FOI-R--1504--SE
December 2004
ISSN 1650-1942
Underlagsrapport

Sofie Pilemalm, Leni Ericson, Niklas Hallberg, Per-Ola Lindell, Maria Andersson

Utveckling av Riskhantering

Ledningssystem
581 11 Linköping

TOTALFÖRSVARETS FORSKNINGSINSTITUT

Ledningssystem
Box 1165
581 11 Linköping

FOI-R--1504--SE

December 2004

ISSN 1650-1942

Underlagsrapport

Sofie Pilemalm, Leni Ericson, Niklas Hallberg, Per-Ola Lindell, Maria Andersson

Utveckling av Riskhantering

Utgivare	**Rapportnummer, ISRN**	**Klassificering**
Totalförsvarets Forskningsinstitut - FOI	FOI-R--1504--SE	Underlagsrapport
Ledningssystem	**Forskningsområde**	
Box 1165	4. Spaning och ledning	
581 11 Linköping	**Månad, år**	**Projektnummer**
	December 2004	E781042
	Verksamhetsgren	
	5. Uppdragsfinansierad verksamhet	
	Delområde	
	41 Ledning med samband och telekom och IT-system	

Författare/redaktör	**Projektledare**
Sofie Pilemalm	Niklas Hallberg
Leni Ericson	**Godkänd av**
Niklas Hallberg	
Per-Ola Lindell	**Uppdragsgivare/kundbeteckning**
Maria Andersson	FMV
	Tekniskt och/eller vetenskapligt ansvarig
	Niklas Hallberg

Rapportens titel

Riskhantering för FMA

Sammanfattning (högst 200 ord)

Att kunna hantera risker är viktigt i allt utvecklingsarbete. Begreppet *risk* avser sannolikheten för att en negativ händelse ska inträffa. Negativa händelser kan för det som har utvecklats (d v s systemet, organisationen etc) innebära lägre kvalitet, högre utvecklingskostnad och förseningar. Riskhantering är ett strategiskt och operationellt verktyg för att maximera verksamheters möjligheter och resultat. Riskhantering består av aktiviteterna *riskidentifiering*, *riskanalys och riskhantering.* Svårigheter vid riskhantering kan exempelvis vara otillräckliga verktyg för riskhantering och integrationen med övergripande utvecklingsprocesser. Processen för riskhantering är tidskrävande och det är dessutom svårt att avgöra om samtliga risker har identifierats.

Syftet med denna rapport är att ge en problembeskrivning för riskhantering samt att ge förslag på hur ett stöd för riskhantering kan utvecklas och implementeras. Utvecklingen av stödet sker i två delar, dels utveckling av riskhanteringsprocess, dels utveckling av datorstöd. Utvecklingen av processen, baserad på ISO/IEC 15 288, genomförs iterativt i de tre stegen *definition av process, identifiering av metoder och tekniker* samt *utvärdering av process.* Därefter utvecklas ett datorstöd för processen. Detta stöd kravspecificeras, designas, implementeras och utvärderas. Datorstödet implementeras som moduler där olika datorstöd för metoder och tekniker kan införas, bytas ut och modifieras oberoende av varandra.

Nyckelord

Utveckling av Riskhanteringen

Övriga bibliografiska uppgifter	**Språk** Svenska
ISSN 1650-1942	**Antal sidor:** 10 s.
Distribution enligt missiv	**Pris: Enligt prislista**

Issuing organization
FOI – Swedish Defence Research Agency
Command and Control Systems
P.O. Box 1165
SE-581 11 Linköping

Report number, ISRN
FOI-R--1504--SE

Report type
Base data report

Programme Areas
4. C4ISR

Month year
December 2004

Project no.
E781042

General Research Areas
5. Commissioned Research

Subcategories
41 C4I

Author/s (editor/s)
Sofie Pilemalm
Leni Ericson
Niklas Hallberg
Per-Ola Lindell
Maria Andersson

