NORGES HANDELSHØYSKOLE

Bergen, Vår 2014

Operasjonell Risikostyring

Utfordringer ved bankers tilnærming til operasjonell risiko som en del av den overordnede risikostyringsprosessen

Herman Vidje

Veileder: Stein W. Wallace

Selvstendig arbeid i Økonomi og Administrasjon –

Økonomisk Styring

NORGES HANDELSHØYSKOLE

Sammendrag:

Målet med denne oppgaven er å identifisere utfordringer ved norske bankers tilnærming til operasjonell risikostyring, som en integrert del av bankenes helhetlige risikostyringssystem. Utredningen er en kvalitativ analyse og av ikke-teknisk karakter, der et overordnet perspektiv blir brukt.

Leseren blir først introdusert for begrepene risiko, operasjonell risiko og Enterprise Risk Management som et grunnlag for forståelse av videre teori og analyse. Deretter presenteres en historisk utvikling av risikostyring og hvorfor Enterprise Risk Management har fått økt oppmerksomhet det siste tiåret. Rammeverket analysen bygger på er en oversikt over ti suksesskriterier for effektiv Enterprise Risk Management av Sim Segal. Kriteriene tar for seg samtlige steg i risikostyringsprosessen: identifisering, kvantifisering, beslutningstaking og rapportering.

Konklusjonen i oppgaven gir uttrykk for flere utfordringer knyttet til å integrere den operasjonelle risikostyringen med bankenes helhetlige risikostyringssystem. Utviklingen innenfor operasjonell risikostyring i norske banker er enda på et tidlig stadium og har ikke nådd et nivå der fullstendig integrering er et faktum. Utfordringene knytter seg til kommunikasjon med aksjonærer både når det gjelder nøkkelrisikoene bankene står ovenfor og presentasjon av den operasjonelle risikostyringsprosessen i praksis. Informasjonen gir dog et godt bilde av rammeverket og retningslinjene for den operasjonelle risikostyringsprosessen. Hovedfokuset fra bankenes side ser ut til å være å tilfredsstille regulatoriske myndigheter, og aksjonærenes interesser settes i andre rekke. Selv om aktørene har flere felles interesser, er enkelte synspunkter ikke sammenfallende. Utfordringene relaterer seg også til det å inkludere korrelasjonsjusteringer i aggregeringen av risikoeksponering, både på tvers av risikokategorier og innenfor operasjonell risiko.

Analysen peker på flere utfordringer som kan være objekter for mer detaljert forskning og som bankene bør undersøke nærmere. For videre forskning kan det være interessent å gå mer i dybden på problemene og finne konkrete og mer tekniske løsninger.

Forord:

Denne utredningen er gjennomført som en avsluttende del av et toårig masterstudium i økonomi og administrasjon ved Norges Handelshøyskole. Oppgaven er skrevet med utgangspunkt i hovedprofilen økonomisk styring.

Enterprise Risk Management er et komplekst og spennende fagfelt som har fått økt oppmerksomhet i nyere tid. Jeg har ingen faglige forkunnskaper fra Norges Handelshøyskole med relevans for emnet, men jeg ble introdusert for temaet under et studieopphold i USA høsten 2013. Innføringen jeg fikk i Enterprise Risk Management inspirerte meg til valg av emne og fokusområde for oppgaven. Dette var et fagfelt jeg ønsket å utforske videre og lære mer om. Oppgaveskrivingen ga meg derfor mye ny kunnskap og lærdom jeg kommer til å ta med meg videre.

Jeg ønsker å takke min veileder Stein W. Wallace for gode diskusjoner og konstruktive tilbakemeldinger underveis i prosessen. Tilbakemeldingene har vært til stor hjelp for strukturering og fremgangsmåte i oppgaven. Videre vil jeg uttrykke min takknemmelighet til de som har hjulpet med korrekturskriving og innspill på oppgaven.

Herman Vidje

Norges Handelshøyskole

20. juni 2014

Innholdsfortegnelse

Ordliste:

ERM: Enterprise Risk Management

CEO: Chief Executive Officer
CRO: Chief Risk Officer
CFO: Chief Financial Officer

SREP: The Supervisory Review and Evaluation Process
CRD: Capital Requirement Directive
SEC: Security & Exchange Commission
COSO: The Committee of Sponsoring Organizations of the Treadway Commission

SOX: Sarbanes-Oxley Act
ICAAP: Internal Capital Adequacy Assessment Process

DCF: Distributional Cash Flow
CAPX: Capital Expenditure

RC: Regulatory Capital
EC: Economic Capital
ROCA: Return on acquired capital
ROI: Return on Investments

Figurliste:

1. Innledning

Utgangspunktet for denne oppgaven er å drøfte utfordringer ved norske bankers tilnærming til operasjonell risikostyring. Risikostyring som styringsverktøy har gjennom årene tilegnet seg betydelig oppmerksomhet og er blitt et styringsverktøy for ledelsen, aktivt brukt i høyt aggregerte beslutninger på både det strategiske, operasjonelle og finansielle plan. Risikostyring er nå langt mer enn det å kjøpe forsikring og sikre seg mot finansiell eksponering, og er ikke kun brukt som kun en kvantitativ kontrollfunksjon (Brian W. Nocco, 2006). Bankenes muligheter med *Enterprise Risk Management* er sentralt i denne endringen, men det er fortsatt utfordringer knyttet til hvordan implementere et effektivt Enterprise Risk Management-system (McKinsey & Company , 2013).

I dagens dynamiske marked er risikobildet i stadig endring og listen over ulike risikoscenarioer og interaksjonen mellom ulike risikoer blir bare lengre og mer kompleks. Risiko som ikke blir kontrollert eller tatt hånd om, vil kunne skade økonomien, banken og ansatte. Et effektivt risikostyringssystem kan derfor bidra til verdiskapning i selskapet og styrke selskapets soliditet. Risikostyring handler om å sikre «early mover» posisjonen i markedet og gjøre bankene forberedt på de hendelser og det uventede som kan oppstå i virksomheten. Historiske hendelser det siste tiåret har sørget for endringer i bankenes strategimodeller og strategiske tankegang. Disse historiske hendelsene, som blant annet Finanskrisen i 2007, har også ført med seg nye lover og reguleringer fra myndighetene som stiller høyere krav til kvaliteten i styring og kontroll av risiko. Det er derfor av stor interesse å gjøre mer forskning på dette feltet.

Motivasjonen for oppgavens fokusområde er rettet mot bankenes evne til å tilpasse seg endringen fra tradisjonell risikostyring til et selskapsvidt risikostyringssystem, med fokus på operasjonell risiko. Det er av interesse å undersøke hvordan norske banker har innrettet seg etter dagens dynamiske risikobilde. Jeg ønsker å se på norske *banker og operasjonell risiko* fordi finansinstitusjoner generelt har hatt en tendens til å være overfokusert på finansiell risiko, da en historisk har sett på finansiell risiko som det eneste viktige risikoaspektet av bankenes virksomhet.

Det er store utfordringer knyttet til bankers operasjonelle risikostyring i årene fremover og effektiv operasjonell risikostyring krever et selskapsvidt risikostyringssystem er.

John Whittaker fra leder av operasjonell risiko i Barclays uttalte at «*enterprise risk management muliggjør at alle elementene av operasjonell risiko kan samles i en database som holder rammeverket for operasjonell risiko; enten det er interne hendelser, risiko og kontrollvurderinger, nøkkelrisiko scenarioer eller måltall. Det tillater oss, gjennom arbeidsflyten som er inkludert i systemer, å linke alle elementer av vårt rammeverk sammen*» (Sisk, 2010).

1.1 Problemstilling

Oppgavens formål er å belyse bankers tilnærming Enterprise Risk Management med fokus på operasjonell risikostyring. I tillegg vil oppgaven vektlegge utfordringer og gjennomførbarheten til bankenes tenkte risikostyring. Det vil si risikotiltakenes operasjonaliserbarhet.

1. *Hvordan kan banker integrere den operasjonelle risikostyringen inn som en del av den helhetlige risikostyringen og eierstyringen i selskapet?*
2. *I hvilken grad er bankenes operasjonelle risikotiltak operasjonaliserbare, og hvilke utfordringer er knyttet til disse tiltakene?*

1.2 Tilnærming

Masterutredningen vil være en kvalitativ og utforskende analyse med utgangspunkt i eksempler fra norske bankers tilnærming til operasjonell risikostyring. Empiriske funn i norske bankers offentlige tilgjengelige informasjon vil bli brukt som analysegrunnlag. Selv om oppgaven vil fokusere på det norske regelverket og analysemomenter er knyttet til norske banker, vil mye av diskusjonen også kunne relateres til banknæringen generelt. Utredningen vil også være av ikke-teknisk karakter, da en for detaljert tilnærming til operasjonell risikostyring med hensyn på modellering og kvantifisering ikke er hensiktsmessig for å belyse problemstillingen. Oppgaven tar ikke sikte på å tjene som noen fasit om hvordan bankene skal utføre og omfavne operasjonell risikostyring, men vil drøfte

utfordringer ved nåværende risikostyringstiltak og eventuelle forslag for fremtiden. Forskningsstrategien er holistisk i sin innfallsvinkel ved at jeg ønsker å se på hver enkelt bank i sin helhet og vil ikke gå detaljert inn i hver enkelt divisjon eller virksomhetsområde i bankene.

Oppgavens utgangspunkt vil være å belyse problemstillingen fra aksjonærenes ståsted. Dette er gjort av hensyn til informasjonstilgang. Risikostyringssystemet til et selskap inneholder i de fleste tilfeller sensitiv informasjon og kan også inneholde informasjon som selskapet anser som konkurransefortrinn i forhold til sine konkurrenter. Av denne grunn må jeg ta utgangspunkt i den informasjonen som ligger offentlig tilgjengelig for aksjonærer og andre stakeholders.

Til analysen er det valgt ut tre forskjellige norske banker, der hovedsakelig risiko- og kapitalstyringsrapporter vil stå for informasjonsgrunnlaget. De tre bankene er større forretningsbanker og jeg har valgt ut disse med hensyn på informasjonsgrunnlaget for diskusjonen. Alle analyseobjektene er børsnoterte selskaper. Nordea, DNB og SpareBank 1 SR-Bank er bankene det hentes utvalgte eksempler fra.

Teorien og forskningen oppgaven bygger på er noe begrenset grunnet det dynamiske risikobildet virksomhetene står ovenfor. På grunn av finanskrisen og andre betydelige risikohendelser har det blitt satt et kraftig fokus på utvikling og forbedring av eksisterende risikostyrings- og ERM-rammeverk. De eldre rammeverkene og modellene har begrenset nytte på grunn av manglende erfaring, lærdom og data fra det som har skjedd det siste tiåret.

1.3 Oppgavens oppbygging

Oppgaven er bygd opp slik at leser først får en innføring i ERM som et selskapsomfattende risikostyringssystem. Innledningsvis presenterer jeg først noen definisjoner som er viktige som utgangspunkt for videre tolkning av oppgavens teoripresentasjon og analyse. Deretter presenteres grunnlaget for utviklingen av bankenes risikostyringssystemer gjennom de to siste tiårene og hvordan ERM er en ny tilnærming til risikostyring som kan skape verdier for virksomheten. Basel II blir så introdusert som det regulerende rammeverket bankene står overfor og gir innsikt i hva institusjonene faktisk er pålagt å gjøre i forhold til sin

risikostyring. Informasjonen fra Basel II fokuserer på krav til operasjonell risikostyring og utvalgte momenter tilknyttet den helhetlige risikostyringen som gjør seg relevant for oppgaven.

Videre presenteres et teoretisk rammeverk for en effektiv ERM-prosess. Det er dette rammeverket analysen vil bygge på. Til slutt legges analysen for oppgaven frem, der det teoretiske rammeverket blir brukt til å analysere utfordringer ved bankenes tilnærming til operasjonell risiko i et helhetlig risikostyringsperspektiv.

2. Definisjoner

2.1 Definisjon av Risiko

Risiko vil i økonomiske termer alltid være knyttet til utfallet av en eller flere hendelser, men utover dette er det lite enighet om en klar definisjon av hva risiko faktisk innebærer.

Det er viktig å definere begrepet risiko før vi begynner å gå dypere i detaljer rundt ERM og risikostyring generelt. Definisjonen av risiko setter en standard for drøftelsen senere i oppgaven og hva jeg mener ved bruken av ordet risiko i videre teori og analyse. Risiko kan defineres med tre hovedpunkter (Segal, 2011):

- *Risiko er usikkerhet.*
- *Risiko inkluderer positiv volatilitet.*
- *Risiko er avvik fra det forventede.*

En tilnærming til det første punktet er at dersom det ikke er en 100 % garanti for at prognosene for fremtiden vil inntreffe som forventet, involverer prognosene risiko. Med denne tilnærmingen er det kanskje vanskelig å tenke seg til noe som ikke involverer risiko. Dette kan også kanskje være riktig tilnærming.

Risiko blir normalt forbundet med tap, spesielt i næringslivet, men det er viktig å fremheve at risiko også kan involvere positive utfall knyttet til uventede hendelser. At risiko også kan ha positive utfall strider med COSOs utbredte rammeverk for ERM (COSO, 2005), men inkluderes av Sim Segal (Segal, 2011) grunnet koblingen mellom risikostyring og risk-return beslutninger på selskapsnivå. Dette er knyttet til det andre punktet i definisjonen over. COSO (COSO, 1991) er en internasjonalt anerkjent og global standard for internkontroll og risikostyringt. COSO publiserte et utvidet ERM-rammeverk i 2004 som fungerer som et veiledende rammeverk for Finanstilsynet og flere banker den dag i dag (COSO, 2005). COSO poengterer også at uventede hendelser kan ha positive utfall, men ser på dette som muligheten til å veie opp for risikoutfall og ikke som en del av risiko i seg selv. Segal argumenterer for at positive utfall må inkluderes i begrepet risiko for å kunne inkludere oppveiing av risikoutfall mellom ulike virksomhetsområder i selskapet, oppveiing på grunn

av flere risikohendelser inntreffer samtidig og kostnadene forbundet med volatilitet. Selv om de to synspunktene kan tolkes likt i en helhetlig sammenheng, er det viktig å poengtere at begrepet risiko, i oppgavens sammenheng, også involverer oppsidene av uventede hendelser.

Det å kun fokusere på risiko som muligheten for tap har lenge vært praktisert innenfor ERM og risikostyring. Det kan fører til systematisk overestimering av alvorligheten eller innvirkningen av risiko. Merk at dette ikke kun gjelder argumentet som ble presentert ovenfor i forhold til positiv volatilitet. Dersom en definerer tap som total kontantstrøm ut av selskapet som følge av tapene, vil selskapet inkludere både forventet tap og det tapet som er utover det forventede. Dette gir ikke et korrekt bilde av faktisk tap i risikokvantifiseringsprosessen. Et eksempel kan fremlegges ved et selskaps risiko i forhold til søksmål. Det er flere tilfeller der selskapet faktisk forventer et vist antall søksmål i løpet av et år. Da er det viktig å presisere at det er kun det som går utover det forventede som innebærer risiko. Dersom kostnadene forbundet med søksmål er lavere enn forventet vil dette være gevinst for selskapet, og tap dersom kostnadene er høyere enn forventet. En slik fremgangsmåte er ofte oversett i risikostyringssammenheng og selskaper unnlater å trekke fra det de faktisk forventer å tape i kvantifiseringen av risiko (Segal, 2011).

2.2 Definisjon av Operasjonell Risiko

Definisjonen og kategoriseringen av operasjonell risiko skal ikke kun fungere som en felles betydning bankene imellom, men også som en definisjon overfor de juridiske aspektene av risikostyringen. Operasjonell risiko kan oppstå innenfor alle de ulike virksomhetsområdene og potensielt viktige prosessene i bankene. Den operasjonelle risikostyringen må derfor være nært knyttet til de underliggende prosessene.

I denne oppgaven defineres operasjonell risiko ut ifra to standpunkter. Den første definisjonen er nyttig for organisasjoner å ta utgangspunkt i med tanke på *selskapets* tilnærming til operasjonell risikostyring (Segal, 2011). Den andre definisjonen er gjort av *myndighetene* med tanke på deres tilnærming til regulering av operasjonell risiko i bankene.

1. *Operasjonell risiko er en risikokategori som relaterer seg til uventede endringer i elementer som er knyttet til den daglige driften av selskapet. Eksempler er risiko knyttet til humankapital, teknologi, prosesser og katastrofer/ulykker.*

2. *Operasjonell risiko er risikoen for dirkete eller indirekte tap som følge av svikt i interne prosesser, menneskelige feil, systemfeil, eller andre tap som skyldes eksterne forhold.*

Definisjon nummer to ble presentert i Basel II-avtalen og representerer den definisjonen myndighetene tar utgangspunkt i ved regulering av bankene (Basel Committee on Banking Supervision, 2001). Den offisielle definisjonen fokuserer dog utelukkende på tapshendelser og tar ikke hensyn til eventuelle oppsider av operasjonell risiko, noe vår første definisjon av risiko gjør. Momentet vil bli diskutert ytterligere i analyse under kapittel 7.

Definisjonen av operasjonell risiko er meget viktig for forståelse av risikokategorien og essensiell for å håndtere risikostyringsprosessen riktig. Identifisering, risikokategorisering og intern og ekstern rapportering være avhengig av klare definisjoner av samtlige risikokategorier i institusjonen.

2.3 Definisjon av Enterprise Risk Management (ERM)

Det grunnleggende fundamentet i Enterprise Risk Management er at selskaper eksisterer for å skape verdier for stakeholders (COSO, 2005). *ERM er en prosess, der selskaper identifiserer, måler, håndterer og synliggjør alle nøkkelrisikoene selskapet står ovenfor, for å øke verdien for stakeholders* (Segal, 2011). Enterprise Risk Management er et risikostyringssystem.

Alle selskaper står overfor usikkerhet og ERM handler om å kvantifisere i hvor stor grad denne risikoen kan påvirke verdien av selskapet og hvor mye risiko som faktisk kan aksepteres. Kanskje en av de viktigste tankene bak denne formen for risikostyring er at risiko ikke bare er noe en ønsker å fjerne, men risiko kan også gi muligheter til å skape verdier i et selskap. Prinsippene bak Enterprise Risk Management søker å fremheve at effektiv håndtering av risiko vil være fordelaktig, både selskapet og selskapets stakeholders, gjennom økt verdi av selskapet. Det er i utgangspunktet ikke skadelig at selskap påføres tap, så lenge disse tapene er forutsett, håndtert og at selskapet klarer å veie opp for tap med profitt generert fra andre aktiviteter (Rochette, 2009). Det er alltid en trade-off mellom risiko og

profitt. Enterprise Risk Management er i litteraturen ansett som en egen form for risikostyring og er blitt et teoretisk begrep for denne formen for risikostyring.

COSOs rammeverk understreker at verdiene *i* selskapet og dermed verdien *av* selskapet, maksimeres når ledelsen klarer å sette en klar strategi og klare mål for å finne en optimal balanse mellom vekstresultat og relatert risiko. Selskapet må effektivt klare å sette inn ressurser for å nå disse målene. Enterprise Risk Management søker å oppnå:

- *Grensene for akseptabel risikoeksponering og selskapets strategi er sammenfallende*

Ledelsen analyserer selskapets totale grense for risiko og bruker denne informasjonen til å overveie ulike strategiske alternativer, sette relaterte mål og utvikle løsninger for å håndtere relatert risiko.

- *Risikostyring som en del av selskapets beslutningsprosess*

ERM søker å identifisere og velge ut alternative responser til et risikoscenario. Enten ved å prøve å redusere innvirkningene av et potensielt risikoscenario på selskapet, fjerne risikoen helt, eller akseptere risikoen. Sistnevnte avhenger av total risikoeksponering i forhold til risikogrensene satt av ledelsen og styret.

- *Identifisere og håndtere muligheten for at flere risikoscenarioer opptrer samtidig og scenarioer som oppstår på tvers av selskapets ulike avdelinger.*

Alle selskaper vil oppleve at ulike risikohendelser vil påvirke ulike deler av organisasjonen og flere avdelinger samtidig. Enterprise Risk Management er et styringssystem som søker å forberede selskaper på å effektiv respondere på korrelerte hendelser som påvirker selskapet og gir muligheten til en integrert respons på slike simultane risikohendelser.

- *Utnytte og gripe muligheter*

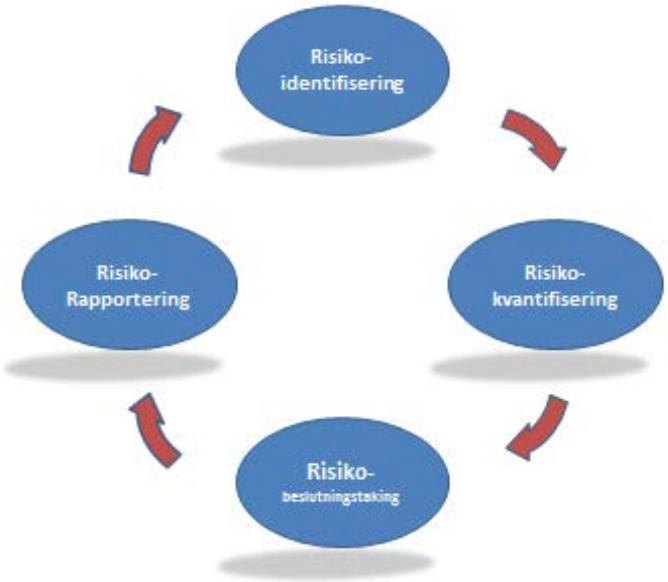
Ved at selskapet bruker ERM til å få en oversikt over hele spekteret av nøkkelrisikoer, gir dette ledelsen muligheten til å være proaktive og utnytte mulighetene risikohendelser kan gi. Nøkkelrisikoer defineres som de risikoene som har størst potensiell innvirkning på selskapet ut fra en individuell vektet avveining mellom sannsynlighet og konsekvens for risikoene.

- *Forbedre bruken av sysselsatt kapital*

Grundig informasjon om potensielle risikoer gjør det mulig å effektivt overveie overordnet kapitalbehov og gir et bedre grunnlag for effektiv kapitalallokeringer for ledelsen.

Et effektivt ERM-system gir selskaper muligheten til å oppnå produktivitets-, effektivitets- og resultatmål og forhindrer unødvendig tap av ressurser. Enterprise Risk Management søker å danne et risikostyringssystem som går utover det å sørge for en effektiv rapportering og etterfølgelse av lover og reguleringer, og ønsker å gi selskapet en proaktiv tilnærming til risikostyring. Dette igjen vil gjøre selskapet mer robust mot uforutsette hendelser og gi økte verdier for både selskap og aksjonærer (COSO, 2005).

ERM kan også fremstilles som en kontinuerlig og integrert prosess (*se Figur 1)* (Segal, 2011).



Figur 1: ERM-prosessen

Det første steget i prosessen er å identifisere nøkkelrisikoene selskapet står ovenfor, som representerer de største potensielle truslene mot selskapet. Dette gjøres vanligvis ved en intern kvalitativ tilnærming og analyse av historiske data med utgangspunkt i en sannsynlighets- og alvorlighetsskala for hver enkelt risiko.

Det andre steget i prosessen retter seg mot kvantifiseringen av de nøkkelrisikoene som ble identifisert i steg én. Tilnærmingen i dette steget er å kvantifisere risikoene individuelt og integrert. Hvor stor innvirkning har individuelle risikoscenarioer og scenarioer der flere

risikohendelser opptrer samtidig, på de valgte måleparameterne? Kvantifiseringen fører tilslutt til et aggregert mål på selskapets totale risikoeksponering.

Det tredje steget i ERM-prosessen omhandler det å inkludere informasjonen, innhentet i de foregående stegene, i selskapets beslutningsprosess. Selskapet må ta stilling til kvantifisert risikoeksponering, fastsette total risikoappetitt og iverksette tiltak for å holde eksponeringen innenfor risikogrenser satt av ledelsen. Risikoappetitt er overordnede risikogrenser for selskapet som helhet.

Det siste steget i prosessen inkluderer intern og ekstern rapportering av risikostyringen som foretas i selskapet. Internt involverer dette steget det å integrerer ERM inn i analyse av resultater og incentivplaner, i tillegg til å rapportere risikoinformasjon fra virksomhetsområdene til ledelsen og styret. På denne måten gis det signaler til ledelsen om at risiko og profitt må ses i sammenheng. Ekstern risikorapportering er kommunikasjon med ulike stakeholders som aksjonærer, ratingbyråer og regulatoriske organer.

3. Historisk utvikling av Enterprise Risk Management

3.1 Fra Risikostyring til Enterprise Risk Management:

Finanssektoren har historie for komplekse kvantitative metoder for å håndtere risiko. Det er nå blitt en økende trend for endring mot en topp-ned tilnærming til risiko, som begynner med økt kontroll og rettferdiggjøring fra styret angående sine handlinger og beslutninger (McKinsey & Company , 2013). Regulatoriske organer og aksjonærer har begynt å stille spørsmål rundt institusjonenes evne til å styre individuelle risikoer som kreditt, markedsrisiko, likviditetsrisiko og operasjonell risiko (se appendix for definisjoner). Risikostyring har fått økt viktighet for overnevnte eksterne aktører i lys av finanskrisen som inntraff i 2007-2008. I tillegg har lover og reguleringer som Basel II og andre bransjestandarder påvirket bankenes tilnærming til ERM.

Det er spesielt i det 21. århundret Enterprise Risk Management begynte å få mye oppmerksomhet og støtte fra næringslivet. Vi ser flere og flere selskaper som omfavner dette strategiske styringsverktøyet og inkluderer ERM som en del av hvordan hele selskapet styres. Selskaper har begynt å få øynene opp for hvilke verdier en effektiv risikostyring kan tilføre selskapet, og hvordan selskapet kan bli mer robust og motstandsdyktig mot uforutsette hendelser. Uforutsette hendelser er noe vi vet daglig inntreffer i driften av selskaper og som selskapene må håndtere for å kunne opprettholde effektiv drift. I et historisk perspektiv har vi sett en tendens til et prospektivt handlingsmønster, noe som nå ser ut til å skifte mot et mer proaktivt syn på risiko. En rekke hendelser av stor betydning etter årtusenskiftet har vært grunnpilaren for disse endringene.

3.1.1 Regnskapssvindel på ledelsesnivå:

I 2001 og 2002 fant det sted en rekke skandaler knyttet til regnskapssvindel som økte fokuset på risikostyring. Noen av de mest betydningsfulle, i ERM sammenheng, var Enron, Tyco og WorldCom. Alle disse selskapene kollapset etter en rekke avsløringer om svindel og flere i ledelsen ble dømt til lange fengselsstraffer. Skandalene som inntraff tidlig på 2000-tallet førte med seg ettervirkninger som det viste seg at skulle sette en ny standard innenfor risikostyring.

Enron-skandalen førte med seg sanksjoner mot styret og satte fokus på ansvarligheten styret har ovenfor selskapets virksomhet. Både Enron- og WorldCom-skandalen resulterte i at styremedlemmer ble holdt personlig økonomisk ansvarlige, og sørget for ny lovgivning. Dette førte igjen til at folk ble mer tilbakeholden til å sitte i styrer. De som satt i styrer ble mer opptatt av risiko og hva ledelsen gjorde for å beskytte selskapet mot nøkkelrisikoer. I flere selskaper der ERM har blitt implementert, har dette vært på grunn av press fra styret på ledelsen (Segal, 2011).

Hendelsene har også ført til et økt fokus på praktisering av risikostyring i selskapet og blant selskapets revisorer. Sarbanes-Oxley Act (SOX) ble innført i USA i 2002, og krevde at selskaper måtte gjennomføre en detaljert prosess for å identifisere risiko og for å skape effektive dokumentering og testing av risikokontroll (Hugh, 2006). Den finansielle rapporteringen ble også viktig, og det å få ledelsen til å formelt «gå god for» rapporteringen. I prosessen med å etterfølge SOX, adopterte mange selskaper en modifisert versjon av COSOs rammeverk fra 1990-tallet (COSO, 2005). Selskaper tok i bruk prosesskart for å identifisere utsatte deler av selskapet og brukte etterhvert også disse kartene til å identifisere risiko og ineffektivitet. Det ble også tilrettelagt for de ansatte å identifisere og adressere risiko ettersom det ble oppdaget og frigjort midler til å ta hånd om denne risikoen (Segal, 2011).

3.1.2 Finanskrisen

Fra millenniumskiftet frem til 2007 var det kraftig vekst i verdensøkonomien. Det var lite som tydet på en krise, og økonomien var tilsynelatende stabil og konjunktursvingningene moderate (Finansdepartementet, 2013).

Oppgangstiden fikk dog en brå vending da finanskrisen inntraff i USA i 2007. En av grunnene som fremheves som årsaken til krisen med utgangspunkt i risikostyring, var et svakt regulatorisk rammeverk som baserte seg på at bankene kunne stoles på til å «regulere seg selv» (Segal, 2011). Flere banker mislyktes i å etterfølge helt essensielle regler når det kommer til sikker virksomhet. De hadde høyt konsentrerte investeringer og feilet på prinsipper om å minimalisere volatiliteten i avkastning. Eksisterende risikosystemer,

ledelsen og styret, overså den stadig høyere risikotakningen (Kirkpatrick, 2009). Risikostyringen i bankene feilet i mange tilfeller på grunn av eierstyrings- og selskapsledelsesprosedyrer og ikke nødvendigvis mangler i datamodeller alene. I mange tilfeller nådde ikke viktig informasjon om bankens risikoeksponering styret eller toppledelsen. ERM i tiden før krisen var også ofte aktivitetsbasert og ikke selskapsbred. I andre tilfeller hadde styret godkjent risikostrategien, men manglet oppfølging av valgt strategi og mangelfulle måltall for å overvåke implementeringen (Kirkpatrick, 2009).

Krisen fungerte som en kraftig nedbrytende hendelse i det daværende landskapet av risikostyringssystemer og praksiser. Det åpnet flere dører for selskaper i forhold til tiltak og aktiviteter som kunne forbedre risikostyring og ERM-programmer. Før krisen var bankenes risikostyring ansett som den beste i sin klasse og andre finansinstitusjoner følte at å kopiere bankenes risikostyring var hovedmålet. Finanskrisen motbeviste dette. I tillegg var observasjonen av de store bankenes fall, en oppvåkning for de resterende bankene som faktisk overlevde krisen. Spesielt ga S&Ps integrering av ERM inn i kredittrating for ikke-finansielle selskap et økt fokus på ERM-aktiviteter, delvis på grunn av den observerte innvirkningen krisen hadde på selskapenes verdikjede (Bessis, 2011).

En annen innvirkning av krisen var at det ble lettere for de involverte i ERM og risikostyring å få ledelsen med på denne prosessen, i tillegg til å vurdere worst-case scenarioer og halehendelser. Ledelsen hadde nå fått åpnet øynene i forhold til hva som faktisk kan skje og hvor ille det kan gå.

3.1.3 Operasjonell Risiko

Operasjonell risikostyring ble for alvor gitt oppmerksomhet med Basel II og de spesifikke forslagene knyttet til ledelse og regulering av operasjonell risiko. Feltet er i kontinuerlig utvikling, men veksten og institusjonaliseringen av operasjonell risiko må sies å ha begynt med myndighetenes innarbeiding av denne risikokategorien i regulatoriske krav. Operasjonell risiko representerer en egen rolle i regulatorenes visjon og gir tentative kart for bankene i å implementere ny praksiser, et nytt risikospråk og nye ideer for å endre styring på selskapsnivå. Organisasjoner har i lang tid vært oppmerksomme på usikkerhet knyttet til sviktende informasjonsteknologi, infrastruktur, svindel, søksmål og lovbrudd for å nevne

noe. Det er likevel først i senere tid at organisasjoner har sett hvor utslagsgivende styring av operasjonelle risikoen er i den helhetlige risikostyringsprosessen (Power, 2006).

Selv om begrepet operasjonell risiko allerede ble introdusert 1991 (COSO, 1991), ble det ikke utbredt før med det første Basel II forslaget. I tillegg ble det i løpet av 90-tallet avdekket en rekke skandaler som ødeleggelsen av Berings Bank og Daiwa Bank i 1995. Bakgrunnen for begge hendelsene ble linket mot regulatorisk svikt. Svikt i operasjonell risikoledelse og hos enkeltpersoner ble i etterpåklokskap identifisert som utslagsgivende faktorer (Andersen L.B, 2010). Ved slutten av 1990-tallet hadde flere bransjer kastet seg på bølgen av operasjonell risikostyring, og særlig regulerende myndighet tilknyttet finans- og banksektoren. I utgangspunktet hadde operasjonell risiko vært innunder en residualpost for risiko i finansinstitusjonene, og var sett på som den resterende risikoen etter at finansiell risiko (markedsrisiko og kredittrisiko) var identifisert og kategorisert (Ernst & Young, 2001).

4. Lover og retningslinjer for risikostyring

Ved en vurdering av utfordringer tilknyttet bankenes operasjonelle risikostyring, er det hensiktsmessig å først danne en oversikt over hva bankene faktisk er påkrevd å gjøre av de norske myndighetene.

4.1 Basel-regelverket

4.1.1 Basel II

Basel II er en videreutvikling av Basel I (1988) og hadde betydelige konsekvenser for norske banker. Kapitaldekningskrav ble allerede innført med Basel I, men Basel II utvidet dette kravet og introduserte nye aspektet ved regulering av risikostyring i finansinstitusjonene. Kapitaldekningskravet representerer krav til bankenes kapitalreserver som skal fungere som en buffer for å dekke uventede tap. Bufferen skal hindre konkurs for den individuelle bank, men reduserer også systemrisiko. Systemrisiko kan eksemplifiseres med at en enkelt banks fall kan føre til ringvirkninger og kollaps andre steder i finansmarkedet. Kapitaldekningskravene er blitt innført med bakgrunn i å sikre soliditeten i finansinstitusjonene og det finansielle systemet som helhet (Harald Karlsen, 2002). Kapitalkravene er også ment for å skape likt konkurransegrunnlag for bankene, uavhengig av landet de opererer i. Det er viktig å merke seg at The Basel Committee on Banking Supervision ikke har nasjonal reguleringsmakt i seg selv, men fungerer som et rekommanderende og veiledende organ for nasjonale myndigheter. EU har valgt å etterfølge avtalen og norske banker blir gjennom EØS-avtalen påkrevd å følge dette rammeverket av Finanstilsynet. Basel III-avtalen ble fremlagt i 2010 og forventes implementert i Norge i løpet av 2019. Endringene i avtalen i forhold til Basel II relaterer seg i svært liten grad til operasjonell risiko og videre analyse, og jeg har derfor valgt å ta utgangspunkt i Basel II i oppgaven.

Basel II ble publisert i endelig form i 2004 (Basel Committee on Banking Supervision, 2004). Hovedinnholdet i Basel-avtalen bygger på tre grunnpilarer. Avtalen vil ikke i sin helhet bli gjennomgått i denne oppgaven, men det vil bli presentert enkelte momenter som relaterer seg til den operasjonelle risikostyringen:

Pilar 1 – Minimum kapitalkrav knyttet til operasjonell risiko:

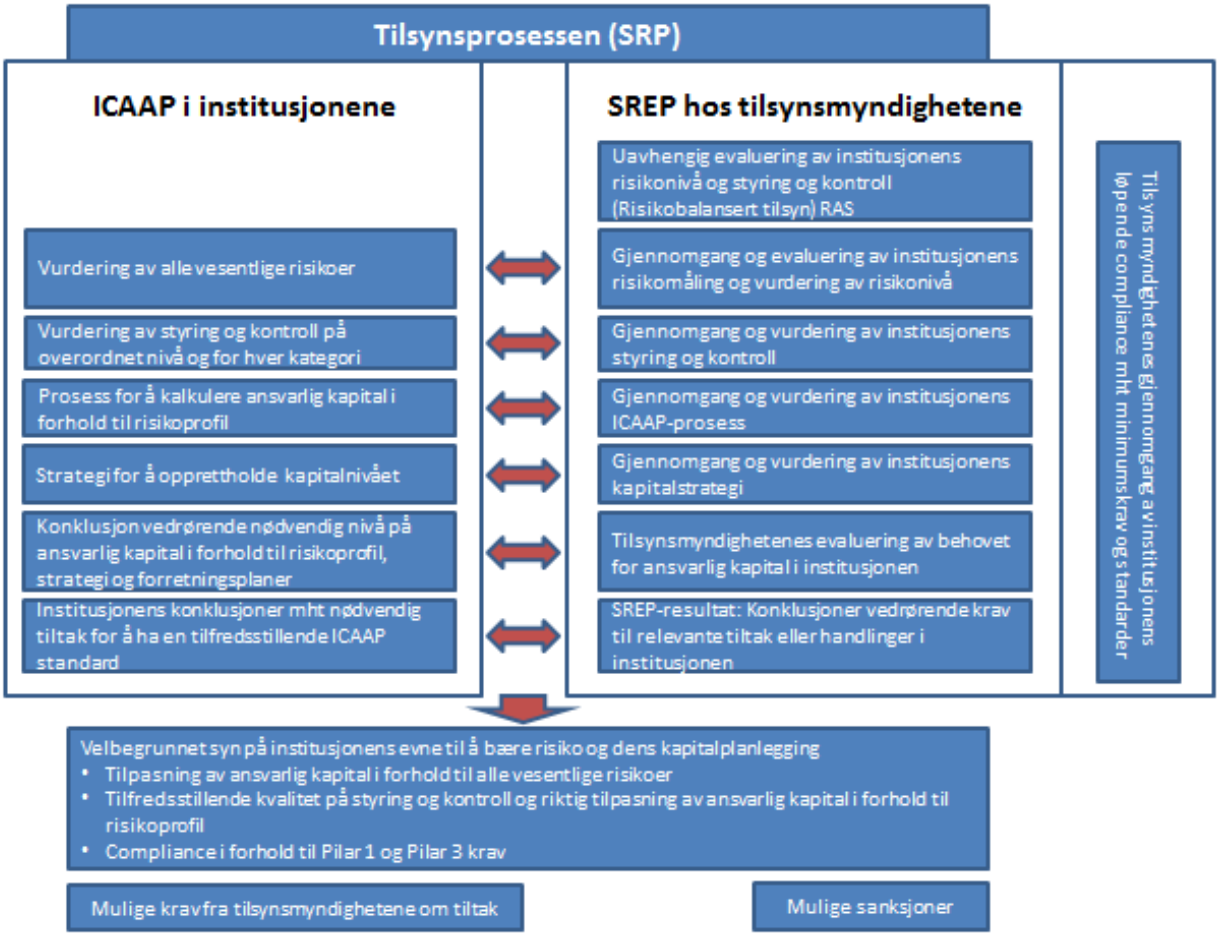
Pilar 1 representerer metoder for å kalkulere hvor mye en bank minimum skulle ha i reservekapital med tanke på at bankenes likviditetsreserver for å takle uventede hendelser. Det eksisterer flere krav knyttet til bankenes beholdning av kapital. Første pilar representerer det som kalles regulatorisk kapital. Det er tre ulike metoder for beregning av regulatorisk kapital tilknyttet operasjonell risiko; basismetoden, sjablongmetoden og avansert metode (Finansdepartementet, 2006). Den siste metoden er ikke aktuell for norske institusjoner på nåværende tidspunkt da operasjonell risikostyring ikke har kommet langt nok i Norske banker.

1. I *basismetoden* er beregningsgrunnlaget 15 % av gjennomsnittlig inntekt de tre siste årene multiplisert med en multiplikator på 12.5.
2. *Sjablongmetoden* tar utgangspunkt i åtte definerte virksomhetsområder (se appendiks tabell 2). Det skal være definert hvilke tjenestekategorier som inngår i områdene. Kapitalkravet settes som et vektet gjennomsnitt av inntekten i de forskjellige forretningsområdene gitt av loven. Forskjellen er at beregningssatsen er ulik (12 %, 15 % eller 18 %) avhengig av forretningsområdet. På denne måten blir det til en viss grad justert for at de forskjellige forretningsområdene står ovenfor forskjellige potensielle operasjonelle risikoer (enkelte aktiviteter og operasjoner vil være tilknyttet mer risiko enn andre). Sjablongmetoden er den metoden som hovedsakelig er brukt i de utvalgte bankene.
3. *Avansert metode* baserer seg på interne kapitalkalkuleringer som må fastsettes på bakgrunn av forventet og uventet tap. Beregningsgrunnlaget skal legge til grunn et konfidensintervall over en ettårs periode på 99,9 prosent. Hovedgrunnen til at norske banker ennå ikke har tatt i bruk denne metoden er manglende oppfylling av krav fra finanstilsynet på ekstern og intern data og velutviklede scenarioanalyser.

Pilar 2 - Tilsynsmessig oppfølging med hensyn til operasjonell risiko og selskapets overordnede risikostyring:

Pilar 2 representerer myndighetenes tillatelse til overvåking av bankenes egen risikostyringspraksis og risikoeksponering. Den inkluderer obligatoriske prosesser for både bankene og regulatoriske myndigheter. Bankene må gjøre en «internal capital adequacy assessment process» (ICAAP) for å demonstrere at de har implementert prosedyrer og

metoder for å sørge for tilstrekkelig kapitalressurser. Ofte fører ICAAP-prosessen til høyere reservekapital, fordi prosessen tar for seg et bredere spekter av risiko og høyere prosentsats av beregningsgrunnlaget enn ved minimumskalkuleringene. ICAAP er en intern kalkulering av kapitalbehovet i bankene som skal representere dagens risikobilde i den respektive banken. Kalkuleringene gjøres enten på bakgrunn av interne modeller, simuleringer eller tilleggskalkuleringer til minimumskravet. De interne kapitalberegningene representerer det vi kaller økonomisk kapital. Økonomisk kapital er den kapitalen bankene selv mener det er forsvarlig å holde for å støtte opp under den risikoen banken påtar seg. Kalkuleringene baserer seg på å konvertere risiko til kapital i banken.



Figur 2 Tilsynsprosessen under Pilar 2 i Basel II-avtalen (Finanstilsynet, Retningslinjer for tilsynsprosessen, 2006)

Finanstilsynet tar utgangspunkt i rammeverket til COSO og veiledninger i Basel II avtalen ved fastsettelse av lover og ved revidering av finansinstitusjonenes risikostyring. Gjennom Pilar 2 settes det også krav til bestemte risikofunksjoner som skal være på plass i banken, og deres arbeid tilknyttet risikostyrings- og internkontrollsystemer. I tillegg stilles det krav til de

ansatte som skal være ansvarlig for dette arbeidet. Det skal finnes skrevne retningslinjer for alle viktige risikotyper, fastsatte grenser for eksponering og krav til risikohåndtering. Risikoappetitt skal vedtas av styret eller ledelsen, altså på selskapsnivå.

Vurdering av risikostyringsprosessen:
Det er slik at styret har det endelige ansvaret for selskapets operasjonelle risikostyring. Det vil si at styret skal gjøre en endelig godkjenning av bankens operasjonelle risikoprofil. Styret skal også sørge for at de retningslinjer og målsettinger som er satt blir fulgt opp og innarbeidet i organisasjonen. Operasjonaliseringen av styrets målsettinger og retningslinjer gjøres av daglig leder, sammen med den øvrige ledelsen.

Styret skal gi retningslinjer for å skille mellom institusjonenes forskjellige funksjoner og forhindre interessekonflikter. Inkludert er også retningslinjer for beredskapsplaner for å sikre kontinuerlig drift og begrensing av tap ved alvorlige driftsforstyrrelser (Basel Committee on Banking Supervision, 2004).

Pilar 3 – Markedsdisiplin med hensyn til operasjonell risiko og selskapets overordnede risikostyring:
Pilar 3 stiller krav til kvalitet i informasjonen om risikosituasjonen i selskapet til offentligheten. I Norge dekkes dette av kapitalkravforskriftene del IX. Pilar 3 har som formål å bidra til økt markedsdisiplin gjennom krav til institusjonene om å offentliggjøre informasjon slik at markedet kan få et overblikk over bankens risikoprofil og kapitalisering, samt styring og kontroll. Informasjonen som skal publiseres risiko- og kapitalstyringsrapportene (Pilar 3-rapportene) er knyttet til organisasjonsstruktur relevant for risikostyring, kapitalkrav delt etter risikotype, kapitalnivå og struktur. I tillegg skal strategier og prosesser fremlegges, samt policyer for bankenes hedging og/eller begrensning av risiko og strategier og prosesser for å overvåke effektiviteten av begrensningstiltak. For banker som ikke bruker den avanserte metoden, gjelder ingen egne krav for rapportering og åpenhet angående operasjonell risiko annet en det generelle kravet til informasjon rundt virksomhetens ulike risikoområder (Basel Committee on Banking Supervision, 2004).

5. Teori og rammeverk for oppgaven

Analysen vil bygge på rammeverket for en effektiv ERM-prosess av Sim Segal (Segal, 2011). I tillegg vil det også brukes supplerende teori som er rettet mer konkret på operasjonell risikostyring. Det vil kun bli fokusert på utvalgte aspekter av ERM-prosessen. Hovedsakelig vil jeg i oppgaven analysere prosessen som involverer bruken av risikoinformasjon i selskapets beslutningsprosess og rapportering, men det vil også være enkelte analysemomenter knyttet opp mot de to første stegene i ERM-prosessen. Analysen vil ha et overordnet perspektiv på hvordan risikostyringssystemet er bygd opp, i forhold til best practice og nevnte rammeverk. Basel II-avtalen vil fungere som et supplerende rammeverk.

5.1 Hovedkriterier for ERM

Segal definerer **10 hovedkriterier** for at selskapets risikostyring skal oppfylle kravene til et effektivt ERM-system:

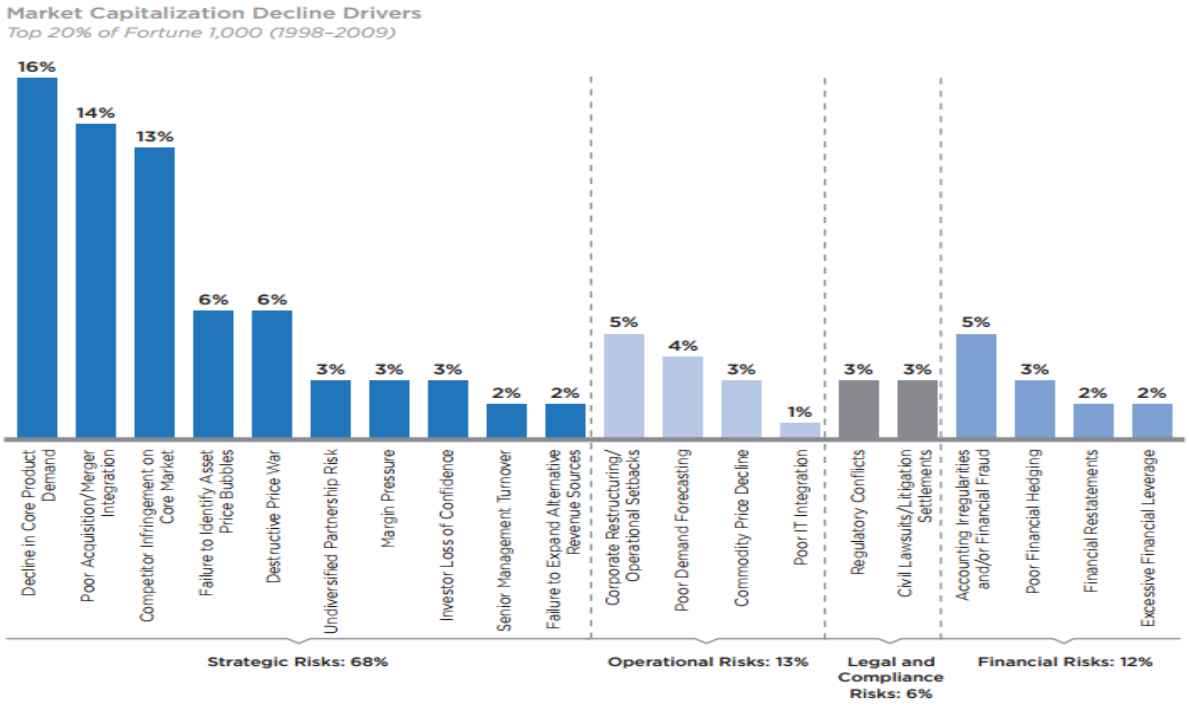
1. Selskapsvidt omfang

ERM må implementeres i alle divisjoner, avdelinger og områder av selskapet. Et selskap kan aldri vite i hvilken del av virksomheten risikohendelsene vil inntreffe. Ofte er det slik at uventede hendelser oppstår der selskapet ikke leter, og selskaper har lett for å overfokusere på hovedområder ved virksomheten og overse områder der det går bra. Risikohendelsene er ikke nødvendigvis proporsjonale med størrelsen til virksomhetsområdet de oppstår i.

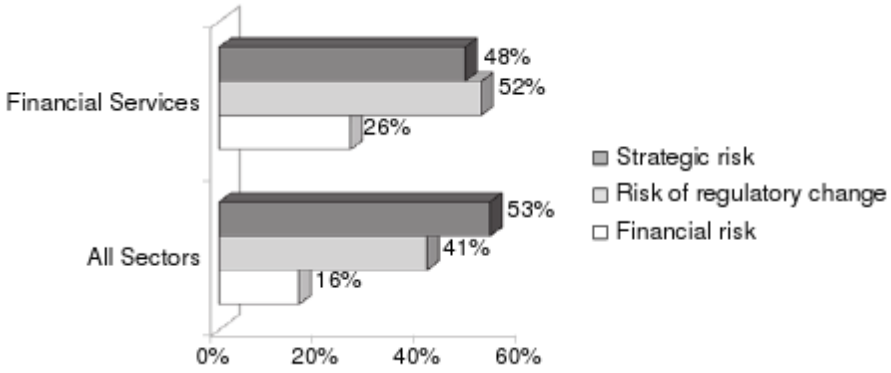
2. Alle risikokategorier inkludert

For å få til en effektiv risikostyring og en helhetlig oversikt over risiko som kan oppstå, må risikostyringssystemet inkludere alle kategorier for risiko. De tre hovedkategoriene er finansiell risiko, strategisk risiko og operasjonell risiko (se tabell 1 i appendiks). Finansinstitusjoner opererer i mange tilfeller med en egen kategori for likviditetsrisiko (under finansiell risiko i denne definisjonen) og forsikringsselskap har en siste kategori for risiko kalt forsikringsrisiko. Faren ved å ignorere en risikokategori eller ved å ikke ha et balansert fokus på tvers av kategorier, er at det kan gi unødvendig høy risikoeksponering for

selskapet og en feilfordeling av ressurser brukt på begrensningstiltak. Tradisjonelt har organisasjoner i alle bransjer hatt et ensidig fokus på finansiell risiko. Senere empiri viser at både operasjonell og strategisk risiko er en langt større del av den totale risikoeksponeringen til selskaper enn før antatt.



Figur 3: Styremedlemmer om de største risikoene selskapet står ovenfor (The Conference Board, 2006)



Figur 4: Risiko etter kategori som har resultert i tap av 50 % eller mer i selskapsverdi (SEB, 2011).

Bakgrunnen for at finansiell risiko tradisjonelt har dominert det subjektive risikobildet i selskaper, er ofte fordi risiko blir kategorisert etter utfall og ikke etter kilde. Majoriteten av risikohendelser vil ha finansielle utfall, men det er ikke alltid finansiell risiko som er kilden.

3. Fokus på nøkkelrisikoer

ERM-programmet skal i utgangspunktet kun fokusere på nøkkelrisikoer selskapet står overfor. ERM er strategisk rettet og fokuserer på en relativt liten liste av risikoer som har størst potensiell innvirkning på selskapsverdi. Det er viktig å merke seg at antall nøkkelrisikoer ikke avhenger av størrelsen til selskapet. Bakgrunnen for et fokus på nøkkelrisiko, baserer seg på styret og toppledelsen, og deres begrensede evner til å fokusere på et for stort antall risikoer. Det er bare én CEO, ett styre og én toppledelse i et selskap. Størrelsen på de potensielle risikoene og risikotypen vil selvfølgelig variere fra selskap til selskap, men antallet vil være noenlunde det samme. Dette er en rak motsetning til måten mange selskaper tilnærmer seg ERM. De lager en uendelig lang liste over alle potensielle risikoer selskapet står ovenfor.

4. Integrering på tvers av risikotyper og virksomhetsområder

Tilnærmet alle selskaper har i utgangspunktet en eller annen form for risikostyring fra den dagen de ble startet. Begrensningen i risikostyringen til mange av dagens selskaper er hvordan hver enkelt type risiko blir styrt og håndtert isolert. Informasjonsteknologirisiko håndteres av IT-avdelingen, menneskerelatert risiko håndteres av HR-avdelingen, osv. Uheldigvis fører denne silotilnærmingen med seg tre vesentlige ulemper:

Ufullstendig:

Risikostyring på silomåten har en farlig svakhet ved at det gir et ufullstendig bilde av selskapets risikoprofil. Metoden fanger opp de fleste grunnleggende typene risiko, men kun der ett risikoscenario inntreffer av gangen. Dette er et godt fundament, men det er også viktig å inkludere risiko som potensielt kan opptrer samtidig, enten det er tilfeldig korrelasjon eller underliggende kausale eller statistiske sammenhenger. Silorisikostyring ignorerer risikokorrelasjon på tvers av organisasjonen og det er ofte urealistisk at bare en risikohendelse opptrer om gangen. Virkeligheten involverer langt mer usikkerhet og kompleksitet.

Silomåten utelater også de største truslene mot selskapet. Dette fordi det ofte er når flere risikohendelser opptrer samtidig, de største truslene mot selskapet oppstår. Etter den første hendelsen er selskapet svekket og det øker sannsynligheten for at en ny hendelse skal inntreffe. I tillegg kan risikoer interagere og skalere hverandre i enten negativ eller positiv forstand. Selv to risikohendelser med kun nedsidepotensiale kan delvis oppveie hverandre.

Ineffektivt:
Dersom en behandler hver risikotype isolert kan det føre til flere former for ineffektivitet. Et eksempel er at en betaler for mye ved for eksempel separate sikringskjøp for relatert risikoeksponering i flere deler av selskapet. Dette kan øke den totale kostnaden ved risikobegrensning. Dårlig kommunikasjon kan være et annet resultat. Mangelen av en standardisert tilnærming og felles rammeverk kan forhindre spredningen av «best practice» i risikostyringen. Kanskje mest kostbart er begrensninger i forhold til å effektivt dele erfaringer og lærdom fra historiske feil, som lett kan gjøre at andre avdelinger gjentar feilen. ERM-systemet søker å integrere styring og kontroll på tvers av risikotyper og virksomhetsområder for å fjerner ineffektivitet. Resultatet kan bli mer effektive og overveide risikobegrensningstiltak og effektiv deling av informasjon i hele organisasjonen.

Internt inkonsekvent:
Den tredje ulempen ved silorisikostyring, er at organisasjonen kanskje vil ha inkonsekvente prognoser for fremtiden relatert til markedet. Virksomhetsområdene kan ende opp med å utvikler uavhengige risikoscenarioer med forskjellige grunnleggende antakelser. Kommunikasjon og koordinering gjennom ERM-prosessen sørger for at selskapet fastsetter ett enkelt sett av prognoser for markedet internt i selskapet.

5. Aggregerte måltall

En av grunnene til at risikostyringssystemet kalles *Enterprise* Risk Management er fordi det skal gi muligheten til å aggregere måltall for risikoeksponering på selskapsnivå. På denne måten kan en gjøre overordnede risikobeslutninger på øverste nivå i selskapet. På et aggregert nivå er det måltall for total risikoeksponering og risikoappetitt som er av interesse. Total risikoeksponering kalkuleres ved en bunn-topp tilnærming, der risikoeksponeringen i de ulike virksomhetsområdene blir summert. Korrelasjon blir inkludert ved aggregering med

hensyn på simultane risikohendelser. Dette er et rent kvantitativt mål og bygger på interne risikokalkuleringer. Risikoappetitt på den andre siden er et kvalitativt mål satt av ledelsen og styret på hvor høy total risikoeksponering selskapet finner akseptabelt. Risikoappetitt beregnes først på selskapsnivå og dernest disaggregeres risikoappetitt ned i virksomhetsområdene. Risikoappetitt på virksomhetsområdenivå benevnes som risikogrenser. Risikoappetitt og risikoeksponering uttrykkes med en sannsynlighet og innvirkning på selskapet.

Et godt aggregert måltall på risiko er selskapsverdi. Da vil total risikoappetitt for eksempel være at sannsynligheten for å tape 6 % av selskapets verdi, ikke skal overstige 14 %. Flere selskaper opererer fortsatt med silorisikostyring og har derfor ikke disse aggregerte elementene i sin overordnede risikostyring. Men uten disse to aggregerte målene, kan faktisk ikke ERM utføre sin hovedfunksjon, som er å håndtere og holde selskapets totale risikoeksponering innenfor selskapets risikoappetitt. Evnen til å produsere disse aggregerte måltallene er også viktig fordi det er det første steget i beslutningsprosessen i ERM.

Tradisjonell risikostyring der risikogrensene settes med utgangspunkt i de ulike virksomhetsområdene vil kunne føre til for lav eller for høy risikobegrensning. En bunn-topp tilnærming resulterer i en ineffektiv bruk av ressursene i organisasjonen, og særlig i finansinstitusjoner der kapitalallokering er en veldig utbredt utfordring.

ERM introduserer en logisk tilnærming til styring av den totale volatiliteten og gir uttrykk for ønsket stabilitet i selskapet og sjokkresistans for ledelsen. Dette er viktig fordi aksjonærer og potensielle investorer også vil ha en slik tilnærming ved vurdering av selskapet. Når risikoeksponering er kalkulert, risikoappetitt er definert på selskapsnivå og risikogrensene er satt for de ulike virksomhetsområdene eller forretningsprosessene, kan mellomledelsen ta beslutninger på lavere nivå.

6. Inkludert i selskapets beslutningstaking

Det har vist seg at mange tradisjonelle risikostyringssystemer hovedsakelig fokuserer på å identifisere, kvantifisere og rapportere risiko til ledelsen og styret. Svakheten med denne tilnærmingen er at risikostyringen får redusert verdi og kan virke overflødig. ERM-prosessen

fokuserer på å faktisk *bruke* risikoinformasjon innhentet i tidligere steg til å fatte beslutninger og iverksette konkrete tiltak for å begrense risikoeksponeringen.

7. Balansert styring av «Risk-Return»

Et annet aspekt ved å inkludere risikostyring selskapets strategiske beslutningsprosess, er at ERM ikke kun involverer risikobegrensning. Før ERM fokuserte ledelsen kun på de negative sidene av risiko. Dette førte til at risikoledelsen ofte sa nei til prosjekter, for å forhindre at virksomhetsområder tok på seg mer risiko. Oppsidepotensialet ble tradisjonelt ikke veid opp mot nedsiden av risiko på en fornuftig måte. På grunn av at potensiell oppsiderisiko for prosjektene ikke ble vurdert, unngikk mellomledere å inkludere risikoledelsen i vurderingen og den endelige avgjørelsen av iverksetting av nye prosjekter. ERM ønsker å inkludere både oppside- og nedsidepotensialet for å kunne gi riktige beslutningsgrunnlag for ledelsen og avveininger i forhold til risk-return på prosjekter og andre driftsrelaterte beslutninger.

8. Korrekt synliggjøring av risiko

Ved implementering av ERM er det sjeldent at det avdekkes nye typer risiko. Dette fordi ledelsen og selskapet allerede har oversikt over nøkkelrisikoene selskapet står ovenfor. En kraftig oversett risiko, på den andre siden, er risikoen for ukorrekt rapportering og synliggjøring av risiko. Med rapportering og synliggjøring i denne sammenhengen menes ekstern informasjonsdeling og kommunikasjon med aksjonærene og andre stakeholders for å gi dem innsikt i selskapets risikobilde og det helhetlige ERM-programmet. En signifikant risiko er ofte meget svak sammenheng mellom det som blir kommunisert til eksterne aktører og det faktiske ERM-programmet i selskapet. Riktig og oversiktlig kommunikasjon av risikoinformasjon gir selskapet et bedre utgangspunkt for å forsvare seg ved potensielle risikohendelser. Problemet oppstår ofte når selskaper ikke informerer om risikoenes potensielle konsekvens på aksjonærverdier. Dersom selskapet forbereder aksjonærene på forhånd, gjennom kontinuerlig kommunikasjon, vil aksjonærene kunne være mer støttende og forståelsesfulle. Mulige forklaringer på hvorfor selskaper ikke presenterer potensielle nøkkelrisikoer med tilhørende konsekvens for selskapsverdien, er blant annet at selskaper ikke har anledning til det. I dette ligger det at de faktisk ikke har et system eller en prosess for å måle risikoens innvirkning på selskapsverdi. En annen forklaring er også at de ikke

ønsker å dele denne informasjonen med offentligheten på grunn av konkurransehemmende effekter.

9. Måle risikoens verdipåvirkning

I ERM-sammenheng representerer ordet *verdi* betydningen av å bruke overordnede måltall i kvantifiseringsprosessen av risiko. Selskapene trenger måltall som fanger opp verdien av selskapet for aksjonærene og potensielle investorer. Ledelsen trenger også måltall som kan støtte opp under deres beslutninger og prestasjonsledelse. Dersom selskapet handles på børsen, vil den viktigste eksterne aktøren være aksjonærene. Aksjonærverdier representeres av markedskapitalisering. Markedskapitalisering defineres som aksjepris multiplisert med antall utestående aksjer. Overfor ledelsen defineres aksjonærverdi som selskapets verdi. Selskapets verdi vil i denne sammenhengen være gitt ved en intern verdivurdering i forhold til hva selskapets er verdt for hovedaksjonærene. Selskapsverdi vil i ERM-sammenheng være en intern verdivurdering basert på generelle verdsettelsesmodeller, inkludert intern informasjon. Ledelsen kan bruke selskapsverdi som et meget effektivt risikomål. Grunnen til dette er at risikoscenarioer kan kvantifiseres med utgangspunkt i innvirkning på *baseline value*. *Baseline value* defineres som verdien av selskapet ved en discounted cash flow-verdsettelse, dersom alt går etter selskapets forventinger. Avvik fra forventingene vil blir sett på som risikohendelser (ref. definisjonen av risiko: avvik fra forventninger). Dermed er *baseline value* det en investor ville betalt for selskapet i dag, dersom de trodde at selskapet vil ha evne til å utføre sin strategiske plan perfekt og at alt vil gå etter selskapets forventninger.

Likevel bruker de færreste selskaper en intern verdivurdering av selskapet av ledelsesgrunner, og enda færre bruker dette målet som en del av risikostyringen. Ofte blir risiko kvantifisert i kortsiktige måltall som påvirkningen dagens balanse eller neste års resultat. Ettersom risikohendelser kan påvirke selskapet i lang tid fremover vil slike kortsiktige måltall ikke være tilstrekkelig for å fange opp den totale risikopåvirkningen på selskapet, og vil heller ikke fungere optimalt som informasjon i selskapets strategiske beslutningsprosess.

10. Hovedfokus på aksjonærene

I tradisjonell risikostyring er det ofte slik at ledelsen fokuserer og basere sin risikostyring på å opprettholde kreditt-rating ovenfor ratingbyråene. I tillegg fokuserer finansinstitusjonene også tungt på å overholde regulatoriske krav og spesielt anvises det da til regulatoriske kapitalkrav. Tradisjonelt har finansinstitusjonenes risikostyring fokusert helt og holdent på å tilfredsstille regulatorene. På den ene siden er dette forståelig på grunn av tradisjonell risikostyrings ensidig fokus på negativ risiko og risikobegrensning. På den andre siden er ERMs tilnærming til risikostyring mer strategisk, og inkluderer også potensielle positive konsekvenser av risiko. ERM fokuserer også på overordnede måltall for selskapet, nemlig selskapsverdi og ikke regulatorisk kapital og økonomisk kapital. Regulatorer og ratingbyråer er fremdeles viktige, men kommer i andre rekke etter aksjonærene. Av den grunn er det ikke optimalt å gjøre regulatorene og ratingbyråene maksimalt fornøyde, fordi det ofte kommer på bekostning av aksjonærene. Eksempel på dette er finansinstitusjoner som holder for mye reservekapital kun for å blidgjøre ratingbyråene. For mye reservekapital resulterer i at en ikke får investert denne kapitalen i andre lønnsomme prosjekter og går glipp av fremtidig vekst og avkastning.

ERM ønsker å rette fokuset mot å øke aksjonærenes verdier. Ratingbyråene og regulatorene blir tatt hensyn til, men bare indirekte, gjennom konsekvensene på selskapsverdi. Å tilfredsstille ratingbyråer og regulatorer vil, til et visst punkt, også være i aksjonærenes interesse. For eksempel vil bankene ved risk-return avveininger, der målet er å maksimere selskapsverdi, også være nødt til å ta hensyn til ratingbyråenes betingelsene, fordi lavere rating vil resultere i redusert verdi av selskapet. Det samme vil være tilfellet for dersom en ikke tar nok hensyn til regulatorenes krav. Bankene vil da kunne bli utsatt for sanksjonere eller handlinger rettet mot selskapet som reduserer selskapets verdi og dermed aksjonærenes verdier.

5.2 Ekstern Risikorapportering og kommunikasjon med aksjonærer

Ekstern risikorapportering er kommunisering av ERM-informasjon til eksterne aktører. Det fokuseres på fire forskjellige stakeholders i Segals rammeverk, men jeg vil hovedsakelig fokusere på frivillig kommunikasjonen med aksjonærer, potensielle investorer og finansanalytikere. Åpenhet med tanke på risiko og risikostyring i bankene, refererer

hovedsakelig til informasjonsdeling og kommunikasjon med aksjonærer og potensielle investorer. Det er viktig å skille mellom to former for kommunikasjon. Informasjonsdelingen inngår i regulering fra myndighetene, men kan også være frivillig fra selskapets side.

Frivillig åpenhet angående risiko er risikoinformasjon som ledelsen selv velger å dele med offentligheten og overgår informasjonskravet fra Finanstilsynet. Et eksempel er årsrapporter og pilar 3 rapporter fra bankene. Det kan argumenteres for at banker med velutviklete ERM-programmer, burde inkludere enkle beskrivelser og bevis for ERM i den frivillige kommunikasjon med aksjonærene. Dette kan gi sterke signaler til aksjonærer og potensielle investorer om at selskapet virkelig har et fokus på risk-return-ledelse og et bedre utgangspunkt for å gjennomføre selskapets strategiske planer.

Graden av frivillig informasjonsdeling påvirkes av flere faktorer. På den ene siden vil ikke selskapet dele for mye informasjon dersom de anser sin risikostyring og kontroll som svak. I tillegg kan risikostyringen anses som et konkurransefortrinn bankene ikke vil dele med konkurrentene. På den andre siden vil de vise aksjonærer og investorer at de har et solid og verdiskapende risikostyringssystem som gjør selskapet mer attraktivt for investorer (Segal, 2011).

Momenter som kan være passende å kommunisere til aksjonærer er for eksempel en sammensatt oversikt over ERM-programmet. Oversikten bør presentere at risikostyringen er selskapsomfattende og at selskapet inkluderer alle kilder til risiko (strategisk-, operasjonell- og finansiell risiko). Det er også viktig å få frem det strategiske fokuset for risikostyringen og hvordan ERM fører til at ledelsen fokuserer på de største truslene selskapet står ovenfor. Et velutviklet ERM-program reflekterer også at ledelsen bruker aggregerte måltall for forståelse av risikoeksponering og definisjonen av risikoappetitt på selskapsnivå. Koblingen mellom risikoeksponering og appetitt representerer også evnen til å effektivt håndtere risikoeksponering innenfor de grenser som er satt. Et annet aspekt det burde legges vekt på ovenfor aksjonærer og potensielle investorer er hvordan ERM kan føre med seg konkurransefortrinn, dersom gjort skikkelig. Det gjennom bedre risk-return-beslutninger ved å linke risikostyringssytement til verdibasert ledelse. I tillegg blir ledelsens intensiver bedre sammensluttet med aksjonærens interesser, ettersom selskapsverdi er den overordnede

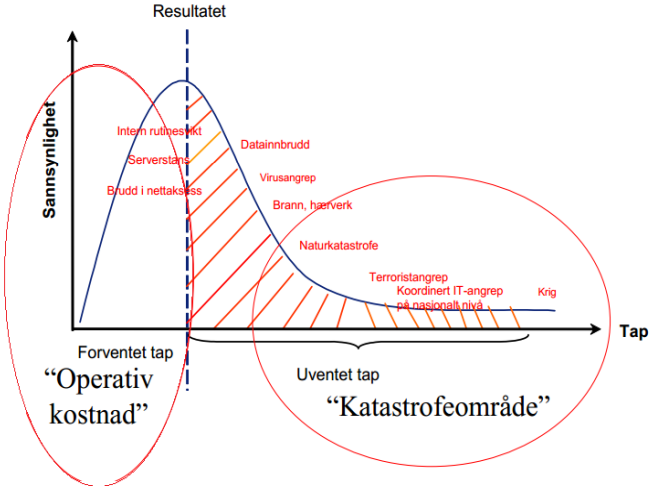
målverdien for ledelsen. Virksomhetsområdenes resultatanalyse blir også forbedret ved bruk av ERM-informasjon (Segal, 2011).

5.3 Operasjonell risiko

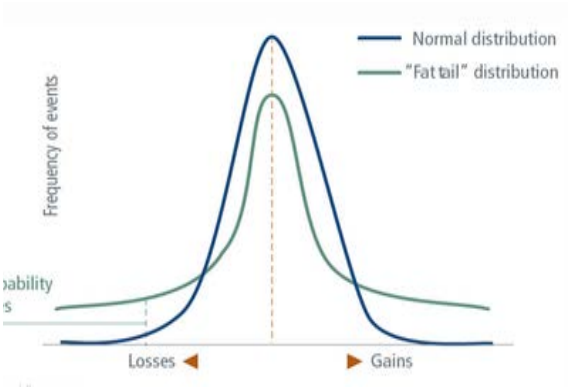
Operasjonell risiko er vesentlig forskjellig fra andre typer risiko bankene står ovenfor, og er integrert i enhver aktivitet bankene foretar seg, og i ethvert produkt. I kontrast med finansiell risiko (markedsrisiko, kredittrisiko og likviditetsrisiko), er operasjonell risiko vanskelig å måle og modellere. Operasjonell risiko materialiseres i finansielle tap gjennom interne eller eksterne hendelser, trender eller endringer som følge av ledelse og eierstyring, interne kontrollsystemer, policyer, organisasjonen, etiske standarder mm. Risikoen er heller ikke like lett å eliminere, da det ikke bare er å selge seg ut av en posisjon i markedet etc. Utfordringene tilknyttet kvantifisering av operasjonell risiko, gjør også at risikokategorien i mange tilfeller blir undervurdert i forhold til dens andel av den totale risikoeksponeringen i et selskap.

Operasjonell risiko har en tendens til å ha større haler i sannsynlighetsfordelinge enn andre typer risiko og generelt et dårligere historisk datagrunnlag. I risikostyringssammenheng representerer haler ytterpunktene i sannsynlighetsfordelingen der midtpunktet representerer forventningene. Ytterst i halene vil vi finne de risikohendelsene som har enorme konsekvenser for organisasjonen, men lav sannsynlighet for å inntreffe (se figur 3 og 4).

Resultatet av manglende datagrunnlag for operasjonell risiko, er at modellene blir ømfintlige og ny data kan gi store endringer i modellenes output. Som et videre ledd av dette vil også operasjonell risikokapital være ustabil. Til tross for dette har regulatorene et mer rigid modellsyn på operasjonell risikokapital enn andre typer risikokapital. Ved at nye data skaper usikkerhet i modellenes kalkuleringer, vil det kunne dempe insentivene for bankene til å investere i og forbedre virksomhetens kontrollprosesser.



Figur 5:Sannsynlighetsfordeling av operasjonell risiko (NIRF, 2007)



Figur 6: Fat tail sannsynlighetsfordeling (Rose, 2013)

Overnevnte sannsynlighetsfordeling gir et bilde av de operasjonelle risikoene finansinstitusjonene står ovenfor og sannsynligheten for at de vil inntreffe.

De vanligste kildene til operasjonell risiko er presentert under (se også appendiks tabell 1):

- *Humankapital* - ansatte yter ikke som forventet, slik som uventede endringer i ansettelse og utvikling av talenter, ytelse/resultat, produktivitet og oppførsel/opptreden.
- *Teknologi* - Teknologien gir ikke den ytelsen eller det resultatet som er forventet. Noen eksempler inkluderer datasikkerhet, konfidensiell og privat data, dataintegritet, kapasitet og pålitelighet.
- *Rettsaker og søksmål* - Uventede søksmål eller dommer mot selskapet
- *Påkrevde standarder* - Grad av standard matcher ikke forventningene (mht kvalitet, sikkerhet, utslipp etc.). Dette gjelder også den finansielle rapporteringen. For finansinstitusjoner gjelder spesielt etterfølging av Basel II og potensielle sanksjoner dersom institusjonene ikke oppfyller de påkrevde standardene for helhetlig risikostyring, rapportering og reservekapital.
- *Ekstern svindel* - Uventede endringer i grad eller antall svindler fra eksterne aktører rettet mot selskapet. Intern svindel faller inn under humankapital.
- *Katastrofer /ulykker* - Uventede natur- eller menneskeskapte katastrofer slik som værrelaterte (orkan, oversvømmelse, tornado, jordskjelv), helserelaterte (pandemier), ulykker (brann), generelle destruktive handlinger (krig, terror og opptøyer) og

spesifikke destruktive handlinger rettet direkte mot selskapet (tukling med produktet eller tjenesten som leveres, angrep på ansatte og sabotasje). Dette inkluderer også uventede menneskeskapte katastrofer forårsaket av ansatte eller agenter som miljøskader etc.

- *Prosesser* - Selskapets prosesser fungerer ikke som forventet.

6. Analyse

Analysen som følger vil fokusere på utfordringer knyttet til å oppfylle de ti kriteriene for en effektiv ERM-prosess i lys av den operasjonelle risikostyringen. Eksempler vil hentes fra de utvalgte bankene. Felles diskusjon gjelder tilfeller der de utvalgte bankene i oppgavene, opererer med samme metode innenfor operasjonell risikostyring eller i sin overordnede tilnærming til risikostyringsprosessen. Avsluttende i analysen vil jeg gjøre noen generaliseringer på tvers av de bankene som blir studert. Det er viktig å merke seg at diskusjon og drøfting ikke nødvendigvis representerer eller gjør seg generaliserbar for alle norske banker, men at analysen skal være med på å kaste lys over potensielle utfordringer og forbedringsmuligheter bankene står ovenfor i årene som kommer. Ikke alle de ti kriteriene i rammeverket lar seg analysere like godt ut i fra den informasjonen som er tilgjengelig. Dermed vil det være en naturlig vektlegging og utdypning av enkelte kriterier, mens noen kriterier vil ha en noe mer kortfattet diskusjon. Eksemplene gitt i analysen er basert på informasjon hentet fra de tre bankenes risiko- og kapitalstyringsrapporter.

6.1 Selskapsvidt omfang

Det først kriteriet innenfor en effektivt ERM-prosess er at risikostyringen bør være av et selskapsvidt omfang. Begrepet selskapsvidt gir uttrykk for at alle virksomhetsområder inkluderes. I både Nordea, DNB og SpareBank 1 SR-Bank virker det tilsynelatende som at den operasjonelle risikostyring er en selskapsomfattende prosess ved at bankene selv uttaler dette i rapportene sine. DNB påpeker for eksempel at deres risikostyring er et konsernovergripende system, som er en riktig tilnærming i forhold til en effektiv ERM-prosess. Det er viktig at risikostyringssystemet omfatter hele organisasjonen fordi banken aldri kan vite hvor den operasjonelle risikoen vil oppstå.

Det er også slik at Finanstilsynet nøye overvåker at kvaliteten i risikostyringen er tilstrekkelig for den regulerte virksomheten i bankene. Strenge regulatoriske krav fører indirekte med seg en tvungen selskapsvid tilnærming for bankene og fungerer slik at institusjonene unngår fallgruver som ikke-regulerte organisasjoner kan havne i. Med strengt

oppsyn unngår en for eksempel å overse virksomhetsområder som genererer høy profitt eller områder som i utgangpunktet er sett på som for små til å generere "betydningsfull" risiko.

Bankerne står likevel ovenfor utfordringer når det kommer til å få ERM-programmene sine ut i alle deler av virksomheten og det kan spekuleres i om risikostyringen faktisk er konsernovergripende. Problemer vil kunne oppstå ved at deler av bankenes virksomhet ikke er regulert, og dermed at regulatorisk- og økonomisk kapital ikke er et risikomål i denne delen av virksomheten. Økonomisk kapital blir brukt som et internt mål både i Nordea, DNB og SpareBank 1 SR-Bank, men risikomålet vil ikke nødvendigvis være aktuelt eller tilgjengelig for de ikke-finansielle tjenestene bankene tilbyr. Flere og flere banker ekspanderer sin virksomhet til også å inkludere for eksempel konsulent og rådgivningstjenester. Disse tjenestene vil ikke nødvendigvis ha kapitalkrav, og det vil være lett for bankene å utelukke fra det helhetlige risikostyringssystemet.

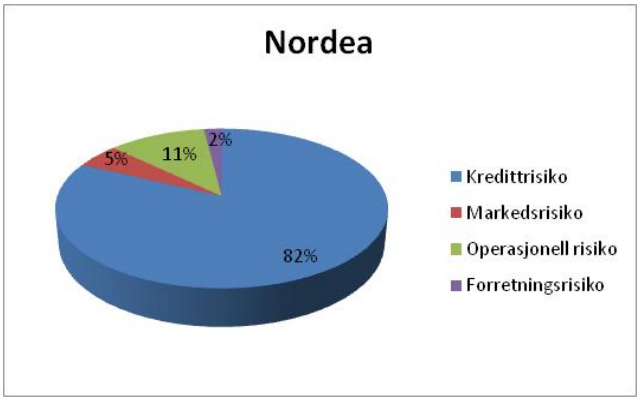
En potensiell fallgruve for dagens banker er betraktningen om at de tjenestene som ikke reguleres, kun står for en forsvinnende liten del av institusjonens totale virksomhet. Bankene skal være oppmerksom på at størrelsen på virksomhetsområdene ikke nødvendigvis har en direkte sammenheng med størrelsen på de potensielle operasjonelle risikoene som kan opptre i disse virksomhetsområdene. Selv om det virker lite sannsynlig at halen for den operasjonelle risikodistribusjonen inkluderer potensiell risiko som oppstår i områder som er en liten del av bankenes totale virksomhet, er det fortsatt mulig. Manglende data på halehendelser gir lite grunnlag for at bankene kan konkludere med slike tjenester ikke genererer potensielle alvorlige risikoer. Operasjonell risikostyring er fortsatt i utvikling, nettopp på grunn av manglende erfaring og kunnskap om potensielle halehendelser. Det er derfor viktig å inkludere alle områder av institusjonens virksomhet i den operasjonelle risikostyringen, fordi en aldri kan vite hvor risiko vil oppstå.

6.2 Alle risikokategorier inkludert

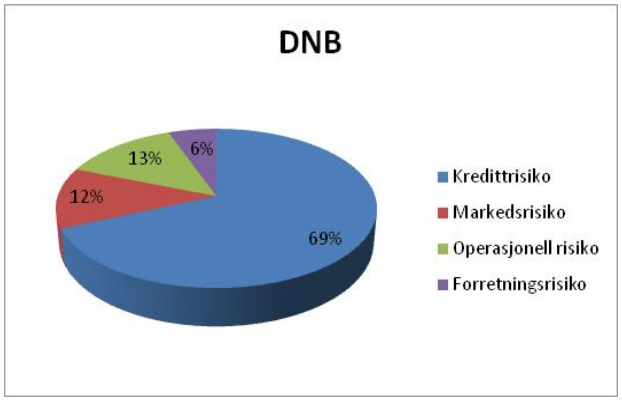
En effektiv risikostyring krever at bankene har den totale oversikten over virksomhetens risikobilde. For å få denne oversikten må bankene inkluderer alle former for risiko i sitt risikostyringssystem. Basel II var et stort skritt i riktig retning for bankene i å inkludere alle risikokategorier, fordi avtalen la vekt på styring og kontroll av operasjonell risiko som

tidligere ikke var inkludert i den regulerende avtalen. På denne måten står bankene nå ovenfor krav for både operasjonell og finansiell risikostyring. Vektleggingen av strategisk risiko, som den siste av de tre hovedkategoriene for risiko, i bankenes rapporter er begrenset og det nevnes kun med få ord i pilar 3-rapporten til Nordea, DNB og SpareBank 1 SR-Bank. Krav fra myndighetene inkluderer enda ikke strategisk risiko og er sannsynligvis bakgrunnen for at bankene ikke deler informasjon tilknyttet styring av denne risikokategorien med det offentlige. Det er dog slik at bankene i all hovedsak har retningslinjer og prosedyrer for strategisk risikostyring, men at diskusjonen foregår internt og at informasjonen anses som sensitiv og konkurransehemmende dersom den kommer ut.

Bankene uttaler også at det fortsatt er problemer tilknyttet kvantifisering av operasjonell risiko i interne modeller, fordi utviklingen av rammeverk og kvantifiseringsmodeller ennå henger etter i forhold til de finansielle modellene. Dette vil si at operasjonell risiko er inkludert som en risikokategori, men at bankene ennå ikke har optimalisert identifiseringsmetodene og kvantifiseringsmodellene på grunn av manglende historisk data og kunnskap. Begrenset kunnskap og data er også bakgrunn for at de norske bankene enda ikke har kunnet ta i bruk den avanserte metoden for beregning av regulatorisk kapital.



Figur 8 Distribusjon av total økonomisk kapital fordelt på risikokategorier Nordea.



Figur 7: Distribusjon av total økonomisk kapital fordelt på risikokategorier DNB.

Diagrammene ovenfor gir et inntrykk av fordeling mellom de ulike risikokategoriene i forhold til den totale økonomiske kapitalen i både Nordea og DNB. Operasjonell risiko er allerede en betydelig andel av den totale økonomiske kapitalen og det uten hensyn på at kvantifisering av operasjonell risiko ennå er en stor utfordring i bankene. Blant annet er det utfordringer tilknyttet skillet mellom operasjonell risiko og kredittrisiko i enkelte tilfeller. Et

eksempel knyttet til overnevnte, er dersom en ansatt innvilger et lån som ikke skulle vært innvilget ut i fra bankens kredittpolicy, og kunden deretter misligholder låntet. Slike tilfeller blir ofte rapportert som kredittrisiko, selv om det definisjonsmessig er en operasjonell risikohendelse. Dette forsterker betydningen av operasjonell risikostyring i finansinstitusjonene, og fremhever de potensielle verdier ved effektiv styring.

6.3 Fokus på nøkkelrisikoer

Fokuset på nøkkelrisikoer innenfor operasjonell risiko er viktig på grunn av den kognitive begrensningen til ledelsen og styret. For bankenes ledelse og styre vil det være tilnærmet umulig å håndtere en liste med flere hundre eller tusen forskjellige risikoer. Dersom bankene ikke har et konkret fokus på nøkkelrisikoer, vil listen over operasjonelle risikoer raskt bli for lang og kvaliteten i styringen, rapporteringen og oppfølging av risikoene og deres eventuelle begrensningstiltak, vil kunne reduseres. I tillegg er det ikke kun operasjonell risiko som skal håndteres av toppledelsen og styret, men også den finansielle og strategiske risikoen. Utfordringen for institusjonene er å ha et selektivt fokus på de operasjonelle risikoene som utgjør hovedtruslene for selskapet. I finansinstitusjoner vil finansiell risiko naturlig utgjøre en større del av det totale risikobildet og operasjonelle risikoer er sannsynligvis ikke majoriteten av nøkkelrisikoer. Det er da enda viktigere å ha kvalitet i identifisering og kvantifiseringsprosessen, slik at ledelsen og risikoavdelingen i bankene kan rapporter kun et selektert antall operasjonelle risikoer til styret og som blir fokusert på i den overordnede risikostyringen.

Prosessene fram mot et eventuelt fokus på nøkkelrisikoer involverer hovedsakelig identifisering og kvantifisering av risiko. Det er i disse to fasene (se tidligere definisjon av ERM-prosessen) at en danner en oversikt over institusjonens risikobilde og skaper et utgangspunkt for prioritering av risiko. Det er avgjørende at ledelsen og styret får informasjon om operasjonelle nøkkelrisikoer, fordi de ikke bare er av betydning for virksomhetsområdet risikoen oppstår i, men også for selskapet som helhet. Potensielle risikoer vil i stor grad kunne påvirke institusjonenes overordnede strategitilnærming, finansielle resultat og eksterne omdømme. Omdømmeskade relaterer seg ofte til for eksempel IT- og informasjonsrisiko.

Nordea gjennomfører en RCSA-prosess (Risk and Control Self-Assesment) som har til hensikt å identifisere og håndtere operasjonell risiko. Prosessen baserer seg på et bibliotek av operasjonell risiko der divisjonslederne bruker biblioteket til å identifisere hvilke risikoer som er relevant for sine respektive virksomhetsområder. Risikoene blir identifisert gjennom en topp-bunn tilnærming med involvering fra ledelsen og en nedenfra-opp tilnærming med scenarioanalyser, hendelsesdatabaser, kvalitativ risikoanalyse, ekspertvurderinger og informasjon fra forretningsprosesser. Biblioteket gir et godt grunnlag for prioritering av risiko og dermed identifisering nøkkelrisikoer. Det som er viktig i en prosess som presentert for Nordea, er at de påkrevde hendelsesdatabasene ikke blir for dominerende i risikoidentifiseringsfasen. Hendelsesdatabasene inneholder ofte veldig mange og spesifikke risikohendelser som i et overordnet perspektiv ikke vil være signifikant betydning for styringen av selskapet. Dersom databasen forblir listen over risikoene selskapet står ovenfor, vil ikke ledelsen ha kapasitet til å følge opp alle risikoene. Resultatet kan bli at ingen risikoer blir fulgt opp tilstrekkelig med tilhørende begrensningstiltak. Fokuset for bankene bør ligge på de risikoene som scorer høyest på prioriteringslisten, ved en avveining av sannsynlighetene for at en risikohendelse vil inntreffe og de konsekvensene risikohendelsen vil ha for selskapet.

Ved å involvere flere informasjonskilder i prosessen vil banken kunne unngå et ensidig fokus på hendelsesdatabasen, og muliggjøre bedre prioriteringer i institusjonens operasjonelle risikostyring. Bankene bør være oppmerksomme på at det å ta utgangspunkt i tidligere tapshendelser i identifiserings- og kvantifiseringsfasen kan føre til et for retrospektivt syn på risiko. Risikohendelser som allerede har opptrådt i virksomheten vil ikke nødvendigvis opptre igjen. Kanskje har bankene allerede iverksatt begrensningstiltak for enkelte av de registrerte tapshendelsene, i tillegg til at en risikotype sjeldent har et identisk hendelsesforløp fra gang til gang. Dersom banken for eksempel opplevde en alvorlig feil ved at en ansatt var delaktig i hvitvasking og hendelsen påførte et betydelig tap, er sannsynligheten høy for at allerede strenge kontrolltiltak er iverksatt og at denne risikoen ikke vil opptre igjen eller på samme vis. Altså er risikohendelsen, selv om den er ført i hendelsesdatabasen og hadde betydelig konsekvenser for banken, ikke nødvendigvis fortsatt en nøkkelrisiko for selskapet. I tillegg bør potensielle risikoer som ikke er registrert i hendelsesdatabasene også vurderes som en del av identifiseringen og kvantifiseringen.

Både Nordea og DNB går konkret inn på ulike nøkkelrisikoer innenfor operasjonell risikostyring i sine rapporter. Dette er viktig å kommunisere til aksjonærer, analytikere og potensielle investorer, fordi de reflekterer forståelse fra bankens side om mulige fremtidige risikoscenarioer. Ved å gi informasjon tilknyttet nøkkelrisikoene, viser banken at de er observante på disse risikoene og er forberedt dersom de vil komme til å inntreffe.

Hvitvasking og terrorfinansiering blir identifisert som to typer operasjonell risiko som bankene er spesielt oppmerksomme på i både Nordea og DNB. Et relatert diskusjonsmoment er her at det er viktig å skille mellom nøkkelrisikoer bankene *faktisk* står ovenfor og risikoer regulatoriske myndigheter *mener* bankene er spesielt utsatt for. Hvitvasking og terrorfinansiering er risikoer myndighetene er spesielt fokusert på i forhold til sin overvåkning på grunn av trusselen mot velferdssamfunnet (Finansdepartementet, 2009). Spørsmålet er da om dette virkelig er operasjonelle nøkkelrisikoer bankene står ovenfor eller om fokuset er hovedsakelig compliance-drevet. Dersom bankene allerede har gjort omfattende tiltak for å forhindre risikohendelser av denne art, kan det være verdifullt å kommunisere det til eksterne aktører, men bør ikke presenteres som en nøkkelrisiko for banken. En risiko som allerede er tatt hånd om og bankene allerede har utviklet omfattende begrensningstiltak for å fjerne, vil ikke lenger være en nøkkelrisiko for institusjonen.

Cyberterrorisme, teknologisk svikt og datatap har blitt et fremtreende problem med den økende bruken av avanserte informasjonssystemer og bankvirksomhet på nett. For å berolige investorer, aksjonærer og kunder er det viktig at slike risikoer blir adressert og at det gis et inntrykk av at dette gjøres noe med. På grunn av konkurransehemmende effekter er det mulig at bankene ikke ønsker å gå ut med detaljer rundt konkrete tiltak, men et overordnet perspektiv på at noe gjøres bør være et minimum. Fra en tidligere undersøkelse kommer det frem at internasjonale banker retter et økende søkelys mot det som blir kalt utradisjonell risiko (Hans Helbekkmo, 2014). Bankene i undersøkelsen fremhever cyberrisiko, informasjonsteknologirisiko og compliance-risiko som de mest fremtredende formene for utradisjonell risiko.

Cyberrisiko og informasjonsteknologirisiko fremheves som potensielle risikoer for fremtiden av Nordea. Det er viktig at bankene har en tilnærmet kontinuerlig prosess med å identifisere og kvantifisere operasjonell risiko, slik at de kan "flagge" nye nøkkelrisikoer dersom de

kvalifiseres til prioriteringslisten over nøkkelrisikoer. DNB nevner kort i sine rapporter at de forventer økende risiko knyttet til IT-sikkerhet og angrep mot bankens informasjonssystemer. De overnevnte risikoene fremstilles også av empiriske undersøkelser å være av store betydning for bankene i tiden fremover. På den ene siden må det presiseres at bankene har individuelle risikobilder i den forstand at listen av nøkkelrisikoer vil være forskjellige fra bank til bank. På den andre siden vil det fortsatt kunne være flere operasjonelle risikoer som er sammenfallende for banknæringen under ett. Som et resultat av teknologisk utvikling, mer avanserte og detaljerte informasjons- og IT systemer og fusjoner og oppkjøp, har bankene økte utfordringer i å oppgradere, integrere og beskytte systemene på tvers av institusjonen, og dette krever store investeringer å få til. De tre bankene representert i oppgaven håndterer betydelig mengder sensitiv data som er utsatt for lekkasje og kriminelle aktiviteter.

Selv om bankene ikke eksplisitt rapporterer en liste med konkrete nøkkelrisikoer til eksterne aktører, er det ikke nødvendigvis representativt i forhold til om de faktisk har nøkkelrisikofokuset internt i institusjonen. DNBs rammeverk for risikoappetitt tyder at dette kan være tilfellet. Rammeverket består av utsagn angående den operasjonelle risikoen som reflekterer de risikoene som ledelsen og styret har vurdert til å ha størst betydning for konsernet. Utsagnene har tilhørende fastsatte grenser for risikoeksponering. På denne måten vil risikoappetitten representere et selektert antall operasjonell risikoer som kan effektivt følges opp av bankens ledelse. Det skaper oversiktlighet og relevans for den overordnede styringen. Operasjonell risiko ble inkludert i DNBs rammeverk for risikoappetitt i 2013. Rapporteringen til ledelsen og styret i både Nordea og DNB er en selektiv prosess som velger ut enkelte fokusområder for den operasjonelle risikostyringen (strategisk operasjonell risikostyring).

6.4 Integrering på tvers av risikotyper og virksomhetsområder

En felles tilnærming til operasjonell risiko som går igjen hos alle bankene representert i oppgaven er, at synet på operasjonell risiko som utelukkende negativt. Det siktes da til at operasjonell risiko er noe bankene ønsker å kvitte seg meg og at denne typen risiko ikke har avkastning knyttet til seg. Faren ved denne tankegangen er at bankene vil kunne tilnærme seg operasjonell risikostyring ved siloledelse og at styringen foregår isolert i hvert enkelt

virksomhetsområde eller isolert for hver risikotype. Dersom det ikke finner sted noen risk-return avveininger på selskapsnivå, er det lett for ledelsen å delegere beslutningsmyndigheten ned til virksomhetsområdenivå.

Videre vil jeg hovedsakelig fokusere på integrasjon på tvers av virksomhetsområdene, som er av størst relevans for Nordea, DNB og SpareBank 1 SR-Bank.

Den vesentlige faren ved delegering av beslutningsmyndighet, er hvis grensene og eksponeringen for operasjonell risiko kun settes og kalkuleres individuelt ved de ulike virksomhetsområdene og ikke først på et aggregert plan. Det henvises da til styring og kontroll av nøkkelrisikoer, og ikke de mindre operasjonelle risikoene som ble identifisert og kvantifisert og som ikke havnet øverst på prioriteringslisten. Aggregering av områdenes risikoeksponering burde gjøres av ledelsen, styret, uavhengige risikokomiteer og eksperter fra virksomhetsområdene for at en skal se områdenes ulike potensielle risikoer i sammenheng og fange opp eventuell interaksjon og korrelasjon mellom risikoene. Ved en silotilnærming til operasjonell risikostyring gjør det seg vanskelig å fange potensielle simultane risikohendelser på tvers av risikokategorier og virksomhetsområder. Antakelser om perfekt positiv korrelasjon eller ingen korrelasjon, vil kunne resultere i redusert verdi av ERM-prosessen. Både DNB og SpareBank 1 SR-Bank antar at perfekt positiv korrelasjon eller ingen korrelasjon mellom de ulike forretningsprosessene er urealistisk, og tar høyde for antakelsen ved å inkludere en diversifiseringseffekt i aggregering av totale operasjonell risikoeksponering.

Risikokorrelasjon kan være et resultat av tilfeldigheter, men kan også ha røtter i statistisk samvariasjon eller underliggende kausale sammenhenger. Statistisk samvariasjon er der en finner en statistisk sammenheng mellom to ulike operasjonelle risikotyper. Det kan enten vise seg at risikotypene har en tendens til å opptre sammen, eller det kan være slik at når den ene risikoen inntreffer, så inntreffer den andre risikoen mest sannsynlig ikke. Korrelasjon som et resultat av underliggende kausale sammenhenger representerer en av de større utfordringene i bankenes operasjonelle risikomodellering. Et eksempel på denne typen korrelasjon kan være at en svak organisasjonskultur kan lettere gi grobunn til internt bedrageri, men også risiko tilknyttet nye produkter og kundebehandling. Dersom bankene kan klarer å inkludere samtlige korrelasjonsrelaterte faktorer i sine modeller for beregning av

økonomisk kapital, vil modellene kunne bli langt mer nøyaktige og et bedre representativt bilde av bankens reelle operasjonelle risiko.

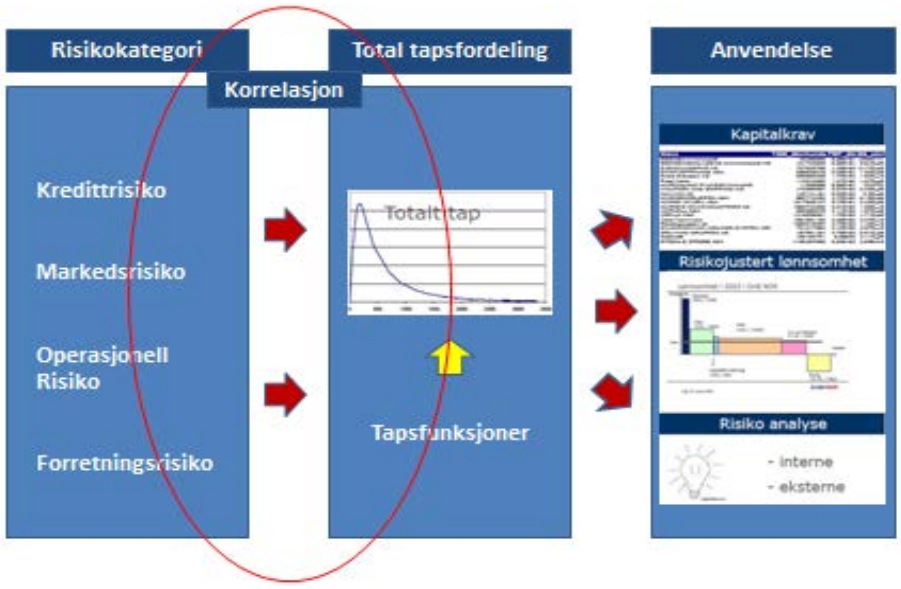
Bankenes modeller tar utgangspunkt i at aggregering av potensielle operasjonell risikoer fører til perfekt positiv korrelasjon, ved at de utvalgte risikoscenarioene, med tilhørende tapsverdier, aggregeres opp ved addering. Total risikoeksponering vil da fremkomme av totalkonsekvensen av alle risikoscenarioene fra forretningsprosessene samlet. Bankene bruker så en diversifiseringseffekt som representerer antagelsen om at ikke alle risikoer vil opptre samtidig (perfekt positiv korrelasjon), men at det finnes delvis korrelasjon $(0 < \rho < 1)$ mellom risiko i de ulike virksomhetsprosessene. En vil da kunne inkorporere noe av kompleksiteten institusjonene står ovenfor i virksomheten, ved at flere risikoer opptrer samtidig i ulike prosesser. På denne måten prøver en å unngå at risikostyringen blir ufullstendig da institusjonene tar hensyn til delvis avhengighet.

SpareBank 1 SR-Bank bruker en etterjustert diversifiseringseffekt for å ta høyde for delvis korrelasjon mellom ulike risikoer, virksomhetsområder og prosessområder. Dette gjøres i aggregeringen av total operasjonell risikoeksponering og etter individuell risikoeksponering er kvantifisert. Det vil kunne være svakheter i denne tilnærmingen ved at beregningsgrunnlaget for diversifiseringseffekten er begrenset og blir ofte gjort på bakgrunn av ekspertvurderinger og erfaring. En slik tilnærming vil kunne føre til for mye eller for lite kapital da diversifiseringseffekten blir lite nøyaktig.

						Risikoprofil	
Forretningsprosesser	Totalkonklusjon risikoprofil	Trend	Risiko-Indikator	Effekt av kontroll- og styringstiltak		Forventet tap	Uventet tap
Betalingsformidling		→			Høy	2	200
Sparing / plassering		↑			Høy	1	100
Finansiering		↓			Middels	17	130
IKT		↓			Høy	1	65
Datterselskap		→			Svært høy	4	250
Sum før diversifisering						25	745
Diversifisering							400
Sum etter diversifisering							345

Figur 9: Illustrasjonseksempel av korrelasjonsjusteringer i operasjonell risiko for SpareBank 1 SR-Bank

Det er fortsatt en stor utfordring for institusjonene å få en effektiv integrering på tvers av virksomhetsområdene fordi utviklingen innenfor operasjonell risikomodellering og det historiske datagrunnlaget ennå er begrenset. Det indikeres også av DNBs modell for beregning av økonomisk kapital. Banken tar utgangspunkt i sjablongmetoden både ved kalkulering av regulatorisk kapital og økonomisk kapital. Ved beregning av økonomisk kapital skaleres beregningsgrunnlaget opp med 25 % fra hva som var grunnlaget ved regulatorisk kapital. Korrigering for delvis korrelasjon skjer også her ved å inkludere en diversifiseringseffekt, dog med bakgrunn i total økonomisk kapital for virksomheten. Korrelasjonsjusteringene blir da gjort på tvers av risikokategori og ikke innenfor kategorien for operasjonell risiko. En av grunnene til at DNB på nåværende tidspunkt bruker en så enkel og lite detaljert modell for kvantifisering av operasjonell risiko, kan være det som er poengtert tidligere om manglende kunnskap, erfaring og utvikling på området. Det eksisterer rett og slett ikke noen ideell modell på nåværende tidspunkt.



Figur 10: Korrelasjonsjusteringer på selskapsnivå i DNB

Som vi ser av eksemplene tar begge bankene hensyn til delvis korrelasjon mellom forretningsprosesser, men kun indirekte ved etterjustering for en diversifiseringsfaktor. Hos SpareBank 1 SR-Bank blir etterjusteringene gjort på operasjonelt risiko nivå, mens DNB

gjør justeringene i enklere modeller på totalrisiko nivå. Det kan argumenteres for at korrelasjonsjusteringene bør gjøres på totalrisikonivå og ikke på operasjonell risikonivå. Bankene vil da kunne inkludere korrelasjon mellom ulike risikokategorier og tar dermed hensyn til at operasjonell-, finansiell og strategisk risiko kan opptre samtidig enten på tvers eller innenfor samme virksomhetsområder eller forretningsprosess.

Felles for begge tilnærmingene er at det kun fokuseres på eventuelle diversifiseringseffekter. Det som da blir glemt er eventuelle eskaleringseffekter. Risikohendelser som opptrer samtidig kan også forsterke hverandre slik at total konsekvens for selskapet blir større enn summen av konsekvenser for de individuelle risikoene. Halehendelser tar ofte form av denne typen risikoeffekt. Det er relativt begrensede data tilknyttet operasjonelle halehendelser hos norske banker og kan være en av grunnene til at bankene utelukkende ser ut til å fokusere på diversifiseringseffekter. Til tross for at norske bankes manglende erfaringer med halehendelser, er det fortsatt avgjørende å ha en plan dersom en slik hendelse en dag skulle ramme bankene.

Motpolen til skaleringseffekter er utjevningseffekter og bør inngå i diversifiseringseffekten. I enkelte tilfeller kan risikohendelser utjevner hverandre slik at den totale konsekvensen blir lavere enn summen av de individuelle risikokonsekvensene. Poenget kan bedre illustreres med et eksempel: En risikohendelse kan være at nettbanksystemet bryter sammen og at bankkundene mister tilgang til nettbanken. En annen risikohendelse opptrer samtidig, og et feilvurdert fond gjøres tilgjengelig på nett for potensielle private småsparere og investorer. På grunn av at nettbanksystemet er nede, vil det ikke være mulig for investorer å kjøpe fondsandeler på nett, og gir banken mer tid på å rydde opp i og begrense utfallet av feilen. Dermed begrenser den første risikohendelsen utfallet av den andre risikohendelsen, og det totale utfallet er langt mindre alvorlig enn summen av de to individuelle risikohendelsene.

Den begrensede håndteringen av risikoavhengighet kan også føre til ineffektivitet i bankene ved redusert kommunikasjon mellom virksomhetsområdene, og dermed redusert spredning av kunnskap og erfaring på tvers av områdene. Effektiv deling av erfaring og lærdom vil kunne hindres av den indirekte tilnærmingen til risikokorrelasjon presentert i eksemplene fra DNB og SpareBank 1 SR-Bank tidligere. Spesielt vil fraværet av direkte samarbeid om å fastsette grad av korrelasjon påvirke kommunikasjonen dem imellom. Informasjonsdeling og

samarbeid er essensielt dersom bankene effektivt skal kunne integrere korrelasjonseffekter direkte i utformingen av risikoscenarioer og i simuleringsprosessen. Dersom simuleringen av potensielle risikoscenarioer foregår individuelt i de respektive virksomhetsområdene, for så å summeres til total operasjonell risikoeksponering, er det fare for at viktig lærdom og erfaring ikke deles på grunn av fravær av kommunikasjon i simuleringsprosessen.

Vi kan ikke utelukke at eksperter og ledelsen fra de ulike virksomhetsområdene likevel samarbeider ved kvantifiseringen av diversifiseringseffekten og utvikling av risikoscenarioer med simultane risikohendelser. Den tilgjengelige informasjonen gir ikke godt nok grunnlag for å konkludere på punktet. Dersom dette er tilfellet, vil det da kunne være muligheter for å dele erfaringer og kunnskap gjennom prosessen som skjer i *etterkant* av kvantifiseringen av de individuelle virksomhetsområdenes risikoeksponering.

Mangel på kommunikasjon og samarbeid på tvers av områder ved fastsettelsen av de ulike virksomhetsområdenes risikoeksponering, vil også kunne gjøre risikostyringen internt inkonsekvent fordi ulike områder tar ulike forutsetninger og antakelser i sine utforming av risikoscenarioer. Ved for eksempel scenariosimulering vil de grunnleggende antakelsene kunne være forskjellig fra område til område ved estimeringen av antall tapshendelser i forhold til ulike tapsintervaller. Et forebyggende tiltak DNB har innført for å unngå ulike forutsetninger på tvers av institusjonen, er de klart definerte rammeverkene vedtatt av styret, ledelsen og risikoavdelingene.

6.5 Aggregerte måltall

En klart definert risikoappetitt for institusjonen sørger for at bankene kan gi klare signaler fra ledelsen og styret til resten av organisasjonen, om hvordan banken ønsker at den operasjonelle risikostyringen skal være i samsvar med institusjonens strategi. Både Nordea og DNB har et definert rammeverk for risikoappetitt, og operasjonell risiko inkluderes i dette rammeverket. DNB uttaler at styret setter langsiktige mål for risikobildet i selskapet gjennom risikoappetitt. Dette forenkler følging av strategien ved at risikogrenser for vært enkelt virksomhetsområde tar utgangspunkt i selskapets totale risikoappetitt. En klart definert risikoappetitt er også verdifullt fordi prosessen med å sette bankenes risikoappetitt er første steg i beslutningsprosessen i ERM. Grensene for operasjonell risiko må defineres før

en kan vurdere eventuelle begrensningstiltak for å redusere eller eliminere individuell operasjonell risikoeksponering i de ulike virksomhetsområdene. Institusjonens risikoappetitt vil også representere bankenes ønskede nivå av stabilitet og totale volatilitet. Det er nettopp dette perspektivet og denne innfallsvinkelen aksjonærene har i sin vurdering av selskapet.

En utfordring bankene vil kunne stå ovenfor, er begrensninger i forhold til å kalkulere total risikoeksponering på grunn av deres bruk av økonomisk kapital som risikoparameter i institusjonenes interne kapitalvurdering og i regulatorisk kapital. Økonomisk kapital blir brukt av alle tre bankene studert i denne oppgaven, og er i utgangspunktet blitt en bransjestandard ved interne kalkuleringer av operasjonell risikoeksponering. Hva vi ser av risikorapportene til DNB, Nordea og SpareBank 1 SR-Bank er også at risikoeksponeringen hovedsakelig aggregert ved å summere økonomisk kapital tilknyttet operasjonell risiko for hvert virksomhetsområde eller forretningsprosess. Utfordringen ved denne tilnærmingen er for det første at virksomhet i bankene som ikke har kapitalkrav, vil kunne bli ekskludert i beregningene av total risikoeksponering. Dette vil da føre til et ufullstendig bilde av hvilken eksponering bankene faktisk står ovenfor. Det andre er at økonomisk kapital som mål, vanskeliggjør kvantifiseringen av operasjonell risiko fordi måltallet ikke nødvendigvis fanger opp fremtidige konsekvenser på inntekter og kostnader med tanke på risikoer som kan påvirke bankene flere år frem i tid. Et koordinert IT-angrep kan være et eksempel på en slik hendelse. I et slikt angrep kan store mengder sensitiv data gå tapt og kundene vil kunne stille spørsmål til bankenes sikkerhetsrutiner og bankens begrensningstiltak. Hendelsen kan svekke bankenes omdømme og redusere fremtidige kontantstrømmer.

At bankene har aggregert totale økonomisk kapital på selskapsnivå, er uansett positivt ved at institusjonene da har viser forståelse for viktigheten av aggregerte måltall og hvordan dette igjen er essensielt for fastsettelse av risikoappetitt som følger bankenes overordnede strategi. Dermed kan bankene delegere risikogrenser (disaggregert risikoappetitt) til de ulike virksomhetsområdene i tråd med strategien. Økonomisk kapital fungerer også som en standard på tvers av virksomheten og gjøre det enklere for institusjonen å ha en felles tilnærming til ERM-prosessen. Dette muliggjør aggregering av risikomåltall, og gjør det enklere for toppledelsen og styret å sette seg inn i risikosituasjonen institusjonen står ovenfor. På grunn av at standardiserte risikomålingsparametere i virksomhetsområdenes

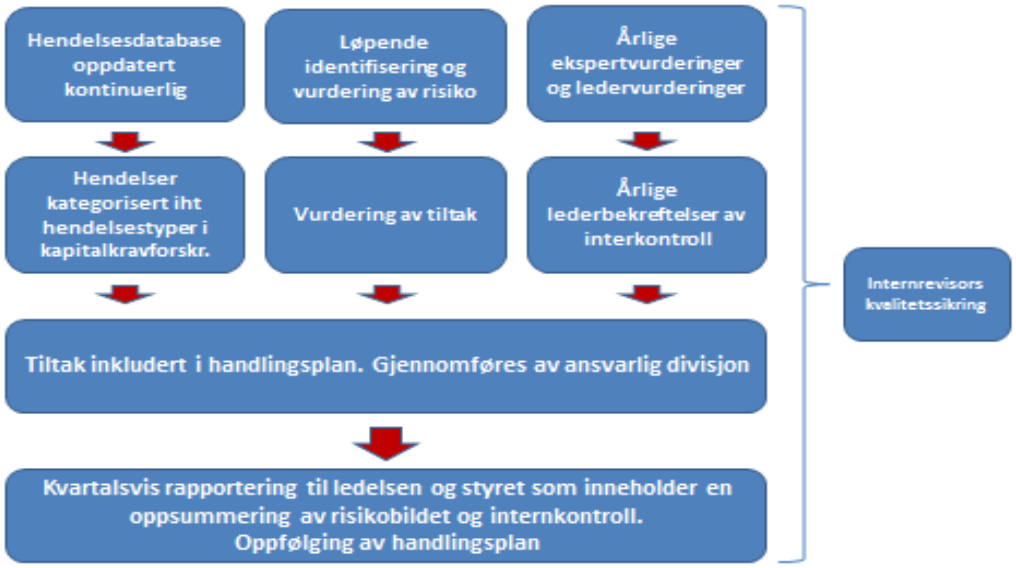
kalkulering av individuell risikoeksponering, forenkles disaggregeringen av selskapets risikoappetitt ned til de forskjellige områdene eller prosessene.

6.6 Inkludert i selskapets beslutningstaking

I de tidligere kriteriene har det vært et sentrert fokus på kvaliteten og overførbarheten i risikoinformasjonen som blir innhentet i identifiserings og kvantifiseringsfasen. Analysen er nå kommet til suksesskriteriene som tar for seg de to siste stegene i prosessen for ERM vi definerte innledningsvis i oppgaven.

Dersom all informasjonen innhentet i tidligere steg ikke blir brukt hensiktsmessig i selskapets beslutningstaking, faller verdien av et ERM-programmet bort. Etter at operasjonelle risikoer er identifisert og risikoeksponeringen er kvantifisert, må informasjonen rapporteres og bankene ta stilling til om de ønsker å iverksette tiltak for å redusere risiko eller om de finner nåværende eksponering og iverksatte tiltak tilfredsstillende. Det eksisterer to ulike tilnærminger til begrensningstiltak. Bankene kan ha et ønske om å redusere volatiliteten i potensielle tap ved å enten redusere sannsynligheten eller konsekvensen av risikoen.

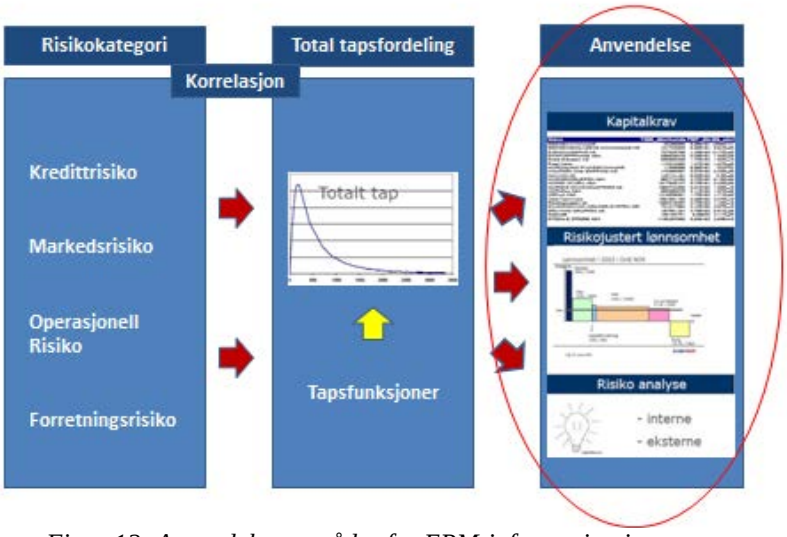
Utfordringen ved flere av dagens risikosystemer i institusjonene er at prosessen stopper etter rapporteringen. Risikoinformasjon blir innhentet og rapportert til ledelsen og styret, men tiltak blir ikke iverksatt hensiktsmessig.



Figur 11: Rammeverk for operasjonell risikostyring i SpareBank 1 SR-Bank

Figuren over gir et bilde av rammeverket til SpareBank 1 SR-Bank for styring av operasjonell risiko. Øverst finner vi informasjonsgrunnlaget innhentet i ERM-prosessen og de tre ulike kildene til informasjon. Deretter ser vi hvordan denne informasjonen er inkludert i vurderingsprosessen av bankens operasjonelle risikobilde og eventuelle tiltak for å redusere risikoeksponeringen. Vurderingene blir så inkludert i en handlingsplan, med konkrete tiltak. Rammeverket reflekterer en god og strukturert inkludering av ERM-informasjon i selskapets beslutningstaking. ERM-informasjonen blir brukt i en handlingsplan som reflekterer ønsket fremtidig risikobilde for institusjonen som også er i tråd med virksomhetens overordnede strategiske mål. I etterkant er det viktig at styret og ledelsen reflekterer over handlingsplanen og den informasjonen som er rapportert. Utfordringen er at de foreslåtte tiltakene blir vurdert og at toppledelsen sørger for at prioriterte tiltakene blir iverksatt.

Informasjon innhentet i tidligere steg blir også brukt til fastsettelse av kapitalkrav for operasjonell risiko, beregning av risikojustert lønnsomhet og intern og ekstern risikoanalyse. Modellen under er hentet fra DNB og viser hvordan den aggregerte risikoinformasjonen blir brukt internt i selskapet. I tillegg bruker linjeledere informasjonen i utviklingen av bestemte styringstiltak for å redusere risikoeksponeringen. Svakheten i rammeverket og utfordringen videre er å få toppledelsen og styret mer involvert i prioriteringen og fastsettelsen av risikoreduserende tiltak. Konsernovergripende operasjonell risiko blir rapportert til styret med tilhørende tiltak.



Figur 12: Anvendelsesområder for ERM-informasjon i DNB

Som et ledd i å inkludere ERM i selskapets beslutningstaking, er også kravene fra Finanstilsynet om utarbeidede beredskapsplaner en viktig faktor. Beredskapsplaner og kontinuitetsplaner utviklet i bankene tar i bruk store deler av informasjon hentet fra hendelsesdatabasen, scenarioutviklingsprosessen og ekspertvurderinger. På denne måten bruker bankene informasjon fra tidligere steg i prosessen til å utvikle handlingsplaner som forbereder institusjonen dersom alvorlige hendelser skulle inntreffe. Forebyggende tiltak, så vel som aktiviteter som gjør institusjonen bedre forberedt på potensielle risikoer, er også en del av beslutningsprosessen. Informasjonen bør bli brukt i forbindelse med forarbeid, responstid og iverksettingstiltak når eventuelle krisesituasjoner skulle oppstå.

Nordea viser eksempelvis et proaktivt syn på risiko med deres fokus på å forbedre kontinuitetsplanene. I lys av spesielt naturkatastrofer og stormen Sandy som herjet i USA i oktober 2012 ble det internt i banken satt et fokus på at kontinuitetsplanene ikke utelukkende skulle fokusere på kontinuitet i drift for *dager* i etterkant av hendelsen men også *måneder*. Dette indikerer et økende fokus på at norske banker faktisk innser at det er mulig at mer katastrofale hendelser kan ramme virksomheten. På den ene siden kan det, ved en mindre teknologisk risikohendelse som svikt i datasystemet, være riktig med et dagsperspektiv på kontinuitetsplanlegging. På den andre siden vil det med mer alvorlige hendelser ofte være nødvendig med kontinuitetsplaner som strekker seg måneder frem i tid. Alvorlige risikohendelser kan faktisk påvirke institusjonen i flere år frem i tid. Dette understrekes ved at de har endret designet på scenarioanalyser for å bedre inkludere effekten av halehendelser. Ikke bare styrker dette den operasjonelle risikostyringen som helhet og fører til en styrket forståelse av operasjonell risiko, men viser også en vilje fra bankens side å gå utover de regulatoriske kravene og styrke selskapets soliditet ovenfor aksjonærene. Planen fokuserer først på rammeverk og rapportering tilknyttet kriseledelse og driftskontinuitet. Dernest fokuseres det på hvordan ulike typer risiko kan påvirke virksomheten. Overnevnte indikerer ovenfor eksterne aktører at banken ønsker å være forberedt på et bredt spekter av risikohendelser, og at de har konkrete planer dersom risikohendelsene skulle inntreffe.

Det må likevel stilles spørsmålstegn om gjennomførbarheten til overnevnte tiltak. Det krever dedikerte ressurser og kunnskap hos ansatte for å få gjennomført endringen i kontinuitetsplanplanleggingen. Nordea har fokusert på trening og opplæring i forbindelse

med endret rammeverk, men utfordringen er at det er tidkrevende og stiller krav til at de ansatte og ledere for de ulike virksomhetsområdene tar seg tid til å gjennomføre det.

Informasjon fra hendelsesdatabasen er også verdifull i beslutningsprosessen. Det refereres da hovedsakelig til registrerte gjentakende tapshendelser med utgangspunkt i samme kilde. Dersom bankene ser at samme type risiko inntreffer med relativ høy frekvens, vil databasen fungere som et varselsystem og indikasjon på hvilke områder av risikostyringen som bør tildeles mer ressurser. Kanskje har bankene allerede innført tiltak for å forhindre denne typen risiko, men at tiltakene ikke har fungert som forventet eller godt nok. Dette kan gi indikasjoner på utilfredsstillende begrensningstiltak og gjør at banken må revurdere eksisterende tiltak og iverksette nye. Det er likevel viktig å være oppmerksom på at informasjonen fra hendelsesdatabasene ikke bør være det eneste informasjonsgrunnlaget for beslutningsprosessen. Som tidligere nevnt, representerer denne typen informasjon et prospektivt syn på risiko som danner et feil grunnlag for beslutninger tilknyttet begrensningstiltak. På grunn av et dynamisk og utviklende bankmiljø, vil det hele tiden være nye potensielle risikohendelser som trer frem. Eksempel på dette er den stadige teknologiske utviklingen som gir grunnlag for nye og ikke allerede loggførte operasjonelle tap. Ineffektivitet oppstår når ledelsen er for fokusert på historiske tapshendelser, som kanskje kan ha rystet institusjonen tidlige, og bruker for mye resurser på å begrense muligheten eller utfallet for samme type risiko.

Mye tyder på at styret, i både DNB, SpareBank 1 SR-Bank og Nordea, hovedsakelig har som oppgave å se over den operasjonelle risikostyringsprosessen, og er ikke direkte delaktig i vurderingen av tiltak for å begrense den operasjonelle risikoen. Styret holder oversikt gjennom rapporteringer fra de to forsvarslinjene som er internrevisjonens uavhengige risikovurdering, og rapporter for risikoavdelingen for operasjonell og compliance risiko. Inkludering av styret i utforming av tiltak mot de største konsernovergripende operasjonell risikoene, vil kunne være av stor betydning på grunn av de potensielle fatale konsekvensene halehendelser kan få for institusjonen. Operasjonell risiko burde også inngå i virksomhetens strategiplanlegging og det er dermed viktig at styret tar del i prosessen med utforming av tiltak for nøkkelrisikoer. Det viser engasjement fra styret og toppledelsen og gir bedre innsikt enn når styret og toppledelsen kun forholder seg til rapporter fra linjeledere og risikoavdelingen.

6.7 Balansert styring av «risk-return»

Inntrykket bankene gir av deres syn på operasjonell risiko, er som tidligere nevnt, at operasjonell risiko er negativt for institusjonen. Risikokategorien blir håndtert med utgangspunkt i at økt risiko ikke representerer økt avkastning for institusjonene. Tolkning av Basel-definisjonen og dermed definisjon gitt av Finanstilsynet vil kunne være et ledd i at operasjonell risiko kun ses på som negativt også fra bankenes side.

Dersom en kun ser negativt på operasjonell risiko, vil det kunne være vanskelig å se hvordan styring av risikokategorien kan integreres inn i et risk-return perspektiv, der avveining mellom avkastning og risiko står i sentrum. Avhengig av innfallsvinkel kan en likevel argumentere for at det finnes avkastning knyttet til å ta på seg operasjonell risiko. En potensiell operasjonell risiko er som tidligere nevnt muligheten for menneskelige feil i daglige operasjoner og drift. Et mulig risikoscenario i denne sammenheng er at en ansatt innvilger et lån til en kunde som egentlig ikke skulle blitt gitt ut i fra de rammeverk bankene har for låneinnvilgelse. I etterkant klarer ikke kunden å betale og lånet forfaller. Med utgangspunkt i et alternativt hendelsesforløp, kan det også tenkes at denne kunden faktisk betjener lånet sitt problemfritt, selv om lånet egentlig aldri skulle vært innvilget. Sistnevnte risikoscenario vil kunne karakteriseres som et positivt utfall av en operasjonell risikohendelse tilknyttet menneskelige feil og kredittinnvilgelse. Risikohendelsen har allerede inntruffet ved at lånet er blitt innvilget på feil grunnlag, men utfallet er positivt fordi banken faktisk får den avkastningen de ønsket på lånet.

Det finnes flere eksempler som kan utfordre bankenes nåværende tilnærming til operasjonell risiko. Utvikling og effektivisering av nye og avanserte IT-systemer kan på den ene siden øke avkastningen i ulike virksomhetsområder ved redusert menneskelig arbeidskraft i relaterte forretningsprosesser. I tillegg kan nettbaserte tjenesteløsninger som nettbank bedre kundens opplevelse av de tjenestene bankene leverer og dermed øke bruken av disse tjenestene. Redusert arbeidskraft og økt omsetning av banktjenester reflekteres positivt i bankenes resultater. Andre virkninger av komplekse og nye IT-systemer vil kunne være økt teknologirisiko gjennom eksponering for hacking og teknologisk sammenbrudd. Teknologien og sikkerheten bak de nye systemene er ikke nødvendigvis like godt kjent eller utviklet som ved de eksisterende IT-systemene. Eksempelet kan direkte relateres til at økt

operasjonell risiko kan føre med seg økt avkastning og at bankene dermed står ovenfor en risk-return beslutning.

Det eksisterer også risk-return beslutninger knyttet til valg og grad av begrensningstiltak. Etter at bankene har kvantifisert den operasjonelle risikoen, står institusjonene ovenfor en beslutningsprosess. Første ledd i denne beslutningsprosessen er at bankene må sette risikoappetitt og risikogrenser og bestemme om risikoeksponeringen er for lav, for høy eller akseptabel. I forhold til operasjonell risiko, er det vanskelig å karakterisere risikoen som for lav. Det med utgangpunkt i at operasjonell risiko ikke nødvendigvis, er et bevist valg i like stor grad som ved likviditets- og kredittrisiko. Etter at dette steget i beslutningsprosessen er gjennomført, må bankene ta stilling til eventuelle begrensningstiltak og valget mellom ulike tiltak som kan tjene samme formål. Kostnadene tilknyttet begrensningstiltak må veies opp mot konsekvensene for banken (kostnader) dersom risikoen skulle inntreffe. Grad av begrensning i tiltakene må også knyttets opp mot bankens strategi og ønskede risikoprofil. I enkelte tilfeller vil det ikke være optimalt å redusere den operasjonelle risikoeksponeringen. Dersom kostnaden ved å redusere risikoen er høyere enn fordelene ved redusert tap, vil tiltaket redusere ROI.

Et eksempel er compliance risiko. Det er dog ikke like synlig da en i utgangspunktet skal oppfylle alle krav og standarder som settes for finansinstitusjonene, men det er allikevel en avveining mellom i hvor stor grad en ønsker å oppnå/overgå disse standardene og hvor stor verdien av dette er. Banker som ønsker å være proaktive i forhold til kommende regulatorisk utvikling eller ønsker høyere interne krav en det som settes av myndighetene. Valg av denne typen gjøres med utgangspunkt i at tiltakene kan bidra positivt på resultatet og dermed øke selskapsverdien. Overnevnte er av hensyn til ROI i risikobegrensningstiltak, og er ikke nødvendigvis direkte relatert til økt avkastning på grunn av økt risiko. I noen sammenhenger vil det å øke kvaliteten på risikostyringssystemet ikke var gunstig for selskapet fordi kostnadene forbundet med kvalitetsnivået er høyere enn potensiell verdi av risikoreduksjon.

Et annet tilfelle er verdien av synergieffekter og brukspotensialet av tiltak iverksatt for å redusere operasjonell risiko. Investeringer i forståelsen av kundenes oppførsel, som i utgangspunktet blir brukt av banker til å oppdage svindel, kan utnyttes videre i forståelsen av kunden og tilrettelegging av kundeservice. På denne måten kan risikostyringsbeslutninger

medføre økt verdi for andre ikke-relaterte virksomhetsfunksjoner. Risikobegrensningstiltak vil ikke nødvendigvis kun iverksettes av hensyn til å redusere tap, men også økt kvalitet i institusjonens prosesser og økt effektivitet.

Investeringer i systemer som tidlig kan varsle om potensielle risikoer og i aktiviteter for å samle prospektiv risikoinformasjon, kan redusere risikoresponskostnader og er på samme måte en risk-return beslutning. Raskere responstid og forberedelser på fremtidige risikohendelser kan redusere kostnaden og tapet av en risikohendelse og hindre risikohendelsen i å få konsekvenser av samme grad som uten slike tiltak. Det er i tillegg viktig å skille mellom risikoer institusjonen ønsker å fjerne helt og risikoer institusjonen ønsker å begrense.

6.8 Korrekt synliggjøring av risiko

Korrekt synliggjøring av risiko relaterer seg i analysen til rapportering og kommunikasjon med eksterne aktører, og da med aksjonærer i fokus. En ofte oversett risiko er svak sammenheng mellom det som blir kommunisert til eksterne og det faktiske ERM-programmet i selskapet.

En utfordring innenfor kriteriet for korrekt synliggjøring av risiko er åpenhet, kommunikasjon og diskusjon rundt potensielle risikofaktorer. Med risikofaktorer, menes potensielle kilder til risiko. Momentet er gjennomgått under *fokus på nøkkelrisikoer*, men diskusjonen i dette avsnitte utdyper tidligere analyse. De norske bankene kan ta lærdom fra de amerikanske og andre større internasjonale banker på området. Ut i fra informasjonen i risiko- og kapitalstyringsrapportene til samtlige banker representert i oppgaven, er det synlig at gjennomsiktighet og åpenhet er begrenset. Hovedsakelig ser vi kun noen potensielle nøkkelrisikoer som utdypes i mer detalj, og utvelgelsen av disse risikoene kan det virke som om fortrinnsvis er compliance-drevet. Det skal det sies at alle banker som er notert på New York Stock Exchange er påkrevd av SEC å rapportere risikofaktorer i sine 10-K rapporter, men det vil likevel kunne være av verdi for norske bankener å gjøre dette på en frivillig basis. Informasjonen kan deles i enten årsrapporten eller pilar 3 rapporten. Gjennom åpenhet og kommunikasjon med aksjonærer og andre eksterne aktører, kan bankene vise forståelse og kunnskap rundt ulike operasjonelle risikofaktorer de selv står ovrnfor, og dermed å gjøre

eksterne aktører klar over hva de selv er oppmerksomme på. Dette vil også kunne resultere i større forståelse fra eksterne aktører dersom risikohendelsen faktisk skulle inntreffe.

Nordea går noe lengre enn de andre to bankene i å dele informasjon om styringen av risikoer som hvitvasking og ekstern kriminalitet. Banken presenterer også flere tiltak de har iverksatt for å begrense/forhindre disse risikoene og henviser til at de er meget forsiktige i forhold til nye og eksisterende kunder i banken. Det eksisterer en detaljert prosess tilknyttet kundeidentifisering, verifisering, kundeaksept, overvåking av kunderelasjoner, informasjonslagring og oppdaging og rapportering av mistenkelige aktiviteter og transaksjoner. De ansatte trenes også i å være oppmerksomme på denne typen risiko. Informasjonen er et ledd i det å være åpen rundt risikostyringen i institusjonen, og gir klare signaler om at Nordea har omfattende prosesser for å forhindre kriminalitet og ytrer et ønske om å fjerne slike trusler.

Det kan også anbefales å bedre synliggjøre ERM-programmene og det å inkludere utvalgte historier om erfaring opparbeidet gjennom adopsjonen av ERM-programmet og utviklingen av risikostyringssystemet. Slike historier kan styrke risikokulturen og vise lærdom opparbeidet gjennom ERM-prosessen, noe som styrker investorenes tillitt. Deling av historiske hendelser kan gi et godt bilde av den kontroll og styring institusjonen har.

6.9 Måle risikoens verdipåvirkning

Det er vanskelig å svare på om bankene måler risikoenes verdipåvirkning med det begrensede informasjonsgrunnlaget oppgaven bygger på. Verdipåvirkning kan måles ved hjelp av interne modeller, og vil i de fleste tilfeller ikke deles offentlig på grunn av innsideinformasjon som tas i bruk i slike verdsettelsesmodeller. I forhold til hvordan bankene måler den operasjonelle risikoen i institusjonen, vil det relativt enkelt kunne la seg overføre til en intern verdsettelsesmodell, da operasjonell risiko hovedsakelig måles i tap og dermed innvirkning på resultat. Problemet som kan oppstå er bankenes manglende evne til å måle fremtidig verdipåvirkning, ved at potensielle operasjonelle risikoer ikke nødvendigvis kun er en engangshendelse som påvirke selskapet der og da, men kan påvirke banken i lang tid fremover. Utfordringer ved å måle verdipåvirkning kan også være manglende evne til å kvantifisere enkelte operasjonelle risikoer. Operasjonell risiko med omdømmeskade som

utfall kan for eksempel være svært vanskelig for ledelsen og risikoavdelingen å måle. Denne typen utfall av operasjonell risiko vil ikke nødvendigvis bare synliggjøres i resultatet eller balansen for inneværende regnskapsår, men også i årene fremover. Bankene vil også kunne være mer utsatte for omdømmeskade på grunn av deres direkte forvaltning av kunders og bedrifters penger.

Ofte resulterer problemene i kvantifiseringen til at bankene måler risikoens påvirkning på selskapet ut i fra kvalitative mål. Kvalitative risikoparametere har redusert overførbarhet og egner seg ikke dersom bankene ønsker å måle verdipåvirkningen. Da vil ekspertvurderinger fra virksomhetsområdene, risikoavdelingen og ledelsen kunne være til hjelp. Selv om slike kalkuleringer ikke nødvendigvis baserer seg på håndfast data, vil de likevel representere stor verdi i fastsettelsen av total risikoeksponering.

Discounted cash flow-verdsettelse vil kunne løse bankenes utfordring med et for ensidig fokus på økonomisk kapital og regulatorisk kapital i sin kvantifisering av risiko. Med utgangpunkt i økonomisk kapital er det vanskelig å måle risikoens verdipåvirkning, men med utgangpunkt i verdsettelsesmodellene er det mulig å hente informasjon til beregning av økonomisk og regulatorisk kapital. Intern verdivurdering vil være en mer detaljert og tungvint prosess som krever utvidede ressursbruk av institusjonen, men er på den andre siden et instrument som er bedre egnet i forhold til å støtte opp under ledelsens og styrets beslutningstaking.

6.10 Hovedfokus på aksjonærene

Ettersom aksjonærenes innflytelse på styret har økt betraktelig de siste tiårene har også virksomhetens mål og strategi i større grad blitt linket opp mot aksjonærverdi. Med et økt fokus på aksjonærverdi er det også naturlig at resultatmål som EPS-vekst og economic value added (EVA) har kommet i fokus. Hovedbekymringene for en aksjonær kan sies å være om avkastningen på investeringene i selskapet vil være lavere enn forventet. På den andre siden kan avkastningen også være høyere enn forventet.

I en risikostyringssammenheng vil en kunne bidra til å øke virksomhetens verdi, gjennom en minimalisering av sannsynlighet og konsekvens av potensielle risikohendelser med hensyn på å maksimere selskapsverdi. Dette er en avveining mellom risiko og avkastning, og et

ønske om å skape verdier når mulighetene oppstår. Av den grunn vil ledelse ut i fra aksjonærinteresser sannsynligvis endre risikostyringstilnærmingen til selskaper i forhold til hva banken ville ved en ren compliance drevet tilnærming. Håndtering av risiko er viktig for aksjonærene.

På den ene siden vil ikke aksjonærene ønske at bankene begrenser seg for mye i forhold til risiko, fordi det i de fleste tilfeller er økt risiko i forbindelse med økt avkastning. En for defensiv tilnærming til risiko, vil kunne gå utover resultatet og føre med seg en ikke-optimal Risk-Return tilpasning. Dette ble også diskutert med tanke på operasjonell risiko, og hvorfor jeg mener det også er Risk-Return avveininger i denne risikokategorien. En for avers holdning til operasjonell risiko vil også kunne resultere i at banken bruker for mye penger på risikoreduserende tiltak. Både DNB og SpareBank 1 SR-Bank uttaler at de ønsker en lav operasjonell risikoprofil. Problemer oppstår dersom ønsket om en lav risikoprofil overskygger effektive Risk-Return avveininger og beslutningene om begrensningstiltak, og at dette påvirker aksjonærverdiene negativt gjennom lavere ROI.

På den andre siden ønsker også de fleste aksjonærer stabilitet. Rollen som en risikostyringsleder vil her gå utover det å fokusere på farene ved risiko og undersøke hvordan total risiko, både oppsiden og nedsiden, vil påvirke balansen og resultatregnskapet. Aksjonærene vil ikke ønske at bankene står ovenfor for høy operasjonell risikoeksponering, da det kan få meget uheldige utfall for selskapsverdien.

Det er gjennom analyse avdekket flere momenter som vil kunne være viktig for en aksjonær, potensiell investor eller analytiker å få innblikk i. Nøkkelrisiko, korrelasjonsbetraktninger og veloverveide risk-return beslutninger er bare noen av dem. Det er dog viktig å poengtere at det er fremdeles mye interessant og nyttig informasjon som kommer på bakgrunn av det som rapporteres, enten fokuset er ensrettet mot regulatoriske myndigheter eller ikke. Det vil selvfølgelig være naturlig for bankene å ha et sterkt fokus på krav fra myndighetene og finanstilsynet ettersom store deler av virksomheten i finansinstitusjonene er regulert. Når så mye ressurser går med på å irettesette seg etter krav og standarder til risikostyring generelt og i alle steg av ERM-prosessen, er det lett for at aksjonærenes interesser blir satt i andre rekke.

For bankene og myndighetene blir utfordringen å finne en integrert tilnærming til risikostyring der hovedfokuset bør være på selskapsverdi og aksjonærer, men at systemet og prosessen for risikostyring samtidig tilfredsstiller myndighetenes krav til kapitalreserver og forsvarlig risikostyring. Ettersom erfaring, kunnskap og handling med operasjonell risikostyring øker og bankenes ledelse får tillitt og gir støtte til ERM-programmet, vil operasjonell risikostyring kunne få økt verdi for virksomheten. Det at en nå ser antydninger til den operasjonelle risikostyringen hovedsakelig er compliance drevet, kan i etterkant utvikle seg til muligheter for institusjonene i å integrere ERM-informasjon som en del av resultatledelsen i institusjonene.

6.11 Generel

6.11.1 Regulatorisk kapital og interne kapitalberegninger

Det finnes store utfordringer tilknyttet beregning av minimumskapital og kvalitet i operasjonell risikostyring. Problemer oppstår også ved at ingen norske banker ennå er kvalifisert til å bruke den avanserte beregningsmetoden i sine interne kapitalberegninger. Som et resultat av dette, er det flere norske banker som bruker sjablongmetoden i interne kapitalberegninger også. Utfordringene oppstår fordi beregningsgrunnlaget for sjablongmetoden ikke har noen direkte tilknytning til den faktiske risikoen selskapet og de ulike virksomhetsområdene tar på seg. Sjablongmetodene bruker et treårig gjennomsnitt av historiske inntekter, men tidligere forklart er det ingen direkte grunn til å konkludere med at virksomhetsområdenes størrelse (inntekt) er sterkt positivt korrelert med områdenes respektive risikoeksponering.

Kapital burde allokeres til virksomhetsområdene på en måte som oppfordrer og insentiverer områdene til å alltid forbedre sin operasjonelle risikostyring. Ved nåværende kapitalberegninger vil ikke områdene belønnes for sine handlinger mot å redusere sannsynligheten eller alvorligheten av ulike risikoer. Risikobegrensningstiltak kan på denne måten redusere ROC dersom de ikke blir fanget opp i hverken regulatorisk kapitalberegninger eller interne kapitalberegninger. ROC reduseres fordi tiltakene kan være kostnadsfulle og vil ikke nødvendigvis generere høyere inntekter for virksomhetsområdet. Dette gjelder spesielt for operasjonell risiko da denne risikokategorien ikke har økt

avkastning med økt risikoeksponering i samme grad som finansiell risiko. For myndighetene, så vel som bankene, er det avgjørende å kunne integrere kapitalkravene og andre styringskrav inn som en del av bankenes operasjonelle risikostyring og insentivering av kontinuerlig forbedring av styringsprosessen. Det overordnede målet med vurderingen av operasjonell risiko og kapitalallokering burde involvere at virksomhetsområdene blir mer sensitive ovenfor operasjonell risikoledelse.

En må likevel påpeke at bankene også har flere egeninsentiver til forbedring av den operasjonelle risikostyringen. Redusert operasjonell risikoeksponering vil kunne reflekteres i et høyere resultat for virksomheten gjennom et redusert antall tapshendelser eller begrensede konsekvenser av tapshendelser.

7. Konklusjon

Operasjonell risiko er et fagfelt det fortsatt er knyttet mye usikkerhet til, på grunn av den begrensede erfaringen bankene har med styring av denne risikokategorien. Metodene og modellene for risikostyring og kontroll i norske banker, er ennå ikke på et stadium der fullstendig integrasjon med institusjonens strategi. Analysen i oppgaven peker på flere utfordringer bankene har i sin overordnede tilnærming til operasjonell risikostyring.

For det første eksisterer det utfordringer i bankenes kommunikasjon med aksjonærene og grad av innsikt banken ønsker å gi det offentlige. Ingen av bankene det er hentet eksempler fra i oppgaven gir et oversiktlig og strukturert bilde av den nåværende operasjonelle risikosituasjonen i institusjonen. Det presenteres kun enkelte risikoer i risiko- og kapitalstyringsrapportene og innfallsvinkelen ser hovedsakelig ut til å være compliance-drevet. Målet for bankene burde være å finne en middelvei, der tilgjengelig operasjonell risikoinformasjon gir godt bilde av bankens ERM-program og risikobilde, men overholder begrensninger i forhold til deling av sensitiv og konkurransehemmende informasjon. Informasjon om den operasjonelle risikostyringsprosessen er på den andre siden inkludert i mer detalj i både Nordeas, SpareBank 1 SR-Banks og DNBs rapporter. Rammeverket for prosessen gir aksjonærene et godt bilde av hvilke retningslinjer styret har satt for intern styring og kontroll.

Bankene ser også ut til å stå overfor en utfordring når det kommer til å inkludere korrelasjonsjusteringer i sine kalkuleringer av operasjonell risikoeksponering og aggregering av total risikoeksponering. Nåværende metoder for å fange opp korrelasjon mellom ulike operasjonelle risikoer og risikokategorier gjøres ved å etterjustere for diversifiseringseffekter. DNB justerer på selskapsnivå og SpareBank 1 SR-Bank på operasjonelt risikonivå. Utfordringen ved å korrelasjonsjustere på operasjonelt risikonivå er at banken da ikke får inkludert potensiell korrelasjon mellom risikokategorier. På selskapsnivå er utfordringen å fange opp korrelasjon mellom ulike operasjonelle risikoer. Korrelasjonen kan være tilfeldig, men korrelasjonen kan også være grunnet statistisk samvariasjon eller underliggende kausale effekter. For fremtiden vil det være hensiktsmessig å inkludere slike effekter i modelleringen av operasjonell risiko.

Det er også viktig at bankene inkluderer all den informasjonen som er opparbeidet gjennom identifisering og kvantifisering av operasjonell risiko i den videre beslutningsprosessen. Utgangspunktet i de tre norske bankene, er at ledere for de ulike virksomhetsområdene har eierskapet til den risikoen som oppstår i sine respektive områder. Resultatet av dette kan være at iverksetting og vurdering av begrensningstiltak gjøres av områdeledere. Styret og ledelsen har imidlertid det overordnede ansvaret for å sørge for at risikotiltak blir vurdert og iverksatt, og retningslinjer i risikostyringsprosessen blir fulgt. Derfor bør styret og ledelsen også inkluderes utforming av risikotiltak og beslutningsprosessen angående bankens operasjonelle nøkkelrisikoer. Beslutningsmyndighet kan heller delegeres til områdeleder ved mindre alvorlige risikoer.

Analysen peker på flere utfordringer som kan være objekter for mer detaljert forskning og som bankene bør undersøke nærmere. For videre forskning kan det være interessent å gå mer i dybden på problemene og finne konkrete og mer tekniske løsninger.

8. Veien videre

En forskningsgruppe ved Universitetet i Stavanger har gjennom de siste årene arbeidet for å utvikle en modell for kvantitativ analyse av operasjonell risiko. Forskningsprosjektet ønsker gjennom samarbeid med norske banker å utvikle operasjonelle risikomodeller som har til hensikt å oppfylle kravet for den avanserte metoden. Forskningen er av spesiell interesse da den avanserte metoden kan muliggjøre en sammenstilling av myndighetenes og bankenes interesser. Dersom de norske bankene får tillatelse av Finanstilsynet til å ta i bruk den avanserte metoden i kalkuleringer av regulatorisk kapital, vil dette også kunne gi økte insentiver for bankene til kvalitet i risikostyringen og kontrollen. Modellen tillater bankene å beregne minimumskapital med utgangspunkt i egne interne vurderinger som tar hensyn til faktiske tapshendelser og risikoeksponering i virksomheten, som igjen er et resultat av kvaliteten i bankenes styring og kontroll av operasjonell risiko. På denne måten har bankene økte insentiver til å allokere ressurser til utvikling og kontinuerlig forbedring av operasjonell risikostyring. Sparebank 1 SR-Bank og DNB er to av bankene som har vært i samarbeid med Universitetet i Stavanger. Nordea har også planer om å ta i bruk den avanserte metoden.

Ingen av bankene har enda implementeringen den avanserte metoden som kreve økt historisk datagrunnlag, videre utvikling og godkjennings fra Finanstilsynet basert på kvaliteten i den operasjonell risikostyringsprosessen. Det blir spennende å se på utviklingen innenfor bankenes operasjonelle risikostyring i fremtiden og videre forskning i etter overgangen til ny modell. Innføring av den avanserte metoden kan ha potensiale til å fremme videre utvikling i operasjonell risikostyring i stor grad.

9. Litteraturliste

Andersen L.B, N. M. (2010). The influence of unhealthy organisational culture on operational risk exposure in financial trading. *European Safety and Reliability Conference.* European Safety and Reliability Conference.

Basel Committee on Banking Supervision. (2001). *Sound Practices for the Management and Supervision of Operational Risk.* Bank for International Settlements.

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

Bessis, J. (2011). *Risk Management in Banking.* Chichester: J. Wiley & Sons.

Bowker, G., & Star, S. (2000). *Sorting Things Out: Classification and its Consequences.* Cambridge, MA: MIT Press.

Brian W. Nocco, N. I. (2006). Enterprise Risk Management: Theory and Practice. *Journal of Applied Corporate Finance*.

COSO. (1991). *Internal Control: Integrated Framework.* Committee of Sponsoring Organizations of the Treadway Commission.

COSO. (2005). *Committee of Sponsoring Organizations of the Treadway Commission.* Hentet 2014 fra http://www.coso.org: http://www.coso.org/publications/erm/coso_erm_executivesummary.pdf

Ernst & Young. (2001). Basel—A Better Use of Control. *Operational Risk Management Promotional Brochure.*

Finansdepartementet. (2006). Kapitalkravsforskriften. *Forskrift om kapitalkrav for forretningsbanker, sparebanker, finansieringsforetak, holdingselskaper i finanskonsern, verdipapirforetak og forvaltningsselskaper for verdipapirfond mv. (kapitalkravsforskriften).* Norway: Finansdepartementet.

Finansdepartementet. (2009, April 15). *hvitvaskingsloven.* Hentet 2014 fra Lovdata: http://lovdata.no/dokument/NL/lov/2009-03-06-11

Finansdepartementet. (2013). *Finansdepartementet*. Hentet 2014 fra Regjeringen: http://www.regjeringen.no/nb/dep/fin/dok/regpubl/stmeld/2012-2013/meld-st-12-20122013/2/3.html?id=714067

Finansdepertementet. (2013, Mars 22). *Regjeringen*. Hentet fra http://www.regjeringen.no/nb/dokumentarkiv/stoltenberg-ii/fin/Nyheter-og-pressemeldinger/pressemeldinger/2013/nye-lovregler-om-kapitalkrav-for-banker.html?id=720596

Finanstilsynet. (2006). *Retningslinjer for tilsynsprosessen.* Finanstilsynet.

Finanstilsynet. (2013, May 30). *Finanstilsynet*. Hentet fra http://www.finanstilsynet.no/Global/Venstremeny/Foredrag_vedlegg/2013/Finansieringsselskapene_2013-end.pdf

Hans Helbekkmo, A. K. (2014). *Enterprise Risk Management - Shaping the risk revolution.* McKinsey & Company.

Harald Karlsen, F. Ø. (2002). *norges-bank.* Hentet fra norges-bank: http://www.norges-bank.no/Upload/import/publikasjoner/penger_og_kreditt/2001-03/regler.pdf

Hugh, M. S. (2006). *Sustained SOX: A Practical Guide for Implementing a Sustainable Sarbanes Oxley Process.* AuthorHouse.

Jørgensen, A. M. (2014, April 17). Bank of the year: Nordea. (O. R. staff, Intervjuer)

Kirkpatrick, G. (2009). Corporate Governance Lessons. *OECD Journal: Financial Market Trends*.

Larsen, B. T. (2010, December). Operasjonell risikostyring i DnB NOR. (Internrevisoren, Intervjuer)

McKinsey & Company . (2013). *Getting to ERM: A roadmap for banks and other financial institutions*. McKinsey & Company .

NIRF. (2007). Styring av Operasjonell Risiko i finansnæringen. Stavanger: Stavanger University.

Nordea. (2012, October 4). *Risk Management in Nordea.* (S. Carlsen, Artist) SAS Institute.

Palm, F. S. (2013, December 20). *American Banker*. Hentet 2014 fra American Banker : http://www.americanbanker.com/bankthink/what-banks-learned-about-risk-management-1064464-1.html

Pjotrs Dorogovs, I. S. (2013). New tendencies of management and control of operational risk in financial institutions. *International Strategic Management Conference*. Elsevier Ltd.

Power, M. (2006, August 20). The invention of operational risk. *Review of International Political Economy*.

Rochette, M. (2009). From risk management to ERM . *Journal of Risk Management in Financial Institutions* , 16.

Rose, G. (2013, November 28). *Portfolio & Money Management*. Hentet fra Morningstar: http://www.morningstar.co.uk/uk/news/114281/risk-management-the-key-to-investing-success.aspx

SEB. (2011, February 11). Root causes of decline. SEB.

Segal, S. (2011). *Corporate Value of Enterprise Risk Management : The Next Step in Business Management.* Hoboken, NJ, USA: Wiley.

Sisk, M. (2010). *Mastering a Mountain of RISK.* Bank Technology News.

Sturm, P. (2013). Operational and reputational risk in the European banking industry: The market reaction to operational risk events. *Journal of Economic Behavior & Organization*.

Tawei Wang, C. H. (2013). Board composition and operational risk events of financial institutions. *Journal of Banking & Finance*.

The Conference Board. (2006). The Role of U.S. Corporate Boards in Enterprise Risk Management.

Litteraturliste analyse:

DNB. (2013). *DNB Bank ASA.* Hentet fra https://www.dnb.no/portalfront/nedlast/no/om-oss/resultater/2013/pilar3-dnb-2013-norsk.pdf

Nordea. (2013). *Nordea Bank Norge Group*. Hentet fra http://www.nordea.com/sitemod/upload/Root/www.nordea.com%20-%20uk/Investorrelations/reports/risk/norway/Nordea_Norge_Capital_

SpareBank 1 SR-Bank (2013) *SpareBank 1 SR-Bank konsern*. Hentet fra https://www.sparebank1.no/portal/3229/3_privat?_nfpb=true&_nfls=false&_pageLabel=page_privat_innhold&aId=1268425648785

10. Appendiks

Tabell 1:

Risikokategori	Risiko underkategori	Definisjon
Finansiell Risiko		**En risikokategori som relaterer seg til endringer i det eksterne markedet, priser, renter og tilbud og etterspørsel etter likviditet. Se markedsrisiko, likviditetsrisiko og kredittrisiko.**
Finansiell	Markedet	Uventede endringer i det eksterne markedet (eks aksjemarkedet), priser (eks råvarepriser), renter (eks lånerenten), som relaterer seg til (a*)* generelle bevegelser i markedet (selv om grunnen ofte er knyttet til samfunnsøkonomisk risiko eller *(b)* en spesiell eiendel på firmaets balanseregnskap). Noen eksempler er valutarisiko, lånerenterisiko og risiko knyttet til aksjemarkedet.
Finansiell	Kredittrisiko	Uventede endringer i kredittmarkedet (tilgjengelighet), priser (kredit spread --> større avstand mellom "risikofri rente" og rente på usikre verdipapirer), eller kredittverdighet fra kredittakers side relatert til (a*)* svingninger i det generelle kredittmarkedet (selv om dette igjen som oftest relateres til samfunnsøkonomisk risiko --> strategisk risiko) eller *(b)*en spesifikk utsteder av «fixed-income» verdipapirer i firmaets balanseregnskap eller (c) hos en motpart hvor selskapet har utvidet kreditt.
Finansiell	Likviditet	Uventede endringer i likviditets- etterspørsel eller tilbud relatert til tre forskjellige nivåer i.f.t. innvirkning *(a)* ikke-planlagt salg av eiendeler, (b) manglende evne til å møte kontraktfestede krav, (c) manglende evne til å betale ned lån. En endring i likviditets tilbud innebærer en manglende evne til å selge eiendeler som planlagt i markedet, i relasjon til pris, volum eller tidspunkt. En endring i likviditetsetterspørselen innebærer en uventet endring i etterspørselen etter likviditet for opsjonsholdere, som eks låneobligasjon-holdere som utøver tidlig salgsopsjoner eller "løp-til-banken" situasjoner der kontoholdere plutselig bestemmer seg for å ta ut midler fra kontoene sine (av betydning).
Strategisk		**En risikokategori som relaterer seg til uventede endringer i nøkkelelementer i strategiformuleringen og/eller utøvelsen av selskapets strategi (ofte forskjeller mellom tenkt strategi og faktisk utøvd strategi). Denne risikokategorien er veldig avhengig av selskapet det**

		gjelder og må tilpasses hvert enkelt selskap.
Strategisk	Strategi	Strategiens levedyktighet; valg av produkter eller tjenester selskapet skal produsere/tilby, distribusjonskanaler eller at faktisk verdi ikke matcher forventet verdi. Dette varierer stort mellom selskaper.
Strategisk	Utøvelse	Strategien er ikke implementert som forventet. Varierer igjen stort mellom selskaper.
Strategisk	Eierstyring	Eierstyringen fungerer ikke som forventet.
Strategisk	Strategiske allianser	Uventede endringer i strategiske allianser som moderselskap eller joint venture partnere.
Strategisk	Konkurrenter	Uventede endringer i konkurransesituasjonen i bransjen slik som nye inntrengere, aggressive handlinger av konkurrenter rettet mot selskapet, priskrig etc.
Strategisk	Leverandør	Uventede endinger i leverandørsituasjonen som leverandørens kapasitet, leverandør mister muligheten til å levere eller endringer i kostnadene knyttet til levering / kostnader knyttet til varer eller tjenester benyttet i produksjonen. Dette inkluderer også uventede endringer i rating byråers ranking eller regulatorisk lisensiering.
Strategisk	Samfunnsøkonomisk	Uventede endringer i økonomien. Dette er ofte kilden til risiko som trigger flere og samtidige uventede endringer i andre elementer, slik som konsumenters disponible inntekt (rammer etterspørselen etter bedriftens varer og/eller tjenester), jobbmarkedet (rammer selskapets faste kostnader), inflasjon/deflasjon (rammer selskapets variable kostnader), elementer relatert til markedsrisiko og kreditt risiko.
Strategisk	Eksterne relasjoner	Uventede endringer i selskapets forhold til eksterne stakeholders med offentlig påvirkningskraft, slik som media, talspersoner for konsumentene, finans analytikere, rating byråer, regulerings ansvarlige og politikere.
Strategisk	Lovgivning / regulering	Uventede endringer i lover og reguleringer.
Strategisk	Internasjonal	Uventede endringer i næringslivet med tanke på utenlandsk næringsvirksomhet og land selskapet opererer i. Det gjelder elementer som regjeringens stabilitet, holdninger mot utenlandske selskaper og tariffer.

Operasjonell		**En risikokategori som relaterer seg til uventede endringer i elementer som er knyttet til den daglige driften av selskapet. Eksempler er risiko knyttet til humankapital, teknologi, prosesser og katastrofer/ulykker.**
Operasjonell	Humankapital	Humankapital (ansatte) yter ikke som forventet, slik som uventede endringer i ansettelse og utvikling av talenter, ytelse/resultat, produktivitet og oppførsel/opptreden.
Operasjonell	Teknologi	Teknologien gir ikke den ytelsen eller det resultatet som er forventet. Noen eksempler inkluderer datasikkerhet, konfidensiell og privat data, dataintegritet, kapasitet og pålitelighet.
Operasjonell	Rettssaker og søksmål	Uventede søksmål eller dommer mot selskapet
Operasjonell	Compliance	Grad av standard matcher ikke forventningene (mht kvalitet, sikkerhet, utslipp etc.). Dette gjelder også den finansielle rapporteringen.
Operasjonell	Ekstern svindel	Uventede endringer i grad eller antall svindler fra eksterne aktører rettet mot selskapet.
Operasjonell	Katastrofer /ulykker	Uventede natur- eller menneskeskapte katastrofer slik som værrelaterte (orkan, oversvømmelse, tornado, jordskjelv), helserelaterte (pandemier), ulykker (brann), generelle destruktive handlinger (krig, terror og opptøyer) og spesifikke destruktive handlinger rettet direkte mot selskapet (tukling med produktet eller tjenesten som leveres, angrep på ansatte og sabotasje). Dette inkluderer også uventede menneskeskapte katastrofer forårsaket av ansatte eller agenter som miljøskader etc.
Operasjonell	Prosesser	Selskapets prosesser fungerer ikke som forventet.

Tabell 2 (Finansdepartementet, 2006)**:**

Forretningsområder	***Tjenestekategorier***	***Prosent***
Foretaksfinansiering	Garantistillelse for fulltegning av emisjoner eller andre offentlige tilbud som nevnt i verdipapirhandelloven kapittel 7 eller plassering av slike tilbud. Tjenester i forbindelse med garantistillelse Investeringsrådgivning Rådgivning og tjenester ved fusjoner og oppkjøp, emisjoner, børsintroduksjoner, kapitalstruktur, strategi mv.	18 prosent
Egenhandel og formidling	Handel for egen regning Pengemegling Formidling av ordre på vegne av investor og analyser i forbindelse med finansielle instrumenter mv. samt utførelse av slike ordrer. Plassering av finansielle instrumenter uten garantistillelse.	18 prosent
Megling for massemarkedskunder (Aktiviteter mot enkeltpersoner eller mindre foretak som definert i del II)	Mottak og formidling av ordre på vegne av investor i forbindelse med finansielle instrumenter mv. samt utførelse av slike ordrer. Plassering av finansielle instrumenter uten garantistillelse	12 prosent
Banktjenester for massemarkedskunder (Aktiviteter mot enkeltpersoner eller mindre foretak som definert i del II)	Inn- og utlån, garantistillelse, finansiell leasing, rådgivning, betalingstjenester, formidling og salg av spareprodukter samt øvrig finansiering til massemarkedet.	12 prosent
Banktjenester for bedriftskunder	Inn- og utlån, garantistillelse, finansiell leasing, eksportfinansiering, prosjektfinansiering, faktoring og øvrig finansiering til bedriftsmarked.	15 prosent
Betaling og oppgjørstjenester	Betalingsformidling Oppgjørsvirksomhet	18 prosent
Tilknyttede tjenester	Depotvirksomhet, verdipapirservice (for eksempel kontoførertjenester, administrasjon av verdipapirer og tilknyttede tjenester), administrasjon av verdipapirlån m.m.	15 prosent
Kapitalforvaltning	Aktiv forvaltning Verdipapirfondsforvaltning Øvrig kapitalforvaltning	12 prosent