Vattenfallsmodellen då de båda bygger på att en linjär process drivs framåt genom ett antal steg i form av till exempel analys, design, implementation och testning. Det finns dock några avsevärda skillnader. Enligt Computer Sweden ger Vattenfallsmodellen inget utrymme för att överbrygga de olika stegen, först när ett steg är helt avslutat kan projektet gå vidare till nästa steg. Inom auktorisation finns ett visst utrymme att gå vidare till nästa beslutsspunkt även om det tidigare steget inte är helt avslutat. Detta beslut fattas av auktorisationsgruppen som i sådana fall lämnar restpunkter som ska uppfyllas. Inom auktorisation och ackreditering

tillämpas dessutom iterering vid framtagande av underlag, vilket inte förekommer i Vattenfallsmodellen.

Ett problem med Vattenfallsmodellen enligt Schwaber är att den är linjär. Testning sker först i slutet av processen och det blir då väldigt kostsamt om IT-systemet måste göras om eller så måste kravställningen ändras. Även i Försvarsmaktens process sker testning sent men eftersom framtagandet av alla underlagen sker genom iterativa processer så reduceras risken för att IT-systemet ska vara långt från att uppfylla kraven då testning utförs. Det finns en begränsning i hur mycket Försvarsmakten kan ändra i kravställningen eftersom då ett IT-system i Försvarsmakten utvecklas är det för att möta ett specifikt behov och det är säkerhetsmålsättningen och MUST:s krav på säkerhetsfunktioner som leder till kravställningen. För att ett IT-system ska kunna ackrediteras är det därför viktigt att IT-systemet kravställs korrekt från början och att denna kravställning sedan följs när IT-systemet utformas. Däremot går det att ändra utformningen av IT-systemet så att till exempel vissa säkerhetsmål inte blir aktuella, vilket kan göras i dokumentet förslag till realiseringslösning. Återigen är det viktigt att ha i åtanke att det inte är lösningen som är det viktiga utan behovet.

Royce definierar några kringprocesser i Vattenfallsmodellen, till exempel dokumentation samt planering och kontroll kring tester, som är två huvudmoment i auktorisation och ackreditering. Eftersom kringprocesser inte explicit leder fram till slutprodukten och dessutom ökar utvecklingskostnaderna menar Royce, liksom förespråkare för ITIL, att det är av yttersta vikt att förankra nyttan med processen för att få ett lyckat projektresultat, vilket även gäller för auktorisations- och ackrediteringsprocessen. Vikten av dokumentation för att kunna styra processen, underlätta kommunikationen, specificera IT-systemet men framför allt för att kunna testa det är central menar Royce. Det är något som det tas fasta på även i auktorisation och ackreditering. Testning och spårbarhet skulle inte vara möjlig utan tydlig dokumentation och detta är ett argument för auktorisation och ackreditering, helt enkelt för att få rutiner kring dokumentation. Enligt Royce är det alltid någon oberoende som ska granska IT-systemet. För auktorisation tillämpas detta, främst då det är IT-system av högre säkerhetsklassning som ska ackrediteras. Dessutom remissas alla dokument internt innan de fastställs. Slutligen så trycker Royce på vikten av att knyta an användaren till IT-systemet innan det är dags för leverans. Därför är verksamhetsanalysen i B2 av stor vikt för att användare och förband som sedan ska sätta IT-systemet i drift är involverade i utvecklingen.

6.4 Rational Unified Process

RUP och Försvarsmaktens auktorisations- och ackrediteringsprocess har många likheter, bland annat beskrivs såväl kravprocessen som användarfall som centralt i båda modellerna.