Project manager
Niklas Hallberg

Approved by

Sponsoring agency
Defence Materiel Administration

Scientifically and technically responsible
Niklas Hallberg

Report title (In translation)
Development of Risk Management

Abstract (not more than 200 words)

It is important to be able to manage risks in all kinds of development. The concept *risk* refers to the probability for the occurrences of negative incidents. The occurrences of negative incidents often imply lower quality of resulting systems, higher costs, delayed delivery, and poorer technical characteristics. Risk management constitutes a strategic and operational tool for maximizing options as well as results of the business. Risk management includes *identification*, *analysis*, and *handling* of risks. Difficulties within risk management are for example the lack of tools and the integration of risk management with the overall system development process. Moreover, the process of risk management is time consuming and it is often hard to decide if all risks have been identified.

The objective of this report is to describe difficulties within risk management and suggest how a risk management support should be developed. The work is performed in two parts: development of the risk management process and development of the corresponding computer support. The development of the risk management process, based on ISO/IEC 15 288, is performed iteratively in three steps, which are definition of process, identification of techniques, and evaluation of process. Thereafter, a computer support for the process is developed. The computer support is specified, designed, implemented, and evaluated. The computer support is suggested to be implemented in modules, permitting support for techniques to be included, exchanged or modified independently of other modules.

Keywords
Risk management

Further bibliographic information

Language Swedish

ISSN 1650-1942

Pages 10 p.

Price acc. to pricelist

INNEHÅLL

1 Inledning

Alla typer av projekt involverar olika former av risker och systemutvecklingsprojekt är inget undantag. Att analysera och hantera risker är en viktig del i systemutveckling (Robertson & Robertson, 1999). Riskhantering är dock något som först under senare decennier explicit inkorporerats i systemutvecklingsprocessen, som ett svar på de problem systemutveckling och kravhantering fortfarande brottas med, exempelvis i form av försenade projekt, överskridna budgetar och färdiga system av otillräcklig kvalité (Karolak, 1996). Under 1980-talet introducerades riskhantering inom systemutvecklingsprojekt inom det amerikanska försvaret och idag ingår riskhantering i många standarder för systemutveckling och kravhantering (Hall, 1998). Trots detta saknas fortfarande dokumentation kring och utvärdering av praktiska erfarenheter av riskhantering i konkreta systemutvecklingsprojekt (Freimut et al, 2001).

Generellt i systemutveckling avses med *risk* sannolikheten för att en negativ händelse skall inträffa som påverkar möjligheten att nå uppställda mål. I detta dokument kommer begreppet *risk* att innefatta den *negativa händelsen* och *sannolikheten* att händelsen inträffar. Med *konsekvenser* avses de effekter som den negativa händelsen har (Hall, 1998). Konsekvenser, i systemutveckling, kan vara lägre kvalitet på det färdiga systemet, högre kostnader, förskjutningar i tidsschema, sämre tekniska karakteristika, och/eller ekonomiska förluster. (Karolak, 1996; Withers, 2000). *Riskhantering* är ett strategiskt såväl som operationellt verktyg vars syfte är att minimera risker och deras konsekvenser. En väl utvecklad riskhanteringsprocess ger god insikt om risker i verksamheten och hur dessa påverkar. Riskhanteringen utgör därmed en viktig del i det vardagliga beslutsfattandet då den tillhandhåller information som medför att mer korrekta beslut kan fattas, vilket ger bättre förutsättningar att uppfylla uppsatta mål (Withers, 2000).

