GÖTEBORGS UNIVERSITET
HANDELSHÖGSKOLAN

Företagsekonomiska institutionen

Inriktning mot Management

Enterprise Risk Management

Hur använder svenska företag ERM?

Kandidatuppsats våren 2012

Pär Berg

Christofer Skoogh

Handledare: Wajda Wikhamn

Förord

Vi vill passa på att tacka de personer som hjälp oss i skrivandet av denna uppsats vårterminen 2012. Vi tackar vår handledare Wajda Wikhamn som med stort engagemang hjälpt oss med förslag på förbättringar och stöttat oss i arbetet. Vi vill också tacka fallorganisationerna som ställt upp på intervjuer samt managementkonsult Peter Findahl som med sin erfarenhet och kunskap i ämnet gett oss värdefulla tips på vägen.

Göteborg, juni 2012

Pär Berg och Christofer Skoogh

Sammanfattning

Titel:	Enterprise Risk Management: Hur använder svenska företag ERM?
Författare:	Pär Berg och Christofer Skoogh
Handledare:	Wajda Wikhamn
Lärosäte:	School of Business, Economics and Law at the University of Gothenburg

Bakgrund: Fler och fler företag arbetar idag med övergripande riskhantering, ofta benämnt Enterprise Risk Management (ERM). Istället för att hantera enskilda risker specifikt på företagets olika avdelningar, sammanställs en konsoliderad riskbild för hela organisationen. På så sätt får företaget en total analys av situationen, där korrelationen mellan olika risker är invägd. ERM syftar också till att fånga de möjligheter som kommer med ett anpassat risktagande. Med bakgrund av detta har COSO lanserat ramverket COSO-ERM, vars mål är att ge vägledning i det ovannämnda det vill säga implementeringsprocessen för att hantera strategiska, operationella, finansiella och legala risker holistiskt över hela organisationen.

Syfte: Författarna syftar i denna uppsats att undersöka hur COSO`s ramverk samt övrig teori runt Enterprise Risk Management korrelerar med den praktiska riskhanteringen i svenska företag. Vidare avser författarna att undersöka om det finns någon diskrepans mellan praktik och teori.

Avgränsning: Denna uppsats presenterar resultatet av hur två undersökta företag på den svenska marknaden arbetar med ERM.

Metod: En kvalitativ fallstudie har utförts på två företag med hjälp av semistrukturerade intervjuer med ett beskrivande syfte.

Struktur: Den första delen innehåller bakgrund, problemdiskussion, frågeställning och syfte, med avsikt att tydliggöra uppsatsens ramar och inriktning samt ge läsaren en inblick i varför ERM är intressant i dagens riskhantering.

I kapitel två presenterar författarna den teorin som ligger till grund för forskningen och ger en inblick i Risk Management, Enterprise Risk

Management och COSO`s kub. Syftet är att skapa en så bred förståelse som möjligt för dessa komplexa koncept.

I det tredje kapitlet presenteras den metod författarna använt för att sammanställa och genomföra uppsatsen. Därtill kommer en kort presentation av fallorganisationernas kärnverksamhet för att läsaren lättare ska förstå riskhanteringen i respektive fallorganisation.

I kapitel fyra presenteras det empiriska materialet som tydliggör hur de utvalda fallorganisationerna arbetar med ERM. Författarna har i denna del valt att ge en övergripande introduktion av de båda fallorganisationernas riskhantering vilken är beskriven utifrån respektive organisations årsredovisning och till viss del intervjuerna. Detta i förhoppning att göra den mer ingående empiriska sammanställningen mer greppbar. Kapitlet är sedan uppdelad i fem block som består av sammanslagningar av de punkter som återfinns i intervjufrågorna (se appendix). Anledningen till att varje specifik fråga från intervjun inte är med är för att författarna anser att det blir för fragmenterat att läsa resultatet och analysen punktat enligt intervjufrågorna och har av de elva punkterna istället valt att arbeta med fem.

I kapitel fem analyseras och diskuteras de empiriska resultaten med den teori som framlagts i kapitel två. Detta görs utifrån samma struktur som i föregående kapitel med fem punkter för att på ett överskådligt sätt kunna följa författarnas resonemang.

I det sjätte kapitlet sammanställs författarnas slutsatser och även en kort diskussion om fortsatt forskning följer.

Resultat: Svenska företag använder ERM och COSO´s verktyg för riskhantering för att få en enhetlig och övergripande hantering av sina risker. I toppen av organisationerna finns tydlig och dokumenterad ansvarsfördelning, processer för rapportering av risker samt en tydlig riskfilosofi. Längre ned i hierarkin blir rollbeskrivningarna mer generella. Företagen anser sig ha fördel av att hantera sina risker övergripande och skaffar sig på detta sätt ett verktyg för att nå sina strategiska mål.

Nyckelord: ERM, Enterprise Risk Management, COSO, Risk Management, CRO

Förkortningar

COSO – Committee of Sponsoring Organizations of the Treadway Commission

CRO – Chief Risk Officer: Chef med det samlade ansvaret för organisationens riskhantering.

ERM – Enterprise Risk Management: Riskhantering ur ett holistiskt perspektiv.

IRM – The Institute of Risk Management

RM – Risk management: Traditionell riskhantering

CIRM – Global Risk & Control Manager (Astra Tech)

EBIT – Earnings Before Interest and Taxes

1 Introduktion

1.1 Bakgrund

Enligt Hoyt & Liebenberg (2011) har intresset för riskhantering och Enterprise Risk Management (ERM) ökat de senaste åren. En effekt av fokuseringen på risker i företagen är att implementering av ERM och Committee of Sponsoring Organizations of the Treadway Commision´s ramverk för riskhantering (COSO) blivit mer utbrett och accepterat bland företag (Power, 2004), (COSO, 2004).

ERM är med sin helhetssyn på hur risker hanteras övergripande i företag en utveckling av Risk Management (RM) som handlade om att hantera finansiell risk och där andra risker, såsom försäkringar och hedging, hanterades separat inom olika områden i företaget. ERM-ramverket syftar till att alla företagens strategiska, operativa och finansiella risker hanteras övergripande och en gemensam riskfilosofi genomsyrar hela organisationen (Beasley & Clune, 2005).

Företagsövergripande riskhantering innebär kort sagt ett stöd för företagen att nå deras verksamhets- och vinstmål samt undvika resursförluster. Alla nivåer inom verksamheten förväntas ta ansvar för riskhanteringen vilket skapar bättre och effektivare beslutsfattandet inom organisationen. Aktieägarnas kapital skyddas också på ett bättre sätt och det medför även en effektivare rapportering samt att lagar och regler följs. Detta kan också anses värdeskapande och ge hållbara konkurrensfördelar genom att det främjar företagets rykte bland intressenterna (COSO, 2004).

Hoyt & Liebenberg (2011) har gjort en undersökning på 177 stycken försäkringsbolag i USA som var verksamma under åren 1995 – 2005 för att undersöka om det finns något samband mellan företag som använder ERM och deras marknadsvärde. I undersökningen används det så kallade Tobins Q som jämför marknadsvärdet på ett företags tillgångar mot, i detta fallet, kostnaden för att införa ERM. Tobins Q tar även med framtida förväntning och värde på ett företag vilket passar en undersökning som undersöker sambandet mellan att införa ERM och värdet på detsamma, då fördelarna av implementeringen inte märks direkt.

Enligt Hoyt & Liebenbergs (2011) undersökning värderas ett företag ungefär 20% högre efter att de implementerat ERM och det visar ett klart samband mellan värdet på ett företag om de arbetar med ERM eller inte. Hoyt & Liebenberg (2011) påpekar också att såvitt dom vet har

inga andra liknande undersökningar gjorts. Författarna till denna uppsats har heller inte hittat liknande undersökningar varför vi utgår från att det finns ett starkt samband mellan ett företags värde och användande av ERM.

Fler och fler företag implementerar ERM i sin verksamhet, konsultbyråer startar speciella avdelningar som enbart arbetar med ERM och ratinginstitut som Standard & Poor har numer med riskhantering som en aspekt när de betygsätter ett företag (Standard & Poor, 2012).

I slutet av 70-talet och början av 80-talet var det många större företag som hade svårt att klara sina finanser och många företag gick även i konkurs där orsaken till detta var bland annat hög inflation och höga räntor men det förekom även tveksamma sätt att sköta företagens redovisning på. Det hände till exempel att företag visade upp positiva årsredovisningar precis innan allvarliga och negativa nyheter för samma företag blev kända. Problemen diskuterades ända upp på kongressnivå i USA och "The National Commission on Fraudent Financial Reporting" bildades för att försöka komma tillrätta med problemen. Fem amerikanska organisationer tog åt sig detta uppdrag: the American Institute of Certified Public Accountants (AICPA), the Institute of Internal Auditors (IIA), the Financial Executives Institute (FEI), the American Accounting Association (AAA) och the Institute of Management Accountants (IMA). Kommittén namngavs efter deras ordförande James C. Treadway till The Committee of Sponsoring Organizations of the Treadway Commission och kallas idag kort och gott för COSO (Moeller, 2007).

I början av 2000-talet ökade intresset för COSO åter igen då världen fick uppleva några stora företagsskandaler. Ett exempel på detta är konkursen av Worldcom där undermålig, och till och med fusk i den finansiella rapportering i redovisningen ledde till konkurs vilken drabbade de anställda och investerare hårt (Jones, 2011).

Som en reaktion på detta stiftades en ny lag i USA, Sarbanes-Oxley Act, förkortad SOX. Det huvudsakliga syftet med SOX var att öka öppenheten och ansvaret i bokföringen genom att reglera den interna kontrollen för bolagsbeskattningen och den finansiella rapporteringen. De företag som är noterade på någon av USA aktiemarknader, som till exempel NASDAQ och AMEX, eller har mer än 300 amerikanska aktieägare tvingas att redovisa sina risker. Det är bland annat av den anledningen många företag i USA har valt att implementera ERM-ramverket. Genom att implementera ERM skapar företagen ett system för att hantera alla slags risker på varje nivå i organisationen med målet att minska den totala riskexponering, få en bättre överblick över riskerna och hur de kan hanteras. Fördelar med ERM är även att kunna utnyttja möjligheter med risker som kan vara lönsamma (Gordon et al. 2009).

Koden för Svensk bolagsstyrning kan beskrivas som den svenska motsvarigheten till SOX men används mer som riktlinjer än en tvingande lag. Inom EU finns regelverken Basel III för bankerna och Solvens II för försäkringsbolagen som de måste rätta sig efter för att minska den finansiella risken. Basel III syftar till att stärka bankernas förmåga att motstå förluster och nya finansiella kriser genom att kräva att bankerna måste ha en viss nivå kapital, att vad som får räknas in i kapitalet skärps (Goodwill får exempelvis inte räknas med i kapitalet på samma sätt som innan) och att reglerna för beräkningen av tillgångar skärps. (Riksbanken)

Företag som är noterade på den svenska aktiemarknaden måste också enligt ÅRL lämna upplysningar I bolagsstyrningsrapporten om bolagens system för hur de hanterar intern kontroll och riskhantering i den finansiella rapporteringen (Deloitte, 2012).

1.2 Problemdiskussion

> *Företagsövergripande riskhantering är en process som genomförs av en organisations styrelse, ledning och annan personal, och som genomförs i ett strategiskt sammanhang och över hela företaget, utformad för att identifiera potentiella händelser som kan påverka organisationen och hantera risker inom ramen för dess riskaptit och ge rimlig försäkran om att organisationens mål uppnås.*
> (COSO, u.d. s.6)

ERM underlättar beslutsfattandet om strategiska åtgärder och att dessa tas i linje med att företagets mål ska kunna uppfyllas. Att kunna identifiera risker och möjligheter kan också vara värdeskapande för företagets intressenter samt skydda aktieägarnas kapital (COSO, 2004).

Sverige har som sagt i dagsläget inga lagar som tvingar företag att ha system för exempelvis intern kontroll, riskhantering och finansiell rapportering utan använder sig av ”koden för svensk bolagsstyrning” som anger en norm för god bolagsstyrning på en högre ambitionsnivå (Kollegiet för svensk bolagsstyrning, 2010).

Till skillnad från Sverige har USA SOX-lagen som syftar till att säkerställa att bokföringen sköts på rätt sätt genom regler för bolagsbeskattningen och den finansiella rapporteringen. Tyskland har idag en liknande lag, KonTraG, som innebär att företag måste införa ett system för riskhantering och intern kontroll och som även ska finnas med i bolagens årsredovisning (von Grebmer, 2007).

För att kunna fatta väl avvägda beslut i en riskhanteringsprocess krävs en solid grund för hantering och insamling av data relaterad till risk och finansiering, samt att systemen kan analysera och tolka komplexa riskmodeller. Vidare bör organisationen för att identifiera risker, exempelvis utföra workshops med personal i nära anslutning till det operativa arbetet. Enhetschefer är enligt teorin den kategori av individer i organisationen som främst sitter på information om kritiska riskfaktorer, då de agerar i närheten av och således har information om marknaden, trender, konkurrenter och vad kunderna efterfrågar (Mauer, 2009).

Risker ska identifieras på varje nivå i organisationen och därefter skapas processer för att hantera dessa och en dokumenterad riskpolicy bör finnas som grund i denna process, samt formella roller för att kunna utföra en systematisk hantering av riskerna (Daukant & Hirst, 2009).

