# Möjligheter och problem med integration av hanteringen av antagonistiska och olycksrelaterade risker

En jämförelse med utgångspunkt från två konsultföretags arbetssätt

***Jon Johansson***
***Jane Nilsson***

**Department of Fire Safety Engineering**
**Lund University, Sweden**

**Brandteknik**
**Lunds tekniska högskola**
**Lunds universitet**

**Report 5183, Lund 2005**

**Rapporten har finansierats av AB Ångpanneföreningen**

# Möjligheter och problem med integration av hanteringen av antagonistiska och olycksrelaterade risker

En jämförelse med utgångspunkt från två konsultföretags arbetssätt

**Jon Johansson**
**Jane Nilsson**

**Lund 2005**

Möjligheter och problem med integration av hanteringen av antagonistiska och olycksrelaterade risker – En jämförelse med utgångspunkt från två konsultföretags arbetssätt.

Jon Johansson
Jane Nilsson

**Report 5183**
**ISSN: 1402-3504**
**ISRN: LUTVDG/TVBB--5183--SE**

Number of pages: 90
Illustrations: Jon Johansson, Jane Nilsson

Keywords
Antagonistic risks, risk, terrorism, sabotage, enterprise risk management, COSO, integration, FEMA, IEC.

Sökord
Antagonistiska risker, risk, terrorism, sabotage, riskhantering, COSO, integration, FEMA, IEC.

Abstract
The aim of this report is to investigate, on the basis of two consult agencies perspectives, what the possibilities and obstacles are to integrate the work with antagonistic and accident related risks. The report is based on two consult agencies where each agency's work procedure is represented by a risk management method. The work with accident related and antagonistic risks is analysed and evaluated compared to four different components. The components are risk management process (IEC's and FEMA's model), driving forces, education and competence, and resources to control risk management with COSO's ERM framework. On the basis of the components the authors discuss the possibilities and obstacles concerning the integration. The results from the analysis are compared with the result from interviews with people working with risk management: The interviewed people were asked how they regard the possibilities and obstacles concerning integration of risk management methods.



Brandteknik
Lunds tekniska högskola
Lunds universitet
Box 118
221 00 Lund

brand@brand.lth.se
http://www.brand.lth.se

Telefon: 046 - 222 73 60
Telefax:: 046 - 222 46 12

Department of Fire Safety Engineering
Lund University
P.O. Box 118
SE-221 00 Lund
Sweden

brand@brand.lth.se
http://www.brand.lth.se/english

Telephone: +46 46 222 73 60
Fax: +46 46 222 46 12

# FÖRORD

Det är många personer som har varit oss till stor hjälp under projektets gång. Hjälpen har varit allt från koncisa idéer till moraliskt stöd och vi vill tacka dessa personer för all support.

Vi vill särskilt tacka företaget AB Ångpanneföreningen och all personal vi varit i kontakt med för stöd med handledare, kontor och andra resurser. Till vår handledare på AB ÅF, Anders Norén, vill vi rikta ett extra tack för tillgänglighet och assistans i svåra stunder.

Ett stort tack riktas till vår handledare, Johan Lundin vid enheten för Brandteknik, för support, kluriga kommentarer och idéer som han har bidragit med under projektets alla faser.

Vi vill även tacka de personer som ställt upp på frågor och intervjuer. Ett speciellt tack riktas till SecMentor A/S för det varma mottagandet i Köpenhamn.

# SAMMANFATTNING

Antagonistiska risker, det vill säga risker relaterade till handlingar utförda med uppsåt, utgör ett bidrag till den totala riskbilden i ett företag. Inställningen till antagonistiska risker har för många förändrats sedan bland annat terrorattacken mot USA den 11 september 2001. Den förändrade inställningen medför ett ökat intresse att ta hänsyn till även dessa risker i en verksamhets riskhanteringsarbete. Genom en samordnad hantering av antagonistiska risker och olycksrelaterade risker finns det hos författarna förhoppningar om att samordningsvinster kan göras inom ett företag.

Projektet syftar till att identifiera möjligheter och problem med en integration av hanteringen av antagonistiska och olycksrelaterade risker utifrån två konsultföretags arbetssätt. De två konsultföretagen är AB Ångpanneföreningen som hanterar olycksrelaterade och SecMentor A/S som hanterar antagonistiska risker. AB Ångpanneföreningen och SecMentor A/S är konsultföretag som används av andra företag som externa aktörer för att hjälpa till med hanteringen av riskerna på företaget.

För att kunna identifiera möjligheter och problem med en integration av arbetssätten, har författarna utfört en analys där hanteringen av riskerna jämförs med varandra. Analysen är utförd efter ett antal komponenter, som författarna anser påverka ett företags riskhantering. De olika komponenterna är:

- *Riskhanteringsprocessen*, där AB Ångpanneföreningens arbetssätt representeras av IEC's modell och SecMentor A/S arbetssätt representeras av FEMA's modell för hantering av antagonistiska risker.
- *Drivkrafter* – anledningarna till att företag arbetar med riskhantering.
- *Utbildning och kompetenser* – den utbildning och kompetens som finns hos de som utför arbetet.
- *Ledning och styrning av riskhantering* med hjälp av COSO's ramverk för ERM.

I analysen jämförs områdena med varandra, komponent för komponent, för att författarna ska kunna resonera kring vad de anser är möjligheter och problem med en integration av arbetet med riskerna.

Analysen visar att det finns vissa möjligheter att integrera arbetet med olycksrelaterade och antagonistsiska risker enligt IEC's och FEMA's modeller. Författarna menar att det till viss del handlar om samma händelseförlopp, när en händelse väl inträffat. Därför anser de att vissa delar av konsekvensberäkningen och riskresponsen, enligt IEC's och FEMA's modeller, bör kunna ske gemensamt eller åtminstone samtidigt. Författarna har dock även identifierat en del problem där de anser att tillvägagångssättet skiljer sig för mycket mellan de båda risktyperna. Exempelvis skiljer sig sannolikhetsbedömningen för mycket mellan IEC's och FEMA's modeller för att samma riskanalysmodeller ska kunna användas. Problemet med sannolikhetsbedömningen medför i sin tur flera andra problem. Till exempel kan det vara svårt att använda samma riskmått om riskernas sannolikhet inte är beräknade på samma sätt.

För att validera resultatet från analysen, utfördes telefonintervjuer med ett antal yrkesverksamma personer. Intervjuerna utfördes för att ta reda på vad de yrkesverksamma ansåg vara möjligheter och problem med en integration. Intervjuerna

användes även till att kontrollera om de komponenter som användes i analysen var väsentliga och om de övergripande slutsatserna var rimliga.

Resultatet från intervjuerna visar att intervjupersonerna i stor utsträckning är samstämmiga. Samtliga ansåg att det i riskhanteringsprocessen finns möjligheter för en integration av beräkningen av konsekvenser samt arbetet med åtgärdsalternativ för att minska respektive risk. Vidare tyckte de att alla risker inom ett företag ska hanteras med ett och samma riskhanteringssystem, för att skapa en övergripande riskbild för ledningen. Dock ansåg de, precis som författarna, att sannolikhetsbedömningen skiljer sig allt för mycket mellan risktyperna för att den ska kunna ske integrerat. Valideringen, med hjälp av intervjuerna, av de komponenter som används i analysen visar att de använda komponenterna kan anses vara väsentliga.

Vid en jämförelse mellan resultatet från analysen och intervjuerna kan både likheter och skillnader ses. Både intervjupersonerna och författarna hade exempelvis samma uppfattning om konsekvensberäkningen, riskresponsen och sannolikhetsbedömningen. Det fanns dock även skillnader mellan intervjupersonernas åsikter och analysen. Författarna tar till exempel upp drivkrafterna som något som kan skapa problem, medan intervjupersonerna inte nämner det som ett problem.

# SUMMARY

Antagonistic risks, i.e. risks related to actions made by intent; contribute to the Enterprise-wide portfolio of risk. The attitude to antagonistic risks has changed since e.g. the attack on USA, 11 September 2001. This change results in a growing interest to consider antagonistic risks when working with risk management. The authors have expectations that a coordinated management of accident related and antagonistic risks will lead to saved resources in a company.

The aim of this report is to investigate, on the basis of two consultant agencies perspectives, what the possibilities and obstacles are integrating the work with antagonistic and accident related risks. The two agencies are AB Ångpanneföreningen that manages accident related risks and SecMentor A/S that manage antagonistic risks. AB Ångpanneföreningen and SecMentor A/S are consultant agencies that are used as external participants to help companies in their risk management work.

To be able to identify the possibilities and obstacles are when integrating the two risk management processes, the authors have made an analysis where the way of managing the two risk types are compared to each other. The analysis is made from a couple of components, which the authors consider affect a company's risk management work. The components are:

- *The risk management process*, where AB Ångpanneföreningen's work procedure is represented by IEC's model to manage accident related risks and SecMentor A/S work procedure is represented by FEMA's model to manage antagonistic risks.
- *Driving forces* – the reasons why a company works with risk management.
- *Education and competence* – the education and competence of the persons that are working with risk management.
- *Resources to control risk management* using COSO's Enterprise Risk Management framework.

In the analysis the risk areas are compared, component by component, to make it possible for the authors to discuss the possibilities and obstacles concerning integration of the two different risk management processes.

The analysis shows that there are some possibilities to integrate the work with accident related and antagonistic risks. The authors advocate that the courses of events, working with antagonistic and accident related risks, in a certain extent are the same. Because of that they conclude that some parts of the estimation of consequence and the risk response, from IEC's and FEMA's models, are possible to integrate. The authors have however also identified some obstacles, where they believe that the work procedures, between the two risks, are too different. As an example they consider that the way of performing probability assessment is too different between the risks to be able to use the same methods. The problem with the probability assessment results in a couple of other obstacles. It can e.g. be hard to use the same measure of risk if the probability is not calculated in the same way.

To be able to strengthen the analysis, a few phone interviews were made. The interviews were carried out with people working with risk management to find out

how they regard the possibilities and obstacles concerning integration. The interviews were also used to verify that the components used in the analysis were essential in risk management and if the overall conclusions were reasonable.

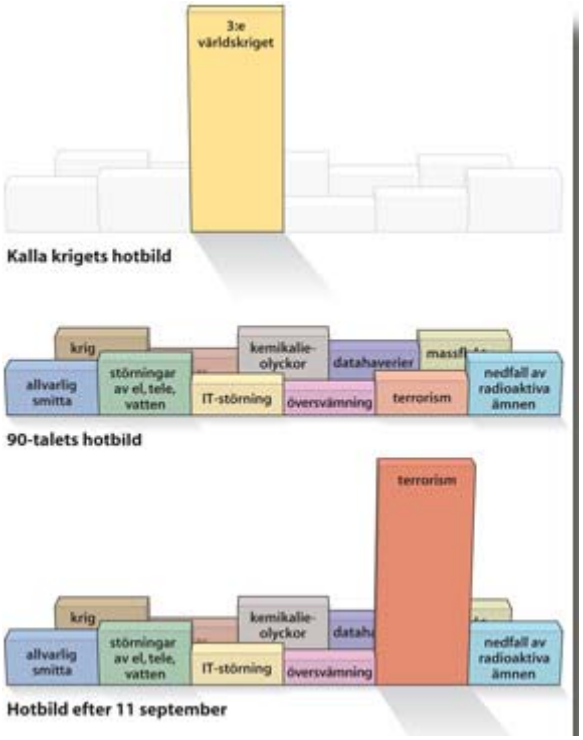
The result from the interviews shows that the interviewed people to a great extent are unanimous. All of them argued that there are possibilities to integrate the estimation of consequence and the risk response, in the risk management process. They also agreed that all risks in a company must be managed in the same risk management system, to give the management an overall portfolio of risk. However they, like the authors, considered that the probability assessment is too different between the risk areas to be able to integrate the work processes. The validation, by means of the interviews, of the components that were used in the analysis points out that the components can be regarded as essential.

When comparing the result from the analysis with the interviews some similarities and differences are detected. The authors and the interviewed people shared the same opinions regarding the estimation of consequence, risk response, and the probability assessment. There are however some differences between the analysis and the result of the interviews. An example of this is that the authors considered the driving forces to be something that might cause problems while the interviewed people did not think of it as a problem.

# INNEHÅLLSFÖRTECKNING

# 1 INLEDNING

Inställningen till antagonistiska hot och risker har för många blivit annorlunda sedan bland annat terrorattacken mot USA den 11 september 2001. Att även antagonistiska risker, det vill säga risker relaterade till handlingar utförda med uppsåt (till exempel terrorism och sabotage), kan utgöra ett bidrag till den totala risken har sedan dess fått större uppmärksamhet i dagens samhälle. Detta illustreras i Figur 1 nedan.




**Figur 1.** Hur den uppfattade hotbilden har förändrats med tiden [1]. Figuren visar på att terrorism har fått en större påverkan på hotbilden efter terrorattacken mot USA den 11 september 2001.

Antagonistiska risker har fått allt större vikt i myndigheters planering [2]. Det är dock viktigt att förstå att enbart en förändrad inställning inte är en lösning [3]. En förändrad inställning är bara en bra start som sedan måste följas upp med handling, det vill säga något måste göras också. På grund av antagonistiska riskers allt större påverkan på hotbilden [4] och att det läggs allt större vikt vid dem från myndigheters sida, torde det vara relevant att ta hänsyn till dessa riskers påverkan och hantera dem även i företag. Som ett steg i ett företags effektivisering menar författarna att det kan finnas möjligheter till en samordnad hantering av antagonistiska risker och olycks-relaterade risker. Genom en samordnad hantering av antagonistiska risker och olycksrelaterade risker finns det hos författarna förhoppningar om att samordnings-vinster kan göras inom ett företag. För att utreda detta måste det först undersökas hur respektive område hanteras och klarlägga möjligheter och problem med en sådan integration eller samordning.

### Företags riskhantering

Med en snabb utveckling i tekniken med större och allt mer komplexa system blir analyserande och förebyggande av risker allt viktigare för att kunna undvika olyckor, vilka i sin tur medför mänskliga och ekonomiska förluster [5]. Detta kan ske genom en väl fungerande riskhanteringsprocess, vilken gör företaget medvetet om sina risker och på så sätt underlättar det förebyggande arbetet med riskerna. För att veta att

resurser läggs på rätt risker, det vill säga utnyttja de mest kostnadseffektiva åtgärdsalternativen som även stämmer överens med företagets policys, gäller det att ha en väl samlad bild av riskerna. Genom att samla alla risker i ett och samma system, erhålls en överskådlig bild av riskerna. För att kunna åstadkomma detta bör alla kända risker finns med, det vill säga även olycksrelaterade och antagonistiska risker. Med en samlad riskbild anser författarna att medvetenheten för riskerna i företaget ökas, vilket i sin tur torde resultera i att riskerna lättare kan hanteras.

Ett företags riskhantering påverkas av flera olika komponenter. Först och främst påverkas det av de risker som är aktuella för företaget i fråga. Dessa risker kan delas upp på flertalet olika sätt beroende på företagets verksamhet, vilka risker som ska illustreras et cetera.

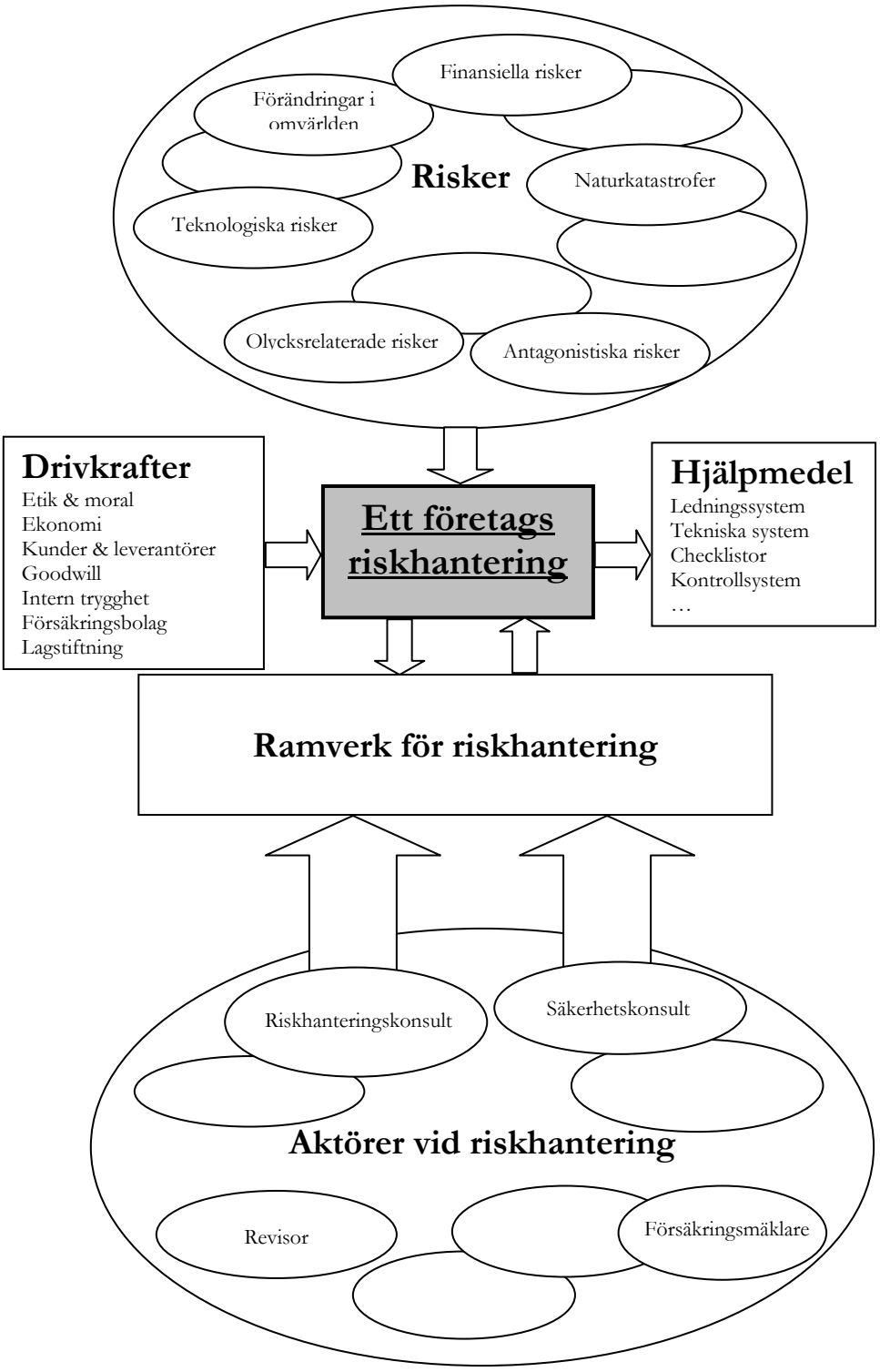
För att ett företag ska hantera de risker som påverkar det, ställs det krav från till exempel myndigheter, samhället och ägare [6]. Dessa krav ställs bland annat i form av lagar.

När företag ska hantera sina risker kan de använda sig av ett ramverk för riskhantering. Ramverk för riskhantering är verktyg för företag, för att få riskhanteringsprocessen att fungera i organisationen. Det är ett sätt att systematiskt strukturera riskhanteringsprocessen eller ett hjälpmedel för att se till så att alla de bitar som behövs finns i systemet för att hantera risker [6]. Att ramverket är skilt från företagets riskhantering i Figur 2 nedan, beror på att författarna vill betona att ramverket är ett hjälpmedel som påverkas av företaget och vice versa. Det är viktigt att ramverket i sig inte ses som lösningen på ett företags riskhantering utan det krävs att företaget använder det på rätt sätt. Ramverket är ett ledningssystem för att hantera risker på ett företag, men detta ledningssystem sköter sig inte själv, utan företaget måste driva det.

Som komplement till ramverket används olika specifika metoder och verktyg för att hantera och beräkna olika risker [6]. Om den specifika expertisen inom ett visst område saknas i företaget, kan företaget välja att ta hjälp av andra aktörer. Dessa olika aktörer kan genom sin expertis bidra med olika delar till företagets riskhanteringsprocess. Aktörerna använder olika modeller för att bearbeta sina respektive områden. Exempel på sådana aktörer är AB Ångpanneföreningen som hjälper företag i hanteringen av olycksrelaterade risker och SecMentor A/S som hjälper företag i hanteringen av antagonistiska risker. Det är dessa båda företag som jämförelsen har sin utgångspunkt från.

Resultatet från riskhanteringsprocessen kan vara olika åtgärder för att till exempel reducera eller kontrollera företagets risker. Åtgärderna kan vara exempelvis införande av tekniska system i form av It-stöd eller ledningssystem för organisationen. Dessa åtgärder påverkas av företagets riskhantering, men det behandlas inte i denna rapport.

Figur 2 illustrerar, i enlighet med texten ovan, författarnas uppfattning om ett företags riskhantering, samt vilka komponenter den kan bestå av. Komponenterna som påverkar ett företags riskhantering ligger till grund för den analys som utförs i rapporten.




**Figur 2** Schematisk bild över författarnas uppfattning om företags riskhantering.

## 1.1 Bakgrund

Examensarbetet är ett obligatoriskt och avslutande moment vid Civilingenjörsprogrammet i Riskhantering vid Lunds tekniska högskola. Projektet omfattar 40 poäng och har genomförts under våren och hösten 2005. Rapporten har utförts med stöd av AB Ångpanneföreningen.

## 1.2 Syfte

Examensarbetets syfte är att identifiera möjligheter och problem med en integration av hanteringen av antagonistiska och olycksrelaterade risker utifrån två konsultföretags arbetssätt.

## 1.3 Målsättning

Målsättningen med examensarbetet är att hitta integrationsmöjligheter som kan leda till att samordningsvinster kan göras mellan AB Ångpanneföreningens och SecMentor A/S's arbete med olycksrelaterade respektive antagonistiska risker. Genom ett samarbete mellan dessa konsultföretag finns det förhoppningar om att på ett effektivt sätt tillsammans kunna leverera en mer komplett och enhetlig produkt till en gemensam kund.

## 1.4 Problemställning

Den övergripande frågeställningen i projektet är *vilka möjligheter och problem finns det med att integrera arbetet med antagonistiska risker och olycksrelaterade risker utifrån de två konsultföretagens arbetssätt?* För att denna fråga ska kunna bemötas behöver först ett antal kringliggande och mer specifika frågor besvaras.

- *Hur ser det antagonistiska hotet ut och vad påverkar riskbilden?*
- *Hur hanteras antagonistiska risker enligt SecMentor A/S?*
- *Hur hanteras olyckrelaterade enligt AB Ångpanneföreningen?*
- *Vad driver företag att arbeta med riskhantering?*
- *Varför ska man arbeta med ERM? Hur är COSO's ramverk uppbyggt?*
- *I vilka delar av ett företags riskhanteringsprocess finns det integrationsmöjligheter i arbetet med antagonistiska och olycksrelaterade risker?*
- *Vad anser yrkesverksamma vara möjligheter och problem med en integration?*

## 1.5 Avgränsningar

Rapporten begränsas till att omfatta endast ett konsultföretag som hanterar olycksrelaterade risker, AB Ångpanneföreningen, och ett företag som hanterar antagonistiska risker, SecMentor A/S. Anledningen till att just dessa företag studeras beror på att arbetet har utförts åt AB Ångpanneföreningen.

I rapporten begränsas företagens arbetssätt till att åskådliggöras av en modell för respektive företag.

Som ramverk för riskhantering har arbetet i rapporten begränsats till att endast undersöka COSO's ramverk för Enterprise Risk Management (ERM).

Telefonintervjuer med yrkesverksamma personer har i projektet endast utförts med personer i Sverige. Vissa av intervjupersonerna har dock erfarenheter från utlandet.

I rapporten tas det inte hänsyn till resultatet från riskhanteringsprocessen som kan vara olika åtgärder som till exempel införande av tekniska system i form av It-stöd eller ledningssystem för organisationen.

## 1.6 Begreppsdefinitioner

Vissa av begreppen nedan är omtvistade och har en rad olika definitioner, ibland beroende på i vilka sammanhang de används. För att göra klarhet i vad som menas med respektive begrepp i denna rapport, redovisas nedan de definitioner som åsyftas.

*Antagonistiska risker:* Antagonistiska risker är risker relaterade till handlingar utförda med uppsåt att skada personer, organisationer eller miljö. Exempel på sådana handlingar är terrorism, sabotage och vandalism. [7]

*Konsekvens:* Konsekvensen är resultatet av en (skade-)händelse. Det kan finnas flera konsekvenser till en och samma händelse och dessa kan uttryckas kvalitativt eller kvantitativt. [8]

*Olycksrelaterade risker:* Olycksrelaterade risker är risker vars orsaker baseras på olyckshändelser, eller icke uppsåtliga felhandlingar som vidare orsakar scenariot. ”Felhandlingen kan bero på bristande kunskaper eller rutiner, stress, plötslig sjukdom, felaktig eller olämplig systemutformning eller information, feltolkning av information eller försummelse.” [9]

*Resulterande risk:* Den resulterande risken (residual risk) är den kvarvarande risken efter de åtgärder som vidtagits, det vill säga efter riskresponsen. [8]

*Risk:* Risk är en sammanvägning av både sannolikhet och konsekvens för en given händelse. Termen risk används generellt endast när det finns åtminstone en negativ konsekvens för händelsen. [8] Sammanvägningen ger att risken totalt sett kan vara stor även om exempelvis sannolikheten är liten, beroende på att konsekvensen är förödande.