6.4.1 Metoder

Enligt Lunell är *iterativ utveckling* av stor betydelse inom RUP. Även auktorisationsunderlagen tas fram iterativt. Analysdokumenten bearbetas till exempel fram iterativt inom B2-underlaget, medan andra dokument som till exempel systembeskrivningen tas fram iterativt över gränsen för beslutsunderlagen då en preliminär systembeskrivning tas fram i underlaget till B3 för att sedan fastställas i B4. Liksom både Booch och Haverblad förespråkar i sina argument för bästa praxis så är det

viktigt att det finns en metod för *kravhantering* eftersom det är oundvikligt att krav förändras över tiden. I auktorisations- och ackrediteringsprocessen finns en begränsning av hur förändring av krav ska hanteras då processen istället fokuserar på att få en så korrekt kravställning från början som möjligt. Det kan dock hanteras till viss del genom att en del säkerhetsmål och MUST:s krav på säkerhetsfunktioner blir inaktuella om en annorlunda design på IT-systemet väljs. RUP står även för *arkitekturcentrerad utveckling* enligt Lunell då arkitekturen är av extra stor vikt vid iterativ utveckling eftersom den då måste kunna anpassas vartefter IT-systemet utvecklas. I auktorisationsprocessen är den tekniska kravspecifikationen och systembeskrivningen av stor betydelse för IT-systemets arkitektur. Lunell menar också att *visuell modellering* en bra metod eftersom olika perspektiv av IT-systemet kan analyseras var för sig. För auktorisations- och ackrediteringsprocessen är det inte direkt tillämpbart eftersom det snarare är en stödprocess till IT-utveckling. Däremot går *upprepad kvalitetsverifiering* att applicera på auktorisation och ackreditering. Upprepad kvalitetsverifiering är extra viktigt när det kommer till iterativa processer menar Lunell. Såväl Booch som Haverblad pekar på vikten av att redan från början bygga in kvalité i IT-system. Hela auktorisations- och ackrediteringsprocessen bidrar till att öka kvalitén hos det IT-system som är under utveckling tack vare en samordnad process där erfarenheter kan dras från andra lyckade eller misslyckade projekt. Det är inte bara IT-systemet som ska hålla en hög kvalité, det är viktigt att även kvalitén på processen är hög och en viktig faktor som bidrar till det är att processen följs som den är tänkt. Enligt Lunell är också *konfigurations- och ändringshantering* viktigt för att hantera de versioner som uppkommer då iterativ utveckling används. Ändringshantering är viktigt för IT-systemet i sig men fyller även en central funktion vad gäller dokumentation inom auktorisation och ackreditering. Det är viktigt att veta när en ändring har skett i ett dokument och av vem för att bibehålla spårbarheten. Det är av stor betydelse att veta att det är den senaste versionen av dokumentet som nya ändringar utförs i, men även viktigt för att veta var eventuella felaktigheter kommer ifrån. Detta hanteras bland annat genom dokumentet Redovisa ändringar av inlämnat B2-underlag genom versionshantering, och motsvarande för de andra beslutspunkterna. Dessutom anges versionsnummer i alla dokument som utgör underlag för beslutspunkterna.

6.4.2 Nyckelegenskaper

Den första av de nyckelegenskaper som Lunell pekar ut för RUP är *användningsfallsdriven utveckling* och han menar att användningsfall är den drivande kraften i hela processen. Användningsfall kommer främst in i auktorisations- och ackrediteringsprocessen i verksamhetsanalysen som utgår just från användningsfall för att fastställa vilka krav som verksamheten har på det IT-system som utvecklas. *Featurebaserad utveckling* går ut på att användningsfall och iterationer delas in efter funktioner. Det är inte fullt tillämpbart på auktorisations- och ackrediteringsprocessen som kan ses som en stödprocess vid utveckling av IT-system. Det finns dock en likhet eftersom featurebaserad utveckling innebär att en helhetslösning tas fram på samma sätt som auktorisation till viss del syftar till att säkerställa att de delar som ska finnas med vid utveckling av ett IT-system finns med. Vidare så har RUP en *riskfokusering* redan tidigt i processen för att reducera risker. I auktorisations- och ackrediteringsprocessen utförs riskanalysen redan i underlaget till B2, det vill säga så fort beslut har fattats att utveckling ska ske. Denna riskanalys renderar i krav som tillsammans med de övriga analyserna utgör säkerhetsmålsättningen, vilken är av stor vikt då den tekniska kravspecifikationen utformas. Säkerhetsmålsättningen är sedan en del av grunden vid

