



Riskacceptans

Kostnadseffektiv riskhantering för IT-system

Henrik Karlzén, Johan Bengtsson, Jonas Hallberg

Henrik Karlzén, Johan Bengtsson, Jonas Hallberg

Riskacceptans

Kostnadseffektiv riskhantering för IT-system

Bild/Cover: Johan Bengtsson

Titel	Riskacceptans – Kostnadseffektiv riskhantering för IT-system
Title	Risk acceptance – Cost-effective risk management for IT systems
Rapportnr/Report no	FOI-R--4521--SE
Månad/Month	December
Utgivningsår/Year	2017
Antal sidor/Pages	55
ISSN	1650-1942
Kund/Customer	Försvarsmakten
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	Ledning och MSI
Projektnr/Project no	E72678
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem
Exportkontroll	Innehållet är granskat och omfattar ingen information som är underställd exportkontrollagstiftningen.

Detta verk är skyddat enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk, vilket bl.a. innebär att citering är tillåten i enlighet med vad som anges i 22 § i nämnd lag. För att använda verket på ett sätt som inte medges direkt av svensk lag krävs särskild överenskommelse.

This work is protected by the Swedish Act on Copyright in Literary and Artistic Works (1960:729). Citation is permitted in accordance with article 22 in said act. Any form of use that goes beyond what is permitted by Swedish copyright law, requires the written permission of FOI.

Sammanfattning

Utformningen av IT-system måste präglas av intressenternas behov för att ge nytta. Dessutom måste de risker som systemen ger upphov till hanteras. Riskhantering tenderar dock att enbart fokusera på riskerna och huruvida de kan accepteras, snarare än att en avvägning görs mot nytta och kostnader.

Under 2017 genomförde FoT-projektet *Metodik för säkerhetsmålsättningsarbete* en studie om riskacceptans. Målsättningen med studien var att identifiera vad som borde påverka beslut om huruvida risker kan accepteras för planerade IT-system inom Försvarmakten. Arbetet utgick från Försvarmaktens egna publikationer samt forskningslitteratur, standarder och branschspecifika vägledningar inom området.

Litteraturen lyfter fram att även om det formella riskacceptansbeslutet tas i slutet av riskhanteringsprocessen måste de underliggande kriterierna för riskacceptans prägla hela riskhanteringsprocessen. Riskacceptansbeslut måste väga in de egna verksamhetsbehoven, både på organisationsövergripande och på systemspecifik nivå. Det är dessutom nödvändigt att väga in lagar och standarder samt behov hos intressenter som kan påverkas av systemet. Forskningen om riskacceptans är dock ganska omogen och det finns många forskningsfrågor som behöver besvaras. Exempelvis är förståelsen av hot en essentiell del av riskhanteringsprocessen – och för riskacceptansen – men hur hoten ska beskrivas är inte klarlagt.

För att förtydliga på vilka grunder som beslut om riskacceptans ska tas inom Försvarmakten behöver övergripande kriterier för riskacceptans formuleras. Dessutom behöver befintliga instruktioner kompletteras med en beskrivning av hur de övergripande kriterierna anpassas och genomsyrar alla aktiviteter i riskhanteringsprocessen. Det är också av vikt att inse att teknik och behov kan förändras snabbt samt att bedömningarna aldrig kommer att vara perfekta, varför det bör finnas utrymme för regelbunden uppföljning av analyser och beslut.

Nyckelord: Riskhantering, riskanalys, riskacceptans, kriterier, kostnad, nytta, ekonomi, informationssäkerhet, IT-system, intressenter, säkerhetsinvestering

Summary

IT systems must be characterised by the needs of the stakeholders in order to be beneficial. Moreover, the risks associated with the system have to be managed. Risk management, however, tends to focus only on the risks and whether they can be accepted, rather than balancing them with the costs and benefits of the system.

In 2017, an R&D project at FOI conducted a study on risk acceptance. The objective of the study was to identify what should influence decisions about whether risks can be accepted for planned IT systems within the Swedish Armed Forces. The work was based on the Swedish Armed Forces' own publications as well as research literature, standards and industry-specific guidelines.

The literature revealed that, although the formal risk acceptance decision is taken at the end of the risk management process, the underlying criteria for risk acceptance must characterise the entire risk management process. Risk acceptance decisions must take into account the organisation's business needs, both at the organisational and system-specific levels. It is also necessary to take laws and standards into account as well as the needs of the stakeholders that may be affected by the system. However, the research on risk acceptance is quite immature and many research questions remain to be answered. For instance, understanding threats is a vital part of the risk management process – and of risk acceptance – but how threats should be described is not clearly specified.

To clarify the basis on which risk acceptance decisions ought to be taken within the Swedish Armed Forces, overall risk acceptance criteria are needed. In addition, descriptions of how the overall risk acceptance criteria should be adapted within the organisation and how they affect the whole risk management process have to be added to existing instructions. It is also important to realise that technology and needs can change rapidly and that the assessments will never be perfect, so regular follow-ups of analyses and decisions are necessary.

Keywords: Risk management, risk analysis, risk acceptance, criteria, cost, benefit, economy, information security, IT systems, stakeholders, security investment

Innehåll

1	Inledning	7
2	Riskacceptans i litteraturen	9
2.1	Forskning.....	9
2.1.1	Avvägningen mot kostnad och nytta	11
2.1.2	Intressenter och moraliska synsätt.....	13
2.1.3	Antagonister	15
2.1.4	Psykologisk bias.....	16
2.1.5	Kommunikation.....	17
2.1.6	Genomförbarhet och förbättring	19
2.1.7	Måtkriterier	21
2.2	Standarder.....	23
2.2.1	Vad riskacceptans innebär	25
2.2.2	Vad som utgör grund för riskacceptansbeslut.....	27
2.2.3	Svårigheter med riskacceptansbeslut	29
2.3	Branschspecifika vägledningar	30
2.3.1	Återfallsrisk i brott inom rättspsykiatri	31
2.3.2	Fysisk samhällsplanering	31
2.3.3	Planering inom kärnkraftsindustrin.....	33
3	En ansats för riskacceptans	34
3.1	Behovsgrunden	35
3.2	Moraliska synsätt.....	39
3.3	Motsättningar och kommunikation	40
3.4	Misstag och kontinuerliga förbättringar	43
4	Slutsatser	45
4.1	Rekommendationer	45
4.2	Fortsatt forskning.....	46
5	Referenser	48

1 Inledning

När arbetet med framtagandet av nya IT-system initieras ska det utgå ifrån identifierade behov i verksamheten. De positiva effekter (nyttan) som IT-system förväntas ge verksamheten kan exempelvis utgöras av kvalitetsförbättringar, tidsbesparingar och kostnadsbesparingar.

Nya IT-system kan även ge negativa effekter för verksamheten. De negativa effekterna innefattar inte enbart risker, utan även kostnader för utveckling, drift och förvaltning av IT-systemen i sig såväl som kostnader IT-systemen orsakar för andra delar av verksamheten. Rationella beslut avseende utveckling av IT-system ställer därmed krav på att nytta, risker och kostnader förknippade med planerade IT-system kan identifieras, mätas och jämföras.

Genom kunskap om förväntade effekter med avseende på nytta, kostnader och risk ges möjligheten att ta avvägda beslut i arbetet med att minska riskerna. I Försvarsmakten är framtagandet av nya IT-system förknippat med en noggrann riskhanteringsprocess (Försvarsmakten, 2013a, 2013b). Riskacceptans beskrivs i H SÄK Grunder (Försvarsmakten, 2013a, avsnitt 2.2.6) enligt följande.

När det gäller risker rörande säkerhetstjänst finns det i regel tydliga krav på säkerhetsskydd varför bedömningen i normala fall tar ställning till om regelverkskraven är uppfyllda. Är kraven uppfyllda och hotbilden i övrigt inte ger anledning att vidta skyddsåtgärder utöver kraven accepteras risken. I praktiken innebär det att nuvarande skyddsåtgärder bedöms som tillräckliga.

Inom Försvarsmakten finns även andra dokument som ger stöd till riskhanteringsarbetet. Ett exempel är Försvarsmaktens gemensamma riskhanteringsmodell (Försvarsmakten, 2009, avsnitt 2.3.5) som formulerar stödet vid ett avslutande riskacceptansbeslut enligt följande.

När den aktuella risken analyserats, har chefen att ta ställning till något eller några av de principiella beslutsalternativen enligt nedan:

- a) Fatta beslut om att den bedömda risknivån är acceptabel i förhållande till sökta effekter eller uppgiftens lösande och kostnader för riskminskning (medvetet risktagande).*
- b) Fatta beslut om skyddsåtgärder med egna resurser för att minska risken till en acceptabel nivå.*

- c) Om de egna resurserna inte är tillräckliga,
hemställa om stöd från högre chef.*

Med anledning av de båda analysmetodernas kortfattade beskrivningar av riskacceptans, är rapportens målsättning att beskriva på vilka grunder beslut om riskacceptans ska tas för att uppnå en rationell avvägning mellan risk, kostnad och nytta – framförallt för Försvarmaktens planerade IT-system. I detta ingår också att reda ut när och hur de specifika beslutsgrunderna kan etableras.

En litteraturstudie med rekommendationer från forskningslitteratur, standarder och branschspecifika vägledningar beskrivs i kapitel 2. En ansats för riskacceptans ges i kapitel 3. Rapporten avslutas i kapitel 4 som presenterar slutsatser med både praktiska rekommendationer för Försvarmakten och förslag för fortsatt forskning.

2 Riskacceptans i litteraturen

I detta kapitel redovisas genomgångar av tre olika litteraturkategorier med avseende på ämnet riskacceptans: forskningsartiklar, standarder samt branschspecifika vägledningar. Avsnittet om forskningen är mer problematiserande till sin natur, vilket medför att det är mer omfattande än avsnitten om standarder och vägledningar.

2.1 Forskning

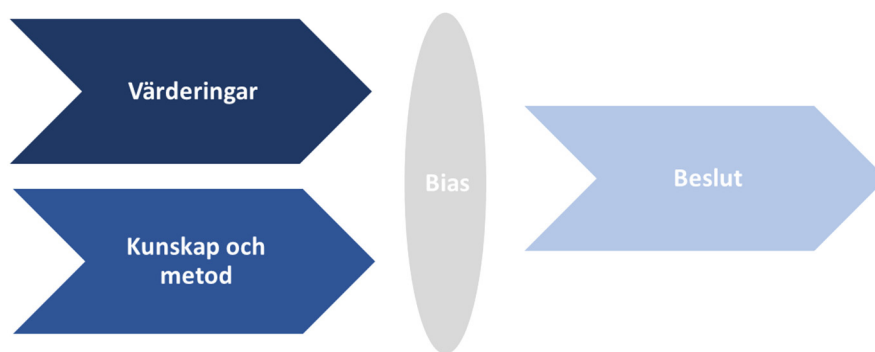
För att hitta relevant forskningslitteratur genomfördes initialt en övergripande sökning för att identifiera lämpliga söktermer. Därefter tog en mer fullskalig sökning i forskningslitteraturlöparen Scopus vid, kompletterat med Google Scholar. Denna andra sökning gjordes efter litteratur som i rubrik, nyckelord eller sammanfattning innehöll något av de engelska begreppen "risk comparison", "risk acceptance", "risk tolerance", "risk acceptability" eller "risk-benefit", som alltså rör just riskacceptans. Även intressant litteratur som refererades i hittade artiklar inkluderades. Fokus låg på forskningsartiklar publicerade tidigare 2012, men sammanställande artiklar tilläts vara från vilket år som helst. Artiklar som nämnde någon variant av "risk criteria" (riskkriterier) togs också med utan årsrestriktion. En annan begränsning gavs av att artiklarna främst borde fokusera på hur kriterier ska erhållas, snarare än redan fastlagda kriterier vars relevans är begränsad utanför artiklarnas studerade kontext. Artiklar inom forskningsområdet medicin beaktades mestadels inte, då de till stor del fokuserade på just redan fastlagda kriterier, vilket är långt från de avvägningar som är fokus i denna studie. Dessutom inkluderades enbart artiklar som var tillgängliga utan särskilt inköp.

En stor del av forskningslitteraturen om risk och riskhantering i allmänhet kan sammanfattas med synen att riskhantering är ett dåligt verktyg för att strukturera öka informationssäkerheten, men att det inte finns något bättre alternativ. Även om det snart är trettio år sedan Baskerville (1991) gjorde denna observation har läget inte förändrats drastiskt. Vidare lyfter Golob och Kožuh (2016) fram hur omogen riskhanteringen är inom kärnkraftsområdet, trots den viktiga kontexten och att det mer eller mindre var där riskhanteringsprocessen föddes. Hansson och Hirsch Hadorn (2017) samt Aven (2016b) poängterar dessutom att dagens riskhantering fokuserar på kvantifiering trots att det konceptuella (såsom terminologi, processteg, struktur och bedömningsgrunder) inte är klarlagt, varför tillräcklig grund för kvantifiering saknas. Eftersom riskhantering anses vara ett oprecist verktyg är det inte förvånande att det nästan helt saknas forskning som explicit berör riskacceptans, som är en del av riskhanteringen. En del artiklar nämner visserligen begreppet riskacceptans, men utan att på allvar diskutera vilka kriterier som är lämpliga. Riskacceptans och specificering av

riskacceptanskriterier – som ska avgöra, eller åtminstone vägleda, om en risk är acceptabel eller inte – kan därmed delvis utgöra nya forskningsområden, åtminstone i kontexten informationssäkerhet (Pan och Tomlinson, 2016).

Ett 60-tal artiklar från den fullskaliga sökningen identifierades som åtminstone delvis intressanta och detsamma gällde ett 20-tal från den inledande sökningen i kombination med artiklar som genom tidigare erfarenhet redan hade identifierats som intressanta. En inledande presentation av avvägningen mellan risk, kostnad och nytta finns i avsnitt 2.1.1. De övriga avsnitten har större fokus på just risk, men en stor del av resonemangen där kan även appliceras på kostnad och nytta.

Om riskacceptansbeslutet ska baseras på den övriga riskhanteringsprocessen, måste rimligen riskacceptansens beslutskriterier prägla hela riskhanteringsprocessen så att resultatet blir ett relevant underlag (Johansen och Rausand, 2014). Det är till och med rimligt att själva beslutet implicit medförs, eller utgörs, av de andra delarna av riskhanteringsprocessen, snarare än att utgöra ett eget explicit steg. Vidare måste beslutskriterierna rimligen bero på intressenternas värderingar och därmed hur de ser på riskerna och de andra aspekterna som påverkar, det vill säga kostnaden och nyttan. Dessutom påverkar både kunskap och metod (Hansson och Hirsch Hadorn, 2017). Psykologisk bias påverkar också (Montibeller och von Winterfeldt, 2015). Som Figur 1 illustrerar kan förståelsen av intressenternas beslut därför utgå från intressenternas värderingar och tolkas utifrån deras (och tolkarnas) kunskap, metoder och psykologiska bias.



Figur 1: Beslut som en funktion av en grund (värderingar), hjälpmedel (kunskap och metod) och den försämrande linsen (bias).

Avsnitt 2.1.2 beskriver därför intressenterna och olika moraliska synsätt. Därefter följer avsnitt 2.1.3 om de illasinnade intressenterna – antagonisterna. I avsnitt 2.1.4 tas bias upp, medan avsnitt 2.1.5 tar upp hur tolkningarna av intressenternas behov kan kommuniceras.

Ibland kan det bli svårt att överhuvudtaget nå ett beslut, det vill säga genomförbarheten kan vara för låg. Detta kan bero på exempelvis alltför mycket bias, men framförallt begränsad kunskap eller en undermålig metod. Genomförbarheten behandlas vidare i avsnitt 2.1.6. Samma avsnitt tar också upp de andra följderna av begränsad kunskap och en undermålig metod, nämligen att beslut visserligen nås men bara av låg kvalitet. Dessa följder ställer dessutom krav på en kontinuerlig förbättringsprocess, varför förbättringar också presenteras i avsnittet.

Ett avslutande avsnitt, 2.1.7, beskriver mätkriterier. I enlighet med tidigare resonemang kan kriterierna lika gärna appliceras på risk som på kostnad eller nytta, även om de i stora delar har sina rötter i riskområdet. Vidare – och också i enlighet med tidigare resonemang – kan dessa kriterier närmast likställas med riskacceptanskriterier. En väl utförd riskhantering i övrigt ger ju upphov till riskacceptansbeslutet, om än implicit.