*Riskanalys:* Riskanalys (risk analysis) är systematiskt bruk av information för att identifiera riskkällor och för att uppskatta risker (riskanalysen utgör en bas för risk-bedömning och riskrespons). [8]

*Riskaptit:* Riskaptit (risk appetite) är den mängd risk som en organisation är villig att acceptera i strävan efter att uppnå mål och visioner. [10]

*Riskbedömning:* Riskbedömning (risk assessment) är en process som innefattar såväl riskanalys som riskvärdering. [8]

*Riskhantering:* Riskhantering (risk management) är koordinerade aktiviteter för att styra och kontrollera en organisation med avseende på risk. [8]

*Riskhanteringsfilosofi:* Riskhanteringsfilosofin (risk management philosophy) beskriver företags föreställning om risk och hur det väljer att genomföra sina aktiviteter och behandla risker. [10]

*Riskhanteringsprocessen* En riskhanteringsprocess är en kontinuerlig process för att arbeta med risker. [11]

*Riskreduktion:* Riskreduktion (risk reduction) handlar om att minska sannolikheten, de negativa konsekvenserna eller båda, för att reducera en risk. [8]

*Riskrespons:* Riskrespons (risk treatment/response) är en process för urval och implementering av åtgärder för att modifiera risken. [8]

*Riskvärdering:* Riskvärdering (risk evaluation) är den process där den uppskattade risken jämförs med givna riskkriterier för att bestämma riskens signifikans, samt för att avgöra om risken är tolerabel eller ej. [8]

*Sannolikhet:* Sannolikhet är graden av trolighet att en händelse ska inträffa. Sannolikhet kan uttryckas kvantitativt, som ett tal mellan 0 (noll) och 1, eller kvalitativt, som exempelvis osannolikt till troligt. [8]

*Sårbarhet* Sårbarhet är oförmågan hos ett objekt, system, individ, et cetera att stå emot och hantera en specifik påfrestning som kan härledas till inre eller yttre faktorer. [12]

*Sårbarhetsanalys:* Det finns idag ingen internationellt vedertagen standard som definierar vad en sårbarhetsanalys är. Det finns dock i likhet med riskanalyser ett stort antal metoder för att utföra sårbarhetsanalyser. Viktigt att notera är att vissa definitioner och tillvägagångssätt uppvisar stora likheter med hur en riskanalys vanligen beskrivs. En gemensam nämnare för sårbarhetsanalyserna är att de till skillnad från riskanalyserna betonar det skyddsvärda i systemet. [12]

*Säkerhet* Säkerhet definieras som avsaknaden av oacceptabel risk. [13]

*Säkerhetskultur:* Säkerhetskultur (risk culture) relaterar till attityder, förhållningssätt, beteenden, normer och värderingar som

en organisation och dess anställda har till säkerhet och risker. [14]

*Säkerhetsskydd:* Säkerhetsskydd är en sammanfattande benämning på åtgärder för att hindra eller försvåra viss hotande verksamhet och omfattar tillträdesskydd, sekretesskydd, infiltrationsskydd, personskydd och kontrollverksamhet inom området. [15]

# 2 METOD

*I detta kapitel beskrivs den metod som använts under projektets gång. Rapportens disposition redovisas även med en kort beskrivning av innehållet i respektive kapitel.*

## 2.1 Metodik

Huvuddelen av informationssökningen har skett genom litteraturstudier. Utöver litteraturstudierna har samtal och diskussioner genomförts med en riskhanteringsingenjör på AB Ångpanneföreningen, ansvariga för riskhanteringen på företag, konsulter inom området för olycksrelaterade risker, samt med konsulter inom området för antagonistiska risker på det danska företaget SecMentor A/S.

### 2.1.1 Litteraturstudier

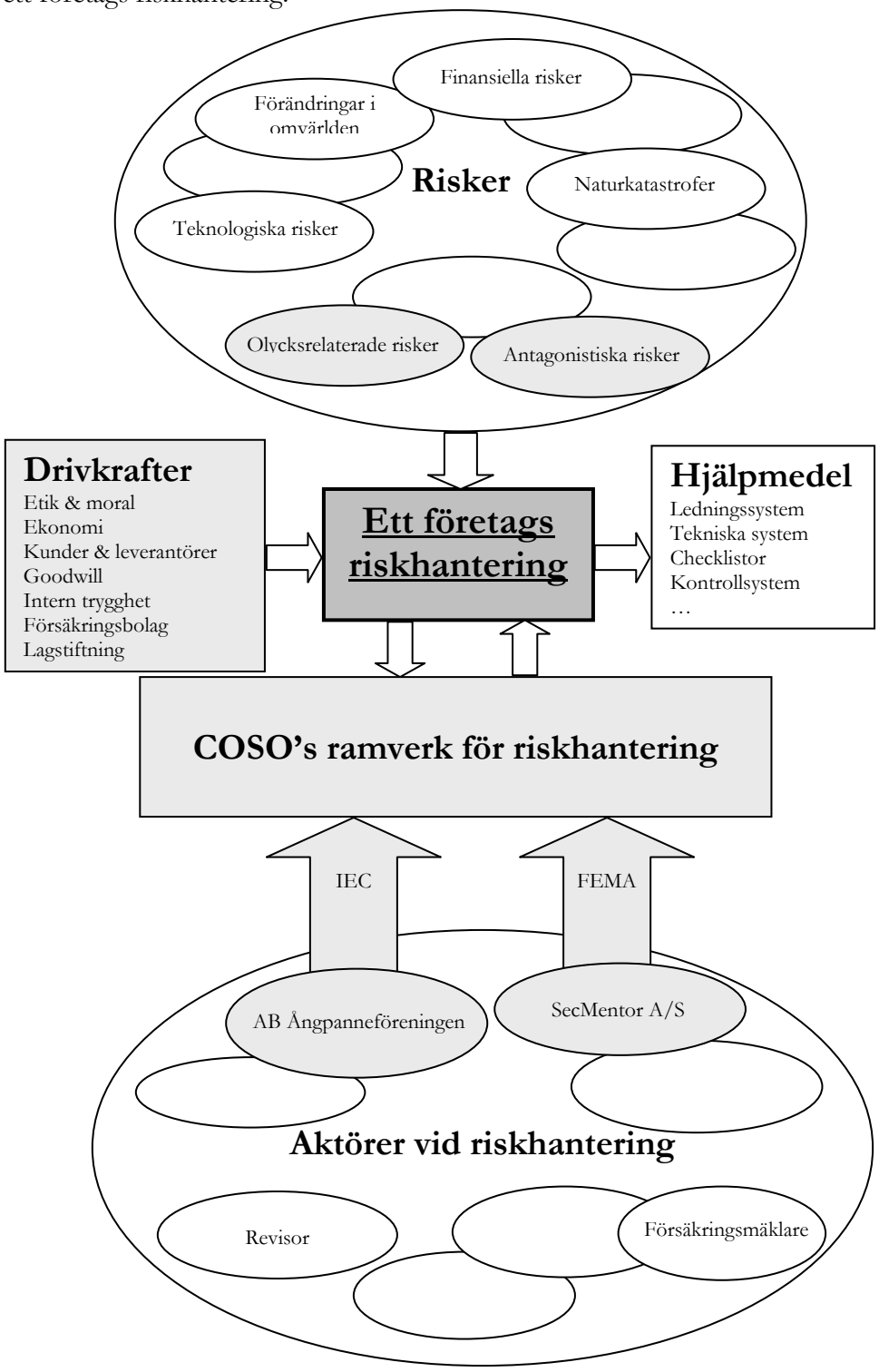
Inledningsvis har litteraturstudier utförts inom respektive område, med tyngdpunkten på antagonistiska risker, för att ge författarna och läsare en överblick över områdena. Dessa litteraturstudier ligger till grund för den introduktion över området för antagonistiska risker som ges i kapitel 3.

Som central utgångspunkt för rapporten har arbetssättet hos två konsultföretag studerats. För antagonistiska risker har arbetssättet på ett danskt konsultföretag, SecMentor A/S, undersökts. För arbetet med olyckrelaterade risker har AB Ångpanneföreningens arbetssätt undersökts. Anledningen till att dessa konsultföretag studerats är att arbetet har utförts åt AB Ångpanneföreningen som vill undersöka möjligheten till samarbete med SecMentor A/S. Undersökningen av deras arbetssätt har skett via intervjuer med personal från respektive företag. Utifrån den undersökningen har författarna låtit en modell få representera respektive konsultfirmas arbete. Valet av modeller har skett efter att via en systematisk litteratursökning i biblioteksdatabaser via LIBRIS [16], LOVISA [17] och ELIN [18], samt på Internet först försökt hitta olika modeller. Författarna har sedan valt de modeller som de anser bäst representera respektive företags arbetssätt. Valet av modell som skulle representera SecMentor A/S har varit svårt då tillgången till modeller för att hantera antagonistiska risker har varit begränsad. I arbetet har det lagts mycket tid på att söka efter modeller, men utan större lycka. Tillgången är dålig och i de fall det finns modeller, lämnas de inte ut på grund av sekretesskäl. Författarna har dock hittat en modell som de anser kan representera SecMentor A/S's arbetssätt. AB Ångpanneföreningens representeras i rapporten av IEC's modell medan SecMentor A/S's arbete representeras av FEMA's modell. Valet att låta en modell representera respektive konsultföretags arbetssätt gjordes för att få en mer strukturerad och övergripande bild av arbetssätten. Ytterligare skäl till att låta modeller representera arbetssätten var att kunna generalisera de slutsatser som dras, förutsatt att de specifika modellerna används.

De drivkrafter som gör att risker hanteras på ett företag finns beskrivna i rapporten. Beskrivningen baseras på litteraturstudier.

För att knyta de två konsultfirmornas arbete till ett företags arbete med riskhantering har ett ramverk för riskhantering studerats närmre. Det ramverk som har studerats i denna rapport är COSO's ramverk för ERM, vilket är ett generellt ramverk för att hantera risker. I rapportens analys beskrivs hur de båda modellerna, IEC's respektive FEMA's, passar in i ramverket.

Figur 3 nedan åskådliggör hur konsultföretagen, ramverket och drivkrafterna passar in i ett företags riskhantering.




**Figur 3** Schematisk figur över författarnas uppfattning om företags riskhantering. Figuren visar hur komponenterna som används i analysen passar in i företagets riskhantering.

Frågor som besvaras i litteraturstudierna är:
*Hur hanteras risker på AB Ångpanneföreningen och SecMentor A/S? Hur hanteras olycksrelaterade risker enligt IEC? Hur hanteras antagonistiska risker enligt FEMA? Hur ser COSO's ramverk för ERM ut?*

### 2.1.2 Komponenter i analysen av integrationsmöjligheter

Analysen har i rapporten utförts med avseende på fyra olika komponenter, där författarna med utgångspunkt från komponenterna har identifierat likheter mellan hanteringen av antagonistiska och olycksrelaterade risker. Komponenterna som ligger till grund för analysen beskrivs i punktlistan nedan. Komponenterna har tagits fram utifrån brainstorming, litteratursökning på Internet och ELIN [18], samt tips från handledare. Komponenterna har valts efter vad författarna anser är relevant vid en jämförelse av arbetet mellan de två områdena, samt vilka komponenter som kan påverka en eventuell integration.

- *Riskhanteringsprocessen* har valts eftersom det är här som risker analyseras och bearbetas. Denna komponent består i rapporten av IEC's modell (se kapitel 4.3) för riskhantering och FEMA's modell (se kapitel 3.5) för hantering av antagonistiska risker. Denna komponent är själva arbetet med riskerna som utförs av konsultföretagen, AB Ångpanneföreningen och SecMentor A/S. För att kunna identifiera integrationsmöjligheter i hanteringen av risker måste själva hanteringen jämföras.

- *Drivkrafter* (se kapitel 5) har valts som komponent eftersom de är anledningen till att ett företag arbetar med riskhantering [6]. Författarna tror att denna komponent kan skilja mellan områdena och att den på så vis kan påverka en eventuell integration.

- *Utbildning och kompetenser* har valts som komponent eftersom de som arbetar med de olika riskerna besitter en viss kompetens. När ett företag köper in en tjänst från en konsult är det deras kompetens de köper. Det krävs specifik kunskap för att kunna använda de metoder och verktyg som används för att hantera risker. Denna kompetens kan skilja mellan områdena och på så vis påverka en eventuell integration.

- *Ledning och styrning av riskhantering på ett företag med hjälp av COSO's ramverk* (se kapitel 6) har valts eftersom om en eventuell integration ska vara möjlig måste de båda riskerna kunna hanteras i samma system. Ett ramverk är till för att strukturera ett företags riskhantering. Ramverket definierar olika steg i en process och förklarar hur de passar ihop [6]. I analysen beskrivs hur de båda riskerna passar in i ramverket (se kapitel 1.1).

För att kontrollera att de komponenter som använts vid analys är väsentliga, har en validering utförts med de intervjuer som genomfördes för att ta reda på vad yrkesverksamma ansåg vara möjligheter och problem med en integration av hanteringen av olycksrelaterade och antagonistiska risker. En jämförelse har gjorts mellan de komponenter författarna kom fram till med de komponenter som intervjupersonerna tog upp (se kapitel 2.1.4).

Frågeställningar som ligger till grund för framtagandet av komponenterna:
*Vilka komponenter är viktiga för riskhanteringsarbetet? Vilka komponenter ska användas som grund vid en analys av möjligheter och problem vid en integration av hanteringen av olycksrelaterade och antagonistiska risker?*

### 2.1.3 Tillvägagångssätt vid analys

Analysen är utförd genom att systematiskt jämföra hanteringen av olycksrelaterade och antagonistiska risker sinsemellan, komponent för komponent. Vid denna genomgång har författarna identifierat likheter och skillnader mellan områdena och sedan resonerat kring vilka möjligheter och problem som dessa skillnader och likheter orsakar.

Vid identifieringen av likheter och skillnader mellan områdena gällande riskhanteringsprocessen, har författarna undersökt vilka steg som finns inom ena området för att sedan se om det finns motsvarande steg inom det andra. Kring dessa motsvarigheter har det sedan förts ett resonemang med avseende på hur dessa steg utförs inom respektive område, för att författarna skulle kunna uttala sig om vilka delar de anser är möjliga att samordna och vilka delar som inte anses vara möjliga att samordna.

När det gäller drivkrafter har författarna fört ett resonemang om vilka möjligheter och problem olika drivkrafter kan medföra för en eventuell integration av hanteringen av olycksrelaterade och antagonistiska risker.

För kompetenskomponenten har det förts ett resonemang kring vilka kompetens-skillnaderna är mellan de båda konsultföretagen.

Slutligen har det förts ett resonemang kring hur de båda risktyperna passar in i ett övergripande ramverk för riskhantering på ett företag, i denna rapport åskådliggjort med COSO's ramverk för ERM. Detta avsnitt beskriver hur de olika delarna från respektive område kommer in i de olika delarna i COSO's ramverk.

Frågeställningar som besvaras är:
*Vad finns det för möjligheter och problem med en integration av antagonistiska med olycksrelaterade risker? I vilka delar av riskhanteringsprocessen finns det integrationsmöjligheter? Hur påverkas dessa av hänsynstagande till antagonistiska risker?*

### 2.1.4 Intervjuer och underlag till validering

Det har utförts intervjuer med ett antal personer som är eller har varit yrkes-verksamma inom respektive område i den privata sektorn. Intervjuerna genomfördes för att validera och möjliggöra en jämförelse med resultatet från analysen av integrationsmöjligheterna. Alla intervjuerna utfördes via telefon och spelades in för att författarna på ett bra sätt skulle kunna dokumentera intervjuerna. Vid intervjuerna fick de yrkesverksamma svara på vad de ansåg vara möjligheter och problem med en integration av hanteringen av olycksrelaterade och antagonistiska risker. De fick även svara på hur de upplever att antagonistiska risker hanteras på företag och om de anser intresset för antagonistiska risker har ökat. Grunden i intervjuerna var dessa två frågor där intervjupersonerna fick tala fritt och svara intuitivt på vad de ansåg. Utifrån det hölls intervjuerna i form av en diskussion, mellan intervjupersonen och intervjuaren, som gick ut på att intervjupersonen fick tala så fritt som möjligt.

Intervjuerna utfördes med nio personer. Personerna har valts ut så att de ska kunna täcka båda områdena, samt både ansvariga för riskhantering på företag och konsulter inom områdena. Intervjuerna har även använts till att göra en validitetstest av de komponenter som författarna tagit fram för att utföra sin analys. Författarnas

komponenter jämfördes med de områden som intervjupersonerna tog upp vid intervjuerna.

För att säkerställa att samtliga personer uppfattade de olika riskerna på samma sätt, definierade författarna de båda riskerna i början av respektive intervju. Resultatet från intervjuerna sammanställdes, där författarna tagit med de delar som var relevanta för examensarbetet. För att kontrollera att resultatet från intervjuerna stämde överens med de intervjuades uppfattningar, fick de intervjuade möjlighet att kontrollera och vid behov korrigera sammanställningen.

Frågor som besvarades var:
*Vad anser yrkesverksamma personer vara möjligheterna och problemen med en integration av hanteringen av olycksrelaterade och antagonistiska risker?*

### 2.1.5 Diskussion

Avslutningsvis för författarna en diskussion om likheter och skillnader mellan resultatet från analysen och resultatet från intervjuerna. Utifrån de likheter och skillnader som diskuteras dras sedan slutsatser i kapitlet slutsatser.

Frågor som behandlas är:
*Eftersom både olycksrelaterade risker och antagonistiska risker ytterst gäller hantering av risker, borde det finnas möjlighet att hantera dem enligt samma principer, åtminstone delar av arbetet? Vilka är fördelarna respektive nackdelarna med att integrera arbetet med antagonistiska och olycksrelaterade risker?*

## 2.2 Rapportens upplägg

För att visa hur rapporten är uppbyggd samt skapa en övergripande bild av rapporten presenteras nedan kort innehållet i respektive kapitel.

*Kapitel 2 – Metod.* I kapitlet har den metod som använts under projektets gång beskrivits. Rapportens disposition redovisas även med en kort beskrivning av innehållet i respektive kapitel.

*Kapitel 3 – Antagonistiska risker.* I detta kapitel beskrivs antagonistiska risker, hur riskbilden påverkas av olika faktorer, vilka aktörer som är aktuella, samt hur antagonistiska risker hanteras. FEMA's modell för hantering av antagonistiska risker åskådliggör i denna rapport hur den typen av risker kan hanteras.

*Kapitel 4 – Olycksrelaterade risker.* Kapitlet beskriver hur olycksrelaterade risker hanteras. Den riskhanteringsmodell som ligger till grund för åskådliggörandet av hanteringen av olycksrelaterade risker är den av IEC framtagna, där de olika stegen i riskhanteringsprocessen beskrivs.

*Kapitel 5 – Drivkrafter.* I kapitlet sker en beskrivning av de drivkrafter som påverkar ett företag att arbeta med riskhantering inom de båda områdena.

*Kapitel 6 – Ledning och styrning av riskhantering på företag.* Detta kapitel beskriver ledning och styrning av riskhantering i form av Enterprise Risk Management (ERM). Som ramverk för detta arbete beskrivs av COSO's ramverk för ERM och dess olika beståndsdelar. Kapitlet är en sammanfattning av COSO's ramverk för ERM [10].

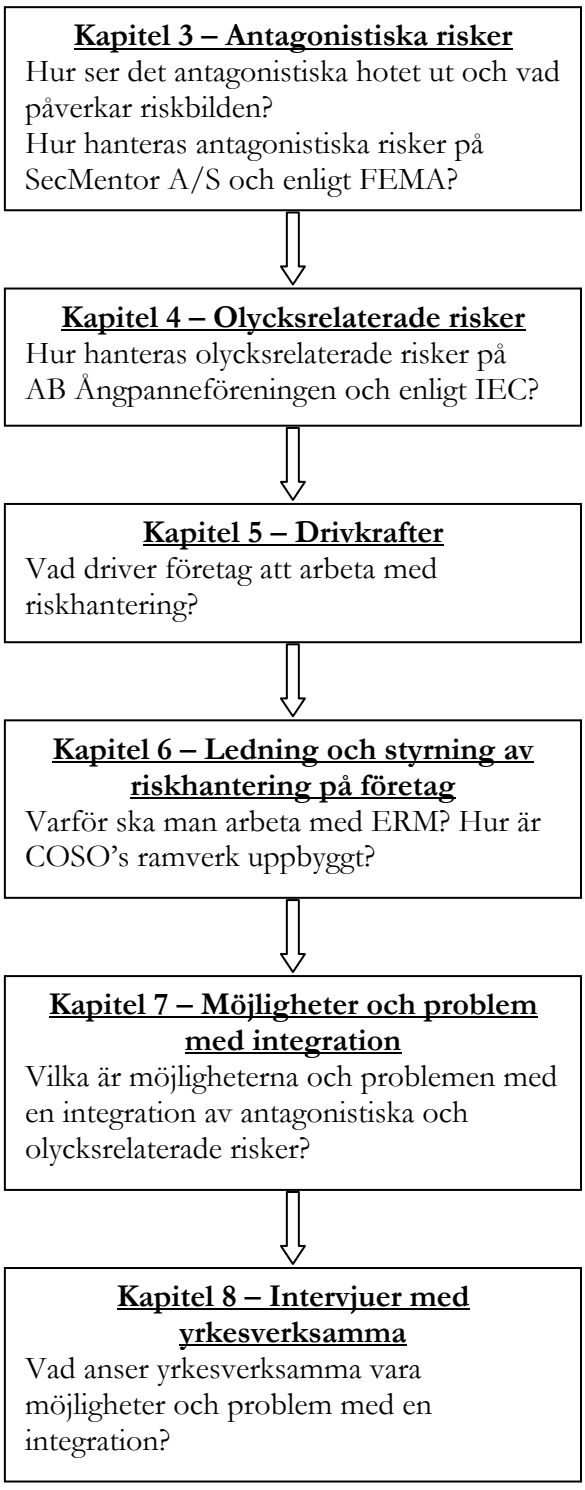
*Kapitel 7 – Möjligheter och problem med integration.* Kapitlet är en analys där författarna själva resonerar kring möjligheter och problem med en integration av hanteringen av olycksrelaterade och antagonistiska risker. Analysen är utförd med utgångspunkt i fyra olika komponenter; riskhanteringsprocessen, drivkrafter, utbildning och kompetenser, samt ledning och styrning av riskhantering med hjälp av COSO's ramverk för ERM.

*Kapitel 8 – Intervjuer med yrkesverksamma.* I detta kapitel redovisas resultatet från ett antal telefonintervjuer som gjordes med yrkesverksamma personer. Intervjuerna utfördes för att undersöka vad yrkesverksamma personer anser vara möjligheter och problem med en integration av hanteringen av olycksrelaterade risker och antagonistiska risker.

*Kapitel 9 – Diskussion.* I detta kapitel förs en diskussion med utgångspunkt från rapportens frågeställningar.

*Kapitel 10 – Slutsatser.* I kapitlet redovisas de slutsatser om möjligheter och problem med en integration av hanteringen av antagonistiska risker och olycksrelaterade risker. Dessa slutsatser har dragits från tidigare förd diskussion.

I Figur 4 nedan presenteras de frågeställningar som har legat till grund för respektive kapitel.




**Figur 4.** Frågeställningar som ligger till grund för respektive kapitel.

# 3 ANTAGONISTISKA RISKER

*I detta kapitel beskrivs antagonistiska risker, påverkan på riskbilden, antagonistiska aktörer, samt hur antagonistiska risker hanteras. FEMA's modell för hantering av antagonistiska risker åskådliggör i denna rapport hur den typen av risker kan hanteras.*

## 3.1 Bakgrundsbeskrivning

Under slutet av 1900-talet har illegal tekniköverföring och transnationell organiserad brottslighet ökat i omfattning och blivit ett allt större hot mot samhället [19]. Terrornätverk och individer har i allt större utsträckning börjat använda sig av omfattande våldshandlingar, vilket tidigare företrädesvis skett i olika slag av inbördeskrig eller mellan stater. Den stora skillnaden är att attentaten riktas mot civila mål som till exempel attackerna i USA den 11 september 2001, attentatet i Madrid den 11 mars 2004 och bomberna i London den 7 juli 2005. Storskaliga attacker med syfte att döda oskyldiga civila har hittills förekommit regelbundet under början av 2000-talet. [20]

Terrorattackerna mot USA den 11 september 2001 dödade omkring 3000 människor och sedan dess har terrorismen i världen uppmärksammats mer än tidigare. Attackerna visade att antagonistiska handlingar inte är inskränkta av nationsgränser. De visade också hur sårbart ett nutida, demokratiskt samhälle kan vara. De uppfattningar som många i västvärlden haft om att terrorister värvas bland fattiga, förtryckta människor utan framtidsutsikter ifrågasattes dessutom, då femton av flygplanskaparna var välutbildade, unga män med trygg medelklassbakgrund. [21]

**Figur 5.** Terrorattackerna mot USA den 11 september 2001, här då två av de totalt fyra kapade flygplanen med arton minuters mellanrum flög in i World Trade Centers tvillingtorn. Byggnaderna föll samman efter drygt en timme, då krascherna och flygbränslet åstadkom så våldsamma bränder att stålkonstruktionen i husen försvagades. Närmare 3000 människor omkom. World Trade Center hade redan 1993 utsatts för ett attentat, då en bilbomb i ett underjordiskt garage vållade stor förödelse och sex personer dödades. [**22**, **23**]

Trots det faktum att antagonistiska risker såsom terrorattacker kan utgöra ett signifikant bidrag till den totala risken på ett företag, förefaller det att antagonistiska handlingar till stor del har blivit negligerade som en bakomliggande faktor. Ett konsekvent antagande i den litteratur som finns tillgänglig, är att det inte är möjligt att förstå fenomenet tillräckligt väl för att kunna kategorisera riskerna associerade till det. Det finns flera svårigheter associerade med att, för exempelvis stora industrier eller anläggningar, inkludera antagonistiska risker i riskanalyser. Hankin och Coster [24] ger förslag på två stycken. En av dem är problemet att hantera antagonistiska risker statistiskt, eftersom avsikten av ett antagonistiskt angrepp kan genereras av en särskild händelse. En annan svårighet är antagandet om att individer inte agerar i ren illvilja.

## 3.2 Påverkan på riskbilden

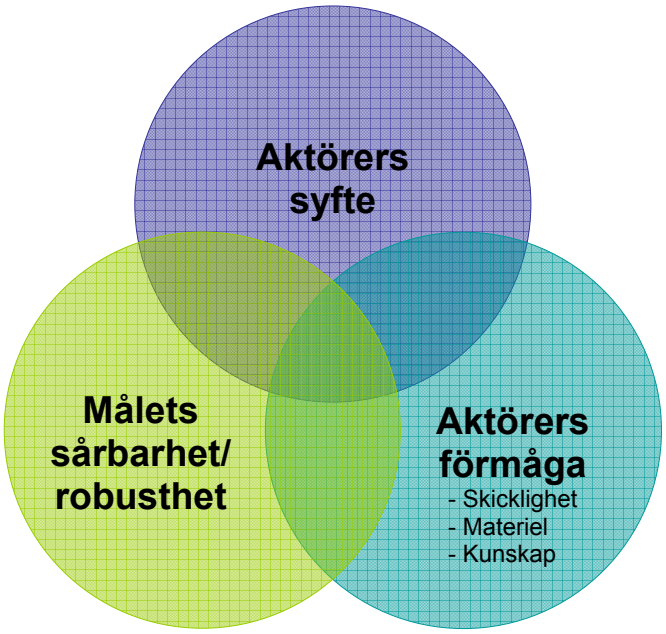
Utvecklingen av hot och risker är, i både tid och rum, nära kopplade till samhällsutvecklingen. De medel som för tillfället finns tillgängliga i samhället används av stater, terrorister, organiserad brottslighet och enskilda aktörer. Konsekvenserna av antagonistiska angrepp avgörs av samhällets uppbyggnad och motståndskraft, det vill säga hur robust eller sårbart samhället är. För att ett antagonistiskt dåd ska kunna genomföras på ett för aktörerna lyckat sätt, krävs att det tänkta målet har en sårbarhet som kan utnyttjas [19].