Relevanta risker sammanställs till en konsoliderad riskrapport för vidare distribution till organisationens ledning. Rapporten utgör ett viktigt underlag för de strategiska besluten. En av grundbultarna i ERM är att kunna leverera adekvat information till rätt individer om hot och möjligheter i takt med att de uppstår. Lyckas man implementera detta på rätt sätt, blir ERM ett mycket kraftfullt verktyg för organisationen. ERM beskrivs i teorin som ett ramverk för alla typer av organisationer då riskerna ofta är samma oavsett form och storlek på företaget (Hoyt & Liebenberg, 2011). Att implementera ERM i varje affärsprocess är dock ett kostsamt och tidskrävande arbete. Ett alternativ är att använda sig av funktionsövergripande ERM, där man istället för att ha en integrerad riskhantering i varje affärsprocess, identifierar risk övergripande i företagets olika enheter. Detta innebär att riskhanteringsprocessen blir mer centraliserad, mindre delegerad samt formella roller saknas och mer ansvar vilar hos berörd enhets- eller avdelningschef (Findahl, 2012).

Mot bakgrund av ovanstående ämnar författarna utröna hur den praktiska tillämpningen av ERM ser ut i svenska företag. Vilka är motiven till användandet av ERM? Arbetar man mer övergripande eller är ERM integrerad i varje affärsprocess? Det har gjorts få empiriska studier på hur man använder ERM i Svenska företag och hur lösningarna ser ut i praktiken.

Då det är en komplicerad och lång implementeringsprocess ställer vi oss frågan hur man tacklar denna komplexitet och hur väl det verkliga användandet speglar teorin av ramverket. Denna diskussion har lett oss fram till uppsatsens frågeställning.

1.3 Frågeställning

Hur använder svenska företag ERM?

För att få en översiktlig och mer hanterbar bild för läsaren över hur företagen arbetar med ERM har vi skapat två underfrågor.

- Vilka är motiven till användandet av ERM?
- Arbetar man mer övergripande eller är ERM integrerad i varje affärsprocess?

1.4 Syfte

Författarna syftar i denna uppsats att undersöka hur COSO`s ramverk samt övrig teori runt Enterprise Risk Management korrelerar med den praktiska riskhanteringen i svenska företag. Vidare avser författarna att undersöka om det finns någon diskrepans mellan praktik och teori och i så fall motiven till detta.

1.5 Avgränsningar

Författarna i denna uppsats har valt att undersöka hur svenska företag använder ERM i praktiken, hur företagen har utformat interkontrollen runt ERM samt hur detta rapporteras. Eftersom konceptet enligt teorin är applicerbart på alla organisationer oavsett typ och storlek (COSO, 2004) har inget urval gjorts på denna grund. Det har heller inte gjorts någon skillnad mellan finansiella eller icke finansiella företag då vår frågeställning endast berör hur organisationer använder ERM. Urvalet har grundats på att företagen använder riskhantering ur ett holistiskt perspektiv.

2 Teoretisk referensram

2.1 Definition av risk

> Traditional *cultures didn´t have a concept of risk because they didn´t need one. Risk isn´t the same as hazard or danger. Risk refers to hazards that are actively assessed in relation to future possibilities. It comes into wide usage only in a society that is future oriented - which sees the future precisely as a territory to be conquered or colonised. Risk presumes a society that actively tries to break break away from its past - the prime characteristic, indeed, of modern industrial civilisation.* (Giddens, 1999 s.22)

Enligt Giddens (1999) har han inte hittat några relevanta bevis på begreppet risk före femton- och sextonhundratalet. Begreppet risk började då användas av upptäcksresande från västvärlden som seglade runt på världshaven. Ordet risk kommer troligtvis från det engelska eller portugisiska språket och betydde då något i stil med att segla ut på okänt vatten. Vidare menar han också att ordet risk borde ha ett samband med någon form av utrymme. I modernare tid när ordet används till exempel inom finansbranschen innefattar betydelsen tid och syftar då på uppskattningen av, eller sannolika utfall för låntagare och långivare. Det finns två sidor av risk, antingen en positiv eller ett negativ effekt och denna indelning kan härledas till i början av industrisamhället. Risk är något som samhället vill kontrollera och det finns en strävan efter att försöka styra sin framtid istället för att lämna den åt slumpen (Giddens, 1999).

Enligt Erikssson Zetterquist (2009) används begreppet “Risk Management” för att hantera och förhoppningsvis kunna handskas med exempelvis hot och oförutsedda händelser och begreppet “Risk” kommer ifrån möjligheten att beräkna sannolika resultat (Eriksson Zetterquist, 2009).

Det finns också skillnader mellan risk och osäkerhet enligt Knight (1921), där han i sin bok skiljer dem åt genom att osäkerhet inte kan kontrolleras medan risk är kalkylerbart. Vidare menar Knight att risken kan minskas beroende på hur väl osäkerheten hanteras. Praktisk skillnad på risk och osäkerhet definieras som att risk i viss mån är möjlig att räkna på och mäta samt kan estimeras av erfarenhet medan osäkerhet inte kan uppskattas på samma sätt då det är en ny situation vi ställs inför (Knight, 1921).

Likt Giddens (1999), blir utfallet av ett risktagande enligt Hopkins (2010) antingen en positivt eller negativ effekt, men kan även resultera i osäkerhet. Därför kan risk helt enkelt innebära en möjlighet, en förlust eller en ökad osäkerhet för ett företag. Varje typ av risk ska analyseras och hanteras var för sig för bästa möjliga resultat. Hopkins (2010) delar upp risker i tre kategorier som också ISO Guide 73/ISO 31000 gör:

- Faror, eller rena risker (hazard or pure risks)
- Osäkra risker (control or uncertainty risks)
- Risker med möjligheter (opportunity or speculative risks)

Överlag pratar man oftast antingen om faror eller risker med möjligheter, nummer ett och tre i punkterna ovan, och enligt Hopkins (2010) förs det en del diskussioner om själva terminologin inom risk management. Dock är det viktigaste att de organisationer som väljer att implementera någon form av riskhanteringssystem i praktiken använder det system som passar bäst för just deras verksamhet.

Det finns risker som endast kan mynna ut i negativa effekter och dessa är faror eller osäkra risker. Sådana risker klassificeras oftast som operationella eller risker företagen kan försäkra sig mot, exempelvis stöld.

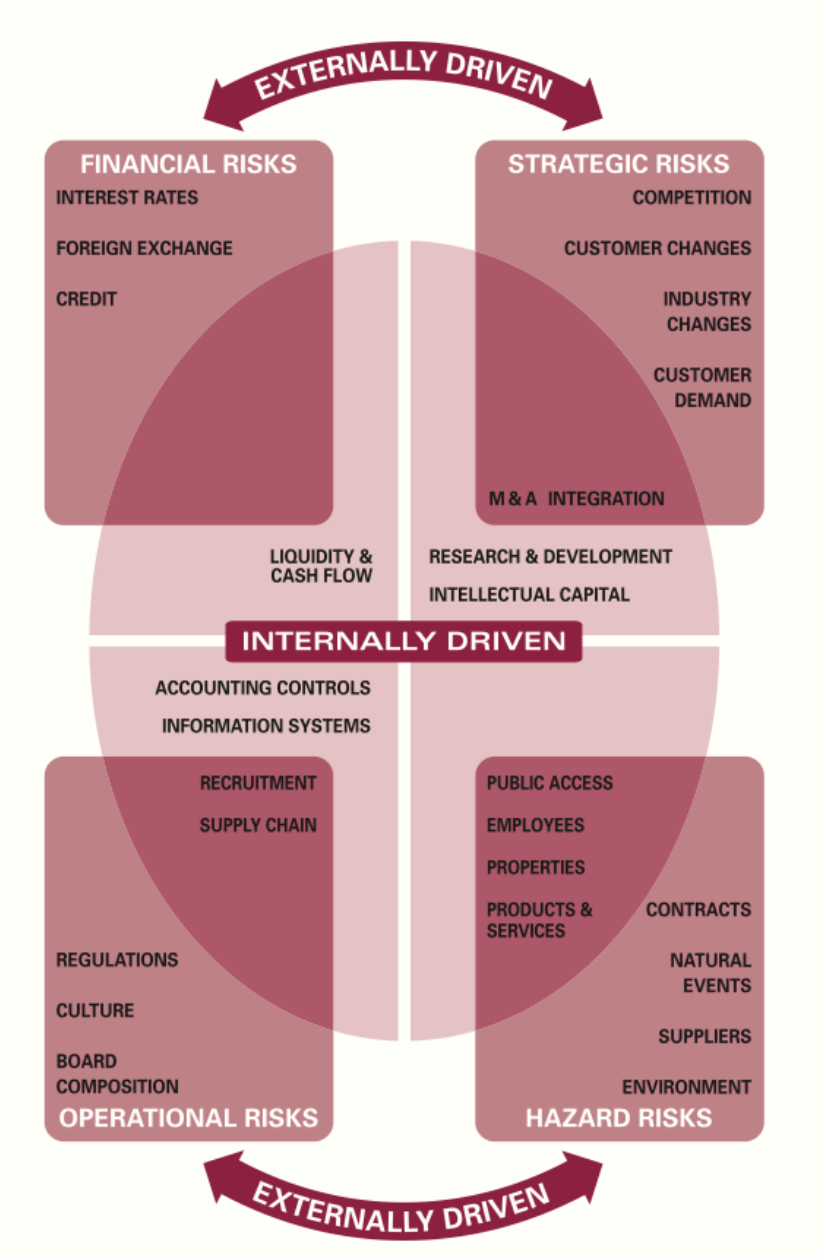
De risker som är osäkra, alltså ger upphov till osäkerhet, finner man oftast i samband med projektledning. Osäkerheten kan kopplas ihop med vad företaget kan vinna på ett visst projekt och detta ställs då emot att projektet blir färdigt i tid, att budgeten hålls och att projektet levereras på det sättet kunden eller beställaren önskade från första början.

Risker med möjligheter, som står sist bland punkterna ovan, är de risker som företagen väljer själva att ta för att förhoppningsvis ge ett positivt utfall. Detta hänger också ihop med riskbenägenhet eller riskaptiten en organisation har. Kort sagt så bestämmer företagen på förhand hur mycket de väljer att spekulera och ta risker utan att det kan skada företagets verksamhet långsiktigt och att gällande strategiska mål efterföljs (Hopkins, 2010).

2.1.2 Interna och externa faktorer

Organisationer och företag påverkas av risker både från sin omvärld, så kallade externa faktorer, och från den interna verksamheten. The Institute of Risk Management (IRM) har tagit fram en modell (se figur 1) av de viktigaste interna och externa riskerna där det tydligt framgår att vissa av riskerna dock kan ha både interna och externa orsaker och därför överlappar varandra.

Figur 1



Figur 1, (IRM, 2002)

De interna risker kan sägas vara specifika för just ett företag och hanteringen av dem blir lättare för de ansvariga än om man jämför med de externa som inte är lika lätta att påverka.

Även om många företag på marknaden liknar varandra i sitt sätt att arbeta är den stora utmaningen för företagen att hantera både de interna och externa riskerna men även kombinationen av dem som kan uppstå. ERM och COSO-verktyget kan då hjälpa företagen att agera proaktivt så att en risk som upptäcks idag inte blir ett framtida problem utan hanteras direkt.

2.2 Riskhantering

Författarna avser med detta kapitel kort beskriva hur ERM har vuxit fram men även ge en övergripande bild och teoretiska motiv till att införa ERM. Då ERM är tätt sammanlänkat med Risk Management (RM) väljer författarna att inleda med en beskrivning av detta koncept, samt visa på skillnader dem emellan, för att skapa ytterligare klarhet för läsaren.

2.2.1 Risk Management (RM)

Stickel (2001) hävdar att risk management handlar om att minimera osäkerheter. Servaes & Tufano (2009) menar att RM kan identifiera värdeskapande nyckelfaktorer och där igenom skapa en fördelaktig position för organisationen.

Traditionellt har risk management varit en reaktiv process fragmenterat över organisationen. Detta liknas ibland vid att organisationen agerar inom funktionsbaserade silos där varje del agerar odynamiskt utan att interagera med organisationens övriga delar (Mauer, 2009). RM-funktionen går ut på att utveckla och implementera processer som minimerar uppkomsten av förluster och minimera den finansiella påverkan av förluster som faktiskt uppstår (Vaughan, 1997), (Mossa, 2007).

Ett problem kopplat till RM är att när man statiskt arbetar för att minimera och undvika risk kan organisationen gå miste om de möjligheter till värdeskapande som kommer med risktagande (Besley & Ghatak, 2005).

2.2.2 Enterprise Risk Management (ERM)

På senare tid har koncept som aggregerar risker från alla nivåer i organisationen och skapar en holistisk bild av risk fått ett starkt momentum.

"ERM has rapidly emerged as the new paradigm for managing the complex portfolio of risks facing an enterprise."

(Tufano, 1996)*;* (Liebenberg & Hoyt, 2003)*;* (Beasley & Clune, 2005)*;* (Slywotzky & Drzik, 2005)*.* Se (Mauer 2009 s.13).

I dess kölvatten kommer koncept som COSO's ramverk vilket denna rapport blickar närmare på. Företag måste alltid hantera risk i sina affärsbeslut. Den främsta nyttan med ERM är enligt (Cumming & Hirtle, 2001), (Lam. 2001), (Meulbroek, 2002) att den minskar volatiliteten i företagets kapitalisering på aktiemarknaden, att det blir billigare att ta upp lån, avkastningen ökar på sysselsatt kapital samt att ERM skapar synergier mellan olika riskhanteringsaktiviteter.