granskningen då samtliga krav ska vara uppfyllda för att IT-systemet ska bli ackrediterat. Den sista nyckelegenskapen Lunell definierar är en *konfigurerbarprocess*, det vill säga att processen ger utrymme för anpassning efter olika projekts egenskaper. På så sätt kan auktorisations- och ackrediteringsprocessen vara en form av RUP som utvecklats efter hur Försvarsmaktens IT-system ska godkännas på bästa sätt. Auktorisations- och ackrediteringsprocessen kan i sin tur sägas vara till viss del konfigurerbar. Exempel på hur detta praktiseras är att auktorisationsgruppen för varje enskilt fall beslutar vilka specifika underlag som ska tas fram inför varje beslutspunkt beroende på specifika egenskaper för varje enskilt utvecklingsfall. Det är dock viktigt att processen inte anpassas allt för mycket eftersom den syftar till att säkerställa att ett IT-system är godkänt att tas i drift med avseende på säkerhet och då måste vissa moment vara uppfyllda. Säkerhetsmålsättning, systembeskrivning med fokus på informationssäkerhet, testning och granskning är moment som alltid måste ingå.

6.4.3 Faser

De faser som beskrivs i RUP liknar de beslutspunkter som definieras i auktorisations- och ackrediteringsprocessen. Skillnaden är att den senare definierar fler beslutspunkter och i varje fas i RUP täcks således fler beslutspunkter från auktorisations- och ackrediteringsprocessen in. *Förberedelsefasen* i RUP kan ses som en kombination av B1 och delvis B2. I förberedelsefasen ska projektet avgränsas och definieras vilket görs inför att B1 ska fattas. Andra enheter som IT-systemet ska samverka med ska identifieras förberedelsefasen. I verksamhetsanalysen i underlaget till B2 identifieras andra IT-system som informationsutbyte ska ske med. Men det kan även fattas beslut om att samverkan med andra IT-utvecklingsprojekt ska ske och detta görs av auktorisationsgruppen som har kontroll över vilka IT-system som finns och vilka som är under utveckling. Förberedelsefasen ska även resultera i målsättning, riskanalys, kostnadsanalys samt tidsplan enligt RUP. Kostnadsanalysen och en grundläggande målsättning skapas i underlaget till B1 medan ett utkast till taktisk-teknisk-ekonomisk målsättning inte utförs förrän i underlaget till B2. I underlaget till B2 utformas även säkerhetsmålsättningen och de fyra analyser som ligger till grund för denna, bland annat riskanalysen.

Därpå följer *etableringsfasen* där behovet som motiverat projektet ska analyseras vidare. Detta sker i auktorisationsprocessen i analysdokumenten som säkerhetsmålsättningen grundar sig på i underlaget till B2. Detta är den mest kritiska fasen i RUP enligt Rational Software och på samma sätt har många intervjurespondenter uttryckt säkerhetsmålsättningen som fundamental för att fortsättningen av processen ska bli lyckad. Enligt RUP ska en prototyp tas fram. I auktorisations- och ackrediteringsprocessen motsvaras detta av att preliminära versioner av dokument tas fram, till exempel preliminär teknisk kravspecifikation och preliminär systembeskrivning i B3 som sedan vidareutvecklas i B4. Etableringsfasen ska resultera i en beskrivning av mjukvaruarkitekturen enligt RUP, vilken alltså motsvaras av systembeskrivningen i auktorisations- och ackrediteringsprocessen. Även analysdokumenten i B2 tas fram genom iterativa processer.

Konstruktionsfasen kan jämföras med underlaget till B4 eftersom IT-systemet kan tillverkas efter att B3 fattats. I konstruktionsfasen ska precis som i underlaget till B4 IT-systemet också testas. För att IT-systemet ska få passera milstolpen för konstruktion måste det vara redo att användas utan att det innebär några stora risker vilket innebär att

även B5, det vill säga beslut om användning måste ha fattats. Konstruktionsfasen omfattar således både delar av B4 och hela B5.