2.1.1 Avvägningen mot kostnad och nytta

En slutsats som kan dras från genomgången av Spouge (2014) är att mycket forskning (och för den delen vägledning) har fokuserat på att sätta specifika gränsvärden för risk i olika situationer och branscher – framförallt olje- och kemikalieindustrin samt vägsäkerhetsområdet – snarare än att ta fram kriterier för att sätta gränsvärdena. En återkommande kritik mot fasta riskgränsvärden är att kostnaden för att få ner risken kan bli oproportionerligt hög (Abrahamsen och Aven, 2008; Baybutt, 2014a; Spouge, 2014). Dessutom kan det innebära att fokus hamnar på just gränsvärdena, snarare än den faktiska risken och säkerheten (Aven och Ylönen, 2016). Det blir lätt en olämplig mekanisk process (Aven och Vinnem, 2005) som ignorerar möjlig nytta (Hansson och Hirsch Hadorn, 2017).

Ett alternativ är att istället fokusera på att minska riskerna bara så länge det är kostnadseffektivt att göra det. Detta alternativ har flera namn, men vanligast är förkortningen ALARP (efter engelskans *as low as reasonably practicable*). Idén är att minska risken från oacceptabel så långt som möjligt, vilket inte nödvändigtvis betyder hela vägen till vad som kan kallas allmänt acceptabelt (Baybutt, 2014b). Kvarstående risk är alltså snarare något som måste *tolereras* – utifrån de risker som finns och hur kostnadseffektiva skydderna är – snarare än något som *accepteras* (Kasperson, 1983; Abrahamsen, Røed och Jongejan, 2013). En möjlig tolkning är att ALARP-zonen ligger mellan gränserna för vad som är tolerabelt respektive acceptabelt (Ge *m.fl.*, 2017) (Figur 2). Det är inte säkert att en acceptabel risknivå kan nås, men strävan är att nå dit, eller åtminstone så lågt som möjligt i ALARP-zonen. ALARP medger alltså användning av system som medför större risk än vad som är uppenbart acceptabelt, om alternativet är inget system alls och förutsatt att den möjliga nyttan väger tyngre än risken och kostnaderna (Richter och Sereaseanu, 2015).



Figur 2: ALARP-zonen (tolerabel risknivå) ligger mellan den allmänt acceptabla nivån och den oacceptabla.

Det saknas dock stöd i litteraturen för exakt hur avvägningen mot kostnad och nytta ska göras. Det finns visserligen en mängd olika teoretiska modeller för ideal investering i informationssäkerhet, men empiri som kan bekräfta dessa teorier saknas. Dessutom bygger de teoretiska modellerna på en rad olika tveksamma antaganden (förenklningar). Dels tas inte befintliga investeringar i beaktande, dels antas nya skyddsåtgärder komma till ett fast pris och till exponentiellt avtagande effekt. Minskad nytta beaktas inte och inte heller att olika steg i angreppssekvenser är beroende av varandra. Med stöd av sådana antaganden drar trots allt Gordon och Loeb (2002) slutsatsen att den optimala investeringen i IT-säkerheten aldrig överstiger $1/e$ (ungefär 37 %) av den maximala förlusten. Forskningen på området sammanfattas i (Hermelin, Karlzén och Nilsson, 2014). Monahan och Silver (2003) framhäver istället att avvägningen måste baseras på en policy (varje organisations egna överväganden), snarare än att det finns ett allmängiltigt svar i vetenskapen.

En del inspiration till att jämföra risk med kostnad och nytta kan hämtas från forskningen om jämförelser mellan olika typer av risker. I exempelvis metrikerna funktionsjusterade levnadsår (eng. Disability Adjusted Life Year) och kvalitetsjusterade levnadsår (eng. Quality Adjusted Life Year) görs en avvägning mellan dödsfall och livskvalitet över tiden (Abrahamsen, Røed och Jongejan, 2013). Att väga in antal år kvar att leva har dock kritiserats som ett slags rå seniorrabatt där livet hos den som är närmare medellivslängden värderas lägre än för yngre personer (Fischhoff, 2015). Vidare är det också vanligt att översätta mellan människoliv och pengar (även om de exakta översättningarna varierar). Då behövs resonering om varför de olika typerna av värden värderas på de sätt de gör (Hansson och Hirsch Hadorn, 2017), vilket görs i nästa avsnitt (2.1.2).

En annan vanlig typ av risk som kan vara svår att hitta lämpliga enheter för är miljöförstöring. Förutom rena bedömningar av hur stort område som drabbas eller hur permanent förstöringen är, kan människors reaktioner på tidigare miljöförstöring mätas. Till exempel fick oljeutsläppet från Deepwater Horizon betydlig mer uppmärksamhet än de elva dödsfallen och den enorma finansiella påverkan (Schmidt, 2016). Slovic (1987) pekar på att jämkning av risker av olika typ kan utelämna faktorer som människor behöver för att kunna bedöma risken.

Dessutom råder det olika meningar om hur direkta förluster (konsekvenser) ska vägas mot indirekta förluster (Ge *m.fl.*, 2017).

2.1.2 Intressenter och moraliska synsätt

Ett vanligt fel i riskhantering som påpekas av forskningslitteraturen är att inte beakta samtliga intressenter. Till exempel kommer experter som anlitas i riskanalyserna falla tillbaka på *sina* värderingar när de saknar fullständig kunskap (Shrader-Frechette, 1991) och de svagaste i samhället beaktas minst (Altarawneh, MacKee och Gajendran, 2016). En utmaning i riskhanteringen är därmed att veta var systemgränsen ska dras och därmed vilka konsekvenser – och vilka intressenter – som ska beaktas. Exempelvis kan gränsen dras vid den egna organisationen, eller på nationell nivå, beroende på hur fullständig analysen ska bli och hur mycket detaljer som ska tas med (Johansen och Rausand, 2014). Om två system ska kopplas samman kan det dessutom vara svårt att avgöra var systemgränserna går för vart och ett av systemen och vilket system som ska ta ansvar för vad (Hallberg, Bengtsson och Karlzén, 2016).

Hansson och Hirsch Hadorn (2017) lyfter fram att ren utilitarism – där mängden lycka ska maximeras – kan leda till att en persons lycka går ut över en annan person och att den totala lyckan, eller risken, därmed bör utvärderas per person. Det gäller att få med alla intressenters argument, både uttryckta och uppdagade preferenser samt underförstådda sådana för de som inte har möjlighet att själva uttrycka dem (Altarawneh, MacKee och Gajendran, 2016; Hansson och Hirsch Hadorn, 2017). Det är viktigt att ta ansvar för, snarare än att förneka, de motsättningar och risker som finns (Altarawneh, MacKee och Gajendran, 2016). Exempelvis verkar förnekande av risker ha bidragit till katastrofen i Fukushima (Golob och Kožuh, 2016). Kopplat till detta kan risker alltså behöva minskas även när det ytligt sett ter sig alltför kostsamt. Kasperson (1983) uttrycker sig skarpare med att människoliv inte ska offras för praktiska begränsningar, vilket ställer tolkningen av hur mycket riskreducering som är rimlig (eng. reasonable; jämför föregående avsnitt om ALARP) på sin spets. En förvaltningsmyndighet eller domstol kan till exempel kräva att riskreducerande åtgärder görs så länge de inte är *kraftigt* oproportionerligt kostnadsdrivande jämfört med riskreduceringen (Abrahamsen, Røed och Jongejan, 2013). Dock låter norska myndigheter oljeindustrin ta fram egna riskacceptanskriterier, snarare än att det görs direkt av myndigheterna som bättre tar hänsyn till samhällets vilja. Å andra sidan är det oklart vilka regleringar som är effektiva och vilka som hämmar innovation och leder till onödiga investeringar (Hermelin, Karlzén och Nilsson, 2014). På samma sätt som enskilda organisationers optimala informationssäkerhetsinvestering blir mindre bra för samhället (Anderson, 2001; Liu, Ji och Mookerjee, 2011) kan myndigheternas regler ge organisationerna problem (Hansson och Hirsch Hadorn, 2017). Anderson *m.fl.* (2012) drar, med

stöd av empiri, slutsatsen att mer pengar borde läggas på proaktiva skydd (exempelvis polisiära åtgärder) för att minska hoten.

Vidare kan det vara värdefullt att redovisa både medelvärden (ungefär förväntad risk) som kan användas i rena utilitaristiska kalkyler och extremvärden som kan peka på vad som kan hända enskilda (Johansen och Rausand, 2014). Detta är relaterat till de resursbegränsningar olika intressenter kan ha. Exempelvis kan personer med större förmögenhet eller tryggare anställning ta större finansiella risker. De faktorer som påverkar denna riskbenägenhet är dock inte helt klarlagda. I en studie visade det sig märkligt nog att män – till skillnad från kvinnor – snarare tar fler risker vid otryggare anställning (Fisher och Yao, 2017). Kanske en skillnad i långsiktighet spelar in, vilket trots allt skulle kunna förklara männens beteenden på ett rationellt sätt. I en annan studie visade sig 37 personer – som arbetade med risk- eller krishantering företrädesvis inom svenska myndigheter – samt 50 studenter som studerade relevanta områden, vara ganska riskbenägna. En anledning kan ha varit att scenarierna nådde toppen av respondenternas konsekvensskala ("en katastrof är en katastrof"), det vill säga när tillräckligt många människor dör så spelar det ingen roll om ännu fler dör (Abrahamsson och Johansson, 2006). Konsekvenser som ter sig oändliga (maximala) förekommer även för organisationer (Jaquith, 2007; Hubbard, 2009; Rakes, Deane och Rees, 2012).

För att väga in riskbenägenheten i riskhanteringen föreslår Hansson och Hirsch Hadorn (2017) att resonering sker utifrån hur illa det kan gå och väger det mot hur bra det kan gå, för att därefter justera med sin riskbenägenhetsfaktor. Hallberg, Bengtsson och Karlzén (2016) såg i en empirisk studie av riskbedömningar att de med mindre tilltro till sina egna svar, främst använde den mittersta och nedre delen av konsekvensskalan. Vidare har Champ, Moore och Bishop (2009) sett att större ovisshet leder till mindre spendering vid köp. Detta kan förklara den föregående studiens resultat, eftersom större konsekvenser förmodligen är förknippade med större skyddskostnad – det vill säga ett större köp. Alltså kan större ovisshet leda till både större felmarginal och till en annan riskbenägenhet.

Klart är att det finns många perspektiv som åtminstone måste övervägas för beaktande. Exempelvis bör ett globalt företag ta hänsyn till kulturella skillnader när riskacceptansbeslut tas (Baybutt, 2016) och beslut som påverkar samhället måste beakta både dagens befolkning och framtidens (Fischer *m.fl.*, 2013). Ett successivt upplägg används inom kärnkraftsindustrin där först kraftverkets design och drift analyseras, sedan fysiska barriärer mot läckage ut i omvärlden, för att slutligen utvärdera effekter på allmänhetens hälsa (Aven och Ylönen, 2016).

Det kan dock vara svårt att veta vilka legitima intressenter som finns. I Nederländerna har myndigheterna delat in olika moraliska synsätt i fyra kategorier som ska beaktas vid riskhantering (DNRA, 2009). Kategorierna har

sitt ursprung i forskningslitteraturen (Kahan *m.fl.*, 2007) och indelas i två axlar, från individualistiskt till solidariskt (kollektivt), och från de som vill ha klara hierarkiska regler (baserade på exempelvis kön, ursprung och förmögenhet) till de som vill ha en mer platt, egalitär (jämlig) struktur. Samma källa redovisar att de egalitära och solidariska är bekymrade över global uppvärmning och vill kontrollera mängden vapen i samhället, medan de individualistiska och hierarkiska tror att regleringar skadar ekonomin eller deras egna möjligheter att försvara sig. Motsättningarna kan också finnas mellan andra grupperingar, exempelvis tror de egalitära och individualistiska att abort är säkert för kvinnorna, medan de hierarkiska tror att det är osäkert. En förklaring kan vara att de hierarkiska lagda ser moderskapet som en viktig traditionell roll för kvinnor. Valfrihet har vissa beröringspunkter med kategorierna eftersom det till exempel kan präglas av individualism eller egalitarism (Kahan *m.fl.*, 2007). Valfrihet vad gäller risktagande har setts påverka riskacceptansen (Altarawneh, MacKee och Gajendran, 2016; Hungr *m.fl.*, 2016). Liknande aspekter är till exempel vana, rädsla, oro och rättvisekänsla (Fischhoff, 2015).

2.1.3 Antagonister

En avsevärd skillnad mellan informationssäkerhet och de områden merparten av riskforskningen inriktar sig på är att det finns antagonister. Antagonister är svåra att modellera (Sjöberg, 1999) och de har, genom bland annat internet, stora möjligheter att verka på avstånd och i det tysta samt med stor grad av automatisering. Detta gör bland annat att tillfälle i någon mån sammanfaller med kapacitet vilket blir en del i kunskapskomplexiteten. En annan sak som försvårar angående antagonister är att deras upplevelse spelar roll för vad som kan kallas angreppsvärdhet (snarare än skyddsvärdhet). Angreppsvärdhet kan närmare förklaras genom att först beskriva de sex olika sätt att värdera information på som presenteras i (Poore, 2000). Information kan värderas enligt vad den skulle kosta att ersätta eller vilken operationell kostnad det skulle innebära om tillgång till den saknades. Dessa två värderingssätt har att göra med hur skyddsvärd informationen är, eftersom den egna organisationen har nytta av den. Två andra värderingssätt har snarare att göra med att någon annan vill åt informationen (oavsett om man själv behöver den), det vill säga hur angreppsvärd den är. Dessa två senare värderingssätt tar sin utgångspunkt i informationens exklusivitet, eller vilket ansvar (eng. liability) individen har att se till att den inte hamnar i orätta händer. De två sista värderingssätten berör både skyddsvärdhet och angreppsvärdhet, nämligen vad informationen skulle kunna säljas för, eller konverteras till.

En annan sak som är speciellt angående antagonister är att straffande skydd kan fungera, eftersom antagonistens intention att angripa åtminstone delvis kommer att variera med risken att åka fast. Cremonini och Martini (2005) använder begreppet *return-on-attack* (avkastning av attack), i likhet med det vedertagna

return-on-investment (avkastning av investering). På sätt och vis kan det ses som att rollerna angripare (antagonist) och försvarare delvis är omvända. Härmed finns också en omvänd asymmetri. På samma sätt som den vanliga asymmetrin, där systemförsvararen måste täppa till alla hål men angriparen bara behöver hitta ett, kan en antagonist tänkas angripa enbart om alla sätt att bli straffad kan undvikas. Spelteori har föreslagits som en lämplig metod för att hantera angriparnas anpassning och förhållandet till försvararen (Paté-Cornell och Guikema, 2002).

2.1.4 Psykologisk bias

En aspekt som försämrar beslutsinsens skärpa är psykologisk bias, ett slags anti-kunskap. Ett exempel på detta är att ovisshet (låg kunskap om framtiden) ofta ses som något negativt, även om ovissheten lika gärna kunde följas av positiva händelser som negativa (Montibeller och von Winterfeldt, 2015). Ett annat exempel är att beslut ofta baseras på förutfattade meningar, där lättillgänglig information övertolkas, bland annat hos kliniker inom rättsmedicinen som lägger större vikt vid de riskfaktorer som ligger inom deras ansvarsområde (Sturidsson *m.fl.*, 2004). Det har ofta underskattats att tolkaren av intressenterna – oftast analytikern eller experten – har stor betydelse i riskhanteringsprocessen (Hassenzahl, 2006). Faktum är att riskbedömningar av olika analytiker visat sig kunna variera med flera magnituder för identiska fall (Abrahamsen, Røed och Jongejan, 2013) och att vilka typer av experter som deltar påverkar (Aven och Guikema, 2011). Vidare har samstämmigheten mellan experter inom informationssäkerhetsområdet i vissa situationer visat sig vara lägre än för lekmän (Hallberg *m.fl.*, 2017; Karlzén, Bengtsson och Hallberg, 2017).