ERM handlar inte bara om att undvika eller reducera risker utan skapar även kännedom om organisationens nyckelkompetens, styrkor och levererar tydliga beslutsunderlag. Detta underlättar för ledningen att aktivt jobba med, och utnyttja uppsidan med de typer av risk där företaget är konkurrenskraftigt. Organisationen kan på så sätt säkra sin tillväxt med ett väl avvägt risktagande.

"We have seen, then, that risk is an inescapable part of doing business and argued that a business should strive toward its optimal risk/return profile." (Lam, 2003 s.7)

2.2.3 Framväxten av Enterprise Risk Management

Att identifiera och prioritera risk är inget nytt koncept och att sprida risk genom försäkringar och andra finansiella produkter är ett väl vedertaget sätt att skydda sig mot risk. Vad som har ändrats med ERM är att alla risker hanteras holistiskt och att riskhanteringen sker på en högre nivå (CAS, 2003).

Anledningen till att fler organisationer implementerar ERM tillskrivs till stor del uppkomsten av Sarbanes-Oxley Act 2002, som reglerar hur listade bolag på NYSE och NASDAQ i USA sköter sin finansiella rapportering. Tanken med regelverket är att förbättra insynen i

företagens finansiella rapportering och ställning (Moeller, 2007). En intilliggande förklaring är också skandalerna i bland andra Berings Bank, Enron och WorldCom som anses ha bidragit till spridningen av ERM (Flyvbjerg et al., 2003). Shenkir & Walker (2006) menar att företag idag möter en allt större komplexitet i den interna och externa kontexten till följd av ökad globalisering, snabbare teknologisk utveckling samt stora mängder information som måste samlas in och tolkas korrekt. Organisationer som inte kan hantera denna komplexitet i en föränderlig värld kommer att lida ekonomiska förluster och således förlora konkurrenskraft. Ovan nämnda anledningar kan ses som bakomliggande faktorer och pådrivande i utvecklingen av ERM.

2.2.4 Enterprise Risk Management som strategi

> *”RM is not just about using derivatives to manage interests rate and foreign exchange exposures – its about using a portfolio approach to manage the full range of risk faced by an enterprise.”* (Lam, 2003, s.4)

Lam (2003) menar att varje företag borde implementera en holistisk riskhantering. Detta för att kunna kontrollera och hantera alla aspekter av risk från alla delar av organisationen och att man där igenom kan optimera förhållandet mellan risk och avkastning.

För att förstå portföljens risker måste man förstå risken i varje individuell del av organisationen samt hur interaktionen dem emellan påverkar den totala riskbilden (CAS, 2003). Vidare menar Lam (2003) att detta är nödvändigt då risker är beroende av varandra. Att då hantera risker isolerat som traditionell RM kan leda till att ett agerande nollställer ett annat, eller i värsta fall ge ett kontraproduktivt resultat.

Låt oss beskriva ett förenklat exempel på detta; ponera att ett europeiskt bolag står i begrepp att göra en större investering som ska betalas i US-dollar. För att skydda sig mot eventuella valutafluktuationer köper finansavdelningen på sig US-dollar samtidigt som försäljningsavdelningen får betalt för sina tjänster samma valuta. Detta agerande leder då till att företaget får en överexponering av den aktuella valutan. Hade istället de olika avdelningarna interagerat med varandra hade man upptäckt denna risk och agerat annorlunda.

Konceptet ERM handlar alltså om att ge företagsledningen en övergripande bild av de risker och möjligheter organisationen möter i den interna och externa kontexten. Tanken är att det ska ge ledningen ett bättre underlag för styrning av verksamheten. Den övergripande riskbilden sammanställs genom att man konsoliderar företagets samtliga risker i en rapport som sedan lämnas över till ledningen. Processen ska vara kontinuerlig och flexibel då den kontext ett företag befinner sig i är under ständig förändring vilket kräver att ERM-processerna följer den utvecklingen och transformeras. Det är också viktigt att initiativtagandet kommer uppifrån och trycks nedåt och ut i alla delar av organisationen (Nocco & Stulz, 2006) samt utgör en naturlig del av företagets riskkultur (Lam, 2003).

2.3 Affärsmodell

I teorin och praktiken är affärsmodell ett brett begrepp, det finns ingen explicit beskrivning av vad en affärsmodell är. För att försöka skapa klarhet i detta börjar Shafer et al (Shafer, Smith, & Linder, 2005) med att bena ut vad en affär är och definierar det som ett agerande som syftar till att skapa värde samt att få avkastning från det skapade värdet, där en modell är en representation av verkligheten. Genom att kombinera dessa koncept kan vi definiera affärsmodellen som en representation av ett företags underliggande kärnvärden och strategiska val för att skapa värde och avkastning. Begreppsparet ”avkastning från det skapade värdet” syftar att beskriva det fundamentala förhållandet att företag måste vara effektiva för att överleva genom att till exempel differentiera sig från konkurrenter. Detta kan göras genom att utveckla nyckelresurser och kärnkompetens, för att skapa produkter och tjänster med premiumvärde.

Osterwalder (2010) är kanske något tydligare i sin beskrivning, då han menar att en affärsmodell utgör grunden för hur en organisation skapar, levererar och bibehåller värde. Och vidare att affärsmodellen utgör en karta för hur strategierna ska implementeras i organisationens struktur, processer och system.

En affärsmodell ska inte förväxlas med ett företags strategi utan syftar till att analysera, testa och validera de strategiska val ett företag ämnar göra, samt belysa operationella komplikationer som följer av dessa, men är alltså i sig inte en strategi. En väl anpassad affärsmodell kan fungera som ett kraftfullt redskap för en organisation men om man utformar affärsmodellen efter bristfällig eller undermålig affärslogik kan detta leda till att användandet blir verkningslöst eller till och med kontraproduktivt (Shafer, Smith, & Linder, 2005).

2.4 COSO-ERM

COSO (Committee of Sponsoring Organizations of the Treadway Commission) Inledde 2001 ett projekt med PricewaterhouseCoopers för att ta fram ett ramverk i syfte att standardisera och systematisera den integrerade riskhanteringen samt skapa en allmän terminologi och definition kring ERM (B & Hertiger, 2005 Winter). År 2004 Lanserade COSO sitt ramverk med målet att hantera alla typer av risk (Strategiska, operativa, finansiella och legala) (Sullivan, 2003) samt att förse ledningen med en sammantagen riskbild som därigenom lättare ska kunna fatta strategiska beslut (Lam, 2003).

COSO ERM föregicks av ett tidigare ramverk från COSO som endast omfattade intern kontroll. Det som skiljer dem åt är framförallt att i COSO´s senare ramverk har man lagt till strategi som ett nytt element. Detta framgår tydligt då interaktionen mellan strategi, mål och risk är en fundamental del av konceptet. Nytt är dessutom att COSO´s senare ramverk har breddat riskfokus och går utanför den interna kontrollen för att skapa en bättre helhetsbild av risk (COSO, 2004).

COSO's ramverk ska användas genom hela organisationen på alla nivåer där definitionen är bred för att kunna passa in i så många organisationer som möjlig. Tanken är att kunna hantera risk proaktivt och företagsövergripande samt att det kopplar samman strategi och risk genom att man agerar utifrån den riskbenägenhet, även kallad riskaptit, ledningen har satt som rimlig. Vidare förser ERM kontinuerligt ledningen med information om företagets prestationer och hur dessa korrelerar med bestämda finansiella och strategiska mål. Denna kontroll ger företagsledningen en tydlig nulägesbild av situationen och en försäkran om att företagets tillväxt och avkastningsmål uppfylls. Överblicken ger således möjlighet att på rätt grunder agera och korrigera processer om så behövs till skillnad från tidigare RM-koncept där man reagerat först när skadan uppstått (Moeller, 2007).

Styrelsen och VD'n har det övergripande ansvaret men det är fundamentalt att alla inom organisationen blir en del av riskkulturen och dess processer. Ramverket föreslår även att en Chief Risk Officer (CRO) tillsätts med ett explicit ansvar för riskarbetet i organisationen. Fundamentala begrepp med ERM är enligt COSO's ramverk att det är en integrerad process i företaget och inte något som sker som en enstaka händelse (COSO, 2004).

- 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.

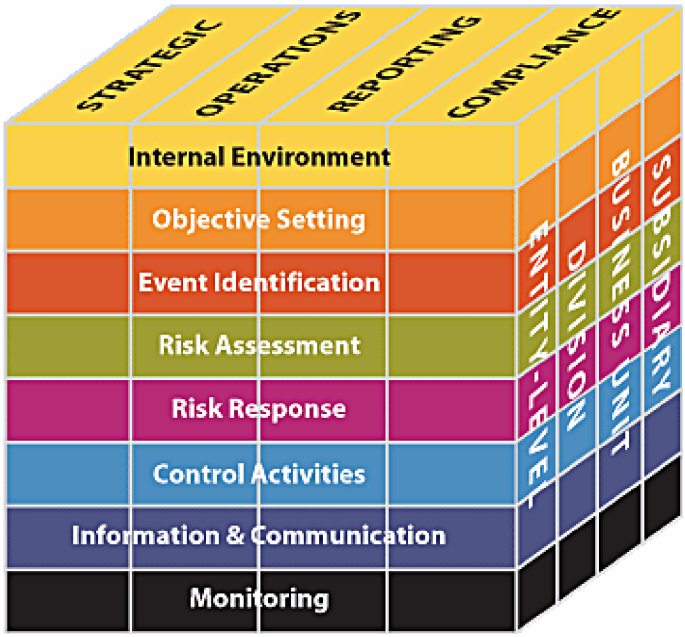
2.5 COSO-kuben

COSO's ramverk är ofta visualiserat som en tredimensionell matris också känd som COSO-kuben. Kuben är indelad i tre huvuddelar (de tre sidorna på kuben). På toppen av kuben återfinns fyra kategorier som innefattar företagets inriktning och mål, dessa står i relation till de åtta sammanlänkade elementen för riskhantering som finns på framsidan av kuben.

"There is a direct relationship between objectives, which are what an entity strives to achieve, and enterprise risk management components, which represent what is needed to achieve them" (COSO, 2004).

På den högra sidan finner vi de olika nivåerna i en organisation. (Se figur 2)

Figur 2



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 (COSO, 2004).

2.5.1 Kategorier

Här finns organisationens mål indelade i fyra kategorier: strategiska, operativa, rapporteringskrav och efterlevnadskrav. Det är inom dessa fyra områden som risker uppstår. För att effektivt kunna hantera dessa risker ska de åtta elementen i ramverket vara implementerade och risken ska hanteras i enlighet med företagets riskbenägenhet på alla nivåer i organisationen (COSO, 2004).

Strategic (Strategiska)

Högt satta mål i linje med organisationens uppdrag, de strategiska faktorerna är samma faktorer som har identifierats som kritiska för att företaget ska vara framgångsrikt. Till exempel bibehålla företagets teknologiska försprång.

Operations (Handling)

Hur effektivt använder organisationen sina resurser, personal, IT-system etc. De kortsiktiga målen och de operativa utmaningar som följer med dessa kan vara mer känsliga för riskhantering. Ett operativt mål kan till exempel vara att hålla nere antalet övertidstimmar till mindre än 3 % av den totalt arbetade tiden. Dessa kortsiktiga mål behöver nödvändigtvis inte påverka de långsiktiga målen. Men de är ändå mycket viktiga, för det är handlingar som påverkar organisationens lönsamhet.

Reporting (Rapportering)

Tillförlitligheten i den interna och externa rapporteringen är mycket viktig för att säkerställa att nyckelindikatorer mäts och övervakas så att ledningen kan vidta åtgärder då de finner detta nödvändigt. Externrapportering ger organisationens intressenter en klar bild av dess prestationer.

Compliance (efterlevnad)

Försäkran om att organisationen efterlever de lagar och restriktioner den lyder under.

2.5.2 Element

2.5.2.1 Internal Environment (Internmiljön)

Alla byggnader behöver en solid grund och i COSO's ramverk är utgörs den av "Interna miljön" (Mauer, 2009).

Internmiljön är startpunkten för den interna kontrollen och utgör grunden för hur organisationen ser på och hanterar risk, detta påverkar således hur företaget sätter strategier och mål. Företaget måste ha en organisationsstruktur som backar upp den riskfilosofi och riskkultur som kommunicerats av företagsledningen. Riskfilosofin ska svara för intressenternas riskbenägenhet samt organisationens strategiska mål, detta påverkar i sin tur vilka risker man tar i affärsprocesserna. En annan viktig del i den interna miljön är organisationens etiska värderingar, ledarstil, kompetens och HRM. Här sätts även de formella rollerna vem som har befogenheter att ta risker och hur åtgärderna ser ut om någon överskrider sina befogenheter etc. Internmiljön skapar även regler och struktur för övriga komponenter av ERM (Moeller, 2007) För att få en bättre överblick kan man dela in internmiljön i åtta underkategorier enl. följande; (Cook, B, 2012)

1. Ledningens riskfilosofi omfattar vilka attityder och vilken syn företaget har på risktagande när man gör affärer. Är risktagandet väl dokumenterat genom riskpolicys och andra dokument där det till exempel framgår vilka risker en person får ta, eller låter man detta ske på magkänsla.

2. Den mängd risk ett företag är villigt att acceptera för att generera avkastning till sina ägare, så kallad riskbenägenhet eller riskaptit. Konceptet ERM handlar om att skapa värde för aktieägarna genom att optimera tradeoff mellan risk och avkastning och därigenom maximera värdet på företaget (Nocco & Stulz, 2006).

3. Styrelsen har översikten över företaget och ska utmana ledningens strategier. För att kunna göra detta på ett effektivt sätt måste styrelsen ha tillräcklig kompetens inom området.