Den sista fasen i RUP är *överlämning* vilken motsvaras av B5 och B6 där B5 innebär att produktägaren fattar beslut om användning som innebär att IT-systemet är centralt ackrediterat. Men för att IT-systemet ska få användas på förbanden måste även beslut om lokal ackreditering och drift, det vill säga B6, ha tagits. I RUP:s överlämningsfas ska kvarstående åtgärder och nya problem som uppkommer under driften omhändertas. Detta motsvaras av B7 som är beslut under IT-systemets livstid inom ramen för beslut om användning. Överlämningsfasen innebär även utbildning och stöd till användare som tas upp i dokumentet krav på användning som skapas i samband med att granskningen utförs i underlaget till B4 och sedan förs in i såväl det centrala som det lokala ackrediteringsunderlaget i B5 och B6 och ska följa IT-systemet under dess livslängd.

6.4.4 Arbetsprocesser

Arbetsprocesserna är den statiska aspekten av RUP, till skillnad från faserna som är iterativa cykler enligt Rational Software. Eftersom faserna och arbetsprocesserna står i relation till varandra går det att finna många likheter mellan arbetsprocesserna och beslutsstegen i auktorisations- och ackrediteringsprocessen på samma sätt som mellan faserna och auktorisations- och ackrediteringsprocessen. Ett exempel på detta är kravprocessen i RUP som syftar till att utvecklare och kund ska vara överens på samma sätt som säkerhetsmålsättningen och den tekniska kravspecifikationen i auktorisations- och ackrediteringsprocessen syftar till att det IT-system som utvecklas stämmer överens med de krav som Försvarsmakten har. I båda processerna är dokumentation, spårbarhet i dokumentation och användarfall nyckelord. Analys- och designprocessen som syftar till att visa hur IT-systemet ska realiseras kan liknas vid systembeskrivningen som ska specificera vad som ska ingå i det IT-system som utvecklas. I implementeringsprocessen är testning central för att säkerställa att alla eventuella brister är omhändertagna innan IT-systemet tas i bruk på samma sätt som testning är central för att ett IT-system i Försvarsmakten ska bli ackrediterat. Testning ska enligt RUP också utföras för att säkerställa att interaktionen mellan komponenter fungerar som den ska. Detta motsvaras av det centrala ackrediteringsunderlaget där tekniska ackrediteringsunderlag för komponenter eller delsystem sammanförs. Testning i RUP sker iterativt för att så fort som möjligt upptäcka eventuella brister enligt Rational Software. I auktorisations- och ackrediteringsprocessen sker testning främst i underlaget till B4 och B5 eftersom det är det verkliga IT-systemet och dess dokumentation som ska granskas, om det inte är ett färdigt IT-system så ändras förutsättningarna. Det går dock att göra en förgranskning för att se till att det är på rätt väg. Implementeringsfasen behandlar även hur komponenter ska kunna återanvändas i andra projekt. Analys av möjligheten att återanvända komponenter i andra IT-system görs även i auktorisationsprocessen men då främst genom att auktorisationsgruppen i B1 analyserar möjligheten att tillmötesgå ett behov med en redan befintlig lösning. Den sista arbetsprocessen i RUP är spridning som kan jämföras med driften i B6. Även om spridningen inte sker förens i slutet är det ändå viktigt att planera för den tidigare enligt såväl RUP som Vattenfallsmodellen. Därför är det viktigt att den beaktas redan i B1 när möjligheten att realisera det behov som uppkommit ska analysera samt i underlaget till B2 då verksamhetens krav på IT-systemet ska analyseras.

6.4.5 Roller, aktiviteter och artefakter

RUP definierar ansvar i projekt genom roller och en individ kan ha flera roller i ett projekt. Bland de organisatoriska kraven i säkerhetsmålsättningen kan det finnas krav som innebär att en del roller inte får fyllas av samma fysiska person på grund av säkerhet. Om en och samma individ har två olika roller som innebär att den utför två olika aktiviteter kan följden bli att denne individ medvetet kan riskera informationssäkerheten till större grad än om två olika individer har ansvar för de två aktiviteterna. Det är dock inte direkt relaterat till roller i processens gång, där det finns en annan viktig aspekt av roller. Som extern konsult i arbetet med auktorisation och ackreditering är det viktigt att beakta vilken roll man innehar. I ett projekt kan det vara rollen som Försvarsmakten, i ett annat projekt industri och så vidare. Det är viktigt att hålla isär de olika rollerna och beakta vilken roll man som konsult innehar i varje enskilt projekt. Artefakt motsvaras av de dokument och underlag som skapas genom auktorisation och ackreditering.