Det faktum att aktörerna lever och verkar mitt i samhället, i olika länder och över nationsgränser gör problemet komplext och svårhanterat. Människor som är beredda att utföra antagonistiska handlingar arbetar ofta i löst förenade, variabla och ickehierarkiska nätverk. Detta gör det svårt att kartlägga och hindra deras verksamhet. För att vålla betydande skador på befolkningen eller samhället är nätverken av terrorister, i strävan efter sina långsiktliga mål, beredda att använda massförstörelsevapen och okonventionella metoder. [19]

Samhällets resurser och utveckling, såsom Internet och videoinspelningar, används för rekrytering, att upprätta kontakter, sprida propaganda och förmedla budskap mellan länder och världsdelar. Teknik och kunskap om produktion av vapen och vapenbärare finns tillgänglig. På så sätt lär antagonistiska grupper av varandras metoder. Även massmedier har en bidragande roll till att de antagonistiska aktörernas hot eller budskap sprids och inspirerar andra aktörer världen över. [21]

Det är viktigt att observera att medverkan i internationella operationer eller politiska ställningstaganden snabbt kan förändra risken för attacker mot svenska intressen [19]. Det är även viktigt att se problemet ur ett vidare perspektiv, att se Sverige som en del av ett större internationellt sammanhang. Många av dagens hot och risker är gränslösa till sin karaktär. Det finns hot mot utländska intressen i Sverige, där konsekvenserna av en attack kan drabba svenska aktörer både indirekt och direkt.

Värderingar av antagonistiska risker innefattar således att bedöma målets sårbarhet, samt aktörers syfte och förmåga. Förmågan kan ses som kombinationen av skicklighet och tillgången till redskap i form av materiel och kunskap. [20] Detta illustreras i Figur 6 nedan.




**Figur 6.** Värderingar av antagonistiska risker innefattar att bedöma målets sårbarhet, samt aktörers syfte och förmåga. Förmågan kan vidare ses som kombinationen av skicklighet, materiel och kunskap.

Projekteringen och inriktningen av samhällets resurser måste utgå från att en förstärkt förmåga är nödvändig för att möta hotet och konsekvenserna av en fullbordad attack. Detta då den potentiella konsekvensen av en attack är stor och sannolikheten är svår att uppskatta eller rent av variabel i tid och rum. Detta gäller såväl proaktiva som reaktiva åtgärder, men även skadebegränsande insatser. [19]

### 3.2.1 Nio faktorer

Det finns enligt Coster och Hankin nio faktorer som har betydelse vid risk-bedömning av antagonistiska risker [24]. Dessa nio faktorer är ytterligare ett sätt att beskriva den komplexitet som påverkar riskbilden.

**Tillgång (Access)**
Tillgång beskriver graden av tillträde som allmänheten har nära eller på den aktuella platsen. Med minskad tillgång anses risken för antagonistiska händelser minska.

**Säkerhet (Security)**
Säkerhet definieras av Coster och Hankin som svårigheten att kontrollera obehörigas tillgång till den aktuella platsen. Med ökad säkerhet anses risken för antagonistiska händelser minska.

**Synlighet (Visibility)**
Synlighet beskriver till vilken grad som inkräktare måste göra sig själva synliga under själva anfallet vid en antagonistisk handling. Med minskad synlighet anses risken för antagonistiska händelser öka.

**Sekundära hot (Secondary hazard)**
Sekundära hot beskriver potentialen att göra skador på annat än den aktuella platsen, det vill säga skador eller hotelser som exempelvis påverkar allmänheten genom utsläpp av farliga material förorsakat av antagonistiska aktörer. Med minskade sekundära hot anses risken för antagonistiska händelser minska.

**Transparens (Opacity)**
Transparens beskriver med vilken lätthet antagonistiska aktörer kan skaffa sig helt fungerande information om en plats och sålunda graden av intern kunskap som krävs för att förverkliga en sekundär händelse. Med minskad transparens anses risken för antagonistiska händelser minska.

**Robusthet (Robustness)**
Robusthet är ett systems förmåga att på ett säkert sätt motstå skadegörelse. På platser med låg robusthet är det således högre sannolikhet att en eventuell attack vållar allvarliga konsekvenser.

**Respons för upprätthållande av lag och ordning (Law enforcement response)**
Respons för upprätthållande av lag och ordning beskrivs som den hastighet och effektivitet som den lokala polisen eller motsvarande svarar med på en antagonistisk handling. Denna faktor är svår att bedöma, då en snabb och verkningsfull respons både kan innebära större och mindre risk för antagonistiska händelser, beroende på aktörernas syfte med attacken. Detta är heller ingen faktor som lätt kan påverkas eller hanteras av företag, men det kan vara nyttigt att känna till den.

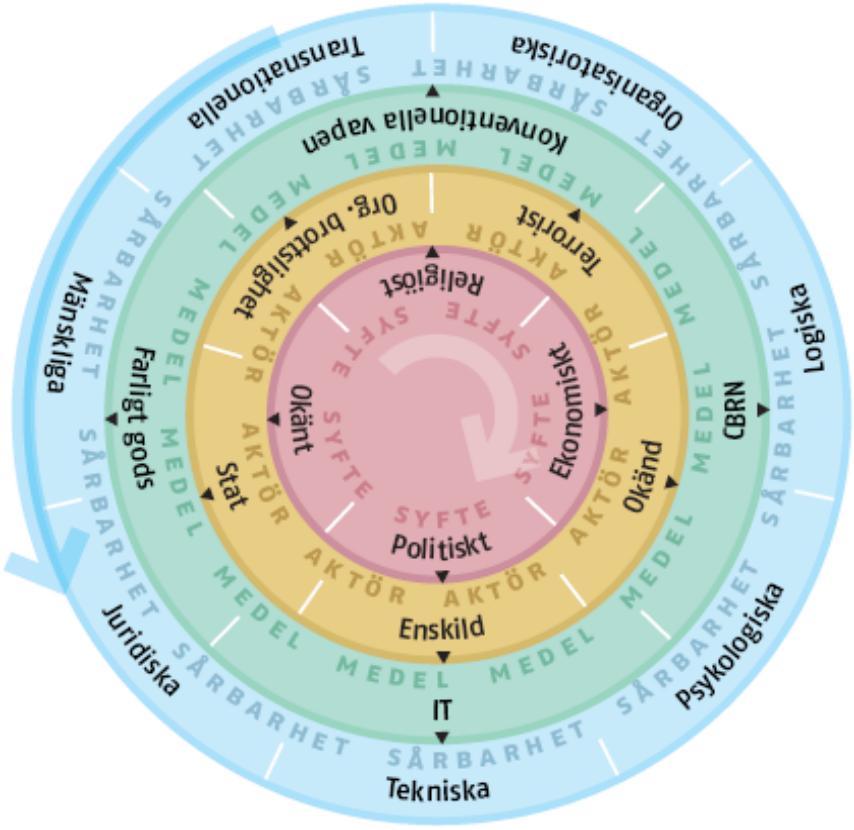
**Offerprofil (Victim profile)**
Offerprofil beskrivs som befolkningskarakteristiska för de som blir utsatta för risken, utöver de som befinner sig på den attackerade platsen. Effekten av ett antagonistiskt angrepp anses vara större när det finns orättvist drabbade, det vill säga när människor som inte har någon anknytning till platsen eller företaget blir offer för den.

**Politiskt värde (Political value)**
Politiskt värde är den symboliska makten av att förstöra ett mål i relation till en antagonistisk aktörs program. Aktörers mål kan i vissa fall väljas för att de har ett politiskt eller socialt värde i sig själva.

## 3.3 Antagonistiska aktörer

Det blir allt svårare att dra en skarp gräns mellan terrorism och exempelvis organiserad brottslighet. Studier visar att terrororganisationer och internationell organiserad brottslighet samarbetar och använder samma resurser. Utvecklingen går mot att samma människor och medel används ofta för olika syften beroende på när de bäst behövs. Sammansmältningen gör att den potentiella faran i dessa hot ökar ytterligare. Falska hot måste ofta behandlas som verkliga hot och är ett annat mer vanligt förekommande problem, eftersom det är resurskrävande för samhället. [19]

Nedan följer en schematisk bild över olika antagonistiska aktörer och komplexiteten i dagens hotbild, se Figur 7 och därefter presenteras de olika aktörerna var för sig.




**Figur 7.** Trissan är tänkt ge en schematisk bild över och beskriva komplexiteten i dagens hotbild. Trissans olika skikt kan snurras separat och genom detta erhålls olika utfall. Trissan är även tänkt beskriva konvergensen mellan de olika skikten. Den gör inte anspråk på att ge en helhetsbild utan tyngdpunkten ligger i att ge en förståelse för komplexiteten i hotbilden. [20]

### 3.3.1 Terrorism

Terror är det latinska ordet för skräck eller skräckvälde. Definitionen av terrorsim är omtvistad, men den vanligaste definitionen är att terrorism innebär organiserade våldshandlingar som är politiskt betingade och syftar till att påverka samhället eller ett lands politik, utan hänsyn till om oskyldiga drabbas [25]. Offren vid terrordåd är mestadels människor som av en slump råkar befinna sig på platsen där attentatet äger rum [26].

Terrorismen riktas mot befolkningen och mot funktioner som har särskilt folkrättsligt skydd. Internationell terrorism med syfte att vålla stor skada har ökat under de senaste åren. Internationella terroristnätverk har visat att de kan använda de resurser som finns i samhället för att genomföra terrordåd. De har även genom olika attentat visat prov på noggrann planering och dolt uppträdande. Attackerna har lett till stora förluster i människoliv och har påverkat viktiga politiska beslut. [19]

En del terrornätverk har mycket långsiktiga mål och kreativiteten är stor inom den projektliknande terrorism som tillämpas inom terrornätverk som Al Qaida, den organisation som tog på sig ansvaret för bland annat attackerna mot USA den 11 september 2001. Detta bidrar till svårigheten i att bestämma konsekvens och sannolikhet för antagonistiska risker, där fantasin kan vara en begränsande faktor i hanteringen.

Antagonistiska organisationer i skilda nationer och regioner har visat ökade benägenheter till att samarbeta. De tillfällen och de medel som enklast och effektivast exploaterar sårbarheterna i samhället används. Kombinationen av olika förmågor och erfarenheter gör att risken för allvarliga och oförutsedda former av angrepp ökar. [19]

Det hittills vanligaste sättet att genomföra ett antagonistiskt angrepp på har varit genom konventionella sprängämnen eller nyttjande av andra farliga ämnen som kan användas som sprängmedel [20]. Ett av de allvarligaste hoten är angrepp med kemiska, biologiska och radiologiska ämnen samt nukleära vapen (CBRN). Masseffektsvapen är ett begrepp som används för fysiska eller elektroniska medel som får stora konsekvenser. Exempel på detta är förutom massförstörelsevapen även omfattande angrepp med elektroniska eller psykologiska vapen. Att sådana attacker inte har utförts beror sannolikt på att de nödvändiga tekniska och operativa förmågorna ännu saknas bland antagonistiska aktörer. [19]


**Figur 8.** Foto: Reuters. Brittiska tidningar dagen efter terrorattackerna mot kollektivtrafiken i London den 7 juli 2005, då 38 människor miste livet och cirka 700 skadades. Dagen innan öppnades G8-mötet i Skottland och London hade dessutom fått förtroendet att arrangera OS 2012.

### 3.3.2 Organiserad brottslighet

Mer eller mindre väl strukturerade sammanslutningar bedriver organiserad brottslighet med syfte att erhålla stora ekonomiska vinster genom illegala aktiviteter. I Italien används uttrycket ”maffia” och den amerikanska motsvarigheten är ”Cosa Nostra”. Det som karakteriserar den organiserade brottsligheten är arbetsdelning för minimerad upptäcktsrisk, liksom utnyttjande av personliga, affärsmässiga och politiska förbindelser. Den organiserade brottslighetens omfattning är svår att fastställa, bland annat därför att offer och vittnen ofta är ovilliga att samarbeta med myndigheter. [27]

Organiserad brottslighet har ett destruktivt inflytande på rättsstaten och instabilitet blir dess följd. Globalisering kombinerat med instabila stater som basområden för organiserad brottslighet har lett till fördelaktigare premisser för internationella kriminella organisationer. Det krävs stora samhällsresurser för att häva organiserad brottslighet när den väl har etablerats i ett samhälle. [19]

### 3.3.3 Extrema grupper

Det finns extrema grupper, såsom den nazistiska vit makt-miljön och fristående vänstergrupper, som kan hota rikets inre säkerhet. De fristående grupperna präglas av idéer som frihetlig socialism, anarkism och syndikalism. Vilket hot dessa grupper på sikt utgör mot samhällets säkerhet och beredskap är svårbedömt. Internationaliseringen av grupperna kan göra dem mer resursstarka. Detsamma är fallet om de lyckas knyta till sig personer som på olika sätt har särskild kunskap. [19]

Enstaka händelser kan öka stödet för extrema grupper och benägenheten att använda politiskt motiverat våld kan utlösas av enstaka händelser. Exempel på detta är den utveckling som har skett i Nederländerna efter mordet på en kulturpersonlighet som kritiserat islamistiska grupper och sedvänjor. Efter mordet har våld riktats mot moskéer och andra muslimska centra. [19]

### 3.3.4 Enskilda aktörer

Svårförutsedda och svårförstådda handlingar kan utföras av människor som lider av en psykisk störning eller som på något sätt har en förvrängd verklighetsuppfattning. Även mer rationellt handlande människor kan förorsaka stora skador i ett system. Det kan vara personer som känner sig orättvist behandlade eller hyser agg mot samhället eller mot sin arbetsgivare. [19]

Vanligtvis kan inte en enskild individ vara ett hot för samhällets säkerhet och beredskap. Enskilda individer, insiders, med särskilda kunskaper kan dock skada myndigheter eller företags verksamheter, antingen genom fysiskt eller informations-systemsrelaterat sabotage. Insiders kan hota samhällets säkerhet genom att stjäla information från sin arbetsgivare. [19]

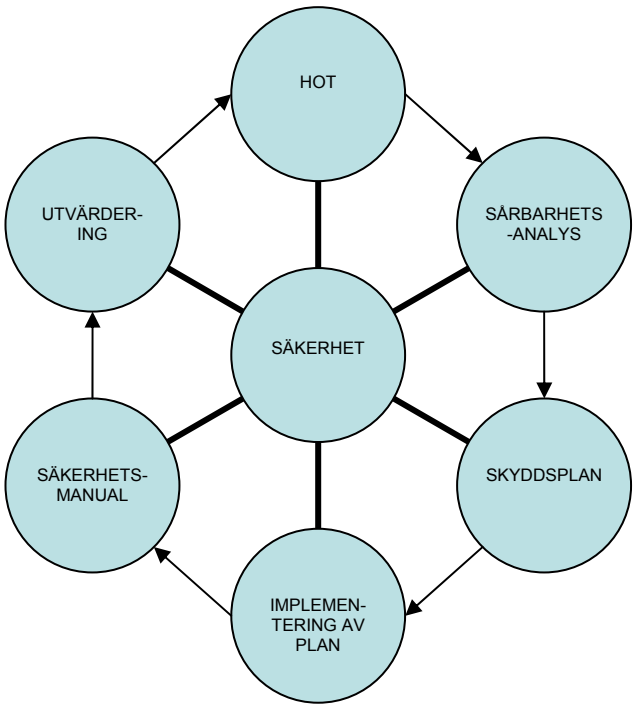
En sårbarhet som kan få allvarliga konsekvenser för krishanteringssystemet är att vissa samhällsfunktioner är beroende av nyckelpersoner. Denna sårbarhet kan undvikas genom att personal- och nyckelpersonsfrågor är en naturlig del av kontinuitetsplanering och risk- och sårbarhetsanalyser. [19]

## 3.4 SecMentor A/S

SecMentor A/S är ett danskt konsultföretag som inriktar sig på hantering av antagonistiska risker. Materialet i kapitel 3.4 är en sammanfattning av uppgifter från SecMentor A/S [28]. I kapitel 3.5 beskrivs FEMA's modell för hantering av antagonistiska risker som i rapporten åskådliggör SecMentor A/S arbetssätt. SecMentor A/S har ingen uttalad modell men FEMA's är den som författarna anser representera deras arbete. Modellen är dock framtagen för att analysera antagonistiska risker i höga byggnader.

SecMentor A/S's metod för att analysera ett företag sker i stort sett i tre faser (inledande möte, sårbarhetsanalys, samt skyddsplan). Processen är menad som en iterativ process som hela tiden hittar nya risker som måste åtgärdas. Företagets

anställda har bland annat tidigare erfarenheter från militären och är därtill examinerade till ”sikringsleder med specialisering inom security, säkerhetsledning och brand”.




**Figur 9.** SecMentor A/S bedömningsprocess av antagonistiska risker. Bedömningsprocessen består av ett antal byggstenar som ska verka i ett kretslopp i strävan efter ständiga förbättringar. [28]

### 3.4.1 Inledande möte

När SecMentor A/S ska utföra en riskbedömning med avseende på antagonistiska risker på ett företag, börjar de med att träffa representanter för företaget. Vid dessa möten bestäms avgränsningar för bedömningen samt vilken riskaptit företaget har, det vill säga vilken risk företaget är villigt att acceptera.

### 3.4.2 Sårbarhetsanalys

När det inledande mötet är genomfört, börjar SecMentor A/S utföra en sårbarhets-analys på företaget. Till sin hjälp användes de anställda vid företaget, vilka har bra kännedom om företaget och dess verksamhet.

I analysen delas företaget in i skyddsnivåer, där den tredje nivån innehåller de värden som är mest skyddsvärda i företaget. Indelningen sker för att skaffa sig en bild över företagets tillgångar så att svagheter i verksamheten kan identifieras.

Sårbarhetsanalysen börjar med att inventera miljön kring verksamheten, för att sedan gå inåt i organisationen (både konkret och schematiskt). Saker som beaktas vid analysen är till exempel trafiktäthet (dag respektive natt), gatubelysning eller annan belysning, insyn (dagliga rutiner som posthantering, leveranser), lokalpolitik (kriminell belastningsnivå inom det lokala området), samt profil (vilken framtoning företaget utstrålar, balans mellan arbetet med att uppnå säkerhet och säkerhetsskydd). Andra saker som det tas hänsyn till är olika rutiner (vaktstyrkor, leveranser, posthantering, sophämtning), hur receptionen fungerar, samt hur lätt det är att ta sig in till olika delar av företaget.

När sårbarhetsanalysen utförs sker det utifrån de i förväg fastställda områdena:

- Personalsäkerhet
- Materielsäkerhet
- Kontorssäkerhet
- Informationssäkerhet
- Fysisk säkerhet
- Brandsäkerhet och följverkningar
- Industrispionage
- Säkerhetsåtgärder mot terrorverksamhet
- Rapportering

**Personalsäkerhet**
För att säkerställa att inga oönskade personer finns i organisationen sker analys av företagets anställningsrutiner, samt rutiner för att kontrollera redan anställd personal. Till exempel anses att belastningsregister bör kontrolleras vid anställning och tystnadsplikt ska skrivas under.

Personalsäkerheten handlar även om skydd för den egna personalen och deras trygghet.

**Materielsäkerhet**
Materialsäkerhet är åtgärder för skydd av verksamhetens materiel såsom bärbara datorer, mobiltelefoner, verktyg, fordon, försändelser och annat material. Svinnet kan exempelvis minska om det är tillåtet att låna från företaget.

**Kontorssäkerhet**
När det gäller kontorssäkerhet analyseras hur åtkomsten är till respektive skyddsnivå, vilka som kan komma in var, om obehöriga kan ta sig in och så vidare. Det ska även tas hänsyn till rutiner som vem som tömmer papperskorgar, eller var skräpet tar vägen.

**Informationssäkerhet**
Analysen behandlar rutiner som har med hur information sprids, vilka som har tillgång till viss information och hur lätt det är att komma åt den. Känslig information (exempelvis forskning och strategiplaner) bör endast behandlas som klassificerade dokument, samt i för ändamålet anpassade nätverk eller enskilda datorer. Klassifikationen av dokument kan ha olika steg, exempelvis UNCLASSIFIED – RESTRICTED – CONFIDENTIAL – SECRET.

**Fysisk säkerhet**
Fysiskt säkerhetsskydd är den disciplin som är mest känd, då den ofta är synlig. Med den fysiska säkerheten menas analys av portar, galler och låsta dörrar, samt hägn. Den fysiska säkerheten har ett betydligt signalvärde, det vill säga vilka signaler som verksamheten sänder ut.

**Brandsäkerhet och följverkningar**
För att undvika att bränder uppstår, görs en genomgång av företaget för att kontrollera att alla brandtekniska installationer fungerar som de ska, samt att alla brandtillbehör (brandfiltar, handbrandsläckare) finns tillgängliga. Det sker även en

klassifikation av brand- och explosionsfarliga områden i verksamheten. För att klara av en eventuell brand får företaget hjälp med att försäkra sig mot bränder.

**Industrispionage**
Alla verksamheter har konkurrenter som vill skaffa sig fördelar för att öka sin vinst. Det är viktigt att se till att företagshemligheter hålls inom företaget. I detta område bör det beaktas vilka som kan ha intresse av organisationen, hur de kan gå till väga et cetera. Detta kan även gälla den egna personalen, där någon kan vilja sälja information eller ha information till sitt eget företag.

**Skyddsåtgärder mot terrorverksamhet**
Skyddsåtgärder mot terrorverksamhet är ett viktigt område och ska ingå i säkerhetsmanualen (se kapitel 3.4.3). Korrekt genomförande och kontroll av säkerhetsåtgärderna medför en minskad risk för terrorhandlingar mot verksamheten.

**Rapportering**
Ingen händelse får komma som en överraskning så att en ledande medarbetare uttalar sig till pressen utan att ha vetskap om aktuell angelägenhet.

Alla säkerhetsrelaterade händelser, stora som små, ska rapporteras till ledningen. Händelser ska rapporteras direkt och senare uppföljas skriftligen.

Medarbetare på alla nivåer ska veta vem som ska uttala sig till pressen och ska kunna hänvisa till denne, i stället för att uttala sig själv.

Sårbarhetsanalysen utvärderar hur väl rapporteringsrutinerna fungerar samt ger förslag på möjliga förbättringar.

### 3.4.3 Skyddsplan

Det sista steget är att göra en skyddsplan, vilket är det åtgärdspaket som föreslås för företaget. När skyddsplanen är färdig ska alla åtgärder köpas in och implementeras korrekt.

Vid implementeringen är det viktigt att arbeta med inställningen till åtgärderna, säkerhetskulturen. En verksamhet kan köpa sig fattig på säkerhetsskydd utan nytta, om verksamhetens medarbetare inte har en positiv inställning till säkerhet och säkerhetsskydd.

Med det färdiga skyddet på plats skrivs en säkerhetsmanual. Säkerhetsmanualen är en dokumentation av företagets arbete för att uppnå säkerhet och de rutiner som finns det. När alla åtgärder är implementerade sker en utvärdering av dem för att undersöka om de åstadkommer som det var menat, samt för att se hur stor den resulterande risken är. Processen blir iterativ då företaget efter utvärderingen börjar om från början, för att ytterliggare förbättra säkerheten.

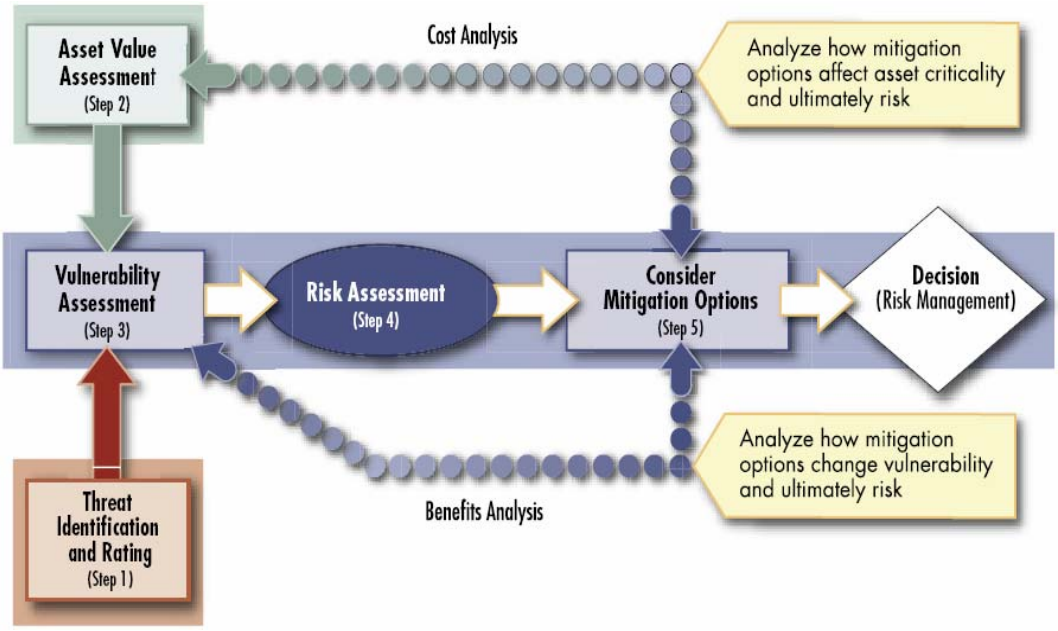
## 3.5 Riskbedömning av antagonistiska risker enligt FEMA

Kapitel 3.5 är en genomgång av FEMA's modell för hantering av antagonistiska risker. Denna modell är den som författarna anser bäst representera SecMentor A/S arbetssätt. Materialet i kapitlet är en sammanfattning av FEMA's manual [29]. Valet av modell som i rapporten representerar SecMentor A/S var svårt då tillgången till modeller för att hantera antagonistiska risker är begränsad. I arbetet har det lagts mycket tid på att söka efter modeller, men utan större lycka. Tillgången är dålig och i de fall det finns modeller, lämnas de inte ut på grund av sekretesskäl. Författarna tycker sig dock ha hittat en modell som de anser kan representera SecMentor A/S's arbetssätt.

The Federal Emergency Management Agency (FEMA), i USA, har utvecklat en manual för att utföra en riskbedömning vars mål är att minska effekten av eventuella olyckor som är initierade av människan. Det är en kvalitativ metod för risk-bedömning som bygger på en metod som är framtagen åt Department of Veterans Affairs (VA) genom The National Institute for Building Sciences (NIBS). Manualen är ursprungligen framtagen för byggnader men kan även användas för andra kritiska infrastrukturer. Ett av de primära målen med manualen är att skapa en allmän terminologi inom området.