Generellt inom systemutveckling brukar risker relateras till *projekt, process* och *produkt* (Hall, 1998). Risk uppstår dock i alla situationer där ogynnsamma avvikelser i det förväntade eller önskade resultatet kan inträffa. I systemutveckling finns risker på alla generaliseringsnivåer av processen, allt från projektet i sin helhet till exempelvis bedömning av enskilda krav och systemegenskaper. Risker finns även vid till exempel val av metod för att samla in kund/användardata och vid val av språk för implementation. Det anses extra viktigt att genomföra riskhantering vid utveckling av helt nya system, där okända risker kan resultera i konsekvenser sent i processen. Eftersom kravhantering är en så vital del av systemutveckling är också riskhanteringen i denna del viktig för ett lyckat resultat. Fördelarna med en adekvat riskhantering i kravhanteringen är bland annat att de krav som riskerar orsaka problem för systemutvecklarna identifieras på ett tidigt stadium. Därmed är det möjligt att planera eventuella åtgärder för att minska riskerna till exempel genom att modifiera kravet. Att identifiera risker till krav avslöjar också ofta om informationen angående ett krav är tillräcklig eller om mer kunskap måste samlas in (Sommerville & Sawyer, 1997).

1.1 Processer för riskhantering

Riskhantering skall genomföras som en egen process som följer såväl systemets utvecklingsprocess som livscykel. Risker skall vidare identifieras på ett så tidigt stadium som möjligt och dokumenteras tillsammans med värdering av konsekvenser. För de risker som bedöms som stora eller medförande allvarliga konsekvenser utarbetas *åtgärder* eller *åtgärdsplaner*. Direkta risker bör åtgärdas genast medan det utarbetas beredskapsplaner till indirekta risker (Withers, 2000). Riskhantering beskrivs ofta i faserna (Robson, 1997):

- Riskidentifiering
- Riskanalys
- Riskåtgärdande, det vill säga planering av åtgärder

I ekonomiska termer innefattar riskhantering att beakta det dagliga hanterandet och utvecklandet av en produkt/system (Karolak, 1996). Detta innefattar exempelvis kostnader, resurser och tidsschema. Dessutom, enligt standarden för systemutveckling i ISO/IEC 15 288 (2002), är syftet med riskhantering att minska effekterna av händelser som kan resultera i ändringar i kvalitet och tekniska karakteristika. En ansats för identifiering av risker är att ha en detaljerad planering för de olika stegen i utvecklingen av en produkt/system. Varje aktivitet i utvecklingsstadiet ges ett startdatum, datum för färdigställande, beskrivning av uppgiften/produktfasen samt vilken/vilka som är ansvariga (Karolak, 1996). Riskhantering är något som skall följa ett systems hela livscykel och appliceras övergripande för systemutvecklingen som helhet och i samtliga systemutvecklingsfaser. I ISO/IEC 15 288 (2002) standarden föreskrivs följande steg för riskhantering:

- *Riskanalys*
  - Risker identifieras, definieras och kategoriseras.
  - Möjligheter och konsekvenser av risker identifieras, definieras, värderas och kvantifieras utifrån förutbestämda kriterier. En prioritering av risker görs också utifrån detta.
- *Riskåtgärdande*
  - Strategier för att möta varje risk specificeras.
  - En riskstatus görs tillgänglig och kommuniceras. Den bör även innehålla definitioner av acceptansgrad för varje identifierad risk.
  - Åtgärder för risker som överskridit accepterade tröskelvärden identifieras och dessa risker behandlas utifrån detta.

1.2 Typer av risker

I systemutvecklingsprojekt finns ett stort antal av risker. Ibland skiljs det på tekniska och verksamhetsorienterade risker (Karolak, 1996). Till de första hör risker som relaterar till systemets *funktionalitet, kvalitet, pålitlighet, användbarhet, prestanda, underhåll* och *återanvändbarhet.* Till de senare hör risker relaterade till *budget* och olika typer av *kostnader* samt *vinst* och *förlustmarginaler*. Risker kan också relatera till den övergripande projektprocessen och dess planering med hänsyn till *tidsplanering* och *flexibilitet* (Karolak, 1996).

Vikten av riskhantering i samband med kravhantering bedöms som allt viktigare (Sommerville & Sawyer, 1997). Exempel på typer av risker som är relaterade till kravhantering är:

- *Prestandarisker* – krav kan ha negativ effekt på systemets övergripande prestanda.
- *Säkerhetsrisker* – krav kan ha negativ effekt på systemets övergripande säkerhet.
- *Processrisker* – krav kan orsaka att förändringar måste göras i den övergripande utvecklingsprocessen.