6.5 Scrum

Att Scrum i en artikel i Computer Sweden kritiserats för att inte vara lämpligt för stora system och stora organisationer med outsourcing är ytterligare ett argument för att det inte är lämpligt att använda vid Försvarsmaktens auktorisation och ackreditering då Försvarsmakten är en mycket stor organisation och outsourcing sker i högsta grad till såväl FMV som konsultfirmor som Combitech. För att Scrum ska lyckas är det viktigt att det är ett nära samarbete mellan uppdragsgivare och utvecklare eftersom produkten itereras fram. Eftersom Försvarsmakten lämnar uppdraget till FMV som sedan ofta lämnar det vidare till extern konsult så begränsas samarbetet till möten och samtal vid utvalda tillfällen. I Försvarsmaktens process tas till exempel verksamhetens krav i beaktning i verksamhetsanalysen och därför är det viktigt att den blir utförligt gjord, eftersom användarnas deltagande efter det är begränsat. De dagliga möten som förespråkas i Scrum och som även ska hållas i samma lokal blir svåra att hålla när det är personer från många olika delar i Försvarsmakten men även från helt andra organisationer som ska träffas. Dessutom är det inte ovanligt att personerna befinner sig på spridda platser i landet geografiskt sett vilket gör det ännu svårare att hålla dagliga möten i samma lokal. Då det visat sig svårt att få till enstaka analysmöten i underlagen till säkerhetsmålsättningen torde det vara omöjligt att hålla de dagliga möten som Scrum förespråkar. Dessutom är sprinttiden begränsad till mellan en och fyra veckor, vilket i många fall är alldeles för kort för att vara tillämpbart på de underlag som tas fram till auktorisation och ackreditering, speciellt då det är stora IT-system det rör sig om. Den långa handläggningstiden och svårigheterna att få till möten innebär att Scrum inte heller går att tillämpa mellan de olika beslutsstegen i auktorisationsprocessen. Även om underlagen till auktorisation och ackreditering tas fram iterativt så faller det inte i ramen för vad Scrum förespråkar. Lösningen på att Scrum inte är anpassat för stora IT-system skulle kunna vara att dela upp IT-systemet i mindre delsystem, vilket till viss del sker i auktorisations- och ackrediteringsprocessen. Men även om IT-systemet bryts ner i mindre delsystem kvarstår till exempel en komplex kravställning på alla IT-system inom Försvarsmakten.

I Computer Sweden kritiseras Scrum också för att vara en metod som skapar problem spårbarhet, vilket skulle vara ännu en faktor till att inte applicera metoden på Försvarsmaktens auktorisation och ackreditering där spårbarhet är ett nyckelord då ett IT-system ska granskas. Vid ackreditering granskas IT-systemet och då är det oerhört

viktigt att se varifrån varje krav kommer. Saknas spårbarhet faller hela möjligheten till granskning. Om ett försök att tillämpa Scrum vid auktorisation och ackreditering skulle göras skulle det troligen resultera i att modellen skulle modifieras vilket innebär att dess poäng går förlorad. Till skillnad från RUP så ger inte Scrum utrymme för anpassning utan är tänkt att följas enligt dess ursprungskoncept.