4. Etiska värderingar. Vilka värderingar står organisationen för och hur agerar organisationen när dessa inte efterlevs.

5. Kompetens. Organisationen måste ha kunskapen och kompetensen som krävs för att uppfylla de mål och krav som ställs. Ledningen måste dessutom ha förmågan att ta tillvara på kompetensen.

6. Organisationsstruktur. Hur är organisationen strukturerad, centraliserad eller decentraliserad där den förra standardiserar medan den senare blir delegerande. Det finns inget rätt eller fel här, men under olika omständigheter kan det ena sättet fungera bättre än det andra.

7. Ansvarsdelegering. I vilken grad använder sig organisationen av ”empowerment”.

8. HRM. Hur tar man han om sin personal. ”Risk management is not only about establishing the right control systems and processes – it is also about having the right people and risk culture.” (Lam J. , 2003)

Objective Settings (Målsättning)

Målsättning innefattar processen med att sätta upp organisationens strategiska mål i linje med företagets vision och dessa mål sätts utifrån företagets riskbenägenhet (Moeller, 2007). Mål och strategier måste vara utstakade för att företaget ska kunna identifiera hot och möjligheter som kan komma i dess väg i både den interna och externa kontexten. Vidare får organisationen genom sin målsättning möjlighet att identifiera mätbara faktorer för att bedöma för hur effektivt man når uppsatta mål. Det är också viktigt att personalen tar del av organisationens mål och hörsammar dessa och även förstår hur deras enskilda handlingar påverkar uppfyllandet av organisationens mål. ERM (COSO) är ett verktyg för ledningen att skapa mål som speglar företagets vision. Att sätta mål som är i linje med och underbygger företagets strategier är essentiellt för att lyckas (Moeller, 2007). För att underlätta denna process och ge ledningen möjlighet att fokusera delas målen upp i fyra delar. Dessa kategorier återfinns på COSO-kubens topp och är följande;

1. Strategi (Strategic)
2. Handling (Operations)
3. Rapportering (Reporting)
4. Eftergivenhet - Efterlevnad av lagar och regler (Compliance)

Adekvat och korrekt rapportering ger ledningen goda möjligheter att övervaka organisationens processer, prestationer och att man når uppsatta mål.

Det är viktigt att sätta relevanta och tydliga mål för organisationer i deras strategiska arbete och dessa får inte grundas på vaga eller allmänna antaganden. S.M.A.R.T.-kriterierna är en bra grund att utgå ifrån för att säkerställa att målen är relevanta (Forsyth, 2010).

- Specifikt: Det ska ges en klar bild av vad som ska uppnås
- Mätbart: Mål kan alltid mätas men det är viktigt att det framgår vad som ska mätas, om det är kostnad, tid, kvalitet etc.
- Accepterat: De som ska uppfylla målen måste förstå relevansen av vad de gör.
- Realistiskt: Det ska vara möjligt att uppnå målet.
- Tidsbundet: Det ska finnas en tydlig deadline och prioritering för målet.

Event identifikation (Händelseidentifiering)

Hur till vida ett företag når sina mål eller ej påverkas av många faktorer där man kan dela upp dessa i interna och externa händelser som måste identifieras. COSO's ramverk har valt att göra skillnad mellan händelser med positiva konsekvenser och negativa konsekvenser där den senare klassificeras som risk medan den förra ses i egenskap av möjligheter och bör kommuniceras till ledningen för att bli en del av framtida strategier och planer (Bowling & Rieger, 2005).

Externa faktorer som påverka företagets prestationer är bland annat ekonomiska, politiska, sociala och teknisk utveckling. Medan inre faktorer bland annat utgörs av personal och arbetsprocesser. Ramverket understryker även vikten av att använda sig av de fyra riskkategorierna (strategi, operationella, rapportering och efterlevnadskrav) för att övergripande identifiera risker. Användandet av dessa fyra kategorier i riskidentifieringsarbetet understryker kollaborationen mellan riskhantering och målsättning.

Identifieringsprocessen kan ske genom kontinuerlig och systematisk kontroll i företagets olika processer eller så sker den mer funktionsövergripande. Den senare varianten görs genom t.ex. självutvärderingar eller workshops, där man bildar grupper som kan kombinera erfarenhet och kunskap för att lyfta fram potentiella risker från de olika delarna av organisationen. Detta görs vanligtvis några gånger per år, ofta i samband med kvartalsrapportering. Gemensamt för de båda handlingssätten är att de syftar till att ge

ledningen en bättre förståelse för hur de olika riskerna korrelerar, vilket förenklar arbetet med den totala riskbedömningen.

Risk assement (Riskbedömning)

Här bedöms hur potentiella risker är utifrån två variabler, hur sannolikt är det och vilka blir konsekvenserna om en specifik händelse inträffar. Här skattas risken i förhållande till de mål som hotas och det är även essentiellt att bedöma hur olika risker interagerar och inte bara titta på riskerna var för sig, då den sammanslagna risken kan ge en helt annan bild än att titta på enstaka händelser. Dessa två event kan bedömas genom en kvantitativ eller kvalitativ analys. För att kunna bedöma en händelse analyseras intern, och/eller externt framtagen data. Fördelen med den senare är att man minskar risken för subjektiv bedömning, då den externt framtagna datan i mindre grad speglar den specifika verksamheten (Moeller, 2007).

Response (Riskrespons)

Efter analys ska ledningen fatta beslut om åtgärder för att hantera riskerna, antingen uppåt (om man vill ta mer risk) eller nedåt (för att minska företagets exponering mot den aktuella risken) så att företagets agerande speglar den av styrelsen satta riskbenägenheten. Man kan säga att det är i detta steg riskhanteringen sker, då det är här man beslutar hur organisationen ska bemöta de identifierade riskerna.

Det finns fyra sätt ledningen kan bemöta identifierade risker: (Cook, B, 2012)

1. Undvika. Lämna de aktiviteter som är grunden till risken
2. Reducera. Vidta åtgärder för att minska risken till exempel införa kontroller
3. Dela. Vidta åtgärder för att transferera eller sprida riskerna genom t.ex. försäkringar, headging eller outsourca en aktivitet.
4. Acceptera. Här vidtas inga åtgärder, risken accepteras hellre än att man tillför resurser för att hantera risken

När företaget har beslutat vilken riskrespons man vill använda sig av utarbetas en implementeringsplan fram (Moeller, 2007).

Control activities (Kontrollaktiviteter)

I detta steg implementerar man kontrollaktiviteter och policys för de risker som man i det föregående steget bedömde vara sådana till sin natur att de var i behov av att kontrolleras och förmildras. Med andra ord ska företaget med hjälp av adekvata kontrollaktiviteter skapa en acceptabel nivå av residualrisk, det vill säga den risk som återstår efter man vidtagit åtgärder för att hantera identifierade riskfaktorer (Cook, B, 2012). Det är viktigt med policys och rutiner kring de åtgärder som initieras som riskrespons, så att det finns en tydlighet i vad som ska göras och vem som är ansvarig för respektive process. Det är även viktigt att dokumentera resultatet av åtgärderna för att kunna utvärdera om företaget nått önskat resultat (Moeller, 2007).

Information and communication (Information och kommunikation)

För att kunna hantera risk måste rätt individer få rätt information. Ballou & Heitger (2005) understryker vikten av regelbunden rapportering till ledning och styrelse men även till övriga nivåer i organisationen för att ge underlag att bedöma och hantera risken. Det kan röra sig om intern såväl som extern information. Väl implementerade IT-system samlar och analyserar data och utgör ett kraftfullt verktyg för att logga incidenter och ge tidiga varningssignaler. Viktigt är också att företagsledningen kommunicerar betydelsen av ERM och hur företaget ser på risk och dess riskbenägenhet hela vägen ut i organisationens alla delar, horisontellt som vertikalt. Man bör även upprätta formella roller och ansvar, samt kommunikationskanaler som underlättar för medarbetarna att rapportera riskinformation. Det ska vara möjligt att kommunicera riskinformation genom organisationens alla led, såväl uppåt som nedåt och i sidled för att riskhanteringen ska bli så effektiv som möjligt (Moeller, 2007). Rätt information till rätt individer är av betydelse för att möjliggöra att så många risker som möjligt identifieras. Följande fem punkter nedan bör genomsyra informationen som rapporteras (COSO, 2004).

- 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.

Monitoring (Uppföljning)

Övervakning och vidareutveckling av en organisations riskarbete är nödvändig dels för att upptäcka problem som måste åtgärdas, men även för att ett företags ERM är under ständig transformation. Mål och visioner förändras, lika så måste kontrollaktiviteterna revideras för att undvika att de blir obsoleta och ineffektiva (Moeller, 2007).

2.5.3 Nivåer

De olika nivåerna i en organisation som finns visualiserat på den högra sidan av matrisen (se fig 2) utgör den tredje och sista dimensionen av COSO´s kub. Ramverket är utformat för att genomsyra organisationens alla delar och enheter. Riskhantering ska inte bara ske på ledningsnivå, utan i organisationens alla nivåer. Detta för optimera identifieringen och hanteringen av risk.

2.6 Sammanfattning implementering

Det är viktigt med en väl dokumenterad riskhanteringspolicy tillsammans med ett gemensamt språkbruk kring risk, tydliga ansvarsroller och riskfilosofi. Till detta ska organisationen etablera en riskinventering och bedömningsprocess. Vidare lägger COSO´s ramverk stor vikt vid en transparent och tydlig rapportering samt att det upprättas en konsoliderad rapport till organisationens riskintressenter. Värt att understryka är att mycket arbete bör läggas på att identifiera adekvata avstämningspunkter och parametrar till data insamlingen. Väljer organisationen fel parametrar spelar det ingen roll hur aktuell, läglig, och tillgänglig rapporteringen är eftersom informationen bygger på irrelevant information och ger en missvisande bild. Organisationen bör också implementera någon form av systemstöd för insamling och tolkning av riskdata.

COSO´s modell föreslår också att organisationen etablerar en riskkommitté och/eller en riskansvarig, som i litteraturen ofta benämns Chief Risk Officer (CRO). Denne bör ha en sammanlänkande roll, koordinera organisationens riskaktiviteter, sammanställa riskrapporteringen och föra denna vidare till ledning och styrelse. CRO är också den individen i organisationen som ska agera drivande i det kontinuerliga arbetet med ERM (Lam, 2003).

En CRO´s uppgifter kan punktas upp enligt nedan: (Lam, 2003)

- Bistå med ledarskap, vision och vägledning i arbetet med ERM.
- Etablera ett ERM ramverk för alla divisioner inom organisationen.
- Utarbeta en riskhanteringspolicy, samt en modell för att kvantifiera ledningens riskbenägenhet.
- Implementera relevanta riskindikatorer.
- Allokera kapital i företaget, för att optimera organisationens riskportfölj.
- Kommunicera företagets riskfilosofi till dess intressenter. (B & Hertiger, 2005 Winter)
- Utveckla stödprogram för ERM i företaget.

2.7 Kritik mot COSO-ERM

Som redan diskuterats är tanken med ramverket att ge ledning och styrelse en övergripande bild av organisationens risksituation men enligt Brancato (2006) är ofta styrelser negativt inställda till allt för formaliserade processer och koncept och har en benägenhet att undvika dessa.

En annan kritik som lyfts fram är att det inte ges någon direkt förståelse eller vägledning av själva implementeringsprocessen, utan ramverket framstår som för enkelt och brett. Det anses även har svårt att hantera risker utanför det finansiella och redovisningstekniska området i organisationen då det är präglat av de redovisningsgrupper som tagit fram ramverket. Dessutom är ERM-ramverket baserat på COSO's tidigare ramverk för internkontroll från 1992, inte bara att detta tidigare ramverk anses vara för brett (Shaw, 2006), kritikerna menar också att det är förlegat (Quinn, 2006).

En återkommande kritik mot ERM är att detaljstyrningen och övervakningen av olika processer ned i organisationens olika nivåer gör att blicken inte lyfts. Många gånger kan det vara frågor som är för operationellt och taktiskt komplicerade som tas upp på ett styrelsemöte. Detta kan göra att man kan missa de större risker som är i annalkande (Magretta, 2005). Dessutom är ERM's internkontrollssystem ofta mycket komplexa och det kan vara svårt att korrekt hantera informationen eller tolka signaler som inte passar in i systemet (Power, 2004). Vidare kan denna komplexitet skapa motvilja i arbetet med ERM och dess processer. Kritiker menar också att internkontrollen kan invagga organisationen i en falsk känsla av att det okontrollerbara (läs risk) har blivit kontrollerat (Holt, 2004).

3 Metod

3.1 Design

För att besvara uppsatsens forskningsfråga har författarna valt att använda sig av fallstudier på två olika företag för att samla empirisk data att jämföra med teorin om ERM. En fördel med fallstudier är att det blir möjligt med en djupare och mer precis analys av händelser och processer som kan vara viktiga för organisationens verksamhet (Bell, 2000). Nackdelen med fallstudier är att resultaten inte blir lika generaliserbara som andra metoder (Yin, 2003). Men då det i denna uppsats inte kommer redovisas statistiska och mätbara resultat utan samlad information ska tolkas från de respektive fallföretag passar vald metod bra. Vidare anser författarna den kvalitativa ansatsen var att föredra gentemot den mer generaliserande kvantitativa metoden eftersom den kvalitativa ansatsen ger möjlighet till en djupare förståelse (Jacobsen, 2002) vilket är vad författarna strävar efter i denna uppsats. Insamlingen av informationen sker genom semistrukturerade intervjuer för att författarna önskar en flexibel dialog där följdfrågor kan ställas för att fördjupa och vidareutveckla svaren (Bell, 2000).