Ytterligare ett exempel på bias är en typ av kulturell förnekelse som inträffar när en varningssignal om att ett hot håller på att förverkligas, inte tas på allvar. Det uppstår alltså en kultur där det förnekas att tillräcklig kreativitet för att förutse hotets förverkligande saknas (Pidgeon, 1998; Paté-Cornell, 2012). Ett exempel som tillskrivits sådan förnekelse är förlusten av rymdfärjan Challenger 1986 och dess besättning (Pidgeon, 1998). Ett annat är Tjernobyl-katastrofen samma år, där sovjetiska myndigheter verkar ha bedömt sitt säkerhetsarbete som överlägset det amerikanska, varför varningssignalen Three Mile Island sju år tidigare inte togs på allvar. Ironiskt nog bedömde många i väst efteråt att en olycka som Tjernobyl inte kunde inträffa i väst (Pidgeon, 1998).

En sätt att minska bias har att göra med att minska komplexiteten för de enskilda bedömningarna (Montibeller och von Winterfeldt, 2015). Att då strukturera processen och bryta ner hoten i mindre beståndsdelar verkar vara effektivt, åtminstone för experter (Hallberg, Bengtsson och Karlzén, 2016; Hansson och Hirsch Hadorn, 2017). På så sätt kan varningssignaler uppfattas (Paté-Cornell, 2012) och latent fel observeras, under förutsättning att larm med hög känslighet finns (Anderson, 2001). Ett exempel på att strukturerat resonera om beroenden är

vad som på engelska benämns *cross-impact analysis* (sv. korsinverkansanalys) (Turoff och Bañuls, 2011). Olika faktorer som påverkar riskhanteringen kan relateras till varandra genom en begreppskarta eller en matris med viktade värden som vart och ett motsvarar ett förhållande mellan två faktorer. Detta har exempelvis använts för att analysera skyddsåtgärder mot terrorism (Schoenenberger, Schenker-Wicki och Beck, 2013). Ett annat exempel är en jämförelsebaserad metod – där exempelvis sannolikheter bedöms gentemot varandra i hierarkier (Montibeller och von Winterfeldt, 2015; Hallberg, Bengtsson och Karlzén, 2016). Ökad struktur kan bland annat minska beroenden mellan olika aktiviteter i riskhanteringen, vilket till exempel gör att rätt personer kan ta sig an rätt aktivitet. Dock kan det finnas beroenden mellan olika aktiviteter som gör dem svåra att utföra var för sig. Dessutom är en svårighet med uppdelningen att det måste gå att få ihop aktiviteternas resultat på slutet (Hansson och Hirsch Hadorn, 2017).

Montibeller & von Winterfeldt (2015) rekommenderar också en flexibel och inkluderande process där olika metoder kan användas och ny information anamlas och som präglas av kreativitet. Dessutom rekommenderas det att flera experter anlitas och att experterna får träning och utbildning i sannolikheter och bias. Ett annat sätt att minska bias är att ha olika experter som kan arbeta i grupp där olika alternativa bedömningar får utrymme och olika experter får debattera fritt (Paté-Cornell, 1996; Montibeller och von Winterfeldt, 2015). Det är då viktigt att se till att debatten är fri och inte leder till grupptänkande genom att experterna förstärker varandras (gemensamma) åsikter trots att mängden erfarenhet är begränsad (Paté-Cornell och Fischbeck, 1995). Ett alternativ är att låta experterna granska varandras arbete för att öka kvaliteten och ansvarstagandet (Apostolakis, 2004; Montibeller och von Winterfeldt, 2015). Viktigt att komma ihåg i sammanhanget är att sämre bedömare överskattar sin förmåga, medan bättre bedömare är mer blygsamma (Dunning, 2011).

Flera ytterligare potentiellt bias-minskande alternativ nämns av Montibeller & von Winterfeldt (2015): historiska frekvenser bör separeras från framtida sannolikhetsbedömningar, kostnader och nytta bör separeras från varandra och bedömningar av indirekta konsekvenser bör jämkas med direkta konsekvenser genom en viktning. Som helhet bör det nämnas att både dessa och de tidigare nämnda rekommendationerna för att minska bias i huvudsak är rent teoretiska och saknar empiriska tester.

2.1.5 Kommunikation

Riskhanteringen måste präglas av de intressenter som finns och en transparens (spårbarhet) som möjliggör granskning av att intressenternas behov tillgodosätts (Spouge, 2014). Därför krävs att olika intressenter förstår varandra (och sig själva) och lyckas dra rätt gränser för vad som ska beaktas. Fungerande kommunikation kräver att gjorda antaganden är tydliga (Johansen och Rausand,

2015; Aven och Ylönen, 2016), att begrepp och sätt att uttrycka sig på är entydiga (Johansen och Rausand, 2015; Hansson och Hirsch Hadorn, 2017) och att resonerandet görs på ett distinkt vis (Johansen och Rausand, 2015).

Riskhanteringsprocessen anses ofta medföra god kommunikation mellan beslutsfattare och säkerhetsexperter (Baskerville, 1991). Exempelvis leder formella *business case* (sv. affärsfall; som kan vara en del av riskhanteringen) till att mer pengar avsätts för skyddsåtgärder (ISBS, 2008). Det kan också vara fördelaktigt med visualiserande redovisning, som exempelvis att rita in riskzoner på en karta vid nybyggnation i ett trångt samhälle (Geerts *m.fl.*, 2016). Intressant att notera är att riskmatriser, som ofta används, fungerar dåligt när det råder negativ korrelation mellan konsekvens och sannolikhet – vilket rimligen är vanligt i praktiken. Matriserna kan nämligen ge ett felaktigt intryck av prioriteringsordningen mellan olika risker, även om de kan fungera belysande i vissa situationer (Cox, 2008). Fungerande kommunikation mellan analytiker och verksamhetskunniga överlag är viktigt för att ta fram riskacceptanskriterier med verklighetsförankring (Schmidt, 2016).

En viktig tråd i de senaste tio årens forskning är att tydligt redovisa hur reliabla (tillförlitliga) riskbedömningarna är. Att lägga mer fokus på kunskap om risken, snarare än enbart bedömningen av densamma, förespråkas också i standarden ISO 31000 (SIS, 2011) samt av norska petroleummyndigheten (Aven och Ylönen, 2016). En metod som tar felmarginalen i beaktande presenteras av Garvey, Moynihan och Servi (2013). Paté-Cornell och Fischbeck (1995) föreslår användning av bayesianska sannolikhetsmodeller för att uttrycka måttet av reliabilitet. Goerlandt och Reniers (2016) föreslår att reliabiliteten illustreras av geometriska figurer där figurernas storlek, färg och kontur indikerar reliabiliteten och källan till (den ofullständiga) reliabiliteten. Som framgår av Goerlandt och Reniers (2017) fortgår en akademisk diskussion om huruvida detta är ett lämpligt sätt att belysa reliabiliteten.

Ett sätt att avgöra riskbedömningarnas reliabilitet, är att använda de kriterier som Aven och Ylönen (2016) föreslagit. Ökad expertsamstämmighet, mer rationalitet, mer realism, mer data och ökad möjlighet att modellera de inblandade fenomenen är alla tecken på högre reliabilitet. Ett exempel på hur data kan spela roll är i försäkringsbranschen. När mer data finns (som för dödsfall och bilolyckor) är prediktionsmodellerna rättframma, medan försäkringar mot skadestånd inte har samma tillgång på data (Paté-Cornell och Deleris, 2009). Förutom avsaknaden av data måste också reliabiliteten för data beaktas (Hansson och Hirsch Hadorn, 2017). Viss försiktighet måste till exempel iaktas när historiska data används för att förutsäga framtida skeenden eftersom framtida skeenden inte nödvändigtvis fungerar på samma sätt som skeendena gjorde tidigare (Paté-Cornell och Deleris, 2009; Aven, 2015). Detta kan liknas vid att slutsatser om orsakssamband dras utan att först ha formulerat hypoteser (Hubbard, 2009; Hansson och Hirsch Hadorn, 2017). Något annat som spelar roll

för reliabiliteten är själva metoden eller processen (Gardoni och Murphy, 2014). En linjal kan vara framtagen för att ha millimeterprecision, men om den är felkonstruerad, eller används fel, blir validiteten lägre än avsett. Det bör också observeras att ökad ovisshet inte bara leder till större felmarginal, utan också till generellt lägre konsekvensbedömningar (Hallberg, Bengtsson och Karlzén, 2016).

Att använda försiktighetsfaktorer, det vill säga att med mening överdriva risken, anser Aven (2016a) vara olämpligt, eftersom det gör jämförelser svårare. Försiktighetsfaktorer är dock vanliga vid toxicitetsbedömningar inom bland andra livsmedels- och läkemedelsindustrierna. För att slutsatser från djurförsök ska kunna appliceras på människor används exempelvis en tio-faktor. För att kompensera för individuella skillnader används en tio-faktor till, vilket ger en total faktor på 100 mellan resultat från djurförsök och rekommendationer för människor. Vidare används ytterligare försiktighetsfaktorer, exempelvis för att skilja mellan kort och lång exponering, otillräckliga data, likhet med andra farliga ämnen och den potentiella negativa effektens varaktighet (Dankovic *m.fl.*, 2015).

2.1.6 Genomförbarhet och förbättring

Förutom att ha en genomtänkt riskhanteringsprocess ur ett teoretiskt perspektiv, behöver processen och de relaterade målen också vara genomförbara för att riskhanteringen ska kunna komma till användning (Hansson och Hirsch Hadorn, 2017). Till exempel finns det många olika sätt att bedöma jordskredsrisik, men metoderna är alltför komplicerade för att kunna användas på de platser de verkligen behövs, vilka oftast präglas av fattigdom och därmed begränsad möjlighet att få det stöd som behövs (Hungr *m.fl.*, 2016).

Ett annat exempel är de hot som kallas ”svarta svanar”. De utgörs av mycket svårförutsägbara hot, varför genomförbarheten av korrekta bedömningar är låg. Begreppet och mycket av diskussionerna kring de svarta svanarna förs på andra områden och det är inte klarlagt i vilken utsträckning sådana hot finns, åtminstone inte på IT-området (Hubbard, 2009). Men de snabba förändringarna och komplexa systemen gör de svarta svanarna troliga även inom detta område. Svarta svanar brukar vidare ses som lågsannolika hot, vilket är hot som det är svårt att ha intuitiv förståelse för (Desaulniers, 1991; Hansson och Hirsch Hadorn, 2017). Skydd å andra sidan tenderar att vara specialiserade vilket gör det svårt att möta en okänd risk (Schudel och Wood, 2000). För att trots allt hitta de svarta svanarna innan det är för sent, krävs en helhetssyn på risker och felkällor (Paté-Cornell, 2012; Burns och Miller, 2014) där kreativitet präglar analyserna (Paté-Cornell, 2012). Mer om svarta svanar finns beskrivet i Hermelin, Karlzén och Nilsson (2014).

Den bristande genomförbarheten av riskhanteringsprocessen kan också ta sig uttryck först senare. Exempelvis kan föreslagna skyddsåtgärder få oönskad effekt. En parallell ges av att det finns indikationer att lagar om bilbältesanvändning inte räddat liv totalt sett. Bältena gör att bilisterna känner sig säkrare varför de kör mindre försiktigt. Detta innebär att risktagandet delvis förskjutits från bilisterna som tidigare inte hade bälte till bland andra cyklister som utsätts för (ännu) mer vårdslösa medtrafikanter (Adams, 1999). Anledningen till den hårdare körningen är rimligen att bilisten ser större nytta med det nya – förmodligen snabbare eller trevligare – sättet att köra. Bilisten utnyttjar därmed inte den nya skyddsåtgärden för att öka säkerheten, utan ökar istället nyttan vid samma risknivå: bilbältet tillät en annan avvägning mellan risk, kostnad och nytta. Bilisten kompenserar omedvetet för bältet för att hålla sin risknivå stabil (Adams, 2006). Därmed blev kanske effekten delvis positiv (nyttoökande) men inte på det avsedda sättet (riskreducerande) och negativ (riskhöjande) för cyklisterna, som då drabbas av hotet från biltrafiken. Cyklisterna kan därmed känna sig tvingade att anpassa sitt beteende och ta en annan väg. Stewart (2004) drar slutsatsen att riskkompensationen kan innebära en annan distribution av risk mellan intressenterna – en moralisk fara (eng. moral hazard). Ett annat exempel på riskkompensation från samma källa är att fallskärmshoppning inte är säkrare än tidigare, trots teknisk utveckling som ser till att fallskärmshopparens fallskärm utvecklas vid en viss höjd. Skyddet mot att fallskärmshopparen inte klarar av att själv initiera fallskärmens utveckling har förmodligen gjort fallskärmshopparna mindre försiktiga. Ytterligare exempel är att låsningsfria bromsar, som förhindrar hjullåsning på bilar, har medfört mer aggressiv bilkörning (Stewart, 2004) samt att unga rugbyspelare tacklar hårdare när de bär hjälm (Hagel och Meeuwisse, 2004). Det bör dock noteras att dessa förändrade beteenden inte nödvändigtvis har lett till ökade antal olyckor.

En slutsats som kan dras från ovanstående exempel på riskkompensation är att skyddsåtgärder

- istället för att minska risken kan vara utan effekt på grund av beteendeförändringar
- visserligen kan ha en positiv effekt, men snarare på nytta än i form av riskreducering
- till och med kan flytta risken till en annan intressent.

Att öka säkerhetsmedvetandet snarare än att fokusera på lagar och teknik verkar alltså vara av vikt i dylika situationer. Exempelvis har nederländska cyklister en mycket tryggare miljö vilket leder till en mycket säkrare situation än den för australiska cyklister som har hjälmtvång (Stewart, 2004). Ansvar måste också tas för att minska förflyttningen av risker mellan intressenter, vare sig det är mellan olika typer av trafikanter, samhällsklasser, generationer eller andra (Kasperson, 1983).

Allteftersom kunskap byggs upp kommer det att finnas utrymme för kontinuerlig förbättring. Till exempel kan riskhanteringen dra nytta av teststatistik för att förbättra riskhanteringen och även återkoppla till testningen med de lärdomar som riskhanteringen ger (Erdogan och Stølen, 2012). Organisationen måste också anpassas för processen. Då går det exempelvis att se till att rätt personer involveras vid rätt tidpunkt och möjliggöra att beslut som kan skjutas upp, tas vid senare tillfällen när mer kunskap har inhämtats (Hansson och Hirsch Hadorn, 2017). Vidare lyfter Davis (2005) fram positiva bieffekter som exempelvis ökad kunskapsspridning i organisationen till följd av riskhantering.

En mellanväg kan vara att se till att ett nytt system åtminstone inte är sämre än ett existerande. Det är ju inte rimligt att bara beakta en risk för ett nytt system men inte samma risk för ett existerande system, jämför med Hansson och Hirsch Hadorn (2017). Samma resonemang gäller kostnader och nytta. Jämförelsebaserad riskhantering skulle också kunna spara in mycket analyser och dokumentation som en rent kvantitativ metod kräver. För vägtunnlar i Norge föreslår Abrahamsen, Røed och Jongejan, (2013) därför tre nivåer av riskbedömningar. För tunnlar som inte har speciella utmaningar vad gäller säkerheten (eng. safety) i själva tunneln eller omgivningarna räcker det att göra enligt best practice, ett slags checklistemetod. I nästa nivå kan tunnelarna kräva avvikelser från best practice, men åtgärder som ger samma säkerhet som best practice kan användas och redovisas främst kvalitativt. Först för särskilt svåra tunnlar anser källan att en mer fullödlig riskbedömning behövs. Slutligen är det bra att vara så flexibel i metodiken som möjligt, vilket möjliggör jämförelse med andra system i andra kontexter och organisationer (Spouge, 2014). Samtidigt måste flexibiliteten vägas mot att vara så specifik som möjligt för maximal precision för det aktuella systemet. Apostolakis (2004) går ett steg längre och framhåller att riskhanteringen bör kompletteras med traditionella säkerhetsmetoder som försvar-på-djupet.

2.1.7 Måtkriterier

Johansen och Rausand (2014) föreslog, delvis baserat på en norsk oljebranschstandard, ett antal kriterier för att utvärdera riskmetriker, det vill säga huruvida sättet att mäta risk är bra. Att mäta risk på ett bra sätt är essentiellt för att kunna använda riskhanteringsresultat som beslutsunderlag (riskacceptansbeslutet). Jaquith (2007) har också kriterier för bra riskmetriker, medan Fischhoff m.fl. (1980) har kriterier med det snarlika syftet att utvärdera metoder som använder riskmetriker. Vidare presenterar J. Hansson m.fl. (2011) principer (kriterier) för hur systemutvecklingskrav ska redovisas. Vanem (2012) tar upp principer (kriterier) som ska vägleda etableringen av riskacceptansen. Kriterierna som helhet och vilka källor som täcker vilka kriterier, beskrivs i Tabell 1. De kursiva kriterierna är på en övergripande nivå, medan de inskjutna är på en lägre abstraktionsnivå och sorterar under de övergripande.