- *Implementationsrisker* – krav kan kräva användning av implementeringstekniker som ej förutsetts.
- *Schemarisker* – krav kan vara tekniskt komplicerat, vilket kan hota tidsplanen för projektet.
- *Externa risker* – att implementera ett krav kan innebära att externa kontraktorer måste anlitas.
- *Stabilititetsrisker* – kravet kan vara osäkert och förändras under utvecklingsprocessen.

Ett ökande antal systemutvecklingsansatser betonar också vikten av att hantera risker relaterade till organisatoriska aspekter vid systemutveckling och implementation, exempelvis kompabilitet med existerande organisationskultur och beaktande av icke önskade framtida organisatoriska konsekvenser av systemet (Mohamed & Appalanaidu, 1998).

1.3 Metoder för riskhantering

Ett flertal metoder för riskhantering är också i många fall baserade på tekniker som används i systemutveckling. Riskidentifiering involverar datainsamling i och om systemutvecklingsprojektet som sådant, exempelvis studier av dokumentation och underlag från systemets intressenter. Risker kan identifieras i intressenternas önskemål och behov, men framför allt ur deras krav. En metod för att identifiera övergripande projektrisker är att studera dokumentation och kvalitativa data från organisation och budget. I riskidentifiering bör dock även hänsyn tas till allmänt vedertagen kunskap om riskhantering i systemutvecklingsprojekt (Karolak, 1996). Checklistor anses vara ett bra sätt att täcka samtliga riskområden och typer av risker (Hall, 1998). Riskhantering i den del av systemutvecklingsprocessen som relaterar till kravhantering bör bygga på dokumentation från såväl behovsunderlag som behovsanalys, men framför allt från kravanalys (Kotonya & Sommerville, 1998; Sommerville & Sawyer, 1997).

För riskanalys kan olika typer av tabeller, matriser och beräkningssystem användas, hämtade exempelvis från metrik och relationsanalys (Karolak, 1996). Sannolikheten för att en negativ händelse inträffar och graden av allvar av riskens inträffande kvantifieras numeriskt. Detta ger förutsättningar för att göra en prioritering av riskerna för att kunna besluta vilka av dem som bör åtgärdas. Relationsanalyser kan även genomföras för att identifiera samband mellan olika risker och söka identifiera den risk som orsakar ytterligare risker (Hall, 1998). Trots att numeriska angreppssätt ofta används är riskanalysen en jämförelsevis oprecis process med flera subjektiva antaganden (Redmill, 2002). Därför är ofta övergripande kategorier och kriterier för värdering av risker såsom ”hög”, ”medel” och ”låg” att föredra framför exakta värderingar, även om dessa ger ett mindre precist underlag för prioritering och åtgärder (Sommerville & Sawyer, 1997). Utifrån den genomförda riskanalysen diskuteras olika åtgärdsalternativ för de risker som bör elimineras och åtgärdsplaner för risker som eventuellt bör åtgärdas. Även dessa alternativ värderas ofta, innan ett beslut tas (Karolak, 1996). Åtgärdsplaner och planerade åtgärder bör även tilldelas tidsramar, det vill säga beslut om när eventuella åtgärder ska genomföras (Hall, 1998).

Ett annat sätt att hantera risker i systemutvecklingsprocessen är genom itererade utvärderingar av prototyper, med validering och verifiering. Prototyper kan konstrueras, utvärderas och modifieras kontinuerligt under systemutvecklingsprocessen för att säkra det färdiga systemets kvalitet och användbarhet (Cooper, 2001). Prototyper utgör därmed en testbädd för det färdiga

systemets arkitektur och kan användas för att exempelvis identifiera stabilitetsrisker (kraven som kan förändras under projektets gång) och tekniska risker. De kan också användas för att analysera risker relaterade till en övergång till fullskalig implementation av det färdiga systemet (Young, 2001).