7. Avslutning

7.1 Slutsatser

Auktorisation och ackreditering fyller flera viktiga funktioner. Det samordnar Försvarsmaktens IT-system, skapar kontroll, minskar kostnader i längden eftersom lösningar kan återanvändas och produktägaren säkerställs om att det är ett säkert IT-system som denne sätter i drift. Det är viktigt att utgå från behovet, inte lösningen. Genom att ha en bästa praxis för hur IT-utveckling inom en organisation ska gå till kan några vanliga faktorer som ofta bidrar till att projekt i allmänhet, och IT-utvecklingsprojekt i synnerhet, misslyckas undvikas. Chansen att nå en lyckad utveckling av ett nytt IT-system ökar om det finns metoder som hanterar kvalité, kommunikation, komplexitet, riskhantering, målsättning, plan för drift och avveckling, spårbarhet samt användarfall. Fördelarna med processen bör förankras i organisationen för att processen ska få stöd inom verksamheten och därmed följas som det är tänkt. Nyttan med kringprocesser, exempelvis dokumentation och testning, har ett extra stort förankringsbehov eftersom de inte explicit leder fram till slutprodukten. Att både expertis och användare deltar i utvecklingen är ytterligare en metod för att förankra arbetet i hela verksamheten. Roller och ansvar måste definieras.

Att faser ibland påbörjas utan att tidigare faser avslutats är en tids- och kostnadsmässig risk eftersom arbetet då kan inledas på fel spår. Beslutspunkter tappar då sin funktion. För stora organisationer är det extra viktigt att ha en bästa praxis för IT-utveckling eftersom komplexiteten ofta ökar desto större organisation det rör sig om. För organisationer med IT-system som hanterar information som omfattas av ett stort skyddsvärde är det av ännu större vikt att ha en bästa praxis eftersom dessa har en tydlig kravspecifikation för vad IT-systemet måste innehålla redan i ett initialt skede efter vilken IT-systemet sedan måste utvecklas. En agil metod för att driva processer av det här slaget framåt är inte lämpligt eftersom de inte passar för stora IT-system och stora organisationer som det rör sig om i det här fallet. Det är dock viktigt att beakta att även om processen är linjär så kan underlagen med fördel utvecklas iterativt.

En bra säkerhetsmålsättning och kravspecifikation är avgörande när det gäller informationssäkerhet för att få en fortsatt lyckad process. Testning är viktigt för att säkerställa att IT-systemet uppfyller samtliga krav innan det sätts i drift. Att ackreditera IT-system har ytterligare fördelar genom att granskningen resulterar i kvarstående åtgärder och krav på användning så att det finns en medvetenhet om vilka brister och restriktioner som finns när IT-systemet tas i drift.

Auktorisationsprocessen följer till stor del grunderna för traditionell projektmetodik. Den del som studerats i den här uppsatsen kan sägas följa en linjär process medan Försvarsmakten arbetar enligt en livscykelprocess. Processen saknar en avslutningsfas där det ges utrymme för återkoppling från det gångna projektet. Att ge möjlighet till återkoppling skulle innebära en vinst för kommande processer där tidigare lärdomar och erfarenheter då kan tas med in i nya projekt och spridas vidare inom organisationen. Ett uttalat moment för återkoppling tycks saknas i flera modeller som beskrivs som livscykelmodeller.

7.2 Förslag till framtida forskning

I denna uppsats har främst den del av Försvarsmaktens livscykel som Combitech deltar i studerats. Intressant vore att studera beslut som tas under drift för att knyta samman hela livscykelperspektivet. Även en fördjupning av interaktionen mellan systemsäkerheten och informationssäkerhet är en möjlighet till framtida utredning.

Ett annat ämne för vidare studier är att jämföra Försvarsmaktens process med ackreditering av IT-system inom andra organisationer för att påvisa skillnader eller likheter som kan leda till en förbättrad process.

8. Referenslista

8.1 Tryckta

Arraj, Valerie, (2010). ITIL: *The Basics* i Best Management Practise, OGC.

Booch, Grady, (2004). ”Software Development Best Practises” i Kructhen, Phillipe, *The rational unified process: an introduction,* Boston: Addison-Wesley.

Clark, Jane, (2007). *Everything you wanted to know about ITIL in less than thousand words* i Best Management Practise, Connect Sphere Limited.

Försvarsmakten (2004). *Direktiv för försvarsmaktens informationsteknikverksamhet, DIT 04.*

Försvarsmakten (2006a). *Handbok Säkerhetstjänst Informationsteknologi,* Stockholm: Försvarsmakten.