För att kunna skapa en säker omgivning är det många faktorer som måste beaktas. Figur 10, FEMA's modell för hantering av antagonistiska risker, beskriver bedömningsprocessen för att identifiera de bästa och mest kostnadseffektiva åtgärderna mot antagonistiska risker.

Ett stort problem när det gäller antagonistiska risker är att det är svårt att förutspå hur, när och varför en aktör slår till. Antagonistiska angrepp kategoriseras ofta som låg sannolikhet och hög konsekvens.




**Figur 10.** FEMA's modell för hantering av antagonistiska risker [29].

### 3.5.1 Hotanalys (Threat identification and rating)

Innan riskbedömningen påbörjas måste varje organisation bestämma sig för vilken risk organisationen är villig att acceptera, det vill säga fastställa sin riskaptit. Det är riskaptiten som sedan är avgörande i valet om det ska utföras riskreducerande åtgärder eller ej.

Det första steget i FEMA's modell är att utföra en hotanalys. Denna går ut på att identifiera möjliga hot och analysera dessa. Att identifiera möjliga hot kan vara svårt eftersom de är svåra att förutspå. När det gäller antagonistiska risker är det viktigt att förstå vilka aktörer som kan vara intresserade av att skada berörd organisation, samt att hålla sig uppdaterade om bland annat deras tillvägagångssätt. Denna sorts information införskaffas genom att kontakta och rådfråga säkerhetsorganisationer och myndigheter som till exempel svenska Säkerhetspolisen. Utifrån den information som de kan bistå med väljs primära hot som sedan bedöms utifrån sannolikhet att antagonistiska aktörer utför en handling samt konsekvensen av den. En vanlig metod att utvärdera antagonistiska hot är att analysera fem faktorer: existens, kapacitet, historik, syfte, förberedelser.

- Existens – Vem eller vilka kan vara ett hot mot företaget?
- Kapacitet – Vilken kapacitet har de? Vad har de tillgång till för medel, vapen et cetera?
- Historik – Vad har hänt tidigare? Hur ofta? Hur gick aktörerna till väga?
- Syfte – Vad kan de potentiella aktörerna vilja uppnå?
- Förberedelser – Vet företaget om någon bevakat dem eller möjligen närliggande organisationer?

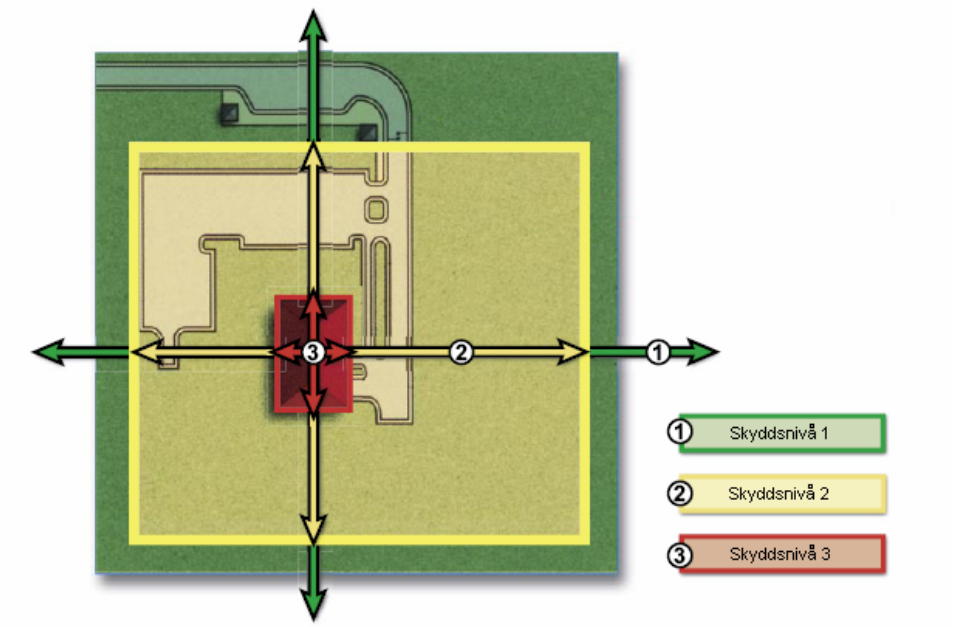
Hotanalysen kan variera från ett översiktligt hotscenario till en detaljerad analys av en specifik grupp eller person. Utifrån analysen bestäms sedan sannolikheten för de olika hoten. I manualen ges ett antal arbetsblad och tabeller som kan användas som understöd vid bedömningen av sannolikheten. Manualen översätter sannolikheten för hotet till en tiogradig skala som sedan kan vägas samman med tillgångsvärderingen och sårbarhetsanalysen. Bedömningen utförs av en grupp medarbetare från organisationen, samt med experter inom området.

### 3.5.2 Tillgångsvärdering (Asset value assessment)

För att ta reda på var företagets viktigaste resurser finns och värdera dessa är det en fördel om medarbetare från organisationen medverkar i arbetet. Det är viktigt att inte bara tänka materialistiskt, utan att även att bedöma människorna i organisationen, samt deras kunskaper. Ett företags mest värdefulla resurser är medarbetarna i företaget.

Tillgångsvärderingen sker i tre steg, där det första är att identifiera organisationens kärnfunktioner som är nödvändiga för att driva organisationen efter en möjlig attack. Det andra steget är att utvärdera företagets infrastruktur och identifiera alla resurser och värden i företaget. Utvärderingen sker utifrån en genomgång av företaget där det uppskattas kostnaden av en eventuell händelse, hur många som skadas, vad som påverkas inom och runt organisationen, samt om det skadade kan ersättas och då hur snabbt och till vilken kostnad. Detta kvantifieras sedan till en tiogradig skala, för att ge större överblickbarhet.

Manualen använder sig av det traditionella sättet att dela in det fysiska området i tre skyddsnivåer, med de mest skyddsvärda resurserna i den tredje nivån (se Figur 11). Indelningen sker för att få en klarare bild av vilka tillgångar och resurser som behöver skyddas. Detta blir även en faktor att väga in i valet av åtgärd, då den tredje nivån ska ha högre skydd än de två första.




**Figur 11.** Enligt FEMA delas det fysiska området traditionellt in i tre olika skyddsnivåer, där det mest skyddsvärda finns i nivå tre [29].

### 3.5.3 Sårbarhetsanalys (Vulnerability assessment)

Nästa steg i processen är att utföra en sårbarhetsanalys av de tidigare identifierade tillgångarna utifrån den hotbild som finns. Sårbarhetsanalysen är en fördjupad analys av företagets funktioner och processer för att identifiera svagheter och möjliga åtgärder för att reducera sårbarheter. Analysen baseras på de identifierade hoten, värderingen av företagets värden, samt säkerhetsnivån (riskaptiten). Sårbarhets-analysen utförs av en samlad grupp medarbetare som har en bred och djup erfarenhet från olika delar av organisationen. Gruppen leds av en person som även står i kontakt med ledningen.

Analysen utförs som en genomgång av företaget, dess funktioner och processer. Som hjälp vid analysen används checklistor. När analysen är utförd bedöms sårbarheten på en tiogradig kvalitativ skala med givna kvantitativa mått mellan 1 och 10. Sårbarheten bedöms efter tid till att företaget har återhämtat sig. Nyckel-komponenterna i denna skala är företagets svaghet och de problem en eventuell antagonistisk aktör kan möta vid ett försök att åstadkomma skada. Bortfallet av funktioner vid eventuell attack finns även med i bedömningen. Denna bedömning med hjälp av den tiogradiga skalan kan sedan vägas samman med hotanalysen och tillgångsvärderingen.

### 3.5.4 Riskbedömning (Risk assessment)

I riskbedömningen vägs sannolikheten (hotanalysen) samman med konsekvensen (tillgångsvärderingen) och sårbarheten till en sammanlagd risk för organisationen. Riskbedömningen kan ske med hjälp av flera olika metoder och tekniker. Ett exempel är att göra en sammanvägning genom att multiplicera de kvantifierade värdena från tillgångsvärderingen, hotanalysen och sårbarhetsanalysen och på så sett få ett numeriskt värde på risken.

För att utföra en riskbedömning finns det ett antal olika metoder att tillgå. Det gemensamma målet för dessa är att identifiera de tillgångar som är utsatta för högst risk, samt utvärdera åtgärder som kan reducera dessa risker.

Manualen använder sig av ett flertal matriser för att väga samman de tidigare delarna i processen till ett sammanlagt värde. Dessa värden används sedan för att inbördes kunna jämföra de olika riskerna och på så sett identifiera de risker som är i störst behov av att reduceras.

### 3.5.5 Åtgärdsförslag (Consider mitigation options)

För att identifiera, välja och implementera de mest lämpade åtgärder som finns tillgängliga, måste generella åtgärdsmål och nyttan av respektive åtgärd utvärderas.

I åtgärdsförslagssteget utförs en mer noggrann identifiering och bedömning av de möjliga åtgärder som kan vidtas för att reducera riskerna. Vid identifieringen och bedömningen av åtgärderna är det viktigt att observera att vissa åtgärder kan påverka även andra risker, genom reduktion (rondering av vakter motverkar många olika risker) eller möjligtvis ökning (trappor från övre plan för utrymning kan ge mer åtkomst för obehöriga eller återinrymning) av dem.

Potentiella åtgärder kan delas in i tre olika grupper:

- Motverka attack.
- Försena attack.
- Motverka konsekvenserna av en attack.

### 3.5.6 Beslut (Decision)

När olika åtgärdsförslag har identifierats måste de granskas utifrån bland annat kostnaden att utföra dem, nyttan av dem, estetiken, samt deras acceptans bland anställda. Granskningen utförs för att de mest lämpade åtgärderna ska kunna väljas och implementeras.

# 4 OLYCKSRELATERADE RISKER

*Kapitlet beskriver hur olycksrelaterade risker hanteras. Den riskhanteringsmodell som ligger till grund för åskådliggörandet av hanteringen av olycksrelaterade risker är den av IEC framtagna, där de olika stegen i riskhanteringsprocessen beskrivs.*

## 4.1 Bakgrundsbeskrivning

Mänsklig verksamhet medför risker. Genom hela vår historia har hantering och kontroll av dessa risker byggt på generationers samlade erfarenheter. Industrialiseringen med införandet av ny teknik ledde till en ny situation. Eftersom det många gånger saknades erfarenheter kombinerades de få olycksdata som fanns med ingenjörsmässiga kalkyler. Detta var första början på dagens riskanalyser. [5]

Under 1800-talet byggdes det svenska järnvägsnätet upp vilket medförde användande av tryckkärl. Denna användning resulterade i många olyckor, vilket i sin tur resulterade i ökad offentlig kontroll. Liknande utveckling kan ses inom flera andra teknikområden. Det typiska vid denna tid var dock att riskhanteringen i första hand kom som en reaktion på inträffade olyckor. [5]

Idag är situationen dock annorlunda. Med en snabb utveckling i tekniken och med större och allt mer komplexa system blir analyserande och förebyggande av risker allt viktigare [5]. En viktig grundsten i att bedöma risker är erfarenheter, men med en snabb utveckling och kort ekonomisk livslängd blir dessa mer sällsynta. Denna tekniska utveckling tillsammans med ökad exponering av olyckor i media ställs det allt högre krav på riskhantering. [30]

Med olycksrelaterade risker menas här tekniska händelser kopplade till säkerhet, hälsa och miljö som uppkommer på grund av mänskliga fel eller utmattning av en komponent.

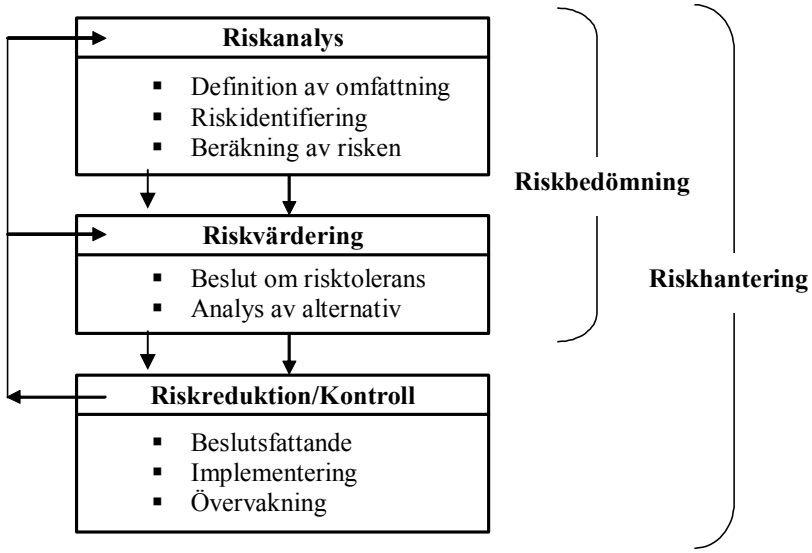
## 4.2 AB Ångpanneföreningen

AB Ångpanneföreningen (ÅF) är en av Sveriges största tekniska konsultfirmor och är aktiva inom flera olika områden. En av deras avdelningar arbetar med brand- och riskfrågor där en av uppgifterna är att utföra riskanalyser samt ge förslag på åtgärder om så behövs. Riskfrågorna som de arbetar med är olycksrelaterade risker som är kopplade till säkerhet, hälsa och miljö. I denna rapport har författarna valt att åskådliggöra AB Ångpanneföreningens arbetssätt med IEC's modell för riskhantering. AB Ångpanneföreningen jobbar inte alltid strikt efter denna men det är den modell som författarna anser bäst representera företagets arbetssätt. Som undantag från IEC's modell utför ÅF ingen värdering och kontroll av åtgärderna utan detta får företaget själva utföra. Beslutet om vilka risker som ska hanteras och vilka åtgärder som ska genomföras tar företaget självt men kan få hjälp av ÅF i besluten. [31]

De som arbetar med riskhantering på AB Ångpanneföreningen är Civilingenjörer inom riskhantering med brandingenjörsexamen som grund eller brandingenjörer. Detta motsvarar en högskoleutbildning på mellan 3,5 och 4,5 år.

## 4.3 Riskhanteringsprocessen enligt IEC

För att ett företag ska kunna hantera sina risker på ett bra sätt krävs det att deras risker identifieras, värderas och hanteras på ett passande sätt. För att det ska ske strukturerat kan arbetet utföras enligt IEC's (International Electrotechnical Commission) modell för riskhantering. I deras modell delas riskhanteringsprocessen in i tre faser: riskanalys, riskvärdering samt riskreduktion. De olika faserna (se Figur 12) sker kontinuerligt som en iterativ process. Innehållet i dessa faser beskrivs nedan.




**Figur 12.** Riskhanteringsmodell, översatt till svenska, enligt IEC [**32**]. Riskhanteringsprocessen delas in i tre steg, där riskerna först analyseras för att sedan värderas och slutligen reduceras det vill säga åtgärder tas fram och implementeras. Processen är iterativ och ska ske kontinuerligt.

### 4.3.1 Riskanalys (Risk analysis)

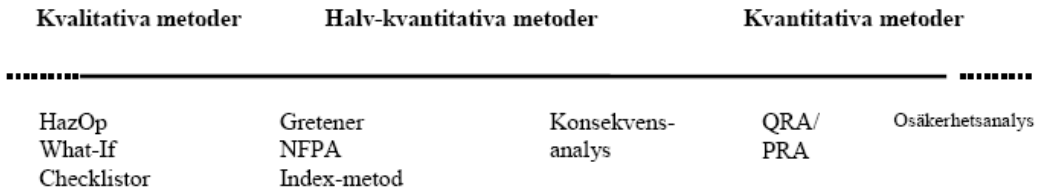
Att utföra en riskanalys innebär en strukturerad genomgång av det valda området eller systemet för att om möjligt identifiera och kartlägga eventuella risker. En viktig grundsten för att identifiera och beräkna risken är tillgången till statistik och tidigare erfarenheter (empiriska skattningar). Dock är tillgången till statistik inte alltid lika god. Om det bara finns lite statistik tillgänglig kan till exempel feldata för ingående komponenter vägas samman eller en bayesianska metoder användas (logiska system). Vid total avsaknad av statistik måste sannolikhetsbedömningen förlitas på subjektiva expertbedömningar (expertbedömningar). För system går det att skilja på ovanstående tre olika sätt att bedöma sannolikheter [30].

Riskanalysen delas in i tre steg (se Figur 12). Det första som sker i en riskanalys är att omfattningen av analysen bestäms. Avgränsningen kan vara i form av vilka riskgrupper eller vilken del av systemet som ska analyseras.

Nästa del i riskanalysen består i att med hjälp av statistik och andra olika metoder identifiera möjliga risker. Metoderna kan vara exempelvis HAZOP, What if?, checklistor eller grovanalys. Valet av metod beror på situationen och bestäms utifrån analysens syfte och mål.

När riskerna är identifierade analyseras de utifrån sannolikhet och konsekvens, det vill säga risken beräknas. Vid beräkningen används även här statistik och andra metoder som hjälp. Analysen kan utföras kvantitativt eller kvalitativt.

De metoder som används i riskanalysen kan vara av många olika slag beroende på omfattnings- och detaljeringsgrad. Ett vanligt sätt att dela in metoderna är efter deras kvantifierbarhet (se Figur 13). De delas då in i grupperna kvalitativa, semi-kvantitativa och kvantitativa.




**Figur 13.** Indelning av riskanalysmetoder efter kvantifierbarhet [**33**].

**Kvalitativa**
Kvalitativa metoder används vid grovanalys men även vid riskidentifieringen och beskriver skeendet av en händelse vid olika förutsättningar. [34]

**Semi-kvanitativa**
De semi-kvantitativa metoderna, eller även kallade graderings- och indexmetoderna, är något mer strukturerade än de kvalitativa och innehåller någon form av mått på sannolikheten och konsekvensen. Måtten behöver inte nödvändigtvis vara siffermått men de ger rangordningsmöjligheter. [34]

**Kvantitativa**
De kvantitativa metoderna är de metoder som ger ett kvantitativt värde på konsekvensen och sannolikheten. Till gruppen hör även de metoder som bara beräknar konsekvensen av en händelse. Denna grupp kallas även deterministiska eftersom de resulterar i ett fast värde. Det vanligaste är dock att konsekvensen och sannolikheten vägs samman till ett riskmått. [34]

**Riskmått**
Tre vanliga sätt att beskriva en risk är som riskindex, individrisk samt samhällsrisk. Riskindex (semi-kvantitativ metod) är en siffra eller tabell för en enkel presentation. Individrisken beskriver risken för en individ att befinna sig inom ett riskområde. Det presenteras ofta som riskkonturer som visar den förväntade frekvensen av en händelse som orsakar en viss nivå av skada i ett specifikt område. Samhällsrisk är risken för en grupp människor inom riskområdet. Samhällsrisken beskrivs ofta i form av en FN-kurva som visar den ackumulerade frekvensen för olyckor som funktion av antalet omkomna. [33]

### 4.3.2 Riskvärdering (Risk evaluation)

För att kunna hantera en risk måste ett företag bestämma sig för i vilken omfattning det är villigt att acceptera risker, det vill säga bestämma sig för sin riskaptit. Detta Riskvärderingen är sedan en jämförelse av riskerna gentemot företagets riskaptit. För de risker som ligger över riskaptiten måste åtgärder utföras för att sänka dem till acceptabel nivå. Framtagandet av möjliga åtgärder kan ske på olika sätt, till exempel genom brainstorming och erfarenheter. När de olika åtgärdsförslagen är framtagna följer en svår uppgift i att värdera dem mot varandra, för att välja det bästa för företaget. Som hjälp vid värderingen används olika beslutskriterier: [30]

- Teknologibaserade kriterier
  - ”Använd bästa möjliga teknik”
- Rättighetsbaserade kriterier
  - Nollriskansats
  - Begränsa risken så den inte överstiger $10^{-x}$
- Nyttobaserade kriterier
  - Kostnad-nytta-analys
  - Kostnad-effekt-analys
  - Multiattributiv nyttoteori
- Hybrid-kriterier
  - En blandning av ovanstående kriterier

**Teknologibaserade kriterier**
Teknologibaserade kriterier innebär att den bästa möjliga tekniken alltid används utan hänsynstagande till åtgärdens kostnad. [30]

**Rättighetsbaserade kriterier**
Nollriskansats innebär att risken inte accepteras, utan ska i stället elimineras helt på sikt, oavsett kostnad.

Ett fast värde som acceptanskriterium bestäms på förhand och medför att alla risker som är högre ska åtgärdas. [30]

**Nyttobaserade kriterier**
Vid nyttobaserade kriterier vägs fördelarna av en åtgärd mot nackdelarna. Åtgärden antas endast om fördelarna överstiger nackdelarna.

Kostnad-nytta-analysen innebär att fördelarna och nackdelarna med åtgärden värderas i monetära medel, så de kan jämföras med varandra.

Kostnad-effekt-analysen innebär att företaget sätter upp mål för hur mycket risken ska minska med under en begränsad tidsperiod. Sedan gäller det att uppnå detta mål till så låga kostnader som möjligt.

Multiattributiv nyttoteori innebär att företaget sätter upp ett övergripande mål som bryts ner i undermål och delmål. Dessa måls uppfyllelse mäts med hjälp av olika attribut, där fördelarna och nackdelarna spaltas upp. Den åtgärd där fördelarna överväger nackdelarna mest väljs sedan. [30]

**Val av kriterie**
Mattson menar att valet av kriterie ska göras utifrån fyra olika värderingar. Dessa värderingar är [30]:

- I allmänhet avspegla samhällsmedborgarens preferenser.
- Kunna redovisas offentligt och då i huvuddrag förstås av majoriteten av samhällsmedborgarna.
- Ha hög validitet (det som ska mätas mäts) och reliabilitet (samma resultat ska fås vid upprepade mätningar).
- Vara operationell. Med det menar han att beslutsfattarna/utredarna bör ges en modell som avspeglar hur olika åtgärder påverkar måluppfyllelsen.

### 4.3.3 Riskreduktion/kontroll (Risk reduction/control)

Det sista steget i IEC's modell för riskhantering innebär att de identifierade riskerna hanteras och kontrolleras, det vill säga att åtgärderna beslutas och genomförs. Åtgärderna kan exempelvis delas in i fyra olika kategorier enligt nedan [35].

**Riskreducerande**
För att sänka en risk så att den kommer under företagets riskaptit, reduceras den genom olika åtgärder. Eftersom en risk är uppbyggd av sannolikhet och konsekvens är det båda eller någon av dessa som reduceras.

**Riskundvikande**
Om kostnaderna för åtgärderna anses för höga samtidigt som risken anses för hög för att kunna acceptera kan företaget tvingas undvika risken genom att sluta med aktiviteterna som ger upphov till den.

**Riskacceptans**
Risker som ligger inom företagets riskaptit accepteras som de är. Det kan även gälla risker där kostnaden för en åtgärd anses överstiga nyttan.

**Riskdelande**
En åtgärd för att sänka en risk är att flytta eller dela bitar av eller hela risken. Ett vanligt sätt att dela en risk är till exempel genom att försäkra sig mot risken.

# 5 DRIVKRAFTER

*I kapitlet sker en beskrivning av de motiv som driver ett företag att arbeta med riskhantering.*

En verksamhet utför riskhantering av många olika anledningar, så kallade drivkrafter. Drivkrafterna kan vara enligt nedan.

## 5.1 Etik och moral

Verksamheter vill av etiska skäl undvika eller minska de risker som samhället utsätts för. [11]

## 5.2 Ekonomi

Verksamheter ser en vinning i att utföra riskhantering för att sänka sina kostnader och därmed öka vinsten. [11]

## 5.3 Kunder och leverantörer

Kunder och leverantörer ställer krav på utförande av riskanalyser för att de ska kunna vara säkra på att de får eller får leverera sina varor. [11]

## 5.4 Goodwill

Verksamheter vill undvika av risker som kan försätta organisationen i dålig dager, samt om möjligt få positiv publicitet genom att sköta sina risker på ett bra sätt. [11]

## 5.5 Främja arbetsklimatet genom intern trygghet

Uttrycket ”glada medarbetare är goda medarbetare” beskriver verksamheters vinning i att främja arbetsklimatet genom intern trygghet och kan även vara ett incitament till riskhantering.

## 5.6 Försäkringsbolag

Försäkringsbolagen ställer krav på företagen att de ska hantera sina risker för att de ska försäkra dem. Företaget kan sänka sina försäkringspremier med hjälp av bra riskhanteringsarbete.

## 5.7 Lagstiftning

Det ställs i ökande omfattning krav på verksamheter att utföra riskhantering, i form av lagar och förordningar. Kraven som ställs beror på verksamhetens art och vissa organisationer kan beröras av många olika krav [11]. För att få en bättre uppfattning om hur många lagstiftningar med tillhörande föreskrifter det finns som rör säkerhet, hälsa och miljö, utarbetade Lars-Olof Carlsson och Hans Hoppe en sammanställning 1999. Sammanställningen är inte komplett men ger en uppfattning om antalet lagar som ställer krav. Nedan ges några exempel på lagar som ställer krav inom de olika områdena.

### 5.7.1 Olycksrelaterade risker

Genom Sveriges medlemskap i EU har Sverige förbundit sig att överföra EG-direktiv till svenska regler. Seveso II-direktivet är ett så kallat minimidirektiv för att förebygga och begränsa följderna av allvarliga olyckshändelser där farliga ämnen

ingår. Seveso II-direktivet infördes i svensk rätt genom i första hand Sevesolagen (SFS 1999:381) med tillhörande förordning (SFS 1999:382), men även genom Arbetsmiljöverkets föreskrifter (Förebyggande av allvarliga kemikalieolyckor, AFS 1999:5), samt föreskrifter från Räddningsverket (SRVFS 1999:5).

Under arbetsmiljölagen (SFS 1977:1160) med tillhörande föreskrifter hamnar frågor om organisatoriska system för att förebygga och begränsa allvarliga kemikalieolyckor och frågor om riskbedömningar, samt riskanalyser. Teknisk processäkerhet med tillhörande regelverk och intern plan för räddningsinsatser är andra tillsynsområden. Meningen med lagstiftningen är att arbetsgivaren med dokumenterade rutiner och genom handling, när som helst ska kunna visa att han vidtagit alla de åtgärder som krävs i föreskrifterna.

Andra exempel på lagar som innehåller krav på riskanalyser är plan och bygglagen (SFS 1987:10), miljöbalken (SFS 1998:808), samt lag (SFS 2003:778) om skydd mot olyckor. Samtliga dessa lagar har tyngdpunkten på olycksrelaterade risker.