Det finns idag ett antal av mer övergripande metodologier för att stödja riskhantering i systemutvecklingsprojekt. Ett exempel är RISKIT som har detaljerade steg och verktyg för hela riskhanteringsprocessen (Kontio et al, 1998).

1.4 Problem i riskhantering

Även om riskhantering idag är en explicit del av många systemutvecklingsansatser är processen för riskhantering i sig inte oproblematisk. Exempel på problem innefattar svårigheten att överblicka systemutvecklingsprojekt och att identifiera dess samtliga risker. Riskhantering är också en tidskrävande process som kan komma i konflikt med snäva budgetar och tidsramar. Vidare saknas mer specifika och konkreta verktyg för just riskhanteringsprocessen, trots de metoder som pekades på ovan. Ett exempel på detta är datorstöd. Många systemutvecklare saknar dessutom kunskap om riskhantering, först på senare år har detta lyfts fram som en viktig del i systemutveckling. Det finns också svårigheter med att integrera riskhantering med den övergripande systemutvecklingsprocessen (Karolak, 1996). Vidare har ett traditionellt sätt att se på riskhantering varit att enskilda risker beaktats isolerade från varandra. Även olika riskers samspel och integrering med varandra bör beaktas. Eliminerade risker kan förstärka andra risker i en fortlöpande process. Dokumentation och spårbarhet mellan olika risker samt mellan övergripande risker för hela systemutvecklingsprocessen och dess olika faser (t ex kravhantering) är av största vikt.

2 Genomförande

Processen för riskhantering som finns definierad i standarden ISO/IEC 15 288 utgör grunden i utgångspunkten för utvecklingen av ett stöd för riskhantering, men har utvecklats för att överkomma några av de problem som beskrivs ovan. Genomförandet beskrivs i relation till de två delsyften, riskhanteringsprocess och datorstöd för riskhanteringen.

2.1 Riskhanteringsprocess

Utvecklingen av processen för riskhantering sker i tre steg, *Definition av process, Identifiering av metoder och tekniker* samt *Utvärdering av processen.* Dessa steg itereras kontinuerligt för att förbättra processen.

2.1.1 Definition av process

Med utgångspunkt från ISO/IEC 15 288 definieras en process för riskhantering bestående av de två delprocesserna *riskanalys* och *riskåtgärdande*. Var och en av dessa delprocesser innefattar ett antal aktiviteter. Initialt måste en systematisk ansats till hur risker ska identifieras, värderas och behandlas upprättas. Detta inkluderar fastställandet av händelser som negativt skulle kunna påverka systemets, projektets eller organisationens existens. Notation för hur risker ska uttryckas i passande termer, med mätvärden, utifrån kostnad, tid eller tekniska attribut ska fastställas. En första systematisk ansats till hur åtgärder ska hanteras med avseende på exempelvis tidsramar bör också initialt fastställas.

2.1.2 Identifiering av metoder och tekniker

För att stödja genomförandet av definierade aktiviteter i processerna riskanalys och riskåtgärdande behövs metoder och tekniker. Dessa identifieras i vedertagen litteratur.

Exempelvis kan metoder, beräkningsmodeller och matriser hämtade från Quality Function Deployment (QFD) komma att användas. QFD härstammar från Japanskt kvalitetstänkande och Just-in-time produktion, men har under senare år även utnyttjats i kravhantering vid systemutveckling (Karlsson, 1998; Karolak, 1996). QFD erbjuder verktyg för att etablera spårbarhet mellan intressenternas önskemål på systemet och de tekniska krav systemet bör uppfylla. Därmed skapas möjligheter att värdera, prioritera och ta beslut om den slutliga kravspecifikationen. Här används bland annat en matris kallad House of Quality (HOQ) (Karlsson, 1998). Den är framför allt användbar i prioriteringen av krav som kan relateras till riskhanteringsprocessen, då prioriteringen i sig innefattar exempelvis värdering av krav gentemot de tids- kostnads- och resursramar projektet erbjuder. De verktyg QFD tillhandahåller kan användas även i den specifika riskhanteringsprocessen, för att exempelvis värdera risker och sätta dem i relation till varandra, samt identifiera de risker som överskrider definierade tröskelvärden och bör åtgärdas.