Tabell 1: Kriterier för att mäta på ett bra sätt. Symbolen ● betyder att kriteriet täcks in av källan. Källor: a = Johansen och Rausand (2014); b = Fischhoff m.fl. (1980); c = Jaquith (2007); d = J. Hansson m.fl. (2011); e = Vanem (2012). Innebörden är definierad enligt källa (a), utom för verifierbarhet som kommer från SIS-TR 50 (2015) samt de två sista som är enligt källa (b).

Kriterium	Källa					Innebörd
	a	b	c	d	e	
<i>Validitet</i>	●	●		●	●	Fullständighet, detaljrikedom
Reliabilitet	●					Analytikersamstämmighet, visshet
Rationalitet	●	●				Logisk, sund och underbyggd bas
Kontextuellt	●		●			Beaktar kontexten
Specificitet	●					Beaktar specifikt system
Jämförbarhet	●					Allmängiltighet (system)
Konsistent	●		●			Allmängiltighet (riskskala/rankning)
<i>Verifierbarhet</i>						Kan kontrolleras mot specifikation
Transparens	●	●		●		Klara motiveringar och ursprung
Kommunikativt	●		●	●		Koncis men förståelig redovisning
Otvetydighet	●			●		Klar systemgräns och detaljnivå
<i>Genomförbarhet</i>	●	●	●	●	●	Användbar, resursbeaktande
<i>Förbättring</i>		●				Främjar lärande, metodförädling; attraherar personal

Att mäta risk på ett sätt som är *godkänt* – som har stöd av och informerar intressenterna (Johansen och Rausand, 2014) – kan förstås som att relevant (*kontextuell, specifik och jämförbar*) risk ska mätas på ett ”vettigt” (*reliabelt, rationellt och konsistent*) sätt, varpå *validitet* uppnås. Dessutom ska risken mätas på ett *verifierbart* sätt där mätningen redovisas *transparent, kommunikativt och otvetydigt*. Läggs detta samman med tabellens två sista kriterier blir slutsatsen att risker ska mätas på ett valitt och verifierbart sätt ur ett teoretiskt, praktiskt (genomförbart) och förbättrande perspektiv.

Värt att notera är att tabellen inte uttryckligen nämner ordet risk. Det verkar inte heller finnas någon anledning till att kriterierna inte lika gärna kan appliceras på att mäta kostnad eller nytta – särskilt som en av källorna behandlar systemutvecklingskrav. Som tidigare nämnts i rapporten (exempelvis i avsnitt 2.1, som inleder forskningsgenomgången) är dessutom själva riskhanterings

utförande (mätningen av åtminstone risk) kritisk för ett relevant underlag för riskacceptansbeslut. Besluten kan till och med implicit utgöras av riskhanteringarna. Med andra ord kan riskmetrikkriterierna kanske i själva verket likställas med riskacceptanskriterier. Dessutom kan de på sätt och vis ses som en sammanfattning av forskningsgenomgången.

2.2 Standarder

Det finns flera olika internationella och nationella standarder som föreskriver hur riskhanteringsprocesser ska realiseras i organisationer. Urvalet av standarder för denna analys utgörs av:

- internationella standarder för informationssäkerhet från ISO/IEC, vilka Försvarsmakten refererar till i exempelvis H Säk Grunder (Försvarsmakten, 2013a)
- internationella standarder för riskhantering i allmänhet från ISO/IEC, vilka ISO/IEC-standarderna för informationssäkerhet relaterar till
- en serie nationella standarder från USA (NIST) som berör hantering av informationssäkerhetsrisker.

Urvalet av standarder återfinns i Tabell 2. Standarderna har analyserats för att avgöra vilket stöd de ger med avseende på riskacceptansbeslut och resultatet av denna genomgång beskrivs i de följande avsnitten (2.2.1–2.2.3).

Tabell 2: Standarder som har analyserats.

Id	Beteckning	Titel	Referens
27001	ISO/IEC 27001:2013	Information technology – Security techniques – Information security management systems – Requirements	(ISO/IEC, 2013)
27005	ISO/IEC 27005:2011	Information technology – Security techniques – Information security risk management	(ISO/IEC, 2011)
TR 50	SIS-TR 50:2015	Terminologi för informationssäkerhet	(SIS, 2015)
31000	SS-ISO 31000:2009	Riskhantering – Principer och riktlinjer	(SIS, 2011)

Id	Beteckning	Titel	Referens
31004	ISO/TR 31004:2013	Risk management – Guidance for the implementation of ISO 31000	(ISO, 2013)
31010	ISO/IEC 31010:2009	Risk management – Risk assessment techniques	(ISO/IEC, 2009)
Guide 73	ISO Guide 73:2009	Risk management – Vocabulary	(ISO, 2009)
800-30	NIST Special Publication 800-30, Revision 1	Guide for Conducting Risk Assessments	(NIST, 2012)
800-37	NIST Special Publication 800-37	Guide for Applying the Risk Management Framework to Federal Information Systems	(NIST, 2010)
800-39	NIST Special Publication 800-39	Managing information security risk	(NIST, 2011)

I denna rapport benämns dokument utgivna av standardiseringsorganisationer som standarder, även om de i vissa fall snarare utgörs av rapporter och vägledningar. För att referera till standarderna används de id-beteckningar som återfinns i Tabell 2.

Mer specifikt baseras urvalet på att den internationella standarden 27005 handlar om hantering av informationssäkerhetsrisker. I 27005 refereras det till 27001 som därmed också har inkluderats i urvalet. Försvarmakten refererar i samband med begreppsdefinitioner i H Säk Grunder (Försvarmakten, 2013a) till Guide 73, vilken utgörs av begreppsdefinitioner för riskhantering i allmänhet. Guide 73 ligger också till grund för avsnittet om riskhantering i TR 50, som har ersatt SIS HB-550 (SIS, 2007), vilken H Säk Grunder och H Säk Infosäk refererar till. Guide 73 och TR 50 har därmed inkluderats i urvalet. 27005 refererar även till 31000-serien med standarder för hantering av risker i allmänhet. Eftersom 31000-serien är inriktad på riskhantering och därmed innehåller mer omfattande beskrivningar av ämnet än 27000-serien, har standarderna 31000, 31004 och 31010 inkluderats i urvalet. Av de nationella standarderna är de från National institute of standards and technology (NIST) i USA relativt omfattande med hänsyn till hantering av informationssäkerhetsrisker, varför standarderna 800-30, 800-37 och 800-39 också inkluderats.

De olika aktiviteterna i riskhanteringsprocessen benämns genomgående med de begrepp som används i standarden 27005 – även vid diskussion av andra standarder. Enligt 27005 inleds riskhanteringsprocessen med aktiviteten *fastställande av kontext*. Därefter följer riskbedömningen som består av de tre aktiviteterna *riskidentifiering*, *riskanalys* och *riskutvärdering*. Efter riskbedömningen följer aktiviteterna *riskbehandling* och slutligen *riskacceptans*. Från dessa två sista aktiviteter kan genomförandet återgå till den första aktiviteten om behov finns.

2.2.1 Vad riskacceptans innebär

Begreppet riskacceptans definieras i ISO-standarderna kortfattat som ett beslut relaterat till en specifik risk (Guide 73). I TR 50 omnämns riskacceptans som ett beslut i en kommentar kopplad till definitionen av kvarstående risk. Begreppet används dock inte vidare i det dokumentet. Däremot beskrivs riskutvärdering som en process där riskanalysens resultat jämförs med riskkriterier för att avgöra om riskerna är acceptabla. Samma formulering återfinns i 31000. I 27001 finns det krav på att ”riskägare” ska identifieras under riskbedömningen och att dessa sedan ska acceptera kvarvarande risker när en riskbehandlingsplan har tagits fram, utan att det närmare specificeras vad en riskägare är.

ISO-standarderna har alla en liknande struktur för riskhantering (utgående ifrån 31000). I 27005 införs dock, i enlighet med kraven i 27001, också en specifik aktivitet för riskacceptans som säkerställer att kvarstående risker accepteras explicit av ansvariga inom organisationen. Detta sker genom formella och dokumenterade beslut efter att en godkänd riskbehandlingsplan har tagits fram. Det kan också innebära att risker som inte uppfyller acceptanskriterierna ändå accepteras för att det finns omständigheter som motiverar det och att det inte är praktiskt att uppdatera kriterierna innan aktuellt riskacceptansbeslut fattas. Sådana beslut visar dock på behov av att uppdatera riskacceptanskriterierna. Processen som 31000 föreskriver för riskbehandling, innehåller ställningstagande gällande godtagbarheten hos kvarstående risker, vilket i princip motsvarar riskacceptansaktiviteten i 27005.

Såväl 27005 som 31000 använder begrepp kopplade till riskacceptans i beskrivningen av aktiviteten riskutvärdering. Enligt 27005 utgår riskutvärderingen från riskutvärderingskriterier och riskacceptanskriterier som ska ha formulerats innan riskbedömningen inleds. Aktiviteten relaterar till riskacceptans eftersom det uttrycks att beslut som fattas inom aktiviteten i huvudsak baseras på vilken risknivå som är acceptabel. Det är dock oklart på vilket sätt detta avspeglas i resultatet, då utdata från riskutvärderingen ska vara en lista med prioriterade risker som utgör indata till riskbehandlingen.

Beskrivningen av aktiviteten riskbehandling i 27005 inkluderar också beslut relaterade till riskacceptans. Om riskerna är acceptabla behöver inget göras, men det betyder att det måste avgöras om de är acceptabla.

I 800-30 används begreppet riskacceptans som benämning för ett av fem sätt att hantera en risk. Innebörden är att inget görs åt risken och motsvarar därmed ISO/IEC-standardernas val att behålla risker. Riskacceptans används i 800-30 även i betydelsen att formellt godkänna de risker som har identifierats. Det verkar dock som att riskacceptans och risktolerans används synonymt, vilket skapar viss språkförbistring. Det uttrycks i standarden att valet av metod för att bedöma risker utgör ett medvetet val som återspeglar organisationens riskacceptans (eller risktolerans). Enligt 800-37 består uppgiften för de som fattar riskacceptansbeslut av att avgöra om riskerna för organisationens verksamhet (avseende uppdrag, funktion, anseende och rykte), organisationens tillgångar, individer, andra organisationer och nationen, är acceptabla. Därmed finns det många faktorer som är viktiga att beakta vid riskacceptansbeslut.

Enligt 800-39 kräver adekvat hantering av informationssäkerhetsrisker bland annat att organisationens risktolerans fastställs och kommuniceras inom hela organisationen. Risktolerans är enligt 800-39 den nivå av risk eller grad av ovisshet gällande risker som organisationer är villiga att acceptera för att uppnå strategiska mål och den påverkar alla delar av riskhanteringsprocessen. Specificeringen av risktoleransen ska inkludera riktlinjer för hur den påverkar beslutsfattande. Informationssäkerhetsrelaterad risktolerans ska definieras för hela organisationen med beaktande av alla verksamhetsfunktioner. Värderingen av kvarstående risk för att avgöra vad som är acceptabelt påverkas av den nivå som sätts av organisationens risktolerans.

Riskacceptansbeslut beskrivs i standarderna som formella godkännanden, beslut eller aktiviteter som avslutar den aktuella iterationen av en riskhanteringsprocess. Något som framträder tydligt i studien av standarderna är att beslut som har betydelse för riskacceptansen ska tas vid flera tillfällen tidigare under riskhanteringsprocessen, eller till och med innan den inleds. Eftersom riskacceptansbeslut ska baseras på väl specificerade kriterier, kommer den aktivitet där dessa kriterier definieras att utgöra en form av övergripande riskacceptansbeslut. Kriterierna kommer sedan att användas vid till exempel riskutvärderingen och riskbehandlingen, varför kriterierna bör vara fastställda och kända av de personer som är involverade i dessa aktiviteter. I linje med detta föreskriver flera standarder att riskacceptanskriterier ska specificeras som en del av den kontext i vilken riskhanteringsprocessen utförs och innan riskhanteringen inleds.

2.2.2 Vad som utgör grund för riskacceptansbeslut

Ett krav i 27001 är att kriterier för informationssäkerhetsrisker, inklusive riskacceptanskriterier, ska formuleras och underhållas. Enligt 27005 ska dessutom de förutsättningar som ges av riskacceptanskriterierna styra vilken riskhanteringsansats som används. Vidare ska organisationer skapa sina egna skalor för olika nivåer av riskacceptans.

Enligt 800-30 ska organisationer avgöra vilka nivåer och typer av risker som ska accepteras på en organisationsövergripande nivå, hur ovissheten i bedömningarna ska identifieras och kompenseras för samt vilka risknivåer som kan tolkas som att inga vidare analyser av de underliggande faktorerna behövs. Enligt 800-39 etablerar ledningen organisationers risktolerans både formellt – genom exempelvis strategidokument och vägledningar – och informellt – genom exempelvis belöning respektive bestraffning av olika handlingar, graden av konsistens hos åtgärder och krav på ansvarstagande. Riktningen som sätts av ledningen och tolkningen av organisatoriska värden och prioriteringar är betydande faktorer för hanteringen av risker inom organisationen. Fastställande av en organisatorisk risktolerans ger enligt 800-39 förutsättningar för en otvetydig övre gräns avseende vad organisationen är villig att riskera avseende verksamhet (inklusive uppdrag, funktioner, anseende och rykte), tillgångar, individer, andra organisationer och nationen. I verkligheten kan dock sällan sådana fastställda risktoleranser direkt användas i verksamheten. Riskacceptansstrategier ger ett ramverk för riskacceptans utifrån ett organisatoriskt perspektiv och vägledning som försäkrar att accepterade riskers omfattning är i linje med organisationens riktlinjer. Mer explicita strategier för riskhantering ger praktiska och pragmatiska lösningar för att hantera risker.

Enligt 31010 kan ett enkelt stöd för riskacceptansbeslut baseras på att en risknivå fastställs och nyttjas som gräns för vilka risker som är acceptabla respektive inte acceptabla. Detta är dock sannolikt en väl stor förenkling då det inte återspeglar ovissheten som finns i bedömningarna av såväl riskerna som vilken risknivå som ska användas för att klassificera riskerna som acceptabla respektive icke acceptabla. Ett annat angreppssätt är att dela upp riskerna i tre nivåer: en övre nivå med icke tolererbara risker som behöver minskas oavsett kostnad, en mellannivå där avvägning mellan kostnader och fördelar är avgörande samt en lägre nivå med risker som kan försummas eller är så små att inga åtgärder krävs. Konceptet ALARP (as low as reasonably practicable) utgår från denna indelning (se även avsnitt 2.1.1).

De val av skyddsåtgärder som sker under riskbehandlingen har potentiellt stor betydelse för riskacceptansbeslutet. I 27005 listas kategorier för möjliga begränsningar som ska beaktas när skyddsåtgärder väljs ut. Dessa kategorier utgörs av begränsningar relaterade till: tid, ekonomi, teknik, verksamhet, kultur, etik, miljö, juridik, användbarhet, personal samt befintliga kontroller.

Standarden 31010 innehåller korta genomgångar av 31 tekniker för riskbedömning (riskidentifiering, riskanalys och riskutvärdering), från Brainstorming till Multi-criteria decision analysis. En gradering av teknikernas användbarhet för de olika delarna av riskbedömning presenteras också. 11 av teknikerna klassas som användbara för riskutvärdering och 10 klassas som mycket användbara. Ett exempel på en teknik som kan användas för att avgöra ifall risker är acceptabla eller ej är riskmatriser. I 31010 beskrivs också för- och nackdelar med användningen av riskmatriser. Fördelarna är att riskmatriser:

- är relativt lättanvända
- ger en snabb rankning av risker i olika risknivåer.

Nackdelar är att:

- matrisernas dimensioner behöver anpassas efter aktuell situation och ger därmed inte grund för jämförelser mellan analyser från olika situationer
- det är svårt att definiera skalorna entydigt
- variationen mellan olika personers bedömningar ofta blir stor
- det inte går att aggregera risker
- det är svårt att jämföra risker med olika typer av konsekvenser
- mer detaljerad analys ger fler risker med lägre risknivåer.