### 5.7.2 Antagonistiska risker

Inom området för antagonistiska risker är lagstiftningen under stark utveckling. Dagens lagstiftning, säkerhetsskyddslagen (SFS 1996:627), uttrycker att ”*det säkerhetsskydd ska finnas som behövs med hänsyn till verksamhetens art, omfattning och övriga omständigheter*”. Lagen är avsedd att skydda ”rikets säkerhet” och tar därmed ringa hänsyn till enskilda individers säkerhet.

Med säkerhetsskydd avses i lagstiftningen:

- Skydd mot spionerі, sabotage och andra brott som kan hota rikets säkerhet.
- Skydd i andra fall av uppgifter som omfattas av sekretess enligt sekretesslagen (1980:100) och som rör rikets säkerhet.
- Skydd mot terroristbrott enligt 2§ lagen (2003:148) om straff för terroristbrott (terrorism), även om brotten inte hotar rikets säkerhet.

Säkerhetsskyddet ska enligt säkerhetsskyddslagen förebygga:

- Att uppgifter som omfattas av sekretess och som rör rikets säkerhet obehörigen röjs, ändras eller förstörs (informationssäkerhet).
- Att obehöriga får tillträde till platser där de kan få tillgång till uppgifter som avses i punkten ovan eller där verksamhet som har betydelse för rikets säkerhet bedrivs (tillträdesbegränsning).
- Att personer som inte är pålitliga från säkerhetssynpunkt deltar i verksamhet som har betydelse för rikets säkerhet (säkerhetsprövning).
- Säkerhetsskyddet ska även i övrigt förebygga terrorism.

Regeringen planerar att lägga fram en ny antiterroristlag under hösten 2005. Där tas bland annat det känsliga förslaget upp att militären ska få vidgade funktioner under polisens ledning i fredstida kriser. [36]

# 6 LEDNING OCH STYRNING AV RISKHANTERING PÅ FÖRETAG

*Detta kapitel beskriver ledning och styrning av riskhantering i form av Enterprise Risk Management (ERM). Som ramverk för detta arbete beskrivs av COSO's ramverk för ERM och dess olika beståndsdelar. Kapitlet är en sammanfattning av COSO's ramverk för ERM [10].*

## 6.1 Vad är ERM och varför arbeta med det?

ERM är en process i ett företag för att kunna identifiera och analysera risker utifrån ett integrerat företagsbrett perspektiv [37]. Många organisationer arbetar redan med riskhantering på flera nivåer i företaget, men det speciella med ERM är att riskerna förs upp till ledningsnivå och studeras uppifrån som en del av företagets totala riskprofil [37]. Det ger företagen en mer övergripande syn på sin riskbild, vilket leder till att de lättare kan identifiera sina nyckelrisker [38, 39].

Fördelen med att arbeta med ERM är att det ger förbättrad förmåga genom bland annat förbättrad riskrespons och lättare att identifiera och hantera verksamhets-täckande risker. ERM ger inte en riskfri verksamhet men möjliggör för ledningen att verka i omgivningar med fler risker. Det är viktigt att se ERM som en process i verksamheten och inte som en isolerad del. Arbetet ska penetrera verksamhetens alla aktiviteter och är som mest effektivt när det blir en väsentlig del av infrastrukturen. Ett väl fungerande arbete med ERM kan ge ledningen en försäkran på att företagets mål uppfylls.

Fundamentala begrepp med ERM är enligt COSO's ramverk [10]:

- Det är en integrerad process i företaget och inte något som sker som en enstaka händelse.
- Arbetet berör alla inom hela organisationen på alla nivåer.
- Appliceringen sker genom att sätta strategier.
- Syftet med ERM är att identifiera händelser som potentiellt kan påverka verksamheten samt hantera de risker som faller inom företagets riskaptit.
- Ger ledningen en rimlig försäkran om att företaget inte utsätts för något oväntat.
- Den är styrd mot att företagets mål ska uppfyllas.

## 6.2 COSO's ramverk för ERM

Rapporten är utförd med The Committee of Organizations of the Treadway Commissions (COSO) ramverk för Enterprise Risk Management (ERM) som grund. Anledningen till att COSO's ramverk används i denna rapport beror på att en ökande andel företag börjar införa ERM i sin organisation [39, 40]. Ökningen beror till stor del på tillkomsten av Sarbanes-Oxley Act 2002, som är ett regelverk för börsnoterade bolag på NYSE och NASDAQ i USA. Syftet med regelverket är att minska risken för felaktig rapportering och bedrägerier, samt att medföra en bättre insyn i företags finansiella rapportering och ställning [41]. För Europas vidkommande är detta intressant då det finns motsvarande lagstiftning i form av Turnball och Kontrag. För att uppfylla det amerikanska lagkravet är COSO's ramverk för intern kontroll allmänt accepterat [42]. Deras ramverk för ERM är i sin tur framtaget för att bredda deras

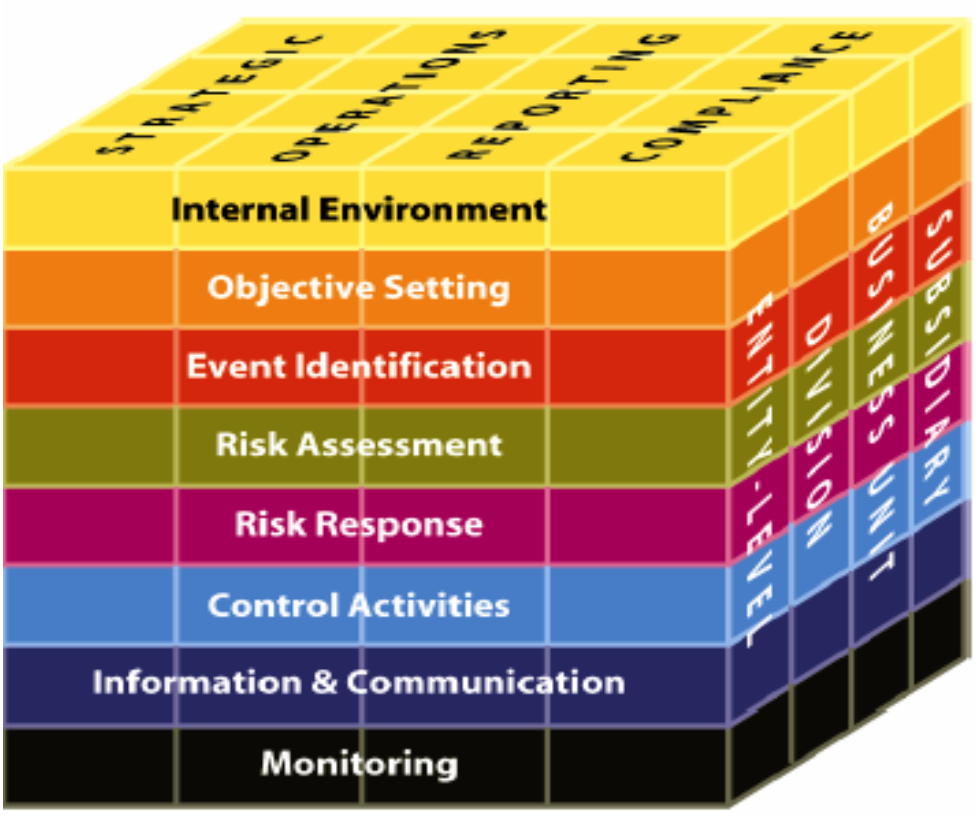
tidigare. Ramverket ska utöver det att uppfylla lagkravet på intern kontroll även ge företagen en mer heltäckande riskhanteringsprocess. Med ett ramverk för ERM försöker COSO skapa en allmän terminologi och en klarare definition av ERM [43]. COSO är en organisation som består av ledande företag i USA.

COSO's ramverk för ERM är framtaget för att komplettera deras tidigare ramverk för intern kontroll och ge företagen en mer robust och omfattande process för riskhantering på ett bredare plan. Ramverket fungerar som ett ledningssystem för att arbeta med riskhantering. Det är ett övergripande ledningssystem som samordnar företagets riskhanteringsarbete med tillhörande rutiner och mindre ledningssystem.

I COSO's ramverk definieras ERM som:

*"Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."* [10]

Ramverket delar in arbetet i tre huvuddelar: åtta element (se kapitel 6.2.1), olika nivåer i företaget, samt fyra kategorier (se kapitel 6.2.2). Indelningen visualiseras bäst i form av COSO's kub (se Figur 14).




**Figur 14.** COSO's kub [10]. Kuben är en visualisering av hur COSO's tre huvuddelar är sammanlänkande. Arbetet med de olika elementen och strategierna ska ske på alla nivåer inom ett företag.

### 6.2.1 Element

Ramverket är indelat i åtta element (se framsidan av Figur 14):

**Inre miljö (Internal environment)**
Den inre miljön omfattar organisationen, och lägger grunden för hur risker uppfattas och hanteras inom verksamheten. Den påverkar hur strategier och mål sätts upp, hur affärsaktiviteter struktureras, hur risker identifieras, analyseras och behandlas. Detta första steg påverkar resterande element i processen. Som en del av den inre miljön sätter ledningen upp en riskhanteringsfilosofi, bestämmer företagets riskaptit och skapar förutsättning för en säkerhetskultur. Den inre miljön innefattar även organisationens etiska värderingar, kompetens och utveckling av personal, ledningens ledarstil samt hur de tilldelar befogenheter och ansvar.

Riskhanteringsfilosofin kommuniceras ut till personalen via policys och andra kommunikationskanaler. Ett företags riskhanteringsfilosofi är viktig eftersom den reflekterar vad företaget vill åstadkomma med sin riskhanteringsprocess och påverkar hur elementen kommer att efterlevas. För att arbetet med att hantera risker inom företaget ska bli bästa möjliga måste de ha en riskhanteringsfilosofi som alla anställda förstår och efterlever. Det är även viktigt att ledningens filosofi stämmer överens med företagets och att de agerar efter denna. Deras filosofi återspeglas genom hela organisationen.

Ett företags riskaptit är direkt knuten till deras strategier. Med hjälp av att sätta strategier inom ERM har ledningen möjlighet att välja strategier som är i linje med företagets riskaptit.

**Målsättning (Objective setting)**
Inom företagets vision sätter ledningen upp strategiska mål som i sin tur delas upp i delmål genom organisationen som är i linje med företagets strategi. Det är viktigt att sätta upp mål innan det går att avgöra vad som påverkar att de uppnås. ERM försäkrar att ledningen har en process för att sätta upp mål och att målen är i linje med företagets vision. Uppsättandet av mål som stödjer och är i linje med valda strategier är kritiskt för att lyckas. För att underlätta att målen uppfylls delas de upp i fyra kategorier. Uppdelningen av företagets mål ger ledningen en möjlighet att fokusera separata delar i ERM. De fyra kategorierna är:

- Strategi (Strategic)
- Handling (Operations)
- Rapportering (Reporting)
- Eftergivenhet - Efterlevnad av lagar och regler (Compliance)

Det är viktigt att få all personal att förstå organisationens mål. För att kunna uppnå organisationens mål måste varje individ i organisationen veta hur deras handlingar interagerar med och påverkar uppfyllandet av målen.

I strävan efter att uppnå de strategiska målen görs bedömningar av alternativa strategier. Vid denna bedömning identifierar ledningen risker som förknippas med de strategiska valen samt bedömer innebörden av riskerna. När organisationen sätter upp mål kan de identifiera faktorer som bedömer hur väl de lyckas i sitt arbete. Faktorerna är nyckelelement som måste gå rätt för att målen ska uppnås.

Organisationen får genom målsättningen även chans att identifiera mätbara kriterier, med fokus på faktorerna, för att mäta prestationer.

Pålitlig rapportering förser ledningen med exakt, fullständig och lämplig information. Det ger ledningen underlag vid beslutandet och övervakandet av organisationens aktiviteter och prestationer.

För att sätta upp direkt uppföljningsbara mål rekommenderas det att använda sig av de så kallade SMART-kriterierna som vägledning [44, 45]. Det är ett antal kriterier som bör beaktas vid målsättning.

- Specifik – det ska tydligt anges vad som vill uppnås.
- Mätbar - de ska vara möjliga att följa upp med hjälp av resultatindikatorer, nyckeltal eller liknande.
- Accepterat - de ska vara accepterade och uppfattas som relevanta av dem som ska genomföra den aktuella verksamheten.
- Realistisk – de ska vara möjliga att uppnå.
- Tidssatt – tidpunkten då målen ska vara uppnådda ska anges.

**Händelseidentifiering (Event identification)**
Interna och externa händelser som kan påverka uppfyllelsen av verksamhetens mål måste identifieras och delas in efter risker och möjligheter. I COSO's ramverk ses händelser med positiva konsekvenser som möjligheter och händelser med negativa konsekvenser som risker. Som en del i händelseidentifieringen beaktar ledningen yttre och inre faktorer som kan inverka på en händelse. Med yttre faktorer menas ekonomiska, affärer, natur, politiska, sociala och tekniska. Inre faktorer inkluderar infrastruktur, personal, process, och teknik. Tekniker för händelseidentifiering behandlar både framtida och tidigare händelser. Genom att samla händelserna både horisontellt och vertikalt genom organisationen kan ledningen skapa sig en bättre förståelse för relationen mellan dem, vilket ger nyttig informationsbas inför riskbedömningen.

| Event Categories | | |
|---|---|---|
| **Internal Factors** | **External Factors** | |
| **Infrastructure**<br>• Availability of assets<br>• Capability of assets<br>• Access to capital<br>• Complexity<br>• Mergers/ acquisitions<br>**Personnel**<br>• Employee capability<br>• Fraudulent activity<br>• Health and safety<br>• Judgment<br>• Malfeasance<br>• Security practices<br>• Sales practices<br>**Process**<br>• Capacity<br>• Design<br>• Execution<br>• Suppliers/ dependencies<br>**Technology**<br>• Data<br>– Acquisition<br>– Maintenance<br>– Distribution<br>– Confidentiality<br>– Integrity<br>• Data and system availability<br>• Capacity<br>• System<br>– Selection<br>– Development<br>– Deployment<br>– Reliability | **Economic**<br>• Capital availability<br>• -Credit<br>– Issuance<br>– Default<br>– Concentration<br>• Liquidity<br>– Market<br>– Funding<br>– Cash flow<br>• Market<br>– Commodity prices<br>– Interest rate<br>– Unemployment<br>– Indices<br>– Exchange rate<br>– Equity valuation<br>– Real estate values<br>**Business**<br>• Brand/ trademark<br>• Competition<br>• Consumer behavior<br>• Counterparty<br>• Fraud<br>• Industry standards<br>• Ownership structure<br>• Publicity<br>• Product relevance | **Technological**<br>• Electronic commerce<br>• External data<br>• Emerging technology<br>**Natural Environment**<br>• Biodiversity<br>• Emissions, effluents and waste<br>• Energy<br>• Fire<br>• Natural disaster (earthquake, flood, etc.)<br>• Sustainable development<br>• Transport<br>• Water<br>**Political**<br>• Governmental changes<br>• Legislation<br>• Public policy<br>• Regulation<br>**Social**<br>• Demographics<br>• Corporate citizenship<br>• Environmental stewardship<br>• Privacy<br>• |

**Figur 15.** Kategorier vid händelseidentifiering [10]. Som hjälp vid identifieringen av potentiella risker används en checklista med olika händelsekategorier.

Identifieringen sker bland annat med hjälp av en genomgång av verksamheten i grupp. Gruppen består av ledning, personal från olika delar av verksamheten och externa aktörer. Genom att kombinera erfarenhet och kunskap från olika delar av organisationen kan viktiga potentiella händelser identifieras som annars kunde ha missats. Till sin hjälp använder sig organisationen av olika händelsekategorier vid genomgången för att lättare kunna identifiera potentiella händelser (se Figur 15).

### Riskbedömning (Risk assessment)

Vid riskbedömningen analyseras hur en potentiell händelse kan påverka företagets mål. Analysen sker med avseende på sannolikhet och konsekvens som bas. När risken beskrivs görs det genom att beskriva förväntade värdet eller ett ”worst-case” scenario. Det är viktigt att undersöka hur olika händelser interagerar eftersom det kan få mycket större konsekvenser än om de bara ses som enstaka händelser. Riskbedömningen utförs för både ej hanterade och kvarvarande risker som är relevanta för verksamheten och dess aktiviteter.

Ett företags riskbedömningsmetoder består normalt av en kombination av både kvalitativa och kvantitativa tekniker. Kvantitativa metoder ger möjligtvis mer precision och används på mer komplexa och sofistikerade aktiviteter som supplement till kvalitativa metoder. Valet av metod bör spegla behovet av precision och kulturen i företaget. Precis som vid händelseidentifieringen sker den kvalitativa uppskattningen av sannolikhet och konsekvens i grupp. Gruppen består även här av ledning, personal med erfarenhet från olika delar av organisationen och externa aktörer.

När en händelse analyseras kan data från observationer av forna händelser användas som input. Företag som för statistik över händelser inom verksamheten underlättar för en mer noggrann bedömning. För att förbättra analysen ytterliggare kan extern data användas. Internt framtagen data baserad på verksamhetens egna erfarenheter kan dock reflektera mindre subjektiva uppskattningar än externt insamlad data. Detta eftersom internt framtagen data är verksamhetsspecifik.

Vid en riskbedömning finns det vanligtvis en rad olika resultat kopplade till den potentiella händelsen vilket ledningen sedan beaktar vid riskresponsen.

**Riskrespons (Risk response)**
Ledningen tar beslut om vilken åtgärd som ska utföras så att riskerna sänks eller höjs till företagets riskaptit. Åtgärderna utvärderas efter till exempel kostnad-nytta, återstående risk, om de påverkar andra risker och åtgärdens design. Effektiv ERM kräver att riskerna reduceras så att de kommer innanför företagets riskaptit. De olika åtgärderna delas in i olika kategorier:

- Riskreducering – åtgärder utförs för att sänka sannolikheten eller konsekvensen av en potentiell händelse.
- Riskundvikande – åtgärder tas för att sluta med aktiviteterna som ger upphov till risken.
- Riskaccepterande – inga åtgärder utförs.
- Riskdelande – åtgärder utförs för att reducera sannolikheten eller konsekvensen genom att flytta eller dela delar av risken. Vanligt är att till exempel försäkra produkter.

För att ge ledningen tillräckligt underlag för val av åtgärder identifieras potentiella åtgärder inom alla kategorierna. Efter beslut om åtgärd har tagits görs en implementeringsplan samt riskerna analyseras igen för att undersöka om väntat resultat uppnåtts.

Vid bedömningen av risk ser ledningen dem från antingen en företagsbred syn eller ett portföljperspektiv. Med en övergripande syn över riskerna kan ledningen avgöra om de olika enheternas riskprofiler stämmer överens med dess och företagets riskaptit, relativt till målen.

**Kontrollaktiviteter (Control activities)**
Policys och rutiner skapas och implementeras för att försäkra sig om att åtgärderna som valts i riskresponsen utförs ordentligt och att de har den väntade effekten. Kontrollaktiviteter är en del av processen för att uppnå företagets mål. Vid framtagandet av kontrollaktiviteter är det viktigt att veta hur de förhåller sig till varandra. En kontrollaktivitet kan kontrollera flera olika risker men det kan också behövas flera aktiviteter för att kontrollera en risk. Det finns många olika typer av kontrollaktiviteter som förebyggande, manuella, dator och ledningskontroller.

**Information och kommunikation (Information and communication)**
Relevant information måste identifieras och kommuniceras ut på rätt sätt och i rätt tid för att möjliggöra för anställda att utföra sina uppgifter. Information behövs på alla nivåer för att en organisation ska kunna identifiera, bedöma och åtgärda risker och uppfylla dess mål. Den kan vara både intern och extern, det vill säga den kan komma från de egna leden samt från kunder och leverantörer.

Kommunikation ska väcka medvetenhet om vikten och relevansen av effektiv ERM, kommunicera företagets riskaptit och risktolerans, implementera och backa upp allmänt riskspråk, och underrätta personalen om deras roller och ansvar när det gäller påverka och stödja elementen i ERM. Kommunikationskanaler ska försäkra att personal kan kommunicera riskbaserad information genom organisationen. De ska kunna föra information både uppåt och direkt i sidled till andra avdelningar för att få ett effektivt riskarbete.

Den information som går ut till personalen måste komma i rätt omfattning för att de ska kunna ta den till sig. Det är lätt att alldeles för mycket information kommuniceras ut. Ledningen måste även tänka på att sättet som informationen levereras på påverkar hur riskerna uppfattas.

För att stödja effektiv ERM kan företaget samla och använda sig av historiska och nutida data. Historiska data möjliggör för företaget att skaffa sig insyn i hur de fungerar under olika förhållanden och kan på så sett ge tidiga varningar vid potentiella händelser. Historiska data kan även användas vid bedömning av sannolikhet av potentiella händelser eller konsekvens på företagets mål.

För att upprätthålla bra information så att så många risker som möjligt identifieras bör punkterna nedan beaktas. [10]

- Passande – informationen ska ha rätt detaljnivå.
- Läglig – informationen ska komma när den behövs.
- Aktuell – informationen ska vara den senast tillgängliga
- Precis – informationen ska stämma.
- Tillgänglig – informationen ska kunna nås av dem som behöver den.

**Övervakande (Monitoring)**
Övervakningen sker för att ett företags ERM förändras över tiden. Åtgärder och kontrollaktiviteter kan åldras och bli mindre effektiva, företagets mål kan förändras med mera. Vid sådana förändringar måste ledningen veta om det för att kunna revidera systemet och fortsatt vara effektiva.

Övervakningen av ERM är en process för att kunna bedöma närvaron och funktionen av dess element samt kvaliteten på prestationen. Det är en process som sker både kontinuerligt och som separata utvärderingar och är till för att identifiera problem så de kan åtgärdas. Kontinuerlig övervakning är inbyggt i de normala aktiviteterna på ett företag och ger vanligtvis viktig feedback effektiviteten av ERM. Dock är en separat utvärdering nyttig för att kunna fokusera på ERM elementen.

Det finns en mängd olika utvärderingsmetoder tillgängliga som till exempel checklistor, frågeformulär och flödesscheman. Som en del av företagens utvärderingsmetod jämför vissa sin process med andra företags.

### 6.2.2 Kategorier

COSO's ramverk är utvecklat som ett övergripande ramverk som ska kunna hantera alla typer av risker på ett företag. Företagets risker delas i ramverket in i fyra olika kategorier. Kategorierna är:

- Strategi (Strategic) – strategiska risker är risker som har med förändringar i företagets omvärld som till exempel förändrat kundunderlag, konkurrens, räntor mm.
- Handling (Operations) – risker som är kopplade till företagets agerande, det vill säga i deras verksamhet. Risker som har med exempelvis styrelsens sammansättning, informationssystem, ekonomiska system och företagskultur att göra.
- Rapportering (Reporting) – hänför sig till rapporteringen inom verksamheten. Rapporteringen är viktig för att riskhanteringen ska fungera över huvud taget.
- Eftergivenhet (Compliance) – Efterlevnad av lagar och regler. Det ställs många olika lagar på ett företag. Lagkravet beror på typ av verksamhet med mera. COSO's ramverk är framtaget för att uppfylla lagkravet på inre kontroll. Eftergivenhet är de risker som måste hanteras enligt lag.

Olycksrelaterade och antagonistiska risker utgör, beroende på verksamhet, ofta endast en liten del av ett företags riskbild. I de fall dessa risker inte har tillräcklig ekonomisk påverkan, kan följden bli att de bara analyseras och hanteras i enlighet med samhällets lagkrav.

Olycksrelaterade och antagonistiska risker hamnar normalt mest under kategorin eftergivenhet. Viss del av dem kan dock hamna under handling. Eftersom båda risktyperna har att göra med säkerhet, hälsa och miljö kan det dock finnas ekonomisk vinning i att hantera dem mer än vad som krävs enligt lag. Ett säkert företag där personalen trivs och känner sig trygga kan återgälda sig i mindre personalomsättning, sjukskrivningar mm. Detta är saker som kan vara kostsamma för ett företag.

### 6.2.3 Nivåer

Ramverket är konstruerat för att genomsyra hela organisationen. Riskhantering ska fungera i organisationens alla nivåer och inte bara ske på ledningsnivå. Detta för att på ett bra sätt kunna identifiera och hantera företagets alla tänkbara risker.

# 7 MÖJLIGHETER OCH PROBLEM MED INTEGRATION

*Kapitlet är en analys där författarna själva resonerar kring möjligheter och problem med en integration av hanteringen av olycksrelaterade och antagonistiska risker. Analysen är utförd med utgångspunkt från en systematisk jämförelse av fyra olika komponenter; riskhanteringsprocessen, drivkrafter, utbildning och kompetenser, samt ledning och styrning av riskhantering med hjälp av COSO's ramverk för ERM.*

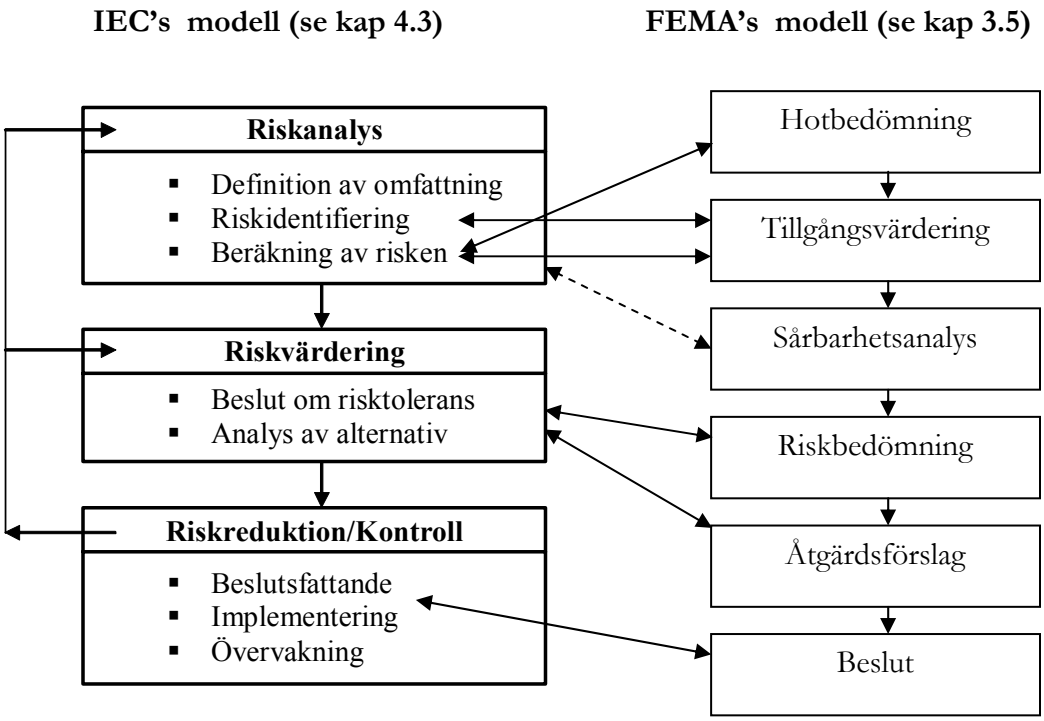
Eftersom olycksrelaterade och antagonistiska risker på många sätt handlar om samma typ av risker borde det enligt författarna finnas möjligheter till integration inom ett eller flera steg i riskhanteringsprocessen. Skillnaderna i den initierande händelsen orsakar dock stora problem när det gäller integration av hanteringen av riskerna. Möjligheterna och problemen med en eventuell integration kommer att belysas i denna analys.

Analysen har utförts med utgångspunkt i ett antal komponenter för att studera möjligheter och problem med en integration av hanteringen av antagonistiska risker. Utförandet bygger på en systematisk genomgång där områdena jämförs med varandra, komponent för komponent. Vid genomgången har författarna identifierat likheter och skillnader mellan områdena och sedan resonerat kring vilka möjligheter och problem som dessa likheter och skillnader orsakar vid en integration av arbetet med olycksrelaterade risker. Komponenter som det har tagits hänsyn till är riskhanteringsprocessen, drivkrafter, utbildning och kompetenser, samt ledning och styrning av riskhantering med hjälp av COSO's ramverk för ERM. För noggrannare beskrivning av valet av komponenter och tillvägagångssättet vid analysen, se kapitel 2.1.2 och 2.1.3.

## 7.1 Riskhanteringsprocessen

Riskhanteringsprocessen för de olika områdena har jämförts med varandra där författarna undersökt vilka steg som finns inom ena området för att sedan se om det finns motsvarande steg inom det andra. Kring dessa motsvarigheter har det sedan förts ett resonemang med avseende på hur dessa steg utförs inom respektive område, för att författarna skulle kunna uttala sig om vilka delar de anser är möjliga att samordna och vilka delar som inte anses vara möjliga att samordna.

Kopplingen mellan de olika stegen i IEC's modell för riskhantering och i FEMA's modell för hantering av antagonistiska risker finns beskrivet schematiskt i Figur 16.




**Figur 16.** Figuren är ett försök till att schematiskt visa hur stegen i IEC's modell för riskhantering motsvarar stegen i FEMA's modell för hantering av antagonistiska risker. Observera att figuren inte gör anspråk på att vara komplett, eftersom gränserna och stegen i processerna på olika sätt är flytande och går in i varandra. De båda modellerna är svenska översättningar av orginalutförandet.

### 7.1.1 Riskidentifiering

*Riskidentifieringen* i IEC's modell för riskhantering motsvaras av *tillgångsvärdering* och *sårbarhetsanalys* i FEMA's modell för hantering av antagonistiska risker.

Vid riskidentifieringen i IEC's modell och tillgångsvärderingen i FEMA's modell utförs arbetet som en genomgång av valt system inom både antagonistiska risker och olycksrelaterade risker. Identifieringen utförs i form av brainstorming i en grupp bestående av anställda från den egna organisationen som känner till systemet där genomgången sker.

Tillvägagångssättet, det vill säga genomgången av systemet i grupp, är detsamma för båda riskområdena, men tankesättet vid genomgången skiljer sig. När det gäller antagonistiska risker, enligt FEMA's modell, sker identifieringen genom att företagets alla värden, som till exempel personal och viktiga maskiner, identifieras. Därefter utförs en sårbarhetsanalys av dessa värden, det vill säga det undersöks hur väl skyddade värdena är, vilka svagheter skyddet har och hur en aktör skulle kunna komma åt värdena.

För olyckrelaterade risker, enligt IEC's modell, är tankesättet mer inställt på vad som kan fallera och orsaka skada. De medverkande använder sig även av de erfarenheter de besitter, samt statistik inom området. Vid identifieringen finns det ett flertal olika metoder som är allmänt vedertagna, där motsvarigheter inom området för antagonistiska risker saknas.

Vid en jämförelse mellan de båda modellerna kan en stor skillnad genast identifieras. I IEC's modell utförs en riskanalys där motsvarande delsteg även finns i FEMA's

modell. Dock utförs det i FEMA's modell även en sårbarhetsanalys. En stor skillnad mellan en riskanalys och en sårbarhetsanalys är skillnaden i tankesättet. Skillnaden är att en riskanalys har sin utgångspunkt i en riskkälla och sedan tar hänsyn till vad som kan hända, medan en sårbarhetsanalys tar hänsyn till det skyddsvärda och sedan till vad som kan hota det [12].

En integrerad riskidentifiering, enligt IEC'smodell, och tillgångsvärdering, enligt FEMA's modell, med undantag från sårbarhetsanalysen, medför problem eftersom det finns stora olikheter i vad det är som identifieras. Kvalitativa metoder, till exempel HazOp, What If? och checklistor, som är utvecklade för olyckrelaterade risker används främst för att identifiera risker och utifrån dem vad som kan gå fel [34]. Detta skiljer sig från FEMA's modell för hantering av antagonistiska risker, där det är värden som behöver skyddas som identifieras. Eftersom det inte är samma sak som eftersökts anses det vara svårt att utnyttja samma metoder. Det skilda tankesättet medför att en integration av riskidentifieringen inte anses vara möjlig, eftersom det skiljer för mycket. Dock anser författarna att riskidentifieringen och tillgångsvärderingen med fördel kan utföras samtidigt, så att de kan dra nytta av varandra med utbyte av identifierade risker, för att på så sätt få en mer heltäckande riskidentifiering eller tillgångsvärdering.

En samtidig riskidentifiering och tillgångsvärdering ses även, av författarna, som en styrka inför sårbarhetsanalysen för de antagonistiska riskerna, eftersom det inte nödvändigtvis är de mest värdefulla resurserna i ett företag som är viktigast att analysera. Företeelser som kan orsaka stor skada, men som inte är speciellt värdefulla för företaget, kan förbises i tillgångsvärderingen medan de lättare identifieras i risk-identifieringen.

### 7.1.2 Beräkning av risk

Beräkning av risk sker på likartat sätt för både antagonistiska och olycksrelaterade risker i IEC's respektive FEMA's modell, det vill säga som en sammanvägning av sannolikhet och konsekvens. Skillnaden är att det i FEMA's modell även tas hänsyn till sårbarheten. Beräkning av risk i IEC's modell motsvarar en del av *riskbedömningen* i FEMA's modell för hantering av antagonistiska risker.

**Sannolikhetsbedömning**
Sannolikhetsbedömningen motsvaras av *hotanalysen* i FEMA's modell för hantering av antagonistiska risker och är i IEC's modell för riskhantering en del av *beräkning av risk*, vilket i sin tur är en del av *riskanalysen*.

För att kunna göra en så noggrann sannolikhetsbedömning som möjligt är bedömningen beroende av tillgången till statistik och erfarenheter [46]. Det finns olika metoder för att räkna ut sannolikheten för olyckrelaterade risker. Dessa metoder kan vara både kvalitativa och kvantitativa [34]. Beräkningen av sannolikheten för en viss skadehändelse kan ske antingen med direkt statistik för skadehändelsen, med beräkning av skadehändelsen med hjälp av statistik för delhändelser som sedan räknas samman till en gemensam sannolikhet [11] eller med hjälp av expertbedömningar.

När det gäller antagonistiska risker, enligt FEMA's modell, sker sannolikhets-bedömningen i det som kallas hotanalys. Denna analys sker som en kvantifiering, med hjälp av tabeller, för att kunna jämföra olika antagonistiska risker sinsemellan.

Analysen är en osäker metod, då den är en uppskattning utifrån till exempel insamlad data om organisationer, samt vilka aktörer som kan hysa agg mot verksamheten. Sannolikheten är svår att bedöma eftersom antagonistiska handlingar kan uppkomma mer slumpartat än för olyckrelaterade risker. Organisationer behöver inte följa ett visst mönster. Detta medan olycksrelaterade risker kan byggas på erfarenheter av att en viss komponent håller en viss tid eller kan användas ett visst antal gånger. Det finns en lång erfarenhetsgrund för att bedöma olycksrelaterade risker, vilket gör att sannolikheten för dem kan bedömas med mindre osäkerheter än för antagonistiska risker.

De två sätten att bedöma sannolikhet utförs på helt olika sätt, det vill säga varken samma metoder eller data kan användas. Detta gör att en integration av arbetet inte anses vara möjlig på denna punkt.

**Konsekvensberäkning**
Konsekvensberäkningen motsvaras av *tillgångsvärderingen* i FEMA's modell för hantering av antagonistiska risker och är i IEC's modell för riskhantering en del av *beräkning av risk*, vilket i sin tur är en del av *riskanalysen*.

Det finns olika metoder för att beräkna konsekvensen av olycksrelaterade risker, exempelvis metoder för beräkning av utsläpp och tanksprängningar. Vissa av dessa metoder ger kvantitativa värden på till exempel hur stort riskområdet (det av händelser påverkade området [33]) blir, hur stort område som blir kontaminerat är eller om byggnader rasar.

För antagonistiska risker, enligt FEMA's modell, används tillgångsvärderingen som konsekvensberäkning. Det sker en bedömning av hur mycket av värdena som påverkas och utifrån det görs kvantifieringen med hjälp av tabeller.

Tillvägagångssättet att beräkna konsekvensen av respektive risktyp skiljer sig. Detta trots att själva händelseförloppet, för tekniska risker som tanksprängningar eller gas-utsläpp, efter det att det initierats anses kunna vara detsamma. Med ett liknande händelseförlopp anses konsekvenserna också likartade och därmed kunna beräknas gemensamt, med samma metoder. Det finns dock skillnader. Till exempel vissa antagonistiska risker som terrorism, kan antas ge största möjliga skada, så kallat "worst case", eftersom aktörerna vill att händelsen skada så mycket eller så många som möjligt [24]. Worst-case-beräkningar används dock även inom olycksrelaterade risker.

Författarna menar att de metoder som används för att beräkna konsekvenser för olycksrelaterade risker bör kunna användas för de antagonistsiska risker som har liknande händelseförlopp som för de olycksrelaterade riskerna. Det skulle innebära en klar utveckling av de antagonistiska riskernas konsekvensberäkning, jämfört med den kvantifiering som sker via FEMA's modell i dagsläget. Det är inte alla antagonistiska risker som har liknande händelseförlopp som för olycksrelaterade, men för de som har undviks dubbel beräkning. Händelser som där någon gör hål i en tank, framkallar en tanksprängning eller startar en brand är exempel på saker som kan hända inom båda risktyperna men bara behöver beräknas för en av dem. Visserligen är vissa beräkningar väldigt lätta och det sparas ingen tid på att göra dem en gång istället för två, men när det exempelvis gäller simuleringar som tar långt tid kan mycket tid sparas.

Om beräkningen av konsekvens utförs gemensamt för antagonistiska risker och olycksrelaterade risker, tror författarna att det är lättare att hålla en jämn nivå av osäkerheter på beräkningarna och därmed underlättas jämförelser mellan olika händelser. Som det är nu görs mer noggranna beräkningar för olycksrelaterade risker vilket kan göra det svårt att jämföra riskerna mellan varandra i riskvärderingen. Författarna menar att det är lättare att jämföra risker med lika mycket osäkerheter än att jämföra en risk med mycket osäkerheter med en som bara har lite osäkerheter. Det är dock en fördel som är svår att utnyttja i ett större perspektiv, eftersom sannolikheterna inte anses kunna jämföras då de är av olika riskmått. Därmed är det heller inte möjligt att jämföra risken i sig, eftersom det således blir olika riskmått för den sammanlagda risken, när hänsyn har tagits till både sannolikhet och konsekvens.

### 7.1.3 Riskvärdering

*Riskvärdering* i IEC's modell för riskhantering motsvaras av *riskbedömning* i FEMA's modell för hantering av antagonistiska risker.

Resultatet från beräkningen av risk uttrycks i ett riskmått, riskindex, individrisk eller samhällsrisk.

Antagonistiska risker beräknas i FEMA's modell med hjälp av indextabeller (semi-kvantitativ metod), vilket ger ett slutligt kvantitativt resultat. Kvantifieringen görs för att riskerna ska kunna jämföras inbördes på ett någorlunda bra sätt.

För att olycksrelaterade och antagonistiska risker ska kunna jämföras med varandra, på ett rättvist sätt, krävs att de är beräknade med samma riskmått. Eftersom sannolikhetsbedömningen av antagonistiska risker är av den karaktär som den är, anses möjligheterna till ett gemensamt riskmått för de båda riskerna vara starkt begränsade. I IEC's modell kan användaren dock använda valfri modell efter vilket syftet är och vilken detaljnivå som krävs (se kapitel 4.3.1). I de fall där hög detaljnivå inte krävs kan liknande riskmått användas.

Vid riskvärderingen, i IEC's modell, och riskbedömningen, i FEMA's modell och COSO's ramverk, sker en jämförelse mellan företagets risker och riskaptit. För att det ska kunna utföras integrerat, bör riskerna inom båda områdena ha samma riskmått. Eftersom det tidigare har klargjorts att en användning av samma riskmått inte anses vara möjlig, kommer det även att medföra att integrationen av riskvärdering och riskbedömning anses svår. Dock behöver ett företag göra någon sorts jämförelse mellan de både risktyperna. Eftersom företaget har begränsat med resurser måste jämförelsen göras för att dessa resurser ska kunna användas på bästa sätt. Jämförelse blir kanske inte optimal men den ger åtminstone företaget en grund för att välja var resurserna ska läggas.

Vid riskvärderingen och riskbedömningen kan det vara intressant att jämföra risker med varandra, men ett stort problem ligger i att analysen av antagonistiska risker är komplex och mer osäker. Detta bidrar till sämre underlag vid riskbedömningen och eftersom det inte är samma riskmått för antagonistiska riskerna och de olycks-relaterade riskerna, blir jämförelser mellan dem svåra att göra. Författarna menar dock att det är en fördel att värdera de olika risktyperna vid samma tillfälle och av samma grupp av personer, då helhetsbilden anses bli bättre och att således jämförelsen med företagets riskaptit inom de olika områdena blir lättare. Genom att samma grupp gör värderingen bör en jämnare nivå kunna hållas. Den jämnare nivån

på bedömningen hålls eftersom samma grupp medför samma subjektiva bedömningar. De subjektiva bedömningarna kan annars spela en avgörande roll. De subjektiva bedömningarna härstammar att olika personer har olika riskperception, det vill säga olika personer uppfattar samma risk olika. Författarna anser att det dock bör finnas med experter inom respektive område vid denna värdering.

**Analys av alternativ**
*Analys av alternativ* i IEC's modell för riskhantering motsvaras av *åtgärdsförslag* i FEMA's modell för hantering av antagonistiska risker.

När åtgärdsförslag tas fram, i IEC's respektive FEMA's modell, för de olika riskerna, sker det genom brainstorming med hjälp av de personer som utför riskanalysen. Detta sker på liknande sätt för de båda risktyperna. Beslutet om vilka åtgärder som ska genomföras tas av ledningen med hjälp av de som utfört analyserna. Besluten kan tas utifrån olika beslutskriterier se kapitel 4.3.2. Även detta sker på liknande vis i IEC's och FEMA's modeller. Då tillvägagångssätten är ungefär desamma för de båda modellerna, anses det finnas möjligheter till integration. Det är dock svårt att jämföra de olika risktyperna inbördes, men helhetsbilden som en samtidig hantering av riskerna skapar anses kunna underlätta när resurserna fördelas i enlighet med ledningens önskan och företagets policys. Författarna menar att en samtidig identifiering av åtgärdsalternativ underlättar för de ansvariga att hitta riskreducerande åtgärder inom båda områdena. Framförallt kan problemet med att åtgärderna ibland motverkar varandra undvikas. När det förebyggande arbetet hanteras samtidigt tror författarna att de medverkande får en bättre helhetssyn av möjligheter och problem. Den samtidiga hanteringen kan åstadkommas bland annat genom att hantera både olycksrelaterade och antagonistiska risker i ett övergripande riskhanteringssystem, som till exempel COSO's ramverk för ERM.

Problemet med att jämföra åtgärderna mellan de olika områdena, eftersom riskerna kan ha olika riskmått och osäkerhet, medför att beslutskriterierna måste modifieras. Till exempel kan sannolikheten ställa till problem. Det medför att jämförelsen endast kan ske utifrån till exempel konsekvenserna. På något sätt måste kriterierna modifieras för att en jämförelse ska kunna vara möjlig. Det är dock viktigt att beslutsfattarna är medvetna om att det är en jämförelse med mycket osäkerheter och tar det i beaktande vid beslutet. Även om jämförelsen inte blir optimal så ger den beslutsfattarna en grund för att kunna fördela företagets resurser på bästa sätt.

### 7.1.4 Riskreduktion och kontroll

Kontrollaktiviteter i IEC's modell består av *implementering* och *övervakning* inom området för olycksrelaterade risker. Motsvarande steg för uppföljning och kontroll-aktiviteter saknas i FEMA's modell.

För att se till att åtgärderna implementeras och efterföljs krävs uppföljning. Uppföljningen kan ske genom kontrollaktiviteter där så mycket som möjligt bör ingå i kontrollerna, utan att de blir för svåra. Komplexa och svåra kontrollaktiviteter medför sämre kontroller eftersom de kan bli för omständliga för personen som utför dem eller eftersom de tar för mycket tid i anspråk. När till exempel en operatör ska utföra kontroller enligt en checklista bör dessa inte ta upp för mycket tid av arbetet. Dessutom bör det ske en ordentlig genomgång av varför kontrollerna sker så att alla ser vikten i dem. Kontroller som bara utförs för att ledningen ska se att de är utförda blir inte lika väl utförda som om till exempel operatören är motiverad till att utföra

dem [47]. Genom ett integrerat kontrollsystem för antagonistiska och olycksrelaterade risker, menar författarna att vissa kontroller kanske kan undvikas eller åtminstone kan de skötas tillsammans i samma rutiner. Författarna menar att vissa kontroller som utförs kan vara samma för olika genomförda åtgärder. Färre separata kontroller kan både spara tid och underlätta för de anställda att följa rutinerna (kontrollerna). Det kan även bli lättare att motivera de anställda till att följa kontrollerna när det inte finns så många olika som tar tid från de ordinarie arbetsuppgifterna. Författarna anser att kontrollaktiviteterna bör skötas gemensamt för att om möjligt kunna integrera vissa kontroller. För många olika kontroller kan öka stressen att hinna med allt, vilket i sin tur kan leda till dåligt utfört arbete [47].

Det kan dock finnas problem med en integration av kontrollerna för de båda risktyperna. Om de kontrollrutiner som införs blir alltför omfattande och komplexa, vilket kan leda till att de blir för svåra eller tidsödande. Detta kan i sin tur leda till att personalen har svårare att se nyttan av dem. Det krävs motiverad personal för att undvika att fel begås i deras arbetsuppgifter [47]. Författarna menar att för komplexa kontroller kan medföra att personalen inte ser nyttan i dem och de blir därför lidande. Det är därför viktigt att kontrollerna inte blir för komplexa vid en eventuell integrerad kontroll.

## 7.2 Drivkrafter

När det gäller drivkrafter har författarna fört ett resonemang om vilka möjligheter och problem olika drivkrafter kan medföra för en eventuell integration av hanteringen av olycksrelaterade och antagonistiska risker.

Drivkrafterna för att arbeta med riskhantering av olycksrelaterade respektive antagonistiska risker är i det stora hela av samma slag. Drivkrafterna kan dock få olika dignitet beroende på vilken risktyp som avses.

Med en integrerad hantering av antagonistiska risker och olycksrelaterade risker är det möjligt att fokus hamnar på bara ett av områdena, exempelvis om något av dem är dominerande. Det är därför viktigt att se till att fokus bibehålls på båda områdena, så att inga risker negligeras eller förbises.

### 7.2.1 Etik och moral

Beroende på hur ett företag profilerar sig, eller beroende på vilka etiska och moraliska värderingar företaget har, kan antagonistiska respektive olycksrelaterade risker väljas att behandlas olika. På så sätt kan exempelvis drivkraften vara större och därmed riskaptiten bli mindre för antagonistiska risker än för olycksrelaterade risker, eller vice versa.

### 7.2.2 Ekonomi

Den ekonomiska drivkraften borde vara lika stor för de båda risktyperna, då det handlar om att med hjälp av riskhantering sänka sina kostnader. Då gäller det att satsa på de mest kostnadseffektiva åtgärderna och således borde inte risktypen i sig vara avgörande.

### 7.2.3 Kunder och leverantörer

Kunder och leverantörer kan ställa olika höga krav på hanteringen av olycksrelaterade risker och antagonistiska risker, till exempel beroende på vilken inställning de har till de respektive riskerna.

### 7.2.4 Goodwill

I enlighet med drivkraften etik och moral, kan antagonistiska respektive olycksrelaterade risker väljas att behandlas olika med avseende på företagets goodwill. Beroende på hur ett företag vill framtonas, eller beroende på vilka värderingar företaget vill associeras med, kan antagonistiska respektive olycksrelaterade risker väljas att behandlas olika. På så sätt kan exempelvis drivkraften vara större för att hantera antagonistiska risker än för att hantera olycksrelaterade risker, eller vice versa.

### 7.2.5 Främja arbetsklimatet genom intern trygghet

Eftersom olika personer har olika uppfattning om risker, kan olycksrelaterade respektive antagonistiska risker få olika betydelse för olika personer. Detta kan bidra till att drivkrafterna blir olika starka för de båda risktyperna.

### 7.2.6 Försäkringsbolag

I likhet med att kunder och leverantörer kan ställa olika krav på företags riskhantering med hänsyn till de olika områdena (olycksrelaterade risker och antagonistiska risker), kan försäkringsbolag göra det samma. Ett sätt att kontrollera det är att sätta premierna för olika risker i relation till vilka åtgärder som vidtas inom respektive område. Detta medför att drivkraften kan variera i storlek för de olika risktyperna beroende på hur försäkringspremierna ändras med förebyggande åtgärder.

### 7.2.7 Lagstiftning

De lagmässiga kraven är fler inom området för olycksrelaterade risker än inom området för antagonistiska risker, vilket gör incitamentet större inom området för olycksrelaterade risker.

## 7.3 Utbildning och kompetenser

En jämförelse av utbildningsnivån mellan de som arbetar med olycksrelaterade risker på AB Ångpanneföreningen och de som arbetar med antagonistiska risker på SecMentor A/S visar att det är något högre akademisk utbildningsnivå inom olycksrelaterade risker. Arbetet och metoderna på SecMentor A/S bygger mycket på långa erfarenheter som tillförskansats via exempelvis militärtjänstgöring.

Författarna gjorde eftersökningar via Internet på olika utbildningar, kurser och krav som finns inom de olika områdena. Detta gjordes för att kunna vederlägga de skillnader i utbildningsnivå som gällde för de två konsultföretagen. Undersökningen ledde dock till att uppfattningen stärktes om att det generellt sett finns skillnader i utbildningsnivå inom de båda områdena.

## 7.4 Integration i COSO's ramverk för ERM

Det har för denna komponent förts ett resonemang kring hur de båda risktyperna passar in i ett övergripande ramverk för riskhantering på ett företag, i denna rapport åskådliggjort med COSO's ramverk för ERM.

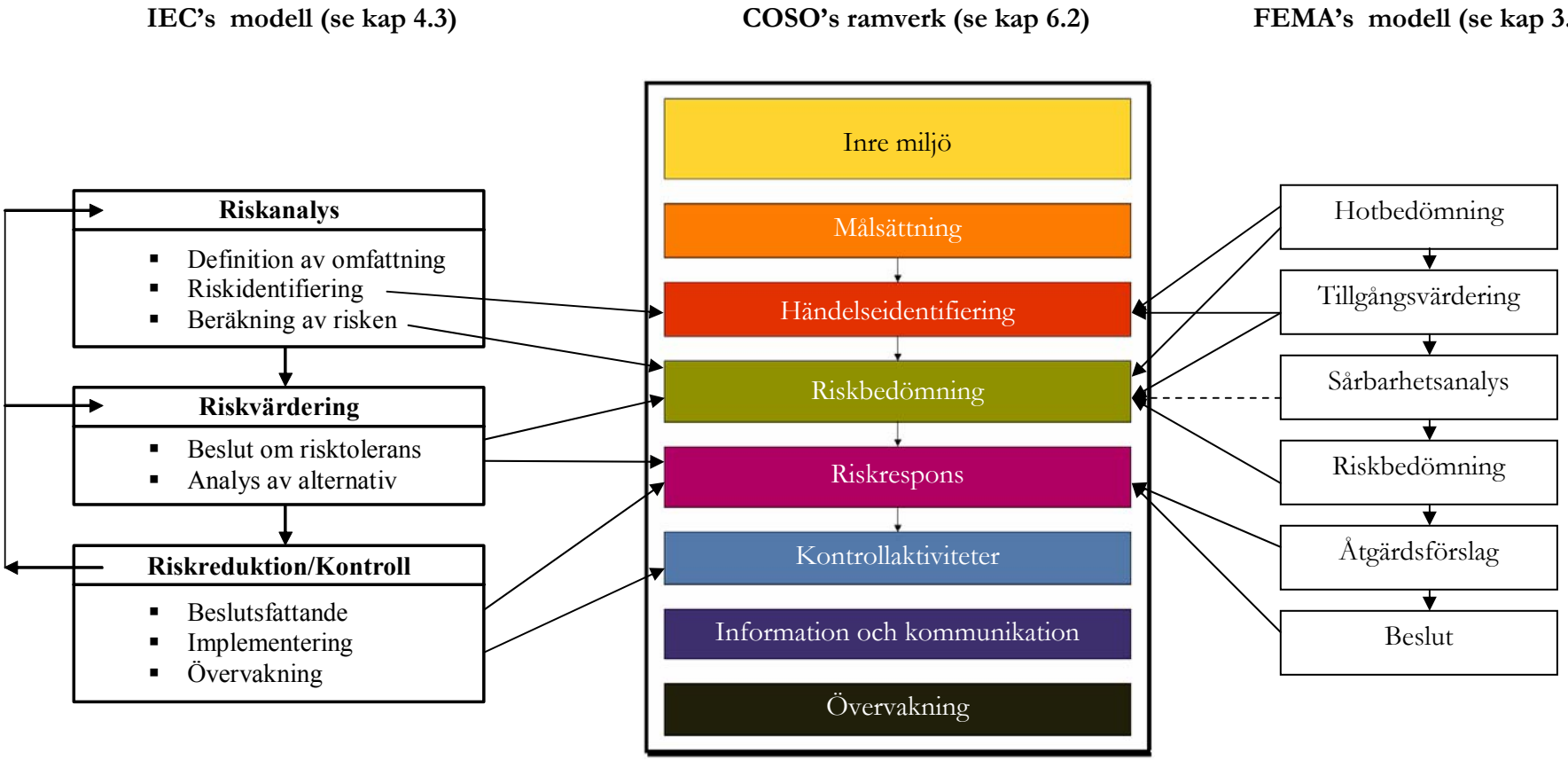
Författarna anser att det är en fördel att ha ett övergripande ramverk för alla företagets risker. På så sätt skapas bättre förutsättningar för att strukturera arbetet och att hålla det på en jämn nivå sinsemellan de olika risktyperna. Ett och samma system eller ramverk för samtliga risker bäddar för större överblickbarhet och på så sätt underlättas det att fördela nödvändiga resurser.