3.2 Fallorganisationerna

Ett viktigt kriterie som varje fallorganisation behövde uppfylla var att det jobbade med en övergripande riskhantering. Detta för att författarna ska ha möjligheten att undersöka vilka processer de har implementerat och vilka rutiner de har kring dessa, för att få en fungerande holistisk riskhantering och således svar på frågan “Hur använder svenska företag ERM?”.

Författarna satte ingen gräns för hur stort företaget skulle vara men företrädesvis önskades företag av större storlek som verkar både i Sverige och utomlands. Detta för att kunna täcka så mycket som möjligt av ERM och COSO’s verktyg och teorier. Ett större internationellt företag antogs också använda riskhantering mer ingående samt att nyckelpersoner med djup kunskap i ämnet borde vara lättare att identifiera.

Andra AP-fonden och Astra Tech som är de valda fallföretagen i denna uppsats anser författarna passar bra för att besvara vår forskningsfråga då det ena är en organisation med finansiell inriktning, (AP-fonden) och det andra är mer inriktad på utveckling och försäljning av produkter (Astra Tech).

3.2.1 Andra AP-fonden

I Andra AP-fondens årsredovisning från 2011 går det att läsa att de är en av norra Europas största pensionsfond och förvaltar 216,6 miljarder kronor i princip alla olika slags tillgångar över hela världen. Deras uppdrag som kapitalförvaltare är från riksdagen att långsiktigt maximera avkastningen på det svenska pensionskapitalet (Andra AP-fonden, 2011).

3.2.2 Astra Tech

Astra Tech utvecklar, tillverkar och marknadsför dentala implantat samt avancerade produkter till sjukvård inom urologi och kirurgi och har idag ungefär 2200 annställda i 16 länder. Företaget grundades 1948 och har sedan dess arbetat med innovationer för att förbättra människora livskvalitet. Deras omsättning uppgick år 2010 till 3,9 miljarder kronor (Astra Tech, 2012).

Att använda organisationer i skilda branscher borde rimligtvis ge ett bra underlag till fördjupning i ERM och COSO om det visar sig att likheter, men också skillnader kan utrönas i själva användandet av verktygen.

3.3 Tillvägagångssätt

Efter ett möte med Peter Findahl som är konsult inom risk management fick författarna hjälp att hitta en kontaktperson att intervjua på Andra AP-fonden som kunde passa uppsatsen bra. Ett möte bokades via mail med Andra AP-fondens Head of Risk Management. För mötet avsattes en och en halv timme där dokumentationen skedde via inspelning som också är ett av det mest vanliga sättet att dokumentera en intervju på enligt Rubin & Rubin (2005). Även anteckningar fördes av författarna under intervjun som stöd för följdfrågor. Material transkriberades sedan ordagrant för att inte någon form av information skulle gå till spillo eller tolkas på fel sätt.

Andra intervjun bokades med Global Risk & Control Manager (CIRM) på Astra Tech i Mölndal och denna gång fick respondenten frågeunderlaget skickat till sig för att kunna förbereda sig inför mötet. Den beräknade tiden på en och en halv timme fick kortas ned till en timme men detta var inte ett problem då Astra Tech´s CIRM är mycket väl insatt i ERM och COSO och kunde på ett mycket effektivt sätt besvara våra frågor på hur Astra Tech arbetar med ERM. Även denna gång spelades intervjun in för att sedan ordagrant transkriberas.

Båda intervjuerna var semistrukturerade vilket författarna anser är det bästa sättet att få ut så mycket information som möjligt av respondenten då följdfrågor kan ställas vilket kan öka förståelsen i ämnet.

I kommande kapitel, resultat, analys och slutsats har författarna valt att löpande redovisa resultatet av undersökningen och inte strikt utgå från intervjufrågorna för att ge läsaren ett jämnare och mer lättförståeligt flöde i texten.

4 Resultat

Författarna kommer i detta kapitel lägga fram den empiriska informationen som samlats in genom intervjuer och genomgång av de utvalda bolagens årsredovisningar. Frågorna som ställdes var baserade på intervjufrågorna (se appendix). Vid vissa tillfällen krävdes dock ytterligare frågor och en mer utbroderande diskussion för att säkerställa att författarna tolkat svaret korrekt. Vi har valt att strukturera kapitlet efter ett antal rubriker för att ge en så klar och överskådlig bild som möjligt. I nästföljande kapitel kommer författarna att analysera den samlade informationen med det teoretiska ramverk som presenterats i kapitel 2.

4.1 Översiktlig riskhantering inom fallorganisationerna

4.1.1 Andra AP-fonden

I Andra AP-fondens förvaltningsberättelse beskrivs riskhanteringen som ett löpande arbete som utförs av tre fristående men samverkande riskfunktioner: riskbudgetering, compliance och risk management. Till risk management hör ytterligare tre områden, kreditrisk, likviditetsrisk, och operativ risk. Den sistnämnda beskrivs uppstå genom icke ändamålsenliga eller misslyckade interna processer. Dessa identifieras med hjälp av olika metoder så som självutvärdering, processanalys, riskindikatorer och workshops. Riskerna analyseras utifrån sannolikheten att de inträffar samt vilka konsekvenser detta får. Med hänsyn till denna analys prioriteras riskerna och en åtgärdsplan tas fram.

I fondstyrningsrapporten framgår det att det är styrelsen som är ytterst ansvarig för fondens internkontroll och formandet av fondens riskpolicy. Risk management-avdelningen säkerställer att ramverket efterlevs såväl i sin helhet som i sina delar. Man har även ansvaret

för den löpande interna kontrollen av finansiella och operativa risker. Denna uppföljning bygger enligt rapporten på att det finns en transparent riskrapportering och analys som sker dagligen till fondens ledning och löpande till styrelsen.

Andra AP-fonden använder ERM utifrån en egen modell de tagit fram med hjälp av en extern konsultfirma som de kallar för Andra AP-fondens riskträd, för att kategorisera och typifiera operativa risker. Där har de delat in operativa riskerna i sex stycken olika kategorier följt av risktyper för varje kategori.

4.1.2 Astra Tech

Då Astra Tech var en del av Astra Zenecas koncern fram till 2011 så ingick dem även i deras årsredovisning. Ur denna kan utläsas att man arbetar kontinuerlig med att säkerställa att de har effektiva rutiner för riskhantering till stöd för arbetet att nå deras strategiska mål och tillgodose företagets intressenter, samt att leva upp till företagets grundvärderingar.

Affärsverksamheten övervakas både på extern och intern nivå för att upptäcka förändrade risker samt att säkerställa att dessa hanteras på ett lämpligt sätt när de uppkommer. Styrelsen har definierat koncernen riskbenägenhet genom att utrycka de acceptabla risknivåerna för koncernen med hjälp av tre nyckeldimensioner: resultat och kassaflöde, avkastning på investeringar samt potentiella inverkan på företagets anseende.
För att nå företagets långsiktiga mål som ligger inom ramen för koncernens riskbenägenhet ansvarar linjechefer för identifiering och hantering av risker. Detta gör det möjligt att göra både kvalitativa och kvantitativa bedömningar av risknivån som företaget är beredda att acceptera för att nå de långtgående målen. Denna struktur för ERM bygger på en egen variant av COSO-kuben.

4.2 Fallorganisationernas interna riskmiljö

Båda respondenterna svarar att det finns en övergripande dokumenterad riskpolicy för koncernen där bland annat företagets riskbenägenhet är uttryckt tillsammans med processbeskrivning, beslutsordning, rapportering och krav på efterlevnad för bolagen. Detta kan vi även läsa i respektive företags årsredovisning. I Astra Zenecas årsredovisning framgår att det finns normer, riktlinjer och stödjande verktyg för dem som arbetar med riskhanteringsprocesserna. Dock nämner Astra Tech´s Global Risk & Control Manager (CIRM) att de beskriver riskpolicyn som generaliserande då koncernens aktiviteter är så pass olika i sin natur, som produktion, forskning och utveckling samt marknadsföring.

På Astra Tech görs riskrapportering vid varje bokslut som sker en gång per år samt vid budgetering, prognosuppdatering och rolling business uppdate som sker en gång i kvartalet. När de gör sin treåriga budgetering en gång om året får alla dotterbolag även lämna in en riskkarta mot de målen de ställt upp. Ansvarig på Astra Tech samlar in all information från de olika delarna och sjutton dotterbolagen i organisationen på möten var tredje månad och tillsammans med riskkommittén skaffar de sig en total bild av riskerna. Varje sektion har en ansvarig för riskrapporteringen och det är oftast VD eller finanscheferna i de sjutton olika dotterbolagen som Astra Tech har.

Andra AP-fondens Head of Risk Management beskriver det övergripande ramverket med tre nivåer:

- Lagstadgade placeringsrisker.
- VD´s riktlinjer som beskriver hur avkastning ska skapas, hur risker ska hanteras, mål med förvaltning, hur verksamheten ska bedrivas och organiseras och detta utgör ett ramverk för den interna verksamheten.
- Investment guidelines som talar om vilka respektive förvaltare har för befogenheter. Det finns även ett dokument där det tydligt framgår vad som händer om man överskrider dessa och dessutom riskloggas överträdelserna. (Detta är något som däremot Astra Tech inte har.)

Rapportering av risk sker löpande till styrelsen via kvartalsmöten, som framgår både av årsredovisningen och av intervjun med Andra AP-fonden.

4.3 Målsättning inom fallorganisationerna

Båda respondenterna nämner att företagets strävan mot att nå sina målsättningar ska stå i relation till deras riskbenägenhet, alltså hur mycket risk de är beredda att acceptera för att nå sina mål. Detta är också i linje med vad COSO´s ramverk uttrycker gällande riskbenägenhet kontra långsiktiga mål.

Andra AP-fonden använder sig av strategiska mål på 3-5 år där deras strategiska portfölj skapas utifrån om man tror att marknader är effektiva eller inte. En gång om året gör de smärre uppdateringar i den övergripande portföljen med information från långtgående prognoser på 30-40 år där de tittar på statistiska mätningar på samhälleliga förändringar. Med matematiska övningar sammanställer de sedan den optimala portföljen och får ett svar

på hur mycket av varje tillgång de ska inneha för att möta avkastningskraven samtidigt som man speglar företagets riskaptit.

Astra Tech delar också in sina strategiska mål på 3-5 år och en mer långsiktig strategisk plan på 10 år. När Astra Tech verkade under deras förra ägare Astra Zeneca arbetade de med mer fokus på långsiktiga mål. Nu med amerikanska ägarna har fokus ändrats något mot mer kortsiktig mål då Astra Tech har ett börsnoteringstryck på sig i och med inträdet på den amerikanska börsen. Detta innebär att riskhanteringen är mer detaljstyrd än under de tidigare ägarna. Astra Tech har en långsiktig målbild men delar upp sina risker som kort- och långsiktiga där de långsiktiga målens risker bryts ned och hanteras med kortsiktiga mål.

4.4 Process för riskhantering

I både Astra Zenecas och Andra AP-fondens årsredovisning framgår att det finns normer, riktlinjer och stödjande verktyg för dem som arbetar med riskhanteringsprocesserna. I arbetet med den löpande riskhanteringen nämner båda respondenterna självutvärdering och workshops som verktyg för att samla in information. Astra Tech gör avstämningar med samtliga funktionschefer en gång i kvartalet och med ledningsgruppen en gång per år och har även workshops i respektive styrelse och ledningsgrupp på de olika dotterbolagen. Dotterbolagen har även en skyldighet enligt företagets policy att den 20:e varje kvartal lämna in en riskrapport. Risk Control Committee arbetar sedan fram en konsoliderad bild av riskerna.

På andra AP-fonden använder man utöver de två nämnda metoderna, (worksshops och självutvärdering) även en risklogg för att identifiera operativa risker som ska användas av personal på daglig basis. Varje månad skickas en riskrapport till styrelsen. Utöver denna månadsrapporterings skall avstämning ske varje halvår samt en gång per år vid årsbokslutet.

Ur Astra Zenecas årsredovisning går att läsa att de strävar efter att ha en så integrerad riskhanteringsprocess som möjligt. Astra Tech´s CIRM menar att riskhanteringen är integrerad i affärsprocesserna på så sätt att inga beslut får tas av ledningsgruppen utan att en rapportering om riskerna har mottagits. Operativa aspekter av risk hanteras av produktionscheferna på respektive avdelning. Hur detta exakt går till får författarna inget bra exempel på, då detta förfarande ser olika ut beroende på vilket dotterbolag i koncernen det gäller. Rapporter om riskhanteringen måste vara med vid varje årsbokslut och varje dotterbolag måste kunna visa på att de tagit upp sin riskhantering varje månad och har även detta som en stående agenda under veckomöten. Dokumentationen om riskhanteringen sparas och lämnas sedan tillsammans med årsredovisningen en gång per år.

Andra AP-fonden beskriver att de arbetar mer övergripande med sin riskhantering, men i vissa affärskritisk processer arbetar de med avstämningspunkter. Förvaltare som handlar kan till exempel inte godkänna sina egna ordrar utan detta måste godkännas av så kallad four eyes approval av två personer “back office”.

