Risikostyring som en integrert del av virksomhetsstyringen.
- faktorer som kan bidra til at risikostyringen integreres som en del av virksomhetsstyringen.

Risk management as an integrated part of the corporate governance.
- factors that can contribute to integrate risk management as a part of the corporate governance.

Miriam tesfaghiorghis og Anne reidun kjesbu

Handelshøyskolen ved UMB
Masteroppgave 30 stp. 2013

UNIVERSITETET FOR MILJØ- OG BIOVITENSKAP

Forord

Denne masteroppgaven er skrevet på Handelshøyskolen ved Universitetet for miljø- og biovitenskap (UMB). Oppgaven er skrevet som en avsluttende del av et toårig masterstudium i økonomi- og administrasjon, og tilsvarer 30 studiepoeng.

Masteroppgaven skrives som et bidrag til en bedre forståelse for hvordan risikostyringen kan integreres som en del av virksomhetsstyringen, da kriser og konkurser i det siste tiåret gjentatte ganger har vist oss viktigheten av dette. Oppgaven har fokus på hva teori, tidligere forskning, lovgivning og rammeverk for «beste praksis» sier om faktorer som er viktige for integreringen. Vi har også vært nysgjerrige på å få et bilde av hvordan dette fungerer i praksis, og har dermed intervjuet fire norske selskap med stor internasjonal virksomhet. I den anledning ønsker vi å takke informantene i disse virksomhetene, som har vært til stor hjelp i denne oppgaven; Gro Haugom i Yara ASA, Trond Stabekk i Kongsberg Automotive ASA, Rolf Arnljot Strøm i Orkla ASA og Svein Stolpestad og Frank Are Berggren i Jotun AS. Alle informantene har møtt oss med åpenhet, og vist engasjement for oppgaven.

Vi ønsker også å rette en stor takk til vår veileder, dosent Kjell Gunnar Hoff, for positiv innstilling, konstruktive tilbakemeldinger og gode innspill gjennom hele perioden. Til slutt ønsker vi å takke våre nærmeste for støtte og motivasjon gjennom hele prosessen.

Prosessen har vært svært lærerik, men til tider tidkrevende. Vi er veldig glade for å ha fått jobbet med et tema som vi anser som meget spennende og dagsaktuelt.

Ås, 12.06.2013

Miriam Tesfaghiorghis

Anne Reidun Kjesbu

Sammendrag
Denne oppgaven drøfter faktorer som er avgjørende for å integrere risikostyringen som en del av virksomhetsstyringen. Den finansielle krisen fra 2008 har satt risikostyring på dagsorden. Ikke nok med at risikobildet utvides, men risikoene blir også stadig mer komplekse samtidig som virksomhetene blir mer sårbare. Forskning viser at flere virksomheter har lidt store økonomiske tap som et resultat av at risikostyringen ikke har vært fullt ut forstått, og at den ikke inngår i selskapets styringsstruktur (corporate governance). Dette har ført til en økning i regulatoriske krav, med formål om å bidra til forbedring og utvikling av virksomheters risikostyring. For å lykkes med risikostyringen, bør den være en integrert del av selskapets virksomhetsstyring og ikke i en såkalt «silo-basert» tilnærming hvor risikoene blir behandlet separat og uavhengig av hverandre.

Denne oppgaven er hovedsakelig i to hoveddeler. Den første delen er en presentasjon og gjennomgang av den viktigste teorien om helhetlig risikostyring og virksomhetsstyring, herunder sentrale rammeverk og anbefalinger. Oppgavens andre del er en analysedel som er basert på dybdeintervjuer av fire norske selskaper med stor internasjonal virksomhet, som opererer i ulike bransjer. Vi ønsker å se nærmere på deres rutiner for risikostyring i lys av aktuell teori og forskning. Målet er å finne ut hvordan virksomheter kan tilrettelegge sine rutiner for identifisering og vurdering av risiko, risikohåndtering og kontrollaktiviteter, kommunikasjon og rapportering, samt hvordan ulike roller og ansvar bør fordeles for å lykkes med en helhetlig risikostyring.

Funnene i vår studie tyder på at det er flere faktorer som er avgjørende for å lykkes med integreringen. Blant faktorene er bedriftskulturen og lederens subjektive vurderingsevne svært viktig. I tillegg vil en desentralisering av risikostyringen med myndiggjøring og ansvarliggjøring av alle ansatte bidra til en god helhetlig risikostyring. Risikorutiner bør bygges inn i hver enkelt arbeidsprosess, hvor også retningslinjer må foreligge krystallklare. De ansatte må forstå hvilke risikoer som kan oppstå innenfor sitt ansvarsområde. Videre bør det foreligge en organisasjonsstruktur med hensiktsmessige ansvars- og rollefordelinger, noe som må henge sammen med virksomhetens risikostyring. Vi ser at virksomhetene også bør balansere hvor mye av styringen som skal foregå gjennom mennesker og hvor mye som skal legges i styringssystemene. Rapportering om risikoer bør inngå som del av den vanlige resultatrapporteringen til styret og ledelsen, men bør imidlertid begrenses til kun de viktigste risikoforholdene slik at ledelsen kan konsentrere seg om de viktigste tingene. I tillegg er det viktig at risiko sees på som en mulighet, ikke bare en trussel.

Abstract

In this thesis we will discuss the factors that are critical for integrating a firm's risk management as part of its corporate governance. After the financial crisis in 2008, risk management has become more of a focus area. Not only have the types of risks expanded, but the risks are becoming more complex as well as the firms are becoming more vulnerable. Research shows that companies have suffered huge financial losses as a result of not fully understanding how to manage risks, but it also shows that they have not included the risk management in the company's corporate governance. This has led to an increase in regulatory requirements, aiming to contribute to the improvement and development of the company's risk management. For the success of enterprise risk management, risk management should be integrated as part of the corporate governance and not as a separate and independent part.

This thesis is divided into two main parts. The first part is a presentation and discussion of the main theory of enterprise risk management and corporate governance, including central framework and recommendations. The second part includes an analysis which is based on in-depth interviews of four Norwegian companies with large international business operating in various industries. We want to take a look at their risk management procedures in the light of current theory and research. The goal is to find out how businesses can adapt their procedures for identifying and assessing risk, risk responses and control activities, communication and reporting, and how roles and responsibilities should be distributed to achieve the success of enterprise risk management.

The findings of our study suggest that there are several factors that are critical to the success of the integration. Among the factors, the corporate culture and the manager's subjective judgment are very important. In addition, a decentralization of the risk management with empowerment and accountability of all employees contribute to an enterprise risk management. Risk management procedures should be built into every working position in the company, where the guidelines must be completely clear. Employees must understand the risks that may occur within their remit. Furthermore, there should be an organizational structure with appropriate roles and responsibility distributions, which must be related to the enterprise risk management. Companies should also balance the amount of control that will take place through people and how much control to place through the management control systems. Risk reporting should be included as part of the regular performance reporting to the Board and management, but should be limited to only the most important risk factors to help

executives concentrating on the most important things. In addition, it is important to look at risks as a possibility, not only a threat.

Innholdsfortegnelse

Figurliste

Tabell liste

DEL I: INTRODUKSJON

1. INNLEDNING

Virksomheter er til en hver tid utsatt for negative og uforutsette hendelser som vil kunne påvirke virksomhetens drift og lønnsomhet. Flere konkurser og kriser i kjente virksomheter de siste årene har påvist viktigheten av god risikostyring, samtidig som forskning viser at måten risikostyringen har vært utført på har vært utilstrekkelig og ikke godt nok integrert i virksomhetsstyringen. Det har blitt et økt fokus på å integrere risikostyringen i den generelle virksomhetsstyringen, noe som har ført til at en helhetlig tilnærming til risikostyring har vokst frem. Lovgivningen har innført strengere krav til risikostyring, i tillegg til at en rekke komiteer og foreninger har gitt ut en beste praksis for hvordan helhetlig risikostyring kan benyttes for å oppnå en bedre styring. Virksomhetsstyring er avhengig av god risikostyring, og omvendt. For å kunne takle de negative og uforutsette hendelsene, må virksomhetene utarbeide en helhetlig risikostyringsstrategi som går på tvers av funksjoner og landegrenser, slik at risikostyringen ikke bare blir noe som gjøres ved siden av virksomhetsstyringen. Med bakgrunn i dette, ønsker vi å identifisere hvilke nøkkelkarakteristika som kan bidra til at risikostyringen blir en integrert del av virksomhetsstyringen.

Denne oppgaven er delt i to hoveddeler. I den første delen presenterer vi den viktigste teorien om helhetlig risikostyring, inkludert lovgivning, sentrale rammeverk og anbefalinger. Videre vil vi i del to gi eksempler på hvordan risikostyring fungerer i praksis i dag, basert på intervjuer av sentrale medarbeidere i fire norske selskap med stor internasjonal virksomhet. Ved å samle resultatene fra de fire virksomhetene, teori, forskning og «beste praksis» får vi dermed et bilde av hvilke forhold som er avgjørende for å integrere risikostyringen som en del av virksomhetsstyringen. Deretter vil vi analysere funnene og diskutere disse, og til slutt komme med vår anbefaling.

1.1. Bakgrunn for oppgaven

Det blir stadig mer utfordrende for virksomheter å takle de raske endringene i virksomhetens omgivelser. Ingenting tyder på at risikobildet vil bli mindre i tiden fremover. Dagens markeder, i eksempelvis deler av Europa, er i skrivende stund preget av nedgangskonjunkturer. Behovet for god risikostyring øker. Globalisering, nye markeder, prosjekter, produkter og teknologi representerer endringer som innebærer nye risikomomenter. Fra forskning og teori, synes det som om risikostyringen ikke er helt ut forstått i praksis. Det foreligger dessuten flere barrierer som gjør at virksomheter ikke har lykkes med å implementere en helhetlig risikostyring. For å kunne lykkes med forretninger i dagens marked, må virksomhetene løfte den fragmenterte risikostyringen opp på et helhetlig og strategisk nivå (Bellamy & Vikdal 1999). Helhetlig og integrert risikostyring handler om å være mer forberedt, noe som hjelper ledere til å bruke mer tid på å drive forretning og mindre tid på å slukke branner.

På grunnlag av dette er det identifisert et behov for å få risikostyringen som en integrert del av virksomhetsstyringen, slik at virksomhetene kan være bedre rustet til å håndtere dagens raskt endrede markedsforhold.

1.2. Problemstilling

Forskning har identifisert et gap mellom virksomhetens virksomhetsstyring og risikostyring. Vi har sett tilfeller hvor dette utføres i to adskilte deler, eller at virksomhetene ikke har lyktes med å samkjøre denne styringen. For å lykkes med risikostyring, bør den integreres som en del av virksomhetsstyringen. I denne oppgaven ønsker vi derfor å finne svar på følgende:

Hvilke faktorer bidrar til å få risikostyringen som en integrert del av virksomhetsstyringen?

Vi har illustrert vår problemstilling i figur 1 under.

Figur 1: Gap mellom virksomhetsstyring og risikostyringen

1.3. Oppgaveavgrensing

I tabellen nedenfor viser vi avgrensingen av oppgaven ved å beskrive hva som er oppgavens formål og ikke.

Formålet med oppgaven er:	**Formålet med oppgaven er ikke:**
- Å finne avgjørende faktorer som vil bidra til at risikostyringen integreres i virksomhetsstyringen. - Å lære av hvordan fire norske selskaper med stor internasjonal virksomhet utfører helhetlig risikostyring i praksis. - Sammenligne funnene mot teori, forskning og beste praksis for så å finne frem til faktorer som tydelig peker seg ut som avgjørende. - Fungere som en kilde og inspirasjon til hvordan virksomheter kan bygge opp rutiner for risikostyring, slik at risikostyringen blir en integrert del av virksomhetsstyringen.	- Å påvise at det er et behov for helhetlig risikostyring i en virksomhet. - Å gi en fullstendig analyse av virksomhetene vi har intervjuet - Å konkludere på om virksomhetene vi har intervjuet har tilfredsstillende og hensiktsmessige rutiner for risikostyring.

Tabell 1: Oppgaveavgrensning

1.4. Oppgavens struktur og oppbygning

Oppgaven inneholder 5 deler, inkludert introduksjonsdelen (del I).

- Del II**:** Teoretiske begreper og perspektiver

  I *kapitlene 2-6* vil vi presentere teoretiske begrep og perspektiv på risikostyring. Dette inkluderer bakgrunn for økt risiko, ulike typer risiko virksomheter utsettes for, samt utviklingen av risikostyringsbegrepet. Vi ser også nærmere på begrepet helhetlig risikostyring (Enterprise Risk Management), samt fordelene med å innføre dette. Deretter vil vi gi en oversikt over ulike krav og rammeverk som virksomheter må forholde seg til med hensyn til risikostyring. Her presenteres en rekke lovverk, anbefalinger, og rammeverk som er aktuelle i dag. Vi vil også se nærmere på virksomhetsstyringen (corporate governace), og hvordan den kobles til selskapets risikostyring. Til slutt har vi på grunnlag av teori og forskning som vi har presentert,

laget en samling av beste praksis for ulike deler av risikostyringen; som er henholdsvis identifisering og vurdering av risiko, risikohåndtering og kontrollaktiviteter, kommunikasjon og rapportering, samt roller og ansvar. Vi fant det mest hensiktsmessig med denne inndelingen da virksomhetene vi intervjuet presenterte sin risikostyring i disse delene, samt at rammeverk og anbefalinger presenterer risikostyringen i lignende oppdeling. Dette gjorde sammenligningen mot teori noe enklere og mer oversiktlig.

- Del III: Valg av metode

  I *kapittel 7* presenterer vi valg av metode, herunder bakgrunn for metodevalg.

- Del IV: Empirisk analyse

  Kapitlene 8-9 er vår analysedel. I kapittel 8 presenterer vi funnene fra dybdeintervjuene med de fire virksomhetene. I kapittel 9 analyseres og diskuteres funnene i lys av teori, forskning og beste praksis. Vi begynner her med en kort oppsummering av virksomhetenes viktigste trekk ved de ulike delene av risikostyringen, og deretter drøfter vi hva vi anser som de viktigste trekkene for å lykkes med en helhetlig risikostyring.

- Del V: Avslutning

  I kapittel 10 vil vi oppsummere oppgaven og komme med vår konklusjon og anbefaling, samt forslag til videre forskning.

DEL II: TEORETISKE BEGREPER OG PERSPEKTIVER

2. RISIKO OG RISIKOSTYRING

I dette kapittelet skal se på bakgrunnen for økt risiko, og definere risiko og risikostyringsbegrepet. Vi skal se på eksempler på ulike typer risiko virksomhetene må forholde seg til, og til slutt utviklingen av risikostyringsbegrepet.

2.1. Bakgrunn for økt risiko

Næringsdrivende står ovenfor en økende globalisering, en mer dynamisk konkurransesituasjon samtidig som kompleksiteten i teknologien fortsetter å øke. I tillegg ser vi en utvikling av mer komplekse prosjekter innen flere bransjer og at produktlivssyklusen stadig blir kortere. Dette gjør at risikoeksponeringen vokser, blir mer kompleks, mangfoldig og er i stadig endring. Virksomhetene opererer nå i helt andre omgivelser sammenlignet med bare for 5 år siden (Chapman 2012). Endringer i strategier, som for eksempel investering i fremvoksende markeder, store omorganiseringer, outsourcing av nøkkelprosesser og utvikling av nye produkter, kan bidra til å øke virksomhetens risikoeksponering. I en vurdering av hvordan risikostyring utføres i 14 store globale virksomheter i slutten av 1990 tallet, kom det frem at spekteret av risiko som bedrifter følte de måtte håndtere hadde blitt vesentlig utvidet og fortsatte å vokse i antall (Chapman 2012).

Nyere forskning har vist at risikoeksponeringen ikke er fult ut forstått av virksomhetene, og at måten risikostyringen gjennomføres på har vært utilstrekkelig. Simkins og Fraiser (Fraser & Simkins 2010) påpeker at en alvorlig hendelse ofte må finne sted for at risikostyring skal settes i fokus, og konsekvensene av dette kan ofte bli overreaksjoner eller uheldige prioriteringer. Flere konkurser og kriser i kjente virksomheter de siste årene har imidlertid ført til at flere har satt risikostyring på dagsorden. Etter terroristangrepet på World Trade Center og Pentagon 11.september 2001, fikk risikostyring større fokus da det syntes å ha vært utført utilstrekkelig løpende risikoplanlegging før angrepet. Da energiselskapet Enron gikk konkurs i desember 2001 og telekommunikasjonsselskapet WorldCom i juli 2002, ble utilstrekkelig eierstyring og risikostyringens «sårbare» side synlig. Dette skyldtes hovedsakelig mangel på integritet i finansiell rapportering og overholdelse av regelverk samt operasjonell svikt. Hendelsene viste verden at ingenting er for stort til å kollapse (Fraser & Simkins 2010). Mangelen på å forstå og håndtere risiko blir også sett på som en driver til den globale

finanskrisen i 2007-2010. Styrene i den finansielle sektoren ble beskyldt for å være hensynsløse, grådige og dysfunksjonelle. Omfanget av risiko hadde ikke blitt anerkjent, forstått eller tilstrekkelig håndtert i den finansielle industrien (Chapman 2012).

Blant flere norske virksomheter finnes det også lignende erfaringer og utfordringer. Professor i petroleumsøkonomi, Øystein Noreng fra Handelshøyskolen BI, hadde i 2010 en uttalelse om Statoil i Dagens Næringsliv; *«vekst internasjonalt innebærer også at Statoil utsetter seg for betydelig høyere risiko. Selskapet ville trolig gått konkurs hvis det hadde blitt utsatt for en ulykke av samme omfang som British Petroleum opplever, hvor katastrofen strømmet over fire millioner fat olje ut i Mexicogolfen»* (Dagens Næringsliv 2010).
I januar 2013 så vi også et eksempel på risikoen ved å operere i politisk ustabile områder. Angrepet mot Statoils gassanlegg i In Amenas i Algerie omtales som det verste terrorangrepet mot næringsliv de siste ti årene. Lars Christian Cacher, sjef for internasjonale operasjoner i Statoil har uttalt at *«terror er en risiko for energibransjen i tiden fremover» (Lindeberg 2013).*

Usikkerheter og risikoer er ikke noe nytt, men risikoen og dens natur har endret seg. Risiko har beveget seg fra kun å omhandle det finansielle perspektivet til nå også å inkludere:

- *Direkte trusler*, slik som terror.
- *Avbrytelser fra industrielle aksjoner*, for eksempel dersom underleverandører går konkurs.
- *Sikkerhetsutfall*, som kan oppstå i virksomhetens produkter, rutiner, personal og prosjekter.
- *Voksende erfaring om overførbare risikoer*, slik som for eksempel i servicelevering og forsikring.
- *Mer innovasjon* i virksomhetene.
- *Ødelegging av virksomhetens rennommé.*

*(*Hallaråker *& Vig 2006)*

Med dagens utvikling og kompleksitet i markedet, hjelper det ikke kun å forhindre at de store krisene skal oppstå. Virksomhetene må i tillegg *gjøre tingene riktig, og gjøre de riktige tingene,* gjennom drive forretningene effektivt og målrettet i den løpende driften (Bellamy & Vikdal 1999). For å forbedre en organisasjons evne til å håndtere risiko, må risikokapasiteten utvides til at flere ansatte deltar, forbedring av kommunikasjon om risiko, samt sikre effektivt lederskap og kulturforandringer (Hallaråker & Vig 2006).

2.2. Hva er risiko og risikostyring?

Mennesker og organisasjoner har ulike holdninger og forståelse av hva risiko er, og begrepet kan dermed defineres på ulike måter. Begrepet kommer fra det italienske ordet «risicare», som betyr å våge (Aven 2007). The Committee of Sponsoring Organizations of the Treadway Commission (COSO)[1] (Øvsthus & Kristiansen 2005) definerer risiko som «*muligheten for at en hendelse oppstår og virker ugunstig inn på oppnåelsen av målsettingene»*. ISO/IEC Guide 73[2] definerer risiko som «*en kombinasjon av sannsynligheten for en hendelse og dens konsekvenser» (*Hallaråker & Vig 2006*).*

Felles for definisjonene av risiko er usikkerheten med hensyn til utfallet av en hendelse. (Hallaråker & Vig 2006). I litteraturen knyttes begrepet ofte til noe negativt og truende. Dette er noe, som i følge Aven (Aven 2007), organisasjoner må forsøke å unngå eller i hvert fall redusere. Risikobegrepet er også nært knyttet til muligheter, og kan således betraktes som positivt og nødvendig. Med muligheter involvert må sammenhengen mellom risiko og avkastning vurderes. På den ene siden vil man utforske mulighetene, og på den andre siden unngå tap. Hendelser eller handlinger kan således representere en fare eller en mulighet for virksomhetens mål og strategier. Dette skaper utfordringer og må derfor balanseres.

Det er når det arbeides med *beslutninger under usikkerhet* at risikostyring er viktig. Risikostyring har som formål å sikre en balanse mellom utvikling og skapelse av verdier og unngå ulykker, skader og tap (Aven 2007). Risikostyring er alle tiltak og aktiviteter som blir gjort for å styre risiko. For å kunne styre risiko må virksomhetene følgelig ha innsikt i risikoforhold, effekten av ulike tiltak og i hvilken grad risikoen lar seg styre. Samtidig er det nødvendig med metoder, prosesser og strategier for å kunne kartlegge og styre risikoene (Aven 2007). Risikostyring handler dermed om å identifisere vesentlige risikoer og deretter iverksette mottiltak. På denne måten blir det totale risikobildet akseptabelt for den risiko virksomheten tolererer.

Risikostyring handler ikke bare om å etablere de riktige kontrollsystemene og prosessene, men også om å ha de riktige menneskene og den riktige risikokulturen. Disse to forholdene må balanseres. En bedrift kan overleve, og til og med blomstre, hvis den har gode mennesker og dårlige prosesser. Det kan den derimot ikke hvis tilfellet hadde vært det motsatte. Til syvende og sist blir en bedrifts risikoprofil drevet av de ansattes beslutninger og handlinger.

[1] COSO er et felles initiativ av fem virksomheter fra den private sektoren som utvikler rammeverk og veiledning om helhetlig risikostyring og internkontroll (Øvsthus & Kristiansen 2005).
[2] ISO/IEC Guide 73 gir ut generiske definisjoner for termer knyttet til risikostyring (Standard 2010).

Selv om risikostyringsprosesser, slik som rapportering og tilsyn, er nyttig til overvåking, så er det også viktig å passe på at de riktige menneskene er på plass. I tillegg til at de er motivert av den riktige kulturen og insentivene (Lam 2003).

2.3. Ulike typer risiko

En bedrift kan være utsatt for mange ulike typer risikoer. Vi har valgt å dele opp risikokildene i interne og eksterne faktorer. De interne faktorene skiller seg ut fra de eksterne ved at de i stor grad er generert internt og dermed innenfor innflytelsesområdet til enhver virksomhet. De eksterne faktorene derimot, er hovedsakelig utenfor virksomhetens kontroll. På grunn av dette kan den eksterne risikoen være vanskelige å forutsi og kontrollere (Chapman 2012). Tabellen nedenfor viser de ulike risikotypene vi skal se nærmere på i denne oppgaven.

Interne påvirkninger	Eksterne påvirkninger
Finansiell risiko	Juridisk risiko ("compliance risiko")
Operasjonell risiko	Politisk risiko
Teknologisk risiko	Markedsrisiko
	Sosial risiko

Tabell 2: Interne og eksterne påvirkninger

2.3.1. Interne påvirkninger

2.3.1.1. Finansiell risiko

Finansiell risiko defineres som en intern risikofaktor, som betyr at den i en stor grad kan kontrolleres av virksomheten. Finansiell risiko er eksponering for uønskede hendelser som svekker lønnsomheten og de ekstreme forholdene som fører til virksomhetens kollaps. Dette kan inkludere svikt i finansielle systemer, regulatoriske avvik eller problemer med å overholde ulike krav, negative endringer i valutakurser, stor avhengighet av en enkel leverandør, tap av en viktig kunde, tap av utenlandske investeringer samt dårlig sikringsbeslutninger. I tillegg til dette kan finansiell risiko også inkludere dårlige beslutninger ved investering i anlegg, maskiner og bygninger (Chapman 2012).

Omfanget av finansiell risiko er stort, eksempler på slike risikoer kan være:

	Type risiko:	Beskrivelse av risiko:
Finansiell risiko	*Likviditetsrisiko*	Et resultat av en kortsiktig manglende evne til å møte finansielle forpliktelser, slik som betaling til leverandører eller ansatte
	Kredittrisiko	Et resultat av manglende betaling av varer som leveres til kunder
	Renterisiko	Påvirker forbrukernes disponible inntekt. Dette kan resultere i en forverring av handel for både forhandlere og produsenter
	Inflasjon	Inflasjon på for eksempel investeringsprosjekter i form av kontantstrømmer og diskonteringsrenten over prosjektets levetid
	Valutarisiko	Ved at forventede kontantstrømmer fra utenlandske investeringer blir negativt påvirket av svingninger i valutakurser.
	Derivatrisiko	Oppstår på grunn av spekulasjoner i markedet eller svingninger ved for eksempel å kjøpe på et tidspunkt frem i tid med sikte på å anskaffe en vare til en pris lavere enn prisen som er gjeldene på tidspunktet.
	Systemrisiko	Tap som et resultat av feil grunnet feil i forretningsprosedyrer, prosesser eller systemer og kontroller.
	Outsourcingrisiko	Motparten har ikke klart å levere varene til avtalt tid, eller brutt kontraktbetingelsene

Tabell 3: Oversikt over ulike typer av finansiell risiko

2.3.1.2. Operasjonell risiko

I følge FSA (Financial Services Authority) er operasjonell risiko tilstede i alle bedrifter, og er kanskje den største risikoen bedriftene står ovenfor (Financial Services Authority 2003). Baselkomiteen, et internasjonalt organ for sentralbanker, definerer begrepet som *«risikoen for tap som et resultat av utilstrekkelig eller sviktende interne prosesser, mennesker, systemer eller fra eksterne hendelser» (Basel Committee on Banking Supervision 2004)*. Selv om definisjon er utarbeidet for banksektoren, har den en bred anvendelse. FSA fastslår viktigheten av at bedrifter selv må definere hva operasjonell risiko betyr for dem selv, sett i forhold til spekteret av dens virksomhetsaktiviteter og driftsomgivelser (Basel Committee on Banking Supervision 2004). Bedrifter må definere operasjonell risiko i forhold til sluttproduktet, og de ressursene og prosessene som blir brukt for å produsere dette (Financial Services Authority 2002b)

Omfanget av kildene til operasjonell risiko er stor. *FSA Integrated Prudential Sourcebook (Financial Services Authority 2002a)* beskriver operasjonell risiko til blant annet å omfatte følgende:

	Type risiko:	Beskrivelse av risiko:
Operasj. risiko	*Forretningsmessig risiko*	Negative endringer i en bedrifts marked, kunder eller produkter eller endringer i de økonomiske og politiske omgivelsene som opererer i. I tillegg anses også strategisk risiko i form av at bedriftens planer, støtte systemer eller implementering av disse planene, og som har en negativ effekt på bedriften
	Kriminalitetsrisiko	Tyveri, bedrageri og hacking.
	Katastroferisiko	Brann, oversvømmelser samt andre naturkatastrofer og terroristaktiviteter
	Risiko knyttet til informasjonsteknologi	Uautorisert tilgang, avsløring og datakorrupsjon

Tabell 4: Oversikt over ulike typer av operasjonell risiko

2.3.1.3. Teknologisk risiko

Teknologi kan hjelpe en virksomhet med å øke produktiviteten, redusere kostnader og drive veksten. Tidligere ble teknologi, som for eksempel IKT, brukt til å fjerne administrative og byråkratiske byrder, slik at personalet kunne bruke mer tid på å gjøre sine opprinnelige jobber. Nå er IKT blitt et redskap for virksomhetsplaner og vekst. I de konkurranseutsatte omgivelsene bedriftene i dag opererer i, kan en effektiv bruk av teknologi bidra til økt og bærekraftig verdi for interessentene. Denne forbedrede verdien blir ofte drevet av teknologiinvesteringer, optimalisering av ressurser og løpende vedlikehold, for å bevare påliteligheten. Teknologiske endringer representerer både muligheter og trusler sett i sammenheng med markedsandel og markedsutvikling. Introduksjon av ny teknologi i en bedrift kan imidlertid også åpne dører for en rekke ødeleggende risikoer, som kan føre til svekkelse av lønnsomhet, rykte og konkurransefortrinn eller i verstefall føre til virksomhetssvikt (Chapman 2012).

Det er en rekke årsaker til teknologisk risiko:

	Beskrivelse av risiko:
Tekn. risiko	Mangel på investering i teknologi, og den resulterende svekkelsen av evne til å konkurrere.
	Utilstrekkelig teknologisk ledelse og spesielt styring av IKT-prosjektet
	Utilstrekkelig ledelse av outsourcing
	Utilstrekkelig, upassende eller dårlig håndtering av teknologiske investeringer i form av produksjonsprosesser, produktdesign og/eller informasjonsstyring. Med dårlig håndtering menes dårlig kontinuitetsplanlegging, sikkerhet eller beskyttelse av intellektuell eiendom
	Utilstrekkelig beskyttelse mot virus, hacking og tap av konfidensiell informasjon

Tabell 5: Oversikt over ulike typer av teknologisk risiko

2.3.2. Eksterne påvirkninger

2.3.2.1. Juridisk risiko

Bedrifter opererer ikke i isolerte omgivelser, og må ofte samarbeide med andre virksomheter for å utnytte mulighetene. Virksomhetens aktiviteter kan være underlagt et bredt spekter av juridiske forpliktelser. Eksempel på slike forpliktelser er kontraktsforpliktelse, som oppstår når to eller flere personer inngår en juridisk bindende avtale med hverandre.

Det kan være mange kilder til juridisk risiko. Vi har i tabellen nedenfor listet en rekke faktorer som kan betraktes som juridisk risiko for en virksomhet:

	Beskrivelse av risiko:
Juridisk risiko	Brudd på lovgivninger,samt å få påtale for dette
	Unøyaktig oppføring av informasjon i form av feilinformasjon, materiell unnlatelse eller villedende meninger
	Mangler kunnskap om virksomhetens forpliktelser, og kan ikkje bevise at virksomheten har operert i henhold til loven eller å gjenkjenne og effektivt håndtere juridiske trusler
	Rettslige uenigheter med utenlandske handelspartnere som følge av for eksempel følge av mangel på forståelse av forskjellen med de lokale lover og utenlandske lover.
	Brudd på opphavsrett (copyright)
	Tap av omdømme, som et resultat av en tiltale eller uenighet med en kunde, partner eller leverandør.

Tabell 6: Oversikt over ulike typer av juridisk risiko

2.3.2.2. Politisk risiko

Når virksomheter etablerer seg internasjonalt, vil dette også medføre større grad av risikoer, her er politisk risiko i andre land ofte en krevende risiko å håndtere (Godal 2013). Et eksempel på dette er terroraksjonen i Algerie som vi omtalte innledningsvis. Før en virksomhet velger å etablere seg i et land, bør den overvåke landets politiske stabilitet, rettsvesen og menneskerettssituasjon. Etter etablering bør virksomheten i tillegg kontinuerlig overvåke sikkerhet, helseforhold og risikoen for korrupsjon. Ofte kan gode samfunnsengasjementer bidra til å redusere politisk risiko. I tabellen under er eksempler på hva politisk risiko er:

	Beskrivelse av risiko:
Politisk risiko	Terroranslag
	Politiske omveltninger
	Beslaglegging av verdier
	Korrupsjon

Tabell 7: Oversikt over ulike typer politisk risiko

2.3.2.3. Markedsrisiko

Markedsrisiko kan defineres som eksponering for potensielt tap som følge av endringer i markedspriser eller kurser, herunder endringer i aksjekurser, rentenivå og valutakurser. Alle virksomheter er eksponert for en form for markedsrisiko, men omfanget av eksponeringen varierer mellom ulike bransjer og virksomheter innenfor en bransje (Chapman 2012).

James Lam (2003) har identifisert tre typer av markedsrisiko: handelsrisiko, eiendel/gjeld mislighold og likviditetsrisiko. Handelsrisiko omfatter risikoen virksomheten står ovenfor i sine investeringer og handelsporteføljer som følge av endringer i renter, valutakurser, aksjekurser og råvarepriser. Eiendel/gjeld mislighold oppstår som følge av forskjeller i renten som påvirker eiendelene og gjelden i balansen. Likviditetsrisiko er risikoen for at en virksomhet ikke vil være i stand til å skaffe midler til å oppfylle sine finansielle forpliktelser etter hvert som de forfaller (Lam 2003).

Disse risikoene kan videre deles inn i flere risikotyper, og er oppsummert i tabellen nedenfor.

	Type risiko:	Beskrivelse av risiko:
Markedsrisiko	*Renterisiko*	Risikoen for økonomiske tap som følge av rente svingninger
	Valutarisiko	Risikoen for en negativ tilbakebetaling eller kostnader som følge av endringer i valutaprisene.
	Råvarerisiko	Risikoen for svingninger i råvareprisene
	Egenkapitalrisiko	Risikoen for svingninger i aksjeverdifondene.
	Basisrisiko	Risiko som følge av ulikheter i likviditet og ufullkommenheter i markedet.

Tabell 8: Oversikt over ulike typer markedsrisiko

2.3.2.4. Sosial risiko

Samfunnsansvar handler om hvordan verdier skapes, og hvordan bedriften påvirker mennesker, miljø og samfunn (NHO 2013). At en virksomhet tar samfunnsansvar, er en viktig forutsetning for å skape lønnsomhet og aksjonærverdier på lang sikt. Det oppstår ofte risikoer og muligheter for virksomhetene i spennet mellom lønnsomhet og i hvilken grad de vektlegger etikk, miljø og sosiale forhold. Dersom en virksomhet ikke tar hensyn til sosiale forhold i et land de etablerer seg, vil dette kunne medføre et ødelagt rennommé, som videre kan føre til konkurs. Ulike samfunnsgrupper legger også stort press på virksomhetene på å ta samfunnsansvar. Her er blant annet Næringslivets Hovedorganisasjon aktive og bidrar til å gi rettledning til virksomheter (VIPE 2013). I tabellen under ser vi noen eksempler på hva som kan ligge i sosial risiko:

	Beskrivelse av risiko:
Sosial risiko	Ødelagt rennommé på grunn av dårlig moralsk og etisk opptreden
	Bøter og reaksjoner i form av brudd på menneskerettigheter
	Virksomhetens (under) leverandører benytter umoralsk barnearbeid
	Virksomhetens forretninger ødelegger samfunn hvor de er etablert

Tabell 9: Oversikt over ulike typer sosiale risikoer

2.3.2.5. Andre eksterne faktorer

Andre eksterne faktorer kan være økonomisk risiko og miljømessig risiko. Økonomisk risiko kan dreie seg om samfunnets økonomiske tilstand, enten et bestemt land eller flere land. Dette kan føre til at en virksomhet ikke får solgt sine produkter, og kan dermed få store økonomiske problemer. Miljømessige risikoer kan for eksempel være ulike naturkatastrofer. En naturkatastrofe kan føre til store ødeleggelser og kostnader for en virksomhet, både på eiendeler og mennesker.

2.4. Utvikling av risikostyringsbegrepet

Det finnes flere tilnærminger til risikostyring. Risikostyringen har tidligere hatt et smalt omfang, som i litteraturen ofte omtales som den *tradisjonelle risikostyringen* eller en «silo-basert» tilnærming. I en slik tilnærming behandler virksomhetene risikoer hver for seg i såkalte «siloer», hvor hver silo representerer en risiko. For eksempel vil internrevisjonen håndtere finansiell rapporteringsrisiko, forretningsenhetene håndtere prosjektrisiko, og

treasury deals [3]vil håndtere valuta risiko. Virksomhetene analyserer hver «risiko silo» separat og utvikler egne strategier for hver enkelt risiko (Davenport & Bradley). Hvert område eller avdeling i virksomheten har sine egne former for rutiner, begreper eler løsninger. Problemene oppstår når de ulike prosessene skal samkjøres i virksomheten, og kan skape vanskeligheter når virksomheten skal få et helhetsbilde, eller se hvordan de ulike risikoene i organisasjonen henger sammen (Hallaråker & Vig 2006).

Utviklingen av stadig åpnere markeder og større konkurranse har gjort det stadig mer krevende å nå de mål som ledere og eiere setter for sine virksomheter, selv i gode tider. Det har ført til et økt behov for styringsmetoder som bidrar til å skape verdier for eierne. Helhetlig risikostyring, også omtalt som *Enterprise Risk Management (ERM),* utvider den tradisjonelle risikostyringen ved at det søker å inkludere helheten av de ulike risikoene virksomheter står ovenfor (Hallaråker & Vig 2006). Risikostyringen betraktes nå som et nytt element i strategisk ledelse ved at forretningsstrategien linkes opp mot dag-til-dag-risikoer (Noreng 2002). Helhetlig risikostyring har blitt en ny trend i virksomhetsstyring innenfor privat og offentlig virksomhet fra tidlig på 2000-tallet. Utviklingen har også funnet veien til Norge, og flere norske ledere er i ferd med å forstå at helhetlig risikostyring kan være et viktig supplement til dagens styringssystem.

Forskjellen mellom helhetlig risikostyring og den tradisjonelle tilnærmingen når det gjelder håndtering av risiko, er at helhetlig risikostyring krever et høyt nivå av tilsyn av alle risikoene samlet i virksomheten, i stedet for mange ulike tilsynsmenn som håndterer spesifikke risiko i «siloer». I en helhetlig risikostyring har virksomheten ofte en risikoansvarlig (Chief Risk Officer) eller en avdeling for helhetlig risikostyring som skal styre hvor mye risiko foretaket kan tolerere, vurdere risikoreduserende tiltak og ellers skape et helhetlig system for risikostyringen i virksomheten

(Banham 2005).

[3] Med *treasury deals*, menes en avdeling i virksomheten som utelukkende jobber med finansielle avtaler. (Wikipedia 2013b)

Tabell 10 nedenfor viser hva som karakteriserer de ulike tilnærmingene til risikostyring.

Faktor	Tradisjonell risikostyring	Risikostyring	Helhetlig risikostyring (ERM)
Perspektiv	Fysiske trusler	Alle trusler	Trusler og muligheter
Fokus	Spesifikke prosjekter	Spesielle operasjoner	Hele virksomheten og sammarbeidspartnere
Utføres av	Spesialister	Noen ledere	Alle
Detaljnivå	Komplekse analyser	Detaljerte analyser	Generelle vurderinger
Timingen	Engangs..	Regelmessig	Kontinuerlig
Språk	Forskjellige termer	Samme termer, men forskjellig perspektiver	Felles språk og perspektiv
Salgsargumenter	Strengere kontroll	Bedre beslutningstaking	Bedre koordinerte beslutningstaking og ansvarliggjøring
Rapporter	Detaljerte engangsrapporter	Høyt nivå, men oppdelte rapporter	Integrerte akselererte forretningsrapporterer
Verktøy	Data analyser	Undersøkelser	Kulturendring for å integrere ERM til arbeidsrutinene
Mål	Lavere forsikringspremier	Risiko identifiseres og håndteres i risiko registre	Mål oppnådd i tråd med et sett av verdier
Omfang	Overholdelse	Operasjonell	Strategisk
Visjon	Beskytte bedriftens ressurser	Beskytte styret og lederne	Utvikle en risikosmart arbeidsstyrke og styrke bedriftens omdømme
Drivere	Eksterne trussler	Administrerende direktør og risikoansvarlig	Interessenter, Administrerende direktør og risikoansvarlig

Tabell 10: Oversikt over ulike tilnærminger til risikostyring (Pickett 2005)

I den tradisjonelle tilnærmingen til risikostyring, er funksjonene adskilt der hver silo har sine egne verktøy for rapportering. Det kan oppstå problemer fordi de uavhengige systemene ikke kommuniserer med hverandre på tvers av de ulike forretningsområdene. Denne manglende koordineringen skaper videre ineffektivitet. I motsetning til dette gjør helhetlig risikostyring det mulig for virksomheter å dra nytte av en integrert tilnærming å håndtere risiko på. Helhetlig risikostyring krever at virksomheten ikke bare analyserer hver risiko separat, men også analyserer sammenhengen mellom de ulike risikoene (Davenport & Bradley). En helhetlig risikostyring gjør at fokuset til risikostyringsfunksjonen beveger seg fra defensivt til i større grad mot offensivt og strategisk (Liebenberg & Hoyt 2003).

3. HELHETLIG RISIKOSTYRING (ERM)

I dette kapittelet skal vi definere helhetlig risikostyring og ytterligere belyse hva som ligger bak denne definisjonen. Vi skal også se nærmere på tidligere forskning knyttet til forståelsen og implementeringen av helhetlig risikostyringen, og til slutt se på fordelene en slik tilnærming tilfører virksomheten.

3.1. Hva er helhetlig risikostyring (ERM)?

COSO definerer helhetlig risikostyring som følgende:

«en prosess, påvirket av organisasjonenes styre, ledelse og annet personell anvendt i en strategisk setting på tvers av organisasjonen, utviklet for å identifisere potensielle hendelser, som kan ha en effekt på organisasjonen, håndtere og styre risikoer innenfor dens risikoappetitt for å besørge rimelig sikkerhet med hensyn til oppnåelse av organisasjonens mål».

(Øvsthus & Kristiansen 2005)

Helhetlig risikostyring inkluderer følgende momenter:

- Risiko fra alle nivå i virksomheten
- Utnytter sikringer- og porteføljeeffekter fra behandling av risiko kollektivt
- Risikostyringen koordineres med risikovurdering, risikotiltak og risikoovervåkning
- Fokuserer på virkningen av virksomhetens overordnede samlede finansielle og strategiske mål. (Miccolis et al. 2001)

Dette er altså en prosess som skjer på tvers i bedriften, og involverer personell på alle nivåer i organisasjonen. Helhetlig risikostyring skal sørge for å øke virksomheters evne til å avstemme risikoappetitten med strategien. Samtidig knytter den vekst, risiko og verdiskapning sammen. I tillegg tar helhetlig risikostyring sikte på å øke beslutningsevnen vedrørende risikotiltak for å minimere operative overraskelser og tap (Øvsthus & Kristiansen 2005).

Som det fremgår av COSO sin definisjon, understrekes det at det er en direkte relasjon til de strategiske omgivelsene, og at målet med helhetlig risikostyring er å hjelpe virksomheter med å nå deres avkastningsmål. Fraser og Simkins (2010) hevder at helhetlig risikostyring må være forankret i og direkte koblet til virksomhetens strategi for at den skal være verdiskapende (Fraser & Simkins 2010). På samme måte må helhetlig risikostyring være en del av strategiske planleggings- og gjennomføringsprosessen for at den skal være effektiv.

Risikostyringsprosesser kan ikke skape risikofrie omgivelser, men helhetlig risikostyring kan bidra til at ledelsen kan operere mer effektivt i omgivelser der virksomhetens risikoeksponering aldri er statisk (Chapman 2012). Virksomhetens suksess avhenger dermed av ledelsens evne til å håndtere usikkerhet i arbeidet om å nå det ønskede målet.

3.2. Tidligere funn av virksomheters forståelse og innføring av helhetlig risikostyring

Helhetlig risikostyring er et relativt nytt innen den akademiske forskningen, og det første forskningsstudiet ble publisert for omkring 14 år siden. Mye av litteraturen er hovedsakelig knyttet til bruken av finansielle risikostyringsverktøy for å øke virksomhetens og aksjonærenes verdi. Det viser seg å være lite empirisk bevis og relevant litteratur om verdien av helhetlig risikostyring. Mangelen på klare empiriske bevis kan synes å begrense vekst av bruken av helhetlig risikostyring. Flere studier viser at det fortsatt er mange bedrifter som enda ikke har tatt i bruk verktøyet. Blant annet identifiserte Hoyt og Liebenberg (Liebenberg & Hoyt 2003) bare 26 bedrifter som hadde tatt i bruk helhetlig risikostyring i tidsrommet 1997-2001.

En ferskere studie av Pagach og Warr (2007) fant at bare 138 bedrifter i USA hadde tatt i bruk et helhetlig risikostyringsrammeverk (Pagach & Warr 2011). Et annet eksempel er resultatene fra undersøkelsen av *Economist Intelligence Unit*, hvor det kom fram at bare 41 prosent av selskapene i Europa, Nord-Amerika og Asia har tatt i bruk noe form for helhetlig risikostyring (Kleffner et al. 2003). Det hevdes at mangel på forståelsen av hvilke fordeler helhetlig risikostyring gir, kan være svar på dette (Rasid 2012). Dette var bakgrunnen for at Hoyt og Liebenberg i 2011 gjennomførte en studie om verdien av helhetlig risikostyring. Formålet med studiet var å kartlegge spesifikke bedrifter som hadde implementert et helhetlig risikostyringsprogram og deretter vurdere verdien av virkningene programmet ga. Forskerne valgte å fokusere på amerikanske forsikringsselskaper, for å kunne kontrollere de forskjellene som oppstår på grunn av regulatoriske og markedsmessige forskjeller på tvers av bransjer. Det ble funnet en positiv relasjon mellom bedriftens verdi og bruken av helhetlig risikostyring. Forsikringsselskapene med et helhetlig risikostyringsprogram hadde høyere verdi enn andre forsikringsselskap.

The Conference Board gjorde i 2007 en studie hvor det kom frem at virksomheter i første omgang innførte helhetlig risikostyring for å kunne tilpasse seg nye lovgivninger. Flere styrer

og daglig ledere prøver i dag å endre sin tilnærming til helhetlig risikostyring fra å fokusere på overholdelse av regler, til en mer strategisk vinkling. Dette på grunnlag av en større forståelse for at når risikostyringen integreres i hele virksomheten vil den også være mer verdiskapende (Fraser & Simkins 2010).

The Institute of internal auditors research foundation[4] utførte en global undersøkelse blant flere ulike bedrifter i forskjellige bransjer for å finne ut mer om helhetlig risikostyring i praksis (Fraser & Simkins 2010). Ved å intervjue administrerende direktør, leder for risikostyring, internrevisorer samt interne rådgivere ville de finne ut mer om problemer knyttet til implementering og bruken av helhetlig risikostyring. En analyse av benchmarking undersøkelsene indikerte følgende:

- Et ønske om et felles rammeverk, samt en ordning for eierstyring og selskapsledelse var nøkkeldriverne for å innføre helhetlig risikostyring. I tillegg er det ofte et krav fra selskapets eiere. Andre drivere for implementeringen var et økende konkurransepress, et ønske om stabile resultater, etterfølge reguleringer, virksomheten hadde nylig opplevd en katastrofal hendelse, prissvingninger eller regulering av børsen.
- Virksomhetene så på helhetlig risikostyring som et verktøy for å få forbedre kontrollen med forretningsproblemene, samt få en mer stabil trend for resultatene.
- Det var helst de større bedriftene som benyttet seg av helhetlig risikostyring.
- Toppledere fører helhetlig risikostyringsaktiviteter, og internrevisjonen spiller en betydelig rolle ved implementeringen av helhetlig risikostyring.
- Forskerne identifiserte topp fem hindringer virksomhetene møter på med helhetlig risikostyring:
    - Organisasjonskulturen
    - Ledelsen er ikke kjent med fordelene med helhetlig risikostyring
    - Manglende formaliserte prosesser
    - Språk og definisjoner
    - Mangel på verktøy
- Andre barrierer var mangel på tilpassede IT-systemer, mangel på riktig kompetanse. Videre synes kostnadene å være for store og helhetlig risikostyring virket for krevende.

[4] The IIA Research Foundation gir årlig ut publikasjoner og forskningsresultater innenfor områdene revisjon, risikostyring, styring og kontroll samt corporate governance (Norges Interne Revisorers Forening 2013)

- Omfattende risikovurderinger eksisterte i et fåtall av virksomhetene.
- Helhetlig risikostyring kan i utgangspunktet være mer et verktøy for ledelsesinformasjon, heller enn en driver for selskapets resultater
- I virksomhetene benyttes det flere ulike verktøy og matriser for helhetlig risikostyring

3.3. Fordelene med helhetlig risikostyring

COSO- rammeverket hevder at effektiv helhetlig risikostyring gir virksomheter en forbedret evne på flere områder, og kan oppsummeres med følgende (Øvsthus & Kristiansen 2005):

- *Samordne risikoappetitt og strategi*
  Ledelsen evaluerer forskjellige strategiske alternativ og setter mål som passer den valgte strategien. Det etableres videre en basis for drift, rapportering og overholdelse av mål, i tillegg til at mekanismer for å håndtere risiko tilhørende risiko blir utviklet. Alt dette må være i tråd med virksomhetens risikoappetitt.
- *Forbedre beslutninger som gjelder risikohåndtering*
  Risikostyring gir støtte til å identifisere og velge mellom alternative måter å håndtere risiko på.
- *Reduserer driftsrelaterte overraskelser og tap*
  Virksomheten reduserer overraskelser, kostnader eller tap ved at de blir flinkere til å identifisere potensielle hendelser, vurdere risiko og iverksette tiltak.
- *Identifiserer og håndterer flere risikoer samt på tvers av forretningsområder*
  Enhver virksomhet står ovenfor en rekke risikoer som påvirker forskjellige deler av virksomheten. Ledelsen må ikke bare håndtere individuelle risikoer, men også forstå hvordan de henger sammen med andre risikoer. Helhetlig risikostyring gjør det mulig å svare effektivt på konsekvensene av de ulike risikoene og dens påvirkninger. I tillegg til at den koordinerer tiltakene.
- *Utnytter muligheter*
  Ved å vurdere mulige potensielle hendelser, i stedet for bare trusler, kan ledelsen proaktivt identifisere og realisere muligheter.
- *Forbedrer utnyttelsen av kapital*
  Virksomheten kan få pålitelig informasjon gjennom risikostyringsprosessene. Dette gjør at ledelsen effektivt kan vurdere det totale kapitalbehovet og effektivt forbedre allokeringen.

I tillegg kan helhetlig risikostyring bidra til å bygge tillit i interessent - og investeringsmiljøet, noe som blir stadig viktigere desto mer kompliserte omgivelsene blir (Chapman 2012). Institusjonelle investorer, ratingbyråer og regulatorer er mer fokusert og ivrige etter å lære om en organisasjons evne til å forstå og håndtere risiko. Eksempelvis ønsker investorene å forstå graden av risiko deres investeringer utsettes for, og om avkastningen vil bli tilfredsstillende gitt forventet risiko. Når i tillegg styremedlemmer og ledere blir bedt om å forklare rammeverk, retningslinjer og prosesser de bruker for å håndtere risiko, vil helhetlig risikostyring være et strukturert verktøy i etablering, beskrivelsen og demonstreringen av en proaktiv risikostyring.

Fordelene med helhetlig risikostyring kan oppsummeres med tre momenter: forbedring av virksomhetens ytelse, økt organisasjonsmessig effektivitet og bedre rapportering av risiko (Chapman 2012).

4. CORPORATE GOVERNANCE

I dette kapittelet ønsker vi å se nærmere på hvordan virksomheter er organisert og strukturert. Vi skal se på hva som ligger i begrepet «corporate governance» og hvordan dette påvirker virksomhetens risikostyring. Deretter skal vi se på bedriftskulturens påvirkning på risikostyringen, og tilslutt skal vi se på koblingen mellom corporate governance og risikostyring.

4.1. Hva er «Corporate Governance»?

Begrepet «corporate governance», som på norsk omtales som eierstyring og selskapsledelse, er et mye brukt begrep både internasjonalt og i Norge. Vi har videre i denne oppgaven valgt å omtale begrepet uten den norske oversettelsen.

Organization for Economic Cooperating and Development (OECD) definerer corporate governance følgende;

«involves a set of relationships between a company's management, its board, its shareholders and other stakeholders … (and)… provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined».

(OECD 2004)

Det beskriver altså hvordan en virksomhet styres og ledes gjennom retningslinjer, roller og ansvar mellom de ulike aktørene i virksomheten, slik som styret, ledelsen, aksjonærer og andre interessenter. Corporate governance legger føringer i regler og prosedyrer for hvordan forretningsmessige beslutninger skal tas. På denne måten settes det en struktur for å sikre at selskapet når målene sine, samt at prestasjonene overvåkes underveis (OECD 2004).

I en god corporate governance inngår åpenhet og demokrati, hvor beslutninger bør tas kollektivt av eierne, og ikke bare av et fåtall av ledere som kan ha en annen agenda enn eierne. Det bør også tilrettelegges for effektiv overvåking, samt insentiver for styret og ledelsen til å kunne følge opp mål som er til det beste for styret og dens aksjonærer (OECD 2004). Corporate governance handler om å foreta de riktige beslutningene for eierne og øvrige interessenter. Virksomheter med gode corporate governance-prosesser vil skape tillit til offentligheten og tiltrekke seg investorer (PricewaterhouseCoopers 2007).

4.1.1. Norsk anbefaling for eierstyring og selskapsledelse (NUES)

NUES gir ut den norske anbefalingen om corporate governance. Formålet med anbefalingen er at det skal foreligge en klargjøring av rolleinndelingen mellom aksjeeierne, styret og daglig ledelse i norske børsnoterte virksomheter, utover det som står i lovgivningen. Den skal i tillegg bidra til økt verdiskapning, samt bidra til at tillitten blant interessentene øker. Det er av felles interesse at virksomhetene styres på en betryggende måte, da de børsnoterte selskapene står for forvaltningen av en stor andel kapital og er dermed ansvarlig for en betydelig del av verdiskapningen i samfunnet.

Anbefalingen henvender seg i hovedsak til selskapets styre, som har det overordnede ansvaret for at anbefalingen etterleves. De er i tillegg ansvarlig for å utarbeide en samlet redegjørelse for virksomhetens corporate governance (Norsk utvalg for eierstyring og selskapsledelse 2013).

4.1.2. OECD Principles of Corporate Governance

OECD har utarbeidet prinsipper for tiltak for god styring av corporate governace som er gjeldende for dens medlemsland men også land utenfor OECD. Formålet med prinsippene er å bistå landene i deres arbeid med å forbedre og evaluere de institusjonelle og regulatoriske rammeverk for corporate governance. Prinsippene henvender seg først og fremst til både finansielle og ikke-finansielle børsnoterte selskap, men kan også være et nyttig verktøy for å forbedre corporate governance i ikke-børsnoterteselskap. Det fokuseres på styringsproblemer som kan oppstå som et resultat av delingen mellom eierskap og kontroll. Dette kobles ofte til prinsipal- agent forholdet mellom aksjonærer og ledelsen, men også kontrollerende aksjeeiere ovenfor minoritetsaksjonærer.

OECD har identifisert en rekke basis momenter som ligger til grunn for en god corporate governance, som OECD prinsippene bygger på. Prinsippene er ikke ment å være en detaljert beskrivelse for nasjonal lovgivning, men ønsker å identifisere mål knyttet til corporate governance samt komme med forslag om ulike metoder for og nå dem (OECD 2004).

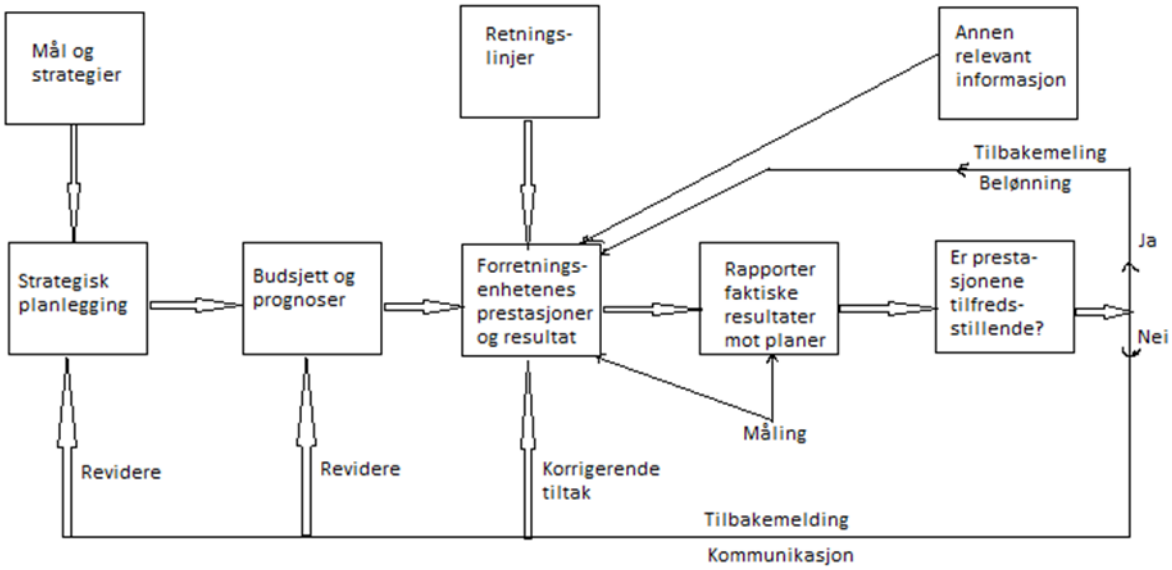
OECD anbefalingen bygger på 6 prinsipper for corporate governance:

1. Å sikre grunnlaget for et effektivt corporate governance rammeverk
2. Aksjonærenes rettigheter og eierskapsfunksjoner
3. Likebehandling av aksjonærene

4. Interessentenes rolle i corporate governance
5. Innsyn og åpenhet
6. Styrets ansvar

(OECD 2004)

4.2. Ledelsens overvåknings- og styringssystem



Figur 2: Generell styring- og overvåkningssystem (Anthony & Govindarajan 2007)

Figur 2 ovenfor, viser en generell modell for hvordan ledelsen styrer og overvåker sin virksomhet, samt måler og følger opp sine underliggende forretningsenheter. I den strategiske planleggingen, fastsettes virksomhetens mål og strategier. I denne prosessen bør også risikostyringsprosessen inkluderes for så også å være del av de videre prosessene i figuren. Basert på strategiene og de overordnede målene utarbeides budsjetter og lignende verktøy for å sette mål for de underliggende selskapene, som også er grunnlaget for hva de måles etter. Virksomheter benytter i dag stor grad av finansielle og ikke finansielle styringsparametere[5] for å måle selskapets utvikling. Ledelsen legger også retningslinjer og rutiner for hvordan avdelingslederne skal arbeide, herunder bør det tydelig fremgå ansvarsområdet. Disse retningslinjene må være krystallklare. Resultatene til forretningsenhetene rapporteres oppover og måles mot budsjett og planer. Gode resultater belønnes, og dårlige resultater krever tiltak,

[5] Styringsparametere omtales også som *Key Performance Indicatoris (KPI'er)*, og vil benytte dette i resten av oppgaven.

og revidering av den strategiske planleggingen og de oppsatte budsjettene(Anthony & Govindarajan 2007).

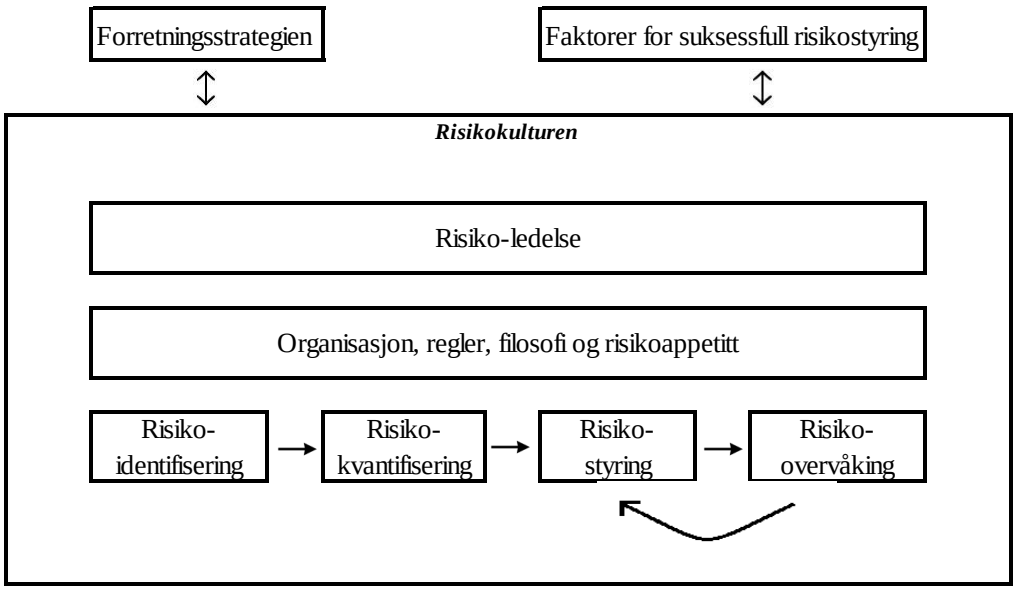
Ledelsens styringssystemer påvirker de ansattes adferd. Ledelsens systemer for styring og overvåking vil påvirke selskapets evne til å nå sine mål, og det må være en samkjøring mellom de ansattes mål og virksomhetens mål. (På engelsk kalles dette «goal congruence»). Når et styringssystem skal utarbeides, er det viktig at det passer med virksomhetens uformelle struktur som ledelsesstil, bedriftskultur og etiske retningslinjer. De etiske retningslinjene kan beskrive i hvilken grad de ansatte forplikter seg til virksomheten, og deres lagånd samt ønske om å gjøre en god jobb for virksomheten. Bedriftskulturen er den viktigste uformelle strukturen, som beskriver selskapets felles tro, delte verdier, og adferdsnormer. Kulturen er svært viktig, da det vil være årsaken til at en virksomhet gjør det bra og en virksomhet gjør det dårlig, selv om virksomhetene er identiske og har samme styringssystemer. I tillegg vil type ledelsesstil være høyst avgjørende, da dette ofte har størst påvirkning på overvåkning og kontroll av selskapet. Videre kan ikke et slikt system fungere uten at det er en klar ansvars- og rollefordeling og at det er fult ut forstått av virksomhetens ansatte. Sistnevnte er også avgjørende for en god kommunikasjon (Anthony & Govindarajan 2007).

4.3. Bedriftskulturens påvirkning på risikostyring

En bedriftskultur kan beskrives som måten en organisasjon tenker, føler og handler på (Entrepreneur 2013). Den kan også beskrives som et sett uskrevne og skrevne regler. De skrevne reglene ligger i selskapets rutiner og instrukser, men dersom det oppstår uventede hendelser som ikke dekkes av rutinene, er det derimot medarbeiderens vurderingsevne som vil være avgjørende. Bedriftskulturen bestemmer hvilken informasjon som er viktig og sentral, og hva som kan utelukkes. Den angir hva som er "passende" atferd når en ansatt skal foreta et valg på vegne av organisasjonen. Vage regler og uklare mål gir rom for å anvende personlig skjønn som ikke nødvendigvis er i tråd med organisasjonens rammer. Derfor er det viktig at det ligger en god risikokultur[6] til grunn (Fraser & Simkins 2010). I figur 3 nedenfor, ser vi at risikokulturen ligger som grunnlag i alle de ulike beslutningsprosessene for helhetlig risikostyring (Banks 2012). Risikokulturen må også henge i tråd med selskapets overordnede strategi. Ofte kan kulturen vinne over strategiene dersom de ikke hører sammen, noe som kan

[6] Med risikokultur menes at ledere og medarbeidere tenker og handler ut fra en risikoforståelse for å oppnå, opprettholde og videreutvikle risikoprofilen til organisasjonen i overensstemmelse med definerte mål (Wiggen 2008)

innebære at strategiene ikke blir gjennomført. Dette er en av risikofaktorene for suksessfull risikostyring.



Figur 3: Den fundamentale risikostyringsprosess (Banks 2012)

For å skape en god bedriftskultur med hensyn til risiko i en virksomhet, er et viktig å sikre at alle ansatte er innforståtte med, og opptrer på en forsvarlig måte innenfor sine rammer av risikovurderinger, og at dette er i samsvar med virksomhetens risikoappetitt. Risikostyring er ikke bare noe ledelsen bør jobbe med, men alle i organisasjonen bør ha et forhold til risikoer og være i stand til å identifisere de. På en slik måte kan organisasjonen være i stand til å reagere på et tidligere tidspunkt (Fraser & Simkins 2010).

Kultur er adferd. Handlinger snakker høyere enn ord. Derfor er det viktig at ledelsen går foran som et godt eksempel. Selskapets risikofilosofi gjenspeiles i hvordan ledelsen styrer selskapet, og er formulert gjennom selskapets retningslinjer, normer, resultatindikatorer og avviksrapporter, samt hvordan det kommuniseres både formelt og uformelt innad i bedriften og utad. Rutiner bør utformes slik at de skaper den ønskede adferden med hensyn til gode beslutningsprosesser og riktig risikohåndtering. Skal man skape en god bedriftskultur kreves en bevisst tilnærming. Risk Manager Magazine (Fraser & Simkins 2010) har definert følgende karakteristikker for å skape en god bedriftskultur med hensyn til risiko:

- Sterkt lederskap i organisasjonen og dens prosjekter
- Ha en deltakende ledelsesstil

- Delegere risikostyringen til hele arbeidsplassen
- Benytte de ansattes kunnskap og kompetanse
- Ansvarliggjøring av de ansatte for sine handlinger
- Muliggjøre identifisering av risiko på alle nivå i organisasjonen
- Avklare kontroller før risikoene oppstår
- Tilrettelegge for god kommunikasjon og samarbeid
- Oppfordre til årvåkenhet med hensyn til risiko i hele organisasjonen

Bedriftskulturen kan være et viktig konkurransefortrinn, siden den er vanskelig å kopiere. Den kommer imidlertid ikke i form av et vedtak på styremøte. Det må etableres eierskap gjennom involvering av organisasjonens ansatte (Ledernytt 2012).

4.4. Koblingen mellom corporate governance og risikostyring

God corporate governance er en avgjørende komponent for å lykkes med helhetlig risikostyring (James Lam, 2003). Grunnen til dette er at det legger til rette for en ovenfra-og-ned overvåkning av risikostyringen. Effektiv corporate governance krever at virksomhetens styre fokuserer på selskapet som helhet samt forvaltning av det, og unngår for mye involvering i detaljstyring av selskapet. På denne måten kan virksomheten styres i den riktige retningen som vil gi størst verdiskapning. Fokuset på corporate governance har hatt en stor drivkraft på endringer i forhold til helhetlig risikostyring (Lam 2003). En beste praksis for corporate governance henviser hovedansvaret for risikostyringen til styret.

OECD har gitt ut prinsipper for en beste praksis for corporate governance, hvor også det fokuseres på styrets ansvar for å påse at selskapet har iverksatt betryggende og hensiktsmessige systemer og rutiner for risikostyring er tilstede i selskapet. Styrets involvering og engasjement er viktig for å lykkes med helhetlig risikostyring. En annen viktig kobling mellom corporate governance og helhetlig risikostyring, er at det må foreligge samme fokus med hensyn til strategisk retning samt involvering fra toppledelsen. Ulike konkurser og skandaler er ofte ikke bare et resultat av dårlig risikostyring, men også for dårlig selskapsstruktur med hensyn til corporate governance. Det henger ofte sammen. Selskap med dårlig struktur og ansvar- og rollefordeling, har også ofte dårlig kompetanse i risikostyring (Lam 2003). For å få til en effektiv risikostyring, må det etableres en hensiktsmessig organisasjonsstruktur. «The Three lines of Defense Model» er en modell som påpeker

hvordan virksomheten kan utarbeide forsvarslinjer, ansvar- og rollefordeling samt kommunikasjonslinjer. (Dette kommer vi nærmere tilbake til i kapittel 6.4).

Risikostyringen bør være en sentral del av de daglige arbeidsprosessene. En rekke aspekt i helhetlig risikostyring er sterkt koblet til styrets arbeid. Blant annet å sette selskapets risikoappetitt og retningslinjer, bestemme organisasjonsstrukturen, samt etablering av bedriftskultur og verdier.

5. KRAV OG RAMMEVERK FOR HELHETLIG RISIKOSTYRING

Etter hvert som det blir mer utfordrende å drive forretninger, vil ulike lover og rammeverk bidra til å forbedre og utvikle virksomhetenes risikostyring ved å representere et absolutt minimum av krav de må forholde seg til.

For store norske internasjonale virksomheter, som opererer i flere ulike land, vil det være flere lover og regler i ulike land å forholde seg til. En virksomhet som er notert på Oslo Børs, vil forholde seg til andre lover og regler enn en virksomhet som tilhører New York Stock Exchange (Hallaråker & Vig 2006). I Norge vil særskilt aksjelovgivningen, regnskapsloven, Norsk anbefaling for Eierstyring og Selskapsledelse (NUES) samt EU-direktivene, stiller krav og oppfordrer virksomhetene til helhetlig risikostyring. I tillegg til lovgivningen vil også ulike komiteer og foreninger også ha en innvirkning på virksomhetenes risikostyring og praksis, herunder COSO sitt rammeverk for helhetlig risikostyring fra 2004 samt den Internasjonale Standarden ISO 31000:2009. Disse rammeverkene som vedrører risikostyring, har som formål å tilrettelegge for risikostyringsprosessene, og bidra til at det tas gode vurderinger og beslutninger (Fraser & Simkins 2010).

Vi ser at lovgivningen legger generelt hovedansvaret for risikostyringen på styret, og er forsiktig med å utdype, presisere eller gi rammen for hvordan ansvaret skal fordeles. COSO-rammeverket og ISO 31000:2009 standarden kommer derimot med anbefalinger til hvordan ansvar og roller bør foreligge i en virksomhet. COSO sitt rammeverk er godt kjent hos myndighetene og mye brukt blant virksomhet i Europa og Nord-Amerika (Hallaråker & Vig 2006). ISO 31000:2009 inneholder praksis fra COSO, PMI (Project Management Institute), den Australske og New Zealands standard (AS/NZS 4360:2004) og andre ledende internasjonale risikostyringsstandarder, og er også en anerkjent standard (Fraser & Simkins 2010).

Vi vil i det følgende gjennomgå de mest aktuelle lover, rammeverk og anbefalinger med hensyn til hva som er mest aktuelt for de fire virksomhetene vi har intervjuet. Dette er følgende:

Lovgivning:

- Aksjelovgivningen
- Regnskapsloven
- Norsk anbefaling for eierstyring og selskapsledelse (NUES)
- EU-krav:-4 og 8 direktiv

Rammeverk for beste praksis:

- COSO – Et integrert rammeverk for helhetlig risikostyring (2004)
- Den Internasjonale Standarden ISO 31000:2009

5.1. Aksjelovgivningen

Aksjelovgivningen angir hovedelementene og de overordnede rammene for virksomheters risikostyring og internkontroll[7]. Styrets ansvar kan leses ut i fra aksjelovgivningen § 6-12 og § 6-13. Her fremkommer det at styret har et forvaltningsansvar og et tilsynsansvar. Hovedelementene i forvaltningsansvaret er å lede organisasjonen, hvor styret tar de overordnede beslutningene som legger føringer for driften av organisasjonen. Videre skal styret fastsette planer og budsjetter for virksomheten, og kan fastsette retningslinjer, i tillegg til at de skal holde seg orientert om selskapets økonomiske stilling. I tilsynsansvaret inngår det at styret skal føre tilsyn med den daglige ledelse og virksomheten, i tillegg til at det kan fastsettes instrukser for den daglige ledelse. I aksjelovgivningen § 3-4 fremkommer det at styret også må påse at virksomheten har en forsvarlig egenkapital. Risikoen og omfanget av organisasjonens virksomhet avgjør om kapitalen er forsvarlig. Dersom egenkapitalen er lavere enn forsvarlig, krever § 3-5 at styret har handleplikt (Justis- og beredskapsdepartementet 1999).

[7] Internkontroll er prosessen som foretas av selskapets styre, ledelse og annet personell, utformet for å gi rimelig grad av sikkerhet med hensyn til selskapets måloppnåelse med målrettet og kostnadseffektiv drift, pålitelig finansiell rapportering og etterlevelse av lover og regler. Internkontroll kan deles i 5 komponenter som alle må være tilstede for at en internkontroll skal være effektivt. Disse er: Overvåkning, Informasjon & kommunikasjon, kontrollaktiviteter, risikovurdering og kontrollmiljø (Solberg 1996).

5.2. Regnskapsloven

Risiko er også omtalt i regnskapsloven. I regnskapsloven § 3-3a står det at årsrapporten skal inneholde en *«beskrivelse av de mest sentrale risiko- og usikkerhetsfaktorene*». Dette er også noe § 5-6, fjerdeledd i verdipapirhandelloven krever at halvårsberetningen til børsnoterte selskap skal inneholde. «Viktige begivenheter» og «sentrale risiko- og usikkerhetsfaktorer» er elementer i beretningene som krever en nærmere beskrivelse av konkrete risikofaktorer som virksomheten er eksponert for. Det er dermed ikke nok med en generell beskrivelse av risikofaktorer for bransjen. Beretningen skal foretas av «ansvarlige personer», som i henhold til norsk lovgivning er styret og ledelsen. Dette betyr at det forventes at styret og ledelsen har en oversikt over risiko og usikkerhet (Finansdepartementet 1999).

5.3. Norsk anbefaling for Eierstilling og Selskapsledelse (NUES)

Norsk Utvalg for Eierstilling og Selskapsledelse (NUES), har utarbeidet en anbefaling som alle børsnoterte selskaper må følge. Kapittel 10 i NUES omhandler risikostyring og internkontroll. Hovedpunktene i anbefalingene har vi oppsummert nedenfor:

1. Styret er ansvarlig for å påse at virksomheten har gode systemer for internkontroll og risikostyring i forhold til omfanget og arten av selskapets virksomhet. Internkontrollen og systemene bør være i tråd med virksomhetens verdigrunnlag og etiske retningslinjer.
2. Styret bør årlig gjennomføre en gjennomgang av selskapets viktigste risikoområder og den interne kontroll.
3. Styret bør i årsrapporten gi en beskrivelse av hovedelementene i selskapets interne kontroll og risikostyringssystemer knyttet til dens finansielle rapportering.

Fra anbefalingen ser vi at i styrets overvåkningsansvar legges det vekt på å holde tilsyn over faktiske risikoforhold samt at de interne kontrollene som er iverksatt fungerer tilfredsstillende. Det er viktig å forstå kontrolltiltakene siden det er den gjenværende risikoen som er igjen etter at kontrolltiltakene er utført (residualrisikoen) som er den reelle eksponeringen for virksomheten. Selv om styret må overvåke disse systemene, er det kun det som er relevant for finansiell rapportering som må redegjøres for i årsrapporten (Norsk utvalg for eierstyring og selskapsledelse 2013).

5.4. EU-krav: 4.- og 8. direktiv

De tre reguleringene vi har sett på til nå, har i hovedsak regulert styrets ansvar og forhold til risikostyring og kontrolloppfølging. I 2008 innførte også EU to nye direktiv som skulle forsterke disse kravene. EUs 4. og 8. direktiv omhandler, i likhet med aksjeloven og NUES, krav til risikostyring, internkontroll og finansiell rapportering. Direktivene retter seg mot styret, og skal bidra til en større grad av involvering (Gaudernack 2008).

EUs 4. direktiv er *Årsregnskapsdirektivet.* Direktivet krever at selskapet skal redegjøre for foretaksstyringen i årsberetningen, i tillegg til en beskrivelse av hovedlinjene i selskapets internkontroll og risikostyringssystemer relatert til finansiell rapportering. Dette kan også ses på som en presisering av de allerede eksisterende anbefalingene fra NUES.

Det 8. direktivet er *Revisjonsdirektivet.* Her stilles det krav til at styret i foretak av allmenn interesse[8] skal etablere et revisjonsutvalg. Utvalget skal bestå av styremedlemmer i tillegg til minst én person som er uavhengig av selskapet og med god kompetanse innen revisjon. Utvalget er ansvarlig for overvåking av virksomhetens generelle risikostyrings og kontroll. Overvåkningen skal i tillegg omfatte regnskapsprosessen og en eventuell internrevisjon. Dette er mye av det NUES også anbefaler for styret (Gaudernack 2008).

5.4.1. Hvordan kan selskapene vurdere om deres overvåkningsansvar er i samsvar med aksjelovgivningen, NUES og EU-kravene?

For at de nevnte kravene skal tilfredsstilles er det nødvendig å se nærmere på hva som ligger bak kravene.

1. Selskapet må ha på plass et system for risikoanalyse, implementering av risikotiltak og overvåkning av disse.

2. Systemet, det faktiske risikoforhold og kontrolltiltak må overvåkes av styret og revisjonsutvalget

3. De faktiske risikoforholdene må beskrives i årsrapporten og halvårsrapporten

4. Hovedlinjene i virksomhetens internkontroll og risikostyringssystemer, som er knyttet til finansiell rapportering, må gjøres rede for i årsberetningen.

[8] Foretak av allmenn interesse er i utgangspunktet foretak med verdipapirer notert på regulert marked, banker og andre kredittinstitusjoner og forsikringsselskap (Finansdepartementet 2009).

For å kunne tilfredsstille overvåkningsansvaret, bør det i praksis være klare rutiner og prosesser tilstede, slik at det er mulig å overvåke dem. Skriftlige retningslinjer for risikoanalyse, risikohåndtering og overvåking bør være på plass. I tillegg bør de ulike rollene til styret, revisjonsutvalget og daglig leder beskrives. Styret bør lage instrukser til daglig leder om hvordan systemet skal se ut, hvordan det skal overvåkes og hvordan de vil motta informasjon. Dette gjør det mulig å kunne overvåke, i tillegg til å kunne underbygge innholdet i en redegjørelse (Ferma & ECIIA 2010).

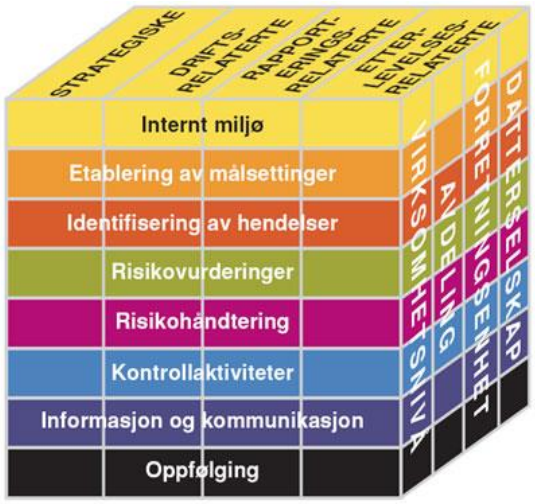
Disse kravene gjelder for selskap av allmenn interesse. Norske AS/ASA har ikke krav på seg til å følge NUES- og EU kravene, og de må dermed heller ikke etablere et revisjonsutvalg, og redegjøre for risiko og kontrollsystemer over finansiell rapportering. Som nevnt tidligere gir NUES en anbefaling som presiserer, men ikke utvider, aksjelovgivningens overvåkningsansvar. Styremedlemmene i norske AS/ASA bør derfor se på NUES og EU-direktivene for å få et bedre bilde av hva styrets ansvar innebærer (Ferma & ECIIA 2010).

5.5. COSO – Et integrert rammeverk for helhetlig risikostyring (2004)

COSO kom i 1992 ut med sitt første rammeverk, *Internkontroll – et integrert rammeverk.* Rammeverket skulle hjelpe virksomheter med å forbedre sine systemer for internkontroll. Ettersom risikostyring har kommet på dagsorden på bakgrunn av en rekke skandaler, så COSO behovet for å utarbeide et slikt rammeverk med fokus på helhetlig risikostyring. I 2004 ble *Helhetlig risikostyring – et integrert rammeverk* gitt ut, i et samarbeid med PricewaterhouseCoopers AS (PwC)[9]. Dette rammeverket er på ingen måte noen erstatning av rammeverket for intern kontroll, men bygger videre og utvider kuben noe (Øvsthus & Kristiansen 2005). Elementene for selve internkontrollen er overvåkning, informasjon og kommunikasjon, kontrollaktiviteter, risikovurdering og kontrollmiljøet.

[9] PricewaterhouseCoopers AS (PwC) er verdens største nettverk av revisorer, advokater og rådgivere, som leverer tjenester innen revisjon, rådgivning, skatt og avgift (PricewaterhouseCoopers 2013).

COSO illustrerer hvordan rammeverket for helhetlig risikostyring henger sammen, ved hjelp av en tredimensjonal kube som vist i figur 4.



Figur 4: COSO-kuben for helhetlig risikostyring

Kuben består av:

- Fire vertikale kolonner som representerer *målkomponentene*
- Åtte horisontale rader med *komponentene* i helhetlig risikostyring
- Virksomheten og dens enheter. Viser at risikostyringen henger sammen i virksomheten som en enhet.

Komponentene er avhengige av hverandre og er avgjørende for om den helhetlige risikostyringen er effektiv. Det vil si at gjennom alle de åtte komponentene i risikostyringsprosessen, må de fire målkomponentene tas hensyn til i tillegg til at hele organisasjonen er inkludert i prosessen. Bakgrunnen for rammeverket er at risikostyringen ikke skal ha en «silobasert» tilnærming, der de ulike forretningsenhetene eller avdelinger på ulike nivåer har separate risikostyringsprosesser. I stedet skal risikostyringen foregå på en felles plattform for hele organisasjonen. Konseptet skal gi bedriftene en forståelse av at de må forstå de risikorelaterte aktivitetene på alle nivå i virksomheten, og hvordan de påvirker hverandre.

5.5.1. Komponentene i helhetlig risikostyring

Den fremste siden av COSO-kuben representerer de åtte komponentene helhetlig risikostyring består av. Komponentene er gjensidig avhengige, og er en integrert del av ledelsesprosesser. Den første komponenten er *internt miljø*. Det interne miljøet er basisen for de andre komponentene, og består av risikostyringsfilosofien i virksomheten, risikoappetitten, integritet og etiske verdier. Hensikten med komponenten er å identifisere de ansattes holdninger til risiko. *Etablering av målsettinger* må til for at virksomheten kan identifisere potensielle hendelser som kan hindre oppnåelsen av disse. Målsettingene må være på linje og samsvar med virksomhetens visjon og risikoappetitt. Den tredje komponenten er *identifisering av hendelser*. Hendelser, interne eller eksterne, som har en påvirkning på implementeringen av helhetlig risikostyringsstrategien eller virksomhetens måloppnåelse, må identifiseres. Når hendelser identifiseres er det viktig å skille mellom muligheter og risikoer. Komponent nummer fire er *risikovurdering*. På dette stadiet vurderer virksomheten sannsynligheten og konsekvensen av potensielle risikorelaterte hendelser, på virksomhetens måloppnåelse. Både den iboende og den gjenværende risikoen blir vurdert. Vurderingen gjøres på grunnlag av å avgjøre hvordan risikoen skal håndteres. Komponent fem i den helhetlige risikoprosessen er *risikohåndtering*. Etter å ha identifisert og vurdert risiko, må det legges en plan for hvordan risikoen skal håndteres. Håndteringen må bringe risikoen i samsvar med virksomhetens risikotoleranse og risikoappetitt. Ulike måter å håndtere risiko på, kan være å unngå, akseptere, redusere eller dele risiko. Prosessens sjette komponent er *kontrollaktiviteter*. Kontrollaktivitetene representerer retningslinjer og prosedyrer som er nødvendig for at risikohåndteringen blir utført på en effektiv måte. Komponent nummer syv er *informasjon og kommunikasjon*. Relevant informasjon blir identifisert og formidlet videre til de ansatte, slik at de kan ivareta sitt ansvar. Prosessen knytter sammen alle de andre komponentene, og foregår både vertikalt og horisontalt i virksomheten. Den åttende og siste komponenten i risikostyringsprosessen er *oppfølging*. Oppfølgingen skal sørge for at den helhetlige risikostyringsprosessen blir gjennomført i henhold til gitte krav. Det er en kontinuerlig prosess, hvor endringer må til ved behov (Øvsthus & Kristiansen 2005).

5.5.2. Målkomponentene

Målsettingene skal hjelpe virksomheten med å fokusere på alle aspekter for måloppnåelse gjennom risikostyringen. Av kuben ovenfor ser vi at virksomhetens måloppnåelse kan forklares ut fra fire målsettinger, der den første er den *strategiske* målkomponenten som er fastsatt på overordnet nivå. Målene er langsiktige og skal være i samsvar med virksomhetens formål. Den *driftsrelaterte* komponenten er rettet mot at virksomhetens ressurser må benyttes på en målrettet og kostnadseffektiv måte. *Rapporteringsrelaterte* målsettinger handler om at virksomhetens rapporteringer må være pålitelig, mens *etterlevelsesrelaterte* målsettinger handler om at virksomheten må overholde lover og regler (Øvsthus & Kristiansen 2005).

5.5.3. Begrensninger ved helhetlig risikostyring

COSO har imidlertid identifisert noen begrensninger ved helhetlig risikostyring. Blant annet kan ikke en helhetlig risikostyring gi sikkerhet for at virksomheten ikke skal mislykkes, noe som kan forklares ut fra flere forhold. Før det første er risiko knyttet til framtiden, og ingen kan forutsi framtiden med sikkerhet. For det andre vil noen hendelser alltid være utenfor ledelsen sin kontroll. Helhetlig risikostyring kan heller ikke gi noe sikkerhet for at målsettingene blir oppnådd. Helhetlig risikostyring kan bare sørge for at ledelsen, og styret som har en overvåkende rolle, blir oppdatert på i hvilken grad virksomheten beveger seg mot måloppnåelse av ulike målsettinger. For det tredje vil ikke alle prosesser alltid gå som planlagt.

5.6. Den Internasjonale Standarden ISO 31000:2009

Den internasjonale standardiseringsorganisasjonen (ISO) er et verdensomspennende forbund som utarbeider og utgir internasjonale standarder, som skal sikre at produkter og tjenester er trygge, pålitelige og av god kvalitet. ISO 31000 ble utarbeidet av arbeidsgruppen for risikostyring i ISOs Technical Management Board i 2009. I 2010 ble den norske versjonen av ISO 31000 fastsatt av Norsk Standard, som er Norges medlem i ISO, og har på norsk fått tittelen *Risikostyring – prinsipper og retningslinjer, NS- ISO 31000:2009* (Standard 2010). Denne standarden beskriver prinsipper, forutsetninger og prosesser for å håndtere risiko på en åpen, systematisk og troverdig måte. Standarden har som formål å hjelpe virksomhetene med å integrere risikostyringsprosessen i dens overordnede forvalting, strategi og planlegging, samt ledelse, rapporteringsprosesser, politikk, kultur og verdier. Standarden er ikke avgrenset

til kun å gjelde en bestemt bransje eller sektor. Den er dermed gjeldende for organisasjoner i både privat og offentlig sektor, foreninger, kommunale foretak, grupper eller personer (Standard 2010).

For at rammeverket skal ha noe nytteverdi, må elementene i rammeverket tilpasses den enkelte organisasjon sine behov. Hvis en organisasjon allerede har etablerte styringspraksiser og prosesser som inkluderer risikostyring eller en form for formell risikostyringsprosess, bør dette sammenlignes og vurderes opp mot denne internasjonale standarden.

Standarden har utarbeidet 11 prinsipper for risikostyring må følges i alle ledd i virksomheten for at risikostyringen skal være effektiv (Standard 2010):

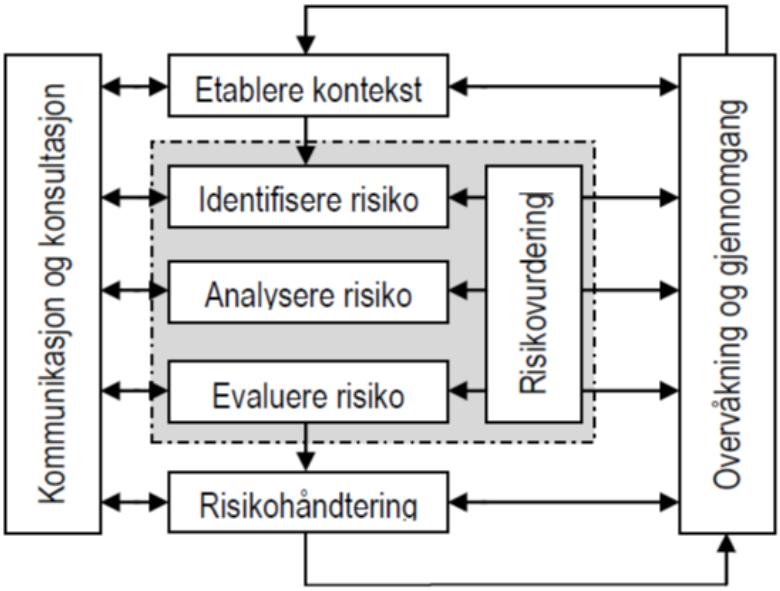
1. *Risikostyring skaper og ivaretar verdier*
2. *Risikostyring er en integrert del av alle organisasjonens prosesser*
3. *Risikostyring inngår i beslutningstaking*
4. *Risikostyring gjelder eksplisitt usikkerhet*
5. *Risikostyring er en systematisk, strukturert og tidsriktig prosess*
6. *Risikostyring bygger på best tilgjengelig informasjon*
7. *Risikostyring er en skreddersydd prosess.*
8. *Risikostyring tar hensyn til menneskelige og kulturelle faktorer.*
9. *Risikostyring er en åpen og inkluderende prosess.*
10. *Risikostyring er en dynamisk og iterativ prosess som er mottakelig for endringer.*
11. *Risikostyring tilrettelegger for kontinuerlig forbedring i organisasjonen.*

ISO 31000:2009 har følgende definisjon av risikostyringsprosessen:

«en systematisk bruk av policyregler, prosedyrer og praksis for styring av aktivitetene kommunikasjon, konsultasjon, bestemmelse av kontekst og identifisering, analysering, evaluering, håndtering, overvåking og gjennomgåelse av risiko».

(Standard 2010)

Figur 5 nedenfor, viser risikostyringsprosessen og komponentene som inngår i denne:



Figur 5: ISO 31000:2009 sin fremstilling av risikostyringsprosessen

I følge standarden bør prosessen være integrert i organisasjonens styring, organisasjonskulturen og praksis. I tillegg bør den være skreddersydd for forretningsprosessene i organisasjonen (Standard 2010).

Kommunikasjon og konsultasjon med interne og eksterne interessenter bør inkluderes i alle de ulike trinnene i prosessen, og det bør derfor utvikles planer for dette tidlig i prosessen. Planene bør inkludere forhold knyttet til risikoen, årsakene til risikoen, eventuelle konsekvenser og tiltak for å håndtere risikoen.

Neste steg i prosessen er *bestemmelse av kontekst*, hvor organisasjonens mål etableres og de eksterne og interne parameterne som skal overveies av styring av risiko blir fastsatt. I tillegg blir omfanget og risikokriteriene for resten av prosessen fastsatt. Risikostyringsprosessens kontekst varierer med organisasjonens behov. Eksempler på kontekst for risikostyring er fastsettelse av mål for risikostyringsaktivtetene, ansvarsområder, omfanget av risikostyringsaktivitetene.

Videre kommer *risikovurderingen*, som inkluderer *risikoidentifisering, risikoanalyse og risikoevaluering*. Formålet med *risikoidentifisering* er å kartlegge risikoer på grunnlag av hendelser som kan påvirke måloppnåelsen, og bør inkludere risikoens årsak og konsekvens. I

en *risikoanalyse* overveies årsakene og kildene til risiko. Samtidig overveies de positive og negativene konsekvensene og sannsynligheten for at konsekvensene inntreffer. Risikoanalysen skal gi innspill til *risikoevalueringen*. I risikoevalueringer skal det tas beslutninger om hvilke risikoer som skal håndteres, og hvor stor prioritet iverksettingen av håndteringen skal få.

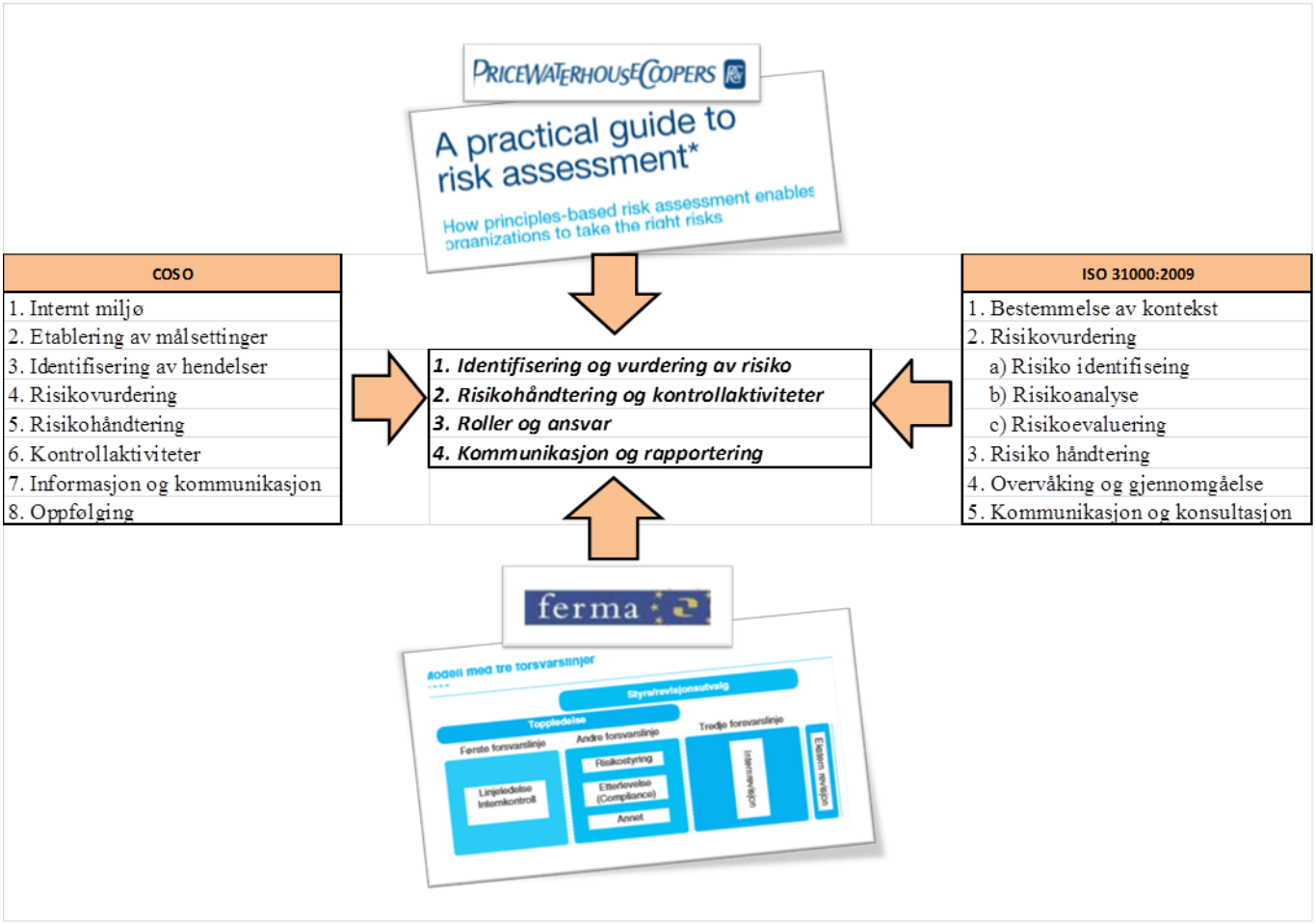
Når risikoen er identifisert, analysert og evaluert, er neste steg å *håndtere risikoen*. «*Risikovurderingen omfatter å velge ett eller flere alternativer for å modifisere risiko og deretter iverksette disse alternativene» (Standard 2010).* Risikohåndteringen er en kontinuerlig prosess, hvor det hele tiden gjøres vurderinger. Risikostyringsprosessens siste steg er *overvåking og gjennomgåelse.* Dette bør være en planlagt del av prosessen og inneholde regelmessig kontroll eller tilsyn. Det kan utføres regelmessig eller ad-hoc. Med overvåking og kontroll kan man løpende tilpasse at kontrollene er effektive og virkningsfulle. Dette utgjør dermed en viktig del av prosessen. I overvåkningen får organisasjonen bredere informasjon av risikovurderingen, lære av hendelser, avdekke endringer i den interne og eksterne konteksten, og identifisere risikoer som oppstår. Resultatene bør loggføres og rapporteres internt og eksternt (Standard 2010).

6. BESTE PRAKSIS FOR HELHETLIG RISIKOSTYRING

Med «beste praksis» mener vi et sett med anbefalte handlinger, samlet fra ulike rammeverk og anbefalinger, som vil bidra til å oppnå suksess med en helhetlig risikostyring.

I takt med utviklingen og kompleksiteten i ulike virksomheter, blir det stadig viktigere med en god struktur for risikostyring samt en kontinuerlig bevisstgjørelse hos sine ansatte. Tidligere var det hovedsakelig kun enkelte bransjer som bank, finans eller IT som jobbet mot en strukturert tilnærming for risikostyring. En strukturert tilnærming og håndtering av risikostyring fremkommer derfor i ulike former i forskjellige virksomheter. Slike ulikheter kan også fremkomme innenfor virksomheten, og det vil kanskje være behov for hjelpemidler som kan hjelpe til med å understøtte disse prosessene (Hallaråker & Vig 2006).

I dette kapittelet vil vi foreta en gjennomgang av rutiner for helhetlig risikostyring, samt hvordan disse kan tilrettelegges og integreres i selskapets virksomhetsstyring. Vi har i denne fremstillingen (se figur 6 nedenfor) tatt utgangpunkt i de rammeverkene og anbefalingene for beste praksis vi har presentert i oppgaven. I presentasjonen av de ulike delene av risikostyringsprosessen vil vi ta for oss teknikker, verktøy og prosesser som skal bidra til få risikostyringen som en integrert del av virksomhetsstyringen.



Figur 6: Risikostyringsprosessen deles i fire deler

Når det gjelder *identifisering og vurdering av risiko*, samt *risikohåndtering og kontrollaktiviteter*, representerer dette rutiner og prosesser som utelukkende fokuserer på risiko. Her foreligger det klart definerte ansvarsfordeling og oppgaver som gjennomføres til faste tider. Disse delene er ofte nye deler som virksomhetene må etablere ved integrering av et helhetlig risikostyringssystem, og må derfor ofte etableres fra grunnen av. *Roller og ansvar* samt *kommunikasjon og rapportering*, representerer virksomhetens evne til å håndtere og integrere resultatene i virksomhetens kjerneprosess. De skal sørge for gjennomføringen av de foreslåtte tiltakene og at systemene fungerer som helhet. Disse to delene inkluderer tilpasninger til allerede etablerte strukturer (Hallaråker & Vig 2006).

6.1. Identifisering og vurdering av risiko

COSO- rammeverket anbefaler å ta risikoidentifiseringen adskilt fra vurderingen av sannsynligheten for og konsekvensen av at hendelsen inntreffer. Dette for å unngå å overse relevante hendelser. I ISO310000:2009 standarden er risikovurderingen en samlet prosess hvor risikoidentifisering inngår.

6.1.1. COSO – rammeverkets anbefalinger

Risikoidentifisering

Identifisering, i følge COSO-rammeverket, innebærer at ledelsen identifiserer potensielle hendelser og ser på hvordan de vil påvirke virksomheten hvis de inntreffer. Hendelser som inntreffer kan ha negativ innvirkning på virksomheten ved at de påvirker mulighetene til å implementere strategi og oppnå målsettinger. Slike hendelser representerer en risiko, og krever at ledelsen håndterer og vurderer hendelsen. En hendelse kan også innebære muligheter. Dette er hendelser med positive konsekvenser, som ledelsen kan kanalisere tilbake til prosessene for fastsettelse av strategi og målsettinger. Hendelsene rangeres fra de som er helt åpenbare til de som er sjeldne, mens konsekvensene rangeres videre fra ubetydelig til kritiske (Øvsthus & Kristiansen 2005).

Ledelsen må vurdere en rekke eksterne og interne faktorer, som utløser mulige trusler eller hendelser, når de identifiserer hendelser. Det er dermed viktig at ledelsen er kjent med disse faktorene, og type hendelser som kan oppstå grunnet disse. Typiske eksterne faktorer kan være økonomiske, miljømessige, politiske, sosiale eller teknologiske. Interne faktorer kan være infrastruktur, medarbeidere, prosess eller teknologi (Moeller 2011).

Teknikker for identifisering av risiko.

Ledelsen kan benytte seg av enten én eller flere teknikker og verktøy for å identifisere hendelser. Teknikkene og verktøyene kan eksempelvis brukes til:

- Identifisere potensielle risikoer eller muligheter ved implementering av en ny forretningsprosess
- Endring i en eksisterende prosess
- Evaluering av en prosess
- Planlegging på strategisk eller enhetsnivå
- Vurdering av nye tiltak eller organisasjonsendringer

Teknikkene kan benyttes periodisk eller kontinuerlig, og angår både fortiden og framtiden.

I det følgende har vi illustrerert hvordan teknikker og verktøy for identifisering av hendelser kan benyttes.

Sjekklister	Ledelsen benytter en detaljert liste over potensielle hendelser som er felles for virksomheter innenfor en bestemt bransje, eller som er felles for en bestemt aktivitet/prosess på tvers av bransjer. En måte å samle den oppsamlede kunnskapen fra andre med erfaring på området.
Workshops med fasilitator og intervjuer	Identifisere hendelser ved å samle opp kunnskap og erfaring hos ledelse, medarbeidere og andre interessenter gjennom strukturerte diskusjoner og intervjuer. Slik blir viktige hendelser, som ellers kunne ha blitt oversett, identifisert.
Prosessanalyse	Forstå sammenhengen mellom innsatsfaktorer, oppgaver, sluttprodukt og ansvar. Når interne og eksterne faktorer som for eksempel påvirker innsatsfaktoren vurderes, så kan virksomheten identifisere hendelser som kan ha innvirkning på oppnåelsen av målsettinger for prosessen.
Ledende hendelsesindikatorer	Ledende hendelsesindikatorer brukes til å overvåke data som har sammenheng med hendelser.
Varsellamper ved endrede verdier	Avvik rapporteres når et forhåndsdefinert kriterium overskrides. Når de overskrides kan det være nødvendig med umiddelbar håndtering. Det må defineres når lederen skal informeres, og dette må samsvare med lederens syn på hvor mye tid som trengs for å iverksette tiltak

Tabell 11: Teknikker for identifisering av risiko (Øvsthus & Kristiansen 2005)

Andre relevante teknikker: Registrering av tapshendelser, fortløpende identifisering av hendelser, innbyrdes sammenhenger mellom hendelser som kan påvirke målsettinger, samt å kategorisere hendelser (Øvsthus & Kristiansen 2005).

Risikovurdering

Ved å vurdere risiko, kan en virksomhet i følge COSO-rammeverket, vurdere i hvilken grad potensielle hendelser kan ha konsekvenser for måloppnåelsen. Ledelsen ser på forventede og uventede hendelser når risikoen skal vurderes. Noen hendelser er uventede, mens andre hendelser er basert på rutinemessige gjentakelser og er allerede håndtert i ledelsesprogrammer eller driftsbudsjettet. Ledelsen vurderer den *iboende* og den *gjenværende risikoen*. Den iboende risikoen er risikoen for en virksomhet *før* ledelsen iverksetter ulike tiltak. Den gjenværende risikoen er den risikoen som er igjen *etter* at ledelsen har iverksatt tiltak for å redusere den iboende risikoen (Øvsthus & Kristiansen 2005).

Risiko vurderes ut i fra sannsynligheten for at en hendelse inntreffer og konsekvensen av den potensielle hendelsen. Virksomheten står ovenfor en utfordring når det skal avgjøres hvor mye oppmerksomhet som bør vies til vurderingen av de ulike risikoene de står ovenfor. Hendelser med lav sannsynlighet for å inntreffe og lav konsekvens hvis den inntreffer, trenger ikke så stor oppmerksomhet. Hendelser med høy sannsynlighet for å inntreffe, og som kan føre til store konsekvenser derimot, må vies betydelig mer oppmerksomhet. Risikoer som befinner seg i mellom disse ytterpunktene er vanskeligere å vurdere (Øvsthus & Kristiansen 2005).

Det må settes en tidshorisont for risikovurderingen, som henger sammen med tidshorisonten for den relaterte strategien eller målsettingene.

Vurderingsteknikker

Når en virksomhet skal vurdere risiko, brukes det en metodikk med kombinasjon av kvalitative og kvantitative teknikker. Kvalitative vurderingsteknikker blir ofte brukt der det er vanskelig å kvantifisere, når det ikke finnes nok data for kvantitativ vurdering eller når det er lite kostnadseffektivt å hente inn eller analysere data. Kvantitative teknikker er ofte mer presise, og brukes på komplekse aktiviteter (Øvsthus & Kristiansen 2005).

Målesystemer

COSO-rammeverket omtaler fire generelle målesystemer når sannsynlighet og konsekvens for potensielle hendelser skal estimeres. Disse er oppsummert i tabellen nedenfor:

Nominelle tall	Hendelsene grupperes i kategorier (f.eks økonomske,teknologiske). Innebærer ingen form for rangering, hvor f.eks. "1" blir vurdert høyere enn "5".
Ordenstall	Hendelsene listes opp i rekkefølge utfra viktighet, og blir ofte rangert i en skala. Nummer "en" 1" dermed viktigere enn "2".
Intervaller	Skala av numeriske like trinn benyttes. Det vil si at hendelse A, B og C kan henholdsvis ha konsekvens 3, 6 eller 9. Ledelsen kan dermed fastslå at forskjellen i potensielle konsekvenser mellom hendelse A og B er den samme som forskjellen mellom B og C. Det betyr ikke at konsekvensen av en hendelse som er målt til "6" er dobbelt så stor som hendelsen som er målt til "3".
Forholdstall	En konsekvens av en hendelse som har fått "6", vil ha dobbel så stor konsekvens som en hendelse som har blitt tildelt en "3".

Tabell 12: Målesystemer for å estimere sannsynlighet og konsekvens for potensielle hendelser (Øvsthus & Kristiansen 2005)

Målesystemene basert på nominelle tall og ordenstall blir ofte sett på som «kvalitative» teknikker, mens målesystemene basert på intervaller og forholdstall blir ofte betraktet som «kvantitative».

Kvalitative teknikker

Kvalitative risikovurderinger kan enten presenteres i en subjektiv eller en objektiv form. Hvilken kvalitet det er på vurderingene, avhenger av kunnskap og skjønn til de personene som utfører vurderingen, samt hvilken forståelse de har av potensielle hendelser.

Kvantitative teknikker

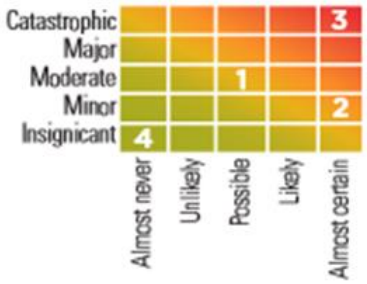
- *Sannsynlighetsmodeller:*
  Det finnes flere teknikker basert på sannsynlighet. Felles for disse er at de måler sannsynligheten og konsekvensen for ulike utfall, basert på forutsetninger om hvilken fordeling hendelsens atferd har. Sannsynlighet og konsekvens blir vurdert på grunnlag av historiske data eller simulerte resultater som hensyn tar forutsetninger om fremtidig atferd. Eksempler på sannsynlighetsmodeller som ofte benyttes er *Value at risk (Var), cashflow at risk, earings at risk og utvikling av tapsfordelinger.*

- *Teknikker som ikke er basert på sannsynlighet*
  Modeller som ikke baserer seg på sannsynlighet, benytter seg av subjektive forventninger når konsekvenser av hendelser skal indentifiseres. Dette gjøres uten å kvantifisere en tilhørende sannsynlighet, noe som betyr at ledelsen må bestemme sannsynligheten selv. Typiske teknikker som ikke er basert på sannsynlighet er *følsomhetsanalyse, scenarioanalyse og stresstesting.*

- *Benchmarking*
  Benchmarking kan gi ledelsen verdifull informasjon om sannsynligheten for eller konsekvensene av en risiko, basert på erfaring fra andre virksomheter. Med benchmarking er det et samarbeid mellom en gruppe bedrifter hvor det fokuseres på enkelte prosesser eller hendelser, og måltall og resultater blir sammenlignet, ved å bruke felles målenheter og identifiserer forbedringsprosesser.

  Når risikoen er vurdert er det viktig at den blir framstilt på en klar og konsis måte. Dette er spesielt viktig ved kvalitative vurderinger, da risikoer i slike tilfeller ikke blir summert til noe form for tall, slik som ved kvantitative vurderingsteknikker. Det

finnes ulike praksiser på hvordan risikovurderinger kan framstilles. Eksempel på dette kan være risikokart eller numerisk representasjon. I et *risikokart* blir sannsynlighet og konsekvens for ulike risikoer grafisk framstilt. I risikokartet blir risikoene beskrevet slik at det kommer frem hvilke risikoer som er mer betydningsfulle, ved at de har høyere sannsynlighet og/eller konsekvens, og hvilke som er mindre betydningsfulle (Øvsthus & Kristiansen 2005). Risikokartet kan i tillegg utformes som et «varmekart» ved hjelp av fargekoder, hvor rød tilsvarer høy risiko mens grønn lav risiko. Et eksempel på dette er illustrert i figuren nedenfor:



Figur 7: Varmekart (Martens 2012)

6.1.2. ISO 31000:2009 – anbefalinger

Risikoidentifisering og risikovurdering

I følge ISO 31000:2009 er risikovurdering *«en samlet prosess som omfatter risikoidentifisering, risikoanalyse og risikoevaluering» (Standard 2010).* Videre defineres risikoidentifisering som *«en prosess for å finne, gjenkjenne og beskrive risikoer»* (Standard 2010). Prosessen består av å identifisere risikokilder, hendelser og årsaker samt deres potensielle konsekvenser. I tillegg til dette bør årsakene og de potensielle konsekvensene identifiseres. På denne måten får virksomheten en liste med oversikt over risikoer basert på hendelser som kan på noe som helst måte påvirke måloppnåelsen. Det er fare for at risiko som ikke blir identifisert på dette stadiet, ikke vil bli tatt med i videre analyser.

Identifisering av risiko bør:

- Inkludere risikoer uavhengig av hvem som har kontroll over kilden til risikoen.
- Inkludere risikoer uavhengig av om årsaken eller kilden er åpenbar
- Undersøke hvordan risikoene påvirker hverandre og hendelsene som oppstår.

- Bør ta hensyn til et bredt område av konsekvenser, selv om det ikke er klart hva som er kilden eller årsak til risikoen.
- Vurdere potensielle årsaker og scenarier som gir et bilde på hvilke konsekvenser man kan vente seg.

Av rammeverket fremkommer det at det bør benyttes verktøy og metoder som er i tråd med virksomhetens mål og kompetanse, samt for de risikoene virksomheten er eksponert for.

ISO/IEC 31010:2009[10] er en internasjonal standard som utfyller ISO:31000:2009 og gir veiledning om hvordan virksomheten kan benytte seg av systematiske metoder for risikovurdering (Standard 2012).

ISO/IEC 31010:2009 anbefaler følgende metoder for identifisering av risiko:

- Bevisbaserte metoder, slik som sjekklister og behandling av historiske data.
- Systematisk gjennomgang av prosesser for å identifisere risiko ved hjelp av en strukturert tilnærming, gjennomført av en gruppe eksperter.
- Induktive resonneringsmetoder, slik som HAZOP.

I tillegg anbefales det å benytte støttemetoder for å styrke nøyaktigheten og fullstendigheten i identifiseringen. Eksempler på slike metoder er Delphi-metoder hvor det gjentatte ganger blir utført deltakerundersøkelser, eller idédugnader (Standard 2012).

Uansett metode for risikoidentifisering, er det viktig at virksomhetene tar hensyn til menneskelige og organisasjonsmessige faktorer. Identifiseringen bør derfor inkludere avvik fra det som forventes, i form av menneskelige og organisasjonsmessige forhold i tillegg til eksempelvis «programvare»-hendelser (Standard 2012).

[10] IEC er en internasjonal elektroteknisk kommisjon og en verdensomspennende virksomhet for standardisering (Standard 2012).

Dette har ISO/IEC 31010:2009 illustrert i en tabell som viser potensielle metoder for risikovurdering og beskriver hvilken form for vurdering de gir.

Type metode for risikovurdering	Beskrivelse	Påvirkningsfaktorers relevans			Kan gi kvantitative resultater
		Ressurser og kompentanse	Typen og graden av usikkerhet	Kompleksitet	
OPPSLAGSMETODER					
Sjekklister	En enkel form for risikoidentifisering. En metode som viser en rekke typiske usikkerheter som det må tas hensyn til. Brukere henvises til en tidligere utvikket liste, forskrifter eller standarder	Lav	Lav	Lav	Nei
Innledende fareanalyse	En enkel, induktiv analysemetode som har som mål å identifisere farene og de farlige situasjonene og hendelsene som kan forårsake skade for en gitt aktivitet, et gitt anlegg eller et gitt system	Lav	Høy	Middels	Nei
STØTTEMETODER					
Strukturerte intervju og idédugnad	En måte å samle et bredt utvalg av ideer og evaluering på og la en gruppe rangere dem. Idédugnad kan stimuleres ved ledetekst eller ved én-til-én- og én-til-mange-intervjumetoder	Lav	Lav	Lav	Nei
Delphi-metode	En måte å kombinere ekspertoppfatninger på som kan støtte kilden og påvirke identifisering, sannsynlighet og konsekvensberegning og risikoevaluering. Det er en samarbeidsmetode for å skape konsensus blant eksperter. Innebærer uavhengig analyse og avstemming fra eksperter.	Middels	Middels	Middels	Nei
Vurdering av menneskelig pålitelighet (HRA)	Vurdering av menneskelig pålitelighet (HRA) omhandler den menneskelige påvirkningen på systemytelsen og kan brukes til å evaluere hvordan menneskelige feil påvirker systemet.	Middels	Middels	Middels	Ja

Tabell 13: Potensielle metoder for risikovurdering (Standard 2012)

Det anbefales at metodene for risikovurdering bør inneha følgende egenskaper (Standard 2012):

- Riktig og hensiktsmessige i forhold til tilfellet eller virksomheten det gjelder
- Resultatene fra vurderingen må gjøre det enklere å forstå typen risiko og tiltak som kan iverksettes
- Vurderingene må være sporbare og mulige og etterprøve.

6.1.3. «A practical guide to risk assessment» PricewaterhouseCoopers (PwC) – notat

PwC har utarbeidet et notat om hvordan prinsippbasert risikovurdering skal bidra til at virksomhetene tar de riktige risikoene. Risikovurdering defineres som *«en systematisk prosess for å identifisere og evaluere hendelser (slik som mulige risikoer og muligheter) som kan påvirke måloppnåelsen, positivt eller negativt»*. Ved riktig bruk av risikovurderingen skal virksomheten få klare signaler på hvilke variabler den er eksponert for, om det måtte være internt eller eksternt, sett tilbake eller frem i tid. For at risikovurderingen skal gi slike resultater, må en rekke nøkkelprinsipper tas til betraktning. Prosessen skal starte og ende med konkrete forretningsmessige mål om er forankret i virksomhetens viktige verdidrivere. Disse målene skal være grunnlaget for å måle effekten og sannsynligheten for rangeringen av risiko (PricewaterhouseCoopers 2008).

I notatet har det blitt utarbeidet en rekke nøkkelprinsipper som må tas hensyn til hvis risikovurderingen skal gi verdifulle resultater:

1. *Styringen av risikovurderingsprosessen må være klart etablert*
   Det er viktig med tilsyn og ansvarliggjøring av risikovurderingsprosessen for å sikre nødvendig engasjement og ressurser, og for at risikovurderingene skjer på riktig nivå i virksomheten.
2. *Risikovurderingen begynner og ender med konkrete målsettinger*
   Risiko blir identifisert og målt i forhold til virksomhetens mål. Det er derfor viktig å definere mål som er konkrete og målbare på de ulike nivåene i virksomheten.
3. *Risikovurderingsskalaer er definert i forhold til virksomhetens mål i omfang*
   Risiko blir som regel målt i forhold til konsekvens og sannsynlighet for at den inntreffer. Konsekvens skalaene bør gjenspeile måleenhetene som brukes for de

organisatoriske målene, som igjen vil gjenspeile ulike typer konsekvenser (f.eks. økonomisk, mennesker eller omdømme).

4. *Ledelsen danner et porteføljesyn på risiko for å kunne støtte beslutningstakingen*
   Det er viktig å samle risikoene for å få et porteføljesyn som viser hvordan risikoene påvirker hverandre på tvers av virksomheten
5. *Bruke ledende indikatorer for å gi innsikt i potensielle risikoer*
   Key Performance Indicators (KPI'er)[11] og Key Risk Indicators (KRI'er)[12], tidligere omtalt som styringsparametere, brukes ofte til å identifisere faktorer som påvirker måloppnåelsen og signaliserer økt risiko for fremtidige tap. Disse indikatorene kan registreres periodisk, rapporteres på en jevnlig basis eller når ledelsen forespør og gir innblikk i virksomhetens risikoposisjon. Når ledelsen skal identifisere utvikling av selskapets resultat, arbeidsprosesser eller utviklingen av forhåndsbestemte nøkkelrisikoer, er bruk av disse verktøyene svært nyttige (PricewaterhouseCoopers 2008).

Forskjellen på KPI'er og KRI'er, er at en KPI er et mål på hvor godt arbeidet er utført, mens en KRI måler fremtidig negativ påvirkning for selskapet. Dersom indikatorene er hensiktsmessig utformet, har de en stor verdi og kan fungere som varslingssignal på mulige endringer i bedriftens risikoprofil (Fraser & Simkins 2010). KPI'er kan være både finansielle og ikke-finansielle størrelser, og kan ytterlig deles inn i to typer; ytelsesindikatorer og resultatindikatorer. En ytelsesindikator måler selskapets utvikling innenfor en bestemt arbeidsprosess eller adferd. Dette kan for eksempel være antall kundebesøk, utviklingen for læring og vekst for de ansatte. En resultatindikator vil derimot måle effekten av selskapets prestasjoner, ofte er disse finansielle, som for eksempel bruttofortjeneste og markedsandel. Andre målbare størrelser kan være kvalitet, produktivitet, kundetilfredshet, antall reklamasjoner, maskinstopp grunnet maskinfeil, indeks for medarbeidertilfredshet samt ansatt turnover.

Det stilles også stadig større krav til at organisasjoner til en hver tid må være forberedt på at uventede typer risikoer fra uventede kilder kan forekomme. En voksende trend innenfor helhetlig risikostyring, er nettopp bruk av KRI'er.

[11] KPI (Key Performance Indikators) er på norsk styringsparametere. Dette er målbare størrelser som benyttes i virksomhetens styring mot forutbestemte mål (Hoff & Holving 2002).
[12] KRI (Key Risk Indicators) er indikatorer for nøkkelrisikoer er indikatorer som fokuserer særskilt på måling av potensielle trusler, nivå, eller trenden av en bestemt risiko (Wikipedia 2013a).

6.2. Risikohåndtering og kontrollaktiviteter

6.2.1. COSO-rammeverkets anbefalinger

Risikohåndtering

Når ledelsen har vurdert alle relevante risikoer, er neste steg å avgjøre hvordan de skal håndteres. Risikoer kan ikke helt eliminere, men hensikten med helhetlig risikostyring er å finne måter å håndtere risikoen på, slik at risikoen eller konsekvensen av denne reduseres (Hallaråker & Vig 2006). Risikohåndteringen kan deles inn i følgende fire kategorier:

- *Å unngå*

  Ved å unngå risiko, trer man bort i fra de aktivitetene som er en kilde til risiko. Dette kan føre til at muligheter og inntekter går tapt. Det er aktuelt å unngå risiko når risikoene er omfattende, komplekse og uoverskuelige. Dette kan gjøres ved eksempelvis å utsette aktiviteten eller stanse en produksjon.
- *Å redusere*

  Hvis risikoen skal reduseres, blir tiltak iverksatt for å redusere sannsynligheten for og/eller konsekvensen av risikoen. Tabell 14 nedenfor har oppsummert eksempler på tiltak som reduserer sannsynligheten for at en risiko skal inntreffe og konsekvensen av en hendelse.

Reduksjon av :	
Sannsynligheten	**Konsekvensen**
- Iverksette kvalifikasjonsprogrammer	- Lage kriseplaner og kontinuitetsplaner
- Iverksette kontrolltiltak	- Innstallere brannslukkingsanlegg
- Foreta prøver, analyser og produksjonskontroll	- Iverksette interne kontroller og revisjon
- Foreta preventivt vedlikehold	- Foreta helseundersøkelser og opplæring i førstehjelp
- Innføre sikkerhetssystemer og prosedyrer	- Sørge for "backup" rutiner og dublert lagring av informasjon
- Gjennomføre opplæring og utdanning	

Tabell 14: Tiltak for å redusere risiko (Hallaråker & Vig 2006)

- *Dele*

  For å dele risikoen, må virksomheten redusere risikoens sannsynlighet eller konsekvens ved å overføre, eller dele risikoen med andre.
- *Akseptere*

  Risikoen kan aksepteres ved at man ikke setter i gang noen tiltak for å redusere sannsynligheten eller konsekvensen. Herunder har vi risikoer som i utgangspunktet er

så små at tiltak mot dem ikke er hensiktsmessig. Når risikoen er akseptert, erkjennes sannsynligheten for at de vil inntreffe. Oppgaven blir derfor å begrense konsekvensen av den uønskede hendelsen. Dette kan gjøres ved å utarbeide en krise eller katastrofeplan. I tillegg til dette må virksomhetene handle når hendelsen inntreffer, og utbedre skaden fortest mulig etter hendelsen.

Når en risiko blir unngått, vil det ofte si at det ikke er identifisert noen alternative løsninger som reduserer sannsynligheten eller konsekvensen til et akseptabelt nivå. Når en risiko reduseres eller deles, blir risikoen håndtert på en måte som reduserer den gjenværende risiko til et nivå som er innenfor virksomhetens risikotoleranser. Når en risiko derimot aksepteres, vil det ofte si at den iboende risikoen allerede er innenfor virksomhetens risikotoleranse.

Når ledelsen skal vurdere hvilken av disse metodene som skal benyttes, vil dette avhenge av hvilken effekt den har på risikoens sannsynlighet og konsekvens, samt kostnad og nytte. Ofte står det mellom ulike alternativer for tiltak. Når ledelsen analyserer de ulike alternativene, kan også ulike trender, hendelser og framtidsscenarioer tas med i vurderingen. Videre er det viktig at det hele tiden følges med på utviklingen av de valgte tiltakene. Tiltak som ikke er blitt iverksatt, har heller ingen som helst verdi, mens et tiltak som er fullt iverksatt vil antyde til at virksomheten begynner å få kontroll på risikoen (Øvsthus & Kristiansen 2005).

Kontrollaktiviteter

Kontrollaktiviteter er de rutiner og retningslinjer som skal hjelpe til med gjennomføringen av ledelsens valgte former for risikohåndtering. Kontrollaktivitetene kan deles inn på grunnlag av hvilke av virksomhetens målsettinger de berører, og kan følgelig deles inn i: strategiske, driftsrelaterte, rapporteringsrelaterte og etterlevelsesrelaterte (Øvsthus & Kristiansen 2005).

Kontrollaktivitetene blir etablert for å sørge for at risikohåndteringene blir gjennomført på en ordentlig måte og samsvarer med gitte målsettinger. Samtidig representerer også kontrollaktivitetene selve risikohåndteringen. Det er dermed viktig at det er sammenheng mellom målsettinger, risikohåndtering og kontrollaktiviteter. Valg og evaluering av kontrollaktiviteter bør vurderes opp mot relevans i forhold til denne sammenhengen (Moeller 2011).

Kontrollaktiviteter kan være preventive, oppdagende, manuelle, maskinelle eller ledelseskontroller. Nedenfor skal vi se nærmere på eksempler på kontrollaktiviteter som benyttes.

- *Gjennomgang på toppnivå:*
  Toppledelsen går gjennom resultatene av den virkelige driften, og sammenligner dette med budsjetter, prognoser, tidligere resultater og konkurrentenes resultater. Deretter blir ulike tiltak, som for eksempel markedsframstøt, vurdert for å se om man klarer å nå målsettingen.
- *Ledelse på funksjons- eller aktivitetsnivå:*
  De lederne som har ansvar for enkeltfunksjoner eller aktiviteter går gjennom løpende resultater. Med dette kan trender identifiseres.
- *Informasjonsbehandling*
  Kontrollaktiviteter blir gjennomført for å sjekke nøyaktighet, fullstendighet og godkjenning av transaksjoner. Den informasjonen som kommer ut av dette blir direkte koblet for redigeringskontroll.
- *Fysiske kontroller*
  Utstyr, lagerbeholdningen, verdipapirer og kontakter blir fysisk sjekket og telles regelmessig. Samtidig passes det på at de samsvarer med de beløp/antall som er registrert i kontrollfilene.
- *Resultatindikatorer:*
  Ledelsen kan undersøke uventede resultater eller uvanlige trender for å finne forhold som tilsier at manglede evne til å fullføre en nøkkelprosess kan føre til at sannsynligheten for måloppnåelse blir redusert.
- *Arbeidsdeling*
  Arbeidsoppgaver blir fordelt mellom ulike medarbeidere slik at risikoen for feil reduseres.

6.2.2. ISO 31000:2009 – anbefalinger

Risikohåndtering

I ISO31000 standarden omfatter risikohåndtering *«å velge ett eller flere alternativer for å modifisere risiko og deretter iverksette disse alternativene»*. Risikohåndteringen beskrives som en syklisk prosess som begynner med vurdering av en risikohåndtering og deretter

bestemmes det om nivået på den resterende risikoen kan tolereres. Hvis ikke nivået kan tolereres, må det utvikles en ny risikohåndtering. Videre blir effekten ved denne nye håndteringen vurdert (Standard 2010).

Et alternativ for risikohåndtering er å unngå risikoen. Med dette avsluttes aktiviteten som det er identifisert risiko med. Andre mulige alternativer er at risikokilden kan fjernes, sannsynligheten eller konsekvensene kan endres, dele risikoen med én eller flere parter. Videre kan risikoen økes eller tas for å utnytte en mulighet, eller ta risikoen for egen regning som et resultat av en veloverveid beslutning. Disse ulike alternativene kan enten brukes enkeltvis eller i en kombinasjon.

Da det skal tas beslutningen om de best passende alternativene for risikohåndtering, må kostnadene forbundet med iverksettingen vurderes opp mot fordelene ved risikohåndteringen. Dette med hensyn til blant annet juridiske og forskriftsmessige krav. Ved valg av alternativer for risikohåndtering må det også tas hensyn til interessentenes verdier og oppfatning. Interessentene bør i tillegg involveres i beslutningen, hvis risikoen påvirker dem.

Standarden anbefaler utvikling og iverksetting av risikohåndteringsplaner. Med dette verktøyet skal de valgte håndteringsalternativene og implementeringen av disse dokumenteres. Planene bør integreres i virksomhetens styringsprosesser (Standard 2010).

6.3. Kommunikasjon og rapportering

6.3.1. COSO – rammeverkets anbefalinger

Kommunikasjon

For at risikoen skal kunne identifiseres, vurderes og håndteres, og for i det hele tatt å styre virksomheten, er det viktig med informasjon og kommunikasjon på alle nivåer i virksomheten. Informasjon kan komme fra både interne og eksterne kilder, være økonomiske og ikke-økonomiske og komme i kvalitativ og kvantitativ form. Felles er at det blir lettere å håndtere endrede betingelse (Øvsthus & Kristiansen 2005).

Informasjon kan komme i store datamengder, og behandlingen av informasjonen kan være en utfordring for ledelsen. Dette kan løses ved å bygge opp en infrastruktur av informasjonssystemer. På denne måten kan virksomheten fange opp, behandle, analysere og

rapportere relevant informasjon. Informasjonssystemer kan både være formelle og uformelle. Kommunikasjon med kunder, leverandører, myndigheter, sammen med deltakelse på faglige seminarer og medlemskap i foreninger, kan gi verdifull informasjon for identifisering av risiko og muligheter.

Virksomheten kan benytte seg av både historiske og nyere data for å støtte en effektiv helhetlig risikostyring. Med historiske data er det mulig for virksomheten å måle de faktiske resultatene som er oppnådd opp mot mål, planer og forventninger. Samtidig kan virksomhetene få innsikt i oppnådde resultater under varierende forhold. Dette gjør at ledelsen kan se sammenhenger og identifisere trender, som kan gjøre det mulig å si noe om framtidige hendelser og resultater. Nyere data gjør at virksomheten kan holde seg oppdatert på om de holder seg innenfor sin etablerte risikotoleranse, slik at ledelsen kan identifisere avvik fra forventningene (Øvsthus & Kristiansen 2005).

Informasjonen bør kommuniseres i en for og i et perspektiv som muliggjør at de ansatte kan ivareta sitt ansvar, og bør skje både vertikalt og horisontalt i virksomheten (Øvsthus & Kristiansen 2005).

Rapportering

Rapportering av sentrale risikoer har som formål å forbedre og gi støtte til beslutninger som tas, og rapporteres både ekstern og internt. Ekstern rapportering er rapporter som ofte benyttes av investorer, banker og finansinstitusjoner og offentlige myndigheter, mens intern rapportering benyttes mellom de ulike nivåene i en virksomhet. Hensikten med intern rapportering er at ledelsen på ulike nivåer har relevant informasjon tilgjengelig for å fatte beslutninger. Det finnes ingen lovpålagte krav om hvordan de interne rapportene skal utformes. Hallaråker og Vig anbefaler likevel at antall standardiserte rapporter som utarbeides bør være begrenset. Dette gjør at det blir en felles forståelse for rapportene innad i virksomheten. Det understrekes også at virksomhetene må utforme sine rapportformer i henhold til sin kultur og tekniske forutsetninger (Hallaråker & Vig 2006).

Før evalueringen av hver organisasjonsenhet som helhet kan utføres, må det foreligge en aggregering på det respektive organisatoriske nivå. For hver organisasjonsenhet bør det være en risikoansvarlig som har ansvaret for å hente inn data fra ulike risikorapportører og aggregere dette på ønsket nivå. Når aggregeringen skal opp på et overordnet nivå, anbefaler

Halaråker og Vig at risikoansvarlig (CRO) bør være ansvarlig for å samle virksomhetens risikoanalyser i en overordnet evaluering (Hallaråker & Vig 2006).

6.4. Roller og ansvar

Administrerende direktør i en virksomhet har det endelige ansvaret for gjennomføringen av den helhetlige risikostyringen, men for at risikostyringen skal nå ut i hele virksomheten må alle de ansatte ta et ansvar. Mellomledere og andre ledere må sørge for at virksomhetens filosofi for risikostyring blir overholdt og være i stand til å håndtere risikoer innenfor sine ansvarsområder i henhold til risikotoleranse og risikoappetitt. Ansvaret til de øvrige ansatte handler om å utføre helhetlig risiko i overensstemmelse med etablerte retningslinjer og rutiner. Styret har et overvåkningsansvar, hvor de skal «påse» at virksomheten operer i henhold til risikoappetitten (Øvsthus & Kristiansen 2005).

For at risikostyringen skal fungere optimalt, er det avgjørende med en hensiktsmessig fordeling og koordinering av arbeidsoppgavene i en virksomhet. Alle deler av virksomheten bør ha ansvar for håndtering av risiko innenfor sitt arbeidsområde (Ferma & ECIIA 2010). Uten dette vil i verste fall ikke vesentlige risikoer bli avdekket og kommunisert i tide.

FERMA/ECIIA[13] har gitt ut en anbefaling hvor de blant annet gir en oversikt over roller og ansvar som skal sikre hensiktsmessig risikostyring (Ferma & ECIIA 2010).

- *Styret*

  Styret skal føre tilsyn med og veilede ledelsen ved fastsettelse av virksomhetens risikoappetitt, og holde seg informert om de mest vesentlige risikoene virksomheten er eksponert for samt om toppledelsen håndterer dette på riktig måte (i forhold til den fastsatte risikoappetitten).
- *Administrerende direktør og ledelsen*

  Administrerende direktør og ledelsen har ansvaret for og eierskapet til virksomhetens risikostyring. Innehaver av rollen skal sørge for å sette «tonen på toppen» ved å passe på at både det interne miljøet og risikokulturen i virksomheten er positiv.
  Linjeledelsen skal ledes, samtidig som det skal sørges for at virksomhetens samlede

[13] Federation of European Risk Management Association (FERMA) er en sammenslutning av 20 nasjonale risikostyringsforeninger i 18 land (Ferma & ECIIA 2010).
European Confederation of Institutes of Internal Auditing (ECIIA) representerer 33 nasjonale internrevisjonsinstitutter (Institutes of Internal Auditors) i Europa (Ferma & ECIIA 2010).

risikoaktiviteter er i samsvar med virksomhetens samlede risikoappetitt. Administrerende direktør skal videre iverksette tiltak slik at risikoen er i samsvar med den fastsatte risikoappetitten, dersom det er forhold som fører til et gap mellom dagens situasjon og risikoappetitten.

- *Linjeledelsen*
  Linjelederne har ansvaret for bestemte prosesser, funksjoner eller avdelinger, og får delegert ansvar fra toppledelsen. Disse lederne står dermed får den praktiske utførelsen av de daglige risikostyringsprosessene. De identifiserer, vurderer og bestemmer tiltak for hvordan risiko skal følges opp.

FERMA/ECIIA anbefaler opprettelse av en sentral risikostyringsfunksjon som koordinerer risikostyring i virksomheten. De mener utnevnelse av en egen risiko ansvarlig (Chief Risk Officer (CRO)) er beste praksis. For mindre virksomheter er dette kanskje ikke hensiktsmessig, og det anbefales her å gi dette ansvaret til en annen topplеder. Denne personen er ansvarlig for å følge opp utviklingen av risikostyringen, samt å hjelpe linjeledere med rapportering av informasjon vedrørende risiko gjennom virksomheten. Vedkommende skal rapportere til styret gjennom administrerende direktør (Ferma & ECIIA 2010). En risikoansvarlig, eller en med lignende rolle, skal:

- Skape et helhetlig system for risikostyring ved å fastsette retningslinjer, definere ansvarsområder og roller samt utarbeide mål for gjennomføringen.
- Fastsette et rammeverk for risikostyringen for avdelinger eller bestemte prosesser i virksomheten.
- Forbedre risikostyringskompetanse i hele virksomheten.
- Skape et felles språk for risikostyringen
- Hjelpe ledelsen med å utvikle risikorapportering, samt og følge opp risikorapporteringsprosessen.
- Rapportere om utvikling og anbefale administrerende direktør og styret nødvendige tiltak.

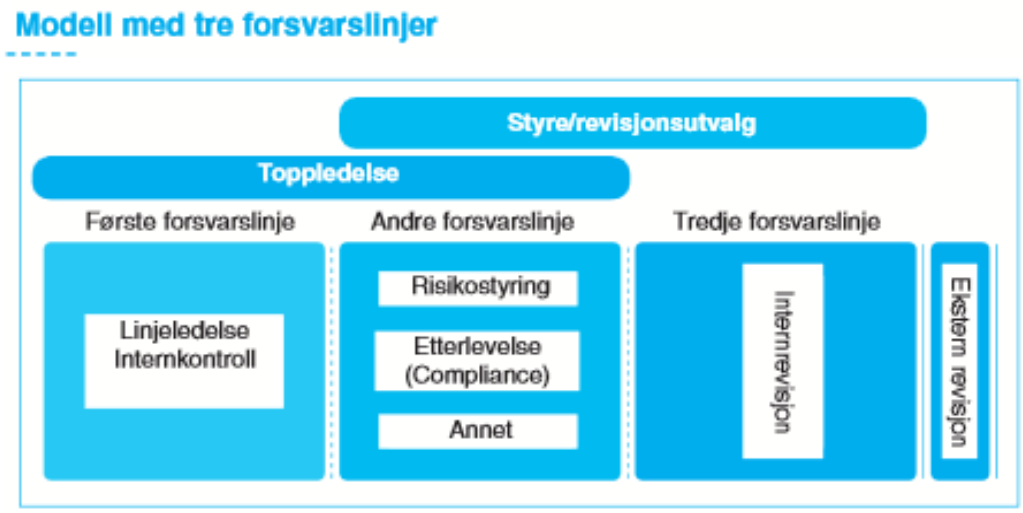
FERMA/ECIIA mener også at etablering og opprettelse av en profesjonell uavhengig internrevisjonsfunksjon er beste praksis. Funksjonen er ansvarlig for å gi en objektiv bekreftelse til styret og ledelsen på at risikoene er forstått og håndtering på en tilstrekkelig måte. De skal i tillegg fremlegge løsninger som kan forbedre organisasjonens virksomhetsstyring, risikostyring og kontrollstruktur. På denne måten fungerer de dermed

som en internrådgivningsfunksjon. Internrevisor tilfører virksomheten merverdi ved at den utfører sine oppgaver på en systematisk og strukturert metode (Gaudernack 2008). Dette anbefales som beste praksis for ikke bare store og mellomstore, men også får mindre virksomheter da de ofte ikke har mulighet til å etablere en organisasjonsstruktur som skal fange tilstrekkelig med prosesser for virksomhets- og risikostyring.

Revisjonsutvalg består av representanter fra styret og fungerer som et saksforberedende organ for styret. Utvalget har risikostyring på agendaen, som skal gi styret tilbakemelding om deres vurderinger vedrørende risikostyringen i virksomheten. Informasjon for å gjøre vurderingene innhenter de selv eller ved hjelp av revisjonsfunksjonene. Det anbefales at utvalget skal gjennomgå alle virksomhetens forsvarslinjer, i tillegg til samhandlingen mellom dem.

6.4.1. «The three Lines of Defence Model»

For at styret og administrerende direktør skal kunne holde tilsyn med og følge strategiene og prosessene for risikostyring på en tilfredsstillende måte, er det behov for bekreftelser fra ulike deler av virksomheten. «The Three Lines of Defence Model» illustrerer samhandlingen mellom de ulike aktørene innen virksomhetsstyring og risikostyring og bidrar til god corporate governance, Modellen er illustrert under:



Tabell 15: The three lines of Defence model (Ferma & ECIIA 2010)

- *Første forsvarslinje – Linjeledelsen*
  Linjeledelsen «eier» risikoen, og er ansvarlig for selve utførelsen av risikovurdering, risikostyringen og tiltak for å redusere risikoer. De har også ansvaret for at internkontroller holdes ved like og at de er hensiktsmessige.
- *Andre forsvarslinje - Risikostyringsfunksjon og Etterlevelse (Compliance[14])*
  Risikostyringsfunksjonen tilrettelegger og har tilsyn med gjennomføringen av risikosyringsprosessene hos linjeledelsen. De sørger også for at risikorelatert informasjon blir rapportert i hele virksomheten. Noen virksomheter har i tillegg valgt å opprette en egen uavhengig etterlevelsesfunksjon, som skal følge opp at virksomheten ikke pådrar seg offentlige sanksjoner, økonomiske tap eller tap av omdømme, som et resultat av brudd på lover, forskrifter eller retningslinjer. Funksjonen skal rapportere til administrerende direktør, og fungerer dermed som et viktig verktøy for toppledelsen.
- *Tredje forsvarslinje – Internrevisjonsfunksjonen*
  Internrevisjonsfunksjonen skal gi styre og ledelse bekreftelse at virksomheten har hensiktsmessige systemer for risikostyring, og med dette føre tilsyn over første- og andreforsvarslinje.
- *«Fjerde forsvarslinje» - Ekstern revisjon*
  Ekstern revisjon betraktes ofte som den fjerde forsvarslinjen, og skal gi virksomhetens aksjonærer, styret samt ledelsen bekreftelse på at årsregnskapet gir et riktig bilde av virksomhetens drift. Informasjon vedrørende risiko samlet inn av eksternrevisor er imidlertid begrenset til risiko knyttet til finansiell rapportering.

FERMA/ECIIA mener de tre forsvarslinjene er pålitelige informasjonskilder som styret kan benytte for å påse og følge opp at risikostyringsprosessene fungerer hensiktsmessige (Ferma & ECIIA 2010). Gjennom forsvarslinjene, vil viktige roller og oppgaver avklares og dermed bidrar til en enkel og effektiv måte å forbedre kommunikasjonen i risikostyringsprosessene på (The inistitue of internal auditors 2013).

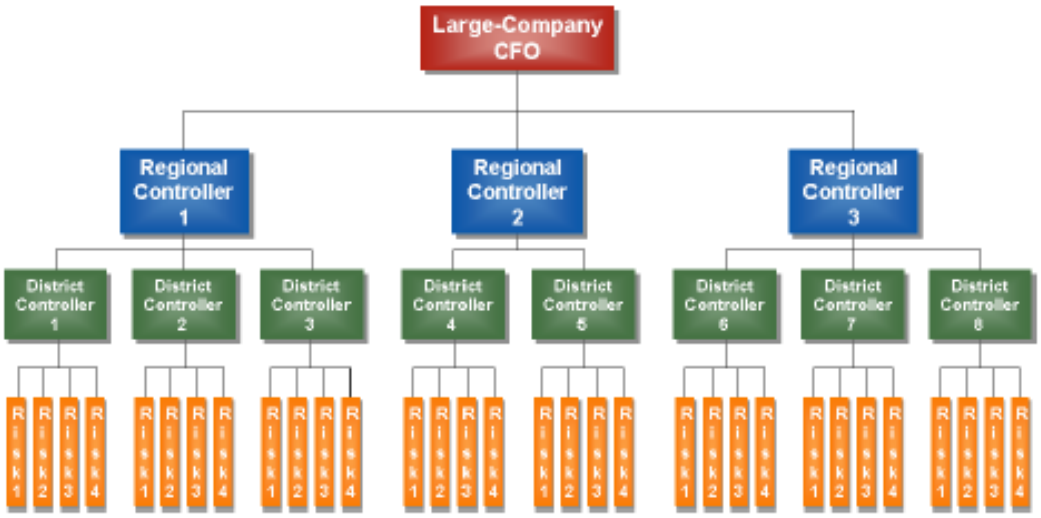
6.5. Virksomheters tilpasning til helhetlig risikostyring

Ingen bedrifter innfører et helhetlig risikostyringssystem på samme måte. De fleste tar opp elementene i et helhetlig risikostyringssystem gradvis og over tid. Enkelte bedrifter starter

[14] Med *compliance* menes en avdeling i selskapet som jobber særskilt med at virksomheten overholder lover og regler (Ferma & ECIIA 2010).

med og lagvis å legge til flere risikokilder, en om gangen, inn i sine nåværende prosesser for risikovurdering. Andre bedrifter setter seg inn i alle risikokilder men en gang i alle aktuelle prosesser, men som en håndterlig liten undergruppe i prosessene som et eget pilotprosjekt. De fleste søker å finne tidlige gevinster for en fremdrift og derav reklamere for en videre utvikling og implementering av helhetlig risikostyrings prosessesene. Videre tror forskerne at helhetlig risikostyring vil bli en høyst integrert del av virksomheters virksomhetsstyring i det 21 århundre. Det vil påvirke hvordan organisasjoner styres og hvordan de er strukturert. Det vil ha stor påvirkning på hvordan internrevisjon utføres, samt legger opp til en god dialog mellom risikoansvarlig og administrerende direktør i selskapet.

Flere faktorer påvirker omfanget av virksomhetenes system for overvåking. COSO har gitt ut et rammeverk for overvåking hvor spesielt to faktorer er omtalt; virksomhetens *størrelse* og *kompleksitet*. I større virksomheter har verken toppledelsen eller styret umiddelbar nærhet til driften. Det betyr at avstanden til risiko blir større, som illustrert i figur 8, noe som fører til at virksomheten er avhengig av overvåkingsprosedyrer utført av andre ansatte. I mindre virksomheter derimot, står toppledelsen nærmere driften og er dermed nærmere risikoen og de relaterte kontrollene, som illustrert i figur 9. I slike virksomheter er det behov for en mindre grad av overvåkingssystemer (COSO 2008).



Figur 8: Stort selskap, med lang avstand fra toppledelsen til risiko

Figur 9: Lite selskap, med kort avstand fra toppledelsen til risiko

I tillegg er noen virksomheter mer komplekse enn andre. Faktorer som kan påvirke kompleksiteten er bransjekarakteristika, regulatorisk krav, antall produkt eller tjeneste utvalg eller grad av sentralisering kontra desentralisering. Graden av kompleksitet henger sammen med risiko. Det betyr at i virksomheter med høy grad av kompleksitet, vil man finne mer intense systemer for overvåking ved hjelp av direkte informasjon. Dette i motsetning til mindre komplekse virksomheter hvor man kan forvente å finne systemer for løpende overvåking ved hjelp av indirekte informasjon (COSO 2008).

6.6. Kritiske suksessfaktorer og fallgruver for helhetlig risikostyring

I kapittel 6.5 så vi at det ikke er noe fasit for hvordan helhetlig risikostyring skal integreres på en mest mulig vellykket måte. I tillegg til de presenterte rammeverkene i denne oppgaven, finnes det flere rammeverk for helhetlig risikostyring. Å tilpasse disse rammeverkene til egen virksomhet kan i midlertid by på utfordringer. I dette kapittelet vil vi presentere kritiske suksessfaktorer som må være til stedet for en vellykket helhetlig risikostyring, samt identifiserte fallgruver.

Følgende momenter er identifisert som kritiske suksessfaktorer, og må ligge til grunn for en vellykket risikostyring (Lam 2003):

- Det er viktig med et *sterkt og synlig engasjement fra toppledelsen* for at helhetlig risikostyring skal fungere. Det gjelder spesielt engasjement fra administrerende direktør, finansdirektøren og en eventuell leder for risikostyring.
- *Etabler en dedikert gruppe av kryss-funksjonelle ansatte* for å drifte helhetlig risikostyringsimplementeringen og som også følger opp videre drift
- En nøye *kobling mellom helhetlig risikostyring og de strategisk og finansielle målene* til virksomheten, samt kobling til forretningens planleggingsprosesser

- Introdusere *helhetlig risikostyring som et ekstra verktøy* i virksomhetens allerede eksisterende og aksepterte prosesser, i stedet for å introdusere dette som et nytt system for seg selv.
- *Tilegne seg ekstern kunnskap*
- Innføring av en helhetlig risikostyring *bør skje gradvis*

I en studie gjennomført av Manab, Othman og Kassim (Manab et al. 2012) ble de kritiske suksessfaktorene for effektiv helhetlig risikostyring undersøkt. Undersøkelsen omfattet både finansielle og ikke-finansielle virksomheter, og det ble funnet at organisasjonskulturen er en av de mest kritiske suksessfaktorene for gjennomføring av helhetlig risikostyring. Andre kritiske suksessfaktorer som ble identifisert var etterlevelse/compliance, ressurser, kryss-funksjonelle ansatte, kunnskapsforvaltning og autoritet eller makt.

PwC har identifisert følgende fallgruver for effektive risikovurderinger (PricewaterhouseCoopers 2008):

1. *Risikostyring blir sett på som et engangstiltak som gir begrenset verdi*
   Vurderingene må være en gjentagende prosess som integreres i den allerede eksisterende virksomhetspraksisen, tilpasser seg endringer og gir mer enn en engangsverdi.
2. *Mengden av den innsamlede informasjonen og data er vanskelig å tolke og bruke*
   Verktøy og veiledning er nødvendig for å sikre konsistens i den innsamlede data, vurdering og rapportering.
3. *Resultatene av risikovurderingene blir ikke fulgt opp*
   Uklarhet og dårlig ansvarsdeling rundt målene kan føre til at de resultatene fra risikovurderingene ikke blir fulgt opp. Det er derfor viktig at det legges vekt på klare mål, bestemme eierskap og knytte dem til risikoene som blir vurdert.
4. *Å overkontrollere risiko kan være kostbart og sette stopper for innovasjonen*
   Virksomhetene må finne ut hvor mye risiko som er akseptabelt og hvor mye svingninger de kan tåle. Risikotiltak på prioriteres baser på en nytte-kostnadsanalyse og tilgjengeligheten av ressurser. Mangel på dette kan føre til at virksomhetene overkontrollerer risiko, noe koster virksomheten mer en nødvendig og/eller er en byrde for dens evne til å gripe muligheter.
5. *Risikovurderingene blir for gamle, og gir de samme resultatene hver gang*
   Virksomhetene må oppdatere den innsamlede data, prosessene og rapporteringene. De

må kontinuerlig oppdatere sine vurderingsteknikker og mekanismer for å forbedre analysene av risiko og for å skape bedre responsmekanismer for å håndtere overraskelser.

6. *Risikovurderingene blir lagt til dag-til-dag oppgavene uten å bli integrert i forretningsprosessene*

   Det er viktig at risikovurderingsprosessen blir forankret og integrert i den eksisterende virksomhetsstyringen. Dette kan gjøres ved å integrere diskusjon av risikovurderingene eksplisitt i møtene for virksomhetens planlegging, gjennomføring og evaluering.

7. *Altfor mange ulike risikovurderingen utføres på tvers av virksomheten*

   En felles tilnærming for utførelse av risikovurdering bør defineres. Dette bør gjøres ved hjelp av for eksempel felles verktøy, en integrert vurderingsprosess eller fleksible rapporteringer.

8. *Risikovurderingene hindrer ikke den neste store katastrofen.*

   Risikovurderingene må ikke bare vurdere tidligere erfaringene, men også fremtidsrettede analyser

DEL III: VALG AV METODE

7. METODE

Metode kan beskrives som et verktøy som kan benytter for å samle inn data. I dette kapitelet vil vi drøfte valg av metode og begrunnelse for dette valget.

7.1. Undersøkelsesdesign

Ved valg av design bestemmer man seg for hva slags undersøkelsesopplegg som skal følges, og hvilke metoder som skal benyttes når data skal samles. Det skilles mellom kvantitativt og kvalitativt forskningsdesign. *Det kvantitative* er analytisk og teoritestende, og brukes ofte der det søkes forklaring og benytter gjerne hypoteser for å teste teorier. *Kvalitative metoder* derimot, egner seg mer i tilfeller hvor det foreligger usikkerhet ovenfor hvilke trekk som skal måles. Kvantitative metoder kan beskrives som mer *rigid* i forhold til kvalitative metoder som kan beskrives som er mer *fleksibel (Askheim & Grenness 2008)*.

Formålet med vår oppgave er å få bedre innsikt i et område hvor det ikke er mye forskning. Vi ønsker å lære mer om hvilke faktorer som er avgjørende for å integrere risikostyringen som en del av virksomhetsstyringen. Av den forskningen som foreligger, finnes det ulike praksiser og anbefalinger for hvordan dette kan gjøres, men det er dernest ikke sagt at dette er et «fasit svar». Virksomheter har ulike praksiser på dette området. Det betyr at vi må samle inn informasjon på et dypere nivå, og med dette få tilgang til informasjon vi egentlig ikke vet at vi ønsker. Med kvantitativ spørreundersøkelse er det vanskelig å få utført dette, da vi ikke får mulighet til å komme med oppfølgingsspørsmål dersom nye aktuelle tema dukker opp i løpet av tiden det spørres. Vi vil dessuten risikere kun å få den informasjonen vi spør om, med mindre vi ikke åpner for kommentarer i denne type undersøkelse. En kvalitativ design derimot, er ofte eksplorativt ved at den søker en mer dypgående forståelse for tema som undersøkes. Med en slik design får vi muligheten til å kartlegge bakgrunnen for svarene informanten kommer med ved at vedkommende kan utdype hva som ligger bak svaret.

Vi har på bakgrunn av dette valgt et kvalitativt eksplorativt design, slik at vi får muligheten til å gå mer i dybden og samtidig gi informanten mulighet til å gi et mer utfyllende svar og snakke fritt om andre tema de mener er relevante. På denne måten får vi en bedre forståelse for hvorfor de ulike risikostyringsrutinene benyttes, og hvordan dette kan integreres i virksomhetsstyringen.

En kvalitativ undersøkelsesmetode har også svake sider. Metoden er først og fremst ressurskrevende. Dybdeintervjuene kan ta lang tid, og den innsamlede data kan være kompleks, samt vanskelig å tolke. Dataen kan i tillegg være ustrukturert og uoversiktlig. Ved bruk av kvalitativ metode er det en nærhet mellom forsker og informant. Hvis denne nærheten blir for tett, kan dette bli en svakhet og få uheldige virkningen. Blant annet kan dette føre til at evnen til kritisk refleksjon svekkes. Det er også problemer med generalisering ved bruk av en kvalitativ tilnærming. Det er vanskelig å vite hvor mange objekter som må undersøkes før vi kan begynne å generalisere. Muligheten for å generalisere vil være nokså begrenset, da kvalitativ undersøkelsesdesign ofte kun inkluderer et lite antall studie objekter. (Askheim & Grenness 2008)

7.1.1. Casestudie

Kvalitative undersøkelser kan gjennomføres på mange forskjellige måter. I denne oppgaven skal vi se på risikopraksisen i fire ulike virksomheter, og har derfor valgt en casestudie. Casestudie kjennetegnes ved at forskeren samler inn mye informasjon fra et fåtall enheter eller caser over en periode på uker, måneder eller år. Dette gjøres gjennom detaljert og omfattende datainnsamling. Det kan benyttes forskjellige datakilder, men alle kildene er tid- og stedavhengige.

Johannessen, Christoffersen og Tufte (2011) skiller mellom to dimensjoner i designen av casestudier. Den ene dimensjoner går på hvorvidt det foreligger én enkeltcase eller flere caser, mens den andre handler om temaet som skal analyseres og hvorvidt det brukes én eller flere analyseenheter. Samlet resulterer dette i fire designstrategier for casestudier. I denne oppgaven har vi valgt *en enkeltcasedesign med flere analyseenheter*. Det betyr at vi får informasjon fra flere enheter innenfor studiet av et avgrenset system.

Casestudier blir ofte gjennomført ved hjelp av kvalitative teknikker, slik som observasjoner eller dybdeintervjuer, som vi skal se nærmere på i kapittel 7.3.

7.2. Utvalgsstrategi

I vårt arbeid med å finne aktuelle virksomheter vi skal se nærmere på, har vi avgrenset utvalget for vår studie med følgende kriterier:

- Et norsk selskap med stor internasjonal virksomhet

- At vi får kontakt med sentrale personer i bedriften
- Informantene skal være leder for risikostyring, risikoansvarlig, medlemmer i styret eller andre som har innsikt i risikostyringsprosessen på et overordnet nivå, samt generelle trekk ved virksomhetsstyringen.
- Beliggenhet i Oslo eller omegn

Ved valg av virksomheter var vi opptatte av å finne norske selskap med stor internasjonal virksomhet, da disse er eksponert for flere ulike risikotyper som må håndteres. Det er viktig at virksomhetene er solide og har eksistert i lang tid, slik at de har stått ovenfor kriser gjennom tidene som de har håndtert. Vi søker med andre ord etter virksomheter som er bevisste på sin risikostyring. For å sikre oss dette har vi lest årsrapporter og nettsidene til utvalgte virksomheter, for å undersøke om de omtaler risiko og risikostyring her.

Vi ønsker å velge virksomheter innenfor ulike bransjer, for å kunne gi undersøkelsen en større bredde og trekke konklusjoner på et bredere og mer generelt grunnlag. Vi har bevisst valgt å utelukke finans og forsikringsbransjen, da det ofte foreligger egne og strengere krav i denne bransjen. Valg av ulike bransjer vil i tillegg føre til at flere virksomheter kan dra nytte av funnene i denne oppgaven

Virksomhetene som oppfyller våre kriterier er:

- *Yara ASA* – et norsk gjødsel- og kjemikalieselskap, og verdens ledende leverandør av mineralgjødsel.
- *Kongsberg Automotive ASA* – globalt teknologiselskap som utvikler, produserer og markedsfører systemer og komponenter for personbiler og nyttekjøretøy.
- *Jotun AS* - ledende produsent av maling og pulverlakk.
- *Orkla ASA* – et av Norges største børsnoterte selskaper, som har virksomhet innen merkevare, aluminiumsløsninger og finansielle investeringer.

Disse virksomhetene er ulike i forhold til omfang, størrelse, type virksomhet og marked de opererer innenfor. Virksomhetene benytter seg dessuten av ulike styringsverktøy og ulik utforming. Det som er felles for studieobjektene er at de har interesse for problemstillingen som vår oppgave tar opp. En nærmere presentasjon av virksomhetene finnes i kapittel 8.1.

Når det kommer til antall informanter som skal være med i studien, er en god strategi å intervjue til det ikke kommer ny informasjon fra neste virksomhet (Johannessen et al. 2011).

Målet er ikke å generalisere og dra bastante konklusjoner, men få et generelt bilde av situasjonen sett fra ståstedet til en med mye kunnskap om risikostyringen i sin virksomhet. Grunnet oppgavenes tidsfrist hadde vi kun mulighet til å intervjue fire virksomheter.

Neste steg i prosesser var å komme i kontakt med virksomhetene. Vi ønsket å intervjue den representanten i virksomheten som innehar mest kunnskap innenfor risikostyring, da vedkommende kan gi oss et best mulig bilde av risikostyringen på et overordnet nivå. Denne måten å velge ut informanter på kalles *kriteriebestemt utvelgelse* og anbefales som strategi i tilfeller der informantene må oppfylle bestemte kriterier for å delta i studien (Johannessen et al. 2011). For å finne denne personen benyttet vi oss av snøballmetoden. Her rekrutteres informantene ved å forhøre seg og finne ut av hvilke personer som vet mest om temaet som skal undersøkes.

På forhånd utarbeidet vi et skriv med beskrivelse av hva vi ønsket å finne ut av. Vi fant tidlig ut at det er vanskelig å komme i kontakt med de ønskede informantene via mail. Dette har resultert i flere oppfølgende telefonsamtaler. Vi opplevde at de vi først kom i kontakt med i de ulike virksomhetene, var behjelpelige slik at vi kom i kontakt med riktig person. Etter hvert som vi fikk kontakt med de riktige personene, ble henvendelsene møtt meget positivt, og vi inngikk avtaler om intervju.

Vi fikk kontakt med alle bedriftene vi sendte ut henvendelser til. I tabellen nedenfor har vi presentert vårt utvalg:

Navn	Bedrift	Stilling
Gro Hagom	Yara ASA	Head of Risk Management
Trond Stabekk	Kongsberg Automotive ASA	Executive Vice President & CFO
Svein Stolpestad	Jotun AS	Group Vice President, Strategy and Business development
Frank Are Berggren	Jotun AS	Group Business Development Manager
Rolf Arnljot Strøm	Orkla ASA	Vice President & Head of financial planning and analysis

Tabell 16: Utvalget

7.3. Valg av målinger

Når det gjelder intervjumetode, benyttet vi oss av et semi-strukturert dybdeintervju med et ontologisk perspektiv. Et slikt perspektiv sier at menneskers kunnskap, forståelse, samhandlinger og erfaringer gir det som undersøkes mening (Johannessen et al. 2011). Ved å bruke et semi-strukturert dybdeintervju vil informantene kunne svare fritt ut i fra hvordan vedkommende forstår spørsmålet og det er dermed ingen svaralternativer. Vi varierte

rekkefølgen på de ulike temaene og spørsmålene som følger, ut ifra hva informantene svarer. Med dette fikk informantene mulighet til å snakke fritt om sine oppfatninger, i tillegg til at informasjon som vi ikke visste fantes i utgangspunktet kom frem. Dette fikk vi stilt oppfølgingsspørsmål til. Dette vil kunne gi mer detaljert data, i tillegg til at dataene ikke vil være påvirket av andre som er tilstede, i motsetning til ved et gruppeintervju.

Vi utformet en intervjuguide som vi benyttet oss av under intervjuene. Dette for å sikre at alle temaene og problemstillingene ble tatt opp i alle intervjuene. Intervjuguiden delte vi inn i fire tema; *identifisering og vurdering, risikohåndtering og kontrolltiltak, kommunisering og rapportering og roller og ansvar*. Temaene er valgt på grunnlag av vår problemstilling og hvordan vi har valgt å strukturere denne oppgaven. I følge Johannesen et al. (2011) kan et delvis strukturert intervju gi en fin balanse mellom standardisering og fleksibilitet. Vår teoretiske forarbeid var viktig i utformingen av intervjuguiden, noe vi også dro nytte av under intervjuene. Spørsmålene i intervjuguiden ble formulert på en enkel og forståelig måte, uten vanskelig akademiske faguttrykk. Intervjuguiden finnes i vedlegg 1.

På grunnlag av informasjonen de ulike informantene ga kan vi finne likheter og ulikheter. Vi har tatt høyde for at på grunn av fleksibiliteten i denne type intervjuer vil intervjuene bli nokså forskjellig i form av hvilke temaer informantene legger mest vekt på. I tillegg har vi også tatt høyde for at spørsmål/oppfølgingsspørsmål, som i utgangspunktet ikke var med i intervjuguiden, kan dukke opp underveis.

Under intervjuene benyttet oss av lydopptak. Dette for at vi i ettertid kan gi en best mulig gjengivelse av dataen som er ble samlet inn. Det gjorde at det ble enklere for oss å stille oppfølgingsspørsmål og konsentrere oss om hva som ble sagt. Siden vi var to som utførte intervjuene passet vi på at vi hadde hver vår rolle under intervjuene, slik at vi unngikk å prate i munnen på hverandre. Etter hvert som intervjuene blir avsluttet satt vi oss ned hver for oss og notere ned det vi mente var det viktigste som kom fram.

Vi hadde som mål å møte informantene ansikt til ansikt, og helst unngå telefonintervjuer. Det er flere årsaker til dette. Ved å møte informantene tror vi det er en høyere sannsynlighet for at vedkommende tar seg mer tid og svarer mer utfyllende. Det vil også være enklere å se på informantenes reaksjon på det de blir spurt om ved å observere kroppsspråket. Vi tror i tillegg vi kan knytte sterkere bånd til informantene når vi møter dem ansikt til ansikt (Askheim & Grenness 2008). I tillegg anbefaler Askheim og Grenness å gjennomføre intervjuene i

respondentens kjente omgivelser for å sikre en god atmosfære. Dette var det mest praktiske for begge parter i vårt tilfelle.

Vi ble tatt godt i mot og opplevde åpenhet blant alle respondentene. Det var tydelig at vårt tema engasjerte respondentene og de var villige til å diskutere. Vi åpnet hvert intervju med å fortelle om vår oppgave, og hvilken rolle deres virksomhet vil ha i oppgaven. På denne måten fikk de også en bedre forståelse for undersøkelsen. Respondentene fikk så mulighet til å fortelle om sin bedrift i korte trekk. Vi opplevde at vi fikk mye verdifull informasjon ut av dette, da faktorer som historie, organisasjonsstruktur og bransje er avgjørende for hvordan risikostyringen i en virksomhet fungerer. Etter hvert gikk samtalen ned på et mer detaljert nivå. Respondentene fikk gjennom hele intervjuet komme med innspill eller avklaringer til de ulike temaene vi diskuterte.

I forkant av intervjuene brukte vi tid til å innhente skriftlig data om de ulike virksomhetene og hver respondent. Det er viktig å få god innsikt i virksomhetene, for å kunne forstå valg av styringsmetoder og risikostyringsprosesser. I tillegg har vi forsøkt å innhente mest mulig data om hver respondent og han/hennes rolle i virksomheten.

7.4. Dataanalyse

Askheim og Grennes definerer dataanalyse som «systematisering av data slik at eventuelle mønstre og strukturer trer frem» (Askheim & Grenness 2008). Å analysere kvalitative data anses ofte som en krevende prosess. Dette kommer av at det er en fare for å trekke feilaktige konklusjoner eller overse data. For å kunne legge et godt grunnlag til å trekke konklusjoner, systematiserte vi den innsamlede data og så etter mønstre i svarene til respondentene.

Ved at vi har vært to under intervjuene og analysearbeidet, blir faren for å trekke feil konklusjoner eller overse data til en viss grad minimert. Vi valgte å transkribere alle intervjuene ordrett, for og ikke gå glipp av noe data. Transkribering av intervjuene kan være svært tidkrevende, men siden vi kun hadde fire intervjuer valgte vi å gjøre dette. Intervjuene var i tillegg spredt over en periode på fire uker, som betyr at vi ikke fikk begynt med analysen før fire uker etter første intervju. Ved å transkribere hele intervjuet var det dermed ikke noe fare for at vi skulle glemme noe data.

7.5. Vurdering og validitet og reliabilitet

Det stilles også krav til *validitet* og *reliabilitet* når undersøkelsene skal kvalitetsvurderes. Med validitet og reliabilitet mener vi om resultatene er gyldige og om de er til å stole på (Askheim & Grenness 2008). Informasjonen vi samler inn kommer fra beskrivelser gitt av risikoansvarlige i de ulike virksomhetene. Vedrørende reliabilitet kan vi dermed risikere å få avvik mellom hva informantene faktisk gjør og hva de forteller oss at de gjør. Dette kan komme av at de i utgangpunktet har et fast rammeverk for risikostyring som de skal følge men som de avviker fra, eller at de anser det som sensitivt å avvike fra dette. For best mulig å unngå dette avviket stilte vi konkrete spørsmål, i tillegg til at vi ba om eksempler slik at vi på en best mulig måte kunne få et riktig bilde av den faktiske situasjonen.

For å sikre best mulig validitet var vi avhengige av å komme i kontakt med de personene med mest mulig innsikt i hvordan risikostyringsprosessene fungerer i virksomheten. Vi må ta høyde for frafall, og at vi ikke kommer i kontakt med den vi ønsker. I tillegg er det viktig at vi ikke ender opp med å analysere informantens holdning, i stedet for det virksomhetene virkelig gjør.

Rutiner og prosesser rundt risikostyring kan i tillegg anses som sensitiv informasjon hos virksomhetene. Dette kan gjøre at vi ikke får tilgang til all data vi måtte ønske. For å løse dette problemet, har vi gjort det klart for informantene at informasjonen kan holdes konfidensielt om ønskelig.

Ved å bruke en metodetriangulering, som vil si å bruke flere datainnsamlingsmetoder, vil vi kunne oppnå en bedre effekt på både pålitelighet og gyldighet i de ulike studiene (Askheim & Grenness 2008). I tillegg til dataen vi samlet inn gjennom intervjuer, benyttet vi oss også av andre skriftlige datakilder. Alle virksomhetene har fyldige årsrapporter hvor risikostyring og risikohåndtering inngår, og vi kunne derfor kvalitetssikre våre funn med dette. Dette kan bidra til en triangulæreffekt, som vil øke kvaliteten på arbeidet vårt. For å øke kvaliteten på dataen ytterligere kunne vi ha intervjuet flere personer i virksomhetene som har kunnskap innen område vi ønsker å se på. Vi anser dette imidlertid som svært tidkrevende og var i utgangspunktet fornøyd med våre intervjuobjekter, og valgte dermed ikke å gjøre dette.

DEL IV: EMPIRISK ANALYSE

I denne delen vil vi i kapittel 8 begynne med å presentere resultatene vi fikk fra dybdeintervjuene av de fire virksomhetene. Som nevnt innledningsvis har vi delt opp rutinene for helhetlig risikostyring i fire deler. Videre vil vi i kapittel 9 foreta en analyse av funnene og se dette i lys av tidligere forskning og beste praksis, samt drøfte de viktigste funnene.

8. PRESENTASJON AV FUNN FRA DYBDEINTERVJUENE

Vi begynner dette kapittelet med en kort introduksjon av virksomhetene vi har intervjuet. Deretter skal vi se nærmere på hvilke rutiner og praksis de ulike virksomhetene har for å få risikostyringen som en integrert del av virksomhetsstyringen. Disse er systematisert etter de fire delene:

- Identifisering og vurdering av risiko
- Risikohåndtering og kontrolltiltak
- Kommunikasjon og rapportering av risiko
- Roller og ansvar

8.1. Presentasjon av bedriftene

Tabell 17 på neste side viser en presentasjon av virksomhetene vi har intervjuet. Det er viktig å merke seg at det er fire forskjellige selskaper som er eksponert for ulike typer og grad av risiko. Virksomhetene har ulik størrelse, opererer i ulike bransjer og er ulikt styrt og organisert. Dette er faktorer som påvirker hvordan risikostyringen blir håndtert i virksomhetene. Felles for dem er at de er norske virksomheter med stor internasjonal virksomhet som står ovenfor ulike risikoer som de må forholde seg til, og at de har lang erfaring med risikostyring etter å ha eksistert i mange år. Hensikten er ikke å sammenligne bedriftene på tvers, men å trekke frem kritiske suksessfaktorer som synes å være avgjørende for å få til en god helhetlig risikostyring[15].

[15] Informasjonen i tabell 17 er hentet fra årsrapportene fra 2012 (Yara 2012), (Kongsberg Automotive 2012), (Orkla 2012), (Jotun 2012).

Bedrift	YARA	KONGSBERG AUTOMOTIVE	ORKLA	JOTUN
Visjon	Utvikle seg fra å være en ledende aktør til en som utformer den nitrogenbaserte kjemi industrien	Styrke kjøreopplevelsen	Utvikle mennesker - skape verdier	Utvikle, produsere og markedsføre produkter og tjenester som møter de løpende krav til kostnadseffektivitet, miljøhensyn og høy kvalitet
Strategi og mål	En lønnsom og bærekraftig vekst gjennom et sterkt fundament	Forbedre kjøreopplevelsen, samt gjøre den tryggere, mer komfortabel og berekraftig.	Gi aksjonærene en lagsiktig avkastning, godt over aksjemarkedets gjennomsnitt	Ekspandere i fremvoksende markeder (organisk vekst)
	Levere økonomiske resultater og driftsresultater på toppnivå	Levere førsteklasses produkter til en global kjøretøy-industrien	Styrke sin posisjon som Nordens ledende merkevareselskap, fokus på lokal smak	
Kjernevirksomhet	Verdens største leverandør av mineralgjødsel og bidrar til matforsyning og fornybar energi til verdens voksende befolkning	Global leverandør av ingeniør tjenester, design, produksjon for setekonfort, drivere og bevegelseskontrollsystemer, flytende enheter og og industrielle datautstyr.	Nordens ledende leverandør av merkevarer og konseptløsninger til dagligvarehandel og storhusholdning, samt bakerier/kantiner. Har også virksomhet innenfor eiendom, vannkraft, aluminium og finansielle investeringer	Omfatter utvikling, produksjon, markedsføring og salg av ulike malingssystemer til hjem, skipsfart og industri
Omsetning i 2012	84,5 mrd	7,3 mrd	30 mrd	13, 5 mrd
Antall ansatte	8 100	11 000	28 000	8 740
Børsnotert	Ja	Ja	Ja	Nei
Eierstruktur	Den norske stat (36,21 %), Fidelity Investment (2,0%), BlackRock (2,4%), Van Eck Global (2,0%), Andre (50,8%), Folketrygdfondet (6,6%)	DnB ASA (6,50%), Verdipapirfondet Handelsbanken (3,80%)	44 253 aksjonærer i 2012, Utenlandsandelen er 46 %	Gleditch familien: 54 %, Orkla: 42,5 %, ca. 400 aksjonærer
Organisasjons struktur	*3 forretningssområder:* - Oppstrøm (produksjon) - Industri (biprodukter) - Nedstrøm (salg, markedsføring og bedriftsstøtte)	*4 forrentingsområder:* - Interior - Driver Line - Fluid Transfer - Drive Control	*5 forretningsområder:* - Orkla Food - Orkla Confectionary & Snacks - Orkla Home&Personals - Orkla food Ingredients - Orkla international	*4 forretningsområder:* - Jotun Coatings - Jotun Paints - Jotun Dekorativ - Jotun Powder Coatings
Omfang/ spredning	Salgskontor i over 50 land og salg til 50 land 130 produksjonssteder i 18 land	32 produksjonsanlegg rundt i verden	Orkla omfatter bl.a Sætre, Stabburet, Nidar, Idun, Sapa og Borregaard. Øvrige virksomheter er Jotun, Sapa, Hydro Power, Orkla Financial Investment	36 produksjonsfasiliteter i 19 land 71 selskap i 45 land
Trekk ved styringssystemet	Hvert segment styres som en separat og strategisk enhet	Ansvarliggjøring av hver enkelt avdelings/enhetsleder Ledelsen utgjør en liten stab, kort vei opp fra enhetene, ingen byråkrati	Ledere på enkelte nivå ansvarliggjøres, ingen detaljsstyring fra ledelsen Strategisk målsetning for hver enkelt enhet er å slå fjorårets resultat.	Lokal myndiggjøring Fokus på langsiktighet
Sentrale risikoer	Strategisk risiko, compliance risiko operasjonell risiko, finansiell risiko, politisk/økonomisk risiko	- Finansiell risiko - Markedsrisiko - Operasjonell risiko	Risiko relatert til lønnsomhet, HMS, mattrygghet, informasjonssikkerhet, finansiell rapportering, omdømme, samfunnsansvar og compliance.	- Forretningsmessig risiko - Operasjonell risiko - Risiko mot individet

Tabell 17: Oversikt over virksomhetene vi har intervjuet

8.2. Identifisering og vurdering av risiko

Vi skal i dette avsnittet se på hvordan virksomhetene identifiserer og vurderer risiko, herunder vurdering av potensielle hendelser og hvordan konsekvenser av disse kan påvirke måloppnåelsen.

8.2.1. YARA

Hos Yara er identifisering og vurdering av risiko en integrert del av alle forretningsområder, og det foreligger definerte retningslinjer for hvordan dette skal utføres. Arbeidet med identifisering av risiko starter ved den årlige strategiprosessen, hvor risikoer forbundet med strategiene kartlegges. Hver enkelt forretningsenhet er ansvarlig for å utarbeide en egen risikoprofil. Deretter slås alle de enkelte risikoprofilene sammen i en overordnet profil for hele selskapet, som oppdateres kvartalsvis.

Ved identifisering av risiko har Yara fått et økt fokus på måling av trender og utvikling ved hjelp av KPI'er. Det er et krav at alle KPI'er skal ha en direkte tilknytning til forretningsplanen. KPI'ene har forskjellige farger ut fra hvor alvorlige de er, og de oppdateres på løpende basis. Er det et rødt tegn, er risikoen alvorlig og det må umiddelbart iverksettes tiltak. Videre er gult noe som må håndteres snarest, mens grønt indikerer at ingen vesentlige forhold er avdekket. Yara har to perspektiver på hvordan risiko måles; konsekvenser målt i finansielle termer, og konsekvenser målt i ikke-finansielle termer, slik som omdømme. Videre vurderes risikoene ut i fra konsekvens og sannsynlighet. Her benyttes det et Excel-verktøy, hvor de ulike risikofaktorene blir registrert og beskrevet. I denne vurderingen brukes det en kombinasjon av både kvalitative og kvantitative teknikker. Hensikten med vurderingen er å bestemme om nivået er akseptabelt eller ikke, for å prioritere den risikoen som har potensialet for å påvirke Yaras ytelser. Verktøyene Yara bruker for dette er illustrert i figurene nedenfor. Risikoene blir videre målt basert på iboende og gjenværende risikoer.

Likelihood					
	1	2	3	4	5
Description	Rare	Unlikely	Moderate	Likely	Almost certain
Frequency	Theoretically possible	Likely once every 5 - 20 years	Likely once every 2 - 5 years	Likely least once every 2 years	Likely to occur this year
Probability	< 5%	5 - 20%	20 - 50%	50 - 75%	75 - 100%

Figur 10: Risiko vurdert etter sannsynlighet

Consequence					
	1	2	3	4	5
Financial	**Insignificant loss** < 25 MNOK	**Minor loss** 25 - 100 MNOK	**Moderate loss** 100 - 1.000 MNOK	**Substantial loss** 1.000 - 5.000 MNOK	**Major loss** > 5.000 MNOK
Strategic objectives	**None**	**Minor impact on business unit objective**	**Moderate impact** on one or more business unit strategies	**Failure** of major business unit strategy. No short to medium term solution	**Failure to meet strategy,** business viability threatened
Human Resources	Routine matter	Short term productivity matter	Loss of personnel	High staff turnover. Loss of key personnel	Very high staff turnover, mass leave, large loss of key personnel
Press coverage	**Ignorable** minor notices in the local media	**Neutral** Moderate neutral coverage in local and national media	**Critical** Moderate coverage in national and international media	**Vocal** Front pages, both national and financial media	**Highly critical** High volume, front pages, nationa, international and financial media
Safty	No injury	Minor injury	Injury	Serious injury	Fatal

Figur 11: Risiko vurdert etter konsekvens

8.2.2. Kongsberg Automotive AS (KA)[16]

KA har ikke bestemte verktøy for risikoidentifisering, men mye av risikoidentifiseringen foregår i den løpende forretningsmodellen. Det legges vekt på at alle ansatte bruker sunn fornuft og er godt kjent med risikoene innenfor sitt ansvarsområde, i beslutningene som tas og hva dette betyr for virksomheten. I KA er det fokus på å gjøre gode vurderinger og beslutninger i operativ struktur. Prosessene for identifisering og vurdering utføres løpende helt ut i alle ledd, og risikostyringen er delegert ned til hver arbeidsprosess og hver enkelt ansatt.

I tillegg benytter KA både finansielle og ikke-finansielle KPI'er for å måle selskapets trender og utvikling. Blant annet utarbeides det rapporter på markedsstatus en gang årlig, som kan fungere som et tidlig varslingssignal. Dersom for eksempel volumet av solgte biler faller, er dette noe som vil få innvirkning på hvor mye KA klarer å selge av sine produkter til bilprodusentene. Det mottas også ukentlige statistikker fra kunder på hva som ønskes levert av produkter. Her får KA vite dersom trenden er negativ istedenfor positiv, og således vil de få en trigger dersom noe eventuelt skulle ha endret seg. Er trenden negativ, skal den ansatte benytte seg av bestemte prosedyredokumenter og vedkommende er ansvarlig for å varsle fra dersom risikoer er identifisert.

[16] Vi vil videre i oppgaven bruke forkortelsen «KA» for «Kongsberg Automotive»

Hos KA er det ikke vesentlig store verdier i hver enkelt transaksjon, men det er desto større verdi i hver enkelt kunde-kontrakt. Markedet og bransjen i totalsum er risikoaspektet. I fabrikkene har de blant annet 20 KPI'er bare på kvalitet, da kvalitet er noe av det viktigste for virksomheten. Dette inkluderer måling av KPI'er vedrørende miljø, avfall, og kvalitetsnivået hos leverandører, leveranse, restriksjoner, produktivitet, helse, miljø- og sikkerhet, skader, samt nesten-skader. Her gjelder det å bygge så gode rutiner og arbeidsprosesser at det helst ikke er mulig for de ansatte å gjøre feil. Når det gjelder finansiell risiko, vil trender for valuta og rentenivå overvåkes av sentralt. I tillegg har de ulike forretningsenhetene budsjetter for året, hvor avvik vurderes i forhold til planene. Dersom avvik identifiseres, løftes dette opp av den enkelte avdelingsleder og videre opp i systemet. KA stenger også regnskapsavdelingen i 3 dager per år, hvor de har en grundig gjennomgang av tallene på hvert forretningsområde for å se om utviklingen er etter forventningene.

KA har også en internrevisjonsfunksjon som bidrar til å avdekke risikoer og svakheter i rutiner og systemer. De foretar gjennomganger hver måned, kvalitetsrevisjoner, revisjon av HR-avdelingen og finansavdelingen. På denne måten får KA verifisert at rutinene de har følges samt at de fungerer tilfredsstillende.

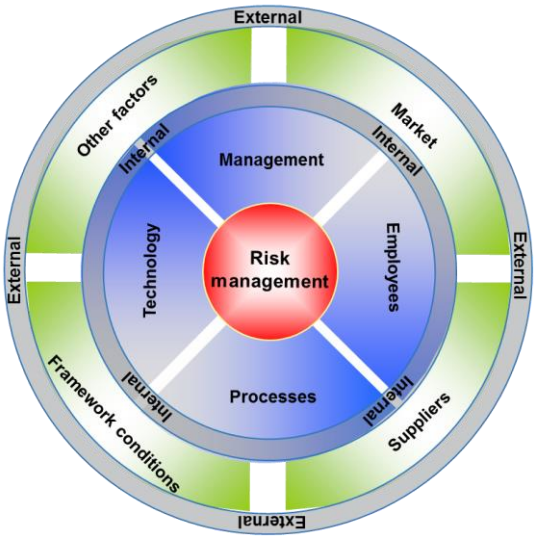
For å vurdere identifiserte risikoer benyttes det bestemte prosedyredokumenter. Her vil det fremgå når et forhold skal flagges eller ikke. I tabellen på neste side ser vi et utklipp av hvordan nøkkelrisikoer er analysert og vurdert på forhånd, hva som kan være indikatorer på risikoene, hvilke handlinger som skal utføres, samt hvem som har ansvaret for å følge det opp og når/ hvor ofte (i vedlegg 2 følger det fullstendige dokumentet).

Key Risk Factor	Early indicators	Risk Reducing Procedures		Actions	Resp.	
		Description	Reference #			Follow up in BoD
Market risk						
Top line, short term	Revenue fluctuation	Rolling forecast	Rolling Forecast Procedure	Monthly reports and Rolling Forecast	HPH/TS	Monthly
Operational risk						
Plant closures	Poor customer PPM	Dedicated, experienced project teams. STC by senior management	KA Site closure guidelines	Report progress on main transfer projects	HPH	Every meeting
	Poor delivery precision		IM 4-051a			
Supplier risks						
Material shortage	Poor delivery precision Poor Quality	Logistic Improvement Plan Quality Improvement Plan	SRT Investigation Procedure IN-PU-018-KA, IN-PU-015-KA	Follow up at Plant Level and BA level Follow up with SQD/Supplier Response Team	VP Pur	Case dependent
Financial risk						
Need to deleverage	Reduction in cash reserve / increase gearing ratio	Need operational cash flow to be in line with cash need for interest and downpayment		RF December will be the basis	TS	Monthly
Reputation risk						
Communication ext.	Negative publicity/info leaks	Communication plan		White paper crisis management	HPH/HJM	Case dependent
Legal risk						
Patent Infringement	Complaints from other players in the industry	Early patent clearance of new products	NPI procedure BL 631	Monitor severe cases in BoD meetings	Group Legal Council	Case dependent

Tabell 18: Oversikt over analyse og vurdering av nøkkelrisiko i KA

8.2.3. Orkla

I henhold til Orklas instruks for risikostyring, skal alle forretningsenheter foreta løpende risikovurderinger. Identifisering av risiko er noe de ansatte i Orkla er ubevisst opptatt av, og det ligger innebygd i bedriftskulturen. Det viktigste for å kunne identifisere risiko, er at hver enkelt ansatt forstår risikoen innenfor sitt ansvarsområde. De ulike enhetene kan ved hjelp av et risikobilde, identifisere de viktigste risikoene på grunnlag av enhetenes verdikjede. Risikobildene vil være forskjellige for de ulike enhetene. Det er opp til hver enkelt leder og ansatt å vurdere hvorvidt en risiko må løftes videre.



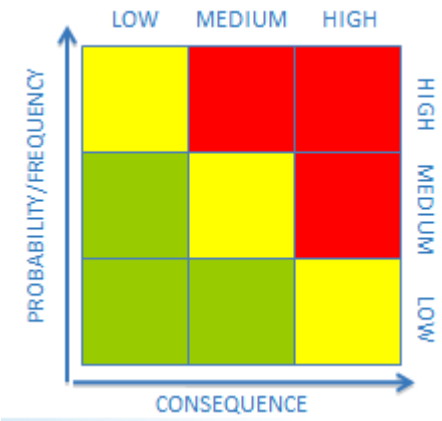
Figur 12: Prosessen for risikoidentifisering i Orkla

Prosessen for risikoidentifisering i Orkla kan forklares ut i fra følgende modell (figur 12):

Modellen systematiserer mulige årsaker til risiko, og deler de inn i risikokategorier. Modellen ser på både interne og eksterne forhold. Interne forhold er ledelsen, de ansatte, arbeidsprosessene og teknologien. De ytre faktorene fokuserer på markedet, leverandørnettverket, rammeverkbetingelser og andre faktorer. Med modellen sikrer selskapet at prosessen for risikoindentifisering dekker hele spekteret av bedriftens mulige risikoeksponeringer.

I Orkla skal alle styrene i de operative datterselskapene minst én gang årlig foreta en grundig analyse av selskapets totale risikobilde og interne kontroll. I tillegg utføres det risikoanalyse som er integrert i selskapets beslutningsprosesser. For å måle utviklingen mot fjoråret benytter Orkla finansielle KPI'er som er med på å identifisere endringer i selskapets omgivelser eller forhold innad, som er ugunstig for selskapet.

I Orkla defineres risiko som et resultat av konsekvens og sannsynlighet. Dette presenteres i en risikomatrise med ulike farger som antyder hvor alvorlig den enkelte risikoen er, slik som illustrert i figur 13. Fargen rød representerer høy sannsynlighet for at en hendelse med alvorlige hendelser inntreffer. Slike hendelser klassifiseres derfor som kritisk og krever umiddelbare tiltak. Sannsynligheten uttrykkes ofte som en prosent eller som en frekvens, mens konsekvens uttrykkes gjerne i pengeverdi.



Figur 13: Risikomatrise

8.2.4. Jotun

Jotun bygger generelt ikke opp egne systemer for å identifisere eller vurdere risiko. Dette utføres gjennom såkalte «business reviews», som er en strukturert gjennomgang av de ulike enhetenes aktiviteter og utføres ofte av konsernledelsen eller andre erfarne ansatte. I «business reviewene» følges forretningsenhetene opp etter en spesifikk bestemt mal, og måles på resultater, utvikling innenfor de spesielle segmentene, samt at prosessene internt vurderes. Det er viktig at de har implementert de riktige systemene, og fått sertifisert de tekniske kvalitetsrutinene. De må også være riktig koblet opp mot Jotun sentrale system. Dette er Jotuns viktigste styringsverktøy, og brukes også til intern benchmarking som også er med på å identifisere mulige risikoer. Blant annet kan man se om problemene i en fabrikk ligner på problemene i en annen fabrikk.

I tillegg benyttes det også KPI'er for å måle utvikling og trender i markedet. De måler blant annet hvor mange krav og reklamasjoner de mottar, og måler trender ut fra dette. Alle slike målinger kontrolleres og følges opp sentralt.

Når det kommer til vurdering av risiko, så gjøres det ofte subjektive vurderinger. Lederne i de ulike forretningsenhetene har stor tillit fra konsernet. Det er viktig å ha en leder med lang fartstid i konsernet, ofte fra hovedkontoret i Norge, som konsernledelsen er godt kjent med. Disse lederne har blitt skolert på de verdiene bedriften er tuftet på. På denne måten sikres det at den riktige kulturen kommer på plass ut i alle enheter, som er viktig for å kunne identifisere og vurdere risikoer. I Jotun er den såkalte pingvinkulturen viktig. Den står for hardførhet, stor grad av fellesskap, samtidig som ansatte skal tørre å stå alene. Kulturen gjør at lederne er innforstått med hva som er innenfor Jotuns risikoappetitt, og sikrer riktige subjektive vurderinger. Det foregår hyppige samlinger, møter og fokus på riktig opplæring. Hos Jotun er det ti ansatte som ikke gjør annet enn å reise rundt og holde kurs for de ansatte ved de utenlandske kontorene. Opplæringen skal skape en sikkerhet for at alle ansatte utfører de forretningsmessige prosessene på samme måte, og på riktig måte. Jotun er svært bevisst på å kun bruke interne kursholdere for å sikre at kulturelementet er med i opplæringen.

Mye av risikovurderingen utføres dessuten ved kartleggingen i forbindelse med strategiprosessen. De ulike forretningsenhetene sammenlignes på tvers og vurderes opp mot hverandre. Som del av strategiarbeidet, utføres det kartlegging av risiko med hensyn til selskapets måloppnåelse. Spesielt når Jotun skal etablere seg i nye land, brukes det mye tid på å kartlegge risikobildet i landet. Når Jotun har identifisert mulige risikoer, blir dette kontrollert mot Utenriksdepartementet (UD), Norsk Utenrikspolitisk Institutt (NUPI) eller andre selskap som har hatt aktivitet i det aktuelle landet. Identifiseringen av landrisiko gjøres dermed både ved å samle inn fakta og ved å dele erfaringer med andre selskap som har vært der tidligere.

8.3. Risikohåndtering og kontrolltiltak

Vi vil nå se på virksomhetenes praksis for hvordan risikoer håndteres, følges opp og overvåkes.

8.3.1. Yara

Yara beskriver risikohåndtering som en pyramide hvor strategiene for risikostyring er på toppen, mens rutiner, regler og prosesser er på bunnen. «Det handler om å ta risiko på toppen, og på bunnen må risiko kontrolleres og reduseres». For å komme fremover, må selskapet akseptere noe risiko.

For å håndtere identifiserte risikoer har Yara tiltaksplaner hvor det fremkommer hvordan de identifiserte risikoene skal håndteres. Disse er også knyttet opp mot aktuelle KPI'er og sikrer synliggjøring og god oversikt over status av risikoforholdene. Yara har strategier for å redusere risiko, samt kontroller for å sikre at risikoene blir styrt optimalt. Selskapet vurderer tiltakene utfra kostnadene for kontroll og potensielle fordeler redusering av risikoen vil gi (eksempel på hvordan tiltaksplanene blir utformet finnes i vedlegg 3). Forretningsområdene og stabsfunksjonene er ansvarlige for å forberede beredskapsplaner for risikoer med liten sannsynlighet men stor innvirkning hvis de inntreffer. Når risikoene er håndtert, blir den gjenværende risikoen kontinuerlig overvåket for å passe på at risikoene holder seg på et akseptabelt nivå. Selskapet oppdaterer sin risikoprofil ved behov, men minst en gang årlig. Tiltaksplanene blir vurdert og oppdatert hvert kvartal. På denne måten sørger de for at den gir et riktig bilde på risikoens gjeldende status og handlingsplanene. Planene blir videre presentert under de kvartalsvise møtene med forretningsområdene.

Alle organ og funksjoner i Yara overvåker og vurderer selv innenfor sine ansvarsområder om det er behov for å iverksette korrigerende tiltak vedrørende finansielle og operasjonelle risikofaktorer. Både finansielle og ikke-finansielle KPI'er overvåkes.

8.3.2. Kongsberg Automotive (KA)

I KA legges det stor vekt på at hver enkelt leder må håndtere risikoer innenfor sitt ansvarsområde. For å håndtere risikoer, må selskapet drives godt og det må foreligge gode rutiner, gode arbeidsprosesser samt riktig opplæring. Det er også avgjørende å ha de riktige menneskene.

«En virksomhet kan ha all verdens gode rutiner og systemer, men med feil mennesker vil det likevel gå galt»
-Trond Stabekk, Executive Vice President & CFO i Kongsberg Automotive AS.

De ansatte må vite hva som forventes av dem, ha kjennskap til risikoene og selskapets risikotoleranse. KA har stort fokus på å ha krystallklare retningslinjer på tvers av kulturer og geografiske avstander, slik at det ikke er tvil om hvordan arbeidet skal utføres.

Når en risiko må håndteres, settes det ofte opp et kvalifisert team som jobber særskilt med dette. Her kan ansatte fra HR, advokater, ansatte i konsernet eller ledelsen involveres for å håndtere beslutningsprosessen. Alle beslutninger som tas innebærer å balansere risikovillighet, som vil bunne ut i en samlet sum av risiko for selskapet. I risikohåndteringen blir også utviklingen av KPI'ene fanget opp av detaljoppfølgingen hos de enkelte fabrikkene til forretningsområdene. Herfra rapporteres det viktigste videre fra forretningsenhetene til styret.

«Dersom de ansatte skal bruke all sin tid til å eliminere risiko, er det ikke mye man får gjort. En viss grad risiko må aksepteres, ellers kommen man ikke fremover. I takt med at omgivelsene endres seg, må virksomheten også tilpasse styringssystemet sitt».
-Trond Stabekk, Executive Vice President & CFO i Kongsberg Automotive AS.

8.3.3. Orkla

Risikovurderingen generelt, håndteres i det daglige på et overordnet nivå. På enhetsnivå, vil identifiserte risikoer innenfor en bestemt ramme, følges opp uten at styret involveres. For å sikre løpende oppfølging, vil risikobilde til de ulike forretningsenhetene følges opp av styrene i forretningsenhetene. Her fokuseres det spesielt på endringer mot foregående år og effekten av de risikoreduserende tiltakene.

Orkla benytter fire ulike tilnærminger for å håndtere risiko. Selskapet kan velge å kvitte seg med risikoen, ved at de for eksempel velger å kutte ut et forretningsområde som er ustabilt. De kan også velge å behandle risikoen, ved at det iverksettes tiltak for å redusere risikoen. Den tredje metoden er å overføre risikoer, som kan gjøres ved at risikoen for at en bygning brenner ned overføres ved å forsikre bygningen. En fjerde metode er at risikoen kan

aksepteres. Orkla understreker også viktigheten av å se på risiko som en mulighet. Skal selskapet tjene penger må det også ta risikoer.
Figur 14 nedenfor illustrerer de fire strategier som Orkla bruker for å håndtere risiko.

Figur 14: Orklas fire strategier for håndtering av risiko

Den største fallgruven ved håndtering av risiko, er at de ansatte ikke forstår risikoen eller at håndteringen ikke er ordentlig gjennomtenkt. For å unngå dette, legger Orkla fokus på å snakke samme språk rundt risikoer.

8.3.4. Jotun

For Jotun er det viktig at alle ansatte følger rutinene og utfører arbeidsoppgavene riktig. Hvis de for eksempel får saltutslag og malingsavfall i ballasttankene på en supertanker, kan dette koste 150 millioner å reparere. Risikoen stiger i de forretningsmessige prosessene, og det får dermed større oppmerksomhet. Måten Jotun strukturerer selskapene på, følger en spesifikk mal. De ser på resultater og utviklingen innenfor de spesielle forretningsområdene samt i interne prosesser. Når Jotun får inn reklamasjoner og krav blir mye av dette registeret i en sentral database og deretter fulgt opp. Her følger de spesielt med på trender og utvikling. Dette følges opp av den enkelte forretningsenheten, og den overvåkes sentralt av en garanti- og forsikringsavdeling.

Det er ofte subjektive vurderinger knyttet til hvor alvorlig et risikoforhold er, og hvordan den skal håndteres. Her kommer verdien av Jotun sin bedriftskultur inn, og er felles for hele

virksomheten. Når det for eksempel brenner i gatene i Egypt er det opp til den lokale lederen i landet hvordan han skal håndtere dette. Det brukes mye tid på å utvikle ledere og ansatte. Jotun har en kultur som er mer mulighetstenkende enn risikotenkende. Selskapet styrer sin virksomhet i større grad gjennom mennesker, og ikke i kompliserte systemer. De har god erfaring med å holde lenge på sine ansatte, noe de ser på som en gevinst, samt at det dermed er mindre behov for så automatiserte systemer som andre store selskaper ofte har.

Måten Jotun håndterer den operasjonelle risikoen på karakteriserer de som «hands on». Hvis det oppdages problemer i et av landene Jotun er lokalisert i, kontaktes lederen i landet direkte. Er landet eksponert for en spesiell type risiko, sendes en representant ned for å bidra til å løse problemet. I de senere årene har Jotun fått en større grad av sentrale funksjoner og sentral overvåking i risikohåndteringen. Kontrollen med hvordan de driver sine prosesser har blitt styrket, og en sentralteknisk enhet skal påse at enhetene driver sine prosesser forsvarlig. Jotuns virksomheter er spredt i flere forskjellige markeder rundt i verden. Utrykket «legg ikke alle eggene i samme kurv», beskriver hvordan selskapet håndterer risiko i sin vekststrategi. De mener dette også er en viktig faktor for at de klarte seg godt under finanskrisen.

Jotun har virksomhet i land hvor korrupsjon er utbredt. Dette er noe de har nulltoleranse for, men det representerer likevel en utfordring. De har ingen fasitsvar på hvordan dette skal håndteres, men prøver å unngå å komme opp i slike situasjoner. *«Du må bare si veldig høyt at vi vil ha det hvitt, da havner du ikke i den situasjonen»*. Jotun har blitt flinke på å håndtere slik risiko. Ved å ta kontakt med representanter på et høyt nivå i det aktuelle landet, for eksempel guvernøren, ministere eller ambassadører, unngår de at byråkratene hindre dem.

«Mye av virksomhetsstyringen legger vi i de ansatte, og ikke i systemer»
-Svein Stolpestad, Group Vice President - Strategy & Business Development Jotun.

8.4. Kommunikasjon og rapportering av risiko

Når risikoer er identifisert og vurdert, må de kommuniseres til riktig tid til riktig nivå. Vi vil nå se på hvordan virksomhetene utfører denne delen av sin helhetlige risikostyring.

8.4.1. YARA

Hos Yara utarbeides det kvartalsvise rapporter i forbindelse med den årlige strategiprosessen, hvor ledere på de ulike nivåene involveres. To ganger årlig oppdateres status til styret, samtidig som det foregår en direkte rapporteringslinje etter behov om det skulle oppstå store endringer. Det utføres også kvartalsvis gjennomganger per forretningsområde, hvor risiko i større grad har fått innpass og blitt en del av dagsorden. Identifiserte endringer av risikoer kommuniseres ofte først til revisjonsutvalget. Dette utgjør første instansen på oppdatering av risikobildet, og tas videre til styret ved behov. Det er revisjonsutvalget som også evaluerer kvartals- og årsrapportene, hvor intern og ekstern revisor deltar. I tillegg til den årlige og kvartalsvise rapporteringen, får styret en rapport per forretningsområde, forretningsenhet og produktområde i forkant av kvartalsrapporteringen. Her er det noe begrenset informasjon vedrørende risiko, hvor fokuset er mer på operasjonelt plan og eksponeringsgrenser. Ved årsavslutning utarbeides det også en årsrapport.

Yara har et styringssystem som gir alle deres ansatte oversikt over gjeldende regler og prosedyrer i virksomheten.

8.4.2. Kongsberg Automotive

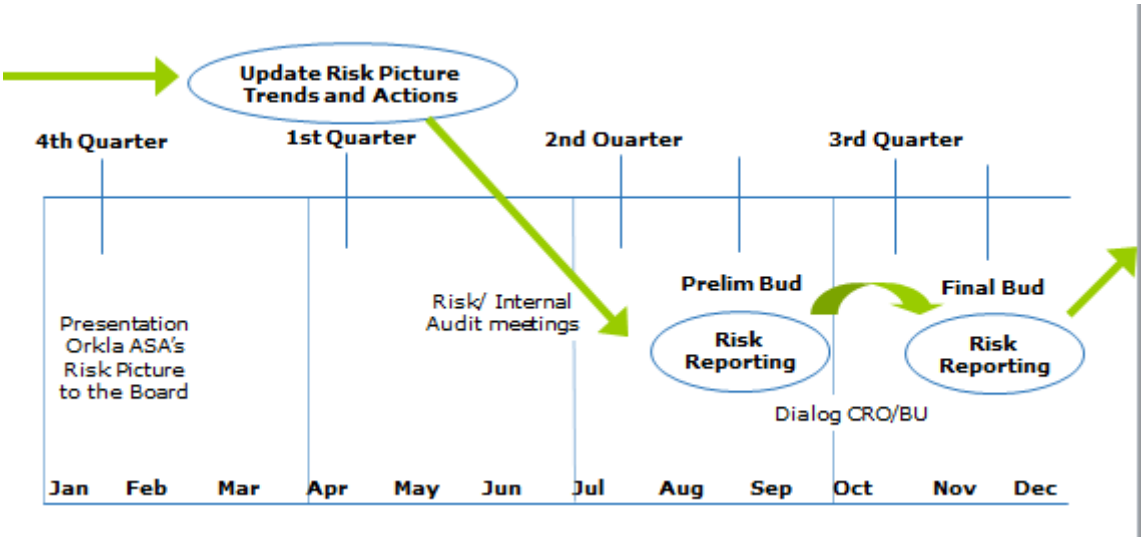
Når det gjelder å kommunisere identifiserte risikoer i KA, er det viktig at de ansatte snakker samme språk både i den enkelte forretningsenhet, men også på tvers av hele organisasjonen. Transparente IT-systemer muliggjør overvåkning fra ledelsens side på avdelinger som er geografisk spredt. Dessuten er det kort vei fra forretningsenhetene og opp til styret. Gjennom detaljoppfølging hos de enkelte fabrikkene, rapporteres det til forretningsområdene. Det viktigste rapporteres videre fra forretningsområde til styret. En del av rapporteringen går også til ledelsen, slik at de har mulighet til å følge opp. Virksomheten har også en rapport, som inneholder tidlige varslingssignaler vedrørende risiko, som utarbeides en gang årlig.

Som et børsnotert selskap, er KA pålagt å ha revisjonsutvalg som forretningsenhetene avlegger finansiell rapportering til.

8.4.3. Orkla

Hos Orkla foretas det løpende kommunisering av risiko gjennom møtene med styrene i de ulike forretningsenhetene. Styringsgruppene har møter med underselskapene flere ganger i året etter et fast oppsett. Her gjennomgås status, planer, utviklingen og strategier. Det rapporteres muntlig, samt at det foregår en løpende formell rapportering hvor det leveres inn skjema til finansdirektøren i Orkla. Videre har styringsgruppene i de ulike forretningsenhetene en gjennomgang med styret i Orkla. Det rapporteres både på periodebasis i tillegg til års-rapportering. I tillegg er det utarbeidet en *Orkla Regnskap Standard*, hvor blant annet Orklas ti hovedprinsipper for økonomisk rapportering er nedfelt.

Figur 15 nedenfor viser en oppsummering av prosessen for risikorapportering i Orkla:



Figur 15: Rapporteringsprosessen i Orkla

8.4.4. Jotun

Jotun baserer mye av sin kommunikasjon og rapportering av risiko gjennom sine «business reviews». Dette sikrer umiddelbar oppmerksom når vesentlige risikoer er identifisert. «Business reviews» utføres ofte av en representant for regionen, region-ansvarlig for et segment, samt gjerne 1-2 personer fra konsernet.

I Jotun er det ikke hensiktsmessig med store rapporteringssystemer. De mener det blir for komplekst, tidkrevende og forsinkende dersom risikoer skal rapporteres først via grønne til røde lys. Noen av risikoene Jotun er eksponert for kan kreve umiddelbare tiltak, noe de har tilrettelagt for med en organisasjonsstruktur hvor det er få kommunikasjonsledd. Det er ikke noe system for aggregering eller automatisk rapportering fra gjennomgangene av

forretningsenhetene, da dette er operasjonelt i hvert tilfelle. Via gjennomgangene per enhet skal Jotun ha kontroll på den operasjonelle risikoen.

Det utføres derimot en formell rapportering for helse – miljø -og sikkerhetsstatuser. Dette foregår som en del av finansrapporteringen, minst en gang årlig. HMS-rutinene blir vurdert sentralt for å kunne følge utvikling og trender hos de ulike enhetene. Dette fordi konsernet ønsker å ha en overvåkning, samt å kunne gi innspill.

8.5. Roller og ansvar

Hvem bør ha ansvaret for en helhetlig risikostyring i en virksomhet, og hvordan bør dette ansvaret fordeles mellom virksomhetens ansatte? Vi vil nå se på virksomhetenes praksis for dette.

8.5.1. YARA

Risikostyringen i Yara er sentralstyrt, mens ansvaret for den daglige operative risikostyringen ligger ute i linjen hos forretningsområdene og stabsfunksjonene. Hvert år vurderer styret virksomhetens viktigste risikoeksponeringer og interne kontrollsystemer. Forretningsområdene og stabsfunksjonene er ansvarlige for å gjøre en risikovurdering, herunder identifisere, vurdere og dokumentere nøkkelrisikoene som påvirker Yara. Finansdirektøren i hvert forretningsområde har hovedansvaret for risikoprosessen innenfor sitt område. I tillegg til dette utfører virksomhetens ledelse en isolert risikovurdering, hvor de har en ovenfra-og-ned-tilnærming. Det er toppledelsen som tar risikoene i forbindelse med strategiprosessen, mens det handler om å kontrollere og redusere risiko nedover i bedriften.

Gro Haugom fikk i 2009 rollen som risikoansvarlig (CRO)[17] da det ble påkrevd fra internrevisor i forbindelse med innføringen av helhetlig risikostyring i Yara. En leder for risikostyring er et viktig verktøy for å hjelpe konsernledelsen med å opprettholde et eget rammeverk for risikostyringen. Haugom fungerer som en koordinator, fasilitator, er ansvarlig for prosesser, prosedyrer samt verktøy for utvikling og rapportering av risikoer. Det er ikke hennes ansvar *å oppdage* risikoer, dette ansvaret ligger ute i linja.

«For å lykkes med en Chief Risk Officer stilling, er det avgjørende med støtte fra ledelsen. Fordelen med å integrere COSO-rammeverket er at det gir en struktur for hvordan det bør jobbes med risiko, samt at det setter navn på tingene. Imidlertid er det ikke ønskelig med en full integrasjon av COSO-kuben, da dette blir for mye byråkrati».
-Gro Haugom, Head of Risk Management Yara ASA

Yara har en internrevisjonsavdeling som jobber parallelt med risikoansvarlig, men med et annet utgangspunkt. Avdelingen er uavhengig av driften, og et viktig verktøy for styret og ledelsen for å revidere risikofunksjonen, og påse at de interne rutinene fungerer slik de bør. Selskapets compliance-avdeling, som koordinerer og fører tilsyn med selskapets overholdelse av lover og regler, har blitt styrket siden 2009 og spiller også en viktig rolle i risikostyringen. Yara har et mål om at disse funksjonene, sammen med risikoansvarlig skal jobbe enda tettere sammen for å få utnyttet hverandres kunnskap. Selskapet har et eget revisjonsutvalg som skal hjelpe styret med blant annet å evaluere risikostyringen i selskapet. Utvalget utfører løpende vurderinger av risiko og kontrollsystemet knyttet til den finansielle rapporteringen.

8.5.2. Kongsberg Automotive

I KA har styret det overordnede ansvaret for risikostyringen. De er ansvarlige for å utarbeide gode rutiner for risikostyring, samt å holde seg oppdatert på at disse følges. Styret skal videre godkjenne at de tiltakene som iverksettes er gode nok for å håndtere risikoene. Videre er hver enkelt linjeleder ansvarlig innenfor sitt ansvarsområde, mens toppledelsen har innsyn.

KA har også internrevisjoner som er med på å avdekke eventuelle svakheter og mangler i selskapets interne kontroller og rutiner. De er i tillegg pålagt å ha et revisjonsutvalg som har mandat til å håndtere finansiell rapportering av risiko.

«Det er ikke ønskelig med en Chief Risk Officer. Med en slik rolle fratas ansvaret fra de som egentlig bør sitte og gjøre de fornuftige vurderingene»
-Trond Stabekk, Executive Vice President & CFO i Kongsberg Automotive AS.

De mener at en slik stilling vil føre til at risikostyringen kommer på siden av virksomhetsstyringen og dermed ikke blir en inkluderende del av virksomhetsstyringen. I KA bygges risikorutinene inn i hver enkelt stilling, slik at ansvaret for risikostyring fordeles.

8.5.3. Orkla

Risikoer, avhengig av størrelse, følges opp innenfor enhetsnivå uten at styret involveres. Forretningsenhetene behandler risikoene på mikronivå selv, og det må opp på et visst nivå av vesentlighet før det tas videre til styret. Administrerende direktør i hver enkelt enhet har ansvaret for risikostyringen innenfor sin forretningsenhet og at alle vesentlige risikofaktorer håndteres på en hensiktsmessig og forsvarlig måte. Dette krever at lederen må ha god kunnskap og kompetanse om risikostyring. Videre er det finansdirektøren i Orkla som sitter med hovedansvaret for hele konsernet.

I Orkla var det tidligere mangel på systematisk risikorapportering og dette ansvaret lå mer lokalt. Behovet for en risikoansvarlig var derfor nødvendig for å skape et felles system for risikostyringen.

«Etter at Chief Risk Officer hadde tilrettelagt for god struktur for håndtering av risiko, falt behovet for en slik stilling etter hvert bort. Det viktige er å ha rett leder på hver avdeling, da det ikke er tid eller ressurser nok til å detaljstyre selskapet»
- Rolf Arnljot Strøm, Vice President & Head of Financial Planning & Analysis

Orklas revisjonsutvalg får presentert det samlede risikobildet for virksomheten og skal vurdere effektiviteten av systemene selskapet har for risikostyring. I tillegg har virksomheten en internrevisjonsfunksjon, som har ansvar for å kontrollere at interne kontrollrutiner for å redusere risiko er etablert og fungerer som de skal. Funksjonen er uavhengig av driften, og rapporterer til styrets revisjonsutvalg.

8.5.4. Jotun

Administrerende direktør i Jotun har det overordnede ansvaret for gjennomføringen av risiko, og det er relativt lite lederen ikke vet på et detaljert nivå. I Jotun er arbeidsprosessene svært viktig, og en del av styringen. Selskapets risikostyring er blitt mer fokusert på at de ansatte følger rutinene i arbeidsprosessene sine siden risikoene stiger i de forretningsmessige prosessene.

Jotun har en egen konsernrevisjonsgruppe som reviderer alle forretningsenhetene, og er ansvarlig for å påse at de er forsvarlig drevet. De forsøker per i dag å styrke sin

internrevisjonsfunksjon, fordi det ligger risiko forbundet med en desentralisert struktur. De mener at desto mer desentralisert en virksomhet er, desto større er behovet for internrevisjon.

Jotun har i tillegg en egen ansvarlig for corporate governance, som blant annet arbeider med selskapets samfunnsansvar, korrupsjon, lover og regler samt etisk adferd.

9. VIRKSOMHETENES RUTINER FOR HELHETLIG RISIKOSTYRING SETT MOT TEORI OG BESTE PRAKSIS

I dette kapittelet vil foreta en analyse av funnene fra virksomhetenes rutiner for helhetlig risikostyring og se dette i lys av teori, forskning og beste praksis (kapittel 6). I slutten av kapittelet vil vi trekke ut viktige hovedfunn og drøfte dette nærmere.

9.1. Identifisering og vurdering av risiko

I tabellen nedenfor har vi oppsummert de viktigste trekkene ved virksomhetenes rutiner for identifisering og vurderingen av risiko som vi presenterte i kapittel 8.2:

YARA	KONGSBERG AUTOMOTIVE	ORKLA	JOTUN
- Identifisering av risiko i forbindelse med strategiprosessen - Risiko måles basert på iboende og gjenværende risiko - Risiko måles på konsekvens og sannsynlighet - Risikoprofil per enhet, og for selskapet totalt sett - Trender og utvikling - KPI	- Utarbeides rapporter på markedsstatus, samt mottar ukentlige statistikker fra kunder - Internrevisjon avdekker risiko og svakheter i rutiner og interne kontroller - Utarbeides matrise med nøkkelrisikoer og tilhørende beskrivelse - Fokus på gode rutiner og at disse følges - Trender og utvikling - KPI	- Identifisering av risiko ligger innebygget i kulturen - Modell som viser årsaker til risiko, risikokategorier og bedriftens risikoeksponering - Risiko måles på konsekvens og sannsynlighet - Årlig analyse av selskapets risikobilde og intern kontroll per enhet - Trender og utvikling - KPI	- Identifisering av risikoer i forbindelse med strategiprosessen - Subjektiv vurdering av risiko per forretningsområde - Strukturert gjennomgang av aktiviteter i alle forretningsområde - Fokus på gode rutiner og arbeidsprosesser - Trender og utvikling - KPI - Kunnskapsdeling med andre selskaper

Tabell 19: Oppsummering av identifisering og vurdering av risiko

For at virksomheten skal få til en vellykket risikostyring og effektiv drift, er det viktig at alle beslutningstakere på alle nivå i virksomheten er oppmerksomme på hvilke risikoer selskapet står overfor. Det er dermed avgjørende å legge vekt på identifiseringen av de vesentligste risikoene, samt hvilke konsekvenser de kan gi. Risikoene som virksomhetene står overfor kan ha ulike årsaker og kilder, i tillegg kan de også ha ulike konsekvenser.

Vi ser at virksomhetene ikke bare bruker én enkel metode for å identifisere de ulike risikoene, men benytter seg av flere tilnærminger. Felles for bedriftene, er bruken av KPI'er for å måle

og identifisere selskapets trender og utvikling for de viktigste risikoene virksomheten er eksponert for. COSO har i sitt rammeverk anbefalt «workshops» som et verktøy for å identifisere risiko. Her blir de ulike aktivitetene i enhetene gjennomgått, og viktige hendelser som kanskje ellers ville blitt oversett kan bli identifisert her. Hvilket resultat disse workshopene gir, vil avhenge av graden av informasjon de ulike medlemmene i teamet sitter med (COSO). Jotun er svært opptatt av riktig sammensetningen av team. COSO understreker også at det er viktig med en erfaren tilrettelegger eller fasilitator i slike gjennomganger. Det bør også utvikles retningslinjer, regler, mål samt definisjon for bakgrunnen av gjennomgangen. Slike workshops er praksis hos flere virksomheter. Orkla har møter med alle styrene i forretningsenhetene, mens ledelsen i Yara har «review-møter» i hvert av forretningsområdene.

For å identifisere risikoer, utarbeider flere av virksomhetene også en analyse av økonomisk og finansiell informasjon. Dette er et nyttig verktøy for identifisering av risikoer, men det bør komme som et tillegg til andre identifiseringsmetoder. Ved å se på budsjett mot regnskap, samt utviklingen fra tidligere perioder, får ledelsen en god pekepinn på avvik og endringer.

Videre opplevde vi at flere av virksomhetene vurderte risikoene etter sannsynlighet og konsekvens. Orkla og Yara rangerer sine risikoer etter sannsynlighet når risikoene er identifisert. I likhet med COSO sine anbefalinger vurderer Yara risiko også etter iboende og gjenværende risiko i den løpende risikovurderingen. COSO-rammeverket anbefaler bruk av «*varsellamper ved endrede verdier av forhåndsbestemte kriterier*». Dette mente imidlertid Jotun er dårlig bruk av ressurser. Enkelte forhold krever umiddelbar handling. Det vil dermed ta for lang tid å få varslet via et slikt system først. Ved å vurdere risikoene etter sannsynlighet vil virksomhetene også kunne rangere de etter hvor viktige de er og hvor stor oppmerksomhet de bør få. Rangeringen kan hjelpe virksomhetene med å utvikle en strategi for risikostyring og allokere ressursene mer effektivt. Her mente Jotun at de hadde et forbedringspotensiale med hensyn til å unngå å allokere ressurser først til den som roper høyest, men heller sikre at det allokeres til det som er viktigst. Ved å lage bedre strukturerte rutiner rundt dette mener de at de kan anvende sin kapital og sine ressurser på en bedre måte. Med et slikt system måtte de imidlertid hatt en annen type felles filtrering og total kartlegging av alle aktivitetene.

Hos flere av bedriftene benyttes også subjektive vurderinger av risiko. Lederne i de ulike enhetene hos Jotun, har etter lang fartstid i selskapet fått god kjennskap til selskapets verdier og rammene for hva som er akseptabelt samt hva som forventes. Dette er med på å bygge opp

den sterke bedriftskulturen vi finner hos Jotun, og som gjør at styret og ledelsen kan være sikre på at riktige risikovurderinger blir gjort i alle beslutningsprosesser. Det presiseres samtidig at de ansatte aldri vil være like, og at de derfor vil ha utfordringer knyttet til subjektive vurderinger. I likhet med Jotun legges det vekt på sunn fornuft hos KA, noe som har utgangspunkt i bedriftskulturen.

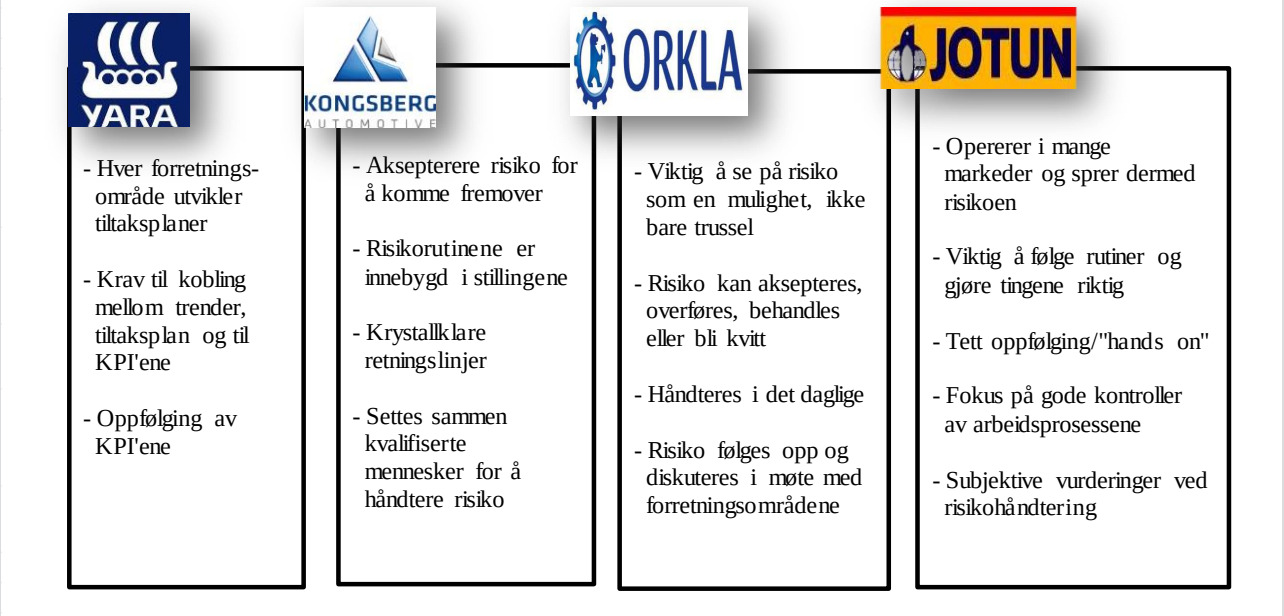
Når risikoer er identifisert og vurdert, understreker COSO viktigheten av å sikre at risikoene også blir fremstilt på en klar og konsis måte. Dette spesielt når det gjelder kvalitative vurderinger. En fin måte å få en visuell fremstilling av de vurderte risikoene på, er å benytte et risikokart ved hjelp av fargekoder. Dette gjør det også enklere å få kommunisert risikoene ut i virksomheten, og hjelper ledelsen med å fokusere på hvilke risikoer som må ha høyest prioritet. Dette ser vi er praksisen i virksomhetene.

Følgende hovedkonklusjoner er blitt gjort om viktige trekk ved rutiner for identifisering og vurdering av risiko:

- Risiko bør rangeres etter hvor viktige de er og hvor stor oppmerksomhet de bør få.
- Lederens subjektive vurderingsevne er viktig
- En regelmessig gjennomgang (workshops) av virksomhetens enheter vil være med på å identifisere risiko som ellers ville blitt oversett
- Når risikoene er identifisert er det viktig å fremstille dem på en klar og konsis måte.
- Bruk av KPI'er er et nyttig verktøy for identifisering og vurdering av risiko
- God bedriftskultur er viktig ved identifiseres og vurdering av risikoer

9.2. Risikohåndtering og kontrolltiltak

I tabellen nedenfor har vi oppsummert virksomhetens viktigste rutiner for risikohåndtering og kontrolltiltak



Tabell 20: Oppsummering av risikohåndtering og kontrollaktiviteter

Jotun karakteriserer seg selv som «mulighetstenkende før risikotenkende». Dette mener de er suksessformelen, og det som også gjør det spennende å jobbe i selskapet. I de andre virksomhetene er det også bred enighet om at det ikke er mye man får gjort om man skal bruke all sin tid på å eliminere risiko. Risiko er nødvendig for å komme seg fremover. Det synes som om virksomhetene har flyttet fokuset fra å kun eliminere risiko, til også å akseptere risiko. Dette synet er sammenfallende med hva forskningen rundt helhetlig risikostyring sier, hvor det er fokus på å fjerne stempelet om at risiko kun er noe negativt. Jon Piercey, visepresident i australske Methodware, mener det er sunt å fjerne det negative fokuset på risiko, og at det ikke lønner seg å konstant jobbe med å fjerne eller minimere risiko (Piercey 2010). Det er viktig at måten virksomheten velger å håndtere sin risiko på, er i tråd med risikoappetitten. En virksomhet kan akseptere risiko hvis den kan tåle de negative konsekvensene risikoen innehar, eller fordi de har overført eller redusert den til et akseptabelt nivå.

Alle de fire virksomhetene er geografisk spredt, noe som er en trygghet dersom markedene i Europa møter nedgangstider. Spredning av risiko samt flere ben å stå på er en bevisst forretningsstrategi fra virksomhetenes sin side.

Videre ser vi at virksomhetene legger stor vekt på å desentralisere risikostyringen nedover til hver enkelt arbeidsprosess. Det er stort fokus på å ha krystallklare retningslinjer, gode rutiner og arbeidsprosesser, slik at muligheten for å begå feil reduseres. Retningslinjene kan bidra til å kontrollere risiko samt til å redusere misforståelse og skaper en felles plattform på tvers av kulturer og landegrenser. Ledernes subjektive vurdering av hvordan risikoer skal håndteres er også avgjørende. Her er det også viktig å ha riktig bedriftskultur. Det er et viktig element også i denne delen av en helhetlig risikostyring. Uten klare retningslinjer og gode holdninger, vil ledelsen være i en situasjon hvor det kjøres en racerbil uten bremser (Lam 2003). Det understrekes at det er mennesker som til syvende og sist utfører arbeidsprosessene, og det legges derfor stor vekt på at de ansatte må forstå sin rolle og sitt ansvarsområdet med hensyn til risikobeslutninger. Som teorien også påpeker, kan en virksomhet ha all verdens gode rutiner, men det kan likevel gå galt dersom menneskene som utfører rutinene svikter.

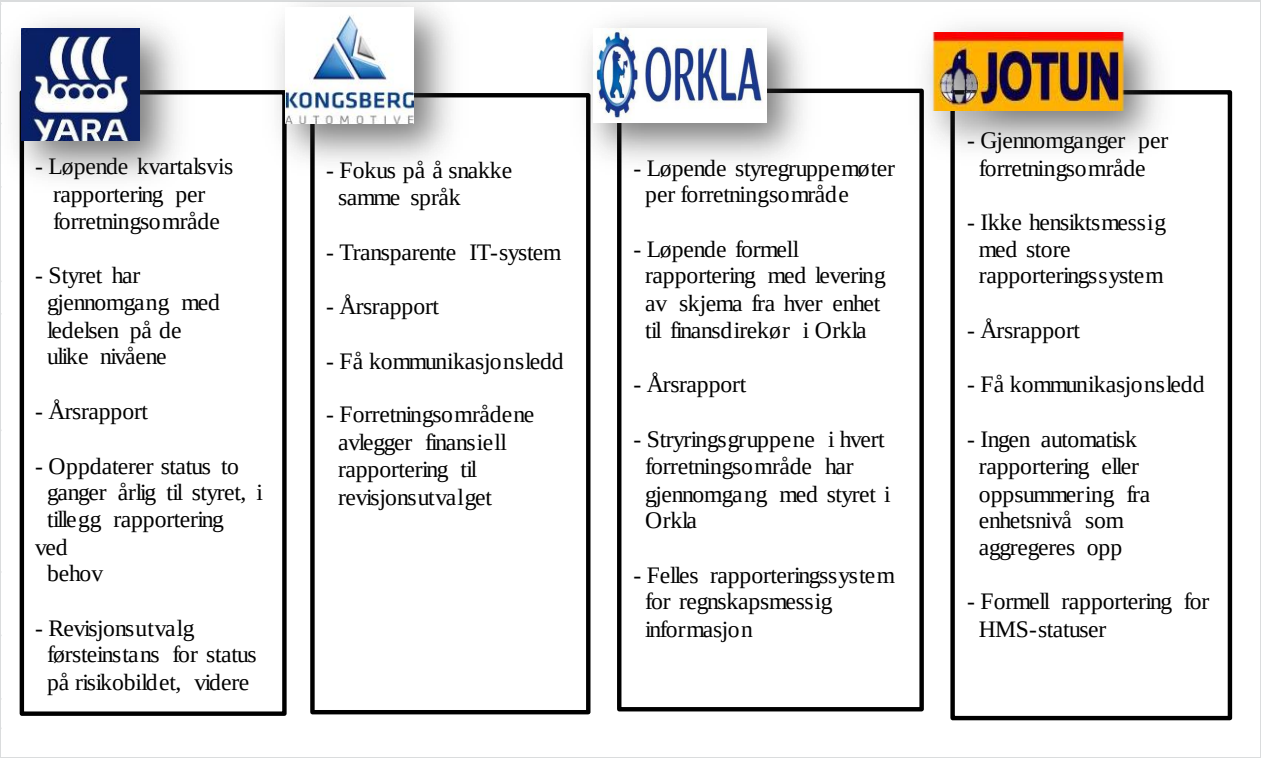
Virksomhetene bruker ikke KPI'er bare til å identifisere risikoer, men også i stor grad som et kontrolltiltak for å overvåke og prioritere risikoene. Dette synes å være et viktig verktøy som holder ledelsen oppdatert om hvordan de ligger an i forhold til måloppnåelse. Hos Yara er det et krav at det skal foreligge en kobling mellom statusen av KPI 'ene og forretningsplanen, noe som sikrer god oversikt og legger til rette for synlighet og tydelige kommunikasjonslinjer. Ellers fant vi også god praksis på bruk av risikokart, hvor handlingstiltak er utarbeidet for identifiserte risikoer. Ledelsen i selskapet foretar periodevise gjennomganger med lederne i forretningsenhetene. Felles for alle virksomhetene, er at det foretas løpende gjennomganger av forretningsenhetene for å sikre tett oppfølging av de underliggende virksomhetene.

Følgende hovedkonklusjoner er blitt gjort om viktige trekk for risikohåndtering og kontrolltiltak:

- Virksomhetene må akseptere risiko for å komme fremover. Det er viktig å se på risikoer som en mulighet, og ikke bare en trussel.
- De ansatte må forstå risikoen i sin arbeidsprosess
- Ledernes subjektive vurdering av hvordan risikoer skal håndteres er viktig
- Retningslinjene for hver enkelt arbeidsprosess må foreligge krystallklare
- KPI'er kan brukes til et kontrolltiltak for å overvåke og prioritere risikoer
- En virksomhet kan ha all verdens gode rutiner, men det vil likevel gå galt dersom det er feil mennesker som utfører rutinene.

9.3. Kommunisering og rapportering av risikoforhold

I tabellen nedenfor har vi oppsummert virksomhetens viktigste rutiner for kommunisering og rapportering av risikoforhold:



Tabell 21: Oppsummering av kommunisering og rapportering av risikoforhold

Hvor ofte det skal rapporteres avhenger hovedsakelig av virksomhetens art. Hos virksomheter som opererer i det globale kapitalmarkedet er det kanskje viktig at risikoen som rapporteres er sanntidsinformasjon som lederne kan overvåke til enhver tid. Virksomheter som opererer i marked der forholdene er mer stabile trenger ikke rapportere så ofte. Rapporter som går til toppledelsen og styret bør imidlertid begrenses til månedlig eller kvartalsvis, slik at ledelsen og styret skal kunne konsentrere seg om de viktigste risikoforholdene.

Felles for virksomhetene er at risiko blir kommunisert og rapportert gjennom møter med hver av forretningsenhetene, som foregår etter et fast oppsett et bestemt antall ganger i året. Virksomhetene benytter seg av ulike rapporteringssystemer. Hos noen av virksomhetene er praksisen å ha formelle systemer for rapportering, mens hos andre rapporteres det etter behov og gjerne muntlig. Bortsett fra HMS-rapporteringen har eksempelvis Jotun ingen formelle rapporteringssystemer. Hos Orkla og Yara derimot, rapporteres det til faste tider etter en bestemt struktur. Det er imidlertid enighet om at dersom det skulle avdekkes ytterligere risikoforhold, rapporteres dette umiddelbart.

I henhold til regnskapsloven § 3-3a, skal årsrapporten inneholde en beskrivelse av de mest sentrale risiko- og usikkerhetsfaktorene. Dette er noe alle virksomheter praktiserer.
En helhetlig risikostyringstilnærming gjør at virksomheten kan prioritere mengden og innholdet som rapporteres til toppledelsen og styret. Samtidig får virksomheten en bredere innsikt i et eventuelt samlet tap, sentrale risikoer samt risikofylte hendelser ved at informasjon aggregeres oppover i systemet.

Målet med en god risikorapportering er å øke åpenheten om risiko i hele virksomheten. Det bør tilrettelegges for en god dialog mellom administrerende direktør og leder for risikostyring i de tilfeller virksomheten har ansatt en egen leder for risikostyring. I alle de fire virksomhetene er det avgjørende at alle ansatte snakker samme språk når risiko skal kommuniseres, både i de enkelte forretningsenhetene og på tvers av virksomheten. Her er kulturen viktig. Leder for risikostyring i Yara jobber med å tilrettelegge for dette, på samme måte som tidligere leder for risikostyring i Orkla gjorde. I Yara jobber de med å bli enda bedre på kommunikasjon og rapportering.

Å rapportere relevant risiko til riktig tid til toppledelsen og styret er imidlertid ikke alltid det som praktiseres i henhold til teorien. I den «silo-baserte» tilnærmingen er det ofte ingen som tar ansvar for den overordnede rapporteringen for risiko, og hver forretningsenhet rapporterer inkonsekvent. Dette kan føre til motstridende rapporter.
I henhold til teorien, anbefales det at en risikoansvarlig for hver enhet skal hente inn data og aggregere dette opp til et overordnet nivå. Dette er praksisen både hos Yara og Orkla. Jotun har ingen automatisk rapportering fra sine forretningsgjennomganger. De fokuserer heller på umiddelbar handling fra en erfaren leder etter hvert som risikoer er identifisert.

Ideelt sett bør rapportering av risiko integreres i virksomhetens samlede rapporteringssystem, noe flere av virksomhetene er opptatt av. Å skille risiko og forretningsmessige rapporter kan sammenlignes med å skille rammene for inntekt og kostnader.

Ulike rammeverk og lovgivninger har kommet med anbefalinger og krav til ytterligere rapportering som et svar på problemer som for eksempel finanskrisen førte med seg. Personene vi intervjuet stiller imidlertid et spørsmålstegn ved om dette vil bidra til at de er bedre skikket til å drive virksomhet og herunder oppnå større verdiskapning. KA mener dette

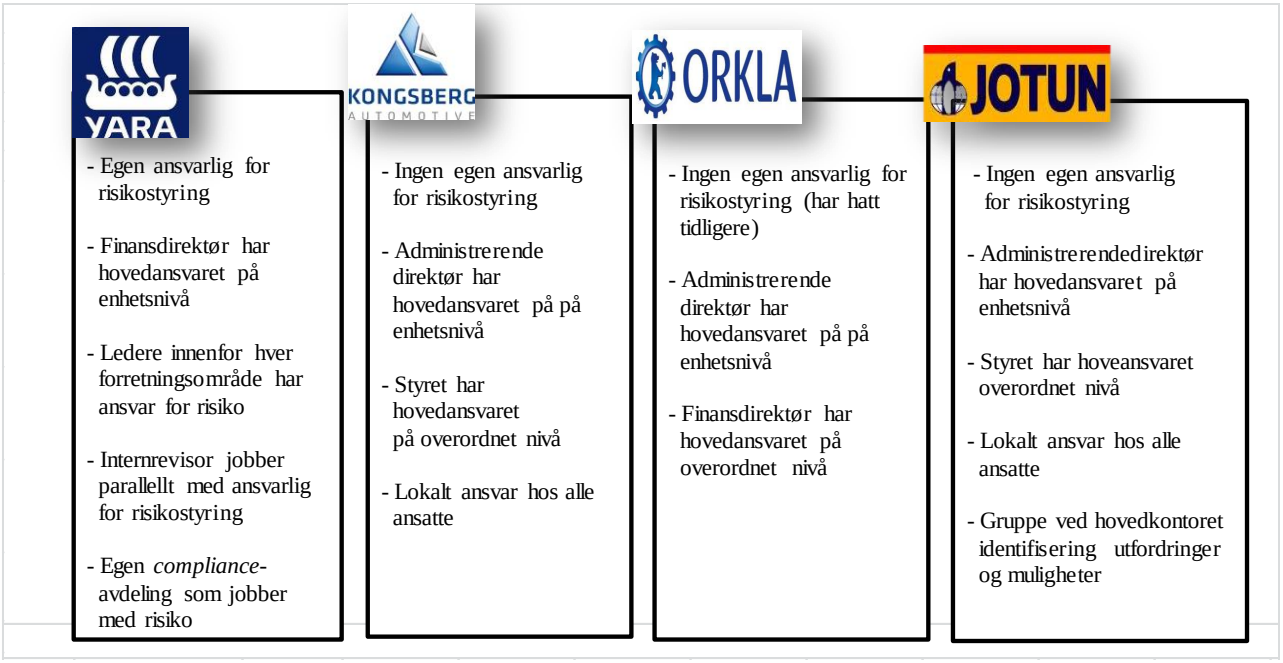
kun bidrar til tykkere årsrapporter. Virksomheter kan ha så mange rapporteringssystemer de bare vil, men dersom det eneste formålet med dette er å kompensere for at mennesker ikke gjør en god nok jobb, så får man kun en god rapportering.

Følgende hovedkonklusjoner er blitt gjort om viktige trekk for kommunikasjon og rapportering av risiko:

- Rapportene til toppledelsen og styret bør begrenses, slik at det fokuseres på de viktigste risikoene og at lederne får konsentrert seg om de viktigste tingene
- En flat organisasjonsstruktur legger til rette for få kommunikasjonsledd
- Mer rapportering fører nødvendigvis ikke til større verdiskapning
- Risikoansvarlig for hver forretningsenhet har ansvaret for å hente inn data og aggregere dette opp til et overordnet nivå.
- Risiko bør kommuniseres i møtene med hver av forretningsenhetene.
- Rapportering vedrørende risikoforhold bør integreres i virksomhetens vanlige resultatrapportering.
- Alle ansatte på tvers av virksomheten må snakke samme språk når risiko skal kommuniseres, dette må innarbeides i bedriftskulturen.

9.4. Roller og ansvar i risikostyringen

I tabellen nedenfor har vi oppsummert virksomhetens ansvars og rollefordeling for helhetlig risikostyring.



Tabell 22: Oppsummering av roller og ansvar i risikostyringen

Felles for virksomhetene er at styret har det overordnete ansvaret for å *påse* at virksomheten har på plass tilfredsstillende og hensiktsmessige rutiner for risikostyring. Styret skal i tillegg holdes oppdatert om selskapets risikosituasjon. Videre har administrerende direktør det overordnede ansvaret for *gjennomføringen* av helhetlige risikostyring, mens linjeledelsen har ansvaret for å identifisere, vurdere samt håndtere av risikoer etterleves. Dette er i tråd med Aksjeloven og andre anbefalinger, for eksempel NUES.

Fra teorien ser vi at et av suksesskriteriene for å innføre et helhetlig risikostyringssystem, er engasjement og involvering fra toppledelsen, noe som også samsvarer med hva bedriftene anser som kritisk for en vellykket helhetlig risikostyring. I Jotun rekrutterer de kun lederne som har hatt lang fartstid internt i selskapet. Dette er også med på å skape den riktige bedriftskulturen i selskapet. Dette vil bidra til å påvirke de ansattes holdninger og verdier, som kan avgjøre utfallet av beslutningene de ansatte står ovenfor i hverdagsrutinene.

Siden Orka har en mer kompleks organisasjonsstruktur enn Jotun, fører dette til at administrerende direktør i Orkla har større avstand til selskapets risikoer, mens Jotuns ledelse ligger tettere på risikoene. Hos Orkla har administrerende direktør ikke like god oversikt over

hva som skjer nede i virksomheten, slik administrerende direktør i Jotun har. Intervjuobjektet i Jotun sier at «det er lite administrerende direktør ikke vet om det som skjer på gulvet». En flat organisasjonsstruktur, kan kanskje også legge mer til rette for en god helhetlig risikostyring.

For en risikoansvarlig, er det viktig å få til et samsvar mellom selskapets beslutningstaking, risikotoleranse og kultur. En slik rolle er nyttig både som en compliance-funksjon, strategisk rådgiver og som en strategisk kontroller. I tillegg vil rollen være en nyttig organisasjonsutvikler for å sette sammen de riktige menneskene i de riktige arbeidsprosessene, i en hensiktsmessig organisasjonsstruktur (Fraser & Simkins 2010). I en studie utført av Beasley, Clune & Hermanson (2005), ble det funnet en positiv korrelasjon mellom å ha en egen leder for risikostyring og en vellykket implementering av helhetlig risikostyring (Fraser & Simkins 2010). En av driverne for å innføre en helhetlig risikostyringsmodell er å få et strukturert felles system. Vi har sett at mye av problemet med den tradisjonelle risikostyringen, har nettopp vært en manglende samkjøring og strukturert håndtering av risiko. Av informasjonen vi har fått av virksomhetene, synes det imidlertid å være mest hensiktsmessig å *ansette en egen leder* for risikostyring først og fremst ved tidspunktet for implementering av helhetlig risikostyring, og inntil systemet er oppe og går. I 2009 fikk Yara opprettet en slik stilling, som de fremdeles har i dag. Tidligere hadde de ikke noe felles risikosystem, dette ble betydelig forbedret med en slik stilling. Vi ser det samme hos Orkla, der de tidligere også hadde et slikt behov men det falt imidlertid bort etter hvert. Stillingen synes derfor kanskje å være mest aktuell som en midlertid prosjektstilling hos virksomheter som ønsker å innføre helhetlig risikostyring. Hos Jotun og KA, ser de ingen behov for en slik type stilling. De argumenterer for at risikostyringen dermed vil komme på siden av virksomhetsstyringen. Det kan derfor synes som de har misforstått denne rollen noe, siden en risikoansvarlig ikke er ansvarlig for å utføre risikostyringen, men heller skal fungere som en koordinator og tilrettelegger. Dette samsvarer også med teori og forskning som hevder at verdien og funksjonen av en slik rolle ikke er fullt ut forstått.

«The Three Lines of Defense model» etterlyser en tettere samkjøring mellom en virksomhets risikoprofil, internrevisor, compliance og risikoansvarlig. Dette viser seg også å være erfaringer fra praksis, blant annet savner lederen for risikostyring hos Yara at disse funksjonene jobber tettere sammen og dermed kan dra nytte av hverandres kunnskap og erfaring. Her har imidlertid FERMA nylig kommet med en anbefaling for hvordan disse

rollene kan struktureres for et bedre samspill. Vi ser også at internrevisor kan bidra positivt i selskapets helhetlige risikostyring.

Gjennomgående ser vi at virksomhetene understreker viktigheten av at hver enkelt ansatt forstår sin rolle i virksomheten og sitt ansvarsområde. Det er stort fokus på å ha de riktige menneskene, og ikke minst, de riktige lederne. Vi ser at beste praksis for ansvars og rollefordeling («The Three Lines of Defence») er godt innarbeidet hos de børsnoterte selskapene. Jotun, som er det eneste av de fire virksomhetene som ikke er børsnotert, har for eksempel ikke revisjonsutvalg og egen ansvarlig for risikostyring.

Følgende hovedkonklusjoner er blitt gjort om viktige trekk i rolle- og ansvarsfordelingen:

- Styret skal påse at det foreligger hensiktsmessige og tilfredsstillende systemer for helhetlig risikostyring.
- Administrerende direktør bør ha det overordnede ansvaret for gjennomføringen av risikostyring og det er avgjørende med engasjement og involvering fra toppledelsen.
- En risikoansvarlig synes å være mest aktuell som en midlertid prosjektstilling i tidspunktet for innføring av helhetlig risikostyring, behovet synes deretter å falle bort.
- En flat organisasjonsstruktur legger godt til rette for en tettere oppfølging og oversikt av risiko for administrerende direktør.
- En internrevisors rolle synes viktigere desto mer desentralisert en virksomhet er
- Det bør være en tydelig og klar ansvars- og rollefordeling for risikostyringen, samt vekt på ansvarliggjøring av de ansatte. «The Three Lines of Defence» modellen gir gir god praksis for hvordan dette bør tilrettelegges.
- Det er viktig med et tett samarbeid mellom internrevisor, compliance-avdelingen og risikoansvarlig.

9.5. *Virksomhetenes syn på rammeverk for beste praksis*

Gjennom intervjuene med de fire virksomhetene, opplevde vi at det var noe skepsis rundt rammeverkene for helhetlig risikostyring. COSO sitt rammeverk synes å være det rammeverket flest virksomheter er kjent med og tar i bruk når en helhetlig risikostyringstilnærming skal innføres (Beasley & Hancock 2010). Det var dette rammeverket også våre fire virksomheter var mest kjent med, men også det som ble rettet mest kritikk mot.

Vi har derfor valgt å se på svakhetene med dette rammeverket, og diskutere hvorvidt rammeverket bidrar til en vellykket og effektiv helhetlig risikostyring.

Det er viktig å merke seg at de åtte komponentene i COSO - kuben, ikke vil fungere likt for alle enheter, da dette ofte vil avhenge av størrelsen på virksomheten, dens omfang i tillegg til andre faktorer som er unike for hver av virksomhetene. Hvordan det blir praktisert i de ulike virksomhetene vil være forskjellig og det finnes dermed ikke noe fasitsvar på hva som er rett eller galt (Kurniawanti 2010).

Siden COSO ofte omtales som å være det mest brukte og viktigste rammeverket for beste praksis innen helhetlig risikostyring, forventet vi at det var mange som benytter seg av det i praksis og at den forbedrer effektiviteten av risikostyringen. Vi opplevde imidlertid at kun en av bedriftene benyttet seg fult ut av COSO som beste praksis. De andre bedriftene benyttet bare deler eller ingenting av den. Paape og Spekle skrev i 2011 en artikkel hvor de hevder at selv om noe forskning presenterer bevis som tyder på at helhetlig risikostyring forbedrer virksomheters prestasjoner, fant de ingen studier som undersøkte virkningene av de konkrete anbefalingene COSO-rammeverket kom med. De stiller derfor spørsmål om hvorvidt rammeverkene faktisk bidrar til forbedret risikostyring. Paape og Spekle mener rammeverket bare gir en bred veiledning, foreslår nøkkelprinsipper og konsepter men etterlater detaljene for hvordan dette skal tas i bruk til virksomhetene selv (Paape & Spekle 2011). Grant Purdy, som blant annet har vært med i utviklingen av ISO 31000:2009, har også merket seg noen svakheter med COSO-rammeverket. Han mener at kuben har mange gode poeng, men syntes det også den er komplisert og lite håndterlig. Han forstår hvorfor mange selskap kan gi opp, eller betale noen for å fortelle dem hvordan de skal implementere en helhetlig risikostyring (Marks 2011). Dette opplevde vi også at var tilfellet i praksis. Yara, som benytter seg av COSO-rammeverket, mener rammeverket gir god struktur for hvordan det bør jobbes med risiko men beskriver likevel COSO-rammeverket som veldig teoretisk og lite praktisk. De mener rammeverket kommer med mange gode ideer, men at det sier veldig lite om hvordan det skal gjennomføres. Videre påpekes det at rammeverket ikke sier noe om hva som skal til for å oppfylle implementeringen av helhetlig risikostyring. Må man gjøre alt? Kan man utføre biter av den? Virksomheten ser ikke at det er nødvendig å gå hele veien ned i organisasjonen, da dette kan skape for mye byråkrati. KA benytter deler av rammeverket, men mener det er for kompleks, og at det kan føre til at mange sliter med å implementere den.

COSO har også utviklet et vedlegg til rammeverket, som har til hensikten å gi praktiske illustrasjoner som kan være nyttig for de som ønsker å ta i bruk teknikker for helhetlig risikostyring. I vedlegget understrekes det imidlertid at materialet ikke er en del av rammeverket. Det understrekes i tillegg at *«beskrivelsene eller eksemplene gir seg ikke ut for å være en anbefalt metode eller å representere en beste praksis»* (Øvsthus & Kristiansen 2005). Forskere mener at det mangler empiriske studier somsystematisk dokumenterer konkrete praksisen for helhetlig risikostyring (Paape & Spekle 2011). De antar derfor at teknikkene som er beskrevet i vedlegget i beste fall er basert på ufullstendige bevis, og at COSO dermed ikke har rett til å presentere disse illustrasjonene som faktiske bestemmelser.

ISO 31000:2009 derimot, har mer fokus på risikostyring som en prosess. Dette gjør at det blir viet mer oppmerksomhet til selve gjennomføringen. Jim DeLoach anbefaler dermed at virksomheter som planlegger å implementere COSO-rammeverket også bør sette seg inn i ISO 31000 og andre rammeverk, for ytterligere perspektiv og veiledning om gjennomføringen og hensyn som må tas (DeLoach 2012).

Når risiko skal identifiseres legges mye av fokuset på interne faktorer, slik som systemer og kultur. Som vi også har sett, starter rammeverket med de interne omgivelsene. Med dette mister man fokuset på den innflytelsen de eksterne interessentene, regulatoriske forhold og det forretningsmessige miljøet har på risikoen virksomheten er eksponert for, dens bedriftskultur og påvirkningen på dens risikoappetitt. Dette kan føre til at bedriftene blir for innovervendt, og glemmer å identifisere de risikoene som gjenspeiler de eksterne faktorene. Videre har ikke rammeverket så mye fokus på de eksterne interessentene. De har utelatt å nevne interessentenes målsettinger og deres innvirkning på beslutninger vedrørende type og mengde risiko virksomheten står ovenfor. Purdy mener dette burde ha blitt inkludert i rammeverket da det kan få som konsekvens at virksomheten isolerer seg fra de eksternes mening og deres interessenters mål (Marks 2011).

Komponentene «risikohåndtering», «kontrollaktiviteter» og «overvåking» kan synes å virke forvirrende. Hvis en virksomhet har en revisjonsavdeling, så er dette en god måte å behandle risiko på for å redusere sannsynligheten for uønskede konsekvenser. Revisjon kan imidlertid også være en del av en styringsprosess eller en del av en overvåkingsstrategi. I ISO 31000 kommer dette klarere frem.

Til forskjell fra ISO 31000, går COSO rammeverket grundigere til verks med grundigere definisjoner og forklaringer. Dette kan være svært nyttig, da det er viktig at definisjonene i seg selv ikke skaper mer forvirring enn forklaring.

9.6. Drøfting av hovedfunn

Mye av fokuset i helhetlig risikostyring har vært å bygge opp systemer og prosesser for risiko- og overvåkningsfunksjoner, risikovurdering, målinger og rapporter. Disse faktorene ser vi på som den «harde siden» av risikostyring. Imidlertid er det minst like viktig at virksomhetene også fokuserer på den «myke-siden» av risikostyring, som kan inkludere risikokultur, opplæring, kompetanse, verdier og menneskene som utfører risikostyringen. Den myke siden kan sees på som utføreren av selve aktivitetene for risikostyring, mens den harde siden tilrettelegger og støtter risikostyringsaktivitetene. Det er ingen tvil om at begge sidene er avgjørende for helhetlig risikostyring, og må derfor balanseres.

I alle rutinene vi gjennomgikk, hadde flere av virksomhetene stort fokus på de ansatte og var svært opptatt av å ha de *riktige* menneskene, i de riktige posisjonene. Med de riktige menneskene mener de å velge faglig dyktige menneskene som samtidig passer inn i bedriftskulturen. Erfarne mennesker, som kjenner til virksomhetens verdier og krav, synes å være en viktig ressurs i helhetlig risikostyring. Med dette til grunn kan KA og Jotun bygge sin risikostyring på gjensidig tillit, og det stoles på de ansatte som tar risikofylte beslutninger. Jotun bruker dessuten mye tid på opplæring og utvikling av dets ansatte for dermed å kunne gi dem mer frihet. Virksomheten opplever at dette fører til lavere turnover og får de ansatte til å bli over lengre tid. James Lam påpeker at ledere er forpliktet til å forstå virksomheten de driver. Dette ansvaret bør ligge på alle som er involvert i virksomheten, så vel som styret, linjeledelsen og øvrige ansatte. Alle ansatte må forstå hvordan deres arbeid påvirker virksomhetens risikobilde, samt andre deler av virksomheten (Lam 2003).

God bedriftskultur synes å ligge til grunn for alle risikostyringsrutinene vi har sett på. Det ligger til grunn for risikoidentifisering, så vel som kommunisering av risiko. Dersom det skulle oppstå situasjoner som ikke er omtalt blant virksomhetens etablerte rutiner, er de ansattes vurderingsevne svært viktig da ledelsen ikke har kapasitet til å detaljstyre hver vurdering og beslutning. Teori og praksis påpeker at kultur vil kunne bidra til forståelse av hva som er viktige trusler, og konsekvenser de kan få for virksomheten.

Jo sterkere en kultur er, jo sterkere er tilliten mellom ledelse og ansatte, og mellom ansatte i de ulike avdelingene. Dette vil kunne føre til mindre kontrollbehov, intern overvåking og færre kompliserte rapporteringssystemer. Av virksomhetene vi intervjuet, var det Jotun og KA som hadde færrest formelle systemer for risikostyring. De så ikke hensikten med slike systemer, og betegnet de som altfor kompliserte. Dette kan forklares ut i fra flere faktorer. Hvis vi tar for oss Jotun, kan det tenkes at selskapet unngår kompliserte systemer fordi de ikke er børsnoterte, og dermed ikke legger så mye lovpålagt press på dette i motsetning til for de børsnoterte virksomhetene. Det kan også forklares ut fra Jotuns styringssystem, hvor det er kort vei fra de ansatte til administrerende direktør, og det dermed ikke er nødvendig med et kontrollbehovregime. Vi merket oss imidlertid også at Jotun og KA var virksomhetene som var mest opptatt av bedriftskultur, og vi fikk inntrykk av at kulturen her var sterk. Jotun er en familieeid bedrift, hvor kulturens røtter og drivkrefter lenge har blitt dyrket. Vi mener derfor at en sterk kultur gjør at virksomhetene ikke trenger like kompliserte systemer for kontroll og internovervåking som en svak kultur gjør. Helhetlig risikostyring handler dermed ikke bare om å etablere de riktige kontrollsystemene og prosessene. Risikostyringen utføres til syvende og sist av menneskene som jobber med prosessene, og hvor beviste de er på risiko kan avgjøre effektivtiten av hele risikostyringen. Virksomheter kan ha samme teknologi, systemer og prosesser, men likevel få ulike resultater. Det kan hevdes at forskjellene skyldes atferden til de ansatte, som med andre ord kan tilsi bedriftskulturen. Det synes ikke å være hensiktsmessig å legge all risikostyring i kompliserte systemer. Virksomhetene må finne en god balanse for hvor mye av virksomhetsstyringen som skal tilrettelegges gjennom systemer og hvor mye styring som skal tilrettelegges gjennom mennesker. Ved styring gjennom mennesker synes det viktig å gi de ansatte muligheter og noe frihet, samt god opplæring. Dette kan bidra til at virksomheten klarer å holde lenger på sine ansatte, noe som kan tillate mindre styring gjennom systemer, og mer styring gjennom mennesker.

Videre legger både teori og virksomhetene vi intervjuet vekt på viktigheten av klar ansvars- og rollefordeling mellom de ulike aktørene i virksomhetsstyringen. Dette viser også viktigheten av en god corporate governance, hvor det blir lagt vekt på hvordan virksomhetens ledelse styrer atferd og beslutninger gjennom tydelige rammer og retningslinjer. Det er ikke bare ledelsen som skal bidra i risikostyringsprosessene, men først og fremst de menneskene som jobber i prosessene til daglig som dermed også bidrar og gjennomfører risikostyringen. Utrykket «den som har skoen på, vet best hvor det trykker» gir et godt bilde på dette. Ledelsene i de fire virksomhetene ser ut til å være opptatt av å delegere ansvaret for

risikostyringen ned i hele virksomheten, slik at de kan bygges inn i arbeidsprosessene til hver ansatt. Virksomhetene følger viktige prinsipper innen god corporate governance ved at de utarbeider krystallklare rutiner og arbeidsprosesser som bidrar til at det gjøres gode vurderinger og beslutninger, og som skal hindre at de ansatte gjør feil. Det synes også som en flat organisasjonsstruktur legger best til rette for god risikostyring, siden det er færre ledd mellom lederen og risikoene. I tillegg vil det være færre kommunikasjonsledd mellom ledelsen og de ansatte. Lav turnover av de ansatte gjør at behovet for tunge styringssystemer kanskje blir mindre.

Vi har sett at virksomhetenes kontrollfunksjoner, slik som internrevisjon og compliance funksjon, er store bidragsytere til virksomhetens helhetlige risikostyring. Virksomhetene har også påpekt at internrevisjonens rolle ofte blir viktigere desto mer desentralisert en virksomhetsstruktur er. Videre ser vi at rollen til en risikoansvarlig, som i flere teorier påpekes som en viktig faktor i helhetlig risikostyring, ikke nødvendigvis synes like viktig ute hos virksomhetene for å lykkes med helhetlig risikostyring. Forskning viser at flere mener at virksomheter ikke bør ha en risikoansvarlig fordi det til syvende og sist er administrerende direktør eller finansdirektøren som bør ha dette ansvaret (Lam 2003). To av virksomhetene stiller seg bak dette argumentet og mener at «*dette fratar ansvaret fra de som egentlig bør sitte og gjøre de fornuftige vurderingene*». En risikoansvarlig kan imidlertid synes å være et viktig bidrag når en virksomhet skal bevege seg fra en «silobasert» tilnærming og til helhetlig risikostyring. Vi har tidligere i oppgaven også argumentert for at det kan løses gjennom en midlertidig prosjektstilling og spesielt i tilfeller der det skal bygges opp et helt nytt system for risikostyring og det dermed kreves en erfaren risikospesialist.

DEL V: AVSLUTNING

10. AVSLUTNING

10.1 Oppsummering og konklusjon

Målet i denne oppgaven har vært å identifisere faktorer som bidrar til å få risikostyringen som en integrert del av virksomhetsstyringen.

I teoridelen innledet vi med å se på viktigheten av risikostyring i et stadig mer uforutsigbart marked. Risikostyringsbegrepet har ikke alltid vært fult ut forstått, og virksomhetene har ofte hatt en «silo-basert» tilnærming til risikostyringen. Vi har sett på utviklingen av risikostyringsbegrepet, og at en helhetlig risikostyringstilnærming vil bidra til å få risikostyringen som en integrert del av virksomhetsstyringen i et selskap. Virksomhetene står ovenfor en rekke lovmessige krav for risikostyring, noe som også viste seg å være en viktig driver for helhetlig risikostyring. I tillegg er det blitt utarbeidet en rekke rammeverk og anbefalinger som skal hjelpe virksomhetene med å integrere risikostyringen som en del av virksomhetsstyringen. Vi benyttet oss hovedsakelig av COSO-rammeverket for helhetlig risikostyring samt den internasjonale standarden ISO 31000:2009, som beste praksis for rutiner som kan benyttes. I ettertid har vi diskutert hvorvidt COSO-rammeverket, rammeverket som var mest kjent blant våre fire casevirksomheter, bidrar til en vellykket helhetlig risikostyring. Våre funn og tidligere forskning viser imidlertid at rammeverket kan oppfattes som for teoretisk og lite praktisk. Vi mener rammeverket likevel gir en god anbefaling og kommer med mange gode poeng for hvordan risikostyringen kan integreres i virksomhetsstyringen. Det kan anbefales å bruke andre rammeverk som supplement når COSO-rammeverket skal benyttes.

Vi ønsket å belyse problemstillingen ytterligere ved å se på hvordan praksis for risikostyring fungerer i fire norske selskap med stor internasjonal virksomhet. Målet her var ikke å sammenligne virksomhetene på tvers, men å finne faktorer som det synes å være en enighet om for virksomhetene, teori, forskning og beste praksis. Vi var opptatt av å se på hvordan rutiner for risikostyring utføres og tilrettelegges i virksomhetene for at risikostyringen er en integrert del av virksomhetsstyringen. Videre presenterte vi funnene fra dybdeintervjuene, systematisert etter de fire områdene; identifisering og vurdering, risikohåndtering og kontrolltiltak, kommunikasjon og rapportering og roller- og ansvar.

Når det gjelder identifisering og vurdering av risikoer, har vi sett at KPI'er og workshops er nyttige verktøy. Budsjett og avviksanalyser og også nyttig, men bør benyttes i tillegg til andre verktøy siden de er for lite dynamiske. En fordel med KPI'er og workshops er at de også er nyttige verktøy i flere deler av risikostyringsprosessen, som for eksempel ved håndtering, kommunisering og rapportering av risikoforhold.

Videre har vi sett at det er viktig å rangere risikoer etter viktighet og etter hvor stor oppmerksomhet de bør få. Dette vil bidra til riktige prioriteringer og til å sikre at ledelsen allokerer ressurser riktig. Identifiserte risikoer bør fremstilles på en klar og konsis måte, her er for eksempel varmekart et anbefalt og godt brukt verktøy.

For å drive forretninger i et stadig mer krevende og skriftende marked, er det viktig å desentralisere ansvaret for risikostyringen ned til hver enkelt arbeidsprosess og arbeidsstilling, slik at hele virksomheten er med på å bidra til en god risikostyring i daglig drift. Det er også avgjørende at de ansatte forstår risikoen i sin arbeidsprosess, og vi har sett viktigheten av at alle ansatte på tvers av virksomheter snakker samme språk rundt risikoene. Risikostyringen bør også samkjøres med virksomhetens overordnede mål og strategier.

Et annet trekk for å integrere risikostyringen som en del av virksomhetsstyringen, er å fokusere på mulighetssiden av risikoer og ikke kun tenke på risiko som en trussel. Ved å bli mer mulighetstenkende kan de ansatte også få en mer spennende arbeidstilværelse, i stedet for at fokuset skal ligge på kun å eliminere risikoer. For å komme seg fremover, må virksomheten akseptere en viss grad av risikoer, i tillegg til at risiko også kan deles, unngås eller håndteres.

Når forhold om risiko skal kommuniseres og rapporteres, har vi sett at rapporter til styret og ledelsen bør begrenses til de viktigste risikoforholdene, slik at de får konsentrert seg om de viktigste tingene. De bør ikke involveres for mye i detaljstyringen, men bør holde det overordnede fokuset. Det kom også frem fra dybdeintervjuene at mer rapportering nødvendigvis ikke fører til større verdiskapning. For en god integrering av risikostyringen og virksomhetsstyringen bør rapportering av risikoforhold integreres i den allerede eksisterende resultatrapporteringen, i tillegg bør det tilrettelegges for få kommunikasjonsledd.

Styret har det overordnede ansvaret for virksomhetens risikostyring, mens daglig leder har ansvaret for gjennomførelsen. Det er viktig at både styret og ledelsen involverer seg i virksomhetens risikostyring, samt at de ansvarliggjør de ansatte for sitt ansvarsområde. Det bør også tilrettelegges for et tydelig ansvar- og rollefordeling. «The Three Lines of Defense»

modellen er god og anerkjent praksis for hvordan dette kan utføres. Modellen tilrettelegger også for et godt samspill mellom de ulike partene i en virksomhet. Spesielt er det viktig at det er et godt samspill mellom compliance-funksjonen, internrevisor og risikoansvarlig, som alle sitter med verdifull erfaring og kunnskap vedrørende risiko. For virksomheter med en flat struktur, ser vi at slike roller blir desto viktigere. Vi har også konkludert med at en egen risikoansvarlig stilling (CRO), synes å være mest hensiktsmessig som en midlertidig prosjektstilling ved innføringen av en helhetlig risikostyringstilnærming.

Til slutt i denne oppgaven så vi at god bedriftskultur er noe som ligger til grunn for alle rutinene vi har sett på. God bedriftskultur bidrar til gode vurderingsevner blant de ansatte, ved at de blant annet får en bredere forståelse for hva som er viktige trusler. God bedriftskultur fører videre til mindre behov for kompliserte overvåkingssystemer og kontrollbehov. Vi har sett at kompliserte systemer og rutiner for risikostyring ikke nødvendigvis er svaret på hvordan risikostyringen kan integreres i virksomhetsstyringen. Systemene skal ikke erstatte at menneskene ikke gjør en god nok jobb. Vi har gjentatte ganger i denne oppgaven poengtert viktigheten av mennesket. Virksomhetene bør balansere styringsfokuset mellom systemer og mennesker.

På bakgrunn av casestudie, teori og beste praksis vi har sett på i denne oppgaven, har vi kommet frem til hvilke faktorer som synes å bidra til å få risikostyringen som en integrert del av virksomhetsstyringen. Faktorene er oppsummert i figuren på neste side.

Figur 16: Faktorer som bidrar til å få risikostyringen som en integrert del av virksomhetsstyringen

10.2. Videre studier

Helhetlig risikostyring er et relativt nytt tema i litteraturen, først i det siste tiåret har vi sett en florering av bøker, artikler, rammeverk og lovgivninger som omtaler tema. I arbeidet med denne oppgaven har vi imidlertid savnet tidligere forskning som ser på faktorer som er med på å integrere risikostyringen som en del av virksomhetsstyringen. Spesielt blant norske virksomheter foreligger det lite forskning innen dette.

For å svare på vår problemstilling var vi nysgjerrige på hvordan risikostyringen faktisk fungerer i praksis. På grunn av oppgavens tidsrammer hadde vi ikke mulighet til å intervjue flere enn fire virksomheter. Ved å intervjue flere virksomheter er det mulighet for å generalisere og dermed dra konklusjoner på et bredere grunnlag. I denne oppgaven har vi ikke fått mulighet til å generalisere, men kun fått en pekepinn på hvilke faktorer som synes å være avgjørende.

10.3. Kildehenvisning

Anthony, R. N. & Govindarajan, V. (2007). *Management control systems*. Chicago: Irwin.

Askheim, O. G. A. & Grenness, T. (2008). *Kvalitative metoder for markedsføring og organisasjonsfag*. Oslo: Universitetsforl. 189 s. : ill. s.

Aven, T. (2007). *Risikostyring: grunnleggende prinsipper og ideer*. Oslo: Universitetsforl. 180 s. : ill. s.

Banham, R. (2005). Enterprising Views of Risk Management. Tilgjengelig fra: http://www90.homepage.villanova.edu/michael.pagano/MBA%208060%20Enterprising%20Views%20of%20Risk%20Management.pdf.

Banks, E. (2012). *Risk culture : a practical guide to building and strengthening the fabric of risk management*. Basingstoke: Palgrave.

Basel Committee on Banking Supervision. (2004). International Convergence of Capital Measurement and Capital Standards.

Beasley, M. S. & Hancock, B. C. B. B. V. (2010). COSO's 2010 report on ERM; Current State of Enterprise Risk Oversight and Market Perceptions of COSO's ERM Framework.

Bellamy, P. & Vikdal, H. M. (1999). Helhetlig og integrert risikostyring. *MAGMA Econas tidsskrift for økonomi og ledelse*.

Chapman, R. J. (2012). *Simple tools and techniques for enterprise risk management*. Chichester: Wiley.

COSO. (2008). Guidance on Monitoring Internal control Systems.

Dagens Næringsliv. (2010). Statoil ville trolig gått konkurs. Tilgjengelig fra: http://www.dn.no/energi/article1944873.ece.

Davenport, E. W. & Bradley, M. Enterprise Risk Management: A Consultative Perspective.

DeLoach, J. (2012). COSO, ISO 31000 or another ERM Framework? Tilgjengelig fra: http://www.corporatecomplianceinsights.com/coso-iso-31000-or-another-erm-framework/.

Entrepreneur. (2013). Corporate Culture. *Entrepreneur*.

Ferma & ECIIA. (2010). *Veiledning i EUs åttende selskapsdirektiv*.

Financial Services Authority. (2002a). Integrated Prudential sourcebook.

Financial Services Authority. (2002b). Operational risk systems and controls.

Financial Services Authority. (2003). Building a framework for operational risk management: the FSA's observations.

Finansdepartementet. (1999). *Lov om årsregnskap m.v. (regnskapsloven)*: Lovdata.

Finansdepartementet. (2009). *Om lov om endringer i revisorloven og enkelte andre lover (gjennomføring av revisjonsdirektivet)*.

Fraser, J. & Simkins, B. J. (2010). *Enterprise risk management*. Hoboken, N.J.. Wiley.

Gaudernack, K. L. J. (2008). Styrets risiko- og kontrolloppfølging: Hva er status etter de nye EU-kravene? : 6-11. Tilgjengelig fra: http://www.pwc.no/no/mentor/mentor-2008-4.pdf.

Godal, O. I. (2013). Internasjonalisering gir økt risiko. *aftenbladet*.

Hallaråker, T. & Vig, J. (2006). *Praktisk enterprise risk management*. Oslo: Kolofon.

Hoff, K. G. & Holving, P. A. (2002). *Balansert målstyring: balanced scorecard på norsk*. Oslo: Universitetsforl.

Johannessen, A., Christoffersen, L. & Tufte, P. A. (2011). *Forskningsmetode for økonomisk-administrative fag*. Oslo: Abstrakt forl.

Jotun. (2012). Annual report 2012: www.jotun.no.

Justis- og beredskapsdepartementet. (1999). *Lov om aksjeselskaper (aksjeloven)*.

Kleffner, A. E., Lee, R. B. & McGannon, B. (2003). The Effect of Corporate Governance in the Use of Enterprise Risk Management: Evidence From Canada. *Risk Management & Insurance Review*, 6 (1): 53-73.

Kongsberg Automotive. (2012). Annual Report 2012: www.kongsbergautomotive.com.

Kurniawanti, I. A. (2010). Critiques towards coso's enterprise risk management(erm) framework in its basic assumptions. *Tahun XX*, 3.

Lam, J. (2003). *Enterprise risk management: from incentives to controls*. Hoboken, N.J.: Wiley.

Ledernytt. (2012). Bedriftskultur er en viktig lederutfordring. *Ledernytt; kunnskap, inspirasjon og entreprenørskap*.
Liebenberg, A. P. & Hoyt, R. E. (2003). The Determinants of Enterprise Risk Management: Evidence From the Appointment of Chief Risk Officers. *Journal of Risk and Insurance*, 6 (1): 37-52.
Lindeberg, A. (2013). In Amenas endrer ikke vår strategi. *Dagens Næringsliv*.
Manab, N. A., Othman, S. N. & Kassim, I. (2012). Enterprise-Wide Risk Management Best Practices: The Critical Success Factors. *OIDA International Journal of Sustainable Development*, 04 (03): 87-96.
Marks, N. (2011). *10 reasons not to like the COSO ERM framework - a discussion with Grant Purdy*. Norman Marks on Governance, Risk Management and Audit.
Martens, D. L. R. F. (2012). Understanding and Communicating Risk Appetite: www.coso.org.
Miccolis, J. A., Hively, K. & Merkley, B. W. (2001). *Enterprise risk management: trends and emerging practices*. Altamonte Springs, Fla.: Institute of Internal Auditors Research Foundation.
Moeller, R. R. (2011). *COSO enterprise risk management : establishing effective governance, risk, and compliance processes*. Hoboken, N.J.: Wiley.
NHO. (2013). *Samfunnsansvar*: NHO. Tilgjengelig fra: http://www.nho.no/samfunnsansvar/.
Noreng, S.-R. (2002). Enterprise Risk Management. *MAGMA Econas tidsskrift for økonomi og ledelse*.
Norges Interne Revisorers Forening. (2013). *The institute of internal auditors (IIA) - vår globale tilknytning*. Tilgjengelig fra: http://www.iia.no/The+Institute+of+Internal+Auditors+%28IIA%29+-+v%C3%A5r+globale+tilknytning.9UFRnI5Y.ips.
Norsk utvalg for eierstyring og selskapsledelse. (2013). *Norsk anbefaling Eierstyring og selskapsledelse*.
OECD. (2004). *OECD Principles of Corporate Governance*.
Orkla. (2012). Orkla årsrapport 2012: www.orkla.no.
Paape, L. & Spekle, R. F. (2011). The Adoption and Design of Enterprise Risk Management Practices: An Empirical Study. *European Accounting Review*.
Pagach, D. & Warr, R. (2011). The Characteristics of Firms That Hire Chief Risk Officers. *Journal of Risk and Insurance*, 78 (1): 185-211.
Pickett, K. H. S. (2005). *Auditing the risk management process*. Hoboken, N.J.: Wiley.
Piercey, J. (2010). Impact of ISO 31000 on Existing ERM Programs. *Methodware*.
PricewaterhouseCoopers. (2007). Din guide for ansvarlig eierstyring og selskapsledelse.
PricewaterhouseCoopers. (2008). A practical guide to risk assessment.
PricewaterhouseCoopers. (2013). *Om oss*. Tilgjengelig fra: http://www.pwc.no/no/om/index.jhtml.
Rasid, N. M. G. S. Z. A. (2012). What Leads Firms to Enterprise Risk Management Adoption? A Litterature Review. *International Conference on Economics, Business and Marketing Management*, 29.
Solberg, M. (1996). *Intern kontroll: et integrert rammeverk : oversettelse av COSO-rapporten*. Oslo: Cappelen akademisk forl.
Standard, N. (2010). *Risikostyring: prinsipper og retningslinjer*. Lysaker: Standard Norge.
Standard, N. (2012). *Risikostyring: metoder for risikovurdering*. Lysaker: Standard Norge.
The inistitue of internal auditors. (2013). The Three Lines of Defense in Effective Risk Management and Control: Is Your Organization Positioned for Success?
VIPE. (2013). *Samfunnsansvar*: VIPE. Tilgjengelig fra: http://www.vipe.no/xp/pub/no/site/tjenester/samfunnsansvar/index.html.
Wiggen, T. M. (2008). Hva er risikostyring?: DNV.
Wikipedia. (2013a). *Key Risk Indicators*.
Wikipedia. (2013b). *Treasury management*.
Yara. (2012). YARA finansrapport 2012: verdiskapning gjennom lønnsom, bærekraftid vekst: www.yara.no.
Øvsthus, K. & Kristiansen, M. (2005). *Helhetlig risikostyring : et integrert rammeverk*. Oslo: Norges interne revisorers forening.

10.4. Vedlegg

10.1.1. Vedlegg 1: Intervju guide

Forståelse for risiko og risikohåndtering

- Hvilke type risiko er bedriften mest eksponert for i dag?
- Hvilke potensielle fremtidige risikoer er bekymringsverdige?
- Hva forstår organisasjonen mht. utrykket helhetlig risikostyring (ERM)?

Risikoidentifisering og vurdering

- Hvordan identifiseres ulike type risikoer? Hvilke type verktøy og teknikker brukes det for å identifisere risiko? (Bruker dere en risiko sjekkliste, spørreskjema, scenarioanalyser som hjelp til å identifisere risiko?)
- Når er en risiko vesentlig eller uvesentlig? Innenfor hvilke rammer/risikoappetitt
- Hvordan vurderes sannsynligheten for at en risiko skal inntreffe? Sannsynlighetsberegninger?
- Hvem har ansvaret for identifiseringen av risiko? (en overordnet gruppe eller hver avdeling som er ansvarlige for dette?)
- Hvordan kommuniseres de identifiserte risikoene ut i virksomheten og hvordan inngår de i planleggingsprosessen?
- Hvis dere har en formalisert prosess; når og hvor ofte foregår risikoidentifiseringsprosessen?
- Hvordan rapporterer organisasjonen risikoer den har identifisert. F.eks. i et risikoregister, en risikodatabase?
- Hvilke verktøy eller teknikker brukes for å vurdere risikoene i organisasjonen?

Ansvar og roller

- Hvem i organisasjonen har hovedansvaret for risikostyringsprosessen? Involveres flere nivå i organisasjonen?
- Hva er ansvaret til de sentrale lederne (CEO, CFO, talsmann osv) i ditt selskap, med hensyn til helhetlig risikostyringssystemet?
- Hvis styret har et revisjonsutvalg: Mottar styrets revisjonsutvalg jevnlig rapporter om bedriftens risikostyringssystem? Hvis ja, beskriv informasjonen som deles med revisjonsutvalget.
- Hvordan involveres en nyansatt (og andre ansatte) i bedriftens forhold til risiko?`(herunder risikoappetitt, håndtering, ansvar, bevissthet)

Risikohåndtering:

- Når en gitt risiko er identifisert, hvordan går dere fram for å håndtere den? (Verktøy, teknikker)
- Etter din erfaring, hva er de typiske fallgruvene i en suksessfull iverksettelse av et kontrolltiltak?

Måle/overvåke og rapportere risiko:

- Hvordan blir risikostyringstiltakene fulgt opp?
- Kan du gi noen eksempler på informasjon som brukes for å overvåke risiko?
- Hvordan rapporteres forhold om risiko inn til ledelse og styret, som en del av den månedlige rapporteringen
- Kan du beskrive noen av KPI'er (Key Performance Indicators) som brukes, og hvordan de hjelper til med å følge opp og håndtere risiko?
- Hvem er ansvarlige for å overvåke risikoen?
- Hvilke (finansielle / ikke-finansielle) parametere legges det vekt på i målingen av virksomhetens utvikling?

Styringsmodell

- Fortelle litt om det virksomhetsstyringssystemet dere bruker og hvordan det følges opp?
  (Budsjett, BM, rullerende prognoser, sentralisert/desentralisert)
- Hvordan håndteres risiko i styringsmodellen? Integrert eller er det adskilte prosesser?
- Utarbeider økonomiavdelingen risikoanalyser underveis eller skjer dette som en del av den periodiske rapporteringen? Hvordan bidrar de i strategiplanlegging?
- Etter finanskrisen har det kommet strengere krav til både virksomhetsstyring og risikostyring, hva har de største utfordringene vært i forhold til deres bedrift?
- Hvilke styrker og svakheter mener du det er ved bedriftens styringssystem i dag når det gjelder risikorapportering og håndtering?
- Hvilke ulike rammeverk, anbefalinger og krav tar dere utgangspunkt i?

Key Risk Factor	Early indicators	Risk Reducing Procedures		Actions	Resp.	Follow up in BoD
		Description	Reference #			
Market risk						
Top line, short term	Revenue fluctuation EBIT shortfall	Rolling forecast Monthly financial report	Rolling Forecast Procedure PR-FI-001-KA	Monthly reports and Rolling Forecast	HPH/TS	Monthly
Top line, long term	Long term profitability	STP process and special analyses	STP process	Targets and focus areas	BoD	March
	Product and customer mix Long term revenue growth			Strategy review	BoD	June
Distressed customers	Late payments, drop in volumes	Secure payments, shorten terms	AR follow up routine	Weekly monitoring	TS	Case dependent
Operational risk						
Plant closures	Poor customer PPM Poor delivery precision Labor conflicts	Dedicated, experienced project teams. STC by senior management	KA Site closure guidelines IM 4-051a	Report progress on main transfer projects	HPH	Every meeting
Warranty	Warranty claims	Warranty agreements	KA warranty handling procedure SKJ 8131, SKJ 8132	Monitor severe cases in BoD meetings	HPH	Case dependent
Natural disaster	Extreme weather, flooding	KA disaster team	Contingency plans	Monitor severe cases in BoD meetings	HPH	Case dependent
R&D Projects (NPI)	Late gate passing's, project delays, missing customer deliverables. Quality concern escalation at customers.	Follow NPI procedure, agree on corrective actions in STC meetings	NPI procedure BL 435 Customer enquiry review BL 466 CSR Matrix FO-PM-002-KA RVS Sheet BL 290 NPI procedure BL 435	Monitoring of all NPI projects in monthly STC meetings Audits of critical/important projects NPI performance reported in CFR report	VP BA MAVO MAVO	Case dependent Case dependent Monthly
MRP systems	Poor delivery precision, extra ordinary freight, material shortage	Standardize MRP systems within KA		Transition plan towards SAP is established	TS	Annually (Quarterly in ExCom)
Supplier risks						
Material shortage	Poor delivery precision Poor Quality Material allocation	Logistic Improvement Plan Quality Improvement Plan	SRT Investigation Procedure IN-PU-018-KA, IN-PU-015-KA	Follow up at Plant Level and BA level Follow up with SQD/Supplier Response Team Severe cases monitored in BoD meetings	VP Pur	Case dependent
Raw material incr.	EBIT shortfall	Purchase STC	PUR-007	Monthly reports and Rolling Forecast	VP Pur	Annually
Supplier finical distress	Supply shortages, request for shorter payment terms	Purchasing Procedure	IN-PU-016-KA	According to procedure	VP Pur	Case dependent
Financial risk						
Need to deleverage	Reduction in cash reserve / increase gearing ratio	Need operational cash flow to be in line with cash need for interest and downpayment		RF December will be the basis	TS	Monthly
Reputation risk						
Communication ext.	Negative publicity/info leaks	Communication plan		White paper crisis management	HPH/HJM	Case dependent
Communication int.	Employee dissatisfaction	Code of conduct	Code of conduct	Case dependent	HPH/JNY	Case dependent
Corporate Governance	Negative public reports	Audits	Group guidelines	Case dependent	HPH	Case dependent
Key personnel						
Succession	Talents leaving KA	Succession planning procedures	Global HR Procedure PG 064	Annual review	CC/JNY	Annually
Mgt training	Negative feedback from org, weak results	Offer professional management training for all managers every year		Report on progress	JNY	Annually
Dissatisfied customers						
New business hold, de-sourcing	Customer Scorecards and feedback	Monthly monitoring of customer scorecards & feedback	KPI reporting instruction - INS 8161	Customer Scorecard status will be reported as part of Customer Focus Report (CFR) introduced in 2012.	MAVO	Monthly
Legal risk						
Patent Infringement	Complaints from other players in the industry	Early patent clearance of new products	NPI procedure BL 631	Monitor severe cases in BoD meetings	Group Legal Council	Case dependent
Product liability claims	Customer complaints, field problems, warranty issues	Insurance coverage	KA insurance program	Monitor severe cases in BoD meetings	Group Legal Council	Case dependent

Risk assessment

Unit	Communications
Department	Branding
Date	17-Dec-2010
Risk nr	1
Risk category	Strategic
Risk title	Brand Strategy and Identity Risk
Risk owner	Bente Slaatten

Inherent risk:

Likelihood	4 - Likely, 50 - 75%
Consequence	3 - Moderate loss, 100 - 1.000 MNOK

Residual risk:

Likelihood	3 - Moderate, 20 - 50%
Consequence	2 - Minor loss, 25 - 100 MNOK
Current risk level	Moderate risk
Control rating	
Risk response	

Risk description

Inconsistent or discontinuous representation of the Yara brand position will create false expectations to our offerings, leading to decrease in sales and margins and overall weakening of our market position and prospects for profitable business in future. Inconsistent or discontinuous representation of the Yara brand identity ranges from stealing and/or misuse of Yara brand identity by other companies to the misuse of identity by Yara itself, weakening our brand protection and brand impact.

Description of current risk mitigation

Powerbrand positioning to avoid inconsistencies in product sales. Central branding tools developed for everybody's use globally (VIM, Web-To-Print, literature and stationary templates). Branding intranet and direct mails. Studio to support 7-24 globally. Regular on-line and on-site trainings.

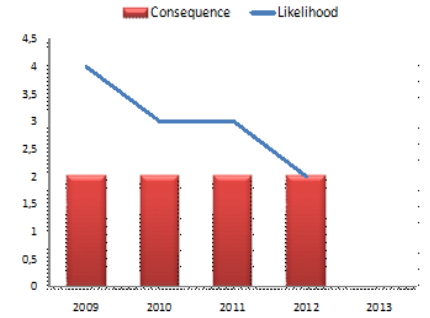
Risk mitigation plan

Action	Action owner	Deadline	Review date	Status	Comments	Date last updated
Improve understanding of Yara brand strategy and identity	A. Künnapuu	31-Dec-2011	31-Dec-2011	Started		17-Dec-2010
Audit compliance of business plans and KPIs with the Yara brand strategy	A. Künnapuu	31-Dec-2012	1-Mar-2012	Started		17-Dec-2010
Establish brand management directives and procedures	A. Künnapuu	31-Dec-2010	31-Mar-2011	Completed		17-Dec-2010
Establishment of brand surveys for improved customer insight to evaluation of	A. Künnapuu	31-Dec-2012	31.06.2011	Started		17-Dec-2010
Centralise and systematize trademark protection procedures	Kirsti C. Velasque	31-Dec-2011	31-Dec-2011	Started		17-Dec-2010
Establish regular auditing of Yara visual identity on internal communications	A. Künnapuu	31-Dec-2011	31-Dec-2011	Started		17-Dec-2010

Trend analysis - residual risk

Brand Strategy and Identity Risk

	2009	2010	2011	2012	2013
Likelihood	4	3	3	2	
Consequence	2	2	2	2	
Risk score	8	6	6	4	



Comments