Ett och samma system minskar också den begreppsförvirring och de oklarheter som generellt finns inom området för riskhantering.

De delsteg i riskhanteringsprocessen som inte är möjliga att integrera bör enligt författarna trots allt samlas eller hanteras i ett gemensamt ramverk, exempelvis COSO's ramverk för ERM. Även om arbetet med riskerna inte går att integrera fullständigt, och på så vis spara exempelvis tid och pengar, finns det möjlighet att med hjälp av ramverkets struktur utvecklas och hanteras effektivare.

Kopplingen mellan de olika stegen i COSO's ramverk för ERM, IEC's modell för riskhantering, samt FEMA's modell för hantering av antagonistiska risker finns beskrivet schematiskt i Figur 17 nedan. Gränserna och stegen i processerna är dock på olika sätt flytande och tenderar att gå in i varandra.

Vid en granskning av figuren nedan kan det konstateras att alla de delsteg som finns med i FEMA's respektive IEC's modell även finns med i COSO's ramverk. Ramverket är till för att skapa en struktur, det vill säga ett sätt att arbeta. Det är ett övergripande ramverk som inte ger någon helhetslösning utan blir vad man gör det till. I ramverkets element går det att använda sig av vilka hjälpmedel man vill för att uppfylla sina mål. Eftersom ramverket ger samma delsteg som IEC's och FEMA's modeller, samt att det ger möjligheten för användaren att själv välja hjälpmedel i form av till exempel metoder och ledningssystem, kan författarna inte se någon anledning till att ramverket inte skulle kunna hantera både olycksrelaterade och antagonistiska risker.




**Figur 17.** Figuren är ett försök till att schematiskt visa kopplingen mellan de olika stegen i COSO's ramverk för ERM, IEC's modell för riskhantering, samt FEMA's modell för hantering av antagonistiska risker. Observera att figuren inte gör anspråk på att vara komplett, eftersom gränserna och stegen i processerna på olika sätt är flytande och tenderar att gå in i varandra. Modellerna är översatta till svenska.

### 7.4.1 Inre miljö

Företagets inre miljö omfattar och påverkar hela organisationen och dess riskhantering. Därmed är den inre miljön i företaget viktig även vad gäller antagonistiska risker, det vill säga hur de hanteras, reduceras och förebyggs. Exempelvis sabotage, fysiskt eller informationssystemrelaterat, orsakas ofta av aktörer från företaget som på något sätt känner sig orättvist behandlade [20], vilket i sin tur påverkas av den inre miljön.

Att göra medarbetare medvetna om risker inom och omkring företaget, bidrar till en god riskhantering och förståelse för en sådan. En riskhanteringsfilosofi som är förstådd av all personal underlättar de anställdas möjlighet att förstå risker och att hantera dem på ett effektivt sätt. Detta gäller likväl förståelse för antagonistiska risker och bakgrunden till dess förebyggande åtgärder.

Risker, såväl antagonistiska som olycksrelaterade, förebyggs med bland annat goda säkerhetsföreskrifter och efterföljande av desamma. Företagets riskhanteringsfilosofi speglas i policys och målsättningar. Det viktigaste är dock att filosofin underbyggs i de dagliga aktiviteterna, inte minst på ledningsnivå. ”Medarbete gör som chefen gör, inte som chefen vill.” [48] Talesättet poängterar att handling väger tyngre än ord. För att erhålla och kvarhålla en god inre miljö måste den framhävas och efterlevas, framför allt på ledningsnivå.

Ett företags riskaptit visar vilka risker företaget är berett att ta, i strävan efter vinst. Eftersom riskaptiten är beroende av de drivkrafter som påverkar företaget, kan den variera något gällande olycksrelaterade respektive antagonistiska risker beroende på vilka policys och därmed vilken framtoning och profil som företaget har. För vidare förklaring hänvisas till kapitel 7.2. Författarna tror dock att det kan vara till fördel att vid samma tillfälle definiera företagets riskaptit med hänsyn till de olika områdena, eftersom det då kan vara lättare att ställa de olika riskerna i relation till varandra.

På många företag är säkerhetskulturen en följd av rådande riskhanteringsfilosofi och riskaptit [10]. En god säkerhetskultur innebär i stora drag att säkerhetstänkande är förankrat i ledningen såväl som hos de anställda och att onödigt risktagande minimeras. Säkerhetskulturen speglar de attityder och beteenden som finns i företaget. I ett företag med en god säkerhetskultur är säkerheten ett basvärde i organisationen. Säkerhetskulturen påverkar således hur risker hanteras inom företaget. Vikten av ett säkert handlande ska alltid vara i tankarna även i stressade och pressade situationer, vilket gäller både antagonistiska och olyckrelaterade risker. Författarna tror att en skillnad kan vara att det är lättare att mentalt föreställa eller förbereda sig på att en olycksrelaterad olycka sker. Detta då tron på människans goda vilja motsäger att någon skulle utföra en handling i ren illvilja [24]. Därmed kan antagonistiska risker och dess relaterade säkerhetsåtgärder vara svårare att anpassa sig till.

Individuella företagsenheter, funktioner och avdelningar kan ha något olika säkerhetskulturer. Dessa olika säkerhetskulturer kan dra åt olika håll, men kan även komplettera varandra och kollektivt representera företagets önskvärda riskaptit och riskhanteringsfilosofi.

Företagets riskhanteringsfilosofi påverkar hur antagonistiska respektive olycksrelaterade risker uppfattas och behandlas i organisationen. Rutinmässiga och dagliga aktiviteter är av stor vikt i riskrelaterade frågor och spelar därför stor roll för företagets hela riskhanteringsprocess. Det är därför viktigt att ledningen fokuserar på både hanteringen av antagonistiska risker och olycksrelaterade risker. En fördel med ett gemensamt system för riskhantering är att ledningen har bättre möjlighet att styra fokus och anpassa bland annat företagets riskhanteringsfilosofi efter båda områdena.

Författarna tror att det är lättare att utforma företagets inre miljö genom att ta hänsyn till både olycksrelaterade och antagonistiska risker vid samma tillfälle, så att inte tvetydigheter eller intressekonflikter dyker upp i efterhand.

### 7.4.2 Målsättning

En företagsledning använder sig av uppsatta mål för att styra och leda sin verksamhet. Målen sätts upp för att driva organisationen framåt, samt för att motivera och sporra anställda till att utföra ett bra arbete. Väl uppsatta mål möjliggör för ledningen att mäta företagets framgång. [10]

De övergripande målen ett företag har, exempelvis att öka vinsterna och minska förlusterna genom god riskhantering, kan delas upp i mindre delmål. Ju mer precisa delmålen blir desto mer kan målen skilja sig för antagonistiska risker och olycksrelaterade risker. Till exempel går det inte att ha ett gemensamt mål för att minska antalet inbrott och minska antalet sjukskrivningar orsakade av olyckor på arbetsplatsen. När målen inom respektive område sätts upp behöver de således inte innefatta båda områdena.

Målen bör, integrerade eller inte, i enlighet med kapitel 6.2.1, uppfylla de kriterier som gäller för uppföljningsbara mål, SMART-kriterierna. Om ett sammansatt mål uppfyller de kriterier som ställs på mål bör det betyda att integrationen av målet är lyckad. Det är dock viktigt att tillse att målen är lika omfattande som de skulle vara om de behandlades var för sig. Problemet med att arbeta med båda områdena samtidigt, är att det kan vara svårt att hålla samma fokus på respektive område som det hade varit om arbetet hade skötts var för sig.

Genom en gemensam och samtidig målsättning finns det möjlighet att uppdaga onödiga intressekonflikter mellan olika mål, tidigt i processen. Detta torde bidra till att konflikterna kan lösas i ett tidigt stadium, innan de blir problem för själva verksamheten. Ytterligare en fördel med att hantera målsättningen samtidigt, är att det blir lättare att jämföra områdena sinsemellan och välja hur företaget ska satsa. Det kan vara mer kostnadseffektivt att satsa inom bara ett av områdena för att till exempel minska företagets riskbild.

### 7.4.3 Händelseidentifiering

Händelseidentifieringen i COSO's ramverk motsvaras av *riskidentifiering* i IEC's modell för riskhantering inom området för olycksrelaterade risker. De delar som är aktuella i FEMA's modell för hantering av antagonistiska risker är *hotbedömning*, *tillgångsvärdering* och *sårbarhetsanalys*.

Händelseidentifiering är då ett företag försöker att identifiera möjliga framtida händelser som kan påverka verksamheten och dess uppsatta mål. Arbetet utförs exempelvis genom att ansvarig samlar en grupp människor från den egna

organisationen som ska vara delaktiga i identifieringen. Gruppen ska arbeta sig genom verksamheten metodiskt, steg för steg, och genom brainstorming identifiera möjliga händelser eller skyddsvärda objekt. För vidare analys hänvisas till kapitel 7.1.1.

### 7.4.4 Riskbedömning

Riskbedömningen i COSO's ramverk motsvaras av *beräkning av risk*, samt *riskvärdering* i IEC's modell för riskhantering. De delar som är aktuella i FEMA's modell för hantering av antagonistiska risker är *hotbedömning*, *tillgångsvärdering*, till viss del *sårbarhetsanalys* och *riskbedömning*.

När ett företag har identifierat de risker som finns inom sin verksamhet görs en riskbedömning. Riskbedömningen är uppdelad i två delar, en del som bedömer sannolikheten att händelsen ska inträffa och en del som bedömer konsekvensen av händelsen. De olycksrelaterade händelser som kan ske inom en verksamhet, kan även utlösas genom uppsåtliga handlingar. När det gäller händelser med stora konsekvenser är de extra intressanta för någon som vill orsaka skada. För vidare analys hänvisas till kapitel 7.1.1 - 7.1.3.

### 7.4.5 Riskrespons

Riskresponsen i COSO's ramverk motsvaras av *analys av alternativ*, samt *beslutsfattande* i IEC's modell för riskhantering. De delar som är aktuella i FEMA's modell för hantering av antagonistiska risker är *åtgärdsförslag*, samt *riskrespons*.

Riskresponsen är framtagande och beslutande av åtgärder för att på något sätt reducera eller eliminera risker. Valet av åtgärd sker exempelvis genom att utföra en kostnad-nytta-analys av de alternativ som identifierats, för att sedan välja det alternativ som är det mest kostnadseffektiva. För att hitta ett så kostnadseffektivt alternativ som möjligt, är det viktigt att väga in så många aspekter som möjligt med det berörda alternativet. För vidare analys hänvisas till kapitel 7.1.4.

### 7.4.6 Kontrollaktiviteter

Kontrollaktiviteter i COSO's ramverk motsvaras av *implementering*, samt *övervakning* i IEC's modell för riskhantering. Denna del saknas i FEMA's modell för hantering av antagonistiska risker. För vidare analys hänvisas till kapitel 7.1.4.

### 7.4.7 Information & Kommunikation

En viktig del av ett företags hantering av risker är information och kommunikation med leverantörer, kunder och egen personal. Informationen är ett verktyg för att såväl antagonistiska risker som olycksrelaterade risker ska kunna identifieras. Det är viktigt att alla ska kunna delge ett företag information på ett lätt sätt. Många olika informationsvägar kan motverka att informationen kommer fram. En gemensam väg underlättar att veta vart man ska vända sig, samt att det ger ett bättre förtroende om informationen alltid kommer från eller hanteras via samma tillförlitliga källa. Den information som kommer in till företaget kommer bland annat genom rapporteringssystem. Ett gemensamt rapporteringssystem för samtliga riskrelaterade frågor underlättar för dem som använder systemet. Den information som går ut måste uppfylla de krav som är ställda på information.

Problem som författarna tror kan uppstå i samband med information och kommunikation är intressekonflikt med den sekretess som ofta är önskvärd inom området för antagonistiska risker. Riskhantering avseende olycksrelaterade risker grundas på öppenhet, information och kommunikation, medan sekretess ofta är en viktig punkt avseende antagonistiska risker.

### 7.4.8 Övervakning

Övervakningen av ramverkets implementering och hur de olika elementen fungerar sker som fortlöpande kontroller eller enskilda utvärderingar. Kontrollerna och utvärderingarna sker på delar av eller hela riskhanteringsarbetet.

Fördelen med att använda ett och samma system för övervakning är enligt författarna att en helhetsbild erhålls, samt att resurser kan sparas genom att inte göra samma arbete två gånger.

Vid enskilda utvärderingar anser författarna att det är bra att bland annat studera integrationen av antagonistiska risker i COSO's ramverk, för att identifiera skillnader mot hur det skulle vara att hantera dessa risker i ett separat system.

# 8 INTERVJUER MED YRKESVERKSAMMA

*I detta kapitel redovisas resultatet från ett antal telefonintervjuer som gjordes med yrkesverksamma personer. Intervjuerna utfördes för att undersöka vad yrkesverksamma personer anser vara möjligheter och problem med en integration av hanteringen av olycksrelaterade risker och antagonistiska risker.*

## 8.1 Intervjupersoner

Ett antal intervjuer har utförts med personer ansvariga för riskhanteringen på olika företag, konsulter som arbetar med hanteringen av olyckrelaterade risker samt konsulter som arbetar med hanteringen av antagonistiska risker. Intervjuerna är utförda för att undersöka vad personer med erfarenhet inom de olika områdena anser vara möjligheter och problem med en integration av hanteringen av olycksrelaterade och antagonistiska risker. Grunden i intervjuerna var att intervjupersonerna fick tala fritt och svara intuitivt på vad de ansåg vara möjligheter och problem med en integration av hanteringen av antagonistiska och olyckrelaterade risker. Utifrån det hölls intervjuerna i form av en diskussion, mellan intervjupersonen och intervjuaren, som gick ut på att intervjupersonen fick tala så fritt som möjligt.

Urvalet av personer grundas på ett försök till att täcka in personer med olika erfarenheter och bakgrunder. Intervjuerna är utförda för att jämföras med resultatet från den analys av integrationsmöjligheter och problem mellan olycksrelaterade och antagonistiska risker som tidigare gjorts i rapporten. Jämförelsen syftar till att slutsatser ska kunna dras beträffande möjligheter och problem med en sådan integration. Intervjuerna har även använts till att göra ett validitetstest (se kapitel 8.3) av de komponenter som författarna tagit fram för att utföra sin analys. Författarnas komponenter jämfördes med de områden som intervjupersonerna tog upp vid intervjuerna.

Intervjuer har utförts med följande personer:

- Bengt Svensson, Risk Chief Officer, E.ON Sverige AB.
- Mats Lindgren, Chef för säkerhet och kvalitet, Preem Petroleum (publ. AB), Preemraff Göteborg.
- Lars-Göran Larsson, revisor, Rödl & Partner Sverige AB.
- Anders Jacobsson, konsult inom teknisk riskhantering, AJ Risk Engineering AB, adjungerad lektor vid Lunds tekniska högskola.
- Anders Norén, konsult inom teknisk riskhantering, AB Ångpanneföreningen.
- Lars Harms-Ringdahl, konsult inom teknisk riskhantering, Institutet för Riskhantering och Säkerhetsanalys, adjungerad professor vid Karlstad universitet.
- Lars-Olof Carlsson, f.d. medlem i Akzo Nobels internationella management-team för SHM-frågor, pionjär inom integrerad säkerhet, hälsa och miljö, numera pensionär.
- Ingemar Grahn, Risk management konsult, Ingemar Grahn risk management konsult.
- Lennart Ädel, avdelningschef personskydd, Securitas AB.

Resultatet från intervjuerna sammanställdes och författarna har tagit med de delar som var relevanta för examensarbetet. För att kontrollera att resultatet från intervjuerna stämde överens med de intervjuades uppfattningar, fick de möjlighet att kontrollera sammanställningen. För att säkerställa att samtliga personer uppfattade de olika riskerna på samma sätt, definierade författarna de båda riskerna i början av respektive intervju.

## 8.2 Intervjuresultat

### 8.2.1 Inledning

En allmän uppfattning är att intresset för antagonistiska risker har ökat de senaste åren. En bidragande faktor till ökningen anses vara den ökade mediala bevakning som de antagonistiska händelserna eller riskerna har fått.

Det finns även en gemensam uppfattning om att antagonistiska risker tidigare har negligerats. De har negligerats delvis för att de anses vara svåra att hantera eller att de har ansetts vara för osannolika [49]. Svensson menar att det arbete som utförs med antagonistiska risker inte sker på ett systematiskt sätt. Det arbete som utförs på E.ON är reaktivt efter händelser i omvärlden eller efter rapporter om hotbilder som företaget abonnerar på. [50] Carlsson anser att det i första hand gäller att påpeka att de antagonistiska riskerna existerar och jaga fram åtgärder. I andra hand anser han att en långsiktig utveckling behövs. ”Det viktigaste är att väcka dem som kan påverka den här typen av risker och få dem till att inse att det är ett fält som redan existerar och att man inte gör vad som borde göras.” [51]

Alla intervjupersonerna anser att det finns möjligheter till att integrera arbetet med antagonistiska och olycksrelaterade risker. Dock skiljer sig till viss del åsikterna åt angående vilka möjligheterna och problemen är med en sådan integration. Svensson säger att de (läs E.ON) idag rent organisatoriskt sett har ett integrerat arbete, eftersom det finns en säkerhetschef med i deras riskhanteringsstab [50]. ”Riskanalys-principerna är tillämpliga även för antagonistiska risker. En enhetlig modell underlättar, särskilt som den är inarbetad på företaget när det gäller olycksrisker.” [52]

### 8.2.2 Riskhanteringsprocessen

**Sannolikhetsbedömning**

En klar majoritet av de tillfrågade anser att det största problemet med antagonistiska risker finns i sannolikhetsbedömningen. De antagonistiska riskerna anses vara irrationella och går inte alls att förutsäga på samma sätt som olycksrelaterade risker [50].

Harms-Ringdahl anser dock att det finns så pass stora problem i de sannolikhetsbedömningar som är av praxis inom olycksrelaterade risker, att han brukar pröva olika tekniker för att undvika de problem som kan genereras härav. Dessa tekniker tror han är möjliga att även applicera på området för antagonistiska risker. [53]

**Konsekvensbedömning**

Alla tillfrågade anser att det i stort sett handlar om samma händelseförlopp när väl en händelse inträffat, antagonistiskt triggad eller ej. Det anses endast vara den initierande händelsen som skiljer. Således anser de tillfrågade att riskernas konsekvensberäkning och konsekvenshanteringen har möjligheter att integreras. Dock bör konsekvenserna

från de antagonistiska riskerna analyseras mer noggrant, där större hänsyn tas till sekundära effekter [49]. Detta eftersom det lättare kan bli dominoeffekter om aktörerna som utför de antagonistiska handlingarna har tillräcklig kunskap, möjlighet och verkligen försöker åstadkomma största möjliga skada [49].

**Riskrespons**
Gemensamt för intervjupersonerna är också att de anser att många åtgärder kan ha motverkande effekt på både antagonistiska respektive olycksrelaterade risker. Det ger att de anser att det vore positivt och att det finns möjlighet att integrera riskresponsen, just för att ta hänsyn till alla effekter av en eventuell åtgärd.

Harms-Ringdahl anser att det finns goda skäl till att integrera arbetet med riskerna vid riskbedömningen så länge dilemmat med sannolikhetsbedömningen undviks. Anledningen är att det vid en bedömning av om riskreducerandeåtgärder ska utföras eller inte, måste båda typerna av risker beaktas eftersom resultatet kanske inte är detsamma för båda riskerna. [53]

### 8.2.3 Drivkrafter

När det gäller drivkrafterna för att utföra riskhantering i det stora hela, menar samtliga tillfrågade att det handlar om ekonomiska aspekter och personsäkerhet.

De organisationer som genuint vill skydda sin verksamhet bryr sig inte om orsaken till händelserna utan vill bara få kontroll över riskerna [31].

De lagkrav som finns på verksamheten har stor inverkan men det är ingen drivkraft, utan bara något som organisationen måste bevaka och uppfylla. Det som verkligen driver arbetet med risker är det ekonomiska samt personalens välmående [50].

De olycksrelaterade riskerna är drivna från flera olika intressenter som anställda, myndigheter och ägare, medan det inte funnits någon stark intressent som tryckt på de antagonistiska riskerna. Dessa tre grupper har inte upplevt antagonistiska risker som en betydande risk jämfört med olycksrisker. [52]

### 8.2.4 Utbildning och kompetenser

Vad gäller möjligheter och problem angående kompetenser, går åsikterna något isär.

Jacobsson tror att samma person kan sköta arbetet med antagonistiska och olycksrelaterade risker i ett företag, dock med hjälp av expertis inom respektive område när det behövs. Han tror även att så sker i dagsläget. [49]

Norén menar att kompetenserna ska hållas isär, men ser möjligheter i att de kan komplettera varandra väl. Han anser att man ska vara medveten om att det handlar om väldigt olika perspektiv, med statistik inom den tekniska riskhanteringen och mer att tänka det otänkbara inom de antagonistiska riskerna, för att sedan agera djävulens advokat. [31]

Harms-Ringdahl anser att som det ser ut idag kan kompetenserna inte mötas och föras samman. Det handlar om skilda traditioner och tankesätt. Det krävs träning för att de ska kunna samarbeta. [53]

Kompetensmässigt anser Lindgren att områdena kan ledas av en och samma person, men om resursbehovet är större än en person anser han att en specialisering underlättar. [52]

### 8.2.5 COSO's ramverk för ERM

De som hade kunskap om COSO's ramverk ställde sig positiva till hanteringen av både antagonistiska och olycksrelaterade risker i ramverket.

Larsson anser inte att det finns några problem med att ta hänsyn till antagonistiska risker i COSO's ramverk för riskhantering, eftersom det är så pass generiskt. Det kan vara ett naturligt inslag i det strategiska och operationella perspektivet. Det är dock beroende av under vilka förutsättningar som riskanalyserna utförs. Vidare anser han att det är viktigt att definiera förutsättningarna för att få någon form av avgränsning och tydlighet i analysen. [54]

En klar fördel är att det genom COSO's ramverk erhålls en klar definition av processen, det vill säga de olika stegen i en riskhanteringsprocess. COSO's ramverk definierar också fokus, det vill säga vad det är som ska bedömas. En god inre kontroll tydliggör ansvarsfördelningen så att inga risker hamnar mellan stolarna. Med ramverkets hjälp blir det mycket klarare och tydligare hur företaget förhåller sig till olika riskexponeringar. Den stora nyttan är att COSO's ramverk ger en väldig tydlighet. [54]

Svensson menar att fördelen med att använda COSO's ramverk är att det ger ett processtänkande i arbetet med riskhantering. Det ger även legitimitet så att det blir lättare att få förståelse för detta arbete. [50]

### 8.2.6 Övrigt

Svensson menar att eftersom antagonistiska risker och olycksrelaterade risker handlar om liknande händelser efter att de väl har inträffat, finns det stora möjligheter till att integrera arbetet med beredskapsplaner och katastrofplanering [50].

Norén anser att vid en eventuell integration av antagonistiska och olycksrelaterade risker finns det ett stort problem i att förlora fokus och därmed endast arbeta med en av riskerna. Då är det lätt att endast ta hänsyn till den risk som är lättast att hantera. Det finns även ett problem i att personer som har arbetat inom ett av områdena gärna använder sig av sina metoder. De metoder som de använder är inte validerade för den andra typen av risk och medför då en stor osäkerhet i resultatet. [31]

Harms-Ringdahl påpekar att det finns både för- och nackdelar med att hantera riskerna i ett gemensamt system. Det finns problem i att det ena området kan bli lidande och allt fokus läggs på den risk som har hanterats tidigare, eftersom de som utför analysen vet hur de ska göra inom "sitt" område. När någon ger sig in på ett annat område än sitt eget, där det finns bättre kompetens blir resultatet av analysen sämre än om de utförts av personer som är vana vid den typen av risker. [53]

Grahn anser att det är en nödvändighet att hantera alla risker i en och samma riskhanteringsprocess. Det gäller att presentera en samlad riskbild för beslutsfattarna, för att de i sin tur ska kunna fatta ett bra beslut. Beslutsfattarna måste kunna jämföra olika risker med varandra, mellan olika riskområde, på ett vettigt sätt, för att de ska kunna fördela tillgängliga resurser där de bäst behövs. [55]

När olycksrelaterade risker hanteras görs det med fördel i all öppenhet, medan det motsatta gäller för antagonistiska risker. Detta kan orsaka problem vid en eventuell integration av arbetet. [52, 53]

## 8.3 Validitetstest av komponenter

För att kontrollera att de komponenter som författarna har använt för att utföra analysen i rapporten, har en jämförelse skett med de områden som intervjupersonerna tog upp. I analysen använde sig författarna av komponenterna, riskhanteringsprocessen (IEC's och FEMA's modeller), drivkrafter, utbildning och kompetenser, samt ledning och styrning av riskhantering med hjälp av COSO's ramverk för ERM.

Samtliga komponenter som används i rapportens analys, togs även upp av intervjupersonerna i intervjuerna. Dock fanns det skillnader i uppfattningen ifall de ställer till problem eller inte. Det faktum att intervjupersonerna tog upp samma områden tyder på att komponenterna är väsentliga för en jämförelse av arbetet med olycksrelaterade och antagonistiska risker.

Samtliga intervjupersoner tog upp delar i riskhanteringsprocessen som möjliga att integrera eller som problemområden för en integration. Det tyder på att det är ett viktigt område vid en eventuell integration.

Intervjupersonerna tog även upp drivkrafterna i intervjuerna. Dock var det ingen som tog upp det som ett problem, vilket tyder på att det inte är ett lika viktigt område. Författarna menar dock, med stöd från litteratur [6], att drivkrafter är en viktig del i arbetet med riskhantering och därmed anses komponenten vara relevant vid en analys.

Kompetensen inom de båda områdena tog flera intervjupersoner upp som ett problem. Dock skiljde sig deras uppfattningar något, vilket tyder på att det är en viktig faktor att ta i beaktande.