2.1.3 Utvärdering av processen

För att utvärdera riskhanteringsprocessen appliceras den i ett antal fallstudier, där data om utfallet samlas in med stöd av kvalitativa metoder såsom intervjuer och observationer. Resultat av utvärderingen påtalar förbättringsförslag på processen.

3 Datorstöd för riskhantering

I riskhanteringsprocesser för systemutveckling saknas idag till stor del konkreta verktyg som stöder den specifika riskhanteringen. I detta projekt utvecklas ett datorstöd för att underlätta riskhanteringen. Detta stöd behöver kravspecificeras, designas, implementeras och utvärderas. Datorstödet implementeras i moduler där olika datorstöd för metoder och tekniker kan införas, bytas ut och modifieras.

Kravspecificering
En kravlista på vad ett datorstöd för riskhantering skall klara av sammanställs med utgångspunkt i beskrivningen av riskhanteringsprocessen. Det är viktigt att datorstödet klarar av exempelvis hantering av spårbarhet och relationsanalys.

Design
En design görs av datorstödet med utgångspunkt från kravlistan.

Implementering
Designen implementeras exempelvis i Microsoft Windowsmiljö utnyttjande Microsoft .Net-plattformen och programmeringsspråket C# med databasstöd från databashanteraren SQL Server.

Utvärdering
Flera utvärderingar av datorstödet som helhet och moduler som innefattar stöd till enskilda metoder och tekniker genomförs. Stödet modifieras och förbättras med utgångspunkt från dessa utvärderingar.

4 Referenser

Cooper, K. K. (2001) *Rapid Prototyping Technology*. *Selection and Application*, Marcel Dekker Inc, New York.

Freimut, B., Harkopf, S., Kaiser, P., Kontio, J. & Kobitsch, W. (2001) An Industrial Case Study of Implementing Software Risk Management.

Hall, E., (1998) *Managing Risk. Methods for Software Systems Development*, Addison-Wesley, Reading, MA.

ISO/IEC 15288, System Engineering – System Life Cycle Processes, ISO/IEC CD 15288 FCDIS, Version 4, Material under bearbetning.

Karlsson, J. (1998) *A Systematic Approach for Prioritizing Software Requirements*, Linköping Studies in Science and Technology, Dissertation No. 526.

Karolak, W. D. (1996) *Software Engineering Risk Management*. IEEE Computer Society Press, Los Calamitos, CA.

Kontio, J., Getto, G. & Landes D. (1998) Experiences in Improving Risk Management Processes Using the Concept of the Riskit Method.

Kotonya, G. & Sommerville, I. (1998) *Requirements Engineering. Processes and Techniques*, John Wiley & Sons, Chichester.

Mohamed, M. Z. & Appalanaidu, U. B. (1998) Informations Systems for Decentralization of Development Planning: Managing the Change Process, *International Journal of Information Management*, Vol. 18, Iss. 1, s. 49-60.

Redmill, F. (2002) Risk Analysis – a Subjective Process, *Engineering Management Journal*, April Issue, s. 91-96.

Robertson, S. & Robertson, J. (1999) *Mastering the Requirements Process*. Addison-Wesley.

Robson, W. (1997) *Strategic Management & Information Systems*, Pitman Publishing, London.

Sommerville, I & Sawyer, P. (1997) *Requirements Engineering. A Good Practice Guide*, John Wiley & Sons, Chichester.

Withers, D. (2000) Software Engineering Best Practices Applied to the Modeling Process, i Joines, J., Barton, R. R., Kang, K. & Fishwick, P. A. (Eds.) *Proceedings of the 2000 Winter Simulation Conference*, s. 432-439.

Young, R. R. (2001) *Effective Requirements Practice*, Addison Wesley.