NORGES HANDELSHØYSKOLE

Bergen, Vår 2021

Integrering av operasjonell risiko i virksomhetsstyring

En flercasestudie av tolv virksomheter

Vilde Isabelle Sævdal og Benedikte Amalie Stokke

Veileder: Øyvind Thomassen

Masteroppgave, Økonomi og Administrasjon, Økonomisk Styring

NORGES HANDELSHØYSKOLE

Sammendrag

Økt globalisering, digitalisering og nyere samarbeidsformer i et komplekst og stadig skiftende miljø medfører både utvidelse og endring av risikoer som virksomheter står overfor. En sentral risiko i alle virksomheter, uavhengig bransje, er operasjonell risiko. Formålet med oppgaven er å identifisere styringsmekanismer som virksomheter benytter for operasjonell risikostyring. Oppgaven tar utgangspunkt i det teoretiske rammeverket, Simons (1995) *Levers of Control,* og tidligere forskningslitteratur på risikostyring. Problemstillingen belyses og besvares med utgangspunkt i en flercasestudie med tolv virksomheter innenfor ulike bransjer som vi har kategorisert innunder: (1) Finansforetak, (2) Fiskeri og infrastruktur og (3) Konsulentselskap.

En avgjørende styringsmekanisme omhandler organisering og ansvarsforhold. Det er viktig at styret og toppledelsen har fullstendig forståelse og kompetanse for hvordan de skal drive med risikostyring i virksomheten. I tillegg er det viktig å tydeliggjøre sentrale roller som er involvert i risikostyring, og at det blir utarbeidet klare mandater og stillingsbeskrivelser som blir tilpasset virksomheten. Det vil også være hensiktsmessig å etablere utvalg og komité for å opprettholde kontroll og styrke risikostyring i virksomheten. En annen avgjørende styringsmekanisme er at internkontroll blir gjennomført og godt dokumentert. Videre er avgjørende styringsmekanismer å utarbeide risikopolicyer og risikorammeverk, samt definere virksomhetens risikoappetitt.

Andre avgjørende styringsmekanismer for operasjonell risikostyring er å benytte risikomatrise, risikolister i rapportering, registrere hendelsesdata og predefinere tiltak med tydelige ansvarsforhold. Det vil også være hensiktsmessig at virksomheter kvantifiserer operasjonell risiko ved metodene KPI, KRI og budsjett. Finansforetakene skal i tillegg beregne kapitalbehov for operasjonell risiko. Virksomheter bør imidlertid veie opp kvantitative indikatorer mot kvalitative, og ledelsens kvalitative vurderinger bør veie like mye som de kvantitative ved operasjonell risiko. Videre viser studiens funn at det er manglende kompetanse på operasjonell risikostyring i virksomheter. For å bygge opp kompetanse og skape en felles forståelse av risikobildet i virksomheten er det hensiktsmessig å benytte risikoverktøy, hendelsesdatabase, overvåke og implementere et godt internt kommunikasjonssystem. I tillegg bør virksomheten legge opp til kontinuerlig diskusjon og involvering i alle ledd for å bygge kompetanse og bevisstgjøring. Det vil bidra til å skape felles

risikoholdninger og en god risikokultur i virksomheten. En god risikokultur er nøkkelen for å drive med god operasjonell risikostyring.

Vår oppgave er et viktig bidrag til den akademiske litteraturen med empiriske beskrivelser av hvordan tolv ulike virksomheter arbeider med risikostyring, samt vår visuelle fremstilling som inkluderer avgjørende styringsmekanismer for god operasjonell risikostyring. Studien gir dermed innsikt for praktikere for hvordan operasjonell risikostyring integreres i virksomhetsstyringen.

Forord

Denne masteroppgaven er skrevet som en del av masterstudiet i Økonomi og Administrasjon ved Norges Handelshøyskole (NHH). Vi ønsker å takke virksomhetene som har tatt oss godt imot og latt oss få et innblikk i deres virksomhet. Videre ønsker vi å takke våre respondenter som har bidratt med kompetanse og som gledelig har besvart alle spørsmål vi har hatt, både i intervjuer og i etterkant. Vi er utrolig takknemlig og ønsker å takke for at vi fikk lov til å bruke deres tid!

Til slutt ønsker vi å rette en stor takk til vår veileder, Øyvind Thomassen for gode diskusjoner og konstruktive tilbakemeldinger underveis i prosessen. Dine gode råd og støtte gjennom hele semesteret har vært uvurderlig for gjennomføring av vår oppgave. Videre vil vi uttrykke vår takknemlighet til venner og familie som har bidratt med innspill på oppgaven.