Försvarsmakten (2006b). *Metodik Säkerhetsanalys. Bilaga till MAACK – Metod och utbildningsstöd för auktorisations- och ackrediteringsprocesserna inom Försvarsmakten.*

Försvarsmakten (2006c). *Metodik Verksamhetsanalys. Bilaga till MAACK - Metod och utbildningsstöd för auktorisations- och ackrediteringsprocesserna inom Försvarsmakten.*

Försvarsmakten (2006d). *Metodik Hot-, risk och sårbarhetsanalys. Bilaga till MAACK – Metod och utbildningsstöd för auktorisations- och ackrediteringsprocesserna inom Försvarsmakten.*

Försvarsmakten (2007a). *Försvarsmaktens författningssamling (FFS 2007:4),* Stockholm: Försvarsmakten.

Försvarsmakten (2007b). *Försvarsmaktens interna bestämmelser (FIB 2007:5),* Stockholm: Försvarsmakten.

Försvarsmakten, (2010). *Grundläggande utbildning i klassificering av Försvarsmaktens information*. Stockholm: Försvarsmakten.

Haverblad, Angelica, (2004). *IT Service Management i praktiken,* Lund: Studentlitteratur.

Haverblad, Angelica, (2006). *IT ur ett affärsperspektiv,* Lund: Studentlitteratur.

Jansson, Tomas och Ljung, Lennart, (2004). *Projektledningsmetodik,* Studentlitteratur.

Kructhen, Phillipe, (2004). *The rational unified process: an introduction,* Boston: Addison-Wesley.

Lunell, Hans, (2003). *Fyra rundor med RUP,* Lund: Studentlitteratur.

Rational Software: “Rational Unified Process, Best Practises for Software Development Teams” *Rational Software White Paper* TP026B, Rev 11/01, Cupertino: Rational Software Corporation.

Royce, Winston W, (1970). “Managing the Development of Large Software Systems”, orginal från *Proceedings,* The Institution of Electrical and Electronics Engineers Inc.

Schwaber, Ken, (1995). *SCRUM Development Process,* Burlington: Advanced Development Methods.

Schwaber, Ken, (2004). *Agile Project Management with Scrum,* Redmond: Microsoft Press.

8.2 Internet

Agile Sweden, (2010). www.agilesweden.org (2010-11-11)

Computer Sweden (2010a). *Kritiken mot Scrum växer,* http://computersweden.idg.se/2.2683/1.187182/kritiken-mot-scrum-vaxer (2010-11-11)

Computer Sweden (2010b). *Ordlista Unified Modelling Language,* http://cstjanster.idg.se/sprakwebben/ord.asp?ord=unified%20modeling%20language (2010-11-15)

Computer Sweden (2010c). *Ordlista Vattenfallsmodellen,* http://cstjanster.idg.se/sprakwebben/ord.asp?ord=vattenfallsmodellen (2010-11-12)

Handbok Umbrello UML Modeller. (2010). *Grundläggande UML,* http://docs.kde.org/development/sv/kdesdk/umbrello/uml-basics.html (2010-11-15)

ITIL (2010). *What is ITIL?* http://www.itil-officialsite.com/AboutITIL/WhatisITIL.asp, (2010-11-22)

Nationalencyklopedin (2010a). *Informationssystem,* http://www.ne.se/lang/informationssystem/211494 (2010-11-16)

Nationalencyklopedin (2010b). *IT-system,* http://www.ne.se/lang/it-s%C3%A4kerhet?i_h_word=IT-system (2010-11-16)

Nationalencyklopedin (2010c) *Riktighet,* http://www.ne.se.ezproxy.its.uu.se/sve/riktig (2010-12-17)

Nationalencyklopedin (2010d). *Sekretess,* http://www.ne.se.ezproxy.its.uu.se/lang/sekretess (2010-12-17)

Nationalencyklopedin (2010e). *System,* http://www.ne.se/lang/system (2010-11-16)

Nationalencyklopedin (2010f). *Tillgänglighet,* http://www.ne.se.ezproxy.its.uu.se/tillg%C3%A4nglighet/327746 (2010-12-17)

SoftDevTeam (2011). *Waterfall Lifecycle Model,* http://www.softdevteam.com/waterfall-lifecycle.asp (2011-01-12)

Tieto Praktisk Projektstyrning, PPS OnLine 12. (Licensmateriel)

8.3 Intervjuer

Gruppintervju: Dzaferagic, Samir, Nützman, Helena, Roswall, Teddy, Sandin, Stefan, Combitech AB 2010-10-23.