Under studien av standarderna identifierades ett antal utsagor i standarderna som ger uttryck för aspekter som är viktiga att beakta i samband med beslut om riskacceptans. Dessutom identifierades ett antal aspekter som ska beaktas vid formulering av riskacceptanskriterier. Eftersom överlappet mellan dessa aspekter är stort och de i generella termer kan beskrivas på samma sätt, återges i Tabell 3 nedan en sammanställning av de identifierade aspekterna.

Tabell 3: Aspekter kopplade till riskacceptans.

Aspekt
aktuella omständigheter
etiska, sociala och humanitära aspekter
andra typer av risker
acceptabla risknivåer och risktyper
framtida behandling av risker
tid risken förväntas existera
lagar, bestämmelser och andra krav

Aspekt	
standarder	
beroenden mellan olika informationssystem	
egna organisationen	mål och genomförandeplaner
	specifika verksamhetskrav
	intressenters intressen
	riskattityd
	påverkan på individer
externa parter	påverkan på individer, andra organisationer och nationen
	intressenters intressen
	riskattityd
riskperception	
grad av ovisshet avseende risker som är acceptabel	
huruvida kombinationer av risker ska beaktas	
uppskattad vinst respektive bedömd risk	
verksamhetens behov i närtid respektive påverkan kopplad till risker på längre sikt	

2.2.3 Svårigheter med riskacceptansbeslut

De studerade standarderna handlar om hur riskhantering ska genomföras och problematiserar inte utmaningen med riskacceptans i speciellt hög grad. 800-39 är i viss mån ett undantag och beskriver att riskacceptans påverkas av abstrakta riskrelaterade koncept, såsom risktolerans, tillit och kultur. Det uttrycks också i standarden att det kan finnas utmaningar gällande ansatsen att organisationer ska anamma en organisationsgemensam risktolerans och ett gemensamt tillvägagångssätt för riskhantering. En utmaning utgörs av faktiska förhållanden; exempelvis kan funktionskritiska delar inte temporärt nedgradera funktionen för att höja säkerheten.

En svårighet med att implementera processer för riskacceptansbeslut ges av den mångtydighet som finns i standarderna. Vidare föreskrivs att ändamålsenliga metoder för riskhantering ska väljas alternativt utvecklas med hänsyn till kriterier för bland annat riskutvärdering och riskacceptans. Med tanke på de generellt sett mycket övergripande beskrivningarna som standarderna ger och framförallt att

metodernas utformning och användning ska vara organisationsspecifik, lär det krävas avsevärd utveckling för att etablera organisationsöverskridande, ändamålsenliga metoder för riskhantering. En utmaning i utvecklingen är att hitta en balans så att metoderna är tillräckligt generella för att gälla hela organisationen och tillräckligt specifika för att fånga de kriterier som gäller för den aktuella organisationsdelen.

Ytterligare en svårighet ges av att enkla och rättframma tekniker som beskrivs kunna stödja riskacceptansbeslut inte ger tillräckligt nyanserade svar. Denna svårighet illustreras av diskussionen av stöd för riskacceptans, såsom riskmatriser, som beskrevs tidigare i detta avsnitt.

2.3 Branschspecifika vägledningar

Även om forskningsartiklar och standarder täcker in en stor del av riskacceptansområdet, finns det anledning att ytterligare fånga några perspektiv. Dessa utgör belysande exempel av vägledningar inom olika specifika branscher där risker och avvägningsproblematiken gör sig särskilt påmind. Fokus för genomgången som beskrivs i detta avsnitt låg på myndigheters vägledningar eftersom de har störst tillämpningsområden.

Resultaten av genomgången upprepade till stor del sådant som setts och nämnts inom forskningen och standarderna. Inom den mest närliggande IT-branschen och därmed myndigheterna Datainspektionen och PTS samt Europeiska unionens Enisa, hittades inget som var tillräckligt relevant att presentera i denna rapport. På toxikologi- och hälsoområdet (i form av Livsmedelsverket och Läkemedelsverket) samt trafiksäkerhetsområdet (i form av exempelvis Luftfartsverket) fanns inte heller något värt att nämna. Inte heller inom de främst privata försäkrings- och revisionsbranscherna hittades något värt att ta upp. Försvarsområdet utöver Försvarsmakten (som i egenskap av utgångspunkt för rapporten är exkluderad i detta avsnitt) visade sig också vara av begränsat intresse, trots en mindre genomgång av utländska försvarsmakters och Natos dokument. Dessa sökningar begränsades dock till engelskspråkiga dokument.

På det generella säkerhetsområdet fanns i dagsläget inget att hämta från Säkerhetspolisen eller Myndigheten för samhällsberedskap (MSB). Vad gäller MSB kan dock något matnyttigt vara på gång i och med den nya utgåvan av deras metodstöd (MSB, 2011) för informationssäkerhetsriskanalyser som planeras att lanseras i slutet av 2017. Från säkerhetsområdet fanns trots allt intressanta saker att notera från underområdet rättsmedicin (avsnitt 2.3.1); från dåvarande Statens räddningsverk (avsnitt 2.3.2); samt från dåvarande Statens kärnkraftinspektion (avsnitt 2.3.3).

2.3.1 Återfallsrisk i brott inom rättspsykiatri

När återfallsrisken i brott ska bedömas inom rättsmedicinen används numera vanligen en kombination av en aktuarisk modell, det vill säga en strukturerad riskbedömning samt en klinisk bedömning, som snarare utgår från den specifika situationen än en generell riskmodell. Kombinationen benämns *strukturerad professionell bedömning* och är inte helt okontroversiell. De renodlat aktuariska, ”mekaniska”, modellerna är överlägsna kliniskt beslutsfattande inom många komplexa områden (Dawes, Faust och Meehl, 1989) samt mer transparenta (SBU, 2005). Tveklöst är i alla fall den aktuariska modellen att föredra om alternativet är en helt klinisk modell. Det finns dock viss indikation att kombinationen, alltså en aktuarisk modell som väger in klinikers bedömning av den specifika situationen, faktiskt förbättrar prediktionsförmågan (Douglas, 2014). Detta talar för att generalister (aktuarier) och specialister (kliniker) bör samarbeta i riskbedömningarna och just forskning om vem som ska göra bedömningarna är av vikt (Sturup *m.fl.*, 2013).

En positiv bieffekt av kliniska bedömningar är att de skapar kontextuell kunskap, kunskap som kan användas för att bättre identifiera skyddsåtgärder (SBU, 2005). Just forskningen om skyddsfaktorer på området har fått stå tillbaka för fokuset på riskfaktorer (Sturup *m.fl.*, 2013). Att väga riskfaktorerna mot skyddsfaktorer är något av det svåraste på området (SOU, 2017). En del i detta är att åtgärder för att motverka brott måste vägas mot den enskildes grundläggande fri- och rättigheter som kan inskränkas av en åtgärd (SOU, 2017). Ett exempel på hur avvägningen mellan den enskildes rättigheter och dess bedömda benägenhet att begå brott redovisas i Monahan och Silver (Monahan och Silver, 2003). Samtliga domare i en studie var villiga att döma en person till tvångsvården en kort tid, förutsatt att sannolikheten att personen skulle begå ytterligare våldsbrott bedömdes vara minst 56 %. Flera av domarna bedömde till och med att gränsen gick lägre än så.

2.3.2 Fysisk samhällsplanering

Under 1997 gav Statens räddningsverk ut en rapport med titeln *Värdering av risk* (Davidsson, Lindgren och Mett, 1997) där det resoneras kring riskacceptans och hur riskacceptanskriterier kan tas fram för användning i samband med den fysiska planeringen av samhället. Fokus är på risker som relaterar till olyckor med konsekvenser på människa, miljö och ekonomi. I rapporten föreslås följande fyra principer bilda en utgångspunkt för riskacceptanskriterier:

1. *Rimlighetsprincipen*

En verksamhet bör inte ge risker som med rimliga medel kan undvikas. Detta innebär att risker som med tekniskt och ekonomiskt rimliga medel kan elimineras eller reduceras, alltid ska åtgärdas (oavsett risknivå).

2. *Proportionalitetsprincipen*

De totala risker som en verksamhet medför bör inte vara oproportionerligt stora jämfört med de fördelar (intäkter, produkter, tjänster, etc.) som verksamheten medför.

3. *Fördelningsprincipen*

Riskerna bör vara skäligt fördelade inom samhället i relation till de fördelar som verksamheten medför. Detta innebär att enskilda personer eller grupper inte bör utsättas för oproportionerligt stora risker i förhållande till de fördelar som verksamheten innebär för dem.

4. *Principen om undvikande av katastrofer*

Riskerna bör hellre realiseras i olyckor med begränsade konsekvenser som kan hanteras av tillgängliga beredskapsresurser än i katastrofer.

Som ett komplement till principerna nämns även att kriterierna ska vara praktiskt tillämpbara och utvecklas i takt med samhällets tekniska, ekonomiska och sociala utveckling, snarare än att vara konserverande.

Författarna förespråkar att en probabilistisk utgångspunkt används för genomförandet av riskvärderingar, där både konsekvensen och sannolikheten för att en konsekvens ska inträffa kombineras. Ett sådant synsätt på riskvärderingar tillsammans med de fyra principerna ovan, beaktas genom att ställa upp kriterier inom de tre områdena *individrisk*, *samhällsrisk (kollektiv risk)* och *kostnads-nyttanalyt*.

Kriterier för individrisk anknyter till fördelningsprincipen och syftar till att säkerställa att enskilda individer inte utsätts för oacceptabelt stora risker. Med individrisk avses oftast risken att omkomma och den uttrycks vanligen som risk per år. Dessa kriterier kan utformas för att motsvara den tredje principen ovan.

Kriterier för samhällsrisk syftar till att begränsa risken för lokala områden eller samhället som helhet. Samhällsrisk inkluderar risker för alla personer som utsätts för en risk, även om det enbart sker vid enstaka tillfällen. Samhällsrisker kan exempelvis vara relevant vid transport av farligt gods där riskerna fördelas över personerna som befinner sig utefter transportleden. Dessa kriterier kan utformas för att motsvara den andra, tredje och fjärde principen ovan.

Kostnads-nyttanalyt används för att rangordna riskreducerande åtgärder. Detta görs genom att kostnaden för att införa en åtgärd jämförs med bedömd nytta som motsvarar kostnaden för de olyckor som åtgärden bedöms förhindra. För att kunna göra denna jämförelse måste nyttan och kostnaden beskrivas enhetligt, vilket traditionellt sett varit i ekonomiska termer. Dessa kriterier kan utformas för att motsvara den första principen ovan.

En slutsats som ges är att det nog inte är möjligt att med hjälp av riskkriterier en gång för alla fastslå vad som är acceptabel risk. Vad som är acceptabelt behöver bedömas utifrån olika sociala, ekonomiska och politiska bedömningar.

2.3.3 Planering inom kärnkraftsindustrin

Borg, Lichtenberg och Lindskog (2005) redogör för en analys av risker i kärnkraftsindustrin. Analysen utgår från den egna verksamheten, med den personal, organisation och teknik som finns, och kompletterar med bland annat politik, ekonomi och lagar samt relationen till andra organisationer och de risker, erfarenheter och synergieffekter det innebär. Det lyfts fram att ovissheten i bedömningarna måste uppskattas och att inte bara riskernas troliga värde ska bedömas, utan också det minimala och maximala. Även faktorer som kan bidra till minskad eller ökad risk bör redovisas. Exempelvis kan svårigheter att anställa kompetent personal öka risken för en okunnig organisation, medan ökad utbildning kan minska risken.

Av vikt är att se till att analysen är tillräckligt omfattande, att beräkningar inte är felaktiga, att risker som delats in i olika kategorier inte överlappar och att gjorda förenklingar är lämpliga. Dessutom bör analyserna göras i grupp där individer av exempelvis olika kön, ålder och grad av optimism deltar samt personer med teknikfokus, ekonomifokus, liksom specialister och generalister. En oberoende moderator som inte är involverad i själva diskussionerna, utan just modererar, är också lämplig att ha. I analysen görs alltid vissa antaganden och dessa antaganden eller förutsättningar måste redovisas. Exempelvis kanske mildare typer av sabotage, olycksfall och naturpåverkan beaktas i analysen, medan större katastrofer undantas. En del av analysen återges i Tabell 4. Som synes kan till exempel tillgång till kvalificerad personal vara en förutsättning, medan utbildning kan utgöra en förbättrande möjlighet, men pensionsavgångar en risk.

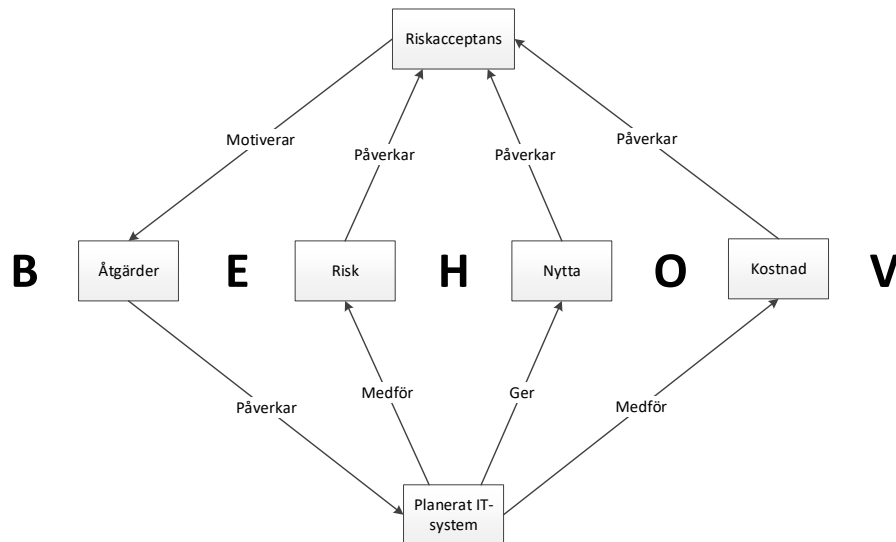
Tabell 4: Exempel på förutsättningar, möjligheter och risker för kategorin produktivitet i kärnkraftsindustrin (efter (Borg, Lichtenberg och Lindskog, 2005)).

Förutsättningar	Möjligheter	Risker
Nuvarande arbetsförhållanden	Nya arbetsmetoder	Långtidssjukskrivning
Tillgång till kvalificerad personal	Utbildning	Pensionsavgångar
	Generationsskifte	Rekryteringssvårigheter
		Generationsskifte

3 En ansats för riskacceptans

Figur 3 illustrerar hur ett planerat IT-system ger upphov till risk, nytta och kostnad, vilket i sin tur påverkar riskacceptansen. Riskacceptansen kan motivera åtgärder som påverkar systemet vilket fullgör kretsen. Som litteraturgenomgången i kapitel 2 visar måste riskacceptansbeslut – och hela riskhanteringsprocessen för ett IT-system – utgå från de intressenter som finns och deras behov. Redan när risker, kostnader och nyttor identifieras måste därför rätt perspektiv och rätt intressen beaktas. I Figur 3 utgör faktorerna åtgärder, risk, nytta och kostnad en diamant, som färgas, klargörs, viktas och formges utifrån behoven.

Detta kapitel utgår från forskningen, standarderna och de branschspecifika vägledningarna och gör en ansats att enhetligt beskriva grunderna och grundproblemen för riskacceptans i Försvarsmakten. Avsnitt 3.1 tar upp vilka grundbehov som behöver beaktas, varpå avsnitt 3.2 beaktar moraliska synsätt som präglar behoven. Avsnitt 3.3 undersöker vilka motsättningar som finns mellan olika intressenter och hur motsättningarna kan lösas. I det avslutande avsnittet 3.4 sätts det praktiska genomförandet på sin spets samt möjligheterna till, och nödvändigheten av, kontinuerliga förbättringar.



Figur 3: Planerade IT-system och riskacceptansen.