4.5 Riskidentifiering, bedömning och roller

Astra Tech har en formaliserad process för att identifiera risker som framgår av både årsredovisningen och intervjun. Däremot har de i dagsläget ingen specifik modell för hur de värderar och beräknar sina risker. Dock har Astra Techs´s CIRM god insyn och kännedom om koncernen då hon tidigare arbetat som controller, är utbildad inom riskhantering på IRM i London och verkat inom företaget många år. Hon är den person som efter att ha samlat in alla risker bedömer, värderar och plottar dessa i en ”risk heat map” (Riskmatris som COSO använder i sitt ramverk) tillsammans med Risk Control Committee. Beslut hur riskerna ska hanteras görs sedan också av desamma. Astra Tech har förutom deras CIRM, som är övergripande ansvarig för organisationens riskhantering, även utsedda personen med riskansvar i de olika dotterbolagen. Oftast handlar detta om en ekonomiansvarig, som i och för sig inte har en officiell titel som exempelvis risk manager, men ändå är ytterst ansvarig för riskhanteringen. Beslut om åtgärder i de olika dotterbolagen, baserat på de risker de rapporterar in, tas tillsammans med Risk Control Committee på huvudkontoret i Mölndal.

Riskidentifieringsprocessen på Andra AP-fonden utförs av flera olika avdelningar, risk-avdelningen, back office, performance och ekonomiavdelningen som sammanställs till en konsoliderad bild av riskerna. Andra AP-fondens Risk Management Committee koordinerar och styr sedan hur de agerar utefter denna riskbild. De är också kontrollerade av McKinsey & Company som extern aktör. Andra AP-fonden har formella roller och det finns tydligt beskrivet i riktlinjerna från VD att olika typer av risker hanteras av personer inom de olika områdena, som exempelvis en compliance officer som ansvarar för de legala riskerna. På lägre nivå är det inte lika tydligt och här saknas också formella roller. Dock finns en befattningsbeskrivning för varje anställd, men detta är ett generellt dokument som inte är kopplat till en specifik individ utan fyller ett mer funktionsövergripande syfte.

En sak som skiljer fallföretagen åt är att Andra AP-fonden använder ett IT-verktyg som de kallar för risklogg där incidenter registreras och Astra Tech i dagsläget inte använder något IT-stöd i sin riskhantering då deras Risk Control Committe manuellt hanterar inkommen information. Dock påpekar Astra Tech´s CIRM att det kan vara nästa steg i processen.

4.6 Styrning, kontroll och rapportering

Då Astra Tech verkar inom ett antal olika marknader och arbetar med innovativa produkter har de olika nivå på hur stor risk de är beredda att ta inom varje område. Deras CIRM berättar att beroende på vilken marknad eller produkt det handlar om sätts ett riskmått, exempelvis hur stor procent av EBIT (Earnings Before Interest and Taxes) som kan riskeras. Astra Tech har även ett system där de värderar riskerna från low till very high, sannolikheten att risken inträffar och om risken är hanterad eller inte. Astra Tech´s CIRM berättar också om små risker som egentligen kan accepteras för att de är just för små för att lägga resurser på. Dock är det så att om det visar sig att samma lilla risk rapporteras in från flera av dotterbolaget vidtas då åtgärder då det kan visa på något som kan bli en större risk. Risk Control Committee på Astra Tech får var tredje månad in riskrapporter från respektive dotterbolag och dessa jämförs med föregående rapport för att se hur risken har utvecklats. Beroende på riskens utveckling och baserat på denna rapport beslutar ledningen om eventuella åtgärder. På Astra Tech har de valt att ha samma system för riskrapporteringen i hela koncernen oberoende av hur stort exempelvis ett dotterbolag är eller vilket område det verkar i. Dock får författarna informationen att när de nu har arbetat med ERM såpass länge, och har en väl grundad riskfilosofi, har de planer på att minska kravet något på de dotterbolag som är mindre och inte är beroende av vissa typer av riskinformation.

I VD´s dokument för Andra AP-fonden finns det tydligt beskrivet vilka nivåer och gränsvärden (risklimiter) som ska följas. Risklemiterna ses över och uppdateras en gång om året då omvärlden är i ständig förändring. Gränser för exponering finns också och beror exempelvis på ratingen av de instrument de handlar med. Systematisk kontroll sker dagligen där fondens risker analyseras och rapporteras till ledningen. Dessa rapporter sammanställs också och rapporteras till styrelsen månadsvis. I VD´s dokument finns även ett kapitel om rapporter och uppföljning som beskriver vad respektive avdelning ska rapportera till vem, med vilken frekvens detta ska ske och med vilket innehåll. Andra AP-fonden skickar varje månad en rapport till styrelsen innehållande marknadsrisk, kreditrisk, och exponering mot olika emittenter. Alla som har ansvar att rapportera risker i organisationen gör detta utifrån samma standard.

5 Analys

Detta kapitel är strukurerat efter samma rubriker som föregående för att göra det möjligt att på ett tydligt sätt kunna analysera och diskutera resultatet och koppla detta till empirin. I nästföljande kapitlet ger författarna läsaren en sammanfattande slutdiskussion.

5.1 Fallorganisationernas interna riskmiljö

Enligt COSO´s ramverk bör organisationen genomsyras av en gemensam riskkultur, det ska vara tydligt på alla nivåer vilket riskbenägenhet organisationen har för att nå sina mål och organisationsstrukturen ska stödja detta. Det är också viktigt att denna riskfilosofi sprids genom organisationen så att alla är väl insatta i hur synen på risk ser ut i företaget och det ska även finnas dokumenterat i en riskpolicy.

Hos båda företagen fann vi att det finns en utarbetad policy som understryker vilken riskbenägenhet organisationen har och hur man ska agera. Båda respondenterna uttryckte även vikten av att denna riskfilosofi antas och den blir kulturskapande i organisationen. Här går det att dra paralleller till COSO´s ramverk och deras dokumenterade riktlinjer för hantering av risk som säger att företagen ska ha en övergripande och holistisk hantering av risker.

Båda undersökta företag visar på att de uppfyller COSO´s krav för den interna miljön då de har dokumentation som gäller hela organisationen där mått på riskbenägenhet finns med som ska relateras till uppsatta strategiska mål. Det finns även tydliga beslutsordningar, krav på rapportering och uppföljning av risker. Det ställs också krav på att regelbunden rapportering av risk ska finnas med på en agenda under exempelvis månadsmöten och även på den punkten visar det sig att företagen uppfyller kraven.

De respondenter som valdes ut för denna undersökning är ansvariga för riskhanteringen på respektive företag och de gav också en tydlig bild av hur det sköttes på ledningsnivå i respektive företag. Författarna tror att det är möjligt att en eventuell vinklad och ensidig bild ges av det egentliga användandet av riskhanteringen i företagen. Som grund för detta påstående är exempelvis CIRM på Astra Tech´s svar att riskansvariga på dotterbolagen ibland inte verkar vara helt insatta i varför, eller hur de ska rapportera sina risker. Detta sägs under intervjun i förbifarten men författarna vill ändå lägga vikt vid detta då det kan visa att det egentligen kanske inte genomsyrar hela verksamheten. COSO´s ramverk är ett komplext

verktyg som måste införas på alla nivåer i en organisation och det är viktigt med ansvariga personer för varje risk och nivå för att en gemensam riskfilosofi ska anammas av hela organisationen (Moller, 2007). Båda respondenterna nämner också i intervjun att det är oerhört viktigt med eldsjälar och inflytelserika personer i organisationen som arbetar med riskhantering. Detta för att förankra verktyget ända från ledning i en hierarkiskt organisation, ända ned till exempelvis kvalitetsansvarig i produktionslinjen på Astra Tech, eller i Andra AP-fonden, handlarna. En anledning till att författarna tycker sig kunna ana en eventuell ensidig bild av hur organisationerna arbetar med EMR kan vara att den praktiska tillämpningen av ERM och COSO kanske inte är lika lätt att implementera i ett företag som teorin säger. Företaget kan värderas upp till 20 % högre med en väl inarbetat riskhanteringsprocess enligt Hoyt & Liebenberg (2011) men författarna anser att det är svårt att säga var exakt detta värde skapas. Vidare menar Hoyt & Liebenberg (2011) att intresset för ERM ökat de senaste åren, så detta borde rimligen innebära en uppåtgående trend att företagen implementerar övergripande riskhantering. Är det för att ERM och COSO´s verktyg för riskhantering verkligen är helt inarbetat i organisationen som värdet på företaget ökar eller kan det föreligga en så kallad ”löskoppling” och är en ”institutionell myt” (Meyer & Rowan, 1977)? Det är möjligt att företagen bara använder ERM och COSO för att de är bundna av lagen samt för att legitimera sin verksamhet hos omvärlden och författarna anser att det är svårt att utröna huruvida de faktiskt blir mer effektiva i sitt beslutsfattande och riskhantering.

5.2 Målsättning inom fallorganisationerna

Andra AP-fonden har tydliga riktlinjer för hur stor risk de får ta som speglar de långsiktiga avkastningskraven och målen. Detta visar sig genom att de sprider risken i sin portfölj genom att ha tydliga regler för hur stor procentuell del av kapitalet som får användas för olika instrument, värdepapper valutor med mera som de handlar med.

Astra Tech har också tydliga regler för hur mycket risk de får ta för att nå sina långsiktiga mål. Då de säljer en mängd olika produkter på olika marknader är också risken olika beroende på vilken marknad och produkt det handlar om. Men sammanslaget är även i detta företag ett procentuellt mått fastslaget för att spegla företagets kort- och långsiktiga mål. Vad som inte framkommer i intervjun men kanske kan anses vara självklart är att Astra Tech i och med sina olika produkter på olika marknader får en naturlig riskhantering genom sin diversifiering. Detta framgår mer tydligt i Andra AP-fonden enligt författarna då de väljer att satsa olika stora delar av sitt kapital i olika värdeinstrument med olika risk. Det framgår inte huruvida Astra Tech exempelvis väljer att gå in på en ny marknad med en ny produkt för att de anser sig vara i ett läge där de kan öka sin risk exempelvis på grund av att ett redan

etablerat område anses ha fått en lägre risknivå än tidigare och så att säga kompensera med en nyetablering för att fylla sin riskkvot. Det vill säga om strategin påverkar deras syn på risk eller risken styr strategin. Dock anser författarna detta egentligen vara samma sak och övervägandet och beslut som tas om detta hanteras inom ramarna för företagets riskhantering genom att det presumtiva värdet ställs i relation till risken.

Författarna anser att båda fallföretagen arbetar med sina risker enligt ERM, om än något olika definierat. Andra AP-fonden som exempelvis kallar ett av sina verktyg riskträd, som är framtaget tillsamman med en extern konsultfirma, skiljer sig lite mot Astra Tech där riskhanteringen mer strikt går efter COSO´s verktyg. Då Andra AP-fonden förvaltar pensionspengar och till viss del är styrt av ett statligt ägande anser författarna att detta kan vara anledningen till att de hellre till viss mån skyddar sig mot risker med eventuell stor uppsida. Under intervjun tolkar författarna Astra Tech som mer benägna att nyttja risker för att nå sina mål, dock beroende på vilken produkt eller marknad det handlar om. Sammanfattningsvis anser författarna dock att båda fallorganisationerna har en klar integration mellan riskbenägenhet och strategisättning mot deras mål i enlighet med COSO´s ramverk och övrig presenterad teori om ERM.

5.3 Process för riskhantering

Det har varit svårt att utröna någon definitiv avgränsning hos de båda fallorganisationerna huruvida de använder en processpecifik användning eller en funktionsövergripande hantering av risker. Andra AP-fonden menar själva att de har en funktionsövergripande ERM. Men då respondenten svarade att vissa kritiska förfaranden övervakas och kontrolleras ner på processnivå kan detta mer liknas med en processpecifik riskhantering enligt författarna.

På Astra Tech sker implementering av kontrollmekanismer i varje affärsprocess i delar av koncernen beroende på vilket affärsområde det handlar om. Ingen av fallföretagen anser författarna ha antingen processpecifik eller funktionsövergripande riskhantering och detta kan bero på att de valt att endast använda de steg som de tydligt ser skapar mervärde. Enligt Hoyt & Liebenberg (2011) ska ERM implementeras i en organisation endast om nyttan överstiger kostnaderna och detta anser författarna vara orsaken till att fallorganisationerna i detta skede arbetar som de gör med ERM.

Power (2004) menar att det finns en risk med att implementera allt för avancerade modeller då de individer som ska arbeta med de nya momenten kan ha ett visst motstånd mot nya

processer och rutiner och således försämra riskhanteringsprocessen. Astra Tech´s CIRM nämner även detta under intervjun och menar att ett bra sätt att implementera nya verktyg och rutiner är att bygga på vedertagna processer i organisationen. Att författarna kan se en skillnad i hur fallorganisationerna arbetar med ERM kan bero på att de har så pass olika verksamheter och de bakåt i tiden således också har hanterat olika typer av risker, rutiner och processer. Detta skulle kunna vara anledningen till att författarna inte funnit att någon av fallorganisationerna jobbar på det ena eller andra sättet, utan snarare ser en hybrid mellan det funktionsövergripande och processpecifika förfarandet.

5.4 Riskidentifiering, bedömning och roller

Vid riskidentifiering kan författarna genom den insamlade empirin konstatera att det finns många punkter hos de båda fallorganisationerna som kan kopplas till vad COSO´s ramverk och andra forskare inom genren föreslår. Bland annat så använder sig fallorganisationerna av workshops för att få en omfångsrik situationsuppfattning från den samlade kompetensen inom organisationen. Fallorganisationerna samlar även information i de operativa leden av vad båda organisationerna benämner som experterna på området, linjechefer och medarbetare som arbetar närmast riskerna. Detta överensstämmer också med vad Mauer (2009) uttrycker.

Ett så likartat förfarande med riskidentifieringen i dessa två skilda branscher anser författarna tyda på att denna del av processen är generiskt betingad och väl vedertagen. Dock måste tonen för organisationens riskbenägenhet och dess relevans vara väl förankrad genom hela organisationen för att detta arbete ska kunna utföras med önskvärt resultat vilket även poängterades av båda respondenterna.