Intervju: Andersson, Magnus, Informationssäkerhetskonsult, Combitech AB, 2010-10-20.

Intervju: Bergengren, Therése, Informationssäkerhetskonsult, Combitech AB, 2010-09-07.

Intervju, telefon: Bergman, Glenn, Informationssäkerhetskonsult, Combitech AB, 2010-10-15.

Intervju, telefon: Dzaferagic, Samir, Informationssäkerhetskonsult, Combitech AB, 2010-09-24.

Intervju: Eklöf, Lena, Informationssäkerhetskonsult, Combitech AB, 2010-09-21.

Intervju, telefon: Johansson, Lena, Projektledare Systemarkitektur, Combitech AB

Intervju, telefon: Jönson, Jan, Senior Advisor Information and Security/Affärsutveckling, Combitech AB, 2010-10-14.

Intervju: Lindskog, Åsa, Informationssäkerhetskonsult, Combitech AB, 2010-09-20.

Intervju: Nützman, Helena, Informationssäkerhetskonsult, Combitech AB, 2010-09-23.

Intervju: Roswall, Teddy, Informationssäkerhetskonsult, Combitech AB, 2010-09-23.

Intervju, telefon: Sandin, Stefan, Informationssäkerhetskonsult, Combitech AB, 2010-11-09.

Intervju: Sunnegårdh, Patrik, Informationssäkerhetskonsult, Combitech AB, 2010-09-20.

Intervju: Tengroth, Ronnie, Projektledare, Combitech AB, 2010-09-21.

Intervju: Törnkvist, Bengt, Senior Project Manager Information & Security, Combitech AB, 2010-09-15.

Intervju: Yngvesson, Anders, Informationssäkerhetskonsult, Combitech AB, 2010-09-20.

Bilaga 1 - Ordlista och begrepp

Begrepp	**Förklaring**
Ackreditering	Godkännande av IT-system ur säkerhetssynpunkt.
Auktorisation	Bemyndigande för produktägare att utveckla Försvarsmaktens IT-verksamhet.
Assurans	Det går att hysa tillit till ett system med avseende på dess specificerade säkerhetsfunktioner.
CIO – Chief Information Officer	Försvarsmaktens sambands- och informationssystemchef.
Evaluering	Granskning av ett IT-system där systembeskrivningen ställs mot krav från säkerhetsmålsättningen och MUST:s krav på säkerhetsfunktioner
FIB	Försvarsmaktens interna bestämmelser
Granskning	Se evaluering.
H Säk IT	Handbok Säkerhetstjänst Informationsteknologi.
Informationssystem	Ett informationssystem är ett system som lagrar, bearbetar och distribuerar information.
IT	Informationsteknik eller informationsteknologi. Ett samlingsbegrepp för datateknik och telekommunikation som möjliggör kommunikation av bilder och ljud.
ITK	Försvarsmaktens informationstekniska katalog. Listar bland annat redan godkänd mjukvara.
MUST	Militärens underrättelse- och säkerhetstjänst
Produktansvarig	Handlägger ärenden åt produktägaren.
Produktägare	Enhetschef i Högkvarteret eller chef för organisationsenhet. Innehar huvudsakligt ansvar för IT-systemet. Utses i B1 av auktorisationsgruppen.
System	Ett system består av ett antal komponenter som samverkar. System avskiljs från varandra genom gränsskikt. Ett system kan delas in delsystem

	eller sammanfogas med andra system till ett stort system.
Validering	Bekräftelse på att krav för viss avsedd användning är uppfyllda. IT-systemet testas för att se att det uppfyller verksamhetskrav.
Verifiering	Bekräftelse på att specificerade krav är uppfyllda. IT-systemet testas för att se att det uppfyller KSF-krav.