Bergen, 01.06.2021

Vilde Isabelle Sævdal

Benedikte Amalie Stokke

Innholdsfortegnelse

Figurliste:

Tabelliste:

1.0 Introduksjon

1.1 Innledning og bakgrunn

Økt globalisering, kriser, katastrofer, skandaler, globale pandemier og strengere krav fra myndigheter, har vist seg å skape store utfordringer og endringer av risikoer som virksomheter står overfor (Noreng, 2002; Hagness, Vatne & Nordheim, 2014; IIA, 2021). Det har medført at virksomheter de siste tiårene har viet mye oppmerksomhet til å styre risiko (Kaarbøe et al., 2013) Risikostyring har på den måten vist seg å være en viktig del av virksomhetsstyring. Grunnen er at risikostyring blir betegnet som et virkemiddel for å styre og kontrollere usikkerhet knyttet til virksomhetens evne til å skape, beskytte og realisere verdier, og for at virksomheten skal nå sine mål (IIA, 2021).

I 2004 omdøpte The Committee of Sponsoring Organization for the Treadway Commission (COSO) risikostyring til helhetlig risikostyring. Dermed ble risikostyring løftet opp på et strategisk nivå i virksomheter ved å fokusere på virksomheters strategiske målsettinger og porteføljen av risikoer på tvers av hele virksomheten (Meidell, 2017). Helhetlig risikostyring har på den måten vokst frem som en helhetlig løsning på hvordan virksomheter kan styre risiko (Kaarbøe et al., 2013). Ved hjelp av helhetlig risikostyring kan ledere identifisere, prioritere og styre risikoer på tvers av virksomhet eller divisjon. Dette kan medvirke positivt på virksomhetens verdiskapning og være med å bidra til å gi virksomheten en ny konkurransefordel (Noreng, 2002). Innføringen av helhetlig risikostyring har derfor blitt sett på som en av de største organisatoriske endringene siden 2000-tallet. Dette har medført fremvekst av nye roller, etablering av nye funksjoner og utvikling av nye verktøy for å styre risiko. Det har i tillegg blitt utarbeidet nye prinsipper, rutiner og prosesser for risikostyring (Power, 2007; Hayne & Free 2014; Meidell, 2017).

God praksis er å ha et helhetlig perspektiv på risikostyring, som integreres på tvers av virksomheten og harmoniseres med andre styringsaktiviteter (IIA, 2021). Med utgangspunkt i IIA (2021) og utviklingen av risikostyring de siste tiårene vil det være interessant å få et dypere innblikk i hvordan virksomheter driver med risikostyring. Virksomheter har i tillegg ulik praksis for risikostyring, som avhenger av virksomheters kompleksitet og størrelse. Dermed er det interessant å gjennomføre en flercasestudie av tolv ulike virksomheter på tvers av

bransjer, for å forklare hvordan virksomheter arbeider med risikostyring. Vi har valgt å avgrense forskningsprosjektet til operasjonell risikostyring. Årsaken til dette er at enhver virksomhet, enten den operer i privat eller offentlig sektor, må forholde seg til problemstillinger tilknyttet operasjonell risiko. Ifølge Finanstilsynet (2016) er operasjonell risiko et vidt fagfelt som griper inn på overordnet styring og kontroll og andre risikoområder. Videre viser Jansrud (2017b) til at ulike risikoklasser alle har en sammenheng med operasjonell risiko, og dermed er det avgjørende at virksomheter klarer å styre operasjonell risiko som kan oppstå. På bakgrunn av dette finner vi det interessant å rette vårt fokus på operasjonell risikostyring.

1.2 Problemstilling og forskningsspørsmål

Med bakgrunn i vår ovennevnte innledning har vi kommet frem til følgende problemstilling:

Hvordan integrere operasjonell risikostyring i virksomhetsstyringen?

For å besvare vår problemstilling har vi utarbeidet tre forskningsspørsmål:

1. *Hvilke operasjonelle risikoer oppstår i virksomheter?*
2. *Hvilke styringsmekanismer benytter virksomheter for operasjonell risikostyring?*
3. *Hvilke styringsmekanismer er avgjørende for god operasjonell risikostyring?*

1.3 Oppgavens tilnærming

For å besvare våre forskningsspørsmål vil det gjennomføres en flercasestudie med tolv virksomheter. Virksomhetene skiller seg i størrelse, og tilhører både privat og offentlig sektor. Det har blitt gjennomført kvalitative dybdeintervjuer med én respondent innenfor hver virksomhet, som har en sentral rolle innenfor risiko- og virksomhetsstyring.

Basert på tidligere forskningslitteratur har vi valgt å integrere risikostyring i et rammeverk for virksomhetsstyring, Simons (1995b) *Levers of Control*. Innenfor rammeverket er det fire styringssystemer og innenfor hvert styringssystem er det ulike styringsmekanismer for risikostyring. Med denne studien ønsker vi å undersøke styringsmekanismer som

virksomheter benytter for operasjonell risikostyring. Vi søker også å komme med avklaringer og avgrensninger om operasjonell risikostyring i virksomheter.