Båda de undersökta företagen använder idag COSO´s riskmatris, risk heat map, för att kvantifiera händelsernas effekter och sannolikhet samt delar upp sina risker efter hur de värderas. Dock skiljer det en del mellan hur värderingen går till då det till stor del är en person som sköter detta på Astra Tech och det på Andra AP-fonden är deras Risk Management Committee som tillsammans värderar riskerna. Även Astra Tech har en kommitté där riskerna behandlas, dock framgår det av intervjun att värderingens slutgiltiga kvantifiering sköts av Astra Tech´s CIRM. COSO´s ramverk säger inte specifikt hur många som ska vara delaktiga i själva värderingen av risken så slutsatsen är att även på denna del följer båda fallföretagen COSO´s ramverk. Astra Tech har ärvt sitt sätt att hantera risker från Astra Zeneca och de har inte ett IT-system för som stöd i sitt arbete. Detta upplevdes i början som något som önskades då COSO´s ramverk förespråkar detta, men så här i efterhand har

det varit en fördel enligt Astra Tech´s CIRM att införa ERM steg för steg och fått en större förståelse och bättre rutiner. Implementeringen av ERM är en lång process och det tar tid att få in rutinerna i organisationen. Problem som kan uppstå är att när personal ska hantera ett nytt system finns det inte bara ett motstånd, att det är en ny rutin som ska göras i det dagliga arbetet, du måste även se till att få in rätt sorts information i systemet. Om användaren är okunniga i vad risk egentligen är och exempelvis rapporterar in problem får du heller inte ut relevant information ur systemet. Författarna anser att det är oerhört viktigt att det finns en klar riskfilosofi och en medvetenhet om vad en risk egentligen är och att detta genomsyrar hela organisationen innan de bygger in sig i ett system. Enligt Brancato (2006) är även styrelser ofta negativt inställda till att införa allt för formaliserade processer och har en benägenhet att undvika detta. Författarna anser att detta stämmer väl överens med verkligheten i detta fallet då COSO´s ramverk är ett komplext och tidsödande arbete som författarna tror kan uppfattas som onödigt innan berörda personer ser nyttan med det. Samtidigt har båda respondenterna gjort det tydligt med vikten av nyckelpersoner i ledningen som talar för ERM och COSO för att få det att fungera på bästa sätt. Att det tar tid och är en hög ingångströskeln tror författarna är för att det tar tid att få gehör för implementeringen.

Andra AP-fonden har ett IT-system som de kallar incidentloggen där de för in sina risker. Även här poängteras vikten av att föra in rätt typ av grunddata för att få fram rätt typ av information som sedan analyseras och rapporteras. Systemet är implementerat med hjälp av en extern konsultbyrå och enligt författarna kan avsaknaden av liknande problem som Astra Tech nämner vara just att de fått extern hjälp. En orsak till detta tror författarna vara att processerna blir mer förankrade hos ledningsgruppen då den externa partnern är inblandad på grund av att det då är ett tidsatt projekt som måste genomföras effektivt för att hålla nere kostnader. Visst kostar det pengar även när man sköter all implementering internt också men en implementering i projektform kan ge mer legitimitet för att det ska genomföras inom satta ramar.

I Astra Tech´s fall har de först nu börjat titta på olika IT-system som kan tänkas underlätta deras arbete med riskhanteringen då de anser att en väl inarbetat riskfilosofi är förankrad i organisationen. Här ser författarna en klar skillnad mellan hur fallorganisationerna följer COSO´s ramverk och övrig teori om ERM då det understryker vikten av ett systemstöd i datainsamlingen. Astra Tech kan i detta avseende anses inte följa COSO´s riktlinjer medan Andra AP-fonden gör det.

Vidare visar organisationerna att det finns tydliga dokumenterade roller i hanteringen av risk, men ju längre ner man kommer i hierarkin desto mer generaliserande blir rollbeskrivningen.

Teorin betonar att det är organisationens management som måste skapa en riskkultur som genomsyrar hela organisationen uppifrån och ner och detta nämner även båda respondenterna vid ett antal tillfällen under intervjuerna. Detta tror författarna är grunden till den tydliga rollstrukturen i toppen av de båda organisationerna. Organisationer behöver vara tydliga och vägvisande i riskhanteringen och således börjar implementera detta i toppen av organisationen.

5.5 Styrning, kontroll och rapportering

Även om de båda fallföretagen skiljer sig från varandra då Astra Tech säljer och utvecklar produkter och Andra AP-fonden är en finansiell verksamhet arbetar de båda på ett snarlikt sätt gällande att de har ett formellt regelverk med gränsvärden. I Andra AP-fondens fall utgår de ifrån procentuellt satta nivåer på respektive form av värdepapper som aktier, räntebärande värdepapper och intern- respektive extern förvaltning de är tillåtna att handla med, och har således en mer exakt mätbarhet i sin riskhantering. Detta skiljer sig något från Astra Tech där riskerna uppskattas mer med erfarenhet och magkänsla än av exakta tal då det är Astra Tech´s CIRM som i slutändan värderar risken med stöd av deras Risk & Control Committee. Dock berättar respondenten på Astra Tech att beroende på vilken marknad eller produkt det handlar om sätts ett finansiellt mått som exempelvis en viss procent av EBIT.

COSO´s ramverk föreslår ett formellt regelverk med satta gränsvärden som organisationen ska rätta sig efter och detta gör också de båda fallföretagen, även om skattningen av deras olika risker görs på något olika sätt. En fråga väcks dock hur väl måtten tas emot längre ned i organisationen hos Astra Tech då dessa kanske kan uppfattas som godtyckligt satta eftersom det i slutändan är i princip en person som värderar riskerna. Denna eventuella tveksamhet borde inte uppstå på samma sätt på Andra AP-fonden då riskmått på olika värdepapper bestäms av marknaden och ratinginstitut. Astra Tech ser själva inte detta som ett problem men under intervjun tolkar författarna att vissa riskansvariga på de olika dotterbolagen är mindre överens med ledningen hur vissa risker ska värderas då de kommer fram att från vissa dotterbolag är riskerna ofta för högt värderade. Enligt (Sveningsson, et al., 2009) utgår ett ledarskap inte från en ”a prioledare” utan en person blir en ledare då denne är accepterad som en person då stor vikt läggs vid vad personen säger. Författarna tolkar då att beteendet med att enstaka dotterbolag ofta övervärderar sina risker kan ha att göra med att sättet riskhanteringen sköts på kanske inte är helt förankrat ända ned i organisationen. Implementeringen av ERM är en lång process så förklaringen till detta borde också kunna bero på att nämnda dotterbolag eventuellt inte nått lika långt i processen som sina kollegor.

Även om vi kan se skillnader i hur riskerna hanteras mellan fallorganisationerna ser ändå författarna starka likheter med hur COSO´s ramverk föreslår hanteringen och hur båda fallföretagen arbetar COSO och ERM.

Vidare har fallorganisationerna en systematisk kontroll av sina risker och ansvariga nedåt i hierarkin där olika personer så att säga är ägare av de olika riskerna. Som författarna nämnt tidigare använder båda fallföretagen en så kallad ”risk heat map” som är en riskmatris där riskerna delas in i hur stora dom är och sannolikheten att de inträffar. Detta är ett verktyg som ingår i COSO´s ramverk och författarnas tolkning av intervjuer och respektive företags årsredovisning är att båda fallföretagen arbetar med ERM helt i linje med vad ramverket rekommenderar på denna punkt. I båda företagen sker också löpande uppdatering på månatlig basis för att se om nya risker har uppkommit samt för att bedöma befintliga riskerna och se huruvida de har förändrats där åtgärder tas beroende på resultat vid avstämningarna.

Hur man följer upp utvecklingen av identifierade risker skiljer sig en del mellan fallorganisationerna. Andra AP-fonden har en mer avancerad struktur och betydligt tätare riskrapportering än vad Astra Tech har. Enligt teorin kring ERM ska organisationerna ha ett transparent system med kontinuerlig rapportering och här anser författarna att Andra AP-fonden arbetar mer i linje med detta än vad Astra Tech gör. Detta skulle kunna härledas till skillnaden i företagens natur. Eftersom Andra AP-fonden jobbar med exakta nyckeltal och risklimiter blir det betydligt mer relevant att samla in denna typ av information dagligen då den är enkel att ställa i relation till organisationens kvantitativa riskmått. Samtidigt skulle också ett enda övertramp i befogenheterna kunna leda till monumentala förluster för Andra AP-fonden. Den europeiska storbanken Societe Generale är ett exempel på detta, där en enda anställd genom en rad transaktioner åsamkade banken en förlust på nästa 50 miljarder kronor (Clark & Jolly, 2008).

Astra Tech jobbar mer med kvalitativ analys som manuellt måste analyseras eller göras kvantifierbar vilket ökar arbetsbelastningen. Det är författarnas åsikt att detta arbeta skulle medföra mer kostnader än vad det skulle göra nytta för företaget att göra denna typ av rapportering varje dag. Detta tolkar författarna som att rapportprocesserna bör anpassas efter vilken typ av organisation det är.

6 Diskussion och slutsats

Grunden i ERM är att organisationens risker konsolideras för att forma en holistisk bild och att ett gemensamt sätt att hantera risker genomsyrar hela verksamheten. I denna undersökning framstår det att båda fallorganisationerna jobbar utifrån detta sätt att hantera sina risker som COSO´s ramverk och ERM-litteraturen förespråkar. Fallorganisationerna har båda processer för hur riskerna i deras verksamhet ska samlas in och förse beslutsfattarna med underlag för att hantera riskerna i linje med att kunna förverkliga deras strategiska mål. Även den så kallade riskfilosofin, där vikten av att ERM och sättet hur risker ska hanteras anser författarna vara förankrat i större delar av de undersökta organisationerna. Den teori om ERM och COSO som författarna tagit del av i arbetet med denna uppsats säger i stora drag samma sak som författarna kommit fram till i insamlingen av empiriska data.

Litteraturen föreslår komplexa system för att hantera datan kring riskhantering och konsultbyråer har även särskilda avdelningar som endast arbetar med ERM och författarnas förväntning innan arbetet med uppsatsen påbörjades var att finna en generallösning med strikta ramar för hur ERM används i organisationer. Under arbetets gång har insikten blivit att riskhantering många gånger handlar om subjektiva bedömningar och att det i stor utsträckning handlar om den mänskliga faktor som avgör hur resultatet blir. I en föränderlig värld anser författarna dock detta som ett sundhetstecken, det som var ett hot idag behöver nödvändigtvis inte vara det imorgon. Under vår intervju med Astra Tech framgick det tydligt att bedömningar och analyser av risker deras organisation utsätts för inte kan hanteras statiskt utan kräver stor erfarenhet och insikt i hur just deras verksamhet fungerar. Hur risker värderas beror helt på hur omvärlden hanteras i relation till organisationernas interna miljö och detta är en analys som kanske inte alltid en maskin kan avgöra.

Även om författarna överlag anser att de båda fallorganisationerna agerar efter ERM och COSO´s ramverk för riskhantering framkommer det saker som kan tyda på det motsatta. Under intervjun på Astra Tech upplever författarna en något inkonsekvent bild av hur enhetligt organisationen egentligen jobbar med ERM då det kommer fram att vissa chefer i koncernens dotterbolag inte är helt insatta i hur deras risker ska värderas som de senare ska rapportera in. Ofta är riskerna på tok för högt satta och detta fenomen kan urskiljas av samma användare återkommande. Frågan författarna ställer sig här är huruvida ERM faktiskt är implementerat och används ned i de operativa delarna av organisationen. Att hela koncernen ska använda ERM är klart uttalat och de olika ansvariga på dotterbolag i olika delar av världen har även genomgått utbildning i verktygen och filosofin på Astra Tech´s huvudkontor i Mölndal. Varför sker dessa misstag då om och om igen från samma bolag? En

förklaring till detta kan vara avsaknaden av ledare inom koncernen som förespråkar vikten av att använda ERM på rätt sätt. Det är viktigt att ledare inom organisationer som ska implementera ERM står bakom och förespråkar verktyget för att det ska ge bäst effekter. Astra Tech´s CIRM nämner även detta under intervjun men författarna tror det är möjligt att nämnda riskansvariga som rapporterar missvisande värdering av risker kanske inte helt förstått innebörden av ERM. En anledning till felrapporteringen kan vara att det är ett uttryck för missnöje och en förtäckt protest mot ytterligare en tidsödande process som uppfattas onödig. Detta skulle då kunna vara ett exempel på vad Sveningsson et al (2009) beskriver som att ledaren, i detta fall Astra Tech´s CIRM, inte fått med sig sina medarbetare och de inte blivit så kallade ”efterföljare” som tillmäter det ledaren säger stor vikt.

Andra AP-fonden säger att de inte arbetar efter COSO´s ramverk men författarna finner ändå en mängd likheter med i deras sätt att arbeta med ramverket. Frågan som kommer upp är vad egentligen COSO´s ramverk tillför? Är det som vilket annat riskhanteringsverktyg som helst? Skaparna av COSO säger att det är ett verktyg som kan användas av alla organisationer oavsett storlek och verksamhet. Samtidigt påstår kritikerna att ramverket är allt för enkelt och brett. Dessa två påståenden står enligt författarna emot varandra och anser att anledningen till att varför så många likheter kan urskiljas mellan Andra AP-fondens ERM och COSO´s ramverk kan vara just för att det är brett och generaliserande. För den saken skull behöver detta inte betyda att COSO´s ramverk inte är ett bra sätt att hantera risker enligt författarna.