3.1 Behovsgrunden

Ett system i Försvarsmakten kan ha som direkt målsättning att ett flygplan ska kunna framföras. Detta mål stödjer exempelvis möjligheten att spana på fienden, vilket i sin tur är av vikt, bland annat för att inte Sveriges territorium ska kränkas. Detta resonemang kan föras vidare genom att konstatera att svenskarna vill slå vakt om sina lagar, vilka i sin tur är i linje med svenskarnas åsikter och värderingar. *All offentlig makt i Sverige utgår från folket*, som det står i Regeringsformen (1974), varför Försvarsmaktens IT-system också måste utgå från folket. Det vore bekvämt om en så övergripande lag var tydlig nog för alla konkreta situationer. Som litteraturen visar måste dock alla till viss del göra sina egna avvägningar och sätta sina egna gränser – ingen universell regel kan ges av vetenskapen (Monahan och Silver, 2003; Johansen och Rausand, 2014). Inte heller regeringen kan vara specifik nog för varje verksamhet (Regeringen, 2017). I specifika situationer finns därför specifika regler som på sätt och vis förtydligar grundlagen. Till exempel finns en Säkerhetsskyddslag (1996), som ytterligare förtydligas i en Säkerhetsskyddsförordning (1996), som i sin tur görs än mer specifik i Försvarsmaktens författningssamling, interna bestämmelser, handböcker och så vidare. Denna struktur finns också beskriven i Försvarsmaktens handbok för informationssäkerhet, H Säk InfoSäk (Försvarsmakten, 2013b). Figur 4 belyser vad som är viktigast (folkets vilja) ned till minst viktigt (direktiv och handböcker) vid framtagandet av ett system. Även om varje nivå kan ge specificering och förtydliganden, är det alltid den allra högsta nivån (folket) som har tolkningsföreträde (och därmed medborgarnas åsikter och värderingar). Därför måste framtagandet av ett IT-system i Försvarsmakten genomsyras av de grundläggande värderingar som finns i samhället. En högre nivå i samhällshierarkin måste alltid gå före en lägre. En risk, kostnad eller nytta som strider mot folkets vilja kan därför knappast ses som möjlig att acceptera, medan risker, kostnader och nyttor som rör till exempel det enskilda systemet kan vara acceptabla.



Figur 4: Samhällshierarkin ur Försvarsmaktens perspektiv, baserad på en figur i (Försvarsmakten, 2013b).

Olika system kan ha olika mycket potentiell koppling till de olika nivåerna i Figur 4. Ett organisationsinternt fakturahanteringssystem kommer knappast att komma i konflikt med en grundlag. Däremot kanske systemet inte tillräckligt beaktar lagar eller förordningar som reglerar ekonomisk redovisning. Gränsdragningen är inte nödvändigtvis helt enkel och de överordnade värdena måste alltid på ett eller annat vis styra. Beroende på systemgränsen kan andras behov också vara en del av organisationens behov – om än utanför systemet – eller externa aktörers behov.

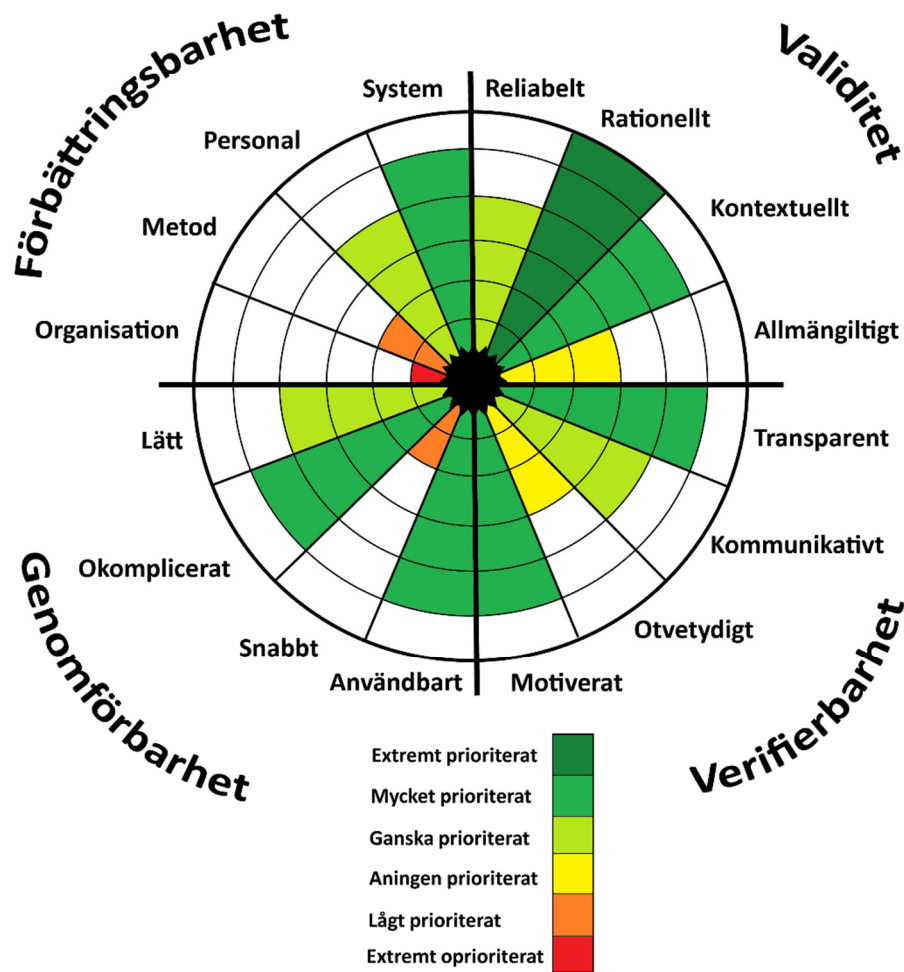
I Tabell 5 redovisas mer konkreta aspekter kopplade till intressenters behov, utgående från standarderna som beskrivs i avsnitt 2.2. Precis som i det avsnittet finns en indelning i aspekter som antingen rör den egna organisationen eller andra intressenter, kompletterat med några generella aspekter (i Tabell 5 enbart av typen tid). För att koncentrera analysen har en del aspekter från standarderna låtits representeras av andra aspekter. Dessutom är det faktum att risker kan vara av olika typ eller beroende av varandra på en alltför generell nivå för att inkluderas i resonemangen här. Riskacceptansbeslutens kostnadseffektivitet utöver organisationens behov (nyttan) inkluderas genom skyddsåtgärders effektivitet och kostnad.

Tabell 5: Aspekter som lyfts fram i standarderna och som påverkar riskacceptansen.

Nr.	Vad ligger till grund för riskacceptans?	Typ
1	aktuella omständigheter	Tid
2	tid risken förväntas existera (långsiktighet)	
3	beroenden mellan informationssystem	Andras behov
4	lagar, bestämmelser och andra krav	
5	etiska, sociala och humanitära aspekter	
6	verksamhetskrav och organisationens mål	Egna behov
7	skyddsåtgärders effektivitet och kostnad	

Aspekterna i Tabell 5 kan delvis relateras till forskningslitteraturens kriterier för riskmetriker (se avsnitt 2.1.7), vilket kan förenkla mätning av aspekterna. Egna och andras behov plus långsiktigheten, kopplar till kriterierna rationalitet, kontextuellt och specificitet. Kriteriet jämförbarhet kopplar till beroenden mellan informationssystem. Skyddsåtgärders effektivitet och kostnad samt aktuella omständigheter kopplar till genomförbarhet. Även om det inte redovisas i tabellen lyfter standarderna också fram andra typer av risker (kriteriet konsistent) samt hur reliabla bedömningarna eller processen är (kriteriet reliabilitet). Kriteriet förbättringsbarhet samt det övergripande kriteriet verifierbarhet finns också med i standarderna, men mindre explicit.

Utgående från en variant av kriterierna för riskmetriker ges i Figur 5 ett exempel på en avvägning mellan kriterier som påverkar riskhanteringsprocessen och riskacceptansbesluten. De fyra övergripande kriterierna (validitet, verifierbarhet, genomförbarhet och förbättringsbarhet) delas in i fyra underkriterier var. Färgen (och mängden ifylld färg) indikerar hur prioriterad varje kriterium är. Vilka kriterier som beaktas i riskacceptansen präglas av validiteten, medan redovisningen får sin form av verifierbarheten. Den praktiska genomförbarheten indikeras av hur användbar, snabb, enkel (okomplicerad) och mödosam (lätt) processen är. Förbättringsbarheten relaterar till hur stort fokus som ligger på att förädla organisation, metod, personal och system. Det är viktigt att notera att värderingarna (färgläggningen) mellan de olika kriterierna i figuren enbart är ett exempel. Varje organisation behöver göra sin egen avvägning.



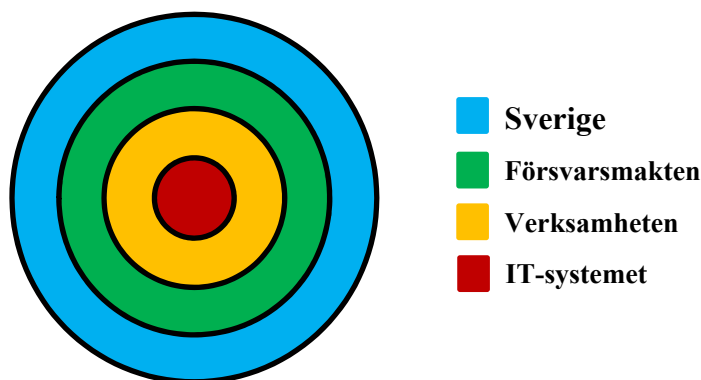
Figur 5: Riskhanteringsprocessen kräver en avvägning mellan validiteten, verifierbarheten, genomförbarheten och förbättringsbarheten samt deras underliggande kriterier. Figuren är inspirerad av <http://www.circlesofsustainability.org>.

Aspekterna i Tabell 5 kan också relateras till den psykologiska teorin *Theory of planned behaviour* (TPB), som bland annat används till att förutsäga säkert och osäkert beteende (Sommestad, Karlzén och Hallberg, 2017). TPB utgår från människors attityder, hur de upplever rådande normer samt hur de upplever möjligheten att efter sammanvägningen av attityder och normer faktiskt agera på det sätt de önskar (beteendekontrollen). Verksamhetskraven och organisationens mål (Nr. 6 i tabellen) kan ses som resultat av organisationens attityd. Skyddsåtgärdernas effektivitet och kostnad (7) kan tillsammans med aktuella omständigheter (1) betraktas som en del av beteendekontrollen. Långsiktigheten

(2) och andras behov (3, 4, 5) kan ses som ett utslag av normerna. Alltså beror riskacceptansen hos en organisation på organisationens attityd, hur organisationen upplever andras normer, den upplevda beteendekontrollen samt viktningen mellan desamma. Hur viktningen mellan de olika aspekterna ska göras beror på värderingarna – det moraliska synsättet. Detta beaktas i nästa avsnitt.

3.2 Moraliska synsätt

Hur mycket ansvar som ska tas kan ses som ett uttryck av ens moraliska synsätt. Av de två axlar för moraliska synsätt som återges i forskningsavsnittet 2.1, exempelvis av Kahan m.fl. (2007), är individualismen kontra solidariteten kanske den mest närliggande och rättframma. Figur 6 illustrerar några olika möjliga perspektiv för riskhantering som är kopplade till detta. Beroende på systemet och den överordnade organisationen, kan (de godartade) intressenterna finnas mycket nära systemet, medan ett väldigt brett perspektiv kan behövas för vissa system där exempelvis risktagaren kan finnas långt från systemet och drabbas av bieffekter (som exempelvis fotgängare bland biltrafiken). Dessa vill inte drabbas av påtvingade risker och kostnader och bli utan en del av nyttan. De kan vara formellt maktlösa men kan påverka genom till exempel media eller politiker.



Figur 6: Olika perspektiv för riskhantering. Källa: (Hallberg, Bengtsson och Karlzén, 2016).

Även axeln som rör huruvida ett hierarkiskt eller egalitärt synsätt appliceras, kan vara relevant. Ett hierarkiskt synsätt präglas av regelefterlevnad och det traditionella, vilket kan ge större fokus på lagar och andra krav samt långsiktighet. De egalitära kan å andra sidan ha plattare beslutsstrukturer och vara mer öppna för förändring, exempelvis vad gäller vilka skyddsåtgärder som ska användas.

Båda axlarna – och därmed alla fyra synsätt – kan påverka hur beredd en person är att följa föreskrifter som till exempel lagar. Medan ett hierarkiskt synsätt som sagt sätter större fokus på lagarna (ordalydelsen), kan ett egalitärt synsätt bättre beakta att lagstiftarna haft samhällets bästa i åtanke vid stiftande av lagarna (andemeningen). Vidare kan dimensionen individualism–solidaritet påverka vilka typer av maktmedel som är effektiva. Exempelvis påverkar nog personlig kritik individualister mer än kritik mot organisationen som helhet.

3.3 Motsättningar och kommunikation

IT-systems intressenter kan identifieras med hjälp av metoderna i (Ward och Chapman, 2008). Först och främst finns intressenter med stort inflytande och stort intresse, det vill säga de som är den främsta drivkraften för systemets utveckling (beställare), alternativt har ett intresse av att påverka på ett för systemet negativt sätt (antagonister). Det finns också de som visserligen har stort intresse, men generellt sett lägre inflytande, det vill säga de som är beroende av systemet. Det rör sig till exempel om leverantörer, anslutande system samt (tyvärr ofta) användare och bieffektdrabbade. Förutom de med stort intresse, finns också de med lägre intresse. Dessa kan ha stort inflytande (som analytiker, experter, granskare och lagstiftare) eller lägre inflytande (som välgörare). Observera att indelningen varierar beroende på systemet och flera andra faktorer, exempelvis hur många leverantörer eller experter det finns att välja mellan. Det kan också finnas andra intressenter som är viktiga att beakta, men denna uppsättning är tillräcklig för att få en generell bild av intressenters påverkan på IT-system.

Tabell 6 listar exempel på intressenter ett IT-system kan ha, från de mest interna till de mest externa aktörerna. Dessutom kopplas intressenterna till de aspekter i Tabell 5 som beskriver intressenternas påverkan på IT-systemet. Aspekter (1) och (2) – det vill säga tidsaspekterna – nämns inte eftersom de utgör en annan dimension.

Tabell 6: Intressenter och de aspekter som beskriver intressenternas påverkan på IT-systemet.

Intressent	Aspekt/-er
Användare	verksamhetskrav och organisationens mål (6)
Beställare	
Anslutande system	beroenden mellan informationssystem (3)
Analytiker	lagar, bestämmelser och andra krav (4) samt skyddsåtgärders effektivitet och kostnad (7)
Experter	
Granskare	
Välgörare	etiska, sociala och humanitära faktorer (5)
Bieffektdrabbade	
Leverantörer	beroenden mellan informationssystem (3) samt skyddsåtgärders effektivitet och kostnad (7)
Lagstiftare	lagar, bestämmelser och andra krav (4)
Antagonister	skyddsåtgärders effektivitet och kostnad (7)

De mest svårhanterliga intressenterna är rimligen antagonisterna. Till skillnad från naturliga hot har antagonisterna egen vilja. En storm kommer oavsett om ett hus är byggt robust eller ej, men en antagonist väljer förmodligen sina mål delvis baserat på sin kapacitet och målets sårbarhet. Intentionen komplicerar alltså. Därmed spelar både systemägarens och antagonisternas bedömning av skydden gentemot antagonisternas kapacitet roll. Alltså är det inte bara antagonisternas kapacitet och systemets skydd som är av vikt för säkerheten, utan även upplevelsen av desamma. Dessutom gör antagonisten sin bedömning av huruvida systemet har information eller funktionalitet som är intressant att angripa för att exempelvis göra ekonomisk vinst, uppnå spänning eller makt, förbättra sitt rykte eller försämra ryktet för systemets organisation. Därmed kan antagonistens angrepp primärt vara riktat mot något annat än det skyddsvärda (som i alla fall drabbas på grund av bieffekter). Dessutom kan intentionen påverkas av de potentiella konsekvenserna. Med andra ord kan sannolikheten för ett angrepp vara positivt korrelerat med konsekvenserna. Det går stick i stäv med det vanliga antagandet att de ur konsekvenshänsyn allvarliga (vanligen icke-antagonistiska) hoten har låg sannolikhet.

Ett mindre extremt exempel än antagonisterna är de olika experter som har en framträdande roll i riskhanteringen – inte minst eftersom det är så svårt att få tillgång till angreppsdata och dylikt. Denna framträdande roll kan göra att deras

värderingar och psykologiska synsätt tar alltför stor plats. Psykologisk bias, som exempelvis förutfattade meningar eller övertolkning av lättillgänglig information, spelar också roll. En säkerhetsexpert kan till exempel tänkas fokusera mycket på att minska risker och knappt beakta de förknippade skyddsåtgärdernas kostnader. Ett annat möjligt problem är att inte beakta olika intressenters riskbenägenhet, vilket kan ha sin grund i resursbegränsningar. Vidare blir expertbedömningarna än mindre reliabla i nya och komplexa situationer, som när tekniken utvecklas snabbt och antagonister anpassar sig för att bättre angripa, eller när reglerna tolkas olika över tid.