1.4 Oppgavens oppbygging

Vi har valgt å strukturere oppgaven i seks hovedkapitler. I første kapittel har vi introdusert bakgrunnen for forskningsprosjektet. I andre kapittel vil oppgavens teoretiske grunnlag bli presentert. Kapittelet inkluderer definisjoner og standarder, samt det teoretiske rammeverket Simons (1995b) *Levers of Control*. I tredje kapittel vil vi redegjøre for metodiske valg, hvor også virksomheter og respondenter vil bli presentert. I fjerde kapittel vil empiriske funn fremlegges fra hver bransje. Empiriske funn legger grunnlag for kapittel fem hvor vi vil sammenligne funn og diskutere dette opp mot eksisterende litteratur. Analysekapittelet er bygget opp etter de tre forskningsspørsmålene. Avslutningsvis vil vi i konklusjonen i kapittel seks besvare vår problemstilling og komme med forslag til videre forskning. Til slutt har vi litteraturliste, i tillegg er samtykkeskjema og intervjuguide vedlagt.

2.0 Teori og rammeverk for oppgaven

I dette kapittelet presenteres teori og rammeverk som vil danne grunnlag for å besvare vår problemstilling og forskningsspørsmål. Innledningsvis redegjør vi for virksomhetsstyring og presenterer rammeverket for virksomhetsstyring som er blitt utviklet av Robert Simons (1995b), kalt *Levers of Control.* Videre inneholder kapittelet eksisterende litteratur på fagområdene risiko og risikostyring, hvor vi deretter integrerer risikostyring i Simons (1995b) rammeverk for virksomhetsstyring. Med utgangspunkt i rammeverket vil det presenteres ulike styringsmekanismer for risiko innenfor hvert styringssystem i rammeverket, som vil bli benyttet som en strukturert tilnærming videre i utredningen. Det vil imidlertid kun redegjøres for teori som omfattes som nyttig og anvendbare for analysedelen.

2.1 Virksomhetsstyring

Malmi & Brown (2008, s. 290) definerer virksomhetsstyring (eng. Management Control) som: "Systemer, regler, praksiser, verdier og andre aktiviteter ledelsen benytter for å styre ansattes beslutninger og adferd, og disse er i overensstemmelse med virksomheters mål og strategier." Det har vært flere litteraturbidrag innenfor virksomhetsstyringsfaget (Malmi & Brown, 2008; Langfield-Smith, 1997; Simons, 1995b). De siste årene har det vært større fokus på sammenhengen mellom virksomhetsstyringssystemer og strategi. Det var imidlertid ikke før på 1980-tallet at strategi eksplisitt ble inkludert som en variabel i forskning på styringssystemer (Langfield-Smith, 1997). Langfield-Smith (1997) og Simons (1995b) trekker frem at virksomhetsstyringssystemer er et viktig virkemiddel for å gjennomføre vellykket implementering av strategi. Robert Simons (1995b) definerer virksomhetsstyringssystemer (eng. management control system) på følgende måte: "Management control systems are the formal, information-based routines and produres managers use to maintain or alter patterns in organizational activities". Simons (1995b) utviklet et rammeverk for virksomhetsstyring, kalt *Levers of Control,* som vil bli presentert i delkapittel 2.1.1.

2.1.1 Rammeverk for virksomhetsstyring

Simons (1995b) utviklet et rammeverk for virksomhetsstyring, *Levers of Control*. Rammeverket beskriver fire ulike styringssystemer: (1) grensesystemet, (2) diagnostisk

systemsystem, (3) interaktivt styringssystem og (4) trossystem. Kjernen i rammeverket er virksomhetens strategi og for å kunne implementere strategien på en suksessfull måte, er det nødvendig å forstå og ta hensyn til de fire styringssystemene. Simons (1995a) mener at ved å kombinere de fire ulike styringssystemene, vil ledere være i stand til å oppfordre til innovasjon og ta initiativ til gode beslutninger. I tillegg vil tydelige grenser og forventninger skape ramme og kontroll for atferden til de ansatte i virksomheten (Simons, 1995a). De fire styringssystemene er presentert i Figur 1, og har til hensikt å utfylle hverandre. I det følgende vil en beskrivelse av de fire styringssystemene bli presentert.

Figur 1: Simons (1995b) Levers of Control

Grensesystem

Grensesystemet avgrenser det akseptable aktivitetsområde for ansatte, og er basert på et lederprinsipp som kalles "the power of negative thinking" (Simons, 1995a). Ifølge Simons (1995a) uttrykkes grensesystemