Operasjonell risikostyring i forsikringsbransjen:

en analyse av krav og praksis innenfor risikostyring og internkontroll

operational risk management in the insurance industry: an analysis of requirements and practices in relation to risk management and internal control

Gyda Hesla-Halvorsen og Oda Halvorsrud Holen

UNIVERSITETET FOR MILJØ- OG BIOVITENSKAP
Institutt for økonomi og ressursforvaltning
Masteroppgave 30 stp. vår 2012

Forord

Denne masteroppgaven er skrevet ved Institutt for økonomi og ressursforvaltning ved Handelshøgskolen UMB. Oppgaven er en avsluttende del av et 2-årig masterstudium i Økonomi og Administrasjon, og tilsvarer 30 studiepoeng.

Denne masteroppgaven skrives som et bidrag til en bredere forståelse av operasjonell risiko i forsikringsbransjen. Vi har hatt et fokus på å sammenstille nåværende og fremtidige krav som påvirker styring av operasjonell risiko. For å få til dette har vi tatt kontakt med to norske forsikringsselskaper og Finanstilsynet. Vi vil i den anledning takke kontaktpersonene og informantene i selskapene som har vært med på å hjelpe og bidra til oppgaven. Videre vil vi takke våre veiledere Ole Gjølberg og Jonas Gaudernack for god veiledning og oppfølging. Vi vil også takke Per Kristian Holte og Peter Schöfer for mange gode innspill og tilbakemeldinger. Ytterligere vil vi få takke Finanstilsynet som ga oss utdypende informasjon til oppgaven. Tilslutt vil vi få takke våre nære som har hjulpet oss gjennom denne prosessen.

”No risk, no money”

Universitetet for miljø- og biovitenskap
Ås, 05.06.2012

Gyda Hesla-Halvorsen

Oda Halvorsrud Holen

Sammendrag

Temaet for denne oppgaven er operasjonell risikostyring i forsikringsbransjen. På bakgrunn av gjeldende lovverk og beste praksis vurderer vi hvordan to forsikringsselskaper styrer operasjonelle risikoer. Vi vil også vurdere hvordan forsikringsselskapene har tatt hensyn til de fremtidige kravene ved operasjonell risikostyring, fra Solvens II- direktivet. Med det bransjespesifikke Solvens II- direktivet vil operasjonell risikostyring få en større betydning for risikostyring i forsikringsbransjen. Dette vil medføre at forsikringsbransjen i Norge vil måtte gjennomføre vesentlige endringer. Ett av kravene fra Solvens II- direktivet er at forsikringsbransjen må ha et helhetlig system for risikostyring. Systemet skal inneholde prosesser og rapporteringsprosedyrer som skal identifisere, måle, overvåke og styre ulike typer risikoer selskapet kan bli eksponert for. En av disse risikotypene er operasjonell risiko. I dag blir operasjonelle risikoer mer eller mindre inkludert i selskapenes risikostyring. Direktivet krever imidlertid en større synliggjøring av hvordan selskapene skal styre disse risikoene. Som et hjelpemiddel til risikostyringsprosessen har vi vurdert fire ulike rammeverk. Disse er vurdert opp mot tre indikatorer. Resultatet fra denne vurderingen viser i hvilken grad rammeverkene tilfredsstiller kravene til et helhetlig system for risikostyring.

Ved å intervjue nøkkelpersoner i to norske forsikringsselskaper har vi funnet ut hvordan styring av operasjonell risiko foregår i praksis, og hvor langt selskapene har kommet med å imøtekomme de kvalitative kravene fra Solvens II- direktivet. Basert på resultatene har vi identifisert likheter og ulikheter i selskapenes risikostyringsprosesser, herunder også forberedelsene for å innfri de kommende kravene. På mange måter styrer selskapene operasjonelle risikoer likt, men strukturen på risikostyringsprosessen skiller selskapene fra hverandre. I tillegg har selskapene kommet ulikt i utarbeidelsen med å imøtekomme kravene fra Solvens II- direktivet. For å gi en status på selskapenes styring av operasjonelle risikoer har vi gjort en modenhetsanalyse. Denne indikerer hvor godt selskapene styrer operasjonelle risikoer per i dag, og hvilke utfordringer de står overfor for å tilfredsstille de forventede fremtidige kravene.

Abstract

The topic of this study is operational risk management in the insurance industry. Based on the current legislation and best practice we will assess how two different insurance companies manage operational risks, and how the future requirements of operational risk management, based on the Solvency II- directive. The directive will increase the significance of operational risk for the insurance companies' risk management, which will result in major changes for the Norwegian insurance industry. One of the requirements is that the insurance companies need a holistic risk management system. This system should include processes and reporting procedures to help identify, measure, monitor and control the risks the companies may be exposed to. One example of this is operational risk.

Today operational risk is more or less included in risk management, but the directive requires a greater degree of visibility in how the companies should manage operational risks in their overall risk management process. As a tool for the risk management process we evaluated four different frameworks against three indicators. These indicators explain how well the frameworks comply with the requirements of an enterprise risk management system. By interviewing key persons in two Norwegians insurance companies we have explored the management of operational risk from a practical point of view, and have assessed how far the companies have come in their work to comply with the qualitative requirements of the Solvency II-directive. Throughout this survey we have elicited knowledge about how the two companies manage their risk processes and how they plan to comply with the Solvency II requirements.

Based on the results we have identified similarities and differences in companies' risk management processes, including preparations to meet the future requirements. In many ways companies manage operational risks equally, but the structure of the risk management process separates companies from one another. In addition, the companies have been different in preparing to meet the requirements of the Solvency II- directive. To provide a status of the companies' management of operational risks, we have made a maturity analysis. This indicates how well companies manage operational risks at present, and the challenges they face to meet the expected future requirements.

Innholdsfortegnelse

Forkortelser

ASL	=	Aksjeloven
ASAL	=	Allmennaksjeloven
CAS	=	Casualty Actuarial Society
CCO	=	Chief Compliance Officer
CEO	=	Chief Executive Officer
CFO	=	Chief Financial Officer
CG	=	Corporate Governance
COSO	=	Committee of Sponsoring Organization
CRO	=	Chief Risk Officer
EIOPA	=	European System of Financial Supervision
ERM	=	Enterprise Risk Management
FAL	=	Forsikringsavtaleloven
FERMA	=	Federation of European Risk Management Associations
FINANSAVL	=	Finansieringsvirksomhetsloven
FINANSTLL	=	Finanstilsynsloven
FORSVL	=	Forsikringsvirksomhetsloven
GRC	=	Governance, risk, compliance
ICAAP	=	Internal Capital Adequacy Assessment Process
ISO	=	International Organization for Standardization
MCR	=	Minstekapitalkrav
NUES	=	Norsk Utvalg for Eierstyring og Selskapsledelse
ORSA	=	Own Risk and Solvency Assessement
PWC	=	PriceWaterhouseCoopers
REVL	=	Revisorloven
RSKL	=	Regnskapsloven
RU	=	Revisjonsutvalg
SCR	=	Solvenskapitalkrav

Figuroversikt Sidetall

Tabelloversikt Sidetall

Diagramoversikt Sidetall

1 Operasjonell risikostyring i forsikringsbransjen

1.1 Innledning

Vi vil i denne oppgaven drøfte og analysere gjeldende og forventede fremtidige krav til styring av operasjonell risiko. Vi vil også vurdere hvordan gjeldende krav foregår i praksis. Styring av operasjonell risiko er en viktig del, men også et lite område av virksomhetens risikobilde. For å håndtere selskapets risikobilde er det viktig å ha gode prosesser rundt risikostyring og internkontroll.

Forsikringsbransjen må i dag forholde seg til strenge krav, lover og regler som skal sørge for at selskapene har god risikostyring og internkontroll. De siste års finanskriser har allikevel vist at styrer over hele verden har tatt for lett på denne oppgaven. På bakgrunn av finanskrisen har det kommet tydeligere frem at det eksisterer behov for solide rammeverk, slik at det er mulig å identifisere, evaluere og håndtere risiko på en god og effektiv måte. Som en konsekvens av finanskrisen ble Solvens II- direktivet introdusert for forsikringsbransjen[1]. Etter innføring av direktivet vil styring av operasjonell risiko ha en mer fremtredende rolle i selskapenes risikostyring og internkontroll. Dette betyr at fokuset på operasjonell risikostyring har økt etter at Solvens II- direktivet ble introdusert. Ettersom bestemmelsene av innholdet i Solvens II- direktivet er under utarbeidelse, finnes det per i dag ingen forskning på hvordan dette vil fungere i praksis.

For å analysere forsikringsbransjens praktisering av styring av operasjonell risiko har vi tatt kontakt med to norske forsikringsselskaper. Det ene selskapet har hovedfokus på skadeforsikring, mens det andre selskapet har hovedfokus på livsforsikring. Vi er ute etter å analysere hvordan disse selskapene praktiserer styring av operasjonell risiko på bakgrunn av gjeldende krav. Vi ønsker også å finne ut hvordan selskapene har forberedt seg på å imøtekomme kravene fra Solvens II- direktivet.

[1] Omnibus II- direktivet ble gitt ut 19. januar 2011 av Europakommisjonen, som et forslag om endringer til direktiv 2009/138/EF. *"Omnibus II- direktivet vil trolig innebære at fristen for å gjennomføre Solvens II-direktivet i nasjonalt regelverk blir 1. januar 2013, og at enkelte deler av regelverket vil tre i kraft i 2013, bl.a. direktivbestemmelser om godkjenning av interne modeller for beregning av solvenskapitalkravet".* En generell utsettelse av ikrafttredelsestidspunktet for sentrale deler av regelverket er satt til 1. januar 2014 (Innst. 192 S (2011–2012)).

1.2 Oppgavens formål

Vi vil i denne oppgaven kartlegge hvordan to norske forsikringsselskaper forholder seg til nåværende og kommende krav i sitt risikostyringsarbeid. Formålet med oppgaven er å få en nærmere innsikt i hvordan operasjonell risiko håndteres i forsikringsbransjen.
For å gjennomføre vår analyse vil vi intervjue nøkkelpersoner som har bred innsikt i bestemmelsene og prioriteringene vedrørende risikostyring og internkontroll i selskapene. Vår hensikt er ikke å sette de to selskapene opp mot hverandre, men vårt ønske er å kartlegge og identifisere likheter og ulikheter ved styring av operasjonell risiko i deres kjernevirksomhet.

Vi håper at oppgaven kan være til nytte for forsikringsselskaper i arbeidet med styring av operasjonelle risikoer. I tillegg håper vi at oppgaven vår kan være til nytte for andre som jobber med risikostyring og internkontroll. Vi håper at oppgaven kan være til inspirasjon og nytte for fremtidige studenter innenfor fagfeltet risikostyring og internkontroll. Vi har en forhåpning om at oppgaven kan øke forståelsen av viktigheten av operasjonell risiko i selskapers risikostyring.

1.3 Oppgavens avgrensning og oppbygging

Som nevnt er styring av operasjonell risiko er et lite område innenfor selskapers risikostyringsprosess. Som regel får andre risikokategorier som finansiell risiko, markedsrisiko og strategisk risiko et større fokus i risikostyringsarbeidet. Årsaken til dette kan være at disse risikoenes sannsynlighet og konsekvens er lettere å identifisere og kvantifisere. Før Solvens II- direktivet ble introdusert eksisterte det ingen direkte krav til styring av operasjonelle risikoer. Dette har påvirket vårt valg av tema til denne oppgaven.

For at innholdet i oppgaven ikke skal gå utover rammene for en masteroppgave har det blitt nødvendig å gjøre noen avgrensninger. De to forsikringsselskapene vi har hatt kontakt med har kontorer og driver virksomhet i utlandet. De må forholde seg til krav og regler i gjeldende land. Vi vil derfor kun fokusere på enhetene selskapene har i Norge. Vi har valgt å legge vekt på kjernevirksomheten i begge selskapene som er henholdsvis skade- og livsforsikring. Begge selskapene har konsesjon for skade- og livsforsikring, men vi vil i denne oppgaven kun fokusere på selskapets kjernevirksomhet. Selskapenes kjernevirksomhet utgjør morselskapet i konsernene. Selv om morselskapet har tilhørende datterselskaper velger vi kun å fokusere på risikostyringen i morselskapet. Hendelser som kan inntreffe, kan både ha positiv og negativ innvirkning på foretakets oppnåelse av mål. Dette er forklart med at hendelser med negativ innvirkning representerer risikoer, mens hendelser med positiv innvirkning

representerer muligheter (COSO 2004). Vi vil begrense denne oppgaven til å kun fokusere på hendelser som kan påvirke selskapet negativt. Vi har valgt å begrense gjeldende krav og beste praksis til det som er mest relevant i denne oppgaven. På grunn av oppgavens tidsrammer har vi valgt kun å ta kontakt med to forsikringsselskaper til vår analysedel.

Våre to problemstillinger i oppgaven er følgende:

1. ***Hvordan styrer to norske forsikringsselskaper operasjonelle risikoer i dag?***
2. ***Hvor langt har to forsikringsselskaper kommet med å imøtekomme de forventede fremtidige kravene fra Solvens II- direktivet?***

Vi har valgt å dele oppgaven inn i to deler, del A og del B. Del A inneholder krav og beste praksis innenfor risikostyring og internkontroll. Denne delen inneholder de overordene rammer for hvordan selskapene på en effektiv og hensiktsmessig måte skal gjennomføre risikostyring og internkontroll. Vi vil trekke frem *krav* fra ulike hold; grunnleggende krav (kapittel 2), bransjespesifikke krav (kapittel 3), kommende krav (kapittel 4) og krav fra Finanstilsynet (kapittel 5). I tillegg vil denne delen inneholde elementer fra *beste praksis*; som rammeverk for risikostyring (kapittel 6) og styring av operasjonell risiko i banksektoren (kapittel 7).

I del B vil vi legge frem sekundær- og primærdata som viser hvordan de to forsikringsselskapene praktiserer risikostyring og internkontroll. Herunder vil vi fokusere på hvordan selskapene styrer operasjonelle risikoer i dag. Del B vil inneholde: offentlig informasjon om selskap 1 og selskap 2 (kapittel 8), metode og dataanalyse (kapittel 9) og analyse av operasjonell risiko (kapittel 10). Oppsummering av del A og del B er i kapittel 11.

Del A) KRAV OG BESTE PRAKSIS

2 Krav til grunnleggende prinsipper for risikostyring og internkontroll

2.1 Innledning

Vi vil i dette kapittelet definere grunnleggende begreper og belyse hvilke krav som er gjeldende for norske selskaper innenfor risikostyring og internkontroll. Forsikringsbransjen må forholde seg til generelle prinsipper og lovverk i sitt arbeid med risikostyring. For å kunne bedre selskapenes styring av risikoer er det blant annet viktig å utdype styrets og ledelsens ansvar, på bakgrunn av lovgivning og anbefalinger. I tillegg har kontrollfunksjonene en sentral rolle i selskapet arbeid mot risikostyring. Avslutningsvis vil vi i dette kapittelet se på økonomiske teorier knyttet til forsikringsbransjen. Disse teoriene gir et innblikk i hvordan risikoer kan oppstå, som danner grunnlaget for risikostyring.

2.2 Sentrale begreper for risikostyring og internkontroll

I dette delkapittelet vil vi definere sentrale begreper som spiller en viktig rolle innenfor som risiko, risikostyring og internkontroll, Corporate Governance og operasjonell risiko. Disse begrepene har vi valgt å utdype fordi de representerer en viktig del i oppgaven. En god forståelse av hva disse begrepene innebærer vil gjøre det lettere å forstå kompleksiteten og elementene i risikostyringen. Selv om flere av begrepene vi har valgt å definere ikke har en felles definisjon har vi valgt ut de definisjonene vi mener er mest dekkende for oppgaven.

2.2.1 Risiko, risikostyring og internkontroll

Generelt defineres risiko i faglitteraturen som muligheten for at en hendelse kan oppstå og påvirke måloppnåelsen negativt. **Risiko** kan også defineres som *"en samling av alle interne og eksterne faktorer som kan påvirke virksomhetens evne til å nå målene eller oppfylle formålene"(*COSO 1992*).* Risiko kan identifiseres ved å stille enkle spørsmål. Eksempler på slike kan være:

- Hva kan gå galt?
- Hvilke muligheter kan gå tapt?
- Hvor stor er usikkerheten eller sannsynligheten for at hendelsen oppstår?

Dette betyr at risiko måles i konsekvens og sannsynlighet (Gaudernack 2011). Risikofaktoren skal vurderes til sannsynligheten for at en hendelse inntreffer, og den forventede konsekvensen.

Hovedessensen i **risikostyring**[2] og internkontroll er at styret skal fange opp vesentlige risikoer og deretter iverksette mottiltak, slik at det totale risikobildet blir akseptabelt for virksomhetens risikoappetitt (Gaudernack 2011). En slik prosess bør gjennomføres på en systematisk måte. Det finnes mange ulike definisjoner av begrepet risikostyring. Finanstilsynet definerer begrepet slik (Finanstilsynet 2009) :

> *Foretakets risikostyring er hva foretaket gjennom strategi, organisering, rutiner og forsvarlig drift gjør for å nå fastsatte mål og sikre sine og kundenes verdier, samt pålitelig rapportering og etterlevelse av lover og regler. Dette innebærer mer enn det som tradisjonelt har vært oppfattet som internkontroll.*

Når det henvises til definisjonen av **internkontroll** vises det ofte til det engelske begrepet "internal control". Denne oversettelsen samsvarer med hvordan Direktoratet for økonomistyring definerer internkontroll[3]:

> *Begrepet internkontroll er direkte oversatt fra det engelske begrepet "internal control", men sistnevnte omfatter langt mer av styringsaspektet enn hva som på norsk ofte snevert forstås som interne kontrolltiltak. Skal vi forstå begrepet "internkontroll" må vi se sammenhengen mellom mål, risiko, styring og interne kontrolltiltak.*

Dette betyr at internkontroll går ut på hvilke valg virksomheten gjør for å sikre sine egne verdier og samtidig sikre en forsvarlig drift av virksomheten. Internkontroll defineres i videste forstand som en prosess, iscenesatt og gjennomført av foretakets styre, ledelse og ansatte.

Den utformes for å gi rimelig sikkerhet vedrørende måloppnåelse innen følgende områder (COSO 1992):

- Målrettet og effektiv drift
- Pålitelig ekstern regnskapsrapportering
- Overholdelse av gjeldende lover og regler

[2] Når det snakkes om *risikostyring og internkontroll* menes regler, metoder, prosedyrer og kontrollsystemer som virksomheter benytter seg av for å kunne ha kontroll over den finansielle situasjonen. Risikostyring og helhetlig risikostyring er to definisjoner som brukes om hverandre. Vi velger å tolke disse definisjonene med samme innhold men med ulik bredde. Innholdet i definisjonen av *helhetlig risikostyring* innebærer en bredere tilnærming til risikostyring på tvers av organisasjonen, fra topp til bunn.

[3] Direktorat for økonomistyring het tidligere Senter for Statlig økonomistyring. Rapport 4/2009 pkt. 2.1.1.

Internkontroll defineres som de tiltak selskapet gjennomfører for å sikre at de når sine mål på en forsvarlig måte.

2.2.2 Corporate Governance

Corporate Governance (CG) defineres ofte på norsk som ”eierstyring og selskapsledelse” (NUES 2012). Det engelske begrepet er mer utfyllende enn det norske, og det er grunnen til at vi bruker det engelske begrepet videre i oppgaven. CG ser i hovedsak på forholdet mellom styret, eierne og ledelsen. OECD definerer CG som (OECD principles of corporate governance 1999):

> *Et system der bedriftshandlingen er styrt og kontrollert i virksomheten. CG strukturen spesifiserer fordelingen av rettigheter og ansvar mellom de ulike aktørene i selskapet som f.eks. styret, ledere, aksjonærer og andre interessenter. CG strukturen spesifiserer også hvilke regler og prosedyrer som skal følges når bedriftsrelaterte beslutninger skal tas. Ved å gjøre dette er strukturen satt på forhånd, og den beskriver hvordan man skal nå og bruke målene for overvåking og kontroll av prestasjoner.*

God eierstyring og selskapsledelse vil over tid styrke tilliten til selskapene og bidra til størst mulig verdiskapning, noe som er ønskelig for både aksjeeiere, ansatte og andre interessenter.

2.2.3 Operasjonell risiko

Operasjonell risiko har den samme definisjonen i Solvens II- direktivet som i Basel II-direktivet (direktiv 2006/48/EF), som er følgende (direktiv 2009/138/EF punkt 27:36):

> *Med operasjonell risiko menes risiko for tap som følge av utilstrekkelige eller sviktende interne prosesser og systemer, feil begått av ansatt eller eksterne hendelser.*

Definisjonen inneholder juridisk risiko. Omdømmerisiko og risiko i forbindelse med strategiske beslutninger må vurderes særskilt (direktiv 2009/138/EF). Denne definisjonen benytter også Finanstilsynet i sitt tilsynsarbeid (Finanstilsynet 2012 (2)). Definisjonen har en forholdsvis generell og vid tilnærming. Hva som skal defineres som svikt i interne prosesser og systemer, menneskelig svikt, eksterne hendelser eller juridisk risiko er det opp til hvert enkelt foretak å definere.

Operasjonell risiko er et risikoområde med fokus på prosess og mennesker, som berører alle virksomheter uavhengig av bransje, stillingsnivå eller hvor man er geografisk plassert. Hvordan man velger å fokusere på operasjonell risiko som en del av selskapets risikobilde er individuelt fra selskap til selskap og bransje til bransje. Men fra Solvens II

kravene vil det med stor sannsynlighet bli utarbeidet et lovverk som skal imøtekomme disse kravene.

Operasjonell risiko handler om *å identifisere og forstå potensielle risikoer, forebygge tap, øke evnen til å oppdage signaler om at en risikabel og uønsket hendelse eller situasjon er i ferd med å inntreffe, samt å etablere tiltak for å håndtere potensiell konsekvenser av slike hendelser* (DNV 2009: 1). Operasjonell risiko kan oppstå i mange situasjoner, med uønskede hendelser. Slike uønskede hendelser kan skape uheldige ringvirkninger i et selskap. Det kan føre til store utslag som kan gi direkte økonomiske konsekvenser. Uønskede transaksjoner, effektivitetstap og tapte forretningsmuligheter er eksempler på slike økonomiske konsekvenser. Uønskede hendelser kan oppstå på grunn av utilstrekkelige og mangelfulle rutiner. Eksempler er slurv, feil, underslag, bedrageri, korrupsjon, brann og terrorangrep (DNV 2009: 1). Disse hendelsene har ulik tilnærming til risikoens sannsynlighet og konsekvens. Noen av hendelsene har høy sannsynlighet og lav konsekvens, mens andre har lav sannsynlighet og høy konsekvens. De har også ulik forutsigbarhet. Noen hendelser gir forventede tap mens andre gir uventede tap. Menneskelig feil ved svikt i rutiner, systemfeil og tap av nøkkelpersoner er eksempler på interne hendelser som gir forventede tap. Naturkatastrofer, brann og terror er eksempler på eksterne hendelser som kan gi uventede tap.

2.3 Krav og beste praksis for risikostyring og internkontroll

I eierstyring og selskapsledelse er god virksomhetsstyring basert på lovverk, anbefalinger og rammeverk av beste praksis, knyttet opp mot risikostyring og internkontroll. Videre vil vi presentere et utdrag av de mest relevante lover og regler innenfor aksjelovgivningen, regnskapsloven, og forskrift om risikostyring og internkontroll. I tillegg presenterer vi et utdrag fra den norske anbefalingen om eierstyring og selskapsledelse, som er en retningslinje for god risikostyring. Vi vil i kapittel 6 introdusere fire rammeverk av beste praksis for risikostyring.

2.3.1 Ansvarsfordelingen mellom styret og daglig leder i aksjelovgivningen

Med aksjelovgivningen menes lov om allmennaksjeselskaper 13. juni nr. 45 1997 (allmennaksjeloven[4]) og lov om aksjeselskaper 13. juni nr. 44 1997 (aksjeloven[5]). Disse to

[4] Allmennaksjeloven er heretter forkortet til asal.
[5] Aksjeloven er heretter forkortet til asl.

lovene er innholdsmessig forholdsvis like, men de gjelder for ulike typer selskaper[6]. Siden oppgaven tar for seg selskaper som er allmennaksjeselskaper, vil vi bruke asal videre i oppgaven. Allmennaksjeselskaper er etter asal § 1-1 2.ledd definert slik:

> *Med allmennaksjeselskap forstås ethvert selskap*
>
> 1. *hvor ikke noen av deltakerne har personlig ansvar for selskapets forpliktelser, udelt eller for deler som til sammen utgjør selskapets samlede forpliktelser, og*
> 2. *som i vedtektene er betegnet som allmennaksjeselskap, og*
> 3. *som er registrert som allmennaksjeselskap i Foretaksregisteret.*

Asal kapittel 6 regulerer blant annet hvilke oppgaver styret og ledelse står overfor. At det er styret som har ansvaret for risikostyring og internkontroll reguleres av asal §§ 6-12 og 6-13. Det følger av § 6-12 at styret har et forvaltningsansvar i virksomheten, og de skal sørge for en forsvarlig organisering av virksomheten. Styrets tilsynsansvar er regulert i § 6-13, og innebærer at det er styret som skal føre tilsyn med virksomheten og daglig ledelse. Paragraf 6-14 angir hva som er daglig leders rolle og oppgaver, og hvordan ledelsen skal forholde seg til styret. Hvilke plikter daglig ledelse har overfor styret fremkommer i § 6-15. I kapittel 3 reguleres krav om selskapskapital. Asal §§ 6-12 og 6-13 setter det overordnede ansvaret og roller for styret og daglig leder. Forskrift om risikostyring og internkontroll, og norsk anbefaling for eierstyring og selskapsledelse bygger sine prinsipper på disse lovbestemmelsene.

[6] Asal gjelder for selskaper som er definert som allmennaksjeselskaper, mens asl er gjeldende for selskaper som er aksjeselskaper.

Lovkrav	Innhold
§6-12 Forvaltningen av selskapet §6-13 Styrets tilsynsansvar	Planer og budsjetter Organisering Retningslinjer for virksomheten Retningslinjer for daglig leder Tilsyn med ledelse og virksomhet Betryggende kontroll
§3-4 Krav om forsvarlig EK §3-5 Handleplikt ved tap av EK	EK skal til enhver tid være forsvarlig ut fra risikoen ved og omfanget av virksomheten
§6-43 Revisjonsutvalgets oppgaver	Regnskapsrapporteringen Risikostyring og internkontroll Revisjon / internrevisjon
§6-14 Daglig ledelse §6-15 Daglig leders plikter overfor styret	Daglig ledelse Følge styrets føringer Holde styret orientert

Tabell 2.1: Oppsummering av aksjelovgivningen (Gaudernack 2012)

Tabell 2.1 gir en oppsummering av hvilke paragrafer i aksjelovgivningen som er relevante innenfor virksomhetens risikostyring og internkontroll. Figuren gir også en oversikt over hvilke paragrafer i asal som er sentrale mellom styret og daglig ledelse.

2.3.2 Forskrift om risikostyring og internkontroll

Formålet med forskrift om risikostyring og internkontroll av 22. september 2008 nr. 1080 (internkontrollforskriften[7]) er å bedre foretakenes risikostyring og internkontroll gjennom å utdype styrets og ledelsens ansvar (Finanstilsynet 2009). Internkontrollforskriften gjelder for foretak underlagt Finanstilsynets overvåkning. Dette omfatter blant annet finansinstitusjoner, verdipapirforetak og forsikringsformidlingsvirksomhet. Forskriften er en presisering og en utvidelse av kravene i aksjelovgivningen (Gaudernack 2009). Forskriftens **kapittel 1** § 2 inneholder en presisering av hvordan foretakene skal tilpasse seg prosessen rundt risikostyring og internkontroll etter art, omfang og kompleksiteten i foretakets virksomhet.

I internkontrollforskriften **kapittel 2** er styrets og daglig leders rolle vektlagt. I § 3 fremkommer det at det er styrets oppgave å påse at risikostyring og internkontroll er sikret i tilstrekkelig grad, og at prosessen har blitt gjennomført på en systematisk måte. I hovedsak har styret ansvaret for å trekke de store hovedlinjene i foretaket og fastsette prinsipper for

[7] Forskrift om risikostyring og internkontroll er heretter forkortet til internkontrollforskriften.

risikostyring og internkontroll, se § 3 nr. 1. Styret skal vurdere hvordan foretaket skal vektlegge forhold av betydning for å sikre forsvarlig drift. Videre er det viktig at styret påser at det blir gjennomført og etablert tiltak for å kunne korrigere eller redusere de svakheter som har blitt funnet (Finanstilsynet 2009 § 3). I § 3 nr. 5 står det at styret har også ansvaret for å påse at risikostyring og internkontroll blir etablert i samsvar med gjeldende lover og praksis. Det er imidlertid daglig leder som har det operative ansvaret for å etablere og utvikle systemer for risikostyring og internkontroll, se § 4. Dette må gjøres etter de retningslinjer og fullmakter som styret har gitt. Etter at kontrolltiltaket har blitt etablert er det daglig ledelse som har ansvaret for å gjennomføre, dokumentere og overvåke tiltakene. Daglig ledelse bør etablere et godt kontrollmiljø på alle nivåer i foretaket for å få til en god risikostyringsprosess (Finanstilsynet § 4). En slik rollefordeling er fornuftig og i tråd med god praksis. Denne rollefordelingen kan også anbefales for virksomheter som ikke er underlagt forskriften (Gaudernack 2009:6).

Kapittel 3 i internkontrollforskriften omhandler risikostyring og internkontroll[8]. Risikostyring blir i denne sammenheng sett på som hva foretaket gjør gjennom strategier, organisering, rutiner og forsvarlig drift for å kunne nå fastsatte mål (Finanstilsynet 2009 § 6). Internkontroll defineres som en prosess som er utført av styret, ledelsen og ansatte, hvor hensikten med prosessen er å oppnå større grad av sikkerhet rundt foretakets målsettinger (Finanstilsynet 2009 § 7).

Figur 2.1: Internkontrollprosessen

Figur 2.1 viser internkontrollprosessen. En slik prosess tar utgangspunkt i at styret og daglig ledelse først må identifisere og vurdere vesentlige risikoforhold innenfor alle områder i virksomheten. Deretter er det viktig å iverksette kontrolltiltak og kontinuerlig følge opp disse tiltakene. Daglig ledelse skal årlig rapportere til styret om vesentlige risikoeksponeringer i virksomheten, både når det gjelder på virksomhetsnivå og for virksomheten samlet, se § 8.

[8] Vi vil i kapittel 6 vise til fire rammeverk av beste praksis for risikostyring og internkontroll.

I denne årlige rapporteringen bør det også gis en status på hvordan internkontrollen har fungert. Etterlevelse og oppfølging av risikoer forutsetter at ledere på alle nivåer i organisasjonen gjennomfører og overvåker vedtatte kontrolltiltak innenfor sitt ansvarsområde. Risikostyring og internkontroll er en "løpende prosess" som modnes, endres og forbedres over tid.

2.3.3 Regnskapslovens behandling av årsberetning, risikostyring og regnskapsrapportering

I lov om årsregnskap m.v. 17. juli nr. 56 1998 (regnskapsloven) § 3-3a fremkommer det at årsrapporten må inneholde en beskrivelse av de mest sentrale risikoene og usikkerhetsfaktorene som virksomheten har stått overfor det siste året. Loven er gjeldende for alle selskaper som er regnskapspliktige i Norge. Det kan være aksjeselskaper, allmennaksjeselskaper, statsforetak og finansinstitusjoner. Årsregnskap og årsberetning skal utarbeides. Etter § 3-2 1.ledd skal årsregnskapet inneholde resultatregnskap, balanse, kontantstrømoppstilling og noteopplysninger.

Vi har sett på årsrapportene fra 2010 og 2011 til selskap 1 og selskap 2. Her har vi undersøkt hvordan selskapene gjennom årene har fokusert på risikostyring og internkontroll, Solvens II- direktivet, operasjonell risiko og ansvarsfordeling.

2.3.4 Norsk anbefaling for eierstyring og selskapsledelse

Norsk utvalg for eierstyring og selskapsledelse (NUES) har utarbeidet den norske anbefalingen om eierstyring og selskapsledelse (NUES 2010). Anbefalingen er forankret i aksje-, regnskap-, børs- og verdipapirlovgivningen. Den inneholder bestemmelser og veiledninger som til dels utdyper og går lengre enn lovgivningen. Formålet med anbefalingen er at selskaper som er notert på regulerte markeder skal ha god eierstyring og selskapsledelse. Anbefalingen skal bidra til å klargjøre rollefordelingen mellom aksjeeiere, styret og daglig ledelse utover det som følger av lovgivningen. Etterlevelse av anbefalingen skal skje på bakgrunn av et "følg eller forklar" prinsipp. Dette betyr at hvis selskapene ikke har fulgt anbefalingen så må de forklare hvorfor dette ikke har blitt gjort. Oslo Børs krever at alle selskaper som er notert på Oslo Børs eller Oslo Axess gir en samlet redegjørelse for selskapets eierstyring og selskapsledelse i årsrapporten. Dette i henhold til anbefalingens hovedpunkter.

Kapittel 1	• Eierstyring og selskapsledelse og styrets forpliktelser.
Kapittel 3	• Selskapets egenkapital.
Kapittel 9	• Styrets arbeid og styrets oppgaver.
Kapittel 10	• Krav styret står overfor innenfor risikostyring og internkontroll.

Tabell 2.2: En oversikt over relevante kapitler i NUES

Tabell 2.2 gir en oversikt over hvilke kapitler i NUES som er relevante innenfor risikostyring og internkontroll, samt hvilket ansvar styret har overfor denne prosessen.

NUES kapittel 1 inneholder en redegjørelse for eierstyring og selskapsledelse, og hvilke forpliktelser styret har i den sammenheng. Styret skal blant annet påse at selskapet har god eierstyring og selskapsledelse. Det bør blant annet bli gitt en samlet redegjørelse for dette i årsrapporten.

Av **kapittel 3** fremkommer det at selskapet bør ha en egenkapital som er tilpasset mål, strategier og risikoprofil. I asal er det dessuten bestemmelser som skal sikre at selskapene til enhver tid har en forsvarlig kapital.

Kapittel 9 i NUES tar for seg styrets arbeid og styrets oppgaver. Etter asal §§ 6-12 og 6-13 har styret det overordnede ansvaret for forvaltningen av selskapet, og for å føre tilsyn med den daglige ledelsen og selskapets virksomhet. Styret bør årlig lage en plan over sitt arbeide med særlig vekt på mål, strategier og en oversikt over hva som konkret skal gjennomføres.

I NUES **kapittel 10** blir kravene som styret står ovenfor spesifisert når det gjelder risikostyring og internkontroll. Styret skal påse at selskapet har god internkontroll og ha hensiktsmessige systemer for risikostyring. I selskaper hvor det er etablert en internrevisjon, bør styret og internrevisjonen sikre at styret kan motta rapporter regelmessig eller ved behov. Styret bør årlig foreta en gjennomgang av selskapets viktigste risikoområder og den interne kontroll. Det blir fremhevet at styret i årsrapporten bør gi en beskrivelse av hovedelementene i selskapets internkontroll og risikostyringssystemer knyttet opp mot den finansielle

rapporteringen. Det er viktig å presisere at anbefalingen ikke er en utvidelse av aksjelovens regler om tilsynsansvar, men en presisering av lovverket (Gaudernack 2009).

2.3.5 Oppsummering

I dette delkapittelet vil vi oppsummere krav og anbefalinger for styret og daglig leder. Oppsummeringen viser de kravene som stilles til styret og daglig leder i forbindelse med ansvarsfordelingen i risikostyringsprosessen.

Styret

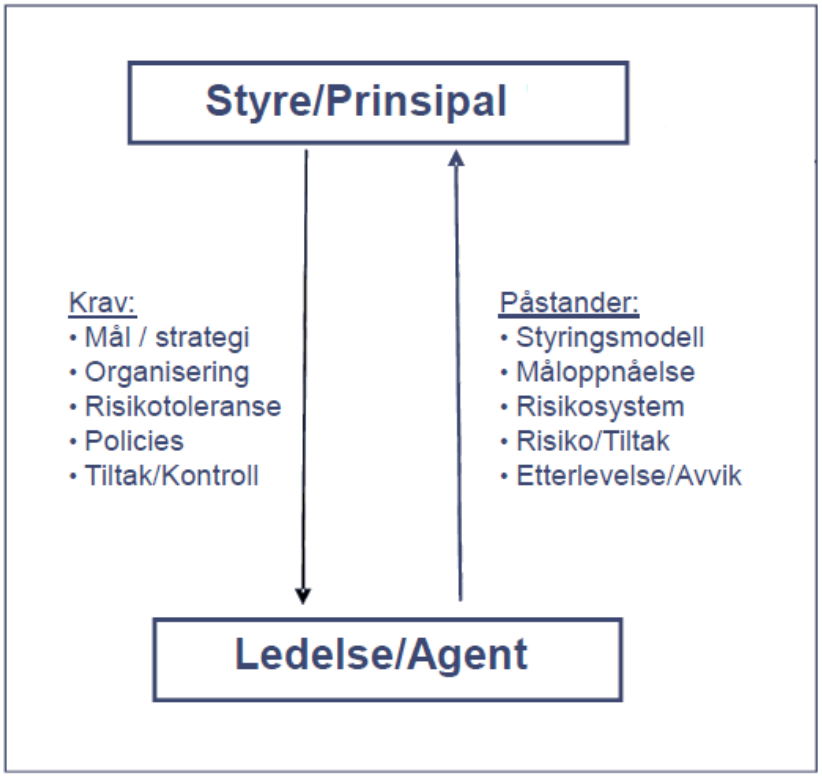
Styret har det overordnede ansvaret for virksomheten som er definert i allmennaksjeloven kapittel 6. I dette kapittelet blir det tydeliggjort at styret både har et forvaltningsansvar og et tilsynsansvar. Styrets overordnede ansvar kommer dessuten frem i internkontrollforskriften. Dette betyr at styret skal påse at selskapet har hensiktsmessige systemer for risikostyring og internkontroll. Styret bør på det overordnede plan fastsette mål, strategier og legge retningslinjene for selskapet. Som en del av styrets overordnede ansvar bør de fastsette hvilken risikoprofil selskapet skal ha, og hvilke risikorammer som er gjeldende. Styret bør videre etablere retningslinjer, og påse at risikostyring og internkontroll blir etablert i samsvar med lover og regler. De må påse at risikostyringen og internkontrollen blir gjennomført og kontrollert på en god måte.

Styrets arbeidsoppgaver og ansvarsfordelingen mellom styret og daglig leder, reguleres i NUES kapittel 9. Kapittel 10 dreier seg om styrets ansvar innenfor risikostyring og internkontroll.

Daglig leder

Hvilke plikter daglig ledelse har overfor styret fremkommer i allmennaksjeloven kapittel 6. Daglig leder skal etablere rutiner for risikostyring og internkontroll, etter at styret har kartlagt hvilke risikoer som selskapet bør fokusere på. Dette kommer frem av internkontrollforskriftens § 4. I følge internkontrollforskriften skal dessuten daglig leder påse at risikostyring og internkontrollprosessen blir dokumentert. Daglig leder skal gi styret relevant og tidsriktig informasjon som kan være av betydning for foretakets risikostyring og internkontroll, som for eksempel informasjon om potensielle risikoer. Samtidig har daglig leder ansvaret for løpende endringer i selskapets risikoer som er i samsvar med styrets

retningslinjer. Daglig leder skal påse at risikostyringen og internkontrollen blir gjennomført, kontrollert og overvåket på en god og forsvarlig måte.



Figur 2.2: Oversikt over ansvarsfordelingen mellom styret og daglig leder (Original hentet fra Gaudernack 2012)

Figur 2.2 gir en oversikt over ansvarsfordelingen mellom styret og daglig leder, og hvilke oppgaver styret har overfor daglig ledelse og motsatt.

2.4 Kontrollfunksjoner

I dette delkapittelet vil vi beskrive hvordan ansvarsfordelingen fungerer mellom kontrollfunksjonene i en virksomhet. Hver kontrollfunksjon i en virksomhet har ansvar for å følge opp sine områder i risikostyringsprosessen. De ulike kontrollfunksjonene vi vil fokusere på er compliance, internrevisjon og ekstern revisor. Disse funksjonene skal kontrollere ulike områder av risikostyringsprosessen i henhold til interne retningslinjer, lover og regler. I tillegg har vi valgt å ta med revisjonsutvalg som en del av kontrollfunksjonene, selv om revisjonsutvalget i utgangspunktet har en rådgivende funksjon for styret.

2.4.1 Revisjonsutvalg

Revisjonsutvalg (RU) skal være både et forberedende og et rådgivende arbeidsutvalg for styret (asal § 6-41), og sikre kvaliteten på selskapets finansielle rapportering. Reglene om RU trådte i kraft 1.juli 2009 (NOU 2010:1), og bør sees i sammenheng med finanskrisen som oppsto noen måneder tidligere. I følge asal må alle børsnoterte selskaper ha et RU (§ 6-41), og at foretak av allmenn interesse må opprette et RU. RU består som oftest av tre medlemmer, og RU- medlemmene velges av og blant styrets medlemmer, se § 6-42. Den økonomiske risikoen kan reduseres hvis en virksomhet har et velfungerende RU og samtidig har et effektivt internkontrollsystem. I følge Gaudernack (2009) skal RU fokusere på:

- Regnskapsrapportering og regnskapet
- Revisor og revisjonen
- Systemene for internkontroll og risikostyring

RU har også ansvaret for å følge opp at selskapets internrevisjon fungerer på en god måte. RU skal også ha løpende kontakt med ekstern revisor ved revisjonen av årsregnskapet. I § 6-43 fremkommer det dessuten at RU skal følge opp revisors uavhengighet. Etablering av RU vil være med på å påvirke hvordan styret og daglig ledelse arbeider med internkontroll og finansiell rapportering. RU skal forsikre seg om at selskapet har gode rutiner for risikostyring og internkontroll. Utvalget skal overvåke de etablerte systemene for risikostyring og internkontroll.

2.4.2 Compliance- funksjon

Compliance- funksjon er en uavhengig funksjon som har til hensikt å bidra til at virksomheten ikke pådrar seg offentlige sanksjoner, økonomiske tap eller tap av omdømme som følge av at virksomheten ikke etterlever lover, regler eller standarder (Gaudernack 2011). Funksjonen skal identifisere, vurdere, gi råd om, overvåke og rapportere om potensielle hendelser som kan påvirke compliance- risikoen. Den skal også rapportere om eventuelle brudd på lover, regler eller standarder. Compliance- risiko defineres som (Finanstilsynet 2012 (1)):

> *Risikoen for at institusjoner pådrar deg offentlige sanksjoner, økonomiske tap eller tap av omdømme som følge av at den ikke etterlever lover, regler og standarder.*

Dette betyr at en compliance- funksjon er en kontrollfunksjon som kun fokuserer på lover, regler og standarder. Compliance- funksjonen bør gi råd til styret og daglig leder om hvilke lover, regler og standarder som er relevante for virksomheten. Samtidig bør compliance-

funksjonen holde styret og daglig ledelse informert. Den skal vurdere hvilke mulige konsekvenser endringer i lovgivningen kan få for virksomheten.

Styret eller daglig leder bør fastsette retningslinjer for compliance, og forsikre seg om at retningslinjene for funksjonen blir kommunisert og forstått av organisasjonen. Ved behov eller ved for eksempel grove lovbrudd bør compliance- funksjonen rapportere direkte til styret. I Solvens II- direktivet kreves det at forsikringsselskaper skal opprette en compliance-funksjon.

2.4.3 Internrevisjon

Internrevisjon er en kontrollfunksjon som er uavhengig av daglig ledelse og administrasjonen. Av internkontrollforskriften § 9 fremkommer det at de fleste virksomheter bør ha internrevisjon. Videre i forskriften fremkommer det at en av oppgavene til internrevisor er å lage en rapport minst en gang i året. Den skal gi status på prosessen rundt risikostyring og internkontroll. Internrevisjonen eller internrevisor rapporterer direkte til styret. Det å ha en internrevisjon er særlig aktuelt i store og komplekse organisasjoner, men det er også anbefalt å ha en slik funksjon i mindre foretak (Gaudernack 2011). Internrevisjon blir ofte sett på som et ledd for å styrke internkontrollen eller som en del av foretakets internkontroll.

Internrevisjon er et eget fagfelt med egne standarder, metoder og etiske retningslinjer. Internrevisjon skal gjennomføres etter standarder[9], og en standard har i økende grad blitt sett på som profesjonens kvalitetsnorm. Standardene er en del av et overordnet rammeverk som inneholder faglige retningslinjer og beste praksis. For at en internrevisjon skal kunne utøve god internrevisjonsskikk er det viktig at internrevisor tar hensyn til objektivitet, uavhengighet og integritet. Det kreves av Solvens II- direktivet at forsikringsselskaper skal ha en internrevisjon.

2.4.4 Ekstern revisor

Revisors oppgaver er regulert i lov om revisjon og revisorer 15. januar nr. 2 1999 (revisorloven[10]). Revisors hovedoppgave er i følge Gaudernack (2011) å bekrefte at det er betryggende, men ikke absolutt, sikkerhet for fravær av vesentlige feil i regnskapet. Det er dessuten essensielt at revisjonen av årsregnskapet har blitt gjort i samsvar med bestemmelsene

[9] Standardene er en del av et overordnet rammeverk som inneholder alle IIAs faglige retningslinjer. Internrevisjonens rammeverk, The International Professional Practices Framework (IPPF), er laget for å gjøre hele spekteret av faglige retningslinjer og beste praksis lett tilgjengelig for internrevisorer.
[10] Heretter forkortet til revl.

i revl. Dette betyr at revisor blant annet skal vurdere om årsregnskapet er riktig, at bokføringene er gode og oversiktlige, og vurdere om det har blitt redegjort for foretaksstyring etter regnskapsloven. At foretaksstyringen har blitt redegjort er meget viktig innenfor risikostyring og internkontroll. I revl § 1-2 fremkommer det at revisor skal utøve sin virksomhet med integritet, objektivitet, og aktsomhet. Av revl § 2-3 fremkommer det at styret i selskapet hvert år skal ha et møte med revisor uten at daglig leder eller andre fra den daglige ledelsen er til stede. Dette er for å kunne drøfte regnskapsmessige forhold der revisor ser vesentlige svakheter og mangler ved vurderingene daglige ledelsen har gjort, og også av hensyn til revisors uavhengighet til den daglige ledelsen. Dette fremkommer også i NUES kapittel 15. God kommunikasjon mellom revisor og styret kan også føre til at risikoer i virksomheten blir oppdaget på et tidlig tidspunkt.

I følge NUES kapittel 15 kan det være nyttig både for styret og daglig leder at revisor møter på de styremøtene hvor årsrapporten skal behandles. På et slikt møte har revisor mulighet til å kommentere regnskapet og eventuelt trekke frem vesentlige endringer i selskapets regnskapsprinsipper. Videre i anbefalingen kommer det frem at revisor årlig bør legge frem en plan for RU hvor det spesifiseres hvordan revisoren ønsker å gjennomføre sitt revisjonsarbeide. Revisor og RU bør møtes minst en gang årlig for at de sammen kan gjennomgå selskapets rutiner og systemer for internkontroll. Der kan de diskutere svakheter i virksomheten og potensielle risikoer. På et slikt møte får RU et innblikk i revisorens arbeidsmetode.

2.5 Økonomiske teorier knyttet til forsikringsbransjen

Forsikringsbransjen er som andre bransjer utsatt for risikoeksponeringer. Som et teoretisk grunnlag for å forstå hvordan risikoeksponeringer kan inntreffe, har vi valgt tre teorier som skisserer problemer som kan oppstå og utgjøre en risiko. Teoriene vi vil gå inn på er prinsipal-agent teorien, asymmetrisk informasjon og moralsk hasard. Hvordan selskapene på mest mulig måte kan håndtere disse risikoene, vil bli belyst gjennom fire rammeverk for risikostyring i kapittel 6.

2.5.1 Prinsipal – agent teori

Agentteori forklarer hvordan kontrakter utformes i en kontekst med asymmetrisk eller ulik informasjon (Busch 1994). Teorien tar opp forholdet mellom en agent og prinsipal. Prinsipalen er den som delegerer arbeidsoppgaver til agenten, og agenten er den som skal

utføre arbeidet (Eisenhardt 1989). Teorien definerer forholden mellom prinsipal og agent som en kontrakt mellom partene der insentiver skal strukturere arbeidet til agenten i riktig retning (Kosnik 1987). Prinsipalen og agenten har ulike mål ved avtaleinngåelse, som regel er prinsipalen avhengig av handlingene til agenten. Ettersom prinsipal og agent har ulike mål kan det oppstå en målkonflikt som gjør at agenten handler i skjul mot egne mål, som kan straffe prinsipalen. En slik situasjon finner vi ofte igjen i et selskap. Det kan for eksempel forekomme mellom styret (prinsipal) og daglig leder (agent). Hvis agenten velger å skjule både informasjon og handlinger for prinsipalen, som kan være vanskelig å avsløre grunnet asymmetrisk informasjon, vil det oppstå agentkostnader. For å hindre slik atferd må prinsipalen iverksette kontrolltiltak som forhindrer dette. Agentteorien blir ofte kritisert for det negative menneskesynet som implisitt viser at det finnes opportunistisk adferd mellom mennesker. Moralsk hasard og ugunstig utvalg i en kontekst preget av asymmetrisk informasjon observeres også i agentteori.

2.5.2 Asymmetrisk informasjon – konsekvens av ulik informasjon

Asymmetrisk informasjon er ett mulig problem når for eksempel en forsikringsavtale skal inngås. Asymmetrisk informasjon oppstår når aktører handler med hverandre, og har ulik tilgang på informasjon om forhold som har betydning for handelen. Dette betyr at agenten har mer informasjon enn prinsipalen, og prinsipalen har dermed ufullstendig informasjon. Asymmetrisk informasjon deles gjerne opp i to deler, som følge av skjult informasjon og skjulte handlinger (NOU 1997:6). En forsikringstaker (agent) kan ha egenskaper eller informasjon om seg selv som er vanskelig for andre å kjenne til. Når forsikringskontrakten inngås kan agenten ha mer informasjon enn prinsipalen kan spore. Et eksempel på dette kan være helse. Dette er tilbakeholdelse av informasjon og kalles *antiseleksjon* eller *ugunstig utvalg*[11].

Ugunstig utvalg tar utgangspunktet i at prinsipalen ikke kan se hvilken hensikt agenten har ved kontraktinngåelse. En mulig negativ konsekvens av ugunstig utvalg er det såkalte ”lemon” problemet hvor de dårlige aktørene i markedet ødelegger for de gode. Et eksempel er at dårlige forsikringstakere fører til at forsikringsselskapet setter premien på forsikring opp (Hendrikse 2003).

[11] Begrepet er på engelsk adverse selection.

2.5.3 Moralsk hasard – konsekvens av skjult handling

For agenten er det mulig å oppnå et godt resultat til tross for dårlig handling. *Moralsk hasard*[12] innebærer at agenten har informasjon om sine egne handlinger som prinsipalen ikke har mulighet til å observere, altså skjulte handlinger. Moralsk hasard går ut på at for eksempel agenten kan foreta handlinger som er fordelaktige for ham selv, men ikke for bedriften, og som ikke kan observeres av prinsipalen. Moralsk hasard er et problem som kan oppstå når to parter inngår en avtale. Problemet oppstår når den ene har uærlige hensikter ved avtaleinngåelse, og for agenten er det mulig å oppnå gode resultater selv med dårlig utført handling. Utfallet vil være et resultat av agentens handlinger, men også av en rekke tilfeldige faktorer som er utenfor agentens kontroll (Hendrikse 2003). Moralsk hasard oppstår når den ene av partene inngår en avtale for å imøtekomme egne mål mot den andres interesse og til vedkommendes kostnad. Moralsk hasard handler altså om atferd, og man tenker ofte på situasjoner hvor prinsipalen har vanskeligheter for å observere hva agenten gjør. En slik situasjon oppstår lettere i en sak som angår skadeforsikring enn ved livsforsikring. Grunnen til dette kan være at den personen som har tegnet en skadeforsikring vil opptre mindre forsiktig siden han har en sikkerhet i at forsikringen dekker utgiftene ved uforsiktig oppførsel.

3 Regulering av forsikringsbransjen

3.1 Innledning

Forsikringsselskaper må følge egne lover og forskrifter som skal regulere drift av forsikringsvirksomhet på en hensiktsmessig måte. I Norge er det er vanlig at forsikringsselskapene fokuserer sin kjernevirksomhet på skadeforsikring eller livsforsikring. Innenfor disse områdene er det igjen ulike typer forsikringsklasser. I dette kapittelet vil vi legge frem hvordan forsikringsbransjen reguleres[13]. Avslutningsvis vil vi legge frem hvilke risikotyper forsikringsbransjen må forholde seg til i risikostyringsprosessen. Hvordan selskapene på mest mulig måte kan håndtere disse risikoene vil bli belyst gjennom fire rammeverk for risikostyring i kapittel 6.

[12] Begrepet er på engelsk moral hazard.
[13] Vi vil trekke frem de lover og forskrifter som vi mener er mest relevante til denne oppgaven.

3.1.1 Forsikringsavtale

Forsikringsavtale er en *"økonomisk avtale som går ut på at en part overlater en risiko, som for eksempel brann, dødsfall, innbrudd, ulykker, til en annen mot å betale et statistisk utregnet vederlag"* (Bokmålsordboka 2012 (1)). Med andre ord handler forsikring om *"å avlaste risiko for økonomisk tap knyttet til uventede hendelser"* (Holthe, Kjesbu og Sellæg 2011: 19). En forsikringsavtale innebærer dermed at et forsikringsselskap sammen med en kunde fordeler risikoen for uønskede hendelser. Uønskede hendelser kan være alt fra skade eller tap av ting til personforsikringer. Forsikringsselskapet tar risiko for negative hendelser som kan inntreffe i fremtiden mot løpende betaling av en beregnet premie. Premieberegning for livsforsikringsselskaper er regulert etter konkrete regler, mens skadeforsikringsselskaper har mer generelle bestemmelser om premiefastsettingen (Holthe, Kjesbu og Sellæg 2011: 29-30).

3.2 Krav til forsikringsselskaper

Lov om forsikringsselskaper, pensjonsforetak og deres virksomhet mv. 10. juni nr. 44 2005 (forsikringsvirksomhetsloven[14]) gjelder for (…) *"forsikringsselskaper, pensjonsforetak og virksomhet som drives av slike foretak"*, se § 1-1. Forsvl regulerer hvordan virksomheter av denne art skal utøve virksomhet, hvordan de skal organiseres, og hvilke krav til soliditet som er gjeldende (Jusleksikon 2012). I forsvl § 1-2 fremkommer det at det er kun forsikringsselskaper og pensjonskasser som kan drive forsikringsvirksomhet. Videre i forsvl § 1-3 skilles det mellom ulike forsikringsbransjer. Det er vanlig å skille mellom personforsikring og skadeforsikring. For å drive forsikringsvirksomhet er det nødvendig med tillatelse eller konsesjon, og dette fremkommer av forsvl. kapittel 2. Av Finanstilsynets konsesjonsregister er det registrert 43 skadeforsikringsselskaper og 12 livsforsikringsselskaper. Forskrift om inndeling i forsikringsklasser som grunnlag for konsesjonstildeling av 18. september 1995 nr 797 gir grunnlag for konsesjonstildeling for skade- og livsforsikring. De ulike forsikringsklassene innenfor skade- og livsforsikring kommer vi tilbake til.

I følge Holthe, Kjesbu og Sellæg (2011:19) *"er de viktigste elementene i et forsikringsselskaps forretningsdrift polistegning/- prising (underwriting) og forvaltning av midler og skadebehandling, i tillegg til øvrige administrative forhold"*. Det første elementet består av polistegning/- prising som består av å finne riktige kunder og å sette en riktig pris på

[14] Forsikringsvirksomhetsloven er heretter forkortet til forsvl.

kontrakten. Når et forsikringsselskap mener at de kan overta en risiko, gjør de dette mot et vederlag kalt *forsikringspremie*. Størrelsen på forsikringspremien vil normalt bli beregnet ut i fra statistiske metoder, og skal i utgangspunktet dekke de utgiftene forsikringsselskapet har hvis en risiko skulle inntreffe (Bull 2008: 24).

Ved forvaltning av midler er det viktig at forsikringsselskaper har en god soliditet slik at de har mulighet til å bære store tap[15]. For å sikre at forsikringsselskapene har god kapitaldekning fører Finanstilsynet tilsyn etter gjeldende krav. Det stilles et minimumskrav til kapitaldekning vedrørende den risikoen selskapet påtar seg, og den skal utgjøre minst 8 % etter forsvl § 6-3. Finanstilsynet fører ofte tilsyn av forsikringsselskaper, mer om deres tilsynsarbeid står beskrevet i kapittel 5.

I lov om forsikringsavtaler 16.juni nr. 69 1989 (forsikringsavtaleloven[16]) kapittel 3 reguleres rammene for en forsikringsavtale.

3.3 Skadeforsikringsselskaper

Forsikringsavtaleloven § 1-1 regulerer avtaler for skadeforsikring:

> *Med skadeforsikring menes forsikring mot skade på eller tap av ting, rettigheter eller andre fordeler, forsikring mot erstatningsansvar eller kostnader, og annen forsikring som ikke er personforsikring.*

Skadeforsikring deles inn i ulike produkttyper for privatpersoner og for selskaper. Forsikringsobjekter for privatpersoner kan være knyttet til bil, båt, hus, hytte etc. For selskaper vil typiske forsikringsobjekter være eiendom, kjøretøy, fabrikker eller installasjoner. I tillegg omfatter skadeforsikring personskader i arbeidsforhold eller ulykkes- og helseforsikringer. *"Personforsikringer kan tegnes av både liv og skadeselskaper, men skadeselskapene kan kun tegne risikoforsikringer av høyst ett års varighet"* (Holthe, Kjesbu og Sellæg 2011: 28).

[15] Solvens II- direktivet er et solvensregelverk som stiller strengere krav til selskapenes solvens.
[16] Heretter forkortet til fal.

De ulike forsikringsklassene kommer frem av forskrift om inndeling i forsikringsklasser som grunnlag for konsesjonstildeling 18. september nr 797 1995 § 2 er blant annet:

- Ulykke (personforsikring)
- Sykdom (personforsikring)
- Kjøretøy (jernbane, luftfartøy og havgående fartøy)
- Brann- og naturskader
- Annen skade på eiendom og eiendeler
- Kreditt og kausjon
- Diverse økonomiske tap

I tillegg er lov om finansieringsvirksomhet og finansinstitusjoner 10. juni 1988 nr. 40 (finansieringsvirksomhetsloven[17]) en relevant lov for skadeforsikringsselskaper vedrørende beregning av operasjonell risiko. Finansavl § 2-9a omhandler beregning av kapitalkrav, hvor paragrafens femte ledd gjelder beregning av operasjonell risiko: *"Beregningsgrunnlaget for operasjonell risiko skal fastsettes som: en andel av gjennomsnittlig inntekt (basis metode), en andel av inntekten innenfor de ulike forretningsområder multiplisert med en indikator på tapserfaring fastsatt av departementet (sjablongmetode) eller på bakgrunn av interne målemetoder for operasjonell risiko (avanserte metoder)"*.

3.4 Livsforsikringsselskaper

Forsikringsavtaleloven § 10- 1 definerer personforsikring følgende:

> *Med personforsikring menes livsforsikring, ulykkesforsikring og sykeforsikring. Forsikringen kan tegnes på forsikringstakerens eller på en eller flere andre personers liv eller helse.*

Fal. kapittel 10 gjelder også for *"(…) andre avtaler om personforsikring, herunder forholdet mellom pensjonskasser og -fonds og medlemmene, så langt de passer"*. Hensikten med å tegne livsforsikringer er å dekke inntektsbortfall for en person i fremtiden, som i hovedsak omfatter pensjonsforsikringer, uføredekninger, etterlattepensjoner og andre produkter som gir utbetaling ved død (Holthe, Kjesbu og Sellæg 2011: 19).

[17] Finansieringsvirksomhetsloven er heretter forkortet til finansavl.

De ulike forsikringsklassene er definert i forskrift om inndeling i forsikringsklasser som grunnlag for konsesjonstildeling 18. september nr 797 1995 § 1:

1. Alminnelig livsforsikring og tilleggsforsikring
2. Ekteskaps- og fødselsforsikring
3. Livsforsikring med investeringsvalg
4. Langsiktig ulykkes- og sykeforsikring
5. Forvaltning av midlene i pensjonskasser og andre pensjonsinnretninger
6. Kapitaliseringsprodukter

Forsikringsklassene gjelder både kollektive og individuelle forsikringer. Klassen alminnelig lovforsikring og tilleggsforsikring omfatter blant annet; kollektiv eller individuell kapitalforsikring med unntak for uføredekning, og kollektiv eller individuell livrente- og pensjonsforsikring med unntak for uføredekning. Klassene ekteskaps- og fødselsforsikring, og langsiktig ulykkes- og sykeforsikring er eksempler på individuelle forsikringer. Eksempler på kollektiver forsikringer er forvaltning av midlene i pensjonskasser og andre pensjonsinnretninger, og kapitaliseringsprodukter.

3.5 Risikokategorier i forsikringsbransjen

Forsikringsselskapene er en del av Norges finansinstitusjoner (Norges Bank 2012 (1)). En av deres oppgaver er å bidra til en bedre håndtering av risiko i landets økonomi. Som en del av risikohåndteringen er risikokartlegging og hvordan risikoene skal forebygges en viktig faktor (Norges Bank 2004: 35). For å kartlegge hvilke risikoer et selskap står overfor er det hensiktsmessig å dele risikoene inn i risikokategorier. Risikokategorier for finansinstitusjonene er: markedsrisiko, kredittrisiko, likviditetsrisiko, operasjonell risiko, juridisk risiko og systemrisiko. I tillegg til disse kommer bransjespesifikke risikoer som det må tas hensyn til. I forsikringsbransjen er risikokategorien forsikringsrisiko et eksempel på dette. Det er individuelt hvordan hvert forsikringsselskap velger å fokusere på de ulike risikokategorier.

Vi vil trekke frem de risikokategoriene som er typisk for hva forsikringsbransjen operer med. Gjensidige forsikring har valgt ut følgende fire risikokategorier (Gjensidige 2012)[18]:

- Finansiell risiko
- Operasjonell risiko
- Forsikringsrisiko
- Strategisk risiko

[18] Vi har valgt å bruke Gjensidiges risikotyper som eksempel. Hvordan Gjensidige har definert risikokategorier kom tydelig frem på selskapets hjemmeside, og derfor valgte vi å bruke disse.

Finansiell risiko er knyttet til selskapets kapitalforvaltning og aktivaallokering, og kan deles inn i tre risikogrupper (NOU 2008: 20, 6.1.4):

- Markedsrisiko
- Kredittrisiko
- Likviditetsrisiko

Markedsrisiko er en type risiko som omfatter tap knyttet til endringer i markedspriser, som renter, valutakurser, varepriser eller egenkapitalverdier (Norges Bank 2004: 34). Forsikringsselskaper gjør finansielle investeringer, som kan bestå av rentebærende plasseringer, eiendom, aksjer, og strategiske og finansielle eierposter i tilknyttede selskaper (Gjensidige 2012).

Kredittrisiko er en risikotype som oppstår når en motpart misligholder sine forpliktelser og ikke betaler innen forfall. Risikoen oppstår når kunden påfører en tredjemann en skade etter forsikringsavtalen er inngått, men før premien er innbetalt (NOU 2008: 20).

Likviditetsrisiko er en risikotype som oppstår når man ikke klarer sine betalingsforpliktelser ved forfall, eller selge eiendeler til en nedsatt pris for å innfri forpliktelsene.

Operasjonell risiko er allerede definert i kapittel 2.2.3. Operasjonell risiko er en sammensatt risikokategori som omfatter juridisk risiko og renommérisiko (Norges Bank 2004: 34). *Renommérisiko* er en risikotype som er knyttet til en hendelse som kan skade virksomhetens omdømme eller rykte. Dette er en risiko som kan skade driften av forsikringsvirksomheten i fremtiden. *Juridisk risiko* er en risikotype som oppstår når lover og regler ikke overholdes. Konsekvensene kan være at en (…) *"kontrakt ikke kan gjennomføres som planlagt, eller at pant ikke kan realiseres som forutsatt"*.

Forsikringsrisiko er en risikotype som knytter seg til (…) *"de premier forsikringsselskapet har krevd for å påta seg forsikringsforpliktelser ikke overstiger de erstatningsutbetalinger som påløper i forbindelse med forsikringskontraktene"* (NOU 2008: 20). Dette kan være forårsaket av flere ting, for eksempel naturkatastrofer som krever store erstatningsutbetalinger eller skader hvor erstatningens størrelse kan være større enn beregnet. Forsikringsrisiko kan oppstå allerede ved inngåelse av forsikringskontrakten, ved en feilberegning av premien. Dette er ofte resultat av en operasjonell feil.

Strategisk risiko er en risikotype knyttet til virksomhetens strategiske mål. I følge Gjensidige defineres strategisk risiko som *"konsernets strategi, holdt opp mot resultater,*

markeds- og konkurransemessige forandringer og endringer i rammebetingelsene" (Gjensidige 2012). De faktorene som er identifisert som kritiske, som har stor strategisk trussel overvåkes særskilt. For å styre denne type risiko benytter Gjensidige seg av konkurrent- og markedsovervåking, og produktutvikling og planprosesser. Å ha størst markedsandeler til sin kjernevirksomhet kan være et strategisk mål, men da er det viktig med slike analyser.

4 Kommende krav: Solvens II- direktivet

4.1 Innledning

Solvens II- direktivet (Europaparlamentets - og rådsdirektiv 2009/138/EF) ble vedtatt 25. november 2009, og er et nytt soliditetsregelverk for forsikrings- og gjenforsikringsselskaper i Europa. Solvens II er en fortsettelse av Solvens I- direktivet. Solvens I- direktivet fokuserte på å revidere og oppdatere det daværende solvensregimet i EU, mens Solvens II- direktivet vil ha et betydeligere bredere omfang. Solvens II- direktivet baserer seg på forslag fremmet av Europakommisjonen for Rådet og Parlamentet 10. juli 2007. Solvens II- direktivet baserer seg på 14 gjeldende direktiver innenfor forsikringsområdet, og er nå blitt slått sammen til ett direktiv som omfatter i overkant av 300 artikler. Ettersom regelverket bygger på fullharmonisering betyr det at implementeringen skjer uten lovendringer i EØS- området (Finanstilsynet 2012 (6)). Et av de viktigste målene i Solvens II- direktivet er å etablere et soliditetssystem som vil gi forsikringsselskaper insentiver til å måle og styre risikoene på en bedre måte (Ronkainen, Koskinen og Berglund 2007). Solvens II- direktivet skal tre i kraft fra 1. januar 2013, men det er forventet at det kommer en utsettelse av ikrafttredelsestidspunktet for regelverket til 1. januar 2014 (Innst. 192 S (2011–2012)). Dette er en prosess som skaper usikkerhet for når hvilke sentrale deler av Solvens II- rammeverket faktisk skal etterleves.

Vi vil i dette kapittelet gi en innføring av hvordan direktivet er bygd opp, og hvilke utfordringer ved implementering av et system for risikostyring gir. Vi vil trekke fram det vi mener er relevant å gjengi fra Solvens II- direktivet til denne oppgavens innhold og omfang. Vi vil også legge frem lovforslag til endringer av relevante lover fra forsikringsvirksomhetsloven og finansieringsvirksomhetsloven. Norsk høringsnotat om gjennomføring av Solvens II- direktivet ligger ett tall foran artikkeloversettelsene fra den

originale utgaven av direktivet. Altså er eksempelvis artikkel 44 i norske høringer referert som artikkel 43 i det originale rammeverket. Vi har valgt å bruke de norske referansene til artiklene videre i oppgaven.

4.2 Oppbygging av Solvens II- direktivet

Strukturen til det nye solvensregelverket bygger på en 3 – pilarstruktur. 3- pilar strukturen i Solvens II- direktivet er tilsvarende i Basel II- regelverket (direktiv 2006/48/EF), som gjelder for kredittinstitusjoner og verdipapirforetak (Prop. 54 S (2011-2012): 6):

- Pilar 1 inneholder kvantitative bestemmelser for beregning av solvenskrav, herunder bestemmelser om verdivurdering av eiendeler og forsikringstekniske avsetninger.
- Pilar 2 inneholder kvalitative bestemmelser for risikostyring og internkontroll, tilsynsmessig overvåkning og kontroll, samt nærmere hjemler for tilsynsmyndighetene for å fastsette høyere solvenskrav for enkeltinstitusjoner.
- Pilar 3 består bl.a. av regler om opplysningsplikt overfor offentligheten og rapporteringsplikt overfor tilsynsmyndighetene.

Figur 4.1: Oppsummering av de tre pilarene i Solvens II- direktivet (Skjævestad 2010)

Figur 4.1 viser en oversikt over hvordan Solvens II- direktivet er bygd opp. Sammen skal pilarene i direktivet skape verdiskapning til virksomhetens interessenter. Bedre styringsprosesser og strengere kapitalkrav skal gjøre forsikrings- og gjenforsikringsselskaper bedre rustet til å takle risikoer som oppstår. Videre vil vi gå inn på hvilke krav som fremkommer fra de ulike pilarene. Vi vil legge frem de sentrale kravene i de tre pilarene, men

med hovedfokus på pilar 2. Vår oppgave har hovedfokus på de kvalitative utfordringene fra direktivet.

4.2.1 Pilar 1

Fra Finanstilsynets høringsnotat om gjennomføring av Solvens II står kravene fra Pilar 1 beskrevet som følgende (Finanstilsynet 2011: 8):

> *Under Solvens II omfatter pilar 1 regler for verdivurdering av eiendeler, forsikringstekniske avsetninger og forpliktelser utover de forsikringstekniske avsetninger. Videre faller regler for beregning og klassifisering av solvenskapital samt beregning av de to kapitalkravene (solvenskapitalkravet (SCR) og minstekapitalkravet (MCR)) inn under pilar 1.*

Videre velger vi å trekke frem bestemmelsene vedrørende kapitalkrav. Kapitalkravene skal erstatte gjeldende europeiske solvenskrav, hvor bestemmelsene kommer fra Solvens I-direktivet. Endringene i det nye soliditetsregelverket inneholder to typer kapitalkrav, SCR (solvenskapitalkravet) og MCR (minstekapitalkravet). Hensikten med de nye kapitalkravene er *"(…) å sikre at institusjonene har evne til å bære uventede tap på sine investeringer"* (NOU 2011: 1, 10.3.1). Et kapitalkrav er kravet til forsvarlig kapitaldekning. Det knytter seg til størrelsen på forvaltningskapitalen i selskapet (NOU 2008: 20). Norges bank definerer kapitaldekning som *"(…) et forholdstall som sier noe om soliditeten til finansinstitusjoner og verdipapirforetak. Det er spesielle regler for hvordan kapitaldekningen skal beregnes"* (Norges Bank 2012). I forsikringsvirksomhetsloven § 6-3 defineres krav til kapitaldekning, *"(…) et forsikringsselskap skal ha en kapitaldekning som til enhver tid utgjør minst 8 prosent av selskapets aktiva og selskapets forpliktelser utenfor balansen, beregnet etter prinsipper for risikoveiing"*. Soliditet er et uttrykk for selskapets evne til å tåle tap. Har selskapet høy egenkapitalprosent, har de god soliditet. Krav til solvensmarginalkrav er gitt i forsvl § 6-4, hvor *"(…) et forsikringsselskap skal til enhver tid ha en kapital som er tilstrekkelig til å dekke solvensmarginen for selskapets samlede virksomhet"*.

Beregning av solvenskapitalkravet skal utføres minst en gang per år, mens beregning av minstekapital skal utføres minst hvert kvartal. Ved vesentlige endringer i selskapets risikoprofil skal kapitalkrav beregnes på nytt. I artikkel 100 til 127 i Solvens II- direktivet står bestemmelser om beregning av solvenskapitalkravet.

Artikkel 100 til 102 beskriver de overordnede bestemmelsene ved beregningen av solvenskapitalkravet. Beregning av *solvenskapital* skal beregnes enten ved bruk av *standardmetoden* eller *intern modell*, som følge av artikkel 100. Av artikkel 101 nr. 4 kreves det at solvenskapitalkravet skal dekke alle typer kvantifiserbar risiko, som forsikringsrisiko,

markedsrisiko, kredittrisiko og operasjonell risiko. Bestemmelsene ved bruk av *standardmetoden* står beskrevet i artikkel 103 til 112, mens beregning av kapitalkravet ved hjelp av en *intern modell* for hele eller deler av kapitalkravet står beskrevet i artikkel 112 til 127.

Hovedstrukturen for standardmetoden av beregning av solvenskapital står beskrevet i artikkel 103 og 104. Den skal minst omfatte risikomoduler som skadeforsikringsrisiko, livsforsikringsrisiko, helseforsikringsrisiko, markedsrisiko, motpartsrisiko og operasjonell risiko, samt en justering for risikoreduserende effekter av forsikringstekniske avsetninger og utsatt skatt (Finanstilsynet 2011: 32). I artikkel 104 nr 7 har selskapene mulighet til å erstatte parameterne, gitt i bruk av standardmetoden med spesifikke selskapsparametere i beregning av forsikringsrisiko.

Den interne modellen må anvendes i selskapets interne styring, og skal være en del av risikostyringssystemet og beslutningsprosesser (artikkel 120). Ved bruk av intern modell kreves det tillatelse av tilsynsmyndighetene. Det er flere krav som skal oppfylles før tillatelse blir gitt ved bruk av interne modeller (artikkel 112).

I artikkel 128 til 131 i Solvens II- direktivet står bestemmelser om beregning av minstekapitalkravet. *"Beregning av minstekapitalkravet gjøres ved en lineær funksjon av forsikringstekniske avsetninger, tegnede premier, udekket risiko, utsatt skatt og administrative kostnader, men med ulike funksjoner for livsforsikring og skadeforsikring"* (Finanstilsynet 2011: 35). Hvis ikke selskapet tilfredsstiller kravet om minstekapitaldekning vil selskapet miste sin konsesjon.

4.2.2 Pilar 2

Pilar 2 inneholder kvalitative krav til selskapets system for risikostyring og internkontroll og tilsynsmessig kontroll og overvåking (Finanstilsynet 2012 (7)). For å sikre hensiktsmessig styring er det viktig at selskapet har etablert et effektivt system for risikostyring og internkontroll. Ikke alle risikoer fanges opp av solvenskapitalkravet i pilar 1, og da kan de kun adresseres gjennom kvalitative krav. Det er viktig at et selskap vurderer sitt kapitalbehov til alle risikoer det kan eller er eksponert for.

Kravene for risikostyring og internkontroll følger av artiklene 41 til 50 i rammedirektivet. Vi vil videre fokusere på kravene til et system for risikostyring og internkontroll. Artikkel 41 gir en innføring i hvilke krav, på et generelt nivå, som kreves av et system for risikostyring. Det er styrets oppgave å vedta retningslinjer som skal vurderes

jevnlig. Systemet for risikostyring skal samsvare med selskapets art, kompleksitet og omfang. Rammeverket krever også at selskapet er integrert i et system for risikostyring og internkontroll. De skal ha etablert kontrollfunksjonene risikostyringsfunksjon, aktuarfunksjon, compliance- funksjon og en internrevisjon. Rammeverket åpner for at selskaper selv kan organisere disse kontrollfunksjonene som de vil. Et mindre selskap kan eksempelvis ha en person som har ansvar for flere kontrollfunksjoner, uten internrevisjon- da den skal være objektiv og uavhengig av operative funksjoner og øvrige kontrollfunksjoner. Hver kontrollfunksjon skal operere under oppsyn av, og rapportere til selskapets styre (Finanstilsynet 2011: 40-41). Av artikkel 42 legger rammeverket frem et "fit and proper" krav, som skal sikre kvalitet hos de ansatte.

Krav til systemet for risikostyring følger av artikkel 44. "*Systemet skal omfatte strategier, prosesser og rapporteringsprosedyrer som skal sikre at selskapet løpende kan identifisere, måle, overvåke, styre og rapportere de risikoene som selskapet er eller kan bli eksponert for og sammenhengen mellom disse* (Finanstilsynet 2011: 41). Risikoområdene som systemet skal dekke er forsikringstegning og avsetninger, balansestyring, investeringer, styring av likviditets- og konsentrasjonsrisiko, styring av operasjonell risiko[19], gjenforsikring og andre metoder for å avdekke risiko. Systemet skal integreres i selskapet, og være en del av selskapets organisasjonsstruktur og beslutningsprosess. Risikostyringsfunksjonen skal være strukturert slik at den understøtter gjennomføringen av systemet for risikostyring. Oppgaver knyttet til interne modeller, som krav om rapportering til styret, skal ligge under risikostyringsfunksjonen.

Av Solvens II- direktivet er det også krav om en aktuarfunksjon. Artikkel 48 regulerer aktuarfunksjonen og dens ansvarsområde. Aktuarfunksjonen skal ha ansvaret for de forsikringstekniske avsetningene, ved å samordne eller koordinere disse beregningene. Aktuarfunksjonen har til hensikt å beregne forsikringsrisiko, ved å sikre at metoder, underliggende modeller og forutsetninger som legges til grunn i beregningene er hensiktsmessige, fullstendige og av god kvalitet. Funksjonen må rapportere til styret om påliteligheten og tilstrekkeligheten av beregningene av de forsikringstekniske avsetningene. Aktuarenes oppgave er å bidra til effektiv gjennomføring av risikostyringssystemet, med vekt på utregning av risikomodeller. Risikomodellene ligger til grunn for beregning av kapitalkravene, både solvens- og minstekapitalkrav.

[19] Operasjonell risiko utdyper vi nærmere i kapittel 7.

Som følge av krav fra artikkel 46 må forsikrings- og gjenforsikringsselskaper ha et hensiktsmessig og effektivt system for internkontroll. Elementer som administrasjons- og regnskapsrutiner, rammeverk for internkontroll og hensiktsmessige rapporteringsrutiner på alle nivåer i organisasjonen må være integrert i systemet. Compliance- funksjon (artikkel 46 nr. 2) og internrevisjonsfunksjonen (artikkel 47) skal begge bidra til at internkontrollen er effektiv og hensiktsmessig. Compliance- funksjonen skal kontrollere etterlevelse av lover og forskrifter, konsekvenser av endringer i juridiske rammer, samt vurdering av risiko ved manglende overholdelse. Internrevisjonens kontrolloppgaver er å evaluere om systemet for risikostyring og internkontroll er hensiktsmessig. Endringer av systemet gjort av internrevisjonen skal rapporteres til styret. De må vurdere hvilke tiltak som skal gjennomføres. Internrevisjonen skal være objektiv og uavhengig fra driftsenhetene.

ORSA: Own Risk and Solvency Assessement

Av artikkel 45 følger krav om etablering av en prosess for egenvurdering av risiko og solvens, som en del av et system for risikostyring. Prosessen Own risk and solvency assessement (ORSA) skal inneholde retningslinjer for hvordan forsikringsselskapene skal vurdere solvens og risiko, samtidig som selskapet skal rapportere resultater fra vurderingen til tilsynsmyndigheter (Finanstilsynet). Det er viktig at selskapet vurderer samlet kapitalbehov med utgangspunkt i deres risikoprofil, vedtatt risikotoleranse og overordnet strategi. Selskapets egenvurdering skal være en integrert del i strategien, og skal kontinuerlig tas i betraktning i strategiske beslutninger. ORSA innebærer prosesser som gjør at egenvurderingen kan identifisere og vurdere risikoer, som kan oppstå på lang og kort sikt. ORSA prosessen er en viktig del av det integrerte systemet for risikostyring for forsikrings- og gjenforsikringsselskaper (Finanstilsynet 2011: 64-65). I Solvens II- direktivet står det ikke utfyllende og beskrivende hva ORSA prosessen skal inneholde, derfor har CEIOPS[20] utarbeidet en rettledende standard (CEIOPS 2008). CEIOPS definisjon av ORSA er følgende (CEIOPS 2008: 5 nr. 9):

> *ORSA er helheten av prosesser og prosedyrer som følges for å identifisere, vurdere, overvåke og administrere og rapportere risiko for å sikre at virksomhetens samlede soliditet er oppfylt til enhver tid.*

[20] Nå EIOPA.

ORSA skal representere selskapets oppfatning og forståelse av selskapets risiko, samlede behov av soliditet, og egne midler til å håndtere risiko. En risikobasert tilnærming krever at selskapet setter av midler som skal være i samsvar med de risikoene de kan bli utsatt for (CEIOPS 2008). Beregning av SCR skal gi et kapitalkrav som skal ta hensyn til alle målbare risikoer. Allikevel er det umulig å beregne inn alle vesentlige risikoer selskapet faktisk kan utsettes for. Derfor er det viktig å bruke andre beregningsmetoder enn standardformelen for å få en riktig tilnærming på selskapets risikobilde (CEIOPS 2008: nr. 12). Hensikten med ORSA er å sikre at selskapet har gode prosesser for vurdering og oppfølging av det samlede behovet for god soliditet. Det er viktig å forstå at ORSA er en del av selskapets risikostyringssystem. Skriftlige retningslinjer om ORSA kreves av direktivet, men innholdet er ikke bestemt. Følgende prinsipper bør selskapet ta hensyn til når det gjelder gjennomførelse av sin ORSA prosess (CEIOPS 2008: nr. 55)[21]:

1. *The ORSA is the responsibility of the undertaking and should be regularly reviewed and approved by the undertaking's administrative or management body.*
2. *The ORSA should encompass all material risks that may have an impact on the undertaking's ability to meet its obligations under insurance contracts.*
3. *The ORSA should be based on adequate measurement and assessment processes and form an integral part of the management process and decision making framework of the undertaking.*
4. *The ORSA should be forward-looking, taking into account the undertaking's business plans and projections.*
5. *The ORSA process and outcome should be appropriately evidenced and internally documented as well as independently assessed.*

Kravet om ORSA (artikkel 45) fra Solvens II- direktivet er motstykket til kravet om ICAAP (artikkel 23) fra Basel II- direktivet (2006/48/EF). ICAAP er en intern kapitalvurderingsprosess, hvor kapitalbehovet skal dekke risikoer som det ikke har tatt hensyn til i beregningen av minimumskravet under Pilar 1. Kapitalkravsforskriften regulerer regler vedrørende kapitalkrav for ”*banker, finansieringsforetak, holdingselskaper i finanskonsern, verdipapirforetak og forvaltningsselskaper for verdipapirfond som har tillatelse til å drive aktiv forvaltning*” (kapitalkravsforskriften § 1 -1). Foreløpig er det ikke utarbeidet et lovverk som skal regulere regler knyttet til kapitalkrav for forsikrings- og gjenforsikringsselskaper i Norge.

[21] Vi har valgt å ikke oversette disse prinsippene siden det ikke finnes noen norsk oversettelse per i dag.

Prinsipper for en god ICAAP- prosess (Jansrud 2009: 8):

1. *Alle banker må ha en ICAAP- prosess*
2. *ICAAP er bankens eget ansvar*
3. *ICAAP er styrets ansvar; prosessens design må være spesifisert og kapitalplanen dokumentert*
4. *ICAAP skal være en integrert del av styringsprosessene og beslutningskulturen i banken*
5. *ICAAP'en må revurderes regelmessig*
6. *ICAAP'en må være risikobasert*
7. *ICAAP'en må dekke alle relevante områder*
8. *ICAAP'en må være fremoverskuende*
9. *ICAAP må være basert på relevante måle- og vurderingsmetoder*
10. *ICAAP'en må lede til et fornuftig resultat*

På mange måter kan en si at Solvens II– direktivet er bygget på mange av de samme prinsippene som Basel II- direktivet. Det er mange likheter mellom kravene fra direktivene. Ettersom kravene fra Solvens II ikke skal være implementert før 1. januar 2014, kan en benytte seg av de erfaringene en har gjort ved implementering av Basel II. Dette gjelder særlig ved kvantifisering av operasjonell risiko. Hvordan har man tatt hensyn til dette kravet i for eksempel banker?

4.2.3 Pilar 3

Artiklene fra Solvens II- direktivet, som går under pilar 3, skal dekke krav om offentliggjøring av informasjon vedrørende selskapets solvens og finansielle stilling og rapportering til tilsynsmyndigheten. Artikkel 51 krever at selskaper årlig skal offentliggjøre en rapport om sin solvens og finansielle stilling. Rapporten skal blant annet inneholde opplysninger og beskrivelser av selskapets resultater, system for risikostyring og internkontroll, hver risikokategori, risikoeksponering, metoder for verdivurdering, forsikringstekniske avsetninger og styring av kapital (Finanstilsynet 2011: 62). I følge artikkel 54 skal vesentlige endringer som påvirker informasjonen selskapet har offentliggjort oppdateres jevnlig.

Av artikkel 35 nr 1 følger krav om rapportering av nødvendige opplysninger for tilsynsmål. Opplysninger som skal rapporteres skal inneholde opplysninger som er nødvendige for å (Prop. 54 S (2011-2012): 46):

a) *Vurdere foretakenes styringssystemer, deres virksomhet, prinsippene som benyttes for vurdering av solvens, bestående risikoer og risikostyringssystemer samt deres kapitalstruktur, kapitalbehov og kapitalforvaltning.*
b) *Treffe enhver hensiktsmessig beslutning som følger av utøvelsen av deres rett og plikt til å føre tilsyn.*

4.3 Endring av lovverk tilpasset Solvens II- direktivet

I Finanstilsynets høringsnotat om gjennomføring av Solvens II (2011) legges det ved forslag til endringer av ny lov som følge av Solvens II- direktivet. Forslaget til lov om endring omfavner forsikringsvirksomhetsloven (forsvl) og finansieringsvirksomhetsloven (finansvl). I høringen legges det frem forslag til endringer i kapittel 6 i forsvl. Videre lovbestemmelser i dette delkapittelet er forslag til en revidert utgave av forsikringsvirksomhetsloven, tilpasset Solvens II- direktivet.

Endringer vedrørende kapitalkrav for operasjonell risiko vil bli beskrevet i forsvl §§ 6-10 og 6-11. Ny lov om solvenskapitalkrav vil bli lovfestet i forsvl § 6-10:

> *Solvenskapitalkravet skal beregnes slik at alle kvantifiserbare risikoer for tap som et forsikringsselskap er eksponert for tas i betraktning, herunder risiko knyttet til forsikringer som forventes overtatt i løpet av de neste 12 måneder. Beregningen skal minst dekke: forsikringsrisiko, markedsrisiko, kredittrisiko og operasjonell risiko.*

En utdypelse av beregningsmetode for solvenskapitalkravet kommer frem i forsvl § 6-10 2. ledd, hvor standardmetoden eller intern modell er to typer som kan benyttes, disse står henholdsvis forklart i forsvl §§ 6-11 og 6-12. I § 6-10 (1) kommer det frem at alle kvantifiserbare risikoer skal inngå som en del av beregningen i solvenskapitalkravet. De kvantifiserbare risikoene som skal vurderes i løpet av de neste 12 måneder, er forsikringsrisiko, markedsrisiko, kredittrisiko og markedsrisiko. Disse bestemmelsene bygger på artikkel 101.

I følge § 6-11 1.ledd skal beregning av *standardmetoden* basere seg på risikomoduler som minst omfatter skadeforsikringsrisiko, livsforsikringsrisiko, helseforsikringsrisiko, markedsrisiko, motpartsrisiko og operasjonell risiko (Finanstilsynet 2011: 112-113). Bruk av *intern modell* i beregning av solvenskapitalkravet må i følge forsvl § 6-12 1.ledd gjennomføres etter tillatelse fra Finanstilsynet. Dette fremkommer også av artikkel 112 i Solvens II- direktivet.

Videre i forsvl § 6-12 3.ledd listes det opp de kravene som må oppfylles for at et forsikringsselskap skal kunne benytte seg av en intern modell (Finanstilsynet 2011: 128):

> *Finanstilsynet kan gi tillatelse til bruk av interne modeller bare dersom selskapets system for å identifisere, måle, overvåke og styre risiko er tilfredsstillende, og selskapet for øvrig oppfyller de krav til interne modeller som følger av forskrift. Tillatelse til bruk av intern modell som delvis dekker det samlede solvenskapitalkravet (partiell intern modell) forutsetter at følgende vilkår er oppfylt:*
> *a) selskapet godtgjør at det begrensede anvendelsesområdet for den interne modellen er tilstrekkelig begrunnet,*
> *b) den interne modellen er bedre i samsvar med foretakets risikoprofil og prinsippene i § 6-10 og*
> *c) den interne modellen er utformet slik at den kan kombineres med standardmetoden forberegning av det samlede solvenskapitalkravet.*

Lovbestemmelsen vedrørende minstekapitalkrav blir foreslått endret i § 6-13. 1. ledd i § 6-13 *"(…) fastslår at minstekapitalkravet skal dekke risikoen for tap av selskapets basiskapital"*. Videre i § 6-13 5. ledd står det beskrevet at departementet kan fastsette nærmere regler for beregning av minstekapitalkravet, som ved forskrift.

Lovbestemmelsene vedrørende selskapenes egenvurdering av risiko og solvens (ORSA) er regulert i § 6-14. § 6-14 2. ledd beskriver hvordan egenvurderingen er en intern prosess som skal sikre at selskapene gjør selvstendige vurderinger av risikoene. For å imøtekomme de identifiserte risikoene må selskapet ha tilstrekkelig kapital. Blant de identifiserte risikoene ligger risikokategorien operasjonell risiko.

Endringene i høringen som gjelder for finansieringsvirksomhetsloven § 2-9 som omhandler beregning av kapitalkrav. Her har det ikke blitt foreslått noen store endringer, bare noen justeringer. I finansvl § 2a-9 4. ledd vil ordlyden være *"I tilfeller hvor det ikke foretas konsolidering etter første eller tredje ledd, kan Finanstilsynet gi pålegg om avsetning av en kapitaldekningsreserve på 100 prosent av balanseført verdi"* (Finanstilsynet 2011: 139). Det foreslås at finansvl § 2a-9 5. ledd skal oppheves (beregning av kapitalkrav for operasjonell risiko), og at finansvl § 2a-9 får et nytt femte ledd som skal lyde *"Ved beregning av ansvarlig kapital på konsolidert basis skal det tas hensyn til hvor effektivt den ansvarlige kapitalen kan overføres og gjøres disponibel på tvers av foretakene i gruppen"* (Finanstilsynet 2011: 139).

4.4 Oppsummering

Forsikringsbransjen vil gjennomgå store endringer som følge av kravene fra Solvens II-direktivet. Endringene kommer til å kreve store ressurser i endringsfasen. Ikke bare må selskapene bruke mye tid på å sette seg inn i det nye regelverket, men de må også legge ned

mye arbeid for å kunne jobbe mot å implementere de kommende kravene. De største utfordringene ved å implementere de kommende kravene er blant annet å ha et integrert system for risikostyring, som skal sørge for å kontrollere risikoene i hele virksomheten. Et IT-system som skal samordne alle avdelingers risikoer vil være utfordrende og kostbart. I tillegg vil selskapene bruke en del tid på å utarbeide sin ORSA prosess. Hvordan selskapene skal kvantifisere operasjonell risiko under solvenskapitalkravet kan også virke som en stor utfordring. For at forsikringsselskapene skal kunne tilpasse seg regelverket på en tilfredsstillende måte, må de ha en tett dialog med Finanstilsynet. Finanstilsynet blir bindeleddet mellom de internasjonale tilsynsmyndigheter og de norske forsikringsselskapene, ved gjennomføring av kravene og tilpasning til lovendringer. I kapittel 5 vil vi gjennomgå hvordan forsikringsselskaper må forholde seg til krav fra Finanstilsynet innenfor risikostyring i dag og i fremtiden, og hvilken påvirkningskraft internasjonale tilsynsmyndigheter har overfor norske forsikringsselskaper.

5 Krav fra tilsynsmyndigheter

5.1 Innledning

I dette kapittelet vil vi vise hvordan forsikringsselskaper må forholde seg til krav fra internasjonale og nasjonale tilsynsmyndigheter, innenfor risikostyring.
Finanstilsynet skal føre tilsyn med forsikringsselskaper og påse at de overholder lover og krav. Det internasjonale organet EIOPA skal igjen føre tilsyn med Finanstilsynet, slik at de påser at internasjonale retningslinjer og regler etterleves. I dag fører Finanstilsynet tilsyn med forsikringsselskaper på to måter, ved dokumentbasert tilsyn og stedlig tilsyn. Hensikten bak tilsynet er å sikre at forsikringsselskaper (…) *er solide og risikobevisste, og har god styring og kontroll* (Finanstilsynet 2012 (7)). For å få en dypere innsikt i hvordan Finanstilsynet fører tilsyn i dag og hvordan de planlegger å føre tilsyn etter de nye kravene fra Solvens II-direktivet, har vi intervjuet to personer fra Finanstilsynet som er sentrale i dette arbeidet. Ettersom Solvens II- direktivet er et EU direktiv vil vi også drøfte hvilken rolle internasjonale tilsynsmyndigheter har, deriblant EIOPA.

5.2 Nasjonale tilsynsmyndigheter

I dette delkapittelet vil vi belyse Finanstilsynets tilsynsarbeid i forsikringsselskaper, og hvordan de forbereder seg på å imøtekomme de fremtidige kravene fra Solvens II- direktivet.

Finanstilsynet[22]er en statlig etat som ligger under Finansdepartementet. Det lovmessige grunnlaget for Finanstilsynets arbeid er festet i lov om tilsyn med finansinstitusjoner mv. 6.desember nr. 1 1956 (finanstilsynsloven[23]). Finanstilsynet har i oppgave å føre tilsyn på ulike finansielle institusjoner som står listet i finanstll § 1, deriblant sparebanker, skadeforsikringsselskaper, livsforsikringsselskaper og finansieringsforetak. Hovedoppgavene til Finanstilsynet står oppnevnt i finanstll § 3 1. og 2. ledd:

> *Tilsynet skal se til at de institusjoner det har tilsyn med, virker på hensiktsmessig og betryggende måte i samsvar med lov og bestemmelser gitt i medhold av lov samt med den hensikt som ligger til grunn for institusjonens opprettelse, dens formål og vedtekter.*
>
> *Tilsynet skal granske regnskaper og andre oppgaver fra institusjonene og skal ellers gjøre de undersøkelser om deres stilling og virksomhet som tilsynet finner nødvendig. Institusjonen plikter når som helst å gi alle opplysninger som tilsynet måtte kreve og å la tilsynet få innsyn i og i tilfelle få utlevert til kontroll institusjonens protokoller, registrerte regnskapsopplysninger, regnskapsmateriale, bøker, dokumenter, datamaskiner eller annet teknisk hjelpemiddel og materiale som er tilgjengelig ved bruk av slikt hjelpemiddel samt beholdninger av enhver art.*

På mange måter kan man si at Finanstilsynet fungerer som en storebror for forsikringsselskapene. Finanstilsynets arbeid består av å se til at forsikringsselskapene følger gjeldende lover og regler. Hvis ikke forsikringsselskapene etterlever de kravene som er satt for å drive forsikringsvirksomhet, vil dette mest sannsynlig bli avdekket i tilsynsarbeidet. Hvis ikke forsikringsselskapene tilfredsstiller gjeldende krav risikerer de å miste sin konsesjon for å drive forsikringsvirksomhet.

Operasjonell risiko inngår i Finanstilsynets oppfølging av institusjonene både ved dokumentbasert tilsyn og stedlig tilsyn. Å få en innsikt i hvordan Finanstilsynet jobber for å sikre god styring og kontroll er et viktig ledd for å forstå sammenhengen i risikostyringsarbeidet. Dessuten vil metodikken mest sannsynlig være den samme når Solvens II- direktivet trer i kraft, hvor operasjonell risiko kommer til å bli mer vektlagt i tilsynsarbeidet også for forsikringsselskaper. For å få en dypere innsikt i hvordan tilsynet jobber og hva de krever av forsikringsselskapene har vi gjort et dybdeintervju av to

[22] Finanstilsynet het frem til 21.desember 2009 Kredittilsynet.
[23] Finanstilsynsloven er heretter forkortet til finanstll.

representanter fra Finanstilsynet. Dybdeintervjuet varte ca. 1 time og informantene fikk ikke intervjuguiden på forhånd. Intervjuguiden fra dette intervjuet finnes i vedlegg 2.

5.2.1 Dokumentbasert tilsyn

Ved dokumentbasert tilsyn gjennomgår Finanstilsynet innrapporterte dokumenter opp mot gjeldende lover og krav. Forsikringsselskapene skal rapportere inn informasjon etter standardiserte metoder. I tillegg kan Finanstilsynet kreve ad hoc rapportering. På Finanstilsynets nettsider ligger en liste over rapporter som alle forsikringsselskaper må innrapportere, store som små. Følgende liste fra Finanstilsynet (2012 (3)) viser gjeldende krav til fastrapportering:

- *FORT - Forsikringsselskapenes offentlige regnskaps- og tilsynsrapportering*
- *Kapitaldekning*
- *Resultat - nøkkeltall*
- *Aktuarrapport for livsforsikringsselskaper*
- *Aktuarrapport for skadeforsikringsselskaper*
- *Betydelige interne transaksjoner i finanskonsern*
- *Regnskaps- og tilsynsrapportering for sjøtrygdelag*
- *Stresstest*
- *Solvensmarginkrav og solvensmarginkapital*

Ved ad hoc rapportering kan Finanstilsynet stille konkrete spørsmål som forsikringsselskapene må rapportere tilbake på. Ad hoc rapportering kan særlig være aktuell når det eksempelvis oppstår uro i finansmarkedene, og det kan være nødvendig med oppdatert informasjon.

Når det gjelder hyppigheten av innrapporteringen forsikringsselskapene gjør er dette noe ulikt. Hvert kvartal må forsikringsselskapene rapportere inn FORT- analyse, nøkkeltall og stresstest. Særlig sistnevnte rapport sier noe om selskapets soliditet, som er et av de viktigste områdene Finanstilsynet fører tilsyn med. Aktuarrapportene innrapporteres bare en gang i året. Som en del av det dokumentbaserte tilsynet bruker tilsynet et early warnings- system (EW) basert på ulike risikoindikatorer. Systemet viser hvordan forsikringsselskapene etterlever gjeldende krav, hvor Finanstilsynet må gjøre en vurdering om det må iverksettes tiltak. Et eksempel på dette er at selskaper må overholde et kapitaldekningskrav på 8 % av risikovektede eiendeler. Det er egne grupper som overvåker og vurderer status på innsendte rapporter fra selskapene. Hvis early warnings- systemet fanger opp noe som det bør rettes oppmerksomhet på, vil Finanstilsynet ta kontakt med det aktuelle selskapet. Dette gjøres hvis

det for eksempel har blitt en forverring i soliditeten. For å følge opp dette kan Finanstilsynet gjøre et stedlig tilsyn. Hvert halvår utarbeider Finanstilsynet en tilstandsrapport, basert på dokumentbasert tilsyn.

5.2.2 Stedlig tilsyn

Når Finanstilsynet utfører stedlig tilsynsarbeid er det på bakgrunn av tre moduler; modul for markeds- og kredittrisiko, modul for forsikringsrisiko i skadeforsikring og modul for forsikringsrisiko i livsforsikring. Modulene består av en *"(…) veiledning for evaluering av institusjonens risikonivå og en veiledning for evaluering av institusjonens system for styring og kontroll av den aktuelle risikoen"* (Finanstilsynet 2012 (5)). Modulene er ment å dekke beste praksis for risikostyring og internkontroll som en rettesnor for hva Finanstilsynet forventer at selskapene skal etterleve. Tilsynet kan omfatte hele virksomheten eller de kan være fokusert på enkelte risikoområder. Når Finanstilsynet utfører stedlig tilsyn reiser de ut til utvalgte forsikringsselskaper. De store institusjonene blir fulgt opp jevnlig, mens de mindre institusjonene i større grad blir valgt ut på bakgrunn av EW- indikatorene. Når Finanstilsynet gjennomfører stedlig tilsyn henvender en seg til selskapets styre. Styret henviser tilsynet til de aktuelle lederne som har ansvaret for de områdene tilsynet vil utforske. I forkant av det stedlige tilsynet ber Finanstilsynet om å motta nærmere definert dokumentasjon. Dokumentasjonen er grunnlaget for gjennomgangen med selskapets administrasjon under det stedlige tilsynet og evalueringen av institusjonen. Det stedlige tilsynet avsluttes med en samtale med styrets leder. Tilsynet skriver en foreløpig rapport til styret, som er unntatt offentligheten. Basert på styrets tilsvar skriver tilsynet endelig rapport (merknader etter stedlig tilsyn). Denne endelige rapporten er ikke unntatt offentligheten, men enkelte avsnitt kan sladdes.

Det er per i dag ikke utarbeidet en egen tilsynsmodul for evaluering av forsikringsselskapenes styring av operasjonell risiko. Operasjonell risiko dekkes imidlertid gjennom delmodulene for evaluering av risikostyring og internkontroll i øvrige risikomoduler.

Når Finanstilsynet fører tilsyn av for eksempel banker bruker de *modul for operasjonell risiko* for å vurdere kvaliteten på risikostyringen og den operasjonelle risikoen i institusjonene. Under Solvens II- direktivet vil en slik modul mest sannsynlig være aktuell for forsikringsselskaper, ettersom selskapenes system for risikostyring blant annet skal inneholde

styring av operasjonell risiko (artikkel 44). Da vi intervjuet Finanstilsynet var vi ute etter å finne ut om man allikevel hadde noen metoder for rapportering av operasjonell risiko i dag, uavhengig av Solvens II kravene. I følge våre informanter er IKT- risiko en operasjonell risiko. I dag har Finanstilsynet en egen IKT- seksjon som skal påse at selskapene følger blant annet forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT- forskriften[24]) 21. mai 2003 nr. 630. IKT- forskriften gjelder for blant annet sparebanker, forsikringsselskaper og verdipapirforetak, se § 1. En av virkemidlene i tilsynet etter IKT-forskriften er hendelsesrapportering. IKT- seksjonen vurderer kvaliteten på det styringssystemet som er etablert, som tilsynet kan gjøre en nærmere undersøkelse ved for eksempel stedlig tilsyn. Krav om hendelsesrapportering fremkommer av IKT- forskriftens § 9, som omhandler krav til avviks- og endringshåndtering.

I intervjuet av informantene i Finanstilsynet var vi også ute etter å kartlegge hvordan de har forberedt seg på å sikre tilsyn av kravene fra Solvens II- direktivet. Vi var altså ute etter å finne ut hvordan Finanstilsynet har planlagt å føre tilsyn med de nye kravene for operasjonell risiko. Fortsatt er det mye usikkerhet rundt hvordan Finanstilsynet vil føre tilsyn etter kravene fra Solvens II- direktivet. Selskapenes ORSA, egenvurdering av selskapets system for risikostyring, vil muligens Finanstilsynet følge samme prosedyre som ved bankenes ICCAP, fra Basel II- direktivet. Det første året bankene utarbeidet ICAAP valgte Finanstilsynet å samle inn fra alle, og siden har de tatt inn ICAAP`en fra de 18 største bankene i Norge pluss et årlig utvalg blant de mindre bankene. På spørsmål om hva Finanstilsynet forventer av innhold til ORSA, svarer de at det er de fortsatt usikre på. Men de ser ikke for seg en standardisert mal som alle forsikringsselskaper skal følge. Det viktigste i selve ORSA-rapporten er at den inneholder den informasjonen Finanstilsynet trenger for å vurdere selskapets risikoprofil og kapitalbehov. Formelt skal regelverket være implementert innen 1. januar 2014, men tilsynet forventer at selskapene planlegger de prosessene som kreves av Solvens II- direktivet. I begynnelsen var det forventet at rammeverket skulle implementeres i 2013, og det har blitt diskutert om mulige overgangskrav. Et mulig overgangskrav kan være å samle inn forsikringsselskapenes foreløpige utkast til ORSA i løpet av 2013.

[24] Heretter omtalt som IKT- forskrift.

Kravet i artikkel 101 i Solvens II- direktivet omhandler krav til beregning av solvenskapitalkravet. Solvenskapitalkravet skal beregnes slik at det dekker alle typer kvantifiserbar risiko, hvor operasjonell risiko er en av kategoriene. Kvantifisering av operasjonell risiko kan by på utfordringer. Hvordan tallfester man risikoen for menneskelige svikt i systemer og prosesser eller eksterne hendelser som terrorangrep og naturkatastrofer? Hvordan Finanstilsynet skal føre tilsyn med om det er avsatt nok kapital til å dekke operasjonell risiko i solvenskapitalkravet, er et spørsmål vi var veldig nysgjerrige på. Men svaret vi fikk var kanskje ikke helt det vi forventet. Finanstilsynet har foreløpig ingen metodikk som skal regne ut en slik størrelse, og de syntes som oss at dette er en vanskelig oppgave. Finanstilsynet legger imidlertid til grunn at selskapene tar stilling til om deres system for risikostyring og internkontroll er av en slik kvalitet at den operasjonelle risikoen må antas å være høyere enn det som følger av det standardiserte kapitalkravet. Tilsynet er opptatt av at selskapene har prosesser for å korrigere og justere slike beregninger underveis i risikostyringsprosessen.

Til slutt spurte vi Finanstilsynet hva som ligger i god styring av operasjonell risiko. Dette er et spørsmål som våre informanter også synes har vært vanskelig å besvare. Informanter kommer allikevel med noen svar de mener kan være viktige faktorer til god styring av operasjonell risiko. Det første eksemplet er synliggjøring av operasjonell risiko i det daglige. Med dette mener våre informanter at operasjonell risiko ikke bare skal være et abstrakt begrep som står i selskapets retningslinjer. For å synliggjøre det er det viktig med gode prosesser, slik at menneskene som står overfor operasjonelle risikoer i det daglige har forståelse og verktøy for å håndtere disse. Videre mener våre informanter at det er viktig å ha en god kultur hvor det er lov til å si ifra hvis noen gjør feil, eller å si ifra hvis feil oppdages som kan utgjøre operasjonell risiko. En systematisk registrering av inntrufne hendelser vil ha en pedagogisk effekt og skjerpe fokus for å forbygge disse i fremtiden. I tillegg mener informantene at det er viktig med god forankring hos ledelsen. Dette betyr at hvis ikke ledelsen formidler viktigheten av å følge opp de rutiner som er satt, for å forhindre for eksempel operasjonell risiko, er det vanskelig å få resten av organisasjonen med på lasset. Våre informanter referer her til ”tone at the top”.

Alt i alt hersker det usikkerhet rundt hvordan kravene fra Solvens II- direktivet skal følges opp på en hensiktsmessig måte, og hvordan tilsynsarbeidet skal foregå. Dette er en

prosess som er under kontinuerlig utvikling og arbeidet med å tilpasse seg kravene fra Solvens II- direktivet har bare så vidt begynt. Tilsynet med operasjonell risiko vil i hovedsak gjøres gjennom de ulike delmodulene for evaluering av risikostyring og internkontroll, men det er naturlig å tro at tilsynet med operasjonell risiko også vil bygge på modul for styring av operasjonell risiko, som brukes i tilsynet med blant annet bankene. Derfor vil vi i neste delkapittel gjennomgå denne modulen.

5.2.3 Modul for operasjonell risiko

Finanstilsynet benytter seg av fem risikomoduler; markedsrisiko, likviditet, kredittrisiko, overordnet styring og kontroll, og operasjonell risiko, i sitt tilsynsarbeid i bank- og finanssektoren. Modul for operasjonell risiko brukes som et verktøy for å kartlegge og vurdere kvaliteten på risikostyringen og den operasjonelle risikoen i institusjonene (Finanstilsynet 2012 (2)). Modulen for operasjonell risiko er utviklet for bruk under stedlig tilsyn og som hjelpemiddel i vurderingen av blant annet bankenes egenvurdering av risikostyringen, altså deres ICAAP – prosess. Denne modulens innhold vil også kunne bli tilpasset for forsikringsselskaper, som en tilsynsmodul for kravene om en ORSA – prosess.

Modulen består av en veiledningsdel og en del som inneholder kontrollspørsmål. Kontrollspørsmålene inneholder spørsmål som er knyttet til selskapets risikostyringsprosess (basert på COSO 2004), oppfølging og kvalitetssikring av pilar-1 krav, registrering av tap og hendelser, og vurdering av tapshendelseskategoriene. Kontrollspørsmålene som brukes i vurdering av tapshendelseskategoriene er basert på kapitalkravforskriften § 44-2. I utgangspunktet er det de bankene som benytter AMA- metoden som skal vurdere disse kategoriene i beregning av operasjonell risiko. Men per i dag er det ingen banker som bruker denne metoden, men allikevel benytter Finanstilsynet seg av vurdering av tapshendelsekategoriene i sitt tilsynsarbeid. Banker som vurderer overgang til AMA- metoden vil måtte foreta en systematisk hendelsesrapportering for operasjonell risiko i en periode **før** en søker om AMA- godkjennelse.

Ettersom modul for operasjonell risiko kan bli gjort gjeldende for forsikringsbransjen, vil vi gå igjennom de syv tapshendelseskategoriene i kapittel 7.

5.3 Internasjonale tilsynsmyndigheter

I dette delkapittelet vil vi trekke frem internasjonale tilsynsmyndigheters betydning for norske forsikringsselskaper. I de siste årene har det skjedd omveltninger i de europeiske

tilsynsorganene. Som et svar på de finansielle problemene som påvirket Europa av finanskrisen 2008, valgte Europakommisjonen å gjøre noen grep som skulle bedre finansinstitusjonenes tilstand (Finanstilsynet 2012 (4)). November 2010 ble det vedtatt et nytt tilsynssystem, og i 2011 ble det implementert[25]. EIOPA er den nye tilsynsmyndigheten som skal føre tilsyn på forsikring og tjenestepensjon. EIOPAs formal er (EIOPA 2012 (1)):

> *EIOPA's core responsibilities are to support the stability of the financial system, transparency of markets and financial products as well as the protection of insurance policyholders, pension scheme members and beneficiaries.*

EIOPA har ansvaret for å utarbeide retningslinjer og standarder for å støtte implementeringen av det nye rammeverket (EIOPA 2012 (2)). Standardene EIOPA utgir kan både være teknisk bindende og retningslinjer som ikke nødvendigvis må gjennomføres (Høringsnotat 2011:4). EIOPAs overordnede ansvar er å beskytte forbrukerne og gjenreise tilliten i det finansielle systemet. Dette med tanke på den finansielle uroen som har vart de siste fire årene etter finanskrisen. De skal sikre høy, effektiv og konsistent regulering og tilsyn, ved å ta vare på alle interessentene. EIOPA jobber også for en større harmonisering i Europa ved helhetlig anvendelse av regler for finansinstitusjoner og markeder (EIOPA 2012 (3)).

I det totale bildet utgjør Solvens II- direktivet nivå 1- bestemmelser. EU- kommisjonen fastsetter gjennomføringsbestemmelser til direktivet, som forsikringsselskapene må etterleve. Gjennomføringsbestemmelsene gitt av EU- kommisjonen betegnes som nivå 2- bestemmelsene. Gjennomføringsbestemmelsene på nivå 2 kommer som forordning, og må inkorporeres i alle EU- medlemsland. Gjennomføring av bestemmelsene i norsk rett kan skje på to måter*; (…) enten som inkorporering i norsk rett ved at en lov eller forskriftsbestemmelse henviser til de aktuelle bestemmelser, eller som transformering ved at bestemmelsene omskrives til norsk lov eller forskrift* (Finanstilsynet 2011: 5). Slik vil Finanstilsynet gjøre kravene gjeldende:

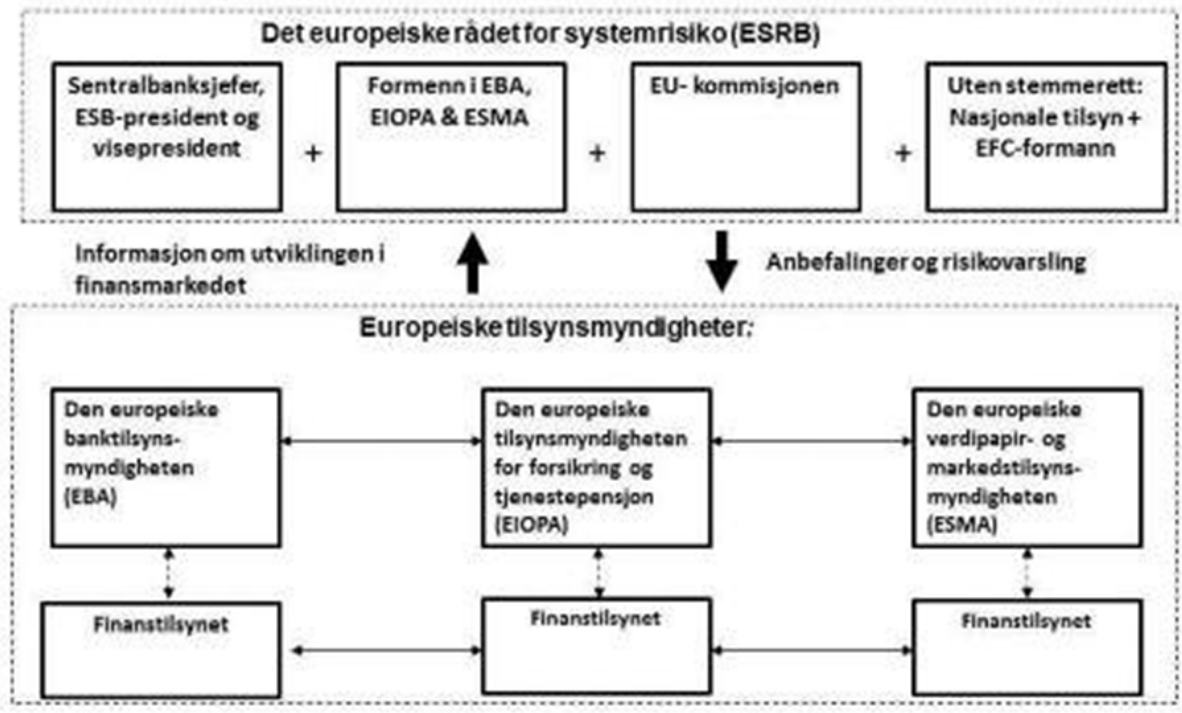
> *Finanstilsynet har lagt til grunn at gjennomføring av forordninger som hovedregel kun skal skje ved inkorporasjon. Det legges derfor til grunn at forordningen gjennomføres i norsk rett ved henvisning i forskrift. Det tas videre sikte på å utarbeide veiledninger som fremstiller regelverket i forordningen i en form som gjør dette lettere tilgjengelig for forsikringsselskapene og allmennheten, og som passer bedre med norsk regelverkstradisjon.*

[25] **EBA** (the European Banking Authority), **EIOPA** (the European Insurance and Occupational Pensions Authority) og **ESMA** (the *European Sales and Marketing Association)*, erstattet organene **CEBS** (the *Committee of European Banking Supervisors)*, **CEIOPS** *(*the *Committee of European Insurance and Occupational Pensions Supervisors)* og **CESR** (the *Committee of European Securities Regulators*) (Finanstilsynet 2011).

> *Det legges til grunn at slike veiledninger får samme rettskildemessige status som forvaltningspraksis og rundskriv.*

I vårt intervju av Finanstilsynet spurte vi om status på utviklingen av de nye lovbestemmelsene til Solvens II- direktivet. Det vi fikk til svar var tilnærmet likt det som allerede står i høringsnotatet om gjennomføring av Solvens II, at det mest sannsynlig vil bli en ny forskrift som vil utfylle lovbestemmelsene. Denne forskriften skal ikke inneholde gjennomføringsbestemmelser fra nivå 2.

Vi var også interessert i forholdet mellom EIOPA og Finanstilsynet i vårt intervju med to representanter fra Finanstilsynet. Informantene svarte at EIOPA hadde en tilsynsrolle på Finanstilsynet. Ettersom hvert enkelt land har ulik tilnærming til hvordan lover skal skrives, hvor noen skriver mye og andre lite, skal EIOPA se til at bestemmelsene gjennomføres på en riktig måte. Finanstilsynet poengterer at de har liten påvirkningsmakt angående retningslinjene og standardene som utarbeides i EIOPA. Finanstilsynet som et nasjonalt tilsynsorgan har ikke stemmerett til å være med å bestemme innholdet i standardene.



Figur 5.1: Den nye strukturen for finanstilsyn i EU (Finanstilsynet 2012 (4))

Figur 5.1 viser forholdet mellom norske og internasjonale tilsynsmyndigheter. De internasjonale tilsynsmyndighetene EIOPA, EBA og ESMA har kontakt med Finanstilsynet

for å sjekke at de overholder europeiske retningslinjer som eksempelvis Basel II og Solvens II. Over de internasjonale tilsynsmyndighetene ligger blant annet EU- kommisjonen, som har det overordnede ansvaret for gjennomføringsbestemmelsene til blant annet Solvens II-direktivet. Det europeiske rådet for systemrisiko (ESRB) har et overordnet ansvar for å overvåke systemrisiko i Europa.

De endringene som er gjort i de internasjonale tilsynsorganene får en konsekvens for blant annet forsikringsselskapene. Særlig nivå 3- bestemmelsene vil inneholde standarder og retningslinjer som påvirker driften i dag. Hensikten er å gjøre forsikringsselskapene bedre rustet ved dårlige tider, men dette gir konsekvenser krever ressurser av selskapene. Nivå 2-bestemmelsene får også en konsekvens for forsikringsselskapene, da blant annet nye forskrifter må overholdes. Foreløpig har ikke bestemmelsene blitt inkorporert i norsk lov, men kravene fra Solvens II- direktivet setter rammer for nivå 1- bestemmelsene.

5.3.1 Standard utgitt av CEIOPS

I oktober 2009 utga CEIOPS et veiledende dokument til bestemmelsene i Solvens II-direktivet (CEIOPS 2009). I dette dokumentet beskrives det blant annet hvordan forsikringsselskapene kan tilpasse seg bestemmelsen vedrørende styring av operasjonelle risikoer (artikkel 44). Styret, ledelsen og kontrollorganene bør godkjenne, overvåke og gjennomgå selskapets system for styring av operasjonelle risikoer. Et slikt system bør omfatte (CEIOPS 2009: 34-37):

- En bred definisjon av operasjonell risiko.
- Effektive prosesser som skal identifisere, vurdere, håndtere, overvåke og rapportere de operasjonelle risikoene selskapet er eller kan bli utsatt for.
- Risikostyringsprosessen bør være i samsvar med selskapets art, omfang og kompleksitet.

For at selskapet skal kunne definere de operasjonelle risikoene foreslår CEIOPS at det bør opprettes et hendelsesregister. Et hendelsesregister skal inneholde selskapets hendelser og nesten- hendelser. Hendelsene skal være kategorisert på en hensiktsmessig måte. Et slikt register vil hjelpe selskapene med å få en oversikt over hvilke hendelser selskapet er utsatt for. Slik vil det være enklere å utarbeide tiltak hvis hendelsene inntreffer i fremtiden. Det foreslås også at det kan være behov for et varslingssystem for risikoer. Videre presiseres det at en hensiktsmessig styring av operasjonell risikoer må være integrert i selskapets risikostyringsprosess.

6 Rammeverk for risikostyring

6.1 Innledning

I dette kapittelet vil vi ha en todelt struktur. I første del vil vi vise hvordan fire risikostyringsprosesser fra fire rammeverk[26] kan gjennomføres. I andre del vil vi vurdere innholdet i risikostyringsprosessene opp mot GRC (Governance, risk og Compliance) og sammenligne rammeverkene. Til slutt i kapittelet vil vi legge frem forskning knyttet til helhetlig risikostyring.

Styring av operasjonell risiko er et område innenfor selskapets risikostyring, og rammeverkene vi presenterer kan benyttes som et hjelpemiddel i styringsprosessen. Artikkel 44 i Solvens II- direktivet (2009/138/EF) krever et system for helhetlig risikostyring. Derfor er det viktig å vurdere beste praksis opp mot kommende krav i risikostyringsarbeidet. Det er imidlertid viktig å påpeke at rammeverkene gir oss et bilde av hvordan en risikostyringsprosess teoretisk *kan* utføres.

Rammeverkene vi har valgt å legge frem for risikostyring er[27]:

- *Helhetlig risikostyring – et integrert rammeverk* (COSO 2004)
- *Risikostyring, prinsipper og retningslinjer* (ISO 31000 2009)
- *A standard of risk management* (FERMA 2002)
- *Overview of Enterprise Risk Management (*CAS *2003)*

6.2 COSO: Committee of Sponsoring Organization

COSO[28] kom ut med sitt første rammeverk *Internkontroll – et integrert rammeverk* i 1992, og rammeverket har både blitt utvidet og presisert gjennom en ny versjon som kom i 2011. I 2004 utga COSO et rammeverk med fokus på helhetlig risikostyring, *Helhetlig risikostyring – et integrert rammeverk*. Disse to rammeverkene er de mest sentrale for vår oppgave. Derfor vil vi ikke gå dypere inn i de andre rammeverkene COSO har utarbeidet, selv om de henger sammen med disse rammeverkene. Rammeverkene for risikostyring og internkontroll er

[26] *"Et rammeverk er en konstruksjon som danner en ramme eller et system av rammer"* (Bokmålordlista 2012 (2)).
[27] Disse rammeverkene hadde vi kjennskap til før vi begynte på denne oppgaven, derfor er disse valgt ut til sammenligning.
[28] COSO er en frivillig organisasjon som ble opprettet i 1985 på et felles initiativ fra fem privat organisasjoner. Disse fem organisasjonene er: The Institute of internal Auditors (IIA), the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), and the Institute of Management Accountants (IMA). Hovedtanken bak å opprette COSO var å utvikle rammeverk og veiledninger til risikostyring og internkontroll gjennom godt lederskap.

anerkjente både av NUES og Finanstilsynet. NUES krever konkrete opplysninger om hvilke rammeverk en virksomhet har benyttet seg av i organiseringen av risikostyring og internkontroll (NUES kapittel 10). Finanstilsynet bygger sin tilsynsmodul for operasjonell risiko på komponentene fra rammeverket, helhetlig risikostyring (COSO 2004), som er beskrevet i kapittel 5.

I dette delkapittelet vil vi vise hvordan risikostyringsprosessen kan gjennomføres i COSO`s rammeverk for helhetlig risikostyring (COSO 2004). Vi velger også å vise til hvordan rammeverket for internkontroll (COSO 1992) er bygd opp, samt den reviderte utgaven (COSO 2011)[29]. Bakgrunnen for dette er at rammeverket for helhetlig risikostyring (COSO 2004) bygger på rammeverket internkontroll (COSO 1992).

6.2.1 Internkontroll – et integrert rammeverk, 1992 og 2011

I rammeverket *Internkontroll – et integrert rammeverk* (COSO 1992) presiseres det at internkontrollen er styrets og ledelsens ansvar, både når det gjelder design, implementering og oppfølging. Rammeverket har siden blitt anerkjent og hyppig benyttet som modell i utviklingen av krav for etablering av god styring og kontroll i næringslivet og offentlig sektor (Gaudernack 2009). Dette gjelder både i Norge og internasjonalt. Rammeverket (COSO 1992) definerer internkontroll slik:

> *Internkontroll er en prosess igangsatt og gjennomført av virksomhetens styre, ledelse og ansatte. Den utformes for å gi rimelig grad av sikkerhet for måloppfyllelse innen følgende områder:*
>
> - *Målrettet og kostnadseffektiv drift*
> - *Pålitelig ekstern regnskapsrapportering*
> - *Overholdelse av gjeldende lover og regler*

[29] Vi velger å ikke vurdere rammeverket for internkontroll opp mot GRC.

Figur 6.1: COSO- kuben (Internkontroll – et integrert rammeverk 1992)

Figur 6.1 illustrerer COSO- kuben. Kubens høyre side illustrer at internkontrollen må utføres og kontrolleres i enhetenes aktiviteter i et selskap. Dette er viktig for at virksomheten skal lykkes med målet om en målrettet og kostnadseffektiv drift. På toppen av kuben ligger de tre målkategorier som skal få organisasjonen til å differensiere aspektene på internkontrollen. Kubens fremste side viser de fem målkomponenter som beskriver stegene i internkontrollprosessen.

Den reviderte utgaven av rammeverket baserer seg på de samme komponentene som i det originale COSO- rammeverket fra 1992. Bakgrunnen for utviklingen av et nytt rammeverk var basert på de endringene som har skjedd i løpet av de siste tjue årene. Dramatiske endringer i miljøet, som økende kompleksitet, mer teknologidrevet, større grad av globalisering, involverende aksjeeiere er bare noen stikkord for utviklingen som har gjort det nødvendig å tilpasse rammeverket til dagens situasjon (COSO 2011).

Det som imidlertid er nytt fra det originale rammeverket for internkontroll (COSO 1992), er de 17 prinsippene som er lagt inn i det nye rammeverket (COSO 2011). Prinsippene er utarbeidet for å oppnå større effektivitet til de ulike komponentene i internkontrollprosessen. Tabell 6.1 viser hvordan de 17 prinsippene utfyller de fem komponentene i rammeverket.

Control Environment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
Risk Assessment	6. Specifies relevant objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change
Control Activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures
Information & Communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring Activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

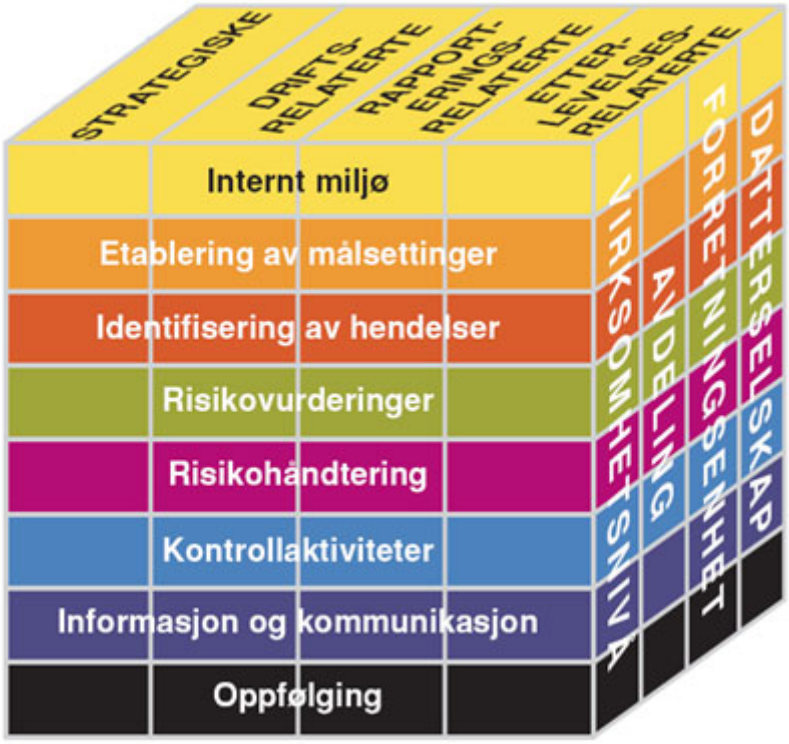
Tabell 6.1: COSO – sammendrag av de 17 prinsippene (2011)

6.2.2 Helhetlig risikostyring – et integrert rammeverk, 2004

I 2004 utga COSO rammeverket *Helhetlig risikostyring – et integrert rammeverk* i samarbeid med PWC. Hensikten bak rammeverket (COSO 2004) er å hjelpe foretak med å få et bredere fokus på risikostyring, hvor internkontroll skal være en del av prosessen.
COSO (2004) har definert helhetlig risikostyring på følgende måte:

> *Helhetlig risikostyring er en prosess, gjennomført av virksomhetens styre, ledelse og ansatte, anvendt i fastsettelse av strategi og på tvers av virksomheten, utformet for å identifisere potensielle hendelser som kan påvirke virksomheten og for å håndtere risiko slik at den er i samsvar med virksomhetens risikoappetitt, for å gi rimelig grad av sikkerhet for virksomhetens måloppnåelse.*

Kuben i figur 6.2 viser hvordan rammeverket for helhetlig risikostyring (COSO 2004) henger sammen. Toppen av kuben viser målkomponentene, og den fremste siden viser komponentene i risikostyringsprosessen. Den siste siden viser at risikostyringen henger sammen i organisasjonen som en helhet. Gjennom alle de åtte stegene i risikostyringsprosessen skal det tas hensyn til de fire målkomponentene slik at risikostyringen blir mest mulig effektiv. For å få til en effektiv drift er det viktig at hele organisasjonen er inkludert i risikostyringsprosessen. Tanken bak helhetlig risikostyring er at risikostyringen ikke skal foregå ”silovis” i datterselskapene, forretningsenhetene, på avdelingsnivå eller på virksomhetsnivå, men å innføre en felles plattform for hele selskapet.



Figur 6.2: COSO- kuben (Helhetlig risikostyring – et integrert rammeverk 2004)

Målkomponentene:

Av figur 6.2 ser vi at fokus på virksomhetens måloppnåelse er definert gjennom fire kategorier. Disse kategoriene gjør det lettere for virksomheten å fokusere på alle aspekter for måloppnåelse gjennom risikostyringen. Selv om kategoriene er atskilte er de også overlappende, slik at en målsetting kan være under flere kategorier.

- Strategiske
- Driftsrelaterte
- Rapporteringsrelaterte
- Etterlevelsesrelaterte

Målkomponenten s*trategisk* inneholder målsettinger på overordnet nivå. Overordnede mål er langsiktige og reelle mål som virksomheten har satt seg. Komponenten *driftsrelaterte* er knyttet mot målsettinger som kostnadseffektiv bruk av virksomhetens ressurser. Disse målsetningene kan også bli påvirket av eksterne påvirkninger. *Rapporteringsrelaterte* og *Etterlevelsesrelaterte* målsettinger omhandler henholdsvis pålitelig rapportering, og

overholdelse av lover og regler i virksomheten. Disse komponentene skal bidra til pålitelig rapportering til tilsynsmyndigheter og etterlevelse av lover og regler.

Komponentene i risikostyringsprosessen:

Det er åtte komponenter i rammeverkets risikostyringsprosess. Disse komponentene henger sammen og er integrert i ledelsesprosesser.

- Identifisering av internt miljø
- Etablering av målsettinger
- Identifisering av hendelser
- Risikovurdering
- Risikohåndtering
- Kontrollaktiviteter
- Informasjon og kommunikasjon
- Oppfølging

Første komponent i risikostyringsprosessen er identifisering av *internt miljø.* Denne komponenten har til hensikt å identifisere de ansattes holdninger til risiko. Det interne miljøet i et selskap kan påvirke holdninger til risiko som filosofi for risikostyring, risikoappetitt, integritet og etiske verdier. Her er det viktig at ledelsen iverksetter planer og retningslinjer for å påvirke de ansattes holdninger til risikostyringen.

Andre komponent er *etablering av målsettinger.* Før ledelsen kan identifisere mulige hendelser, må de definere målsettinger som samsvarer med virksomhetens formål som avspeiler selskapets risikoappetitt.

Komponent nummer tre er *identifisering av hendelser.* Det er viktig å identifisere interne og eksterne hendelser som kan påvirke virksomhetens måloppnåelse. Identifiseringen består av å skille mellom muligheter og risikoer.

Den fjerde komponenten i risikostyringsprosessen er *risikovurdering.* I denne fasen blir risikoer analysert ved en sannsynlighet og konsekvens analyse, for å avgjøre videre håndtering. Iboende og gjenværende risiko blir også vurdert[30].

Komponent nummer fem er *risikohåndtering.* For å håndtere de risikoene som er identifisert og vurdert setter nærmeste leder opp former for risikohåndtering. Dette steget i prosessen handler om å utvikle en handlingsplan for det som er observert. Eksempler på risikohåndtering er å unngå, akseptere, redusere eller dele risikoene. Uavhengig av hvilken

[30] Iboende risiko er sannsynligheten for at en feil oppstår, mens gjenværende risiko er sannsynligheten for at en feil oppstår men ikke blir oppdaget og korrigert (Gaudernack 2011).

form man planlegger å håndtere risikoen på, er det viktig at handlingsplanen er fokusert på å bringe risikoen i samsvar med virksomhetens risikotoleranse og risikoappetitt.
Den sjette komponenten i prosessen er *kontrollaktiviteter*. Aktivitetene som blir iverksatt og implementert skal sikre at risikohåndteringen gjøres på en effektiv måte. Dette krever implementering av retningslinjer og rutiner i organisasjonen.

Komponent nummer syv er *informasjon og kommunikasjon.* Informasjon rundt prosessen skal identifiseres og videreformidles slik at de ansatte kan ivareta sitt ansvar. Målrettet kommunikasjon skal sendes vertikalt og horisontalt i virksomheten.

Den siste komponenten er *oppfølging*. Oppfølging er en kontinuerlig prosess som skal sikre at den helhetlige risikostyringsprosessen gjennomføres i henhold til krav. Oppfølging kan skje gjennom frittstående evalueringer eller løpende ledelsesaktiviteter.

6.3 ISO 31000

Den internasjonale standardiseringsorganisasjonen (ISO) er et verdensomspennende forbund som utvikler og utgir internasjonale standarder (ISO 2012). ISO 31000 er en internasjonal standard som ble utgitt i 2009, og utarbeidet av arbeidsgruppen for risikostyring i ISOs Technical Management Board. Den norske versjonen ble fastsatt i mai 2010 av Norsk Standard, Norges medlem i ISO, og har tittelen *Risikostyring - prinsipper og retningslinjer*, NS- ISO 31000: 2009.

I den internasjonale standarden[31] presenteres det termer og definisjoner, prinsipper og generelle retningslinjer for oppbygging av et rammeverk for risikostyring. Hensikten med standarden er å hjelpe organisasjoner som har til hensikt å integrere risikostyringsprosessen i organisasjonens overordnede forvaltning, strategi og planlegging, ledelse, rapporteringsprosesser, politikk, kultur og verdier (ISO 31000 2009: iv). Standarden kan brukes av organisasjoner i privat og offentlig sektor, foreninger, grupper, personer eller kommunale foretak. Standarden har definert risikostyring følgende:

> *Risikostyring er koordinerte aktiviteter for å rettlede og kontrollere en organisasjon med hensyn til risiko* (ISO 31000 2009: nr. 2.2)[32].

Den internasjonale standarden har utarbeidet 11 prinsipper for risikostyring.

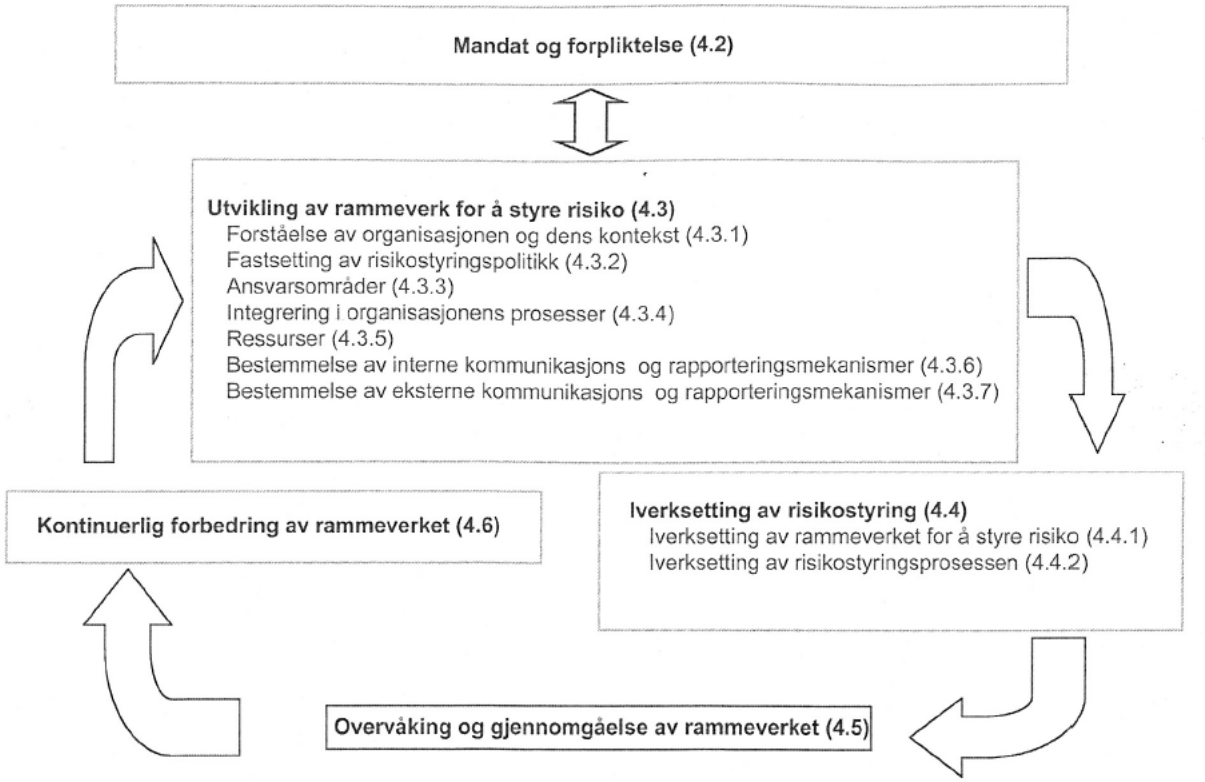
[31] Standarden er delt inn i fem kapitler, hvor alle aspektene under hvert kapittel er nummerert.
[32] Oppbygningen av standarden ISO 31000 er basert på nummerering og merknader. For eksempel omhandler kapittel 2 termer og definisjoner, og hvor 2.1definerer risiko og 2.2 definerer risikostyring. Under hvert punkt (2.1, 2.2 osv.) kan det i tillegg være merknader (merknad 1, merknad 2 osv.).

I følge standarden er prinsippene viktige å følge i alle ledd i organisasjonen for å få en effektiv risikostyring (ISO 31000 2009: 9-10):

1. *Risikostyring skaper og ivaretar verdier*
2. *Risikostyring er en integrert del av alle organisasjoner*
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*

Rammeverket for risikostyring defineres følgende (ISO 31000 2009: nr. 2.3):

> *Rammeverk for risikostyring er et sett av elementer som gir grunnlaget og de organisasjonsmessige løsningene for å utvikle, iverksette, overvåke, gjennomgå og kontinuerlig forbedre risikostyring i hele virksomheten.*



Figur 6.3: Forholdet mellom elementene i rammeverket for risikostyring (ISO 31000 2009: 11)

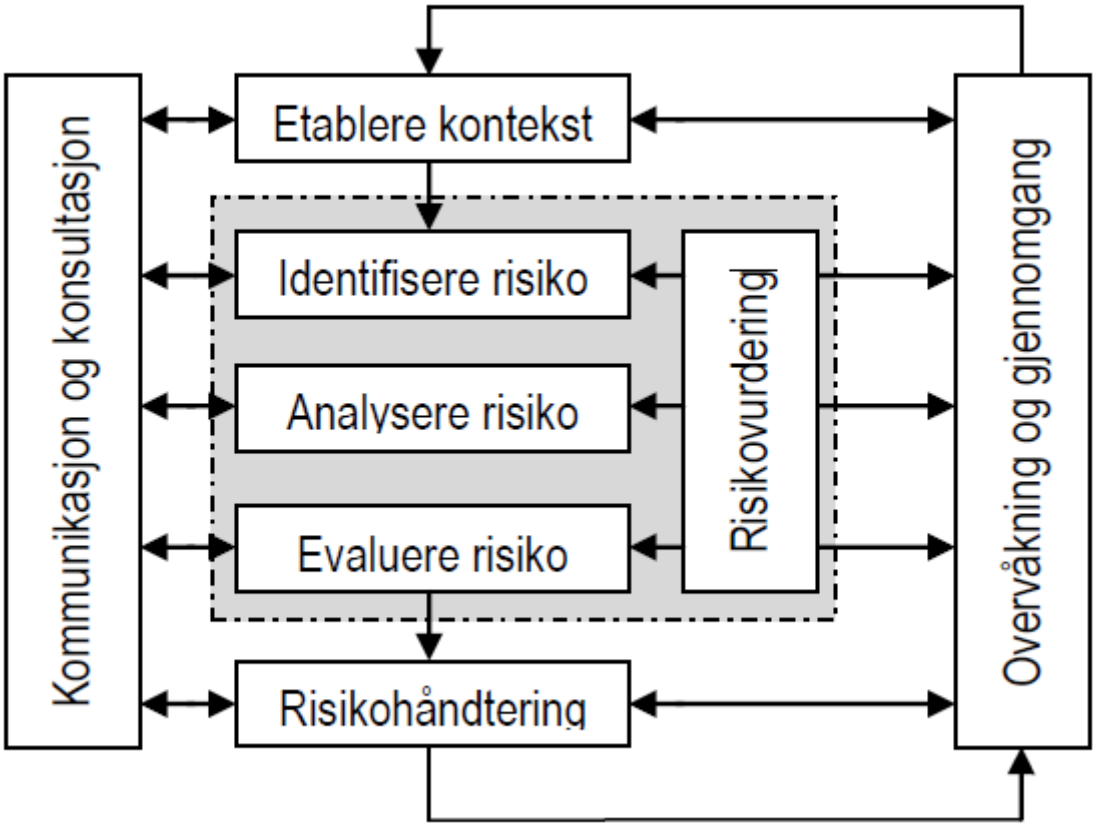
Figur 6.3 viser hvordan rammeverket for risikostyring i standarden er bygd opp. Rammeverket er ment som en veiledning til organisasjoner, som kan benyttes til å integrere risikostyring i deres overordnede styringssystem. For at rammeverket skal være formålstjenlig må det derfor tilpasses organisasjonens egne behov.

Risikostyringsprosessen

Den internasjonale standarden definerer risikostyringsprosess følgende (ISO 31000 2009: 2.8):

> *Risikostyringsprosess inneholder systematisk bruk av politikk, prosedyrer og praksis for styring av aktivitetene kommunikasjon, konsultasjon, bestemmelse av kontekst og identifisering, analysering, evaluering, håndtering, overvåking og gjennomgåelse av risiko.*

Selve prosessen bør være integrert i organisasjonens styring, i organisasjonskulturen og praksis. Den bør være skreddersydd til forretningsprosessene i organisasjonen (ISO 31000 2009: 5.1).



Figur 6.4: Risikostyringsprosessen (ISO 31000 2009: 17)

Figur 6.4 viser risikostyringsprosessen i sin helhet. Figuren består av fem hovedkomponenter:

1. Bestemmelse av kommunikasjon og konsultasjon
2. Bestemmelse av kontekst
3. Risikovurdering
    - Risikoidentifisering
    - Risikoanalyse
    - Risikoevaluering
4. Risikohåndtering
5. Overvåking og gjennomførelse

Fra "boksen" *kommunikasjon og konsultasjon* i figur 6.4 er det piler ut til hele risikostyringsprosessen. Ettersom kommunikasjon og konsultasjon med eksterne og interne interessenter kan gjøres under alle trinn i prosessen, er det viktig å utvikle planer så tidlig som mulig for å få til dette. Standarden trekker frem at en slik plan må inneholde forhold knyttet til risikoen, risikoens årsaker og konsekvenser samt håndteringstiltak.

Etter kommunikasjon og konsultasjon med interessentene er neste steg i prosessen å *bestemme konteksten* til organisasjonen (ISO 31 000 2009: nr. 5.3). I dette steget er det viktig å definere intern og ekstern kontekst. Tabell 6.2 gir en oppsummering av påvirkninger som kan oppstå fra intern og ekstern kontekst.

INTERN KONTEKST	**EKSTERN KONTEKST**
Organisasjonskultur	Kulturelle påvirkninger
Overordnede mål og retningslinjer	Juridiske påvirkninger
Standarder	Økonomiske påvirkninger
Menneskelige ressurser	Konkurranse
Kapital	Politiske påvirkninger

Tabell 6.2: Oppsummering av påvirkninger fra intern og ekstern kontekst

Konteksten til risikostyringsprosessen vil variere etter hvilke behov organisasjonen har. Eksempler på kontekst for risikostyringsprosessen kan være fastsettelse av mål for risikostyringsaktivitetene, ansvarsområder, bredde og dybde av risikostyringsaktivitetene, risikovurderingsmetoder etc.

Etter fastsettelse av organisasjonens kontekst er neste steg i prosessen *risikovurdering*.

"Risikovurdering er en samlet prosess som omfatter risikoidentifisering, risikoanalyse og risikoevaluering" (ISO 31 000 2009: nr. 5.4.1). Under risikovurdering ligger det tre elementer som skal vurderes:

- Risikoidentifisering
- Risikoanalyse
- Risikoevaluering

Formålet med *risikoidentifisering* er å kartlegge risikoer basert på hendelser som kan skape, styrke, forhindre, forringe, utsette eller fremskynde målene organisasjonen har satt. I identifiseringen vil årsaks- og konsekvensanalyser av risikoene være viktige å vurdere. En *risikoanalyse* består av overveielse av årsak til risiko, risikoens positive og negative konsekvenser, og sannsynligheten for at den vil inntreffe. Resultatene fra risikoanalysen skal brukes i *risikoevalueringen* for å ta beslutninger om hvilke risikoer som skal håndteres, og prioritering av iverksetting av risikohåndteringen.

Etter å ha vurdert risikoene er neste steg i prosessen *risikohåndtering*. *"Risikohåndtering omfatter å velge ett eller flere alternativer for å modifisere risiko og deretter iverksette disse alternativene"* (ISO 31 000 2009: nr. 5.5.1). Risikohåndteringen er en prosess som fungerer som et kretsløp, hvor vurderinger gjøres hele tiden. Denne prosessen omfatter å vurdere en risikohåndtering, som avgjør om nivået på restrisikoen kan tolereres. For å gjøre en god risikohåndtering er valg av risikoalternativer og utvikling og iverksetting av risikohåndteringsplaner to viktige elementer.

Siste steg i risikostyringsprosessen er *overvåking og gjennomgåelse*. Overvåking og gjennomgang bør utføres regelmessig eller ad hoc, som en planlagt del i risikostyringsprosessen. Resultatene bør loggføres og rapporteres internt og eksternt. Dette er en viktig prosess i risikostyringsprosessen, hvor man kan endre og sikre at kontrollene er effektive og virkningsfulle. I overvåkingsprosessen får man en bredere informasjon av risikovurderingen, tar lærdom av hendelser, identifisere risikoer som oppstår, og avdekker endringer i den eksterne og interne konteksten (ISO 31 000 2009: nr 5.6).

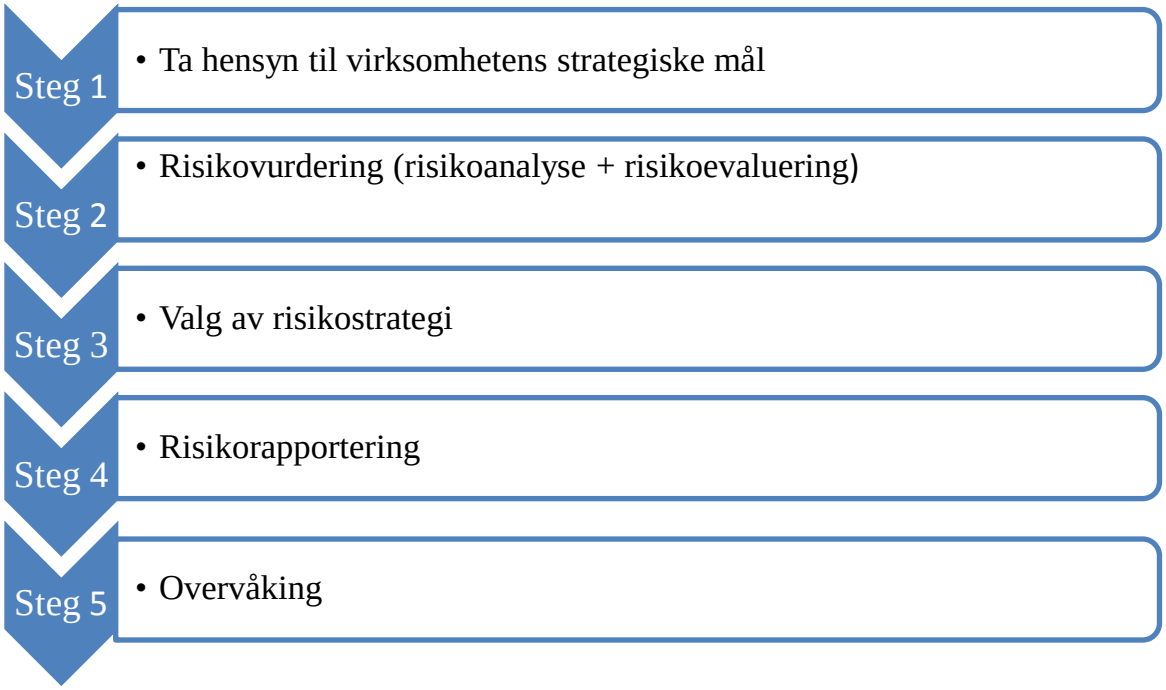
6.4 A Risk Management Standard

FERMA (Federation of European Risk Management Associations) er en organisasjon som hjelper sine medlemmer i Europeiske selskaper med blant annet effektiv bruk av risikostyring (FERMA 2012). FERMA har gitt ut en standard for risikostyring, *A Risk Management Standard* (2002) som er skrevet i samarbeid med tre britiske organer fra offentlig og privat

sektor[33]. Standarden er også gitt ut på flere språk, deriblant på dansk, *Standarden for risikostyring.* Vi har valgt å bruke både den engelske og danske oversettelsen videre i oppgaven. Standarden (FERMA 2002) er basert på beste praksis og er ment som et hjelpemiddel til å integrere risikostyring i en organisasjon. Standarden definerer risikostyring slik (FERMA 2002: 2):

> *Risikostyring er en sentral del av enhver organisasjons strategiske ledelse. Det er den prosessen som organisasjonen metodisk benytter seg av for å håndtere risikoene knyttet til sine aktiviteter, med mål om å oppnå vedvarende nytte innenfor hver aktivitet og over porteføljen av alle aktiviteter.*

Vi mener figuren for risikostyringsprosessen som er vist i standarden (FERMA 2002), er noe uoversiktlig. Figuren henger ikke godt nok sammen med resten av innholdet til risikostyringsprosessen. Derfor har vi valgt å utarbeide vår egen figur basert på forklaringsteksten i standarden (FERMA 2002).



Figur 6.5: Risikostyringsprosessen

Figur 6.5 viser vår figur av risikostyringsprosessen FERMA har beskrevet. Risikostyringsprosessen består av fem steg. Underveis i stegene i figuren er det mulighet for å gjøre endringer og modifikasjoner.

[33] AIRMIC (The Association of Insurance and Risk Managers), ALARM (The National Forum for Risk Management) og IRM (The Institute of Risk Management).

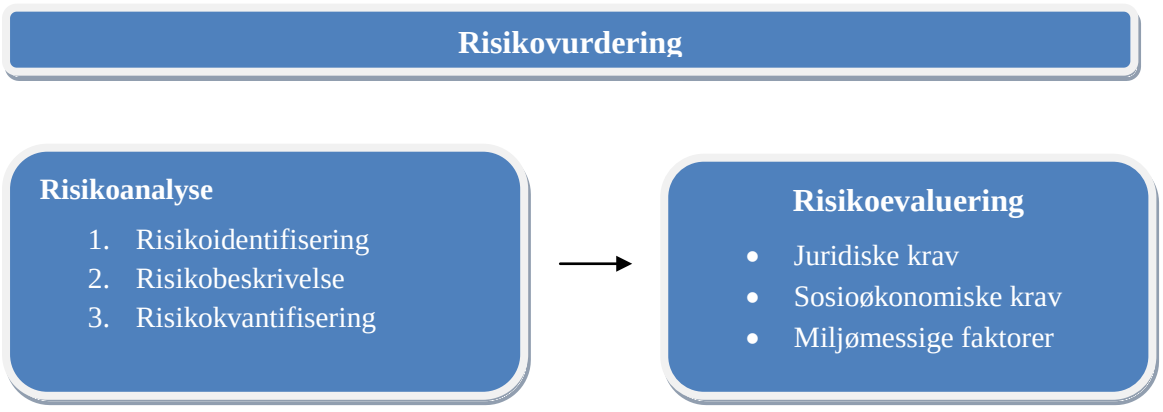
Standarden har definert en klar rollefordeling i risikostyringsprosessen mellom styret, forretningsenhetene, risikostyringsfunksjonen og internrevisjonen, som skal defineres i selskapets risikostyringspolitikk. Risikostyringspolitikken skal også inneholde hvordan selskapet skal ta hensyn til krav om virksomhetens interne retningslinjer, og selskapets risikoappetitt og holdning til risikostyring.

Steg 1:

Standardens hensikt med risikostyring er å tilføre verdi til organisasjonen og dens interessenter ved å støtte virksomhetens **strategiske mål**. De strategiske målene som styret setter for organisasjonen skal skape en ramme for hvordan organisasjonen opererer. Målene som er satt skal være sporbart i det virksomhetens foretar seg, også i risikostyringen. Altså må risikostyring som alle andre prosesser forholde seg til virksomhetens strategiske mål for å være hensiktsmessig og effektiv.

Steg 2:

Steg 2 består av **risikovurdering**. Dette er et todelt steg som består av risikoanalyse og risikoevaluering. For å vise hvordan dette henger sammen har vi utarbeidet en figur som illustrerer forholdet mellom risikoanalyse og risikoevaluering under steget risikovurdering. Figuren 6.7 viser hvordan risikovurderingsprosessen henger sammen.



Figur 6.6: Risikovurderingsprosess

Første steg i risikoanalysen er ***risikoidentifisering***. Standarden legger opp til at man i identifiseringsprosessen bør kategorisere risikoene.

Standarden (FERMA 2002: 6) har gitt følgende eksempler på risikokategorier:

- Strategisk risiko
- Operasjonell risiko
- Finansiell risiko
- Kunnskapsforvaltning
- Compliance

Strategisk risiko inneholder risiko knyttet til virksomhetens langsiktige mål. Den kan påvirkes av tilgjengelig kapital, statlige låntagere, politisk risiko, juridiske og lovmessige forandringer, omdømme og endringer i det fysiske miljøet. *Operasjonell risiko* er definert i kapittel 2.2.3. *Finansiell risiko* er faktorer som påvirkes av eksterne faktorer, som kredittmuligheter, valutakurser, bevegelser i rentenivået eller andre påvirkninger i markedet virksomheten operer i. *Kunnskapsforvaltning* er en risikokategori ledelsen er opptatt av for å styre de kunnskapsressurser virksomheten har. *Compliance* er en risikokategori som kontrollerer risiko forbundet med lover og retningslinjer som virksomheten må forholde seg til. Dette kan være HMS- regler, forbrukerbeskyttelse, databeskyttelse, og andre juridiske forhold (FERMA 2002: 6).

Andre steg i risikoanalysen er ***risikobeskrivelse***. Risikobeskrivelse i standarden inneholder en mer detaljert beskrivelsene av risikoene i risikokategoriene. Tabell 6.3 viser eksempel på hvordan en risikobeskrivelse kan se ut.

1. Name of Risk	
2. Scope of Risk	Qualitative description of the events, their size, type, number and dependencies
3. Nature of Risk	Eg. strategic, operational, financial, knowledge or compliance
4. Stakeholders	Stakeholders and their expectations
5. Quantification of Risk	Significance and Probability
6. Risk Tolerance/ Appetite	Loss potential and financial impact of risk Value at risk Probability and size of potential losses/gains Objective(s) for control of the risk and desired level of performance
7. Risk Treatment & Control Mechanisms	Primary means by which the risk is currently managed Levels of confidence in existing control Identification of protocols for monitoring and review
8. Potential Action for Improvement	Recommendations to reduce risk
9. Strategy and Policy Developments	Identification of function responsible for developing strategy and policy

Tabell 6.3: Detaljbeskrivelse av en risiko (FERMA 2002: 7)

Tredje steg i risikoanalysen er ***risikokvantifisering***. Ved risikokvantifisering[34] kan risikoen være kvantitativ, semi- kvantitativ eller kvalitativ. Det er størrelsen på risikoen som bestemmer hvilken kvantifiseringskategori den tilhører (FERMA 2002: 7). For å vurdere størrelsen på risikoen baserer standarden seg på to faktorer; sannsynligheten for forekomsten og dens konsekvens. Ettersom det kan være vanskelig å tallfeste sannsynlighet og konsekvens på kvalitative risikoer, bruker standarden et graderingsskjema som viser hvor sannsynlig det er for at risikoen vil inntreffe. *Konsekvensen* av risikoen kan både være av positiv og negativ art (muligheter og trusler) som kan kategoriseres i høy, middels eller lav. *Sannsynligheten* for at en risiko inntreffer for trusler og/eller muligheter kan også kategoriseres i stor (sannsynlig), middels (mulig), lav (usannsynlig) på eksempelvis en vertikal akse, og beskrivelse og indikatorer av risiko på horisontal akse (FERMA 2002: 7-8).

Siste ledd i risikovurderingen er ***risikoevalueringen*.** Standarden har tatt med risikoevaluering for å evaluere de identifiserte risikoene opp mot risikokriterier.

[34] *"Med kvantitative beregninger mener vi analyser som setter tall på sannsynligheter og konsekvenser knyttet til et scenario"* (SINTEF 2012).

Risikokriterier kan være juridiske krav, sosioøkonomiske og miljømessige faktorer, interessentenes bekymringer etc. I risikoevalueringen skal det også tas avgjørelser om hvordan man skal avgjøre risikoens betydning og hvorvidt man skal akseptere eller behandle risikoene (FERMA 2002: 10).

Steg 3:

Neste steg i risikostyringsprosessen er valg av **risikostrategi**. Dette steget har standarden tatt med for å sette rammer for hvordan man vil håndtere de risikoene som er analysert. I følge standarden må man i risikostrategien utarbeide og implementere de tiltakene som skal modifisere risikoene, som kan være risikoer som eksempelvis har høy og lav sannsynlighet for å inntreffe. For at risikostrategien skal være hensiktsmessig må den påse (FERMA 2002: 10):

- *En effektiv og virkningsfull drift av virksomheten*
- *Effektive interne kontroller*
- *Overensstemmelse med lover og regler*

Steg 4:

Risikorapportering er neste steg i risikostyringsprosessen. Dette er en prosess i standarden som gjøres både internt og eksternt i virksomheten. Intern rapportering gjøres fra:

- Styret
- Forretningsenhetene
- Hver enkelt medarbeider

Intern rapportering skal bringe informasjon fra risikostyringsprosessen ut til de ansatte i virksomheten. Hvert nivå har sine ansvarsområder de må følge opp, registrere og rapportere videre. *Styret* har det overordnede ansvaret for at informasjonen fra risikostyringsprosessen nås ut til alle interessenter, internt og eksternt. *Forretningsenhetene* trenger informasjon rundt sine ansvarsområder fra risikostyringsprosessen. De bør ha indikatorer som gjør det mulig å overvåke aktiviteter og følge utvikling av målene. De trenger systemer som skal fange opp variasjoner, rapportere systematisk til toppledelsen når risikoer dukker opp. De enkelte *individene* i organisasjonen skal forstå sitt ansvar for å unngå risiko. Ved oppdagelse av ny risiko eller hvis ikke kontrollene fungerer, skal det rapporteres til toppledelsen (FERMA 2002: 11).

Ved *ekstern risikorapportering* gis informasjon av virksomhetens risikostyringspolitikk til interessentene. Den formelle rapporteringen av risikostyringen skal være formulert og tilgjengelig for interessentene, og skal inneholde (FERMA 2002:11):

- Ansvarsinnhold av risikostyring på ledernivå
- Hvilke prosesser som anvendes ved identifisering av risikoer og hvordan de behandles
- Kontrollsystemer til styring av betydningsfulle risikoer
- System for overvåking og kontrollering

Steg 5:

Siste steget i standardens risikostyringsprosess er **overvåking**. Overvåking av risikostyringen defineres som en prosess som fokuserer på å sjekke at de risikoene som er identifisert har blitt vurdert effektivt. Viktige elementer som er viktig å ta hensyn til i standardens overvåkningsprosess er følgende (FERMA 2002: 14):

- Aktiviteter er i overensstemmelse med lover og regler
- Retningslinjer, policies og standarder følges internt
- Identifisere forbedringspotensial i implementerte tiltak/kontroller
- Endringer i intern og ekstern kontekst skal identifiseres og evt. tas hensyn til i risikostyringsprosessen.

6.5 Overview of Enterprise Risk Management

CAS (Casualty Actuarial Society) er en internasjonal aktuar forening som blant annet arbeider med å fremme forsikringskunnskap og tilhørende risikoeksponeringer for sine medlemmer (CAS 2012). I 2003 utarbeidet Enterprise Risk Management Commitee i CAS et konseptuelt rammeverk for helhetlig risikostyring som ble gitt ut i *Overview of Enterprise Risk Management* (CAS 2003). Rammeverket er utarbeidet for å utvide horisonten på risikostyring for aktuarer.

Det kan også benyttes av andre enn aktuarer som et hjelpemiddel til utarbeidelse av eget rammeverk for helhetlig risikostyring.

ERM Framework				
	Types of Risk			
Process Steps	Hazard	Financial	Operational	Strategic
Establish Context				
Identify Risks				
Analyze/Quantify Risks				
Integrate Risks				
Assess/Prioritize Risks				
Treat/Exploit Risks				
Monitor & Review				

Tabell 6.4: Konseptuell tilnærming av helhetlig risikostyring (CAS 2003: 9)

Tabell 6.4 viser den konseptuelle tilnærmingen for helhetlig risikostyring i en to- dimensjonal modell. Stegene i risikostyringsprosessen er definert langs den vertikale aksen, og typer risiko er definert på den horisontale aksen. CAS har definert risikotypene inn i fire kategorier: Hazard risiko, finansiell risiko, operasjonell risiko og strategisk risiko. Stegene i risikostyringsprosessen har CAS hentet fra rammeverket Australian/New Zealand Standard in Risk Management (AS/NZS 4360). CAS bruker følgende definisjon på helhetlig risikostyring (CAS 2003: 8):

> *Helhetlig risikostyring er den disiplinen som en organisasjon i alle bransjer vurderer, kontroller, utnytter, finansierer og skjermer risiko fra alle kilder i den hensikt å øke organisasjonene kortsiktige og langsiktige verdi til sine interessenter.*

<u>De fire risikokategoriene:</u>

- Hazard risiko
- Finansiell risiko
- Operasjonell risiko
- Strategisk risiko

Risikokategoriene er kun listet opp i rammeverket. Derfor vil vi gi en litt dypere forklaring til de ulike risikoene som kan inntreffe under hver risikokategori.

Hazard risiko er en risikokategori som er knyttet til direkte farer fra omgivelsene (internt og eksternt). Disse farene kan være forårsaket av ytre krefter som kan være vanskelig for virksomheten å sikre seg imot, som for eksempel naturkatastrofer og brann. Hazard risiko kan også forekomme internt i virksomheten. Et eksempel på dette er driftsavbrudd som er en direkte fare som kan utgjøre stor risiko. Sykdom og uførhet, direkte eller indirekte arbeidsrelatert, utgjør også en intern risiko for virksomheten. Tyveri og kriminalitet er også en type hazard risiko. Et siste eksempel er erstatningskrav. Dette er en risiko man ikke regner med skal dukke opp, men det er viktig å ha interne rutiner og kontroller slik at dette ikke forekommer (CAS 2003: 10).

Finansiell risiko er en risikokategori som er knyttet til risiko i markedet bedriften operer i, som kan gi negative og positive konsekvenser. Pris på aktivaverdi, rente, valuta og råvare kan svinge opp og ned, som gir konsekvenser for hvordan virksomheten kan handle effektivt i markedet. Lavere pris på råvarer gir virksomheten økonomisk gevinst, noe som gir et positivt utfall for virksomheten. På den andre side kan økte råvarepriser utgjøre en stor risiko for virksomheten, og skape uheldige ringvirkninger. Hvis virksomheten ikke har god nok likviditet, kan det i seg selv utgjøre en finansiell risiko. Inflasjonen kan også utgjøre en stor finansiell risiko.

Operasjonell risiko er definert i kapittel 2.2.3. *Strategisk risiko* er risiko som kan påvirke de strategiske målene virksomheten har satt seg. Selskapets omdømme kan være en risikofaktor som kan skade selskapets strategiske mål. Ved nyetablering av en enhet er det viktig å ta hensyn til kundenes demografiske, sosiale og kulturelle trender. Hvis ikke produktet er tilpasset kundemassen vil dette utgjøre en stor strategisk risiko. Endringer i teknologisk utstyr kan også utgjøre en strategisk risiko. Innovasjoner kan gjøre produksjonen effektiv, men en omstilling kan i et slikt tilfelle være kostbart. En annen innfallsvinkel vil være hvordan konkurrentene adopterer ny teknologiske endringer. Politiske og regulatoriske vedtak, lover og bestemmelser kan også utgjøre en strategisk risiko for driften.

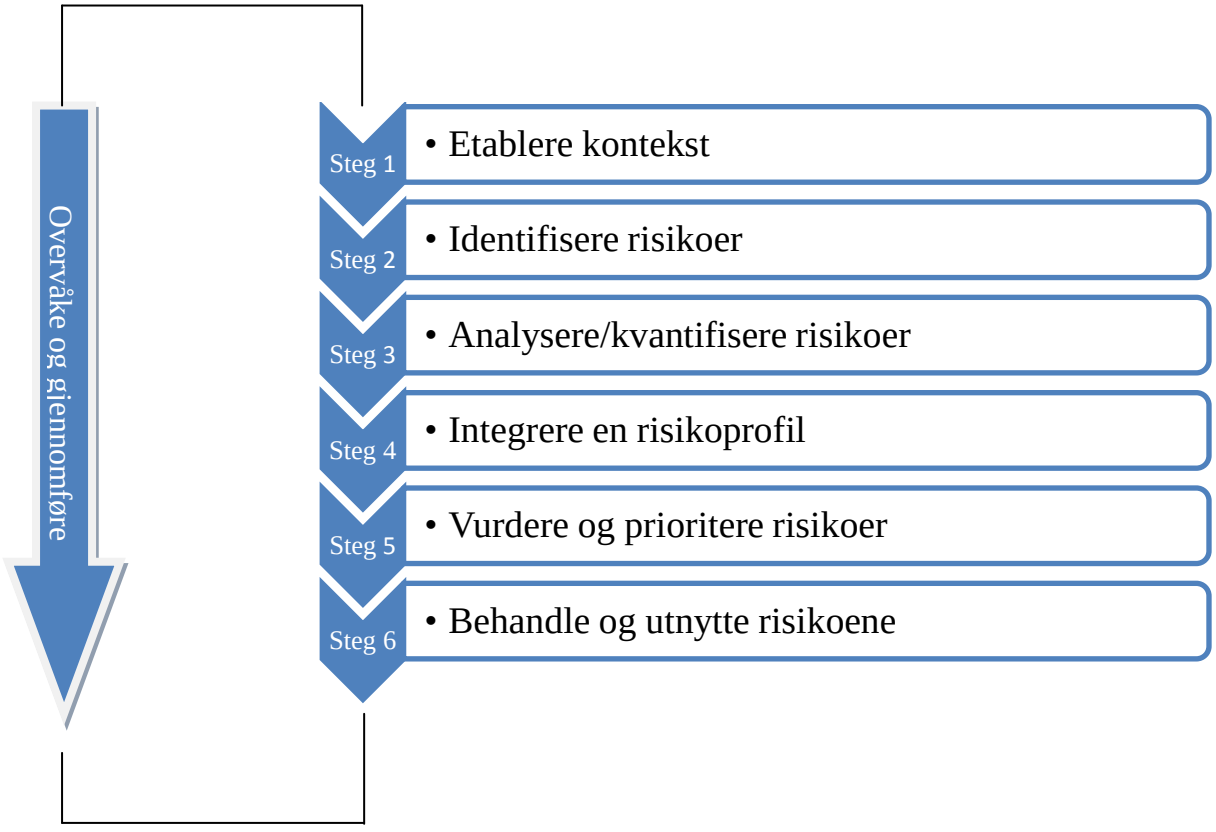
Disse risikotypene er i stor grad overlappende i helhetlig risikostyring. Hensikten bak risikokategoriseringen i rammeverket er å dekke alle vesentlige risikofaktorene som kan oppstå. Disse kan sammen påvirke virksomhetens samlede verdi. I tabell 6.4 ser vi hvordan risikokategoriene ikke alltid kan sees isolert fra hverandre, fordi noen av stegene må sees sammen med alle risikokategoriene. Tabell 6.5 viser en oppsummering av hvordan risikoer kan oppstå i de ulike risikokategoriene.

Hazard risiko	Finansiell risiko	Operasjonell risiko	Strategisk risiko
•Naturkatastrofer •Driftsavbrudd •Arbeidsskader og sykdom •Tyveri og kriminalitet •Erstatningskrav	•Prisendringer •Manglende likviditet •Inflasjon	•Menneskelig svikt i prosesser •Myndiggjøring •Svikt i IT-systemer	•Omdømmerisiko •Konkurranse •Kundekrav •Demografiske trender •Teknologi og innovasjon •Regulatoriske og politiske vedtak

Tabell 6.5: Oppsummering av risikotyper i risikokategoriene

Stegene i risikostyringsprosessen:

Figur 6.7 viser de syv ulike stegene i risikostyringsprosessen. For å få modellen på norsk har vi utarbeidet en figur basert på det opprinnelige rammeverket.



Figur 6.7: Stegene i risikostyringsprosessen

Figuren viser hvordan risikostyringsprosessen i rammeverket kan gjennomføres i syv steg.

Steg 1:

Første steg i rammeverkets risikostyringsprosess er å *etablere konteksten* til virksomheten. Konteksten til virksomheten består av:

- Ekstern kontekst
- Intern kontekst
- Konteksten til risikostyringen

Rammeverket utdyper at *konteksten til risikostyringen* innebærer identifisering av risikokategoriene som skal koordineres ut ifra hele virksomheten, og deretter vedta en felles standard for å beregne risiko (CAS 2003: 11).

Steg 2:

Andre steg i prosessen er å *identifisere risiko*. For å komme frem til de viktigste risikoene i hver risikokategori anbefaler standarden å gjøre undersøkelser i virksomheten for å få frem de ansattes syn på hvilke risikoer som er viktig å prioritere. Workshops, brainstorming etc., er eksempler på metoder for å identifisere risiko. Identifiseringen skal gjøres på et bredt nivå for å få en oversikt over risikobildet. Prioriteringen av risikoen gjøres senere i prosessen (CAS 2003: 11).

Steg 3:

Neste steg er å *analysere eller og kvantifisere risikoer*. Det innebærer å kalibrere sannsynligheten for utfallet av hver risiko. Utfallet av denne prosessen skal gi nødvendig informasjon til de andre stegene i prosessen, som integrering og prioritering av risikoer. De risikoene som har størst sannsynlighet for å inntreffe er nødvendig å ta hensyn til videre i prosessen. Det er fra dette trinnet i prosessen at utvalget for risikoene i hver kategori blir valgt, basert på trusselen de utgjør for virksomheten (CAS 2003: 12).

Steg 4:

Etter å ha prioritert hvilke risikoer som skal prioriteres er neste steg i prosessen å *integrere risikoene*. Det innebærer å koble sammen risikoene, reflektere over sammenhengen mellom risikoene, og uttrykke hvordan de påvirker virksomhetens prestasjonsbaserte indikatorer (CAS 2003: 12).

Steg 5:

Steg fem i risikostyringsprosessen handler om å *vurdere eller prioritere risikoene*. Det innebærer å fastsette utslaget hver risiko utgjør i risikoprofilen virksomheten har bestemt, og prioritere disse (CAS 2003: 12).

Steg 6:

Etter å ha integrert og prioritert risikoene, er sjette steg å *behandle eller utnytte risikoene*. Dette steget i prosessen omfatter flere ulike strategier for å behandle, unngå, redusere eller overføre risikoene (CAS 2003: 13).

Steg 7:

Som et siste steg i prosessen inngår *gjennomgang og overvåking* av det man har definert, analysert og implementert i risikoprosessen. Dette er et steg som også skal gjøres underveis i prosessen. Det krever en kontinuerlig måling av risikomiljøet og utførelse av risikostyringsstrategiene, som gir grunnlag til å vurdere om risiko er skalerbar over en viss periode. Resultatene fra den kontinuerlige gjennomgangen underveis er tilbakemeldinger fra fasene i prosessen som kan justeres og endres på underveis.

6.6 Oppsummering av rammeverkene

6.6.1 GRC: Governance, Risk, Compliance

For å kunne vurdere de fire presenterte rammeverkene vil vi vurdere innholdet opp mot elementene GRC (Governance, Risk og Compliance). Et GRC rammeverk er definert som: *"(…)et integrert og helhetlig system for mennesker, prosesser og teknologi som muliggjør for en organisasjon å sette mål som er kompatible med sine verdier og risikotoleranse under drift innenfor juridiske og etiske grenser"* (Laserfiche 2010: 1). Nøkkelordene ”integrert” og ”helhetlig system” i definisjonen av GRC kjenner vi igjen i kravet fra artikkel 44 i Solvens II-direktivet. Vi mener at definisjonen av GRC rammeverket kan sammenlignes med kravet i artikkel 44 i Solvens II- direktivet. Derfor vil vi sammenligne de fire rammeverkene opp mot GRC, som vil gi oss en pekepinn om de kan benyttes som et system for risikostyring.

Selv om GRC virker som tre selvstendige elementer, er hensikten bak en GRC tilnærming i et rammeverk for risikostyring å tolke disse som tre overlappende elementer som

må integreres og sees i sammenheng[35]. Sondstad og Byrkjelo (2010:6) hevder at disse tre elementene bør være tilstede i et felles rammeverk for å få en helhetlig tilnærming som skal sikre (…) *tilstrekkelig oversikt for styring, kontroll, og ikke minst utvikling og nyskaping.*

De elementene vi ser etter er oppsummert i tabell 6.6. Disse elementene er valgt ut på bakgrunn av våre kilder[36]. Vi har valgt å vurdere innholdet i risikostyringsprosessene opp mot GRC, for å gi forsikringsselskaper en pekepinn på hvilket rammeverk som best kan brukes i kravet om et system for risikostyring.

GOVERNANCE	RISK	COMPLIANCE
• Fordeling av ansvar og roller mellom aktørene i selskapet	• Risikostyring: de prosesser for å identifisere, analysere og håndtere risikoer	• Etterlevelse av retningslinjer og rutiner
• De aktiviteter (prosesser og systemer) som skal sikre måloppnåelse, og at ressurser blir brukt hensiktsmessig	• Fastsette risikotoleranse og risikoappetitt[37]	• Etterlevelse av regelverk

Tabell 6.6: Oversikt over innholdet i Governance, Risk og Compliance.

6.6.2 Oppsummering av rammeverkene sammenlignet med GRC

I dette delkapittelet vil vi oppsummere hvordan de fire rammeverkene inneholder de tre elementene GRC.

<u>Helhetlig risikostyring (COSO 2004)</u>

Innenfor *governance* har rammeverket tydeliggjort roller og ansvar. Styret har i følge rammeverket en ”påse” – rolle for virksomhetens risikostyring. Dette betyr at styret har det

[35] Dette belyses blant annet i artikkelen skrevet av Sondstad og Byrkjelo (2010:6), hvor forfatterne har beskrevet hva et rammeverk for god virksomhetsstyring bør inneholde.
[36] OECD sin definisjon av CG og Sondstad og Byrkjelo (2010).
[37] Med risikoappetitt menes hvor mye risiko en virksomhet er villig til å akseptere for å oppnå verdi. Hvor mye risiko man er villig til å ta kommer an på hva slags risikoeksponering virksomheten står overfor, og de målene man har satt vedrørende verdiskapning. Risikoappetitten en virksomhet setter seg er ulik fra virksomhet til virksomhet, fra bransje til bransje. Helhetlig risikostyring blir i større grad virkningsfullt ved å ha kontroll på hvor mye risiko virksomheten tåler, og ha en tilhørende strategi for å motvirke at risikoen inntreffer (COSO 2012).

overordnede ansvaret for risikostyringen, og skal påse at de mest betydelige risikoene blir fulgt opp. Administrerende direktør har det endelige ansvaret for risikostyringen, og har et "eierskap" til det. Andre ledere har ansvar for å håndtere risiko innenfor sine ansvarsområder, i samsvar med selskapets risikoappetitt. Annet personell som er med i prosessen for helhetlig risikostyring har et ansvar for å følge retningslinjer og rutiner. De tre første målkomponentene (strategiske, driftsrelaterte og rapporteringsrelaterte) i COSO- kuben viser hvordan rammeverket skal sikre at ressurser benyttes hensiktsmessig til virksomhetens målsettinger.

Innenfor *risiko* og risikostyring har rammeverket flere viktige momenter for å sikre god helhetlig risikostyring. Rammeverket viser at styret har et "påse" – ansvar for å overvåke selskapets risikoappetitt. Videre er det ledernes ansvar å fremme etterlevelse av selskapets risikoappetitt i sitt risikostyringsarbeid. Rammeverkets risikostyringsprosess viser tydelig hvilke steg som omhandler risikobehandling; identifisering av hendelser, risikovurdering og risikohåndtering.

Siste komponent i GRC er *compliance.* Dette fremkommer av den fjerde målkomponenten "etterlevelsesrelaterte" i COSO- kuben. Denne komponenten skal sikre etterlevelse av gjeldende lover og regler gjennom hele risikostyringsprosessen. I tillegg kommer det klart frem at "annet personale" enn styret og ledelse skal følge opp selskapets etablerte rutiner og retningslinjer.

ISO 31000 (2009)

Innenfor rollefordeling i *governance* legger ikke standarden opp til hvilke aktører som har roller og ansvar. Standarden legger imidlertid føringer for hvilke ansvarsområder ledelsen har gjennom første komponent i rammeverket for risikostyring, "mandat og forpliktelse" (figur 6.3). Rammeverket utyper hvor viktig der er med forpliktelse hos ledelsen kombinert med strategisk planlegging for å skape en forpliktelse på andre nivåer i organisasjonen. Ledelsens konkrete ansvar er å integrere risikostyringen inn i organisasjonens prosesser, som strategisk planlegging og styringsprosesser for prosjekter og endringer (ISO 31000 2009: nr. 3b).

Innenfor *risiko* og risikostyring har standardens rammeverk fokus på risikovurdering og risikohåndtering. Under steget risikovurdering ligger elementene risikoidentifisering, risikoanalyse og risikoevaluering, før neste steg i prosessen er risikohåndtering.

Siste komponent i GRC er *compliance.* Etterlevelse av juridiske krav kommer frem av tredje element i rammeverket for risikostyring, i komponenten "iverksetting av risikostyring"

i figur 6.3. Standarden foreslår at når en organisasjon skal iverksette risikostyring er det viktig å gå gjennom en sjekkliste, som blant annet inneholder overholdelse av juridiske krav.

A risk management standard (FERMA 2002)

Innenfor *governance* har standarden definert roller og ansvar som skal ligge under selskapets risikostyringspolitikk. Styret har blant annet ansvaret for å fastsette selskapets strategiske mål og sørge for at risikostyringen fungerer effektivt. Rammeverket lister opp flere momenter som viser hvordan styret skal evaluere selskapets system for internkontroll (FERMA 2002:12). Ledere på avdelingsnivå har ansvaret for risikostyringen i den daglige drift. Standarden har også definert hvilke roller risikostyringsfunksjonen og internrevisjonen har i arbeidet med risikostyring (FERMA 2002:13). Steg 1 i figur 6.5 viser at risikostyringen må ta hensyn til selskapets strategiske mål, for å sikre at risikostyringen skal foregå hensiktsmessig og effektivt.

Innenfor *risiko* og risikostyring har standarden definert risikostyringsprosessen i steg 2. Steg 2 i figur 6.5 viser hvordan risikovurderingen gjennomføres i rammeverket. Risikovurderingen inneholder risikoanalyse og risikoevaluering, som viser prosessen for hvordan risikoene skal vurderes (se figur 6.6). I standardens risikostyringspolitikk kommer det frem at den også skal inneholde selskapets holdning til risiko og risikoappetitt.

Siste element er *compliance.* Under steg 2 er compliance beskrevet som en av risikokategoriene under risikoidentifiseringen. Steg 3 i risikostyringsprosessen omhandler valg av risikostrategi, hvor det presiseres at risikostrategien skal være hensiktsmessig og skal blant annet være i overensstemmelse med lover og regler. Overholdelse av interne lover og retningslinjer skal tas hensyn i selskapets risikostyringspolitikk.

Overview of ERM (CAS 2003)

Ettersom den organisatoriske delen av rammeverket er svakt er det vanskelig å gjenkjenne elementene i *governance.*

Innenfor *risiko* og risikovurdering er det stort fokus på hvordan de ulike risikoene i de fire risikokategoriene skal identifiseres og analyseres underveis i prosessen. I steg 5 i figur 6.7 kommer det frem hvordan selskapene må vurdere risikoene opp mot selskapets risikoprofil.

Det siste elementet i GRC er *compliance.* Det fremkommer ikke av rammeverket at selskaper skal ta hensyn til etterlevelse av lover, regler, rutiner og retningslinjer i risikostyringsprosessen.

6.6.3 Sammenligning av rammeverkene mot GRC

Vi vil nå sammenligne de fire rammeverkene mot GRC. For å sammenligne rammeverkene har vi valgt tre indikatorer. Indikatorene skal indikere hvordan hvert rammeverk inneholder de definerte elementene under governance, risk og compliance, som vist i tabell 6.6. Indikatorene vi har valgt er:

- Ikke tilfredsstillende
- Tilfredsstillende
- Beste praksis

Indikatoren *ikke tilfredsstillende* betyr at rammeverket ikke tar hensyn til noen av de definerte elementene under governance, risk og compliance i tabell 6.6. Med *tilfredsstillende* har rammeverket minst ett element, og med indikatoren *beste praksis* inneholder rammeverket begge elementene fra GRC.

	Helhetlig risikostyring (COSO 2004)	**ISO 31000**	**Overview of ERM**	**A risk management standard**
GOVERNANCE	Beste praksis	Ikke tilfredsstillende	Tilfredsstillende	Beste praksis
RISK	Beste praksis	Tilfredsstillende	Beste praksis	Beste praksis
COMPLIANCE	Beste praksis	Tilfredsstillende	Ikke tilfredsstillende	Beste praksis
KONKLUSJON	Beste praksis	Tilfredsstillende	Tilfredsstillende	Beste praksis

Tabell 6.7: Sammenligning av rammeverkene

Tabell 6.7 viser vår sammenligning av rammeverkene. Av tabellen vises det at rammeverket for helhetlig risikostyring (COSO 2004) og A risk management standard (FERMA 2002) tilfredsstiller indikatoren beste praksis. Vi mener at disse rammeverkene inneholder gode kvaliteter som tilfredsstiller et GRC rammeverk, selv om de har noen svakheter hver for seg.

På mange måter vil vi si at de utfyller hverandre, hvor den enes svakhet er den andres styrke. De viktigste kvalitetene vi vil trekke frem er:

- COSO- rammeverket (2004) har en ryddig gjennomgang av hvordan en risikosyringsprosess kan gjennomføres.
- A risk management standard har en tilnærming til fire risikokategorier i risikostyringsprosessen, som gjør det enklere for et selskap å sikre at alle risikokategorier blir avdekket i risikostyringen.

Rammeverkene har en veldig teoretisk fremstilling av hvordan risikostyringen kan gjennomføres i praksis. Denne baksiden har også vært diskutert av andre. Gaudernack (2010) hevder at COSO (COSO 2004 og COSO 1992) ikke fungerer i praksis.

Etter denne analysen vil vi anbefale forsikringsselskaper å bruke en kombinasjon av rammeverkene helhetlig risikostyring (COSO 2004) og A risk management standard (FERMA 2002), som et utgangspunkt i sitt risikostyringsarbeid.

6.7 Fallgruver ved integrert risikostyring

Hva et godt system for risikostyring skal inneholde og hvordan det best skal implementeres har ingen fasit. Det eksisterer mange modeller og rammeverk i tilegg til våre fire utvalgte som viser beste praksis, men å tilpasse det til egen virksomhet kan by på en del utfordringer. Rammeverkene vi har presentert har gode kvaliteter, men når det teoretiske skal implementeres i praksis kan det være vanskelig kun å basere seg på ett rammeverk. Allikevel er det noen fallgruver man bør styre unna for å lykkes med et integrert system for risikostyring. Sondstad og Byrkjelo (2010: 6) mener at det er fire hovedutfordringer knyttet til å etablere et godt system for risikostyring i en organisasjon. Disse fire utfordringene er:

1. Manglende forankring hos ledelsen og i organisasjonskulturen
2. Manglende integrering av risikostyring
3. Risikostyring og risikorapportering er ofte knyttet alene til finansielle indikatorer
4. Risikostyring er nødvendig både for nye og etablerte aktiviteter

Gaudernack skriver også i en artikkel om de vanligste manglene i organiseringen av risikostyring og internkontroll (2009:8-9). Disse manglende/fallgruvene er:

1. Snevert syn på hva internkontroll er
2. Ikke definerte roller og ansvar i risikostyring og internkontroll
3. Manglende fremgangsmåte på å gjennomføre risikovurderinger
4. Etterlevelse/ oppfølging av etterlevelse
5. Dokumentoverflod
6. Internkontroll en egen prosess på siden av virksomheten

Hvordan et forsikringsselskap velger å imøtekomme kravene om et integrert system for risikostyring, som et krav fra Solvens II- direktivet, vil nok være varierende. Foreløpig stiller ikke Finanstilsynet krav om hvilket rammeverk selskapene skal benytte seg av, men at det må integreres et helhetlig system for risikostyring er et faktum.

6.8 Forskning på helhetlig risikostyring

De fire rammeverkene vi har presentert er et hjelpemiddel til hvordan en risikostyringsprosess kan gjennomføres. Selv om et system for risikostyring fremkommer som et krav fra Solvens II- direktivet, har flere forsikringsselskaper verden over allerede en slik tilnærming til risikostyring. Vi vil i dette delkapittelet vise hvordan forsikringsselskaper internasjonalt har tilpasset seg en helhetlig risikostyring, og hvilke utfall dette har gitt forsikringsselskapene.

6.8.1 Implementering av helhetlig risikostyring internasjonalt

Towers Perrin[38] gjorde i 2008 en internasjonal undersøkelse blant forsikringsselskaper for å kartlegge positive sider ved å innføre et system for helhetlig risikostyring. Resultatene i undersøkelsen ble lagt frem i en forskningsartikkel. Det avdekkes seks funn vedrørende risiko og kapitalstyring blant selskaper i hele verden (Towers Perrin 2008 (1): 1). Respondentene som var med i undersøkelsen inkluderer 359 forsikrings- og reassuranseselskaper (gjenforsikringsselskaper) spredd over hele verden[39]. Ulike typer av forsikring er representert hos respondentene, hvor livsforsikring utgjorde 34 %, skadeforsikring (eiendom og havari) 33 %, reassuranse (gjenforsikring) 10 %, helseforsikring 4 %, og resterende 19 % inkluderer flere- linjede forsikringsselskaper (”multiple insurers”) og finansielle grupper (Towers Perrin 2008 (1): 2).

Et av funnene fra undersøkelsen viste at større selskaper har kommet lenger i implementeringsprosessen av helhetlig risikostyring enn mindre selskaper. Med større selskaper defineres selskaper som har en omsetning på over $ 10 milliarder, og mindre selskaper er definert som selskaper med omsetning under enn $ 1 milliard (Towers Perrin 2008 (1): 2). Av undersøkelsen viste det seg at europeiske selskaper har kommer lenger med å utarbeide et system for å implementere helhetlig risikostyring. Risikokontroll er et viktig element i implementering av helhetlig risikostyring, og identifisering av alle risikoene er

[38] Towers Watson er et resultat av fusjoneringen av Towers Perrin og Watson Wyatt, 4. januar 2010.
[39] Av respondentene var 50 % fra Nord- Amerika, 31 % fra Europa, 17 % fra Asia/Pacific, 1 % fra Latin Amerika, og 1 % fra Afrika/Midtøsten.

viktig for god risikostyring. Tall fra undersøkelsen viste at flere europeiske selskaper har dokumentert risikoappetitt og risikobegrensninger fra dag til dag.

I undersøkelsen kom det frem at implementering av helhetlig risikostyring hadde påvirket andre avgjørelser i bedriften, og resultert i endringer i bedriften (Towers Perrin 2008 (1): 8). Nesten 80 % av respondentene rapporterte at innføringen av helhetlig risikostyring hadde påvirket viktige bedriftsavgjørelser over de siste to årene. De aspektene som respondentene mente de hadde endret seg størst på etter innføring av helhetlig risikostyring, var risikoappetitt eller risikostrategi (36 %), eiendel strategi (35 %), reassuranse strategi (33 %) og produktprising (31 %) (Towers Perrin 2008 (1): 8). Dette er tydelig signifikante bevis på at viktige avgjørelser knyttet mot risikostyring blir tatt på et bedre grunnlag etter implementeringen av et system for helhetlig risikostyring. Til slutt i artikkelen vises det til hvordan operasjonell risiko kan utgjøre et svakt punkt i forsikringsselskapers tilnærming til helhetlig risikostyring. Bare 7 % av respondentene mener de har hensiktsmessig styring av operasjonell risiko. Dette kan forklares med at styring av operasjonell risiko ikke står høyt nok på lista over hvilke risikoer som skal prioriteres ved helhetlig risikostyring (Towers Perrin 2008 (1): 10). Forfatterne avslutter artikkelen med dette utsagnet (Towers Perrin 2008 (1): 10):

> *We believe that the recent wave of losses in the financial services industry is resulting in a reassessment of the role of operational risk and the need for its active management.*

6.8.2 Forretningsprosesser og kultur i helhetlig risikostyring

Life insurance CFO survey #19: Embedding ERM, er en forskningsartikkel som ble utgitt i 2008 av Towers Perrin. Artikkelen er basert på forskning knyttet til beste praksis av helhetlig risikostyring i bedriftens forretningsprosesser og kultur ((Towers Perrin 2008 (2): 1). Fra undersøkelsen viste det seg at bruken av verktøy til overvåking og styring av risikoene har økt, ved tilpassing av helhetlig risikostyring i virksomheten. Slike verktøy er utarbeidet for å identifisere og måle risiko, og som et verktøy til å ta gode avgjørelser vedrørende risiko.

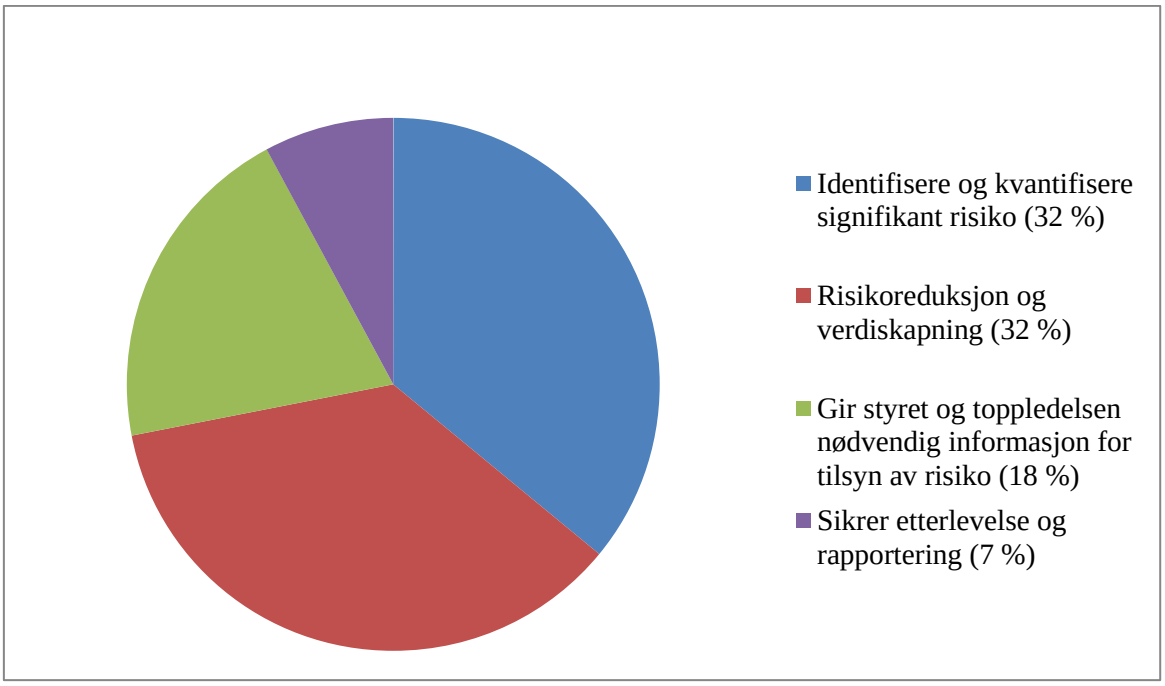


Diagram 6.1: Verktøy til overvåking og styring av risikoer

Diagram 6.1 viser hva respondentene har svart på angående hva de bruker verktøyet til. De fleste av respondentene har brukt verktøyet til enten å identifisere og kvantifisere signifikante risikoer eller til risikoreduksjon og verdiskapning. Dette er ulike informasjonskilder og verktøy som man kan dra nytte av ved implementering av helhetlig risikostyring.

Et annet viktig moment ved å implementere helhetlig risikostyring er hvordan man integrerer den i bedriftskulturen. Det eksisterer flere definisjoner av hva bedriftskultur/organisasjonskultur er, men begrepet er en betegnelse på det som er av felles oppfattelse, overbevisninger, sedvaner og ritualer (Fischer og Sortland 2001: 114). En kan dele inn organisasjonskulturen inn i tre nivåer. Første nivå er kulturelle uttrykk og manifestasjoner. Eksempler på dette er handlinger/atferd, rutiner, prosedyrer, systemer og lignende. Andre nivå er uttrykte verdier og normer. Tredje nivå er grunnleggende antakelser, som er underliggende kulturelle temaer (Fischer og Sortland 2001: 116). *"Hvis bedrifter skal integrere helhetlig risikostyring inn i kulturen, må den inkorporeres til prestasjonsmåling og være en viktig del av et belønningssystem"* (Towers Perrin 2008 (2): 2). I resultatene fra denne artikkelen viser det seg at kun 17 % av selskapene bruker verktøy som måler verdiskapelse fra helhetlig risikostyring, mens 41 % har planer om å innføre det innen 1-3 år ((Towers Perrin 2008 (2): 2).

7 Beste praksis ved styring av operasjonell risiko

7.1 Innledning

Flere av kravene fra Solvens II- direktivet inneholder spesifikke bestemmelser vedrørende styring av operasjonell risiko. Dette fremkommer blant annet av artikkel 44 og 45 i Solvens II- direktivet. Nærmere innhold i bestemmelsene er i belyst i kapittel 4. Ettersom de kvalitative kravene for operasjonell risiko er sammenlignbare med Basel II- direktivet, vil vi vise hvordan kvantifisering og styring av operasjonell risiko har blitt utført i banksektoren.

7.2 Tapshendelseskategorier

Definisjonen av operasjonell risiko i Solvens II- direktivet inneholder tre elementer; tap som følge av svikt i interne prosesser, menneskelige feil eller eksterne hendelser. Dette er områder som er svært brede, og tapskategoriene under hvert av områdene kan være vanskelig å definere, operasjonalisere, og kontrollere. Ettersom det foreløpig ikke har blitt utarbeidet noe norsk lovverk som tilsvarer forskrift om kapitalkrav for forretningsbanker, sparebanker, finansieringsforetak, holdingselskaper i finanskonsern, verdipapirforetak og forvaltningsselskaper for verdipapirfond mv. (kapitalkravsforskriften[40]) for forsikringsselskaper, er det naturlig å bruke denne som et eksempel på å identifisere operasjonell risiko. Kapitalkravforskriften gjelder i utgangspunktet for ”(…) *banker, finansieringsforetak, holdingselskaper i finanskonsern, verdipapirforetak og forvaltningsselskaper for verdipapirfond som har tillatelse til å drive aktiv forvaltning”,* etter § 1-1 1. ledd. Kapitalkravsforskriften del VIII § 44-2 omhandler beregningsgrunnlag av operasjonell risiko. Valg av beregningsmetode ved utregning av operasjonell risiko kan gjøres på tre måter; basismetoden (§ 41-1 1. ledd (a)), sjablongmetoden (§ 41-1 1. ledd (b)) og AMA- metoden (§ 41-1 1. ledd (c)). Videre står det spesifikt hvordan de ulike metodene regnes ut, og på hvilket grunnlag. Beregningsmetodene i kapitalkravforskriften kan gjøres gjeldende for forsikringsselskaper når det nye norske lovverket samsvarer med kravene fra Solvens II- direktivet.

Ettersom Finanstilsynet benytter seg av tapshendelseskategoriene i AMA-metoden, velger vi å gå nærmere inn på denne beregningsmetoden for operasjonell risiko. Kapitalkravforskriftens § 44-2 omhandler *”Forhold som skal hensyntas ved fastsettelse av beregningsgrunnlag”*. I kapitalforskriftens § 44-2 1. ledd står det utdypet at *AMA- systemet*

[40] Heretter fortkortet til kapitalkravforskriften.

skal bygge på interne data, eksterne data, scenarioanalyser og faktorer knyttet til virksomheten og kontroll etter annet til femte ledd. I kapitalforskriftens § 44-2 2. ledd punkt b står det listet opp syv tapshendelseskategorier som skal være beskrevet i virksomhetens interne data. Disse tapskategoriene er følgende:

1. *Internt bedrageri*
2. *Eksternt bedrageri*
3. *Ansettelsesvilkår og sikkerhet på arbeidsplassen*
4. *Kunder, produkter og forretningspraksis*
5. *Skade på fysiske eiendeler*
6. *Avbrudd i drift eller systemer*
7. *Oppgjør, levering og annen transaksjonsbehandling*

Disse indikatorene skal hjelpe selskapene med å bygge opp et vurderingsgrunnlag av interne data for å beregne operasjonell risiko. I kapitalkravforskriften finnes det ingen videre bestemmelser om hvordan selskaper skal vurdere eksterne data og scenarioanalyser. Ettersom det ikke er noen banker som benytter seg av AMA- metoden i dag, kan dette indikere at metoden er for kompleks til å beregne kapitalen for operasjonell risiko. Men disse tapshendelseskategoriene vil kunne hjelpe selskaper med å identifisere operasjonelle risikoer.

7.3 Håndtering og identifisering av operasjonell risiko

Operasjonell risiko er et risikoområde som viser seg å være forholdsvis komplekst. Operasjonell risiko kan være vanskelig å identifisere, som igjen gjør det vanskelig å beregne sannsynlighet og konsekvens. Kompleksiteten gjør det derfor vanskelig å styre og kontrollere operasjonelle risikoer. Selv om Basel II- og Solvens II- direktivene har flere likheter eksisterer det ingen bransjespesifikke tilnærminger på styring og håndtering av operasjonell risiko i finansbransjen. Mangel på bransjespesifikke tilnærminger diskuteres i en artikkel utgitt av Den Norske Veritas (DNV 2009). Her kommer det frem at de prinsippene og definisjonene som er utarbeidet for å håndtere og operasjonalisere operasjonelle risikoer er tildels upresise, generelle og mangelfulle (DNV 2009: 2). Om det er mulig å ha en felles tilnærming til håndtering av operasjonelle risikoer er kanskje vanskelig å oppnå i praksis. Risikobildet i forsikringsvirksomhet og bankvirksomhet har ikke samme tilnærming.

Både Basel II og Solvens II inneholder krav om kvantifisering av operasjonell risiko. Denne type håndtering og tilnærming til operasjonell risiko er tilsynelatende ikke så veldig enkel å utføre i praksis. For hvordan er det mulig å gjøre en presis kvantifisering av eksempelvis menneskelige feil eller terrorhandlinger? Gitt at dette er kvantifiserbart, hvordan vet man at en har satt av nok kapital til å dekke disse hendelsene?

For å kunne avgjøre om en operasjonell risiko er kvantifiserbar er det viktig å forstå at operasjonell risiko utgjør en dimensjon i alle risikokategorier. Det er viktig å forstå bredden av operasjonell risiko og hvordan den påvirker andre risikokategorier. Enkelte betegner operasjonell risiko som en prosessrisiko, som angår hele virksomheten (DNV 2009: 2). Det er også viktig ikke å tolke operasjonell risiko som en "restrisiko" til allerede eksisterende risikokategorier i et selskap (DNV 2009: 2). Ved å ha en bred tilnærming til styring av operasjonell risiko, vil identifiseringen og håndteringen være lettere.

En annen måte å håndtere risikoer på er å benytte seg av et helhetlig rammeverk for risikostyring, som setter alle risikokategoriene i en sammenheng. Et helhetlig rammeverk skal sy sammen alle risikokategoriene og vise hvordan de påvirker hverandre, betydningen de har hver seg, og hvilke muligheter som finnes for å påvirke, velge og styre risikoene. Et eksempel som viser hvorfor det er viktig med et helhetlig syn på risikostyring, er konsekvensene. En operativ feil som feiltasting kan få store økonomiske konsekvenser. Hvordan et selskap kan gjennomføre en risikostyringsprosess viste vi i kapittel 6.

I håndteringen av operasjonell risiko er det viktig å ha et systemperspektiv. Operasjonell risiko og IT henger som regel sammen, og det er viktig å ha et systemperspektiv ved identifisering av operasjonell risiko (DNV 2009: 2). Sammenhengen mellom operasjonell risiko og IT- risiko er noe Finanstilsynet ser på i sitt tilsynsarbeid.

Omdømmerisiko er ikke en del av definisjonen av operasjonell risiko i Solvens II- eller Basel II- direktivets krav til kapitaldekning. Dette er et risikoområde som må vurderes særskilt. Per i dag eksisterer det ingen krav til at omdømmerisiko må integreres i håndteringen av operasjonell risiko. Men sammenhengen mellom operasjonell risiko og omdømmerisiko henger tett sammen. Det er naturlig å ta det inn i identifiseringsfasen (DNV 2009: 2).

Hvordan man kan lykkes i å håndtere operasjonell risiko har fortsatt ingen fasit. Hvilke risikoer man skal ta høyde for, hvordan beregne sannsynlighet og konsekvens, samt å sette en presis beregning av risikoene er tilnærmet lik umulig. Det vil alltid inntreffe hendelser det ikke er mulig å forberede seg på, og som vil utgjøre en trussel for et selskap. Det som imidlertid er viktig for å forhindre at risikoer inntreffer er å skape en god kultur rundt viktigheten av rutiner og retningslinjer, og gode holdninger til det risikoarbeidet man gjør.

7.3.1 Identifisering av operasjonell risiko

I dette delkapittelet vil vi vise hvordan et bankselskap bruker kontrollspørsmål knyttet til hendelser for å identifisere operasjonell risiko. Disse kontrollspørsmålene viser hvordan man i

praksis kan danne et grunnlag for å kvantifisere operasjonell risiko. Norges Bank Investment Management (NBIM) har definert operasjonell risiko i sin årsrapport 2010 som (NBIM 2010: 1):

> *(…) risiko for økonomisk tap eller tap av omdømme som følge av svikt i interne prosesser, menneskelige feil eller systemfeil, eller andre tap som skyldes eksterne forhold som ikke er en av konsekvens av markedsrisikoen i Statens pensjonsfond utland.*

Styringen av operasjonell risiko i NBIM foregår systematisk ved å identifisere hva som kan gå galt og mulige konsekvenser (forventede tap). De jobber også for å redusere sannsynligheten for at noe kan gå galt og hvordan de skal minimere konsekvensen (uventede tap).

NBIM har en bred tilnærming til operasjonell risikostyring. De hevder at operasjonell risikostyring omhandler alle aktivitetene i NBIM. I risikostyringsprosessen fokuserer de på hva som kan gå galt, hvor galt det kan gå, og hva de kan gjøre for å redusere risikoen. I sin årsrapport har NBIM gitt et bilde som viser utfordringer med operasjonell risikostyring. I overført betydning kan disse hendelsene benyttes av forsikringsselskaper ved identifisering av operasjonell risiko. Spørsmålene som er knyttet til hendelsene er (NBIM 2010: 1-2):

- *Handler forvalteren innenfor sitt mandat?*
- *Hva skjer hvis den som skal utføre handelen misforstår beskjeden fra porteføljeforvalteren?*
- *Hva om noen ved uhell legger inn feil verdier i systemene?*
- *Hva om noen eksternt eller internt forsøker å svindle oss?*
- *Hva om systemene ikke fungerer slik de skal?*
- *Hva slags internkontroll skal vi ha på plass for å sikre at denne kjeden av aktiviteter gjennomføres på en robust måte?*
- *Det vil aldri være nullrisiko, så hva er akseptabelt?*

Utfordringen med operasjonell risikostyring er å svare på slike spørsmål, som kan virke vanskelig å svare og håndtere. Hvis disse hendelsene inntreffer kan det være vanskelig å fastsette omfanget og konsekvensen, som gjør det vanskelig å anslå den totale størrelsen for uønskede tap. NBIMs hovedstyret har fastsatt toleransegrensen av alle uønskede hendelser i løpet av et normalår til under 500 millioner kroner, som er et bruttotall som omfatter gevinster og tap. Med gevinst menes positive utfall av uønskede hendelser (NBIM 2010: 2).

7.4 Styring av operasjonell risiko

Vi vil i dette delkapittelet legge frem to eksempler av hvordan styring av operasjonell risiko praktiseres i banksektoren. Hvordan bankene styrer operasjonell risiko kan være nyttig lærdom for forsikringsselskaper[41].

7.4.1 DNB – et eksempel på styring av operasjonell risiko

Vi vil her beskrive hvordan operasjonell risikostyring fungerer i praksis i DNB[42]. Vi har benyttet en artikkel som bakgrunnsinfo skrevet av Saltkjel (2010).

DNB har blant annet endret organisasjonsstrukturen etter at kravene fra Basel II-direktivet ble innført. DNB har en forvaltningskapital på 2 billioner kroner per 30.09.10 og 13 300 årsverk. Dette gjør selskapet til det største finanskonsernet i Norge. Med ca 2,3 millioner privatkunder og over 200 000 bedriftskunder vil ”worst case”- eller bare ”bad-case”- scenarier kunne få store konsekvenser for selskapet og for samfunnet. I artikkelen har forfatteren intervjuet Bjørn Tore Larsen, som er leder for seksjon operasjonell risikostyring og compliance i DNB. I tillegg innehar han rollen som GCO (Group Compliance Officer). Hans seksjon har valgt å samle operasjonell risikostyring og compliance (Saltkjel 2010: 8). Som ved operasjonell risiko er compliance et område som man selv kan påvirke gjennom kvalitet i prosesser og systemer.

Tidligere ble det rapportert fra styringsfunksjonene og til CFO, men etter kravene fra Basel II ble innført har de opprettet en funksjon som de kaller ”risikostyring konsern”. Denne funksjonen har 65 årsverk, og inneholder de tidligere risikostyringsfunksjonene som skal tydeliggjøre risikostyringen i konsernet (Saltkjel 2010: 8). Tidligere foregikk risikostyringen mer ”silo- vis” i risikostyringsfunksjonene, som ikke var like effektiv.

DNB bruker standardmetoden etter Basel II, og ved bruk av standardisert metode må selskapet forholde seg til strenge rapporteringskrav. Kunnskap om operasjonell risiko skal anvendes i styring av virksomheten, og i tillegg er det et krav fra Basel II om at hendelser skal registreres på en systematisk måte (Saltkjel 2010: 10). Styring av operasjonell risiko i egenvurderingen (ICAAP)[43] gjøres i DNB av linjelederne. De har ansvar for å svare på 56 utsagn fordelt på syv tapshendelseskategorier, innenfor operasjonell risiko (Saltkjel 2010: 9). I

[41] Vi velger å bruke to bankeksempler for å vise hvordan styring av operasjonell risisko kan gjøre i praksis. Bakgrunnen for at vi bruker banksektoren som eksempel er fordi de allerede styrer operasjonelle risikoer etter Basel II- direktivet.
[42] Tidligere DnB NOR. Endret navn fra DnB NOR til DNB den 11.11.2011.
[43] ICAAP er motstykket til forsikringsselskapenes ORSA.

tillegg til denne egenvurderingen gjør banken også en annen type vurdering, hvor hensikten er å avdekke konsernovergripende risikopunkter relatert til operasjonell risiko som kan påføre selskapet et negativt resultat. Denne vurderingen er en prosess som inkluderer hele organisasjonen og skjer en gang i året. Ved å engasjere hele virksomheten skapes det en god kultur som også kan skape engasjement hos de ansatte. Neste steg i prosessen er å gi risikopunktene en risikoverdi. Det er denne verdien som er med på å rangere viktigheten av å iverksette tiltak. Samtidig er det viktig å forestille seg hvordan scenarioet kan utarte seg fra en hendelse til et potensielt tap (Saltkjel 2010: 10).

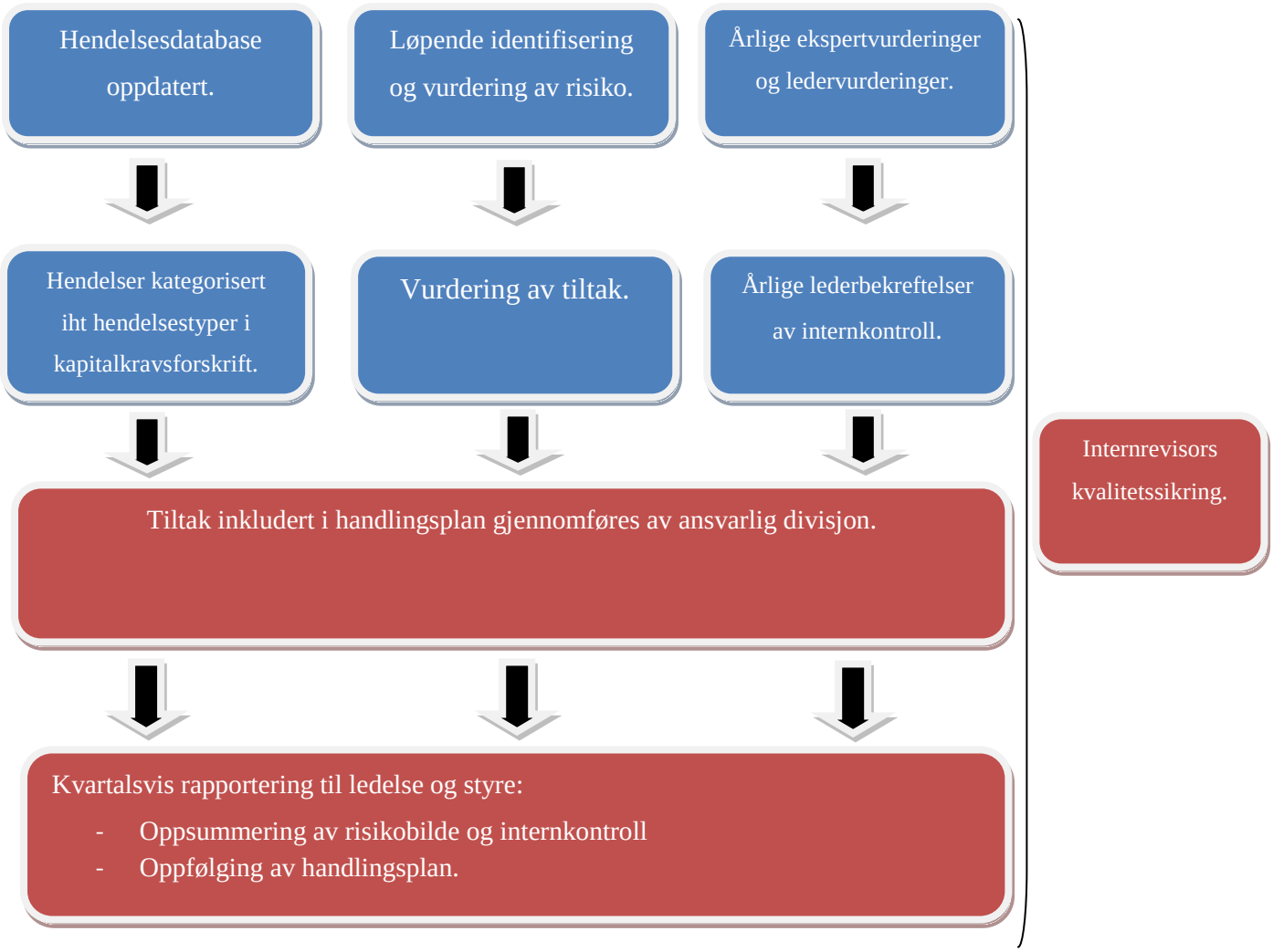
I intervjuet med Larsen fremkommer det at statusrapportering blir sett på som den viktigste delen av risikostyringen. Han sier dette om rapportering: *"Selve prosessen bidrar til engasjement og til å videreutvikle risikotankegangen. Dette er noe av det viktigste vi gjør for å redusere risikoene og skape engasjement rundt hva operasjonell risiko er"* (Saltkjel 2010: 10). DNB har siden 2005 registrert hendelser i en hendelsesdatabase, hvor alle områder i selskapet registrerer hendelser etter gitte kriterier. Av artikkelen kommer det frem at selskapet fra årsskiftet 2010/2011 skal knytte sin hendelsesdatabase opp mot systemet ORX, som er et konsortium av banker som utveksler hendelsesdata (Saltkjel 2010: 11). På spørsmål av hva som er de største utfordringene innen operasjonell risikostyring, svarer Larsen at det er å få opp registreringsraten.

7.4.2 Sparebanken Vest – et eksempel på styring av operasjonell risiko

Vi vil her beskrive hvordan operasjonell risikostyring fungerer i praksis i Sparebanken Vest[44]. Vi har benyttet en artikkel som bakgrunnsinfo skrevet av Øvsthus (2010).

Banken hadde en forvaltningskapital på 105,4 milliarder kroner per 30.09.2010 og 831 årsverk. Som i kapittel 7.4.1.om DNB, har også Sparebanken Vest en egen avdeling for risikostyring og compliance. Denne funksjonen er knyttet til styring, kontroll, rapportering og analyse av risiko. Avdelingen har syv årsverk og har ansvar for bankens risiko- og kapitalstyring. Leder for avdelingen rapporterer til administrerende direktør. Risikostyringen i avdelingen er knyttet opp mot fire risikoområder; kredittrisiko, markedsrisiko, likviditetsrisiko og operasjonell risiko (Øvsthus 2010: 16).

[44] Sparebanken Vest har 63 salgssteder fordelt over de tre vestlandsfylkene og med hovedkontor i Bergen.



Figur 7.1: Et rammeverk for styring av operasjonell risiko i Sparebanken Vest (Øvsthus 2010: 16)

Figur 7.1 viser hvordan Sparebanken Vest har utarbeidet et rammeverk for deres styring av operasjonell risiko. Figuren viser tre veier som gir kilder til informasjon over risikoområdene, og viser avvik i internkontroll. Den første retningen viser en hendelsesdatabase som skal gi informasjon over tapshendelser som faktisk har inntruffet. Den andre retningen viser en løpende identifisering og vurdering av risiko, som skal registrere nye risikoområder og avdekke mulige behov for tiltak. Den tredje og siste retningen skal gi årlige vurderinger av selskapets risiko og internkontroll. Etter informasjon fra disse tre retningene etableres det forbedringstiltak og videre rapportering til styret og ledelse. *"Målet med styringen av den operasjonelle risikoen er å bidra til bankens måloppnåelse, samtidig som etterlevelse av sentrale regler sikres*" (Øvsthus 2010: 16). Sparebanken Vest benytter seg av metodikken i

COSOS `s rammeverk for helhetlig risikostyring. Bakgrunnen for valget av dette rammeverket er Finanstilsynets modul for operasjonell risikostyring (Øvsthus 2010: 16).

I Sparebanken Vest sin årlige vurdering av risiko og internkontroll er det lagt vekt på prosessbeskrivelser som systematisk skal identifisere operasjonell risiko. Ekspertgrupper har vurdert risiko for hvert steg i alle hovedprosesser, og de har benyttet seg av tapshendelseskategoriene i kapitalkravsforskriften som en ”huskeliste”. Etter vurderingen og gjennomgang av risikoene har ekspertgruppen vurdert sannsynlighet og konsekvens for at risikoen vil inntreffe ved hjelp av elektronisk stemmeverktøy (Øvsthus 2010: 17).

Del B) Hvordan praktiserer to forsikringsselskaper styring av operasjonell risiko?

8 Selskap 1 og selskap 2

8.1 Innledning

I dette kapittelet vil vi legge frem offentlig informasjon fra de to forsikringsselskapene vi har vært i kontakt med, som et grunnlag til vår analyse av oppgavens to problemstillinger. Vi vil trekke frem informasjon vedrørende selskapenes størrelse, omfang, kjernevirksomhet og hvilket fokus de har på risikostyring og internkontroll. Informasjonen som vi legger frem har vi hentet fra selskapenes hjemmesider og årsrapporter fra 2010 og 2011. For å anonymisere de selskapene vi har vært i kontakt med har vi valgt å betegne selskapene som selskap 1 og selskap 2.

8.2 Selskap 1

Selskap 1 er et av Norges største livsforsikringsselskap. Selskapets kunder og eiere er; kommuner, fylkeskommuner, helseforetak og bedrifter med tilknytning til offentlig sektor, samt deres ansatte. Hovedforretningsområder til selskap 1 er:

- Livsforsikring
- Skadeforsikring
- Kapitalforvaltning
- Bank og eiendom

Selv om selskapet har ulike forretningsområder er deres hovedprodukt å tilby offentlig tjenestepensjon. Ved inngangen til 2011 hadde 330 kommuner og fylkeskommuner sin pensjonsordning i selskapet. Det samme gjaldt 25 av landets 27 helseforetak og om lag 2 500 bedrifter. Selskapet er ikke børsnotert.

Selskap 1 består av et morselskap og flere datterselskap. Det er til sammen 762 ansatte hvis man ser selskapet under ett. Eksempler på de heleide datterselskapene er eiendom, forsikringsservice og skadeforsikring. Konsernets forvaltningskapital var 291,7 milliarder i 2011, som gjør at selskapet er det største livsforsikringsselskapet i Norge.

8.2.1 Risikostyring og internkontroll i årsrapport 2010 og 2011

Eierstyring og selskapsledelse

Selskapets eierstyring og selskapsledelse er basert på vedtekter, gjeldende lovgivning og interne retningslinjer. I årsrapporten fremkommer det at selskapet har en klar rollefordeling mellom styret, daglig ledelse og kontrollorganer. Selv om selskapet ikke er børsnotert står det i årsrapporten at de allikevel følger den norske anbefalingen for god eierstyring og selskapsledelse.

Styret foretar en årlig gjennomgang av eierstyring og selskapsledelse. Selskapet har som mål å ha en god eierstyring og selskapsledelse. Dette gjelder også i de selskaper de har eierskap. Konsernet benytter balansert målstyring og målkort som en viktig del av den strategiske styringen.

Interne kontrollorganer

Av årsrapporten 2010 fremkommer det at selskapet har opprettet kontrollorganene; kontrollkomité, revisjonsutvalg og internrevisjon. Kontrollkomiteen skal føre tilsyn med selskapets virksomhet. Arbeidet utføres i henhold til forsikringsvirksomhetsloven, selskapets vedtekter og etter instruks gitt av representantskapet. Styret vedtok også å etablere et revisjonsutvalg i 2010. Revisjonsutvalget skal støtte og bistå i å kvalitetssikre styrets arbeid knyttet til finansiell rapportering, revisjon, risikostyring og internkontroll. Konsernets internrevisjon skal foreta uavhengige vurderinger av om selskapets vesentligste risikoer er tilstrekkelig håndtert og kontrollert. Internrevisjonen evaluerer også hensiktsmessigheten og effektiviteten av konsernets styrings- og kontrollprosesser. Internrevisjonen arbeider etter instruks fastsatt av styret og rapporterer direkte til dem.

Operasjonell risiko

Årsrapporten 2010 trekker frem operasjonell risiko som et eget punkt under finansiell soliditet og kapitalforhold. Konsernets operasjonelle risikoer er knyttet til uønskede hendelser som oppstår som følge av svikt i interne arbeidsprosesser, feil begått av ansatte, utilstrekkelig kompetanse eller misligheter og kriminalitet. Det spesifiseres i årsrapporten at alle prosesser i hele verdikjeden er eksponert for ulike typer operasjonell risiko. Selskapet har etablert rutiner for å identifisere, overvåke og treffe nødvendige tiltak som reduserer risikoen for uønskede hendelser. Det er daglig leder som har ansvaret for å ha oversikt og følge opp de avvik som inntreffer. Konsernledelsen utfører årlig en gjennomgang av vesentlige risikoer i

virksomheten. Styret behandler årlig risikovurderinger ut i fra det totale risikobildet. Konsernet har også etablert interne rutiner for uavhengig kontroll og rapportering på ulike nivåer i virksomheten.

Solvens II- direktivet

I årsrapporten fremkommer det at selskapet er godt i gang med forberedelsene til å imøtekomme kravene fra Solvens II- direktivet. Så langt har selskapet gjort tilpasninger til krav om styring og kontroll av risikoer, og foretatt endringer i selskapets soliditetsberegninger. Selskapets egenkapitalmodell sammen med bufferkapital skal styrke soliditeten i selskapet. Selskapet anser seg godt posisjonert til å møte de nye soliditetsreglene.

8.3 Selskap 2

Selskap 2 er en av de ledende aktører innenfor skadeforsikring i Norge. Selskapet ble i 2010 omdannet til et allmennaksjeselskap (ASA), og konsernet ble børsnotert i desember 2010. I dag har selskapet 3120 medarbeidere. I 2011 var driftsinntektene på 19,4 milliarder kroner, mens forvaltningskapitalen utgjorde 88,5 millioner kroner.

Konsernet tilbyr skadeforsikringsprodukter til kunder i Norge, Sverige, Danmark og de tre baltiske landene. I tillegg til skadeforsikring tilbyr de også banktjenester, pensjon og spareprodukter til både privat- og næringslivskunder i Norge. Virksomheten i selskap 2 er inndelt i seks segmenter eller forretningsområder;

- Skadeforsikring – Privat Norge
- Skadeforsikring – Næringsliv Norge
- Skadeforsikring – Øvrig Norden
- Skadeforsikring - Baltikum
- Pensjon og sparing, og Bank

I tillegg til de seks segmentene kommer kapitalforvaltningsenheten, som forvalter konsernets investeringsportefølje.

Kjernevirksomheten i selskap 2 er skadeforsikring. Selskapet har 753 000 privatkunder og 165 000 næringslivs- og landbrukskunder i Norge, og dette gjør selskapet til en stor markedsaktør. For privatkunder i Norge var markedsandelen på 23,8 % og for næringsliv 32 % i 2011.

8.3.1 Risikostyring og internkontroll i årsrapport 2010 og 2011

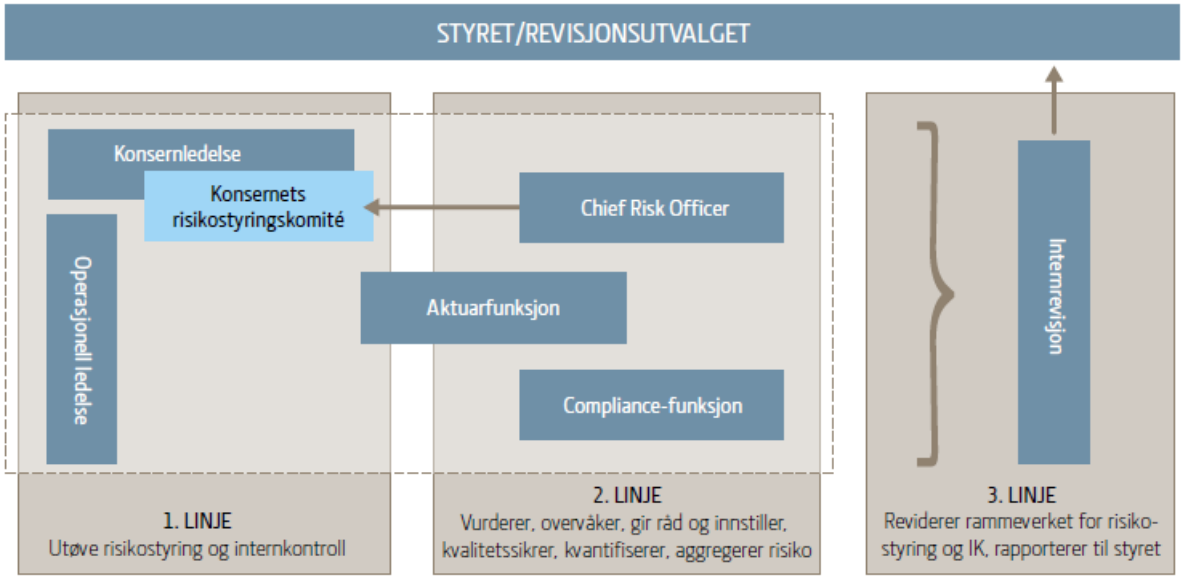
Styring og kontroll

Risikostyring er en integrert del av den daglige virksomheten i selskapet, herunder ligger styring av operasjonell risiko og andre risikokategorier. Risikostyringen består av å identifisere, vurdere og kontrollere selskapets risikoeksponering. I tillegg består risikostyringen av analyser av mulige strategiske beslutningers effekt på risikonivået. Hensikten med dette er å sikre at risikonivået er i tråd med vedtatt risikoappetitt og å støtte selskapets verdiskapning. Ettersom risikostyringen består av selskapets risikokategorier, har de en helhetlig tilnærming til styringsprosessen. Selskapets tilnærming til helhetlig risikostyring skal sikre at ulike risikoer vurderes og håndteres på en konsistent måte.

Formålet med risikostyring i selskapet er todelt. For det første skal ikke risikoeksponeringen overstige risikoevnen. For det andre skal helhetlig risikostyring bidra til verdiskapning for både kunder og eiere. Som en del av risikostyring benytter selskapet seg av målkort som er utarbeidet for konsernets medarbeidere. Målkortet er med på å synliggjøre viktige resultatmål, leveranser og tiltak som igjen kan påvirke konsernets inntjening, verdiutvikling og risikosituasjon.

Ansvarsfordeling

I årsrapportene fremkommer det at linjelederne har ansvaret for den løpende risikostyringen. Dette betyr at vurderingene av risikoene er tett knyttet opp til den forretningsmessige oppfølgingen. Dette gjør at lederne for de enkelte områdene er bevisste på at de også har ansvaret for måloppnåelse innenfor et akseptabelt risikonivå. Styret har naturligvis det overordnede ansvaret for at risikonivået i konsernet er tilfredsstillende mot konsernets soliditet og risikovilje. Styrets overordnede ansvar for risikonivået innebærer å sikre at det eksisterer nødvendige policies, rutiner og rapportering, og se til at lover og forskrifter etterleves. Selskapets konsernsjef har imidlertid det overordnede ansvaret for risikostyringen. Konsernsjefen er leder av konsernets risikostyringskomité som har en todelt rolle. Komiteen har for det første en overvåkende rolle til konsernets totale risikosituasjon. I tillegg har komiteen en rådgivende rolle overfor konsernsjefen innenfor risikostyring.



Figur 8.1: Styringssystemet i selskap 2

Figur 8.1 gir en oversikt over hvordan styringssystemet er organisert i selskap 2, med tre forsvarslinjer. Det er Chief Risk Officer (2. linje) som har ansvaret for å tilrettelegge for risikostyringskomiteens arbeid og fasilitere konsernets internkontrollprosess. I tillegg har selskapet sentraliserte risikokontrollfunksjoner som compliance og aktuar (2. linje). De er uavhengige kontrollnivåer som rapporterer direkte til styret. Konsernet har også en uavhengig internrevisjonsfunksjon (3. linje) som overvåker hvordan risikostyringen og internkontrollen fungerer. Internrevisjonen rapporterer direkte til styret.

9 Metode og dataanalyse

9.1 Innledning

I dette kapittelet vil vi redegjøre for metodene vi har brukt for å få svar på våre hovedproblemstillinger. Vi ønsker å intervjue nøkkelpersoner som er tilknyttet prosessen rundt risikostyring og internkontroll i to forsikringsselskaper. Informantene i selskapene er ledere som har kontrollansvar for selskapets risikostyring og internkontroll. Dermed har de også ansvar for operasjonell risikostyring. Vi har utført fire dybdeintervjuer i selskap 2 og et gruppeintervju med tre personer i selskap 1. Selskapene er i en prosess hvor de skal

imøtekomme kommende krav fra Solvens II- direktivet, som er sentralt ved styring av operasjonell risiko.

Målet med vår undersøkelse er å få oversikt over hvordan styringen av operasjonell risiko foregår per i dag, og hvordan kommende krav påvirker selskapets styring av operasjonell risiko.

9.2 Undersøkelsesdesign

Før en undersøkelse skal gjennomføres må det tas stilling til hvilke type data man trenger. Hvordan man skal skaffe disse dataene, hvordan de skal analyseres, og hvordan undersøkelsen skal gjennomføres, betegnes i forskning som undersøkelsens design (Gripsrud, Olsson og Silkoset 2004: 58). Valg av forskningsdesign avhenger av forskningsspørsmålet. Gripsrud, Olsson og Silkoset (2004) skiller mellom *deskriptive-*, *kausale-* og *eksplorerende* forskningsdesign:

> *Et **deskriptivt design** forutsetter at analytikeren har en grunnleggende forståelse av problemet, og at det har blitt gjennomført tidligere forskning på temaet. Formålet med deskriptiv design er å beskrive situasjonen på et bestemt område. Den skal ikke forklare situasjonen. Observasjon og spørreundersøkelse med et representativt utvalg respondenter fra en målgruppe, er vanlige innsamlingsmetoder som brukes i slike tilfeller.*
>
> *For å kunne undersøke mulige årsaksforklaringer er vi avhengige av et **kausalt design**, som betyr at vi benytter en form for eksperiment. Kausalt design benyttes når man ønsker å undersøke hvordan en variabel kan påvirke verdier på en eller flere variabler. Det stilles høye krav til bevis på årsakssammenheng som gjør at hypoteser og problemstillinger i slike undersøkelser må være svært konkrete.*
>
> ***Eksplorativt design** kan brukes hvis beslutningstakeren har lite kunnskap om problemet som skal undersøkes. Det primære målet med undersøkelsen er å utforske temaet nærmere, siden man på forhånd ikke har noen klar oppfatning av hvilke sammenhenger som kan eksistere. Hovedteknikker for datainnsamling i eksplorativt forskningsdesign vil være dybdeintervjuer eller gruppesamtaler.*

Vår undersøkelse har både elementer av det eksplorative- og det deskriptive designet. Vårt ønske var å gå i dybden på temaet, noe som samsvarer med et eksplorativt design. I følge Gripsrud, Olsson og Silkoset (2004: 59) er en naturlig start i et eksplorativt design å undersøke om det er skrevet noe om temaet (litteraturstudier) før, og deretter undersøke om data er samlet inn av andre (sekundærdata), og tilslutt foreta egen datainnsamling (primærdata). Denne type inndeling har vi i oppgaven. I del A har vi lagt frem krav og beste praksis som norske forsikringsselskaper må forholde seg til ved styring av operasjonell risiko. Dette har vi gjort gjennom litteraturstudier og funnet sekundærkilder. I kapittel 10 vil vi legge frem resultatene fra vår egen studie (primærdata). Resultatene er basert på dybdeintervjuer og gruppeintervju, som er hovedteknikkene for datainnsamling i et eksplorativt design.

Vi mener også at oppgaven har sider som passer til det deskriptive designet. Bakgrunnen for dette er at formålet med denne oppgaven er å beskrive situasjonen på et bestemt område (Gripsrud, Olsson og Silkoset 2004: 61). Vi vil senere i del B bruke vår datainnsamling til å besvare hvordan forsikringsselskaper praktiserer gjeldende krav, og hvordan de ser for seg å praktisere kommende krav fra Solvens II. Før vi startet med oppgaveskrivingen hadde vi en grunnleggende forståelse av oppgavens tema, på bakgrunn av faget "eierstyring og selskapsledelse". Dette gjør at oppgaven har en tilnærming til det deskriptive designet.

9.3 Valg av metode

Ved valg av metode finnes to ulike tilnærminger, *kvalitativ metode* og *kvantitativ metode*. Kvalitativ metode er en tilnærming for analytisk beskrivelse, hvor dataene er i form av tekster som man ønsker å fortolke. Kvantitativ metode egner seg best til å besvare problemstillinger hvor det er ulike data som må fordeles og sammenlignes. I kvantitativ metode arbeider forskeren primært med talldata som statistikk eller data, som er samlet inn i større databaser.

Valg av metode bestemmes av formålet med undersøkelsen. Ved å gjøre en undersøkelse hvor man ønsker å gå i dybden i et tema, er det kvalitativ metode som foretrekkes. Er derimot formålet med undersøkelsen å gjøre en bred og representativ analyse, foretrekkes den kvantitative metoden (Johanessen, Tufte og Kristoffersen 2006: 101). De to tilnærmingene er ikke entydig ulike, men det som skiller metodene er innsamlingen og analyseringen av datamaterialet (Johanessen, Tufte og Kristoffersen 2006: 313).

9.3.1 Kvalitativ metode

Ved valg av metode har vi valgt en kvalitativ tilnærming som gir oss muligheten til å gå mer detaljert inn i undersøkelsen. Ved bruk av kvalitativt design er man ute etter å undersøke hva slags meninger ulike mennesker tillegger ting de erfarer eller opplever (Askeheim og Grenness 2008: 12-13). For å besvare våre problemstillinger velger vi å benytte oss av dybdeintervjuer og gruppeintervjuer. Vår undersøkelse går ut på å innhente primærdata ved at vi selv intervjuer våre intervjuobjekter i forsikringsselskapene. Primærdata kjennetegnes ved at data blir samlet inn direkte i fra mennesker, og blir brukt videre i et spesifikt forskningsprosjekt (Knutsen 2012). Sekundærdata vil i vårt tilfelle være kilder fra eksisterende teorier og rammeverk om risikostyring og internkontroll, med særlig vekt på operasjonell risiko. I tillegg har vi gjort søk for å finne tidligere studier om praktisering av operasjonelle risikoer i forsikringsbransjen. Vår intervjuprosess blir sett på som et personlig intervju, fordi vi vil møte informantene ansikt til ansikt. Våre intervjuobjekter er ikke

randomisert ved tilfeldig utvalg. Informantene er valgt ut etter deres kunnskap og erfaring, og arbeidsområde, på bakgrunn av våre problemstillinger.

9.3.2 Kvalitativt intervju

Kvalitative data samles inn gjennom intervjuer eller observasjoner. Fordelen ved denne metoden er stor grad av åpenhet og fleksibilitet. Formålet med et intervju er i følge Thagaard (2009) å få omfattende informasjon om hvordan andre mennesker kan oppleve sin situasjon, og hvilke synspunkter og perspektiver de har på det temaet som blir tatt opp i intervjuet. Et intervju kan bli sett på som en strukturert samtale hvor målet er å fremskaffe ny kunnskap (Knutsen 2012). Johannessen, Tufte og Kristoffersen (2006) påpeker at det kvalitative intervjuet kan være mer eller mindre strukturert og deler inn intervjuene i fem grupper:

1. *Ustrukturert intervju er uformelt med åpne spørsmål og temaer.*
2. *Semi-strukturert intervju har intervjuguide som utgangspunkt, mens temaet og spørsmålsrekkefølge varierer.*
3. *Strukturert intervju hvor både tema og spørsmålsformuleringer er på forhånd fastlagt.*
4. *Strukturert intervju med faste svaralternativer.*
5. *Gruppeintervju*

Om intervjuguiden

Intervjuguiden er utarbeidet på bakgrunn av våre problemstillinger og fra aktuell teori. Ved utforming av spørsmålene har vi valgt å følge Gripsrud, Olsson og Silkoset (2004:139) sine formuleringer. Disse går ut på å bruke enkle og klare ord, unngå ledende spørsmål, unngå implisitte antagelser, unngå generaliseringer og unngå doble spørsmål. Vi har delt opp intervjuguiden i kategorier som er basert på vår problemstilling. Vi vil analysere likheter og ulikheter i hvordan selskapene definerer, kontrollerer og følger opp styring av operasjonell risiko i dag, samt avdekke hvordan selskapene har forberedt seg på kravene fra Solvens II-direktivet.

Vi har valgt et semi- strukturert design med åpne spørsmål på vår intervjuguide. Guiden skal fungere som en huskeliste og ikke som et spørreskjema. For ikke å måle noe annet enn det som er planlagt er det viktig med korreksjoner, oppfølging av interessante utsagn og nye spørsmål, som er mulig ved en semi- strukturert intervjuguide.

Vi har anslått en lengde på intervjuet til 60 minutter, men intervjuets lengde vil selvfølgelig variere. Dette anslaget opplyste vi om på forhånd.

9.4 Om utvalget

Vårt utvalg består av tre informanter fra selskap 1 og fire informanter fra selskap 2. Vi har samarbeidet med en kontaktperson i hvert av selskapene som vi har hatt løpende kontakt med siden oppstarten av oppgaven. Våre kontaktpersoner har kommet med innspill og ideer underveis i prosessen, og de har vært gode støttespillere for oss. De har funnet informanter som de mener har mest kunnskap og erfaring om risikostyring og internkontroll. Denne måten å finne informanter er en metode som Johanessen, Tufte & Kristoffersen (2006: 106) kaller s*nøballmetoden.* Denne metoden tar utgangspunkt i at man først forhører seg om hvilke personer som har mye kunnskap om temaet som skal undersøkes, og rekrutterer informanter ut i fra dette. I selskap 1 er våre informanter; leder for internrevisjonen, konsernkontroller og direktør for risikostyring og allokering. I selskap 2 er våre informanter: CRO, CCO, leder for internrevisjonen og en direktør for et av forretningsområdene i selskapet.

9.4.1 Fordeler ved dybdeintervju og gruppeintervju

En forutsetning for å kunne gjennomføre et dybdeintervju er at både informant og intervjuer har kunnskap om temaet. Våre informanter er håndplukket av våre kontaktpersoner i selskap 1 og selskap 2, basert på deres kunnskap om vårt tema. Ved å bruke semi- strukturert dybdeintervju som metode gir det oss fleksibilitet og åpenhet. Vi får også muligheten til å oppklare misforståelser umiddelbart, og informantene har en mulighet til å komme med egne innspill og uttalelser. En annen fordel ved dybdeintervju er at intervjueren kan overtale informanten til å fullføre og besvare alle spørsmålene. Intervjueren kan også bli en slags observatør, og observere hvordan respondenten svarer og registrere reaksjoner underveis (Gripsrud, Olsson og Silkoset 2004: 163). Vi har valgt å gi informantene informasjon om oppgavens tema på forhånd. Det gir informanten en mulighet til å forberede seg før dybdeintervjuet. Dette vil styrke svarene, og vi får mer presise og gjennomtenkte svar. Ved et dybdeintervju gis det større muligheter til å få informasjon om informantens erfaringer, kunnskap og verdier (Knutsen 2012). Ved å gjøre et dybdeintervju vil vi kunne avdekke personlige refleksjoner og oppfatninger av hvordan selskapet har prioritert og definert de operasjonelle risikoene. Vi mener at det er de samme fordelene ved et gruppeintervju som ved et dybdeintervju.

9.4.2 Ulemper ved dybdeintervju og dybdeintervju

En ulempe ved dybdeintervjuer er at datamaterialet vi får ut ifra intervjuene kan være vanskelig å sammenstille og analysere (Knutsen 2012). Grunnen til dette er at vi har en semi-strukturert intervjuguide som gjør at det ikke vil være en enhetlig struktur på datamaterialet. Andre faktorer som kan påvirke hvordan informanten svarer, er eksempelvis informantens dagsform, tidspress, eller holdninger informanten har til oppgaven. Disse faktorene er elementer som vi som intervjuere ikke kan påvirke. Det kan gjøre det vanskelig å etterprøve funnene. De svarene vi får er kanskje ikke de svarene noen andre ville ha fått. Vi mener disse ulempene også vil være gjeldende ved et gruppeintervju.

En annen ulempe ved dybdeintervju er at intervjueren kan påvirke svarene til informanten (Gripsrud, Olsson og Silkoset 2004: 163). Vi har et lite utvalg fra selskapene som ikke er representativt. Grunnen til dette er at antall intervjuobjekter er for lavt, og det er dermed ikke mulig å generalisere resultatene (Knutsen 2012). Et dybdeintervju kan være tidkrevende, og slike intervjuer kan ha relative høye kostnader (Gripsrud, Olsson og Silkoset 2004: 163). For vår del har dybdeintervjuene vært meget tidkrevende, men kostnadene har kun vært knyttet til transport frem og tilbake fra intervjustedet. I tilegg til dette mener vi at ved gruppeintervju kan svarene bli mindre nyanserte enn ved dybdeintervju. Det vil være en mulighet for at noen i gruppen svarer annerledes enn hva de ville ha svart ved et dybdeintervju.

9.5 Metodisk kvalitet

Å vurdere den metodiske kvaliteten er nødvendig for å kunne tolke resultatene fra undersøkelsen (Grønmo 2004). Kvaliteten på datainnsamlingen kan ikke vurderes på en generell måte, men den må sees i sammenheng med problemstillingen. Å vurdere kvaliteten på undersøkelsen må gjøres etter at datainnsamlingen er avsluttet. Da kan vurderingen ta hensyn til om svarene på undersøkelsen svarer med problemstillingen, og vurdere om reliabiliteten og validiteten er god nok (Grønmo 2004). Reliabilitet og validitet er de to viktigste kriterieriene i kvalitetsvurderingen av datamaterialet.

9.5.1 Reliabilitet

Reliabilitet[45] handler om påliteligheten til den undersøkelsen man har gjennomført, og om man ville fått samme resultat av undersøkelsen hvis den hadde blitt gjentatt under identiske forhold (Gripsrud, Olsson og Silkoset 2004). Grønmo (2004) definerer reliabilitet som *"graden av*

[45] Et annet ord for reliabilitet er pålitelighet.

samsvar mellom ulike innsamlinger av data om samme fenomen basert på samme undersøkelsesopplegg". Reliabiliteten er høy hvis datamaterialene varierer i liten grad mellom de ulike innsamlingene. Dette gir tillit til data og tolkningen av analysen (Grønmo 2004). Reliabiliteten avhenger også av hvordan datainnsamlingen ble gjennomført.

Ettersom vår datainnsamling baseres på dybdeintervjuer og et gruppeintervju, har vi i utgangspunktet et reliabilitetsproblem. Bakgrunnen for reliabilitetsproblemet er at vi selv har gjennomført intervjuene, og kan dermed ha påvirket intervjusituasjonen og svarene til informantene. I tillegg kan vi ha feiltolket de svarene vi har fått. Men ettersom vi har hatt kontinuerlig kontakt med intervjuobjektene, kan dette styrke oppgavens reliabilitet. Et annet moment er at våre informanter har god kunnskap til fagområdet. Men på en annen side kan reliabiliteten svekkes ved at vi ikke hadde mulighet til å benytte båndopptaker under dybdeintervjuene. Dette betyr at vi har basert våre resultater på notatene vi tok underveis i intervjuet. Dermed har vi ikke gjengitt informantenes egne ord og formuleringer. I gruppeintervjuet benyttet vi båndopptaker slik at vi hadde mulighet til å gjengi informantenes egne formuleringer. Hensikten med våre intervjuer var å få et helhetsinntrykk over hvordan forsikringsselskapene praktiserer gjeldende krav, og ikke gjengi informantenes formuleringer. I tillegg ønsket vi å finne ut hvor langt forsikringsselskapene hadde kommet i prosessen med å lage et system som inkluderer de kommende kravene fra Solvens II- direktivet.

9.5.2 Validitet

Validitet[46] handler om i hvilken grad man kan trekke gyldige slutninger ut i fra de svarene man har fått fra de dataene man har samlet inn. Dette betyr hvor godt man klarer å måle det man har til hensikt å måle eller undersøke. Det er hvordan vi tolker resultatene som valideres, ikke målemetodene eller testene (Gripsrud, Olsson og Silkoset 2004: 72). Selv om reliabiliteten kan være høy og dataene er pålitelige er det ikke bestandig at datamaterialet som er samlet inn har høy validitet. Grunnen til dette kan være at datamaterialet som er samlet inn er lite relevant sett i sammenheng med problemstillingen, og det har da oppstått en systematisk feil (Gripsrud, Olsson og Silkoset 2004: 72). I følge Grønmo (2004) vil validiteten være høy hvis datainnsamlingen resulterer i data som er relevante for problemstillingen. Reliabilitet og validitet henger sammen, og høy reliabilitet er som regel en

[46] Et annet ord for validitet er gyldighet. Validitet kan deles inn i intern og ekstern validitet. Intern validitet gjelder i hvilken grad kausaliteten i undersøkelsen holder mål. Hvis vi påstår av X påvirker Y, må vi være sikre på at det faktisk er X som påvirker Y, og at det ikke er andre variabler som påvirker Y (Gripsrud, Olsson og Silkoset 2004: 69). Ekstern validitet handler om i hvilken grad resultatene fra en studie kan overføres til andre, lignende situasjoner. Ekstern validitet handler om generalisering.

forutsetning for høy validitet. Ved kvalitative intervjuer kan det oppstå dårlig validitet på grunn av feiltolkninger av svarene som ble gitt. Dette problemet kunne ha blitt redusert hvis vi hadde fått mulighet til å benytte båndopptaker i dybdeintervjuene. Ettersom vi fikk mulighet til å benytte båndopptaker under gruppeintervjuet styrker dette deler av undersøkelsens validitet. For å styrke validiteten i oppgavens resultater har vi tatt kontakt med informantene og bedt dem om tilbakemeldinger på våre oppfatninger fra intervjuene.

10 En analyse av operasjonell risikostyring i to norske forsikringsselskaper

10.1 Innledning

I dette kapittelet skal vi analysere resultatene vi fikk fra dybdeintervjuene og gruppeintervjuet fra forsikringsselskapene. Vi velger først å legge frem resultatene fra selskap 1 og deretter fra selskap 2. Resultatene fra intervjuene vil vi strukturere etter våre problemstillinger. For å besvare vår første problemstilling vil vi legge frem resultater som belyser selskapenes risikostyringsprosess knyttet mot operasjonell risiko. For å besvare vår andre problemstilling er vi ute etter å kartlegge hvordan selskapene forbereder seg på å imøtekomme de fremtidige kravene fra Solvens II- direktivet. Basert på dette vil vi trekke frem likheter og ulikheter fra selskap 1 og selskap 2, og gjøre en modenhetsanalyse i slutten av kapittelet.

10.2 Selskap 1

Vi har hatt flere møter med informantene i selskap 1, både før og etter gruppeintervjuet. Dette for å få så presis informasjon som mulig. Gruppeintervjuet ble gjennomført med tre informanter og varte i ca. en og en halv time. I tillegg har vi hatt mailkorrespondanse med alle tre informantene, hvor vi har hatt mulighet til å stille dem spørsmål i etterkant av gruppeintervjuet. En av informantene har også vært vår kontaktperson i selskapet, hvor vedkommende hjalp oss med å finne de rette informantene.

10.2.1 Styring av operasjonell risiko

Selskapet benytter seg av Finanstilsynets definisjon av operasjonell risiko, som igjen er basert på definisjonen i Solvens II- direktivet; *"(…) risikoen for tap som følge av utilstrekkelige eller sviktende interne prosesser eller systemer, menneskelige feil, eller eksterne hendelser"*.
Videre var vi ute etter å finne ut hvordan selskapet identifiserer operasjonelle risikoer. På

spørsmål om hvilke risikokategorier selskapet har definert under operasjonell risiko, kom det frem at selskapet benytter de syv tapshendelseskategoriene. Disse kategoriene er hentet fra kapitalkravsforskriften:

1. *Internt bedrageri*
2. *Eksternt bedrageri*
3. *Ansettelsesvilkår og sikkerhet på arbeidsplassen*
4. *Kunder, produkter og forretningspraksis*
5. *Skade på fysiske eiendeler*
6. *Avbrudd i drift eller systemer*
7. *Oppgjør, levering og annen transaksjonsbehandling*

Identifiseringen av kategoriene har blitt gjort på ledernivå. Dette betyr at ledelsen har lagt føringer for hvilke risikokategorier som skal defineres under operasjonell risiko. Når lederne har hatt en deltagende rolle i identifiseringsfasen, har de større kompetanse og mulighet til å si ifra hvis risikobildet skulle endre seg. Skulle risikobildet endre seg, er det leders plikt og ansvar å rapportere dette videre i organisasjonen.

Ansvarsfordeling

Hver enkelt leder har ansvaret for å kontrollere og følge opp risikoer i sin enhet, og alle risikoene er ”eid” av en konserndirektør. Dette betyr at selskapet har et top- down – perspektiv og et bottom- up – perspektiv. Når det gjelder ansvarsstrukturen ved oppfølging av operasjonell risiko er det konsernsjefen som har det endelige ansvaret. Selv om det finnes et felles styringsdokument for hele konsernet står datterselskapene fritt til å definere egne risikoer, slik at risikoene blir mer tilpasset hvert selskap. Saker eller forhold som er knyttet til risikostyring og internkontroll blir drøftet i datterselskapenes egne styrer, og deretter fremlagt for konsernstyret. Konsernsjefen formidler informasjon fra datterselskapene til styret i morselskapet. I datterselskapene har alle lederne blitt pålagt å skrive et sammendrag av risikostyring og internkontroll i egen avdeling. Dette rapporteres videre til seksjonssjefen, slik at vedkommende får en oversikt over risikostyringen og internkontrollen i seksjonen. Konsernledelsen gjør en skjønnsmessig vurdering av de viktigste risikoene fra seksjonsnivåene, og rapporterer disse til styret. Konsernsjefen bruker også målkort som en rapporteringsmetode ovenfor styret. Styret godkjenner målkortene hvert kvartal.

Direkte avvik fra risikostyringen og internkontrollen fra morsselskapet blir rapportert til styret, men det er avdelingslederen som har ansvaret for å følge opp avviket. Det er den enkelte leder og divisjonssjef som har ansvar for å iverksette tiltak ved hendelser. Etter tre

måneder skal avdelingslederen rapportere om hvordan tiltakene har fungert. I selskapet blir de operasjonelle risikoene rapportert en gang årlig. Selskapet bruker målkort som rapporteringsverktøy. I målkortet fremkommer de overordnede målene til hver enkelt enhet. Hver avdelingsleder har eget målkort som akkumuleres opp til et konsernkort. De operasjonelle risikoene er ikke en del av målkategoriene.

De mest prioriterte risikoene rettet mot livsforsikring

For å få innsikt i hvordan lederne på toppnivå arbeider for å kartlegge selskapets risikobilde, stilte vi et spørsmål om hvordan selskapet prioriterer risikoer knyttet til deres kjernevirksomhet. Hensikten med dette var å se hvordan selskapet prioriterer risikoene, og om disse kan identifiseres med de fire risikokategoriene (se kapittel 3.5). På dette spørsmålet svarte selskapet at de ikke har definert eller vurdert hvilke konkrete risikoer som har høyst prioritet. Videre svarer de at risikoer med høy sannsynlighet og konsekvens alltid er de mest prioriterte risikoene. Eksempler på dette er å ikke miste kunder, og å forvalte kapitalen hensiktsmessig. For å sikre at kapitalen blir forvaltet på en god måte, foregår det daglig oppfølging. Informantene trekker frem at faren for å gjøre feil kan påvirke soliditeten til selskapet. Denne type feil kan være basert på menneskelig svikt, IT- risiko og overholdelse av rutiner og retningslinjer. Videre utdyper informantene hvordan selskapet er utsatt for risikoer de ikke kan håndtere, som iboende risikoer. Et eksempel på dette er at den forventede levealderen øker hvert år.

Når selskapet arbeider med å prioritere operasjonelle risikoer deler de risikoene inn etter utfallet. Selskapet deler utfallene inn i forventet tap og uventet tap. Informantene mener at det er mest utfordrende å se på de uventede tapene av de operasjonelle risikoene. Grunnen til dette er at operasjonell risiko ofte oppstår av en uventet hendelse, slik at det er umulig å estimere et forventet tap.

Rammeverk, lover og regler

Vi var ute etter å få et innblikk i hvordan selskapet forholder seg til gjeldende krav og rammeverk i praksis. Først spurte vi om selskapet har benyttet et teoretisk rammeverk som grunnlag til sin risikostyringsprosess. Informantene mente at selskapet ikke har tatt utgangspunktet i ett teoretisk rammeverk, men at de har hentet inspirasjon fra COSO. Selskapet har brukt COSO som et hjelpemiddel og tilpasset det til sin egen organisasjon. Selskapet følger de lover og regler som de er underlagt. Ved styring av selskapets risikoer

nevner informantene at de har tatt mest hensyn til internkontrollforskriften og kapitalforvaltningsforskriften[47]. I følge kapitalforvaltningsforskriften § 2-1 1. ledd skal *"selskapet ha oversikt over, helhetlig styring av, og god kontroll med de risikoer som oppstår ved selskapets kapitalforvaltning"*.

Fremtidige krav til styring av operasjonell risiko

Etter at Solvens II- direktivet ble introdusert mener informantene at fokuset på operasjonell risiko har endret seg. Informantene mener at direktivet har mange positive og negative sider, men flest positive. En positiv side mener de er kravet om å kvantifisere operasjonelle risikoer som en fornuftig og nyttig prosess. Angående hvor langt selskapet har kommet med å møte de fremtidige kravene, mener informantene at selskapet er der de bør være. Informantene sier at selskapet fortsatt har noen utfordringer igjen, som de selv er klar over og vil følge opp. En av utfordringene er at de fortsatt ikke har noen samlede risikomål for hver risikokategori. Selskapet har frem til nå hatt størst fokus på markedsrisiko, og har ikke laget noen felles risikomål for forsikringsrisiko og operasjonell risiko.

Vi var ute etter å finne ut hvor stor del styring av operasjonell risiko skal utgjøre i selskapets risikostyring og internkontroll. Selskapet har ikke satt av konkrete midler (årsverk og kapital) til å dekke de fremtidige kravene til operasjonell risiko. De antar at ca. 5 årsverk skal ha fokus på operasjonelle risikoer, men at disse personene også vil få andre arbeidsoppgaver.

Kvantifiserbare risikoer

Selskapet startet i fjor med å kvantifisere operasjonelle risikoer. De vil fortsette med dette ettersom kvantifisering av operasjonelle risikoer er et krav fra Solvens II- direktivet. Hvis det oppstår risikoer som er vanskelig å kvantifisere, ønsker selskapet en diskusjon rundt risikoen. Ettersom selskapet er i startfasen med å kvantifisere operasjonelle risikoer, ser de på kvantifiseringen som en dynamisk prosess. Å kvantifisere operasjonelle risikoer vil komme frem som en del av ORSA- prosessen. Selskapet ser for seg å kvantifisere operasjonelle risikoer som kan påføre virksomheten tap av en viss størrelse. Dette betyr at det er kun de operasjonelle risikoene som kan gi selskapene økonomiske tap av en viss størrelse som vurderes i ORSA. En av informantene ga oss et eksempel på dette. I et lite prosjekt med 5-10

[47] Forskrift om livsforsikringsselskapers og pensjonsforetaks kapitalforvaltning 17. desember 2007 nr. 1457.

prosent budsjettsprekk vil ikke bli sett på som en vesentlig operasjonell risiko. Men skjer samme budsjettsprekken i et større prosjekt, kan budsjettsprekken bli klassifisert som en vesentlig risiko. Et forslag til ORSA er under utarbeidelse og skal bli behandlet som en styresak i mai 2012.

Et krav fra Solvens II- direktivet er at forsikringsselskapene må opprette en hendelsesdatabase. En slik database skal inneholde hendelser og nesten- hendelser. Per i dag har ikke selskapet noen hendelsesdatabase hvor hendelser eller nesten- hendelser registreres, men hendelsene blir registrert i avdelingene og i divisjonene. Selskapet er i gang med en prosess for å lage en felles hendelsesdatabase. Informantene ser for seg at det kan bli et problem å sette grenser for hvilke hendelser som skal loggføres.

Refleksjoner

En av informantene bemerket at han syntes det var rart at vi brukte begrepet styring av operasjonell risiko. Vedkommende mener at det er vanskelig å styre en operasjonell risiko, og at man heller konstaterer en operasjonell risiko. Informanten hevder at en operasjonell risiko er vanskelig å overvåke og rapportere løpende, ettersom hendelsen kan oppstå uten forvarsel. Et eksempel på dette er når en trader kjøper istedenfor å selge aksjer ved en feiltakelse.

På spørsmål om selskapet har hentet inspirasjon eller kunnskap fra banken i konsernet, svarer informantene at de ikke har gjort dette. Bakgrunnen for dette er at banken i selskapet er veldig liten sammenlignet med forsikringsvirksomheten, og er kun ett år gammel. Men selskapet har eksterne prosjektledere på Solvens II- prosjektet.

På spørsmål om hvilke utfordringer selskapet har vedrørende de fremtidige kravene, mener i informantene at det kan bli vanskelig å få med seg resten av organisasjonen. Dette innebærer å få de ansatte og lederne til å tenke på risikoer i det daglige. I tillegg mener en av informantene at Finanstilsynet bør lage retningslinjer som er lett å forstå, slik at lederne forstår hvordan de kan følge og fange opp uheldige hendelser. Informantene hevder at dette vil påvirke hvordan operasjonell risiko kan bli mer forankret i organisasjonen. En annen informant mener at det er skrevet mye teori om risikostyring, men at de savner gode eksempler på hvordan selskaper skal gjøre dette i praksis.

10.3 Selskap 2

For å få informasjon fra dette selskapet har vi gjennomført fire dybdeintervjuer med fire ledere som har ulike posisjoner og roller i selskapet. I dette selskapet har vi hatt to

kontaktpersoner. Vår første kontaktperson i selskapet hadde mye erfaring og kunnskap om risikostyring og internkontroll, og var meget engasjert i temaet operasjonell risiko. Gjennom mailutveksling og flere møter med vedkommende har vi fått en god introduksjon til selskapet, og flere innspill til oppgaven. I tillegg var kontaktpersonen vår testpilot på intervjuguiden. Hans sjef ble vår andre kontaktperson, og det var han som hjalp oss med å finne de "riktige" informantene. Denne kontaktpersonen er også en av de fire informantene.

10.3.1 Styring av operasjonell risiko

Selskapet har definert operasjonell risiko i tråd med Basel II- direktivet. Deres definisjon for operasjonell risiko er følgende: *"risikoen for tap som følge av utilstrekkelige eller sviktende interne prosesser eller systemer, menneskelige feil, eller eksterne hendelser"*. Selskapet hadde allerede en definisjon av operasjonell risiko før Solvens II- direktivet ble introdusert, men ettersom disse er like er definisjonen fortsatt gjeldende. Flere av informantene var usikre på om selskapet i det hele tatt hadde definert operasjonell risiko, men at selskapet sannsynelig hadde nedskrevet en definisjon.

For å identifisere risikoene under operasjonell risiko har selskapet benyttet seg av de syv tapshendelseskategoriene fra kapitalkravsforskriften, og i tillegg har de lagt til compliance- risiko. Disse syv tapshendelseskategoriene og compliance- risiko utgjør sammen identifiseringsgrunnlaget for operasjonell risiko. De åtte risikokategoriene er:

1. Internt bedrageri
2. Eksternt bedrageri
3. Ansettelsesvilkår og sikkerhet på arbeidsplassen
4. Kunder, produkter og forretningspraksis
5. Skade på fysiske eiendeler
6. Avbrudd i drift eller systemer
7. Oppgjør, levering og annen transaksjonsbehandling
8. Compliance

<u>Ansvarsfordeling</u>

Risikoprosessen i selskapet har både et top- down perspektiv og bottom- up perspektiv. Dette innebærer at det foregår en evaluering av utfordringene og risikoene på toppnivå. Det er imidlertid avdelingene som har den daglige styringen og ansvaret for å håndtere risikoene. Hver enkelt avdeling skal rapportere oppover i organisasjonen hvis de ser endringer eller nye utfordringer i risikobildet. Vesentlige risikoer skal rapporteres videre til konsernsjefen som igjen rapporterer til styret. Ingen risiko skal bli rapportert til styret før avdelingen har fått mulighet til å iverksette tiltak og korrigere hendelsen selv. Selskapet har en egen komité,

Group Risk Commitee (GRC), som er følger opp selskapets risikoer. Selskapets GRC *"(…) er et rådgivende og utredende organ for konsernsjef i risikorelaterte saker. GRC skal belyse konsernets risikoeksponering og risikostyring overfor konsernsjef, og foreslå eventuelle tiltak. Konsernsjef fastsetter GRCs sammensetning, agenda og møtefrekvens"*[48].

Selskapet bruker målkort som et rapporteringsverktøy. Her har hver enkelt ansatt et ansvar for å følge opp sine risikoområder. Når det oppstår avvik fra målkortet, har selskapet utarbeidet flere interne retningslinjer som de ansatte skal følge for å håndtere avviket. Det er imidlertid et lederansvar å følge opp de risikoene som avdelingen står ovenfor. Målkortene blir fulgt opp kvartalsvis. I selskapet er det CRO som følger opp og "eier" risikoene som den enkelte leder har ansvaret for. Dette blir gjort ved å bruke lederens målkort. Hver enkelt ansatt har et målkort hvor selskapets strategi kommer tydelig frem. Her fremkommer konsernmålene, mål for avdelingen og personlige mål. Internrevisjonen følger opp risikoene ved å foreta stikkprøver eller lage statistikker over de viktigste risikoene. Ansvaret til compliance- funksjonen er i hovedsak å følge opp at selskapet etterlever gjeldende lover og regler.

Selskapet er opptatt av å følge opp og kontrollere risikoer. Et eksempel på dette kan være at en kapitalforvalter får honorar etter hvor mange operasjonelle feil som har oppstått hos forvalteren i løpet av en viss periode. I utgangspunktet har kapitalforvalteren et fast honorar, men skjer det ofte operasjonelle feil, så reduseres honoraret på grunn av dette. På denne måten setter selskapet et press på kapitalforvalteren til å være opptatt av operasjonelle risikoer.

<u>De mest prioriterte risikoene rettet mot skadeforsikring</u>

Selskapet har ikke definert de mest prioriterte risikokategoriene for operasjonell risiko, men de har definert de mest prioriterte risikokategoriene for hele konsernet. De mest prioriterte risikokategoriene for konsernet er blant annet at:

- konsernet ikke skal klare å skape økonomisk vekst
- konsernet skal miste kunder
- konsernet står overfor et sammenbrudd i euro- sonen
- konsernet ikke skal klare å følge endringene av regulatoriske lover og regler
- konsernet ikke skal lykkes utenfor norske grenser

[48] Dette har vi hentet fra selskapets konsernpolicy.

En av informantene hevder at disse risikoene i utgangspunktet er ”forretningsrisikoer”, men som allikevel kan sees i sammenheng med operasjonelle risikoer. Operasjonelle risikoer kan være en utløsende årsak til ”forretningsrisikoene”, og da fungerer ikke det opprinnelige tiltaket.

Selskapets operasjonelle risikoer har ikke høyest prioritet, men alle risikoene er allikevel inkludert i selskapets risikounivers. Når det gjelder operasjonell risiko har internrevisjonen og compliance- funksjonen særlig fokus på omdømmerisiko og compliance-risiko. Bakgrunnen for dette er at selskapet er opptatt av å minimere omdømmerisikoen, ettersom svekket omdømme kan føre til mindre verdiskapning for selskapet. Høyest prioriterte compliance- risikoer rapporteres direkte til styret. Eksempler på dette kan være pålegg fra myndighetene, eller at ansatte i selskapet handler i strid med interne retningslinjer.

Rammeverk, lover og regler

På spørsmål om selskapet har tatt utgangspunkt i et teoretisk rammeverk til sin risikostyringsprosess, svarte informantene at selskapet i hovedsak har brukt COSO ERM-rammeverket (2004). Selskapet har ikke fulgt dette rammeverket slavisk, men de har brukt det som et hjelpemiddel. En av informantene hevder at selskapet har hatt en mer praktisk tilnærming til risikostyringen enn slik rammeverket er utformet. En av de andre informantene var usikker på om selskapet hadde benyttet et spesifikt rammeverk i risikostyringen. Informantene trekker frem at de følger de generelle retningslinjer, lover og regler som selskapet er underlagt. Informantene trekker frem internkontrollforskriften og IKT- forskriften som selskapet har tatt hensyn til ved styring av risikoer.

10.3.2 Fremtidige krav til styring av operasjonell risiko

På spørsmål om hvordan styring av operasjonell risiko har endret seg etter Solvens II-direktivet ble introdusert, svarte en av informantene både ja og nei. Uavhengig av Solvens II-direktivet mente informanten at det ville ha blitt endringer i forsikringsbransjens praksiskrav. En annen informant trakk frem hvordan kravene fra ORSA har ført til store endringer ved større fokus på styring av operasjonell risiko. Den største endringen er knyttet til egenrapporteringen, hvor selskapet må vise at de følger opp de interne systemene og kontrollene. En annen informant trekker frem at de nye reglene setter større krav til å følge opp de operasjonelle risikoene. Videre sier informanten at et hendelsesregister også vil bli en endring for selskapet.

Informantene mener at selskapet har kommet langt med å utarbeide systemer for risikostyring og internkontroll som skal tilfredsstille de kommende kravene fra Solvens II- direktivet. Selskapet har definert funksjoner for lederne i retningslinjene, hvor ledelsesstrukturen og rammeverkene er på plass. De jobber også med å få til en støttefunksjon for rapporteringen. Easy- risk er et elektronisk verktøy som også snart er på plass i selskapet. Systemet skal blant annet bestå av en database hvor hendelser og nesten- hendelser skal registreres, og systemet skal brukes av hele virksomheten. Men selskapet har ennå ikke tenkt på hvor skillet skal gå mellom hva som er en hendelse, og hva som er en nesten- hendelse. Selskapet har skissert ORSA et par ganger, og vist det for styret. Men den endelige ORSA er fortsatt ikke komplett. ORSA vil ikke inneholde egne retningslinjer for operasjonell risiko. En av informantene er usikker på om selskapet noen gang kommer til å ha dette. Selskapet ser for seg å benytte intern modell for å beregne solvenskapitalkrav, hvor de har hatt en tett dialog med Finanstilsynet.

På spørsmål om hvor stor del av operasjonell risiko skal utgjøre i selskapets risikostyring og internkontroll, fikk vi til svar at det vil være ansatte i de ulike avdelingene som jobber med operasjonell risiko som ett av flere arbeidsområder. Eksempler på slike avdelinger kan være i distribusjonsapparatet, skadeoppgjør og IKT- sikkerhet. I selskapets internrevisjon har de lenge hatt fokus på operasjonell risiko, og i denne avdelingen jobber nå fire årsverk med operasjonell risiko. De som jobber med operasjonell risiko går inn i konkrete prosesser eller i avdelinger, og utfører revisjon.

Kvantifiserbare risikoer

Selskapet skal ikke kvantifisere de operasjonelle risikoene, men bruke indikatorer. Eksempler på en indikator kan være kapasitetsutnyttelse eller overkapasiteten på datasystemet. Oppstår det en situasjon hvor det er overkapasitet på datasystemet, må noen gjøre en vurdering av hva som skal gjøres for at systemet ikke skal kollapse. Andre eksempler på en indikator kan være å ta stikkprøver eller utføre kontroller. Etter at en skadeforsikringssak er ferdig behandlet, kan det i etterkant bli tatt stikkprøver for å sjekke at prosedyrene er fulgt. Disse indikatorene skal skissere hendelser som kan inntreffe, og skal inneholde tiltak som kan iverksettes.

En av informantene begrunner hvorfor selskapet ikke kvantifiserer risikoene. En grunn til dette er at det er problematisk å overvåke de risikoene som er vanskelig å kvantifisere. Operasjonell risiko blir ofte sett på som hendelser som oppstår akutt eller uten forvarsel. Det finnes også eksempler på at selskapet har fått varsler på forhånd. Et eksempel på dette er

nedgang av kunder. Selskapet mister kunder, men man antar at dette kun er forbigående, og at antall kunder snart vil øke igjen. Over tid øker ikke antall kunder. Hvis selskapet ikke har satt i gang tiltak for å øke kundemassen, blir dette en forretningsmessig risiko.

En gang i året må alle avdelingslederne beskrive de operasjonelle risikoene og compliance- risikoene som avdelingen står ovenfor. Dette blir gjort ved å kategorisere de ulike risikoene inn i høy, middels eller lav. Ved å rangere risikoene etter disse kategoriene måler selskapet konsekvensene. IT-sikkerheten er også viktig med tanke på å styre operasjonelle risikoer. Selskapet har strenge sikkerhetsrutiner slik at datasystemene alltid skal være aktive.

Selskapet har et hendelsesregister hvor hendelser skal registreres, men per i dag registreres hendelsene litt ”her og der” i fagavdelingene. I fremtiden skal nesten- hendelser registreres i systemet Easy- risk.

Refleksjoner

På spørsmål om selskapet har hentet inspirasjon og kunnskap fra banken i konsernet, har informantene ulikt syn på dette. En av informantene svarte både ja og nei. Ettersom banken er forholdsvis liten og ny, har det vært vanskelig å sammenligne banken med forsikringsvirksomheten. Allikevel har de hatt dialog med banken, og utvekslet kompetanse og erfaringer. Dette har vært av liten betydning. Men en av informantene mente at selskapet burde ha tatt lærdom og kunnskap fra en internasjonal bank som selskapet har kjøpt opp. Denne banken har et system for å følge opp de operasjonelle risikoene og en hendelsesdatabase. Men dessverre så ble ikke dette videreført eller implementert i selskapet.

Selskapet har brukt ekstern hjelp av PWC for å lage systemer for risikostyring og internkontroll. I tillegg har de benyttet PWC til å utarbeide retningslinjer for styring av operasjonell risiko, og for å imøtekomme kravene fra Solvens II- direktivet.
Informantene mener at hovedutfordringene til implementering av Solvens II- kravene er følgende:

- Å få direktivet forankret i organisasjonskulturen og hos hver enkelt ansatt
- Å få systemet Easy- risk til å fungere, og få det implementert i selskapet
- Hvordan selskapet skal kvantifisere tap som følge av operasjonell risiko
- Å lage en god oversikt over hvilke operasjonelle risikoer selskapet kan bli eksponert for, og finne de fremtidige operasjonelle risikoene som ikke er åpenbare

10.4 Likheter og ulikheter av to forsikringsselskaper

Vi vil nå oppsummere likheter og ulikheter hos de to selskapene vi har undersøkt. Først vil vi se på selskapenes overordnede forskjeller for å vise at selskapene er ulikt organisert. Deretter vil vi trekke frem likheter og ulikheter som oppsummerer resultatene fra intervjuene. Til slutt vil vi gjøre en modenhetsanalyse basert på våre to problemstillinger. Her vil vi gjøre en analyse av hvor godt selskapene styrer operasjonelle risikoer i dag, som viser hvor modne selskapene er for å imøtekomme fremtidige krav.

	SELSKAP 1	**SELSKAP 2**
Hva er selskapets kjernevirksomhet?	Livsforsikring	Skadeforsikring
Hva var selskapets forvaltningskapital i 2011?	291,7 milliarder	88,5 milliarder
Er selskapet børsnotert?	Nei	Ja
Hvem er selskapets eiere?	Kommuner, fylkeskommuner, helseforetak og bedrifter med tilknytting til offentlig sektor	Stiftelse og aksjeeiere
Hvor mange ansatte i 2011?	762	3120

Tabell 10.1: Sammenligning av selskap 1 og selskap 2

Tabell 10.1 gir en oversikt over selskapenes hovedforskjeller. Selv om selskapene er ulike på mange vesentlige områder, mener vi at dette ikke vil påvirke hvordan selskapene styrer operasjonelle risikoer. Uavhengig av selskapenes eierforhold må selskapene arbeide for å sikre hensiktsmessig og effektiv bruk av ressurser. Selv om skade- og livsforsikringer inneholder ulike produkter, omgir de seg med de samme operasjonelle risikoene. Til tross for de store forskjellene har vi allikevel grunnlag for å diskutere likheter og ulikheter mot våre problemstillinger.

	SELSKAP 1	SELSKAP 2
Har selskapet en definisjon av operasjonell risiko, og er den i tråd med Solvens II?	Ja	Ja
Har selskapet identifisert risikokategorier under operasjonell risiko?	Ja	Ja
Har selskapet kombinert compliance- risiko inn under operasjonell risiko?	Nei	Ja
Har selskapet en prosess for å analysere de operasjonelle risikoene?	Ja	Ja
Har selskapet en prosess for å håndtere og følge opp operasjonelle risikoer?	Ja	Ja
Bruker selskapet målkort i rapporteringsprosessen?	Ja	Ja
Har selskapet en prosess for å overvåke operasjonelle risikoer?	Ja	Ja
Har selskapet benyttet seg av et teoretisk rammeverk i risikostyringsprosessen?	Ja	Ja
Har selskapet et top- down og bottom- up perspektiv på ansvarsfordelingen?	Ja	Ja
Har selskapet en overordnet som ”eier” risikoene?	Ja	Ja
Har selskapet en compliance-funksjon?	Nei	Ja
Har selskapet en risikostyringsfunksjon?	Nei	Ja
Har selskapet en internrevisjon?	Ja	Ja
Har selskapet utarbeidet en skisse til ORSA?	Ja	Ja
Har selskapet planlagt å benytte seg av intern modell for å beregne solvenskapitalkravet?	Nei	Ja
Har selskapet planlagt å kvantifisere operasjonelle risikoer?	Ja	Nei
Har selskapet utarbeidet et system for å registrere hendelser og nesten- hendelser?	Nei	Ja

Tabell 10.2: Likheter og ulikheter mellom selskap 1 og selskap 2

I tabell 10.2 har vi presentert våre vurderinger av likheter og ulikheter mellom selskap 1 og selskap 2. Disse vurderingene er basert på offentlig informasjon, gruppeintervjuer, dybdeintervjuer, møter, mailkorrespondanse og telefonsamtaler. Dette er informasjon vi har fått underveis i prosessen, og skisserer vår oppfatning av selskapene. Ut i fra tabell 10.2 ser det ut til at selskapene har mange likheter, men disse svarene er mer nyanserte enn det som fremkommer. Dette vil vi diskutere nærmere.

Selskap 2 har definert åtte risikokategorier under operasjonell risiko. De har kombinert compliance- risiko under operasjonell risiko som den åttende kategorien. Denne sammenslåingen har vi sett i eksemplene fra banksektoren i kapittel 7. Denne kombineringen har ikke selskap 1 gjort. Av tabell 10.2 fremkommer det at selskap 1 ikke har en compliance-funksjon. For å sikre at selskapet etterlever lover og regler har selskapets konsernkontroller ansvaret for å følge opp compliance- risiko. Selskap 2 har en risikostyringsfunksjon hvor CRO er leder. CRO er den som ”eier” selskapets risikoer og har det overordnede ansvaret for risikostyringsprosessen. Selskap 1 har ikke en slik risikostyringsfunksjon, men en avdeling som ivaretar selskapets risikostyring. Felles for begge selskapene er at det er konsernsjefen som har det overordnede ansvaret for selskapets risikobilde.

Selskapene har ikke en egen prosess som ”bare” skal ha fokus på å styre operasjonell risiko. Men styring av de operasjonelle risikoene er en del av selskapenes risikostyringsprosess. Begge selskapene har en prosess for å analysere de operasjonelle risikoene. Selskap 2 bruker indikatorer som analysegrunnlag for å måle hvordan de operasjonelle risikoene kan påvirke virksomheten. Selskap 1 analyserer risikoene etter høy sannsynlighet og høy konsekvens. De risikoene som er vanskelige å måle blir diskutert enkeltvis. Det er avdelingslederne som håndterer, følger opp, og overvåker de operasjonelle risikoene. Når en risiko med høy konsekvens har inntruffet vil konsernsjefen se etter at tiltak blir fulgt opp. Begge selskapene bruker målkort som et rapporteringsverktøy i risikostyringsprosessen. I selskap 1 har avdelingslederne hvert sitt målkort, men i selskap 2 har både ledere og ansatte målkort. Felles for begge selskapene er at de eksplisitt ikke inkluderer operasjonell risiko i målkortene.

Begge selskapene har utarbeidet en skisse til hvordan selskapets ORSA skal gjennomføres. Selskap 2 startet tidligere enn selskap 1 med å utarbeide selskapets ORSA. Selskap 2 har allerede laget flere forslag til endelig ORSA. En grunn til dette kan være at selskap 2 ser for seg å benytte en intern modell for å beregne solvenskapitalkrav. Selskapene skal kvantifisere alle risikokategoriene i solvenskapitalkravet, som skal beskrives i selskapets

ORSA. Selskap 1 ser for seg å kvantifisere de operasjonelle risikoene, men de er usikre på hvordan. De ser for seg at dette kan bli en krevende oppgave. Selskap 2 har ikke planer om å kvantifisere operasjonelle risikoer. For å håndtere de operasjonelle risikoene har selskapet valgt å bruke indikatorer for å kartlegge de risikoene som kan oppstå.

Selskap 2 har utformet et system, Easy- risk, som blant annet skal inneholde registrerte hendelser og nesten- hendelser. Selskap 1 er i startfasen med å planlegge et slikt system.

10.4.1 Modenhetsanalyse av selskap 1 og selskap 2

På bakgrunn av våre to problemstillinger har vi gjort en modenhetsanalyse av selskap 1 og selskap 2. Vi er ikke ute etter å sammenligne selskapene opp mot hverandre. Vi vil imidlertid kartlegge med tanke på fremtidige krav. Vi er ute etter å kartlegge hvor store endringer selskap 1 og selskap 2 har foran seg for å imøtekomme kravene.

	SELSKAP 1	**SELSKAP 2**
Benytter selskapet seg av Solvens II- direktivets definisjon av operasjonell risiko?		
Hvor langt har selskapet kommet i prosessen for å identifisere de operasjonelle risikoene?		
Hvor langt har selskapet kommet i prosessen for å måle utfallet av de operasjonelle risikoene?		
Hvor langt har selskapet kommet med å håndtere, kontrollere og overvåke operasjonelle risikoer?		
Hvor langt har selskapet kommet med å utarbeide en endelig ORSA?		
Har selskapet utarbeidet et system som skal inneholde hendelser og nesten- hendelser?		

Tabell 10.3: Modenhetsanalyse av selskap 1 og selskap 2

For å vurdere modenheten til selskapene har vi benyttet av oss av graderingen rødt- gult- grønt. Fargekoden illustrerer vår vurdering av hvordan selskapene tilfredsstiller kravene fra Solvens II- direktivet per i dag. Indikatoren *grønn* illustrerer beste praksis. Med beste praksis mener vi at selskapet er på god vei til å tilfredsstille kravet. Indikatoren *gul* viser at selskapet

er i en prosess hvor de har vurdert kravet, men ikke kommet med noe konkret forslag til hvordan de skal gjennomføre det. Indikatoren *rød* impliserer at selskapet ikke har tatt hensyn til kravet i nåværende praksis.

- Rødt: Umodent
- Gult: Modent
- Grønt: Beste praksis

Status selskap 1

Selskap 1 har startet en prosess for å implementere de nye kravene inn i risikostyringen. Allikevel mener vi at selskapet har for lite fokus på styring av operasjonelle risikoer i nåværende praksis, og at de derfor ikke tilfredsstiller fremtidige krav. Vi mener at selskapet ikke har gode nok prosesser for å analysere hvilke fremtidige operasjonelle risikoer som kan gi konsekvenser. Etter vår mening bør selskapet identifisere områder hvor operasjonell risiko kan inntreffe, og utarbeide tiltak for å håndtere disse. Dette bør være risikoer med både lav og høy sannsynlighet, og med høy konsekvens. Vi mener at det er viktig å ha strategier for å være forberedt på at operasjonelle risikoer inntreffer. Når det gjelder å håndtere, kontrollere og overvåke risikoer skjer dette på avdelingsnivå i selskapet. Våre inntrykk er at avdelingslederne ikke har et spesielt fokus på styring av operasjonell risiko. Vi mener at dette er en svakhet ettersom styring av operasjonelle risikoer skal fremkomme av systemet for risikostyring, fra Solvens II- direktivet. Vår mening er at selskapet har prosessene, men at de ikke har synliggjort hvordan de vil styre operasjonelle risikoer.

Selskapet har per i dag ikke utarbeidet et IT- system for registrering av hendelser og nesten- hendelser, og ikke utarbeidet tilhørende retningslinjer. De bør utarbeide et IT-system hvor hendelser og nesten- hendelser registreres, slik at det kan benyttes av hele organisasjonen. Ved å ha et slikt system vil det bli lettere å identifisere og måle risikoene, samt å beregne konsekvensene av utfallet. Et slikt historisk databasesystem kan gjøre det mulig å kvantifisere de operasjonelle risikoene ved beregning av solvenskapitalkravet. Da vil det være enklere å måle hvor ofte risikoene inntreffer og hvilket økonomisk tap disse vil medføre.

Status selskap 2

Selskap 2 er godt i gang med å imøtekomme de fremtidige kravene innenfor risikostyringen. Etter at kravene ble introdusert har de fått et bredere fokus på hvordan operasjonelle risikoer skal inkorporeres i selskapets risikostyringsprosess. Allikevel mener vi at selskap 2 i dag har noen mangler når det gjelder å håndtere, kontrollere og overvåke operasjonelle risikoer. I dag er det avdelingslederne som skal følge opp denne prosessen, og vi kan ikke se at de har et spesielt fokus på å styre de operasjonelle risikoene. Vi mener at styring av operasjonelle risikoer må synliggjøres mer, på bakgrunn av de fremtidige kravene. Som i selskap 1 mener vi at selskap 2 også har en prosess for risikostyringen i dag, men at de ikke har synliggjort godt nok hvordan de vil styre operasjonelle risikoer.

Selskap 2 er i gang med å utarbeide et IT- system, Easy- risk, som blant annet skal inneholde selskapets hendelser og nesten- hendelser. De har ennå ikke utarbeidet retningslinjer for hvordan dette skal registreres. Vi tror at selskapet vil få systemet på plass innen rimelig tid.

Våre anbefalinger

For at selskapene skal få en god helhetlig risikostyringsprosess (artikkel 44), som skal inneholde alle risikotyper, kan det være hensiktsmessig å bruke et teoretisk rammeverk.
I kapittel 6 vurderte vi fire rammeverk opp mot GRC. Rammeverkene for helhetlig risikostyring (COSO 2004) og A risk management standard (FERMA 2002) vurderte vi til beste praksis. Vi mener at begge rammeverkene har hver sine kvaliteter[49] som sammen kan bidra til god risikostyring. Begge selskapene mangler en prosess som inkluderer å styre operasjonelle risikoer i det overordnede risikostyringssystemet. Disse to rammeverkene kan benyttes som et grunnlag for å få til dette.

Sparebanken Vest har utarbeidet et rammeverk for styring av operasjonell risiko, som er beskrevet i kapittel 7.4.2. Dette rammeverket viser hvordan man kan styre operasjonelle risikoer på bakgrunn av bestemmelsene i Basel II- direktivet. Som et grunnlag for hvordan en operasjonell risikostyringsprosess (ikke helhetlig tilnærming) kan gjennomføres, er dette rammeverket et hjelpemiddel som etter vår mening kan benyttes av forsikringsselskaper.

Disse rammeverkene kan hjelpe selskapene med å synliggjøre operasjonelle risikoer i det overordnede risikostyringssystemet. Som vist i kapittel 5 var dette ett av eksemplene

[49] Disse kvalitetene finnes i kapittel 6.6.3.

Finanstilsynet trakk frem som god styring av operasjonell risiko. For at Finanstilsynet skal vurdere selskapenes risikostyringsprosess vil de mest sannsynlig benytte modul for operasjonelle risikoer. Modulen er bygd opp etter komponentene i COSO- rammeverket (2004). Ved å bruke COSO- rammeverket som et hjelpemiddel for å styre operasjonelle risikoer, vil det være lettere for selskapene å dokumentere denne prosessen. For å identifisere operasjonelle risikoer trekker modulen frem syv tapskategorier. Disse tapskategoriene skal hjelpe til med å danne et vurderingsgrunnlag for å beregne operasjonelle risikoer. Modulens kontrollspørsmål til disse risikokategoriene kan være et hjelpemiddel for å kvantifisere de operasjonelle risikoene. I tilegg kan selskapene bruke et graderingsskjema for å vurdere risikoenes sannsynlighet og konsekvens. Et eksempel på et graderingsskjema er vist i A risk management standard (FERMA 2002).

11 Oppsummering av del A og del B

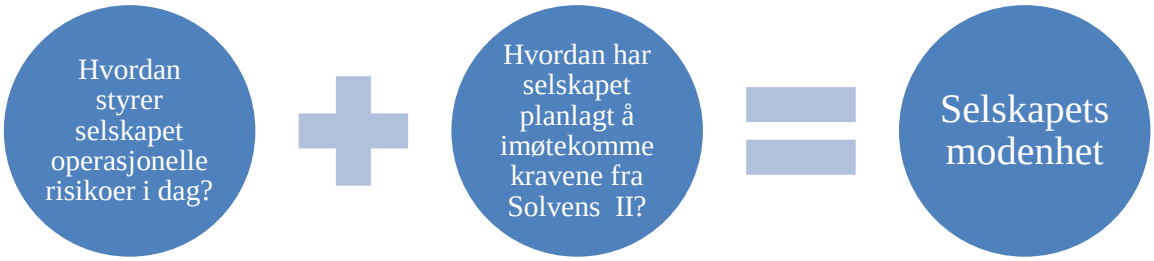
Målet med denne masteroppgaven har vært å belyse to problemstillinger:

1. ***Hvordan styrer to norske forsikringsselskaper operasjonelle risikoer i dag?***
2. ***Hvor langt har to forsikringsselskaper kommet med å imøtekomme de forventede fremtidige kravene fra Solvens II- direktivet?***

Oppgavens del A har en teoretisk tilnærming. Vårt formål med del A har vært å vise hvordan nåværende og fremtidige krav påvirker selskapenes risikostyring. For at et selskap skal kunne følge fremtidige krav, må de forstå og følge gjeldende krav. Derfor har det vært naturlig å ha størst fokus på gjeldende krav, ettersom fremtidige bestemmelser fortsatt er under utarbeidelse. Foreløpig er det kun nivå-1 bestemmelsene i Solvens II- direktivet som er fastsatt. Tilhørende gjennomføringsbestemmelser og tekniske standarder er fortsatt ikke definert som gjeldende krav. Dette betyr at det er vanskelig å si noe om hvordan nivå-1 bestemmelsene vil fungere i praksis.

Oppgavens del B inneholder en empirisk analyse. Vi har gjort en empirisk analyse for å få et innblikk i hvordan to forsikringsselskaper styrer operasjonelle risikoer, og hvordan de ser for seg å imøtekomme forventede kommende krav. I vår undersøkelse har vi sett på likheter og ulikheter hos selskap 1 og selskap 2, sett i sammenheng med våre to problemstillinger. Selskapene har en ulik organisering av risikostyringsprosessen, som skaper likheter og ulikheter i våre resultater. Dette betyr ikke at det ene selskapet har en bedre prosess enn det andre. Disse nyanserte svarene har gitt oss innblikk i hvordan risikostyring kan foregå på ulike måter.

Vi har også gjort en modenhetsanalyse av resultatene fra vår undersøkelse. Modenhetsanalysen viser vår vurdering av hvordan selskapene styrer operasjonelle risikoer i dag, og hvordan de har tenkt å imøtekomme de fremtidige kravene. Modenhetsanalysen bygger på våre to problemstillinger.



Figur 11.1: Selskapets modenhet

Figur 11.1. viser en konseptuell modell av vår modenhetsanalyse. I kapittel 10 vurderte vi selskapets modenhet ut i fra denne modellen. Selskapets modenhet viser hva som gjenstår i hvert selskap for å tilfredsstille kommende krav. Dette er gjort på bakgrunn av selskapenes praksis. Våre funn viser at begge selskapene er på god vei til å imøtekomme de fremtidige kravene. Allikevel viser våre funn at selskap 1 og selskap 2 har et forbedringspotensial når det gjelder fokus på operasjonell risiko i deres risikostyringsprosess.

12 Henvisninger

12.1 Litteratur

Askeheim, Ola. G. A., og Tor Grenness. 2008. *Kvalitative metoder for markedsføring og organisasjonsfag.* Oslo: Universitetsforlaget.

Bull, Hans J. 2008. *Forsikringsrett.* Oslo: Universitetsforlaget.

Busch, Tor. 1994. Økonomisk styring ut fra et kontraktsteoretisk perspektiv. *Økonomistyring og informatikk* 9 (5): 271-292.

COSO. 2012. *Enterprise Risk Management. Understanding and Communicating Risk Appetite.* COSO.

Eisenhardt, Kathleen. M., 1989. Agency theory: An assessment and review. *The Academy of Management Review* 14 (1): 57-74.

Fischer, Grete, og Nils Sortland. 2001. *Innføring i organisasjonspsykologi.* Oslo: Universitetsforlaget.

Gaudernack, Jonas. 2009. Skjerpet styreansvar for risikostyring og internkontroll - krav, fallgruver og praktiske råd. *Praktisk økonomi og finans* 09 (4): 3-11.

Gaudernack, Jonas. 2011/2012. Forelesningsnotater i BUS314, *Eierstyring og selskapsledelse*. UMB.

Gripsrud, Geir, Ulf H. Olsson, og Ragnhild Silkoset. 2004. *Metode og dataanalyse – med fokus på beslutninger i bedrifter.* Kristiansand: HøyskoleForlaget.

Grønmo, Sigmund. 2004. *Samfunnsvitenskapelig metoder.* Bergen: Fagbokforlaget.

Hendrikse, George W. J. 2003. *Economics & Management of Organizations; Coordination, Motivation, and Strategy*. New York: McGrawHill.

Holte, M., A. Kjesbu, og F. E. Sellæg. 2011. Regnskapsføring i forsikringsselskaper. Del I – livsforsikring. *Revisjon og regnskap*11 (1): 19-36.

Holte, M., A. Kjesbu, og F. E. Sellæg. 2011. Regnskapsføring i forsikringsselskaper. Del II – skadeforsikring. *Revisjon og regnskap* 11 (2): 28-38.

Johannessen, Asbjørn, Per A. Tufte, og Line Kristoffersen. 2006. *Introduksjon til samfunnsvitenskapelig metode.* Oslo: Abstrakt forlag.

Kosnik, Rita. D., 1987. Greenmail: A study of board performance in corporate governance. *Administrative Science Quarterly* 32 (2): 163-185.

Norges Bank. 2004. Norske finansmarkeder – pengepolitikk og finansiell stabilitet. *Norges Banks skriftserie nr. 34:* 24-39.

Ronkainen, V., L. Koskinen, og R. Berglund. 2007. Topical modeling issues in Solvency II. *Scandinavian Actuarial Journal* 07 (2): 135-146.

Saltkjel, Janne B. 2010. Operasjonell risikostyring i DnB Nor. *Internrevisoren* 10 (2): 8-11.

Sondstad, Stein O., og Birte Byrkjelo. 2010. Navigering i kjent og ukjent farvann – Integrert risikostyring som kart og kompass. *Internrevisoren* 10 (2): 6-7.

Thagaard, Tove. 2009. *Systematikk og innlevelse: en innføring i kvalitativ metode*, Bergen: Fagbokforlaget.

Øvsthus, Kari. 2010. Styring av operasjonell risiko i Sparebanken Vest. *Internrevisoren* 10 (2): 16-17.

12.2 Lover, forskrifter og direktiver

1956 Lov om tilsyn med finansinstitusjoner mv. (finanstilsynloven) av 6.desember 1956 nr. 1.

1988 Lov om finansieringsvirksomhet og finansinstitusjoner (finansieringsvirksomhetsloven) av 10. juni 1988 nr. 40.

1989 Lov om forsikringsavtaler (forsikringsavtaleloven) av 16. juni 1989 nr. 69.

1997 Lov om aksjeselskaper (aksjeloven) av 13. juni 1997 nr. 44.

1997 Lov om allmennaksjeselskaper (allmennaksjeloven) av 13. juni 1997 nr. 45.

1998 Lov om årsregnskap m.v. (regnskapsloven) av 17. juli 1998 nr. 56.

1999 Lov om revisjon og revisorer (revisorloven) av 15. januar 1999 nr. 2.

2005 Lov om forsikringsselskaper, pensjonsforetak og deres virksomhet mv. (forsikringsvirksomhetsloven) av 10.juni 2005 nr. 44.

1995 Forskrift om inndeling i forsikringsklasser som grunnlag for konsesjonstildeling 18. september 1995 nr. 797.

2003 Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT-forskriften) 21. mai 2003 nr. 630.

2006 Forskrift om kapitalkrav for forretningsbanker, sparebanker, finansieringsforetak, holdingselskaper i finanskonsern, verdipapirforetak og forvaltningsselskaper for verdipapirfond mv. (kapitalkravsforskriften) 14. desember 2006 nr. 1506.

2007 Forskrift om livsforsikringsselskapers og pensjonsforetaks kapitalforvaltning 17. desember 2007 nr. 1457.

2008 Forskrift om risikostyring og internkontroll (Internkontrollforskriften) 22. september 2008 nr. 1080.

2006/49/EF Direktiv av 14. juni 2006 om kravene til investeringsselskapers og kredittinstitutters kapitalgrunnlag (Basel II).

2009/138/EF Direktiv av 25. november 2009 om adgang til å starte og utøve forsikrings- og gjenforsikringsvirksomhet (Solvens II).

12.3 Forarbeider

Innst. 192 S (2011–2012) Innstilling fra finanskomiteen om samtykke til godkjennelse av EØS-komiteens beslutning nr. 78/2011 av 1. juli 2011 om innlemmelse i EØS-avtalen av direktiv 2009/138/EF av 25. november 2009 om adgang til å starte og utøve forsikrings- og gjenforsikringsvirksomhet (Solvens II).

NOU 1997: 6 Rammevilkår for omsetning av legemidler – ”Lønnsomme legemidler”.

NOU 2008: 20 Skadeforsikringsselskapenes virksomhet.

NOU 2010: 1 Medvirkning og medbestemmelse i arbeidslivet.

NOU 2011: 1 Bedre rustet mot finanskriser.

Prop. 54 S (2011-2012) Proposisjon til Stortinget (forslag til stortingsvedtak). Samtykke til godkjennelse av EØS-komiteens beslutning nr. 78/2011 av 1. juli 2011 om innlemmelse i EØS-avtalen av direktiv 2009/138/EF av 25. november 2009 om adgang til å starte og utøve forsikrings- og gjenforsikringsvirksomhet (Solvens II).

12.4 Rammerverk

1992 COSO. *Internal Control-Integrated Framwork.* New York, NY: COSO.

2002 FERMA. *A Risk Management Standard.* United Kingdom: FERMA

2002 FERMA. *Standarden for risikostyring.* Dansk oversettelse av FERMA-standarden.

2003 Casualty Actuarial Society - Enterprise Risk Management Committee. *Overview of Enterprise Risk Management*. CAS.

2004 COSO. *Enterprise Risk Management-Integrated Framwork (Executive Summary).* New York, NY: COSO.

2006 COSO. *Internal Control over Financial reporting – Guidance for smaller Public Companies.* New York, NY. COSO.

2008 CEIOPS. *Issues paper (ORSA).* CEIOPS.

2008 COSO. *Guidance on Monitoring Internal Control Systems.* New York, NY. COSO.

2009 CEIOPS. *CEIOPS` Advice for Level 2 Implementing Measures on Solvency II: System of Governance*. CEIOPS.

2009 Norges Interne Revisors Forening (NIRF). *Etiske regler og standarder for profesjonell utøvelse av internrevisjon.* NIRF.

2010 Laserfische. *GRC: A Framework for Organizational Sustainability.* Laserfische.

2010 Norsk anbefaling for Eierstyring og selskapsledelse, utgitt av Norsk utvalg for eierstyring og selskapsledelse (NUES).

2010 NS-ISO 3100:2009 (norsk standard), *Risikostyring - prinsipper og retningslinjer*. Norske versjon av ISO 31000:2009, utgitt i 2010 av Standard Norge.

2011 COSO. *Internal Control-Integrated Framwork.* New York, NY: COSO.

12.5 Finanstilsynet

Finanstilsynet. 2009. *Veiledning til forskrift om risikostyring og internkontroll. Rundskriv 3/2009*. http://www.finanstilsynet.no/no/Artikkelarkiv/Rundskriv/2009/1-kvartal/Veiledning-til-forskrift-om-risikostyring-og-internkontroll/

Finanstilsynet. 2011. *Høringsnotat om gjennomføring av Solvens II. http://www.finanstilsynet.no/Global/Venstremeny/Aktuelt_vedlegg/2011/3_kvartal/H%C3%B8ringsnotat%20lovforslag%20Solvens%20II%20sendt%20Finansdepartementet.pdf*

Finanstilsynet. 2012 (1). *Modul for evaluering av overordnet styring og kontroll.* http://www.finanstilsynet.no/no/Bank-og-finans/Banker/Tema/Kapitaldekning/Vurdering-av-risiko-og-kapitalkrav-/Risikobasert-tilsyn-banker/Overordnet-styring-og-kontroll-/

Finanstilsynet. 2012 (2). *Modul for operasjonell risiko.* http://www.finanstilsynet.no/no/Bank-og-finans/Banker/Tema/Kapitaldekning/Vurdering-av-risiko-og-kapitalkrav-/Risikobasert-tilsyn-banker/Operasjonell-risiko/

Finanstilsynet. 2012 (3). *Rapportering.* http://www.finanstilsynet.no/no/Forsikring-og-pensjon/Skadeforsikring/Tilsyn-og-overvakning/Rapportering/

Finanstilsynet. 2012 (4). *Reform av tilsynsstrukturen i EU – nye europeiske tilsynsmyndigheter.* http://www.finanstilsynet.no/no/Artikkelarkiv/Pressemeldinger/2011/1_kvartal/Reform-av-tilsynsstrukturen-i-EU--nye-europeiske-tilsynsmyndigheter/

Finanstilsynet. 2012 (5). *Risikobasert tilsyn – forsikring.* http://www.finanstilsynet.no/no/Forsikring-og-pensjon/Skadeforsikring/Tema/Risikobasert-tilsyn-/

Finanstilsynet. 2012 (6). *Solvens II.* http://www.finanstilsynet.no/no/Forsikring-og-pensjon/Skadeforsikring/Tema/Solvens-II/

Finanstilsynet. 2012 (7). *Tilsyn.* http://www.finanstilsynet.no/no/Forsikring-og-pensjon/Skadeforsikring/Tilsyn-og-overvakning/Tilsyn/

12.6 Nettsider og annet

Bokmålsordboka. 2012 (1). *Forsikring.* http://www.nob-ordbok.uio.no/perl/ordbok.cgi?OPP=forsikring+&bokmaal=+&ordbok=bokmaal

Bokmålsordboka. 2012 (2). *Rammeverk.* http://www.nob-ordbok.uio.no/perl/ordbok.cgi?OPP=rammeverk&begge=+&ordbok=begge

CAS. 2012. *About CAS.* http://www.casact.org/about/

Den Norske Veritas. 2009. *Operasjonell risiko angår deg…* http://www.dnv.no/ressurser/publikasjoner/dnvinnsikt/2009/no_1/oprisk.asp

EIOPA. 2012 (1). *About EIOPA.* https://eiopa.europa.eu/about-eiopa/index.html

EIOPA. 2012 (2). *Solvency II.* https://eiopa.europa.eu/activities/insurance/solvency-ii/index.html

EIOPA. 2012 (3). *Welcome to EIOPA.* https://eiopa.europa.eu/home/index.html

FERMA. 2012. *Mission and Objectives.* http://www.ferma.eu/about/mission-and-objectives/

Gaudernack, Jonas. 2010. *Oppfølging av Internkontroll.* http://www.nkrf.no/filarkiv/File/Kurs_og_konferansepdf-er/Nasj-fagkonf-2010/1200_-_Gaudernack.pdf

Gjensidige. 2012. *Risikotyper*. http://gjensidige.com/web/Forsiden/Om+konsernet/Risikostyring+og+kontroll/Risikotyper

ISO. 2012. *About ISO.* http://www.iso.org/iso/about.htm

Jansrud, Are. 2009. *ICAAP: Uavhengige vurderinger.* KPMG. http://www.bankenessikringsfond.no/Global/Sikringsfondet/H%C3%B8stkonferansen%2009%20presentasjoner/Uavhengig%20vurdering%20av%20ICAAP%20v%20Are%20Jansrud.pdf

Jusleksikon. 2012. *Forsikringsvirksomhetsloven.* http://www.harduensak.no/jusleksikon/Forsikringsvirksomhetsloven

Knutsen, Terje. Universitetet i Bergen. http://www.uib.no/demokrati/Intervju%20og%20metoder.ppt.pdf

Norges Bank. 2012 (1). *Finansinstitusjoner*. http://www.norges-bank.no/no/finansiell-stabilitet/det-finansielle-systemet-i-norge/finansinstitusjoner/

Norges Bank. 2012 (2). *Ord og uttrykk.* http://www.norges-bank.no/no/ord-og-uttrykk/#K

Norges Bank Investment Management. 2011. *Operasjonell risikostyring i NBIM.* http://www.nbim.no/no/media-og-publikasjoner/temaartikler/792/operasjonell-risikostyring-i-nbim/

NUES. 2012. *Hva er eierstyring og selskapsledelse.* http://www.nues.no/www/Hva_er_eierstyring_og_selskapsledelse+/

SINTEF. 2012. Kvantifisering av risikobildet. http://www.sintef.no/Teknologi-og-samfunn/Sikkerhet/LyseLNG/Kvantifisering-av-risikobildet/

Skjævestad, Anders. 2010. *Solvens II Forsikringsselskap i en stor bank.* http://www.kpmg.no/arch/_img/9681502.pdf

Towers Perrin. 2008 (1). *Embedding ERM – A Tough Nut to Crack. AN ERM Update on the Global Insurance Industry.* http://www.towersperrin.com/tp/getwebcachedoc?webc=GBR/2009/200901/2008_Global_ERM_Survey_12809.pdf

Towers Perrin. 2008 (2). *Life Insurance CFO Survey # 19: Embedding Enterprise Risk Management.* http://www.towersperrin.com/tp/getwebcachedoc?webc=TILL/USA/2008/200805/CFO_Survey19.pdf

13 Vedlegg

13.1 Vedlegg 1

Intervjuguide – selskap 1 og selskap 2

Intervjuet er beregnet til å vare i ca. 1 time.

Info:

Utdanningsnivå

Stillingstittel/ansvarsområde i selskapet

Generelt om styring av operasjonell risiko:

- Hvordan har selskapet definert operasjonell risiko?
  (Hvis ikke du kjenner til definisjonen? Hvordan definerer du operasjonell risiko?)
- Hvordan har dere kommet frem til denne definisjonen?
  (Hvis du ikke vet det, vet du om det jobbes med å definere operasjonell risiko?)

Hvis ja over:

- Hvilke risikokategorier har selskapet definert under operasjonell risiko?
- Hvordan har selskapet identifisert disse?
- Hvordan kontrollerer og måler dere risikoer som ikke er mulig å kvantifisere?
- Hvilke teknikker bruker dere for å overvåke de kvantifiserbare risikoene?
- Hvilke risikoer er mest prioriterte, rettet mot selskapets kjernevirksomhet? Topp 5
- Hvordan har dere analysert disse topp 5 risikoene?
- Hvilke rammeverk har selskapet benyttet for å identifisere, kontrollere og overvåke risikoer?
- Hvilke retningslinjer, lover eller føringer har dere tatt hensyn til ved styring av operasjonell risiko?

Kommende krav til styring av operasjonell risiko (Solvens II- direktivet):

- Hvor langt har dere kommet i å utarbeide et system for risikostyring og internkontroll?
- Har fokuset på styring av operasjonell risiko endret seg?
- Hvor langt har dere kommet i utarbeidelsen av retningslinjer eller policies for styring av operasjonell risiko i egenvurderingen av risiko (ORSA)?
- Hvor stor del skal styring av operasjonell risiko utgjøre i selskapets risikostyring og internkontroll? (årsverk, kapital avsatt til å dekke operasjonell risiko)

Organisering av operasjonell risiko:

- Hvordan er ansvarsstrukturen organisert for å følge opp operasjonell risiko? (hvem har ansvar for hva)
- Hvordan foregår rapporteringen? (fra ansvarsområdene til styret/toppledelse)
- Hvordan skal dere integrere styring av operasjonell risiko inn i organisasjonskulturen?
- Har dere hentet inspirasjon og kunnskap fra deres bank i konsernet?
- Har dere benyttet ekstern hjelp til styring av operasjonell risiko?

Annet (refleksjoner):

- Hvilke erfaringer har du gjort deg så langt i prosessen?
- Hvilke utfordringer ser du at selskapet har frem mot implementering av kravene fra Solvens II?
- Hva betrakter du som de største utfordringene innen operasjonell risikostyring?

13.2 Vedlegg 2

Intervjuguide – Finanstilsynet

Intervjuet er beregnet til å vare i ca. 1 time.

<u>Tilsyn og rapportering per i dag:</u>

1. Hva innebærer dokumentbasert tilsyn?
    - Hvilke dokumenter føres det tilsyn med?
    - Hvor ofte gjøres det tilsyn?
2. Hva skal rapporteres til Finanstilsynet?
    - Hvilke metoder benyttes i rapporteringsprosessen? (alle de som er listet opp på deres nettsider?)
    - Hva menes med spesifikke beregningsregler? Hva er de og hva innebærer disse?
    - Noen spesifikke metoder for rapportering av operasjonell risiko?
3. Eksisterer det noen artikler som beskriver tilsynsarbeidet?

<u>Tilsyn etter innføring av Solvens II- direktivet (rettet mot operasjonell risiko):</u>

1. Hvordan har Finanstilsynet tenkt å føre tilsyn over forsikringsselskapenes styring av operasjonelle risikoer?
    - Kan du/dere nevne noen metoder/moduler som dere vil bruke (hvilken metodikk)?
2. Hva forventer Finanstilsynet at forsikringsselskapene i Norge har utarbeidet av retningslinjer for å styre operasjonelle risikoer? Krav til innhold og overvåking
3. Hvordan er myndighetsfordelingen mellom EIOPA og Finanstilsynet?
    - Hvilken påvirkningsmulighet har Finanstilsynet overfor internasjonale myndigheter?
4. Hvordan vil kravene i Solvens II- direktivet endre eksisterende lovverk?