När det gäller ett ramverk för riskhantering har intervjupersonerna tagit upp även detta område. Någon anser att det är en nödvändighet i ett företags riskhantering, att risker behandlas i ett gemensamt system.

# 9 DISKUSSION

*I detta kapitel förs en diskussion med utgångspunkt från rapportens frågeställningar.*

Vid en jämförelse mellan resultatet från de intervjuer som utförts (se kapitel 8) och det resultat som författarna kommit fram till i kapitel 7, kan både likheter och skillnader ses. De yrkesverksammas uppfattningar är sinsemellan lika, med några enstaka undantag.

**Ökat intresse för antagonistiska risker**
Alla intervjupersonerna hade samma uppfattning om att intresset för antagonistiska risker har ökat de senaste åren. Flera personer menar att detta är mycket tack vare den ökade framställning som har varit och är i media. Med tanke på Carlssons synpunkt att intresset för antagonistiska risker inte finns eftersom företagen inte beaktar dem, kan medias betydelse låta logisk [51]. Han menar att så fort någon informerar om vikten av antagonistiska risker, kommer även de att hanteras. Den erfarenhet han har, är att de antagonistiska riskerna har negligerats på grund av dålig kunskap om att de existerar och att det som krävs mest är någon som övertygar företag om att dessa är viktiga risker att ta hänsyn till.

Några intervjupersoner hade uppfattningen om att antagonistiska risker har negligerats på grund av att de har varit svåra att hantera. Det har varit lättare att bara ta hänsyn till de risker som det redan finns kännedom om. Med ett ökat intresse kommer även de antagonistiska riskerna behöva tas på allvar. Dessa kommer då att behövas analyseras på ett mer systematiskt sätt för att arbetet ska kunna hålla samma klass som arbetet med olycksrelaterade risker.

**Liknande händelseförlopp**
Precis som i författarnas egna resonemang i kapitel 7, såg intervjupersonerna likheter i riskerna när det gäller vissa händelseförlopp. De händelser som kan ske på grund av en olycka kan även ske på grund av att någon avsiktligt orsakar den. Med dessa händelser avses framförallt händelser som är kopplade till tekniska risker på ett företag inom till exempel processindustrin. Samtliga delade uppfattningen om att det rör sig om så gott som samma händelseförlopp. Detta i sin tur gav att de kunde se integrationsmöjligheter i beräkningen av konsekvenser, eftersom samma händelseförlopp ger samma fysiska konsekvenser. Dock påpekade endast en av intervjupersonerna samma problem, med metoderna, som författarna kom fram till i analysen. Eftersom de metoder som är framtagna för respektive område endast är validerade för det området, kan det innebära problem om de används för risker inom det andra området. Men om det nu handlar om samma händelseförlopp bör samma metoder kunna användas, eftersom de inte tar hänsyn till hur olyckan har inträffat. Detta är dock något som måste undersökas närmre innan en eventuell integration är möjlig.

**Åtgärdshantering**
Nästa del i riskhanteringsprocessen är framtagandet och analysen av åtgärderna. Det såg både intervjupersonerna och författarna som möjlig att integrera eller sköta samtidigt. Intervjupersonerna var alla av uppfattningen att många åtgärder reducerar risker inom båda områdena. Det är därför viktigt att ta hänsyn till det vid val av åtgärd. Författarna tog dock även upp att det kan vara ett problem med att åtgärder kan reducera risken inom det ena området, medan den ökar andra risker inom det

andra området. Det är viktigt att ta hänsyn till denna aspekt, eftersom den totala risken skulle kunna öka trots att företaget lever i tron om att de utför åtgärder för att sänka risken.

**Olika sannolikhetsbedömning**
Vid en jämförelse av sannolikhetsbedömningen för de olika riskerna, kan en tydlig skillnad ses. Bedömningarna skiljer sig tydligt eftersom de bygger på helt olika saker. När en sannolikhetsbedömning utförs för olycksrelaterade risker görs de med utgångspunkt på statistik och erfarenhet från dem som utför bedömningen. Som författarna ser det går det att göra en bra bedömning av sannolikheten om det finns tillgång till rätt statistik. När det gäller antagonistiska risker görs sannolikhets-bedömningen med utgångspunkt på vilka organisationer som finns, om de har intresse av berörd anläggning, tillgång till kunskap med mera. Denna bedömning anser författarna vara mycket svår och väldigt osäker. Bedömningen utförs ofta kvalitativt som sedan kvantifieras för att en risk ska kunna beräknas. Denna uppfattning delas av flertalet av intervjupersonerna, som anser att det är sannolikhetsbedömningen som är det svåra i arbetet med antagonistiska risker. Därför anser författarna att ett integrerat arbete, det vill säga att använda samma metoder och att göra arbetet gemensamt, när det gäller sannolikhetsbedömningen inte är möjlig. De anser att detta arbete skiljer sig i den grad att det bör ske separat.

En av intervjupersonerna menade dock att bedömningen av olycksrelaterade sannolikheter även rör sig om så pass stora osäkerheter att de kan jämställas med de osäker som finns inom antagonistiska risker. Han använder sig av metoder som han bedömer även kan hantera antagonistiska sannolikheter. Det är naturligtvis något som måste undersökas vidare. Sådana metoder skulle medföra att sannolikhets-bedömningen i sådana fall skulle kunna integreras för de båda risktyperna. Det skulle även betyda att andra delar skulle vara lättare att integrera. Författarna står dock fast vid att de anser att arbetssätten för att ta fram sannolikheter skiljer sig allt för mycket mellan IEC's och FEMA's modeller, för att de ska vara möjligt att integrera det arbetet.

**Olika riskmått**
I analysen menar författarna att om en integration av antagonistiska och olycks-relaterade risker överhuvudtaget ska vara intressant, måste de integrerade delarna kunna användas i processens nästkommande steg. En integrerad konsekvens-beräkning skulle kunna betyda en höjning av kvaliteten för de antagonistiska riskerna beräknade enligt FEMA's modell, men kan även innebära en sänkning av kvaliteten för de olycksrelaterade beräknade enligt IEC's modell. Vilketdera av dessa alternativ betyder ändå att konsekvensbedömningen inte passar ihop med respektive sannolikhetsbedömning. På så sätt uteblir vinningen med själva integrationen i detta steg. För att lösa problemet måste sannolikhetsbedömningen för både olycksrelaterade och antagonistiska risker bedömas på liknande sätt. Det är dock något författarna tidigare i arbetet inte menar är möjligt.

**Undvikande av intressekonflikter**
Fördelen med en integration av analyserandet av åtgärdsalternativ är att det blir lättare att identifiera möjliga intressekonflikter mellan riskerna, vilka skulle kunna missas om riskerna hanteras var för sig. Vid en analys av åtgärdsalternativen kan det vara av största vikt att ta hänsyn till ifall åtgärderna reducerar eller rentav ökar risker inom andra områden än enbart inom området där analysen sker. Det kan vara

avgörande om en åtgärd kan reducera risker inom flera områden, eftersom nyttan av den åtgärden i så fall blir större än om endast ett riskområde hade tagits i beaktning. Genom att gruppen som tar fram och analyserar åtgärdsalternativen innefattar experter inom både olyckrelaterade och antagonistiska risker bör deras synsätt vidgas. På så sätt blir det lättare för dem att identifiera intressekonflikter än om arbetet utförts skilt för olycksrelaterade och antagonistiska risker, eftersom expertisen då saknas inom det andra området. Ett integrerat arbete gör det möjlig att välja de mest kostnadseffektiva åtgärderna, och det kan därmed hända att alla åtgärder hamnar inom samma område. Denna möjlighet finns inte om åtgärdsprocessen sker var för sig för de båda områdena.

**Skilda tankesätt**
Som nämndes i analysen kan det finnas ett problem i de kompetensskillnader som finns mellan områdena. Det är även något som flera av intervjupersonerna har bedömt som ett problem. Dock skiljer sig uppfattningarna mellan de olika intervjupersonerna. Vissa anser att arbetet kan utföras av samma person, som dock tar hjälp av expertis från respektive område, medan andra anser att traditioner och tankesätt skiljer sig så mycket att de inte kan kombineras. Vissa påpekade även ett problem i att en eventuell integration av kompetensen kan innebära att arbetet fokuseras på endast det område som personen arbetat med innan och att det andra området hanteras på ett dåligt sätt. Erfarenheter från intervjupersonerna visar att så kan vara fallet när någon försöker sig på ett obekant område.

Just problemet med hur fokus läggs på de olika områdena anser författarna även ligga i drivkrafterna. Det kan vara olika mycket krav på de olika områdena från de olika drivkrafterna, vilket kan göra att det arbetet mellan de båda områdena snedfördelas. Problemet kan då vara att risker försummas. Att problemet med att fokus hamnar fel på grund av drivkrafterna var dock inget som intervjupersonerna påpekade. Orsaken till att de inte påpekade detta kan vara att de inte anser att det är så eller att de kanske inte tänkte på det just vid intervjuerna. Vidare undersökningar får visa om det är ett problem eller inte.

**Ramverk för riskhantering**
För att på ett bra sätt samla de risker som finns inom en verksamhet och skapa en övergripande riskbild, har författarna rekommenderat att allt arbete med risker ska utföras i en och samma riskhanteringsprocess. I rapporten studeras COSO's ramverk för ERM, eftersom det är ett övergripande ramverk och är ett verktyg för att uppfylla det amerikanska lagkravet för intern kontroll, The Sarbane's Oxley act. Motsvarande lagkrav finns i Europa i form av Turnball och Kontrag. Författarna kan inte se något problem till att inte hantera alla risker i samma system och då i detta fall COSO's ramverk. Den uppfattningen delas även av de intervjupersoner som har kommenterat ramverket. De anser att COSO's ramverk är så pass flexibelt, att det inte är en nackdel att hantera även antagonistiska risker i ramverket. Fördelarna med det är att det ger ett processtänkande och en tydlig struktur i arbetet. Med ett gemensamt system för att hantera risker på ett företag får beslutsfattarna möjligheten att se en övergripande riskbild för företaget och därmed på ett bättre sätt kunna göra sina beslut. En annan fördel som författarna till rapporten påpekar, är att den allmänna begreppsförvirring som råder inom båda områdena kan begränsas genom att hantera riskerna i ett och samma system, där en enhetlig definition gäller för varje uttryck.

**Gemensamt rapporteringssystem**
I författarnas analys av hur arbetet med de båda risktyperna kan integreras med COSO's ramverk för ERM, identifierade de ett gemensamt rapporteringssystem som en möjlig integrationspunkt för de båda riskerna. Detta är inget som någon intervjuperson tar upp som någon möjlighet, men författarna anser att ett och samma rapporteringssystem skulle underlätta. Detta eftersom det skulle bli lättare för personal att bara hålla reda på ett system där de vet vem de ska vända sig till. För en organisation blir det även lättare att hålla reda på ett system, istället för två. Att rapportera händelser är inget som är riskspecifikt och bör därför kunna ske i samma system.

**Sekretess**
Två av intervjupersonerna tog upp att det kan finnas problem i att det råder stora skillnader i öppenheten runt riskerna. De olycksrelaterade riskerna hanteras så öppet som möjligt, för att kunna göra medarbetare mer vaksamma på riskerna. Det rakt motsatta gäller för de antagonistiska riskerna, där stor sekretess gäller runt riskerna för att inte ett företags svagheter ska hamna i orätta händer. Detta medför naturligtvis problem, eftersom det är svårt att hålla vissa delar av ett integrerat arbete under sekretess. Följden kan bli att allt arbete hanteras under sekretess, vilket kan leda till en försämring av arbetet med olycksrelaterade risker.

**Lära sig av varandra**
Även om det inte går att integrera alla delsteg i riskhanteringsprocessen, anser författarna att det finns lärdomar som kan utnyttjas från respektive område. Till exempel används det flera metoder för att beräkna konsekvenser vid analyserandet av olycksrelaterade risker enligt IEC's modell, vilket skulle kunna utnyttjas vid arbetet med antagonistiska risker enligt FEMA's modell.

**AB Ångpanneföreningen och SecMentor A/S**
Målsättningen med arbetet var att hitta integrationsmöjligheter som kan leda till ett samarbete mellan konsultföretagen AB Ångpanneföreningen och SecMentor A/S. Författarna menar att det finns stora möjligheter för företagen att samarbeta. Till exempel kan den konsekvensanalys som utförs av AB Ångpanneföreningen utnyttjas även av SecMentor A/S, för att undvika att göra en egen. Det skulle medföra en tidsvinst för SecMentor A/S. Det kan även innebära en ökad kvalitet av konsekvensanalysen jämfört med om de utfört den själva. Det kan även finnas nytta med att utföra ett samarbete för att med respektive företags bakgrund och tankesätt kunna utveckla respektive företags analys. Det kan även finnas fördelar i till exempel åtgärdsförslagen, där liknande åtgärder kan slås samman eller åtgärder som motverkar det andra området kan identifieras

Resultatet av ett samarbete mellan konsultfirmorna skulle vara en bredare produktportfölj att erbjuda sina kunder. Författarna menar att det finns goda förutsättningar för ett lyckat samarbete.

**Begreppsförvirring**
Ett problem som finns både inom områdena och mellan dem är att det råder en allmän begreppsförvirring. Det kan orsaka problem inom ett företag. Att säkerhet kan betyda två olika saker gör det svårt att kunna kommunicera ut rätt saker i organisationen. För ett företag finns lösningen i att använda sig av ett och samma

riskhanteringssystem och dess definitioner. Det löser dock inte förvirringen utanför företaget.

**Endast hjälpmedel**
Författarna vill poängtera att IEC's modell för riskhantering, FEMA's modell för hantering av antagonistiska risker och COSO's ramverk för ERM endast ska betraktas som *hjälpmedel* eller *verktyg* som verksamheter använder sig av för att hantera risker. Ingen av modellerna gör anspråk på att vara komplett och garanterar heller inte befrielse av risk bara för att den aktuella modellen används. Det är verksamhetens ansvar att använda tillgängliga hjälpmedel på bästa sätt för att minimera risker och maximera möjligheter.

**Vad säger resultatet?**
Vid en jämförelse mellan komponenterna som användes i analysen och de områden som intervjupersonerna tog upp i intervjuerna, visade det sig att områdena och komponenterna stämmer väl överens. Att intervjupersonerna tar upp samma områden som författarna använder i sin analys tyder på att komponenterna är väsentliga vid en jämförelse av arbetet med antagonistiska och olycksrelaterade risker. Därför anser författarna att resultatet från analysen kan anses vara relevant.

Vid en eventuell användning av resultatet från rapporten är det viktigt att ha i åtanke att det endast är ett underlag för fortsatt arbete. De områden som identifieras som möjliga att integrera måste undersökas vidare. Författarna vill med resultatet endast identifiera de möjligheter och problem som kan finnas vid en eventuell integration av arbetet med olycksrelaterade och antagonistiska risker, utifrån AB Ångpanneföreningens och SecMentor A/S arbetssätt. Därmed är även generaliserbarheten begränsad till de modeller som behandlas i rapporten.

**Förslag till fortsatt arbete**
Utöver de komponenter som används i rapportens analys, tar någon intervjuperson upp att metoder för att utföra sannolikhetsbedömning och konsekvensberäkningar kan orsaka problem, samt att krishanteringen efter en händelse bör vara möjlig att integrera. Dessa områden kan tänkas vara möjliga faktorer som kan utgöra en grund för ett examensarbete.

I denna rapport hanteras endast förebyggande arbete, men ett lämpligt område skulle kunna vara att titta på till exempel krishantering eller potentiell samordning av viktiga stödsystem som ledningssystem, dokumentation och kontrollsystem.

Resultatet från denna rapport bör användas för fortsatta studier. I dessa fortsatta studier bör de identifierade integrationsmöjligheterna undersökas noggrannare. En sådan möjlighet är till exempel att betrakta metoder för att beräkna sannolikhet, konsekvens eller identifiera risker.

Ett förslag är att göra en case-study där en integrerad analys av båda riskerna utförs. Denna case-study kan sedan utvärderas och jämföras med hur riskerna hanteras normalt.

# 10 SLUTSATSER

*I kapitlet redovisas de slutsatser om möjligheter och problem med en integration av antagonistiska risker och olycksrelaterade risker. Dessa slutsatser har dragits från tidigare förd diskussion.*

- ✧ Resultatet från analysen i rapporten, om att *konsekvensberäkningen* har möjlighet att utföras integrerat för olycksrelaterade risker enligt IEC's modell och antagonistiska risker enligt FEMA's modell, överensstämmer med resultatet från intervjuerna. Alla medverkande anser att eftersom vissa händelser genererar liknande händelseförlopp finns det möjlighet för en integration av konsekvensberäkningen.

- ✧ När det gäller *riskresponsen* överensstämmer resultatet från analysen med resultatet från intervjuerna. Det finns en klar uppfattning om att vissa åtgärder går ihop och motverkar båda typerna av risk, varpå det finns möjligheter till ett integrerat arbete.

- ✧ Med undantag från en intervjuperson visar resultatet från intervjuerna tydligt att det är vid *sannolikhetsbedömningen* i riskhanteringsprocessen som de stora problemen med en integration finns. Denna uppfattning är den samma som författarna kom fram till i rapportens analys.

- ✧ Några intervjupersoner har uttryckt problem i att fokus kan hamna fel vid en eventuell integration av olycksrelaterade och antagonistiska risker, eftersom de ansvariga arbetar med det område de kan sedan innan. Denna uppfattning stämmer bra med analysen i rapporten, med undantag från att författarna tror att anledningen även kan vara de skillnader i drivkrafter som identifierats och därmed inte bara kompetensskillnaderna.

- ✧ Vid en integration av hanteringen av antagonistiska och olycksrelaterade risker anser författarna att det kan finnas problem i att de metoder som används inom respektive område endast är validerade för den risktypen. En eventuell integration medför att samma metoder måste användas, vilket orsakar problem eftersom det inte går att säga hur de kommer att fungera för den andra risktypen. Detta är en uppfattning delas av de personer som intervjuats.

- ✧ Författarnas åsikter och resultatet från intervjuerna pekar på att COSO's ramverk för ERM är så pass generellt, att det kan anpassas efter de flesta risktyper. Därmed ses inga problem i att även ta hänsyn till antagonistiska risker i detta ramverk. Ett gemensamt system för att hantera risker på ett företag ger beslutsfattarna en övergripande bild av företagets riskbild och på så vis också ett bättre underlag för att ta beslut.

- ✧ Skillnader i tankesätt vid hanteringen av de olika områdena ses som ett problem av både de intervjuade personerna och författarna till rapporten. Det ger i sin tur problem i ibland annat händelseidentifieringen.

- ✧ Svårigheten i att integrera sannolikhetsbedömningen, med avseende på de olika riskmått och synsätt som tillämpas inom respektive område, innebär att nästkommande steg i processen försvåras. Dock delar författarna de

intervjuade personernas uppfattning att de delar i riskhanteringsprocessen som kan integreras bör integreras.

I rapporten identifieras både möjligheter och problem som bör undersökas mer noggrant. Fortsatt och djupare forskning inom området är önskvärd för att vidare undersöka integrationsmöjligheter och problem med en integration av antagonistiska och olycksrelaterade risker.

# 11 REFERENSLISTA


1 Wulff P., *Hotbilden – slump, antagonism och mittemellan*, Totalförsvarets forskningsinstitut (FOI), 2002.

2 Bouvin F., samordnare Risk- och sårbarhetsanalyser, Krishanteringsenheten, Krisberedskapsmyndigheten (KBM).

3 Hägg M., analytiker, Centrum för asymmetriska hot- och terrorismstudier (CATS), Försvarshögskolan (FHS).

4 Kulling P., *Har hotbilden förändrats? En tillbakablick på katastrofer under 40 år.*, Kungliga vetenskapsakademins handlingar och tidsskrift, 2004.

5 Grimvall G., Jacobsson P., Thedéen T. (Red) *Risker i tekniska system.* Utbildningsradions förlag.Stockholm 1998.

6 ICF, *Risk management framework for hazardous materials transportation*, Virginia, ICF Consulting, 2000.

7 *Kunskap för säkerhets skull. Förslag till en nationell strategi för säkerhetsforskning*, Verket för Innovatonssystem (VINNOVA), 2005.

8 ISO/IEC, *Risk management – Vocabulary – Guidelines for use in standards*, Guide 73, International Organization for Standardization Organisaion & International Electrotechnical Commission, 2002.

9 Kemikontoret, *Riskhantering 3 - Tekniska riskanalsymetoder*, Kemikontoret 2001.

10 *Enterprise Risk Management Framework*, Committee of Sponsoring Organizations of the Treadway Commision (COSO), Draft.

11 Davidsson G., Haeffler L., Ljundman B., Frantzich H., *Handbok för riskanalys*, Räddningsverket, Karlstad 2003.

12 Nilsson J., Hallin P-O. & Olofsson N., *Kommunal sårbarhetsanalys*, Krisberedskapsmyndigheten (KBM), 2004.

13 ISO/IEC, *Safety aspects –Guidelines for their inclusion in standards*, Guide 51, International Organization for Standardization Organisaion & International Electrotechnical Commission, 1999.

14 Institutet för Riskhantering och Säkerhetsanalys, http://www.irisk.se/riskhant.htm, 050613.

15 Carlsson L-O., föreläsningsanteckningar, Riskhanteringsprocessen, Lunds tekniska högskola, 2005.

16 Det nationella biblioteksdatasystemet, LIBRIS, http://websok.libris.kb.se/websearch/form?type=extended, 051101.

17 Lunds Universitets bibliotek, LOVISA, http://lovisa.lub.lu.se/cgi-bin/webgw/chameleon, 051101.

18 Electronic Library Information Navigator, ELIN, http://hugin.lub.lu.se/cgi-bin/pclient?url=http://elin.lub.lu.se:80/elin?lang=se, 051101.

19 *Så vill vi utveckla krisberedskapen*, Krisberedskapsmyndigheten (KBM), 2005.

20 *Hot- och riskrapport 2004 – gränsöverskridande sårbarheter*, Krisberedskapsmyndigheten (KBM), 2005.

21 Totalförsvarets hemsida, www.totalforsvaret.se, 050525.

22 Nationalencyklopedins Internettjänst, sökord ”WTC”, http://80-www.ne.se.ludwig.lub.lu.se/jsp/search/article.jsp?i_art_id=490943&i_word=wtc, 051005.

23 Bilder WTC, http://www.novatv.nl/index.cfm?achtergrond_id=202&fuseaction=achtergronden.details, 050921.

24 Coster M. & Hankin R., *Risk assessment of antagonistic hazards*, Journal of Loss Prevention in the Process Industries 16, 2003.

25 Nationalencyklopedins Internettjänst, sökord ”terrorism”, http://80-www.ne.se.ludwig.lub.lu.se/jsp/search/article.jsp?i_art_id=326201&i_word=terrorism, 051005.

26 RiskNet, Totalförsvarets forskningsinstitut (FOI), http://www.risknet.foi.se/terrorism/, 051005.

27 Nationalencyklopedins Internettjänst, sökord ”organiserad brottslighet”, http://80-www.ne.se.ludwig.lub.lu.se/jsp/search/article.jsp?i_art_id=276801&i_word=organiserad%20brottslighet, 051005.

28 Lund L., Operation Intelligence Manager, SecMentor A/S, 050531.

29 *Reference Manual – to Mitigate Potential Terrorist Attacks Against Buildings*, Federal Emergency Management Agency (FEMA), 2003.

30 Mattsson B., *Riskhantering vid skydd mot olyckor – problemlösning och beslutsfattande*, Räddningsverket, 2000.

31 Norén A., konsult inom teknisk riskhantering, AB Ångpanneföreningen, Malmö, 050928.

32 IEC, *International standard, Part 3: Application guide – Section 9: Risk analysis of techonlogical systems*, International Electrotechnical Commission, 1995.

33 Nystedt F., *Riskanalysmetoder*, Lund, 2000.

34 Nilsson J., *Introduktion till riskanalysmetoder*, Lund, 2003.

35 Abrahamsson M., Magnusson S-E., *Risk och sårbarhetsanalyser - utgångspunkter för fortsatt arbete*, Krisberedskapsmyndigheten (KBM), 2004.

36 DN’s nätupplaga, http://www.svd.se/dynamiskt/inrikes/did_10087307.asp, publicerad 050708, hämtad 051005.

37 Chapman C., *Bringing ERM into focus*, The Internal Auditor; Juni 2003.

38 Moody M., *ERM takes another step forward*, Rough Notes; Oktober 2003.

39 Moody M., *ERM gains traction*, Rough Notes; Mars 2004.

40 Del Bel Belluz D., *Modern risk management*, CA Magazine, November 2002.

41 Deloitte, revisions- och konsultföretag, http://www.deloitte.com/dtt/section_node/0,1042,sid%253D59816,00.html, 051005.

42 *Enterprise Risk Management Framework – Integrated Framework – Executive Summary*, Committee of Sponsoring Organizations of the Treadway Commision (COSO), 2004.

43 Sullivan L., *Defining ERM*, Risk Management, Sep 2003.

44 Siegert R. & Taylor W., *Theoretical aspects of goal-setting and motivation in rehabilitation*, Wellington South, New Zeeland, 2004.

45 Ekonomistyrningsverket (ESV), http://www.esv.se/amnesomraden/verksamhetsstyrning/attsattamal.4.381a53100408a68b1800011.html, 050826.

46 Kolluru R., *Risk Assessment and Management Handbook – for Environmental, Health, and Safety Professionals*, New York, 1995.

47 Akselsson, R., *Människa, teknik, organisation och risk*, Kurslitteratur till kursen MTOR vid Avdelningen för ergonomi och aerosolteknologi, Lunds tekniska högskola, Lund 2002.

48 Folkhälsoinstitutet, www.prevent.se/doc_pdf/prodblad/halsoaffars.pdf, 051006.

49 Jacobsson A., konsult inom teknisk riskhantering, AJ Risk Engineering AB, adjungerad lektor vid Lunds tekniska högskola, 050929.

50 Svensson B., Risk Chief Officer, E.ON Sverige AB, 050927.

51 Carlsson L-O., f.d. medlem i Akzo Nobels internationella management-team för SHM-frågor, pionjär inom integrerad säkerhet, hälsa och miljö, numera pensionär., 051003.

52 Lindgren M., Chef för säkerhet och kvalitet, Preem Petroleum (publ. AB), Preemraff Göteborg, 051005.

53 Harms-Ringdahl L., konsult inom teknisk riskhantering, Institutet för Riskhantering och Säkerhetsanalys, adjungerad professor vid Karlstad universitet, 050929.

54 Larsson L-G., revisor, Rödl & Partner Sverige AB, 050930.

55 Grahn I., Risk management konsult, Ingemar Grahn risk management konsult, 051006.