Författarna har nämnt det innan men tycker ändå att det är värt att påpeka igen, att den praktiska tillämpningen av ERM och COSO kanske inte är lika lätt att implementera i ett företag som teorin framställer det och är en lång och pågående process. Enligt Hoyt & Liebenberg (2011) kan ett företag värderas upp till 20 % högre med en väl inarbetad riskhanteringsprocess som ERM men författarna anser att det är svårt att säga var exakt detta värde skapas. Hoyt & Liebenberg (2011) menar också att intresset för ERM ökat de senaste åren, så detta borde rimligen innebära en uppåtgående trend att företagen implementerar övergripande riskhantering. Dock ställer sig författarna frågan om det är för att ERM och COSO´s verktyg för riskhantering verkligen är helt inarbetat i organisationen som värdet på företaget ökar eller kan det föreligga en så kallad ”löskoppling” och är en ”institutionell myt” som Meyer och Rowan skriver om i sin artikel från 1977 (Meyer & Rowan, 1977). Använder bara företagen ERM och COSO för att de är bundna av lagen och för att legitimera sin verksamhet hos omvärlden, eller blir de faktiskt mer effektiva i sitt beslutsfattande och riskhantering? Kanske är det en kombination av de båda.

Klart är att båda fallorganisationerna jobbar utifrån en funktionsövergripande ERM med inslag av processpecifika kontroller. Dock inte alls så integrerat i företagets övriga processer som ramverket och ERM teorin uttrycker det. Detta kan bero på att mer tid krävs för att få det helt implementerat ner i alla nivåer. Men också att det blir för komplext att hantera och därför väljer man att inte gå längre. En väg att gå skulle kunna vara att arbeta funktions-övergripande från start, det vill säga ha ERM som fristående process som enkelt kan följas upp och analyseras i kombination med en kontinuerlig integrering av de operativa processerna.

6.1 Förslag till vidare forskning

Författarna anser att för att få en mer verklighetstrogen bild av hur riskhanteringen på fallföretagen ser ut i alla led i organisationen borde intervjuer med personer längre ned i hierarkin också göras för att få en mer nyanserad bild av hur väl riskhantering och COSO är integrerat i verksamheten. En annan fråga vi ser som relevant för vidare forskning är hur organisationen arbetade med riskhantering innan implementeringen av ERM. Detta skulle förhoppningsvis visa vilka metoder och processer som skiljer sig från organisationens tidigare arbete med riskhantering och hur de ser ut efter en implementering av ERM.

Andra intressanta framtida forskningsfrågor är också hur organisationerna organiserar projektet med en implementering av ERM, hur ansvarsfördelningen ser ut, vilka resurser och kompetens som krävs, hur etappindelningen ser ut och varför organisationer väljer att implementera ERM.

7 Litteraturförteckning

Astra Tech, 2012. (u.d.). Hämtat från www.astratech.se: http://www.astratech.se/Main.aspx/Item/658898/navt/76235/navl/76238/nava/76242 den 2 6 2012

B, B., & Hertiger, D. L. (2005 Winter). A building-block approach for implementing COSO:s. *Management Accounting Quarterly , 6* (No 2).

Beasley, M., & Clune, R. (2005). Enterprise Risk Management: An empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy , 24* (6), 521–531.

Bell, J. (2000). *Introduktion till forskningsmetodik* (1:a ed.). Lund : Studentlitteratur.

Besley, T., & Ghatak, M. (2005). Incentive, Risk and Accountability in Organizations. In B. Hutter, & M. Power (Eds.), *Organizational Encounters with Risk* (pp. 149-66). Cambridge : Cambridge Press .

Bowling, D. M., & Rieger, L. (2005 йил 1 -April). Success factors for implementing enterprise risk management: building on the COSO framework for enterprise risk management to reduce overall risk. *Bank Accounting & Finance* , pp. 21-26.

Brancato, C. K. (2006). *The role of U.S. Corporate Boards in Enterprise Risk Management.* The Conference Board.

Casual Actuarial Society. (2003 йил 1-Maj). *http://www.casact.org.* Retrieved 2012 йил 04-05 from http://www.casact.org/research/erm/overview.pdf

Clark, N., & Jolly, D. (2008). *http://www.nytimes.com*. Retrieved 2012 йил 21-5 from http://www.nytimes.com/2008/01/24/business/worldbusiness/24iht-socgen.5.9486501.html?_r=1&pagewanted=all

Cook, B. (2012). *www.FinanceLearningAcademy.com*. Retrieved 2012 йил 10-05 from http://www.financelearningacademy.com/riskmanagement.html

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

COSO. (n.d.). *http://www.coso.org*. Retrieved 2012 йил 12-04 from http://www.coso.org/documents/COSO_ERM_ExecutiveSummary_Swedish.pdf

Cumming, C. M., & Hirtle, B. J. (2001). “The Challenges of Risk Management in Diversified Financial . *FRBNY Economic Policy Review* , 1-17.

Daukant, R., & Hirst, A. (2009 йил 1-Augusti). 4 Steps to ERM . *Canadian Underwriter* , pp. 64-66.

Deloitte. (n.d.). *www.deloitte.com* . Retrieved 2012 йил 12-05 from http://www.deloitte.com/view/sv_SE/se/tjanster/riskhantering/bolagsstyrning/index.htm

Eriksson Zetterquist, U. (2009). Risk and Organizing-the Growth of Research Field. In B. Czarniawska (Ed.), *Organizing in the Face of Risk and Threat* (p. 9). Cheltenham : Edward Elgar Publishing Ltd.

Findhal, P. (2012 йил 10-04). Risk Management Consult .

Flyvbjerg, B., Bruzelius, N., & Rothengatter, W. (2003). *Megaprojects and Risk: an anatomy of ambition* (1:a ed.). Cambridge: Cambridge University Press.

Giddens, A. (1999). *Runaway World. How Globalisation Is Reshaping Our Lives .* London : Prolife Books .

Gordon, L. A., Loeb, M. P., & Tseng, L. Y. (2009). Enterprise risk management and firm performance: A contingency perspective. *Journal of Accounting and Public Policy* (28), 301-327.

Holt, R. (2004). Risk management: the talking cure. *Organization , 11* (2), 251–270.

Hopkins, P. (2010). *Fundamentals of risk management .* London : Kogan Page Ltd.

Hoyt, R. E., & Liebenberg, A. P. (2011). The Value of Enterprise Risk Management . *The Journal of Risk and Insurance , 78* (No 4), 795-822.

International Organization for Standardization. (2009 йил 13-11). *www.iso.org.* Retrieved 2012 йил 12-04 from http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=44651

IRM. (2002 йил 1-Februari). *http://www.theirm.org.* Retrieved 2012 йил 22-5 from http://www.theirm.org/publications/documents/ARMS_2002_IRM.pdf

Jacobsen, D. I. (2002). *Vad hur och varför? Om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen.* Lund: Studentlitteratur .

Jones, M. (2011). *Creative Accounting, Fraud and International Accounting Scandals* (1:a ed.). Hoboken: N.J Wiley.

Knight, F. H. (1921). *Risk, uncertainty and profit.* Boston: Houghton Mifflin Company.

Kollegiet för svensk bolagsstyrning. (2010 йил 1-Februari). *www.bolagsstyrning.se.* Retrieved 2012 йил 05-04 from http://www.bolagsstyrning.se/media/43746/svenskkodbolagsstyrn_2010_korrigerad20110321.pdf

Lam, J. (2003). *Enterprise risk management: from incentives to control* (1:a ed.). Hoboken: N.J Wiley.

Lam, J. (2001 йил 1-April). The CRO Is Here to Stay. *Risk Management* , pp. 16-20.

Liebenberg, A. P., & Hoyt, R. E. (2003). The Determinants of Enterprise Risk Management: Evidence . *Risk Management and Insurance Review , 6* (1), 37-52.

Magretta, J. (2005 йил 1-05). Why business models matter. *Harvard Business Review , 5*, pp. 86-92.

Mauer, F. (2009). Creating Value Through Enterprise Risk Management. *The Journal of Applied Business Research , 25* (3), 13-24.

Meulbroek, L. K. (2002). Integrated Risk Management for the Firm: A Senior Manager's Guide. *Journal of , 14*, 56-70.

Meyer, J., & Rowan, B. (1977). Institutionalized Organizations: Formal Structure as Myth and Ceremony . *The American Journal of Sociology , 83* (2), 340-363.

Moeller, R. R. (2007). *COSO Enterprise Risk Managemetn: Understanding the New Integrated ERN Framework* (1:a ed.). Hoboken : N.J Wiley.

Mossa, I. A. (2007). *Operational Risk Management.* New York: PALGRAVE MACMILLAN.

Nocco, B. W., & Stulz, R. M. (2006). Enterprise Risk Management: Theory and Practice. *Journal of Applied Corporate Finance , 18* (No 4), 8-20.

Power, M. (2004). *The Risk Management of Everything* (1:a ed.). London : Demos .

Quinn, L. R. (2006 йил 1-July). COSO at a crossroad. *Strategic Finance Magazine* , pp. 42-49.

Riksbanken. (n.d.). *www.riksbanken.se*. Retrieved 2012 йил 04-05 from http://www.riksbank.se/sv/Finansiell-stabilitet/Aktuella-regleringsforandringar/Den-nya-bankregleringen-Basel-III/

Rubin, H., & Rubin, I. (2005). *Qualitative Interviewing: The Art of HearingvData.* Thousand Oaks CA.: Sage.

Servaes, H., A, T., & Tufano, P. (2009). The Theory and Practice of Corporate Risk Management. *Journal of Applied Corporate Finance , 21* (4), 60-78.

Shafer, S. M., Smith, H. J., & Linder, J. C. (2005). The power of business models. *Business Horizons* (48), 199-207.

Shaw, H. (2006). *www.cfo.com*. Retrieved 2012 йил 25-04 from http://www.cfo.com/article.cfm/5598405

Shenkir, W. G., & Walker, P. L. (2006). *Implementing Enterprise Risk Management.* Virginia : Institute of Management .

Siegert, L., & Taylor, W. (2004). Theoretical aspects of goal-setting and motivation in rehabilitation. *TOC , 26* (1), 1-8.

Slywotzky, A. J., & Drzik, J. (2005 йил 1 -April). Countering the Biggest Risk of All. *Harvard Business Review* , pp. 78-88.

Standard and Poor. (n.d.). *www.standardandpoors.com*. Retrieved 2012 йил 12-04 from http://www.standardandpoors.com/ratings/erm/en/us

Stickel, E. (2001). Uncertainty reduction in a competitive environment. *Journal of Business research , 51* (3), 169-177.

Sullivan, L. (2003). *findarticles.com* . Retrieved 2012 йил 13-Maj from http://findarticles.com/p/articles/mi_qa5332/is_9_50/ai_n29026827/?tag=content;col1

Sveningsson, S., Alvesson, M., och Kärreman, D. (2009). Ledarskap i Kunskapsintensiva Verksamheter: Hjälteideal och vardagsmagi. In Å. Sterner (Ed.), *Ledarskapsboken* (pp. 30-58). Malmö: Liber .

Tufano, P. (1996). Who Manages Risk? An Empirical Examination of Risk Management Practices in the . *Journal of Finance , 51* (4), 1097-1137.

Vaughan, E. J. (1997). *Risk Management .* New York : Wiely & Sons .

von Grebmer, A. (2007). *Information and IT risk management in a nutshell: a pragmatic approach to ...* (1:a ed.). Norderstedt: Books on demand GmBh Germany .

Yin, R. (2003). *Study Research: Design and Methods.* Calif: Sage.

Appendix

Frågeställning intervjuer ERM

1. Internal Risk environment

- Finns en övergripande riskpolicy utarbetad och dokumenterad som gäller hela företaget? Exempel på innehåll: - Riskbenägenhet- Övergripande ramverk med processbeskrivning, beslutsordning, rapportering och krav på efterlevnad
- 1.2 Finns risk med som egen punkt på dagordningen till styrelsemötena?

2. Objective setting / risk horizon

- 2.1 Hur ser strategin ut? Strategiska mål (3-5 år) Budgetmål (1 år) Operationella mål (månadsvis)
- 2.2 Hur arbetar man med riskhantering i resp målsättningsprocess
- **3. Process for risk management (riskhantering)**
- 3.0.1 Finns en formaliserad och dokumenterad process för riskhantering

3.1 Risk identification

3.1.1 Finns det en formaliserad process/modell för att identifiera risker?

3.2 Risk assessment

- 3.2.2 Finns en formaliserad process och modell för att värdera, bedöma, besluta om åtgärder (risk response)
- 3.2.3 Finns något IT-stöd för ovanstående?

3.3 Roles and responsibility

3.3.1 Vem gör vad i process for Risk management

- Finns formella roller med ett uttalat ansvar?

3.4 Risk -- governance

3.4.1 Vad styr hur man hanterar risker? - Formellt regelverk med t ex gränsvärden

- Inget formaliserat, individuell hantering

3.5 Risk control

3.5.1 Finns systematiska kontroller av hur risker befintliga utvecklas; hur nya risker uppstår etc. Exemplifiera i så fall

3.6 Monitoring and reporting

- 3.6.1 Hur följer man upp utvecklingen av identifierade risker
- 3.6.2 Hur går rapportering till? Vem rapporterar, vad rapporteras, vem får rapporterna?
- 3.6.3 Hur används sinformationen?

3.7 Cross unit standard

3.7.1 Är riskhanteringen desamma för alla organisatoriska enheter?

3.8 Oversight and consolidation

3.8.1 Sammanställs företagets totala riskexponering?