Ett sätt att minska den enskilde expertens inflytande är att använda sig av flera experter, exempelvis genom peer-review eller en fri debatt med andra experter, även om grupptänkande är en möjlighet och fler experter förstås innebär större resurskrav. Borg, Lichtenberg och Lindskog (2005) rekommenderar att experternas karaktäristik är olika, exempelvis med avseende på kön, ålder, grad av optimism och specialisering, teknikfokus samt ekonomifokus. Det finns ingen beprövad metod för att undvika bias men rekommendationerna i forskningslitteraturen är bland annat att öka strukturen; använda viktningar snarare än enbart direkta bedömningar; vara flexibel för nya data; och kontinuerligt träna (Montibeller och von Winterfeldt, 2015). De teoretiska modeller som presenterats i forskningen är än så länge alltför rudimentära för att kunna ersätta experter. Förutom att modellerna inte har testats empiriskt, baseras de på en rad olika antaganden. Exempelvis tar de inte i beaktande att ett nytt system inte börjar på noll, det vill säga de antar bland annat att inga befintliga skyddsåtgärder finns. Modellerna antar också att skyddsåtgärderna tillkommer till ett fixt pris, men med avtagande effekt och att angrepp är enkla och rätlinjiga snarare än bestående av olika villkorade steg.

Eftersom det finns olika intressenter och motsättningar dem emellan, behöver riskhanteringsprocessen kännetecknas av god kommunikation. Experternas förståelse av intressenters behov har redan nämnts. Dessutom måste beslutsfattare förstå experternas resultat, som kommer att ligga till grund för besluten. De populära och lättanvända riskmatriserna har dock begränsat värde när det gäller att se förändringar, tar inte med kostnad och nytta i visualiseringen och har begränsad möjlighet att visa detaljerade analyser. Förutom själva bedömningarna behöver det redovisas hur reliabla bedömningarna är, exempelvis med en felmarginal. Dessa redovisningar är viktiga eftersom empirin är begränsad, det finns många faktorer som minskar experternas objektivitet, den valda riskhanteringsprocessen är inte nödvändigtvis perfekt och antaganden kan ha gjorts. Att redovisa gjorda antaganden och därmed hur bred tillämpning den relevanta analysen eller bedömningen har eller vilka risker, kostnader och nyttor som inte beaktats är viktigt. Så görs exempelvis inom kärnkraftsindustrin.

3.4 Misstag och kontinuerliga förbättringar

Eftersom människor – såväl välvilliga intressenter som antagonister – är svårmodellerade och experternas kunskap och objektivitet är ofullständig, kommer det att uppstå situationer där felaktiga bedömningar och antaganden har gjorts. Till exempel kan tänkta skydd vara dyrare, mindre effektiva, mer nyttominskande, eller ta längre tid att införa, än förmodat. Ett annat exempel kan vara att beslutsfattare är mindre benägna att justera budget eller förändra regler, än förväntat. Ytterligare exempel är antagonister som anpassar sig till införda skyddsåtgärder varför riskreduceringen kan utebli, eller legitima användare som utnyttjar ökade skydd för att nå tidigare oanad nytta (men vid samma risknivå).

Att beakta den praktiska genomförbarheten av riskhanteringen och dess följder är därmed av vikt. Detta är i linje med den psykologiska teorin *Protection motivation theory* – introducerad av Rogers (1975) – som förutom en avvägning mellan risk, nytta och skyddsåtgärders kostnad och effektivitet, väger in den praktiska genomförbarheten (Sommestad, Karlzén och Hallberg, 2015).

Mot denna bakgrund kan möjligheten till justeringar av riskhanteringsresultatet – som kan beakta nya insikter – verka intressant. En sådan justering går visserligen emot tanken med en strukturerad process, men viss forskning indikerar att det kan vara nyttigt i vissa situationer och det används inom rättsmedicinen när sannolikheten att återfalla i brott ska bedömas (Sturup *m.fl.*, 2013). Försiktighet bör dock iaktas och i de flesta situationer verkar det snarare vara negativt med en sådan justering (Dawes, Faust och Meehl, 1989).

En annan möjlighet är att göra ett mer omfattande omtag när nya insikter nås. Då krävs en flexibel och lärande kultur som inte förnekar brister och latent fel. I både forskningslitteraturen och standarderna framhålls att olika typer av lärande är av vikt för att förbättra riskhanteringsprocessen, exempelvis genom återkoppling från riskanalytiker till granskare (även om systemspecifika aspekter begränsar allmängiltigheten). I linje med detta kan själva utförandet av riskhanteringen ge positiva sidoeffekter på systemets kvalitet och säkerhet, eftersom exempelvis både riskhantering och testning har en del gemensamt. Organisationen som helhet kan också förbättras eftersom riskhantering typiskt kräver kommunikation mellan olika organisationsdelar. Inte minst behöver riskacceptanskriterierna kontinuerligt förbättras. Som Kleinmuntz (1990) påpekar bör det dock noteras att det inte nödvändigtvis är samma sak att leta orsaker till skeenden (som i incidenthantering vilket delvis är en typ av lärande) som att riskhantera (prediktera). Det ena är bakåtresonerande, det andra framåtresonerande.

Mot bakgrunden att omtag förmodligen måste göras, kan det vara lockande att ytterligare ifrågasätta den rigorösa – vattenfallsmässiga – riskhanteringen. Det finns också stöd i forskningen (Abrahamsen, Røed och Jongejan, 2013) för att bara använda en komplett och grundlig riskhantering för de allra mest kritiska

systemen. Andra system kan istället jämföras med existerande system och de skydd som utgör best practice kan användas, med liknande upplägg som i KSF (Försvarmakten, 2014). Apostolakis (2004) framhåller att riskhanteringen bör kompletteras med traditionella säkerhetsmetoder som testning, säkerhetskulturförhöjande åtgärder och försvar-på-djupet. På så vis kan generella erfarenheter och best practice kombineras med riskhanteringsprocessen.

4 Slutsatser

Den genomförda studien visar att inte bara risk – utan också kostnad och nytta – behöver vägas in i alla delar av riskhanteringsprocessen. I avsnitt 4.1 presenteras slutsatser kopplade till det praktiska genomförandet av riskhanteringsprocesser inom Försvarsmakten och i avsnitt 4.2 presenteras idéer för framtida forskning.

4.1 Rekommendationer

Innan arbetet inom en riskhanteringsprocess inleds behöver riskacceptanskriterier specificeras. För att det ska vara genomförbart för ett specifikt IT-system behöver det finnas övergripande riskacceptanskriterier som beaktar bland annat verksamheten som IT-systemet ska stödja och Försvarsmakten som helhet. Dessutom krävs anvisningar för framtagande av specifika riskacceptanskriterier utgående från de övergripande riskacceptanskriterierna.

Utöver verksamhetens krav och organisationens mål måste olika intressenters behov beaktas. För att göra detta måste etiska, sociala och humanitära aspekter vägas in liksom lagar och standarder. Det är då centralt att inse att rädsla, valfrihet och oro är rationella faktorer som styr en persons riskacceptans. Hänsyn måste också tas för att vissa konsekvenser kan vara katastrofala och ohanterliga för en enskild individ, även om de inte är det för organisationen eller samhället som helhet. Negativa effekter från ett system som drabbar en intressent måste därmed samordnas med effekter från andra system som påverkar samma intressent. Problematiken kring anslutande system behöver klarläggas så att ansvar tydliggörs och kan tas. Exempelvis kan två IT-system vart och ett för sig ha en acceptabel exponering av information. Men om röjd information från båda systemen aggregeras kan det leda till en oacceptabel konsekvens – som helhet blir risken för stor.

Möjligheten att beakta ett visst systems kontext och detaljer måste vägas mot jämförbarheten mellan säkerhetsanalyser för olika system. Ju viktigare system är, desto fler experter bör involveras i riskhanteringsprocessen och desto större ansvar måste tas för olika intressenters behov. Det är även angeläget att Försvarsmakten förtydligar att riskacceptanskriterierna inte enbart är något som används i ett avslutande formellt beslut, utan att de ska genomsyra hela riskhanteringsprocessen.

Det är också av betydelse att beakta att teknik, hot och behov kan förändras snabbt, varför det bör finnas utrymme för omtag i analyser och beslut – vilket kräver uppföljning. För att på sikt öka kunskapen och förädla metoderna måste lärande främjas, genom till exempel informationsutbyte mellan riskanalytiker och testare; beaktande av analytikens metodförbättringsförslag;

ökade möjligheter till jämförelse mellan olika system; och kultivering av expertis.

Att förbättra kommunikationen mellan inblandade intressenter kan ge stora fördelar. Om chefer inte förstår experter får de svårt att dra nytta av dem. På motsvarande sätt måste analysernas reliabilitet – som indikerar hur mycket det går att lita på resultatet – kommuniceras. Komplexiteten, bristen på data och de kontinuerliga förändringarna gör det nödvändigt att påpeka att det ytterligare behöver förtydligas att riskhanteringsprocessen inte kan genomföras perfekt utan att förenklande antaganden och prioriteringar måste göras. Gjorda antaganden bör vara en tydlig del i redovisningen.

4.2 Fortsatt forskning

Det behövs mer kunskap om hur utformningen av hotbeskrivningar påverkar förutsättningarna för att fatta väl underbyggda riskacceptansbeslut och välja rätt skyddsåtgärder. Ett experiment kopplat till utformningen av hotbeskrivningar genomfördes inom en tidigare studie (Hallberg, Bengtsson och Karlzén, 2016) som indikerade att experters bedömningar av risker blir mer samstämmiga när hot presenteras i en strukturerad tabell istället för löpande text. Den exakta strukturen och vilka hotdelar som ska inkluderas utreddes dock inte. Detta bör undersökas i en framtida forskningsstudie. Exempelvis kan hot behöva beskrivas på ett annat sätt när hotens sannolikhet bedöms än när hotens konsekvens bedöms. I samband med detta kan det också undersökas hur översättning mellan olika typer av risker, kostnader och typer av nytta bör gå till.

En annan möjlig forskningsstudie är att ta reda på hur lika system är och hur likheterna möjliggör nyttjande av tidigare analyser och bedömningar genom en lärandeprocess och katalogisering i stil med KSF (Försvarmakten, 2014). På så sätt kan onödiga och mödosamma upprepningar i arbetet effektiviseras bort. För mer kostnadseffektiva och genomförbara riskacceptansbeslut är det även intressant att studera vilka begränsningar som finns i möjliga skyddsåtgärder – vad gäller deras riskreducerande effekt, kostnad och nyttominskning. En fråga i sammanhanget är hur väl de traditionella säkerhetsprinciperna, som exempelvis försvar-på-djupet, kan ersätta eller komplettera den strukturerade riskhanteringen.

Hur riskbenägenhet tar sig uttryck vore också intressant att studera. Kanske riskbenägenheten kan uttryckas inte bara i termer av till exempel resursbegränsningar utan också som arrogans, vanor, långsiktighet och paranoia för att bilda ett surrogat för tillit eller illvilja. Ett sådant sätt att mäta riskbenägenhet kan öka förståelsen av både välvilliga intressenters beteende och antagonisters.

Studier behöver genomföras för att avgöra riskacceptanskriteriernas betydelse i olika aktiviteter i riskhanteringsprocessen. Exempelvis kan det studeras hur olika uppsättningar med riskacceptanskriterier påverkar samstämmigheten mellan olika bedömare redan vid bedömningen av sannolikhet och konsekvens för enskilda hot. Fortsatta studier kan också tydliggöra hur mycket av kriterierna som kan fås från överordnad beslutsinstans och hur mycket anpassning som måste göras för den egna organisationen eller det specifika systemet.

5 Referenser

- Abrahamsen, E. B. och Aven, T. (2008) "On the consistency of risk acceptance criteria with normative theories for decision-making", *Reliability Engineering & System Safety*. Elsevier, 93(12), s. 1906–1910.
- Abrahamsen, E. B., Røed, W. och Jongejan, R. (2013) "A practical approach for the evaluation of acceptable risk in road tunnels", *Journal of Risk Research*, 16(5), s. 625–633.
- Abrahamsson, M. och Johansson, H. (2006) "Risk preferences regarding multiple fatalities and some implications for societal risk decision making-an empirical study", *Journal of Risk Research*, 9(7), s. 703–715.
- Adams, J. (1999) "Risk, Freedom and Responsibility", In: *The Risk of Freedom. Individual Liberty and the Modern World*. Institute of United States Studies, University of London: London. Institute of United States Studies, University of London, (1998), s. 33–58.
- Adams, J. (2006) "The Failure of Seat Belt Legislation", i Verweij, M. och Thompson, M. (red.) *Clumsy Solutions for a Complex World: Governance, Politics and Plural Perceptions*. London, UK: Palgrave Macmillan, s. 132–154.
- Altarawneh, L., MacKee, J. och Gajendran, T. (2016) "Factors underlying the concept of risk acceptance in the context of flood-prone land use", *International Journal of Safety and Security Engineering*, 6(3), s. 518–528.
- Anderson, R. (2001) *Security engineering: A guide to building dependable distributed systems*. Wiley.
- Anderson, R. m.fl. (2012) "Measuring the Cost of Cybercrime", i *Workshop on the Economics of Information Security*. Berlin.
- Apostolakis, G. (2004) "How Useful Is Quantitative Risk Assessment?", *Risk Analysis*, 24(3), s. 515–520.
- Aven, T. (2015) "Implications of black swans to the foundations and practice of risk assessment and management", *Reliability Engineering and System Safety*. Elsevier, 134, s. 83–91.
- Aven, T. (2016a) "On the use of conservatism in risk assessments", *Reliability Engineering and System Safety*. Elsevier, 146, s. 33–38.
- Aven, T. (2016b) "Risk assessment and risk management: Review of recent advances on their foundation", *European Journal of Operational Research*, 253(1), s. 1–13.
- Aven, T. och Guikema, S. (2011) "Whose uncertainty assessments (probability distributions) does a risk assessment report: The analysts or the experts?", *Reliability Engineering and System Safety*. Elsevier, s. 1257–1262.

- Aven, T. och Vinnem, J. E. (2005) "On the use of risk acceptance criteria in the offshore oil and gas industry", *Reliability Engineering and System Safety*, 90(1), s. 15–24.
- Aven, T. och Ylönen, M. (2016) "Safety regulations: Implications of the new risk perspectives", *Reliability Engineering & System Safety*, 149, s. 164–171.
- Baskerville, R. (1991) "Risk Analysis: An Interpretive Feasibility Tool in Justifying Information Systems Security", *European Journal of Information Systems*, 1(2), s. 121–130.
- Baybutt, P. (2014a) "Numerical risk tolerance criteria in the United States: A critique of the risk criterion used for the New Jersey Toxic Catastrophe Prevention Act", *Journal of Loss Prevention in the Process Industries*. Elsevier Ltd, 32, s. 428–435.
- Baybutt, P. (2014b) "The ALARP principle in process safety", *Process Safety Progress*, 33(1), s. 36–40.
- Baybutt, P. (2016) "Setting Multinational Risk Tolerance Criteria", *Process Safety Progress*, 35(2), s. 153–158.
- Borg, L., Lichtenberg, S. och Lindskog, S. (2005) "Forskning En probabilistisk skattning av de framtida myndighetskostnaderna", (September).
- Burns, W. R. och Miller, D. (2014) "Improving DOD Adaptability and Capability to Survive Black Swan Events", *JFQ*, 72.
- Champ, P. A., Moore, R. och Bishop, R. C. (2009) "A comparison of approaches to mitigate hypothetical bias", *Agricultural and Resource Economics Review*, 38(2), s. 166–180.
- Cox, L. A. (2008) "What's Wrong with Risk Matrices?", *Risk Analysis*. Blackwell Publishing Inc, 28(2), s. 497–512.
- Cremonini, M. och Martini, P. (2005) "Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA)", i *4th Workshop on the Economics of Information Security*, s. 4.
- Dankovic, D. A. m.fl. (2015) "The Scientific Basis of Uncertainty Factors Used in Setting Occupational Exposure Limits", *Journal of Occupational and Environmental Hygiene*, 12, s. S55–S68.
- Davidsson, G., Lindgren, M. och Mett, L. (1997) *Värdering av risk*. Statens räddningsverk. FoU-rapport P21-182/97.
- Davis, A. (2005) "Return on security investment - Proving it's worth it", *Network Security*. Elsevier Advanced Technology, s. 8–10.
- Dawes, R. M., Faust, D. och Meehl, P. E. (1989) "Clinical versus actuarial judgement", *Science*, 243, s. 1668–74.
- Desaulniers, D. R. (1991) "An examination of consequence probability as a

determinant of precautionary intent”.

Douglas, K. S. (2014) ”Version 3 of the Historical-Clinical-Risk Management-20 (HCR-20 V3): Relevance to Violence Risk Assessment and Management in Forensic Conditional Release Contexts”, *Behavioral Sciences & the Law*, 32(5), s. 557–576.

Dunning, D. (2011) ”The Dunning-Kruger effect. On being ignorant of one’s own ignorance”, *Advances in Experimental Social Psychology*2, 44, s. 247–296.

Erdogan, G. och Stølen, K. (2012) ”Risk-driven security testing versus test-driven security risk analysis”, *CEUR Workshop Proceedings*, 834, s. 5–10.

Fischer, K. *m.fl.* (2013) ”On the assessment of marginal life saving costs for risk acceptance criteria”, *Structural Safety*. Elsevier Ltd, 44, s. 37–46.

Fischhoff, B. *m.fl.* (1980) ”Approaches to Acceptable Risk: A Critical Guide”.

Fischhoff, B. (2015) ”The realities of risk-cost-benefit analysis”, *Science*, 350(6260).

Fisher, P. J. och Yao, R. (2017) ”Gender differences in financial risk tolerance”, *Journal of Economic Psychology*. North-Holland, 61, s. 191–202.

Försvarmakten (2009) *Försvarmaktens gemensamma riskhanteringsmodell, Handbok*. M7739-350012. Försvarmakten.

Försvarmakten (2013a) *Handbok Säkerhetstjänst Grunder (H Säk Grunder)*. M7745-734011. Försvarmakten.

Försvarmakten (2013b) *Handbok Säkerhetstjänst Informationssäkerhet (H Säk Infosäk, M7739-352056)*. Ändring 1. Försvarmakten.

Försvarmakten (2014) *KSF: Krav på IT-säkerhetsförmågor hos IT-system, v3.1*. Försvarmakten.

Gardoni, P. och Murphy, C. (2014) ”A Scale of Risk”, *Risk Analysis*, 34(7), s. 1208–1227.

Garvey, P. R., Moynihan, R. A. och Servi, L. (2013) ”A macro method for measuring economic-benefit returns on cybersecurity investments: The table top approach”, *Systems Engineering*. Wiley Subscription Services, Inc., A Wiley Company, 16(3), s. 313–328.

Ge, W. *m.fl.* (2017) ”Methodology for Establishing Risk Criteria for Dams in Developing Countries, Case Study of China”, *Water Resources Management*. Springer Netherlands, 31(13), s. 4063–4074.

Geerts, R. *m.fl.* (2016) ”Societal risk and Urban land use planning: Creating useful pro-Active risk information”, *Chemical Engineering Transactions*, 48, s. 955–960.

Goerlandt, F. och Reniers, G. (2016) ”On the assessment of uncertainty in risk diagrams”, *Safety Science*. Elsevier, 84, s. 67–77.

Goerlandt, F. och Reniers, G. (2017) ”Evidence assessment schemes for semi-

quantitative risk analyses: A response to Roger Flage and Terje Aven”, *Safety Science*. Elsevier, s. 12–16.

Golob, S. och Kožuh, M. (2016) ”Methodology for determining the risk acceptance criteria for the Seveso establishments”, *Process Safety and Environmental Protection*, 100, s. 163–172.

Gordon, L. A. och Loeb, M. P. (2002) ”The economics of information security investment”, *ACM Transactions on Information and System Security*. ACM, 5(4), s. 438–457.

Hagel, B. och Meeuwisse, W. (2004) ”Risk Compensation: A “Side Effect” of Sport Injury Prevention?”, *Clinical Journal of Sport Medicine*, 14(4), s. 193–196.

Hallberg, J. m.fl. (2017) ”The Significance of Information Security Risk Assessments Exploring the Consensus of Raters’ Perceptions of Probability and Severity”, *International conference on Security and Management*, s. 131–137.

Hallberg, J., Bengtsson, J. och Karlzén, H. (2016) ”Beskriva och bedöma hot mot IT-system – Varför är det så svårt?” FOI-R--4330--SE. Totalförsvarets forskningsinstitut, FOI.

Hansson, J., Granlund, H. och Hallberg, N. (2011) ”Att uttrycka krav i materielmålsättningar – Formulera och granska”. FOI-R--3250--SE. Totalförsvarets forskningsinstitut, FOI.

Hansson, S. O. och Hirsch Hadorn, G. (2017) ”Argument-based decision support for risk analysis”, *Journal of Risk Research*. Routledge, 9877(September), s. 1–16.

Hassenzahl, D. M. (2006) ”Implications of excessive precision for risk comparisons: Lessons from the past four decades”, *Risk Analysis*, 26(1), s. 265–276.

Hermelin, J., Karlzén, H. och Nilsson, P. (2014) *Informationssäkerhet och ekonomi – Ett skannande projekt av aktuell forskning*. FOI-R--3297--SE. Totalförsvarets forskningsinstitut, FOI.

Hubbard, D. W. (2009) *The failure of risk management : why it's broken and how to fix it*. Wiley.

Hungr, O. m.fl. (2016) ”A review of landslide risk acceptability practices in various countries”, *Landslides and Engineered Slopes. Experience, Theory and Practice*, (August), s. 1121–1128.

ISBS (2008) *Information Security Breaches Survey*. Technical Report (URN 08/788). Department for Business Enterprise and Regulatory Reform, London, Storbritannien.

ISO (2009) *ISO Guide 73:2009 – Risk management – Vocabulary*.

ISO (2013) *ISO/TR 31004:2013 – Risk management – Guidance for the implementation of ISO 31000*.

ISO/IEC (2009) *ISO/IEC 31010:2009 – Risk management – Risk assessment*

techniques.

ISO/IEC (2011) *ISO/IEC 27005:2011 – Information technology – Security techniques – Information security risk management.*

ISO/IEC (2013) *ISO/IEC 27001:2013 — Information technology — Security techniques — Information security management systems — Requirements.*

Jaquith, A. (2007) *Security metrics: replacing fear, uncertainty, and doubt.* Addison-Wesley.

Johansen, I. L. och Rausand, M. (2014) "Foundations and choice of risk metrics", *Safety Science*. Elsevier Ltd, 62, s. 386–399.

Johansen, I. L. och Rausand, M. (2015) "Ambiguity in risk assessment", *Safety Science*, 80, s. 243–251.

Kahan, D. M. *m.fl.* (2007) "Culture and Identity-Protective Cognition: Explaining the White-Male Effect in Risk Perception", *Journal of Empirical Legal Studies*, 4(3), s. 465–505.

Karlzén, H., Bengtsson, J. och Hallberg, J. (2017) "Assessing Information Security Risks Using Pairwise Weighting", i *3rd International Conference on Information Systems Security and Privacy, ICISSP 2017*. Porto, Portugal.

Kasperson, R. E. (1983) "Acceptability of human risk", *Environmental Health Perspectives*, VOL. 52(3), s. 15–20.

Kleinmuntz, B. (1990) "Why we still use our heads instead of formulas: toward an integrative approach.", *Psychological bulletin*, 107(3), s. 296–310.

Liu, D., Ji, Y. och Mookerjee, V. (2011) "Knowledge sharing and investment decisions in information security", *Decision Support Systems*. North-Holland, 52(1), s. 95–107.

Monahan, J. och Silver, E. (2003) "Judicial decision thresholds for violence risk management", *International Journal of Forensic Mental Health*. Taylor & Francis Group, 2(1), s. 1–6.

Montibeller, G. och von Winterfeldt, D. (2015) "Cognitive and Motivational Biases in Decision and Risk Analysis", *Risk Analysis*, 35(7), s. 1230–1251.

MSB (2011) "www.informationssäkerhet.se. Myndigheten för samhällsskydd och beredskap (MSB)".

NIST (2010) *NIST Special Publication 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems*. Gaithersburg, MD, USA: National Institute of Standards and Technology.

NIST (2011) *NIST Special Publication 800-39: Managing information security risk*. Gaithersburg, MD, USA: National Institute of Standards and Technology.

- NIST (2012) *NIST Special Publication 800-30, Revision 1: Guide for Conducting Risk Assessments*. Gaithersburg, MD, USA: National Institute of Standards and Technology.
- Pan, L. och Tomlinson, A. (2016) "A systematic review of information security risk assessment", *International Journal of Safety and Security Engineering*, 6(2), s. 270–281.
- Paté-Cornell, E. (1996) "Uncertainties in risk analysis: Six levels of treatment", *Reliability Engineering & System Safety*. Elsevier, 54(2), s. 95–111.
- Paté-Cornell, E. (2012) "On 'Black Swans' and 'Perfect Storms': Risk Analysis and Management When Statistics Are Not Enough", *Risk Analysis*, 32(11), s. 1823–1833.
- Paté-Cornell, E. och Deleris, L. A. (2009) "Failure Risks in the Insurance Industry: A Quantitative Systems Analysis", *Risk Management and Insurance Review*. Blackwell Publishing Inc, 12(2), s. 199–212.
- Paté-Cornell, E. och Fischbeck, P. S. (1995) "Probabilistic interpretation of command and control signals: Bayesian updating of the probability of nuclear attack", *Reliability Engineering and System Safety*. Elsevier, 47(1), s. 27–36.
- Paté-Cornell, E. och Guikema, S. (2002) "Probabilistic Modeling of Terrorist Threats: A Systems Analysis Approach to Setting Priorities Among Countermeasures", *Military Operations Research*, 7(4), s. 5–20.
- Pidgeon, N. (1998) "Safety culture: Key theoretical issues", *Work & Stress*, 12(3), s. 202–216.
- Poore, R. S. (2000) "Valuing Information Assets for Security Risk Management", *Information Systems Security*, 9(4), s. 1–7.
- Rakes, T. R., Deane, J. K. och Rees, P. (2012) "IT security planning under uncertainty for high-impact events", *Omega*. Pergamon, 40(1), s. 79–88.
- Regeringen (2017) "Lagrådsremiss. Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag", s. 203.
- Richter, S. och Sereseanu, A. (2015) "Developing effective risk assessment criteria in regulated environments", *2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, (September), s. 564–569.
- Rogers, R. W. (1975) "A Protection Motivation Theory of Fear Appeals and Attitude Change", *The Journal of Psychology*. Taylor & Francis Group, 91(1), s. 93–114.
- SBU (2005) *Riskbedömningar inom psykiatrin Kan våld i samhället förutsägas? En systematisk litteraturöversikt*.
- Schmidt, M. S. (2016) "Making sense of risk tolerance criteria", *Journal of Loss Prevention in the Process Industries*. Elsevier Ltd, 41, s. 344–354.

- Schoenenberger, L., Schenker-Wicki, A. och Beck, M. (2013) "Analyzing a Terror Network from a Systems Thinking Perspective", (EMNet).
- Schudel, G. och Wood, B. (2000) "Adversary work factor as a metric for information assurance", i *Proceedings of the 2000 workshop on New security paradigms - NSPW '00*. New York, New York, USA: ACM Press, s. 23–30.
- Shrader-Frechette, K. S. (Kristin S. (1991) *Risk and rationality : philosophical foundations for populist reforms*. University of California Press.
- SIS (2007) *SIS HB 550: Terminologi för informationssäkerhet, utgåva 3*.
- SIS (2011) *SS-ISO 31000:2009 – Riskhantering – Principer och riktlinjer*.
- SIS (2015) *SIS-TR 50:2015 – Terminologi för informationssäkerhet*. Teknisk rapport, SIS-TR 50:2015.
- Sjöberg, L. (1999) "Consequences of perceived risk: Demand for mitigation", *Journal of Risk Research*. Taylor & Francis, 2(2), s. 129–149.
- Slovic, P. (1987) "Perception of risk.", *Science (New York, N.Y.)*. American Association for the Advancement of Science, 236(4799), s. 280–5.
- Sommestad, T., Karlzén, H. och Hallberg, J. (2015) "A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour", *International Journal of Information Security and Privacy*. IGI Global, 9(1), s. 26–46.
- Sommestad, T., Karlzén, H. och Hallberg, J. (2017) "The Theory of Planned Behavior and Information Security Policy Compliance", *Journal of Computer Information Systems*. Taylor & Francis, s. 1–10.
- SOU (2017) *SOU 2017:61 Villkorlig frigivning – förstärkta åtgärder mot återfall i brott. Betänkande av Frigivningsutredningen*.
- Spouge, J. (2014) *Feasibility of Harmonised Risk Acceptance Criteria for Transport of Dangerous Goods*. European Commission DG-MOVE, Report No. PP070679/4, Rev. 2.
- Stewart, A. (2004) "On risk: Perception and direction", *Computers and Security*, 23(5), s. 362–370.
- Sturidsson, K. m.fl. (2004) "Clinicians' Perceptions of Which Factors Increase or Decrease the Risk of Violence Among Forensic Out-patients", *International Journal of Forensic Mental Health*. Taylor & Francis Group, 3(1), s. 23–36.
- Sturup, J. m.fl. (2013) *Riskbedömning i kriminalvård och rättspsykiatri: sammanfattningsrapport*.
- Svensk författningssamling (1974) "Kungörelse (1974:152) om beslutad ny regeringsform".
- Säkerhetsskyddsförordning (1996) "Säkerhetsskyddsförordning (1996:633), Svensk

författningssamling 1996:633”.

Säkerhetsskyddslag (1996) ”Säkerhetsskyddslag (1996:627), Svensk författningssamling 1996:627”.

Turoff, M. och Bañuls, V. (2011) ”Major Extensions to Cross-Impact Analysis”, *Evaluation*, s. 1–10.

Vanem, E. (2012) ”Ethics and fundamental principles of risk acceptance criteria”, *Safety Science*. Elsevier Ltd, 50(4), s. 958–967. doi: 10.1016/j.ssci.2011.12.030.

Ward, S. och Chapman, C. (2008) ”Stakeholders and uncertainty management in projects”, *Construction Management and Economics*, 26(6), s. 563–577.

Utformningen av IT-system måste präglas av intressenternas behov för att ge nytta. Dessutom måste de risker som systemen ger upphov till hanteras. Riskhantering tenderar dock att enbart fokusera på riskerna och huruvida de kan accepteras, snarare än att en avvägning görs mot nytta och kostnader.

Under 2017 genomförde FoT-projektet Metodik för säkerhetsmålsättningsarbete en studie om riskacceptans. Målsättningen med studien var att identifiera vad som borde påverka beslut om huruvida risker kan accepteras för planerade IT-system inom Försvarsmakten. Arbetet utgick från Försvarsmaktens egna publikationer samt forskningslitteratur, standarder och branschspecifika vägledningar inom området.

Litteraturen lyfter fram att även om det formella riskacceptansbeslutet tas i slutet av riskhanteringsprocessen måste de underliggande kriterierna för riskacceptans prägla hela riskhanteringsprocessen. Riskacceptansbeslut måste väga in de egna verksamhetsbehoven, både på organisationsövergripande och på systemspecifik nivå. Det är dessutom nödvändigt att väga in lagar och standarder samt behov hos intressenter som kan påverkas av systemet. Forskningen om riskacceptans är dock ganska omogen och det finns många forskningsfrågor som behöver besvaras. Exempelvis är förståelsen av hot en essentiell del av riskhanteringsprocessen – och för riskacceptansen – men hur hoten ska beskrivas är inte klarlagt.

För att förtydliga på vilka grunder som beslut om riskacceptans ska tas inom Försvarsmakten behöver övergripande kriterier för riskacceptans formuleras. Dessutom behöver befintliga instruktioner kompletteras med en beskrivning av hur de övergripande kriterierna anpassas och genomsyrar alla aktiviteter i riskhanteringsprocessen. Det är också av vikt att inse att teknik och behov kan förändras snabbt samt att bedömningarna aldrig kommer att vara perfekta, varför det bör finnas utrymme för regelbunden uppföljning av analyser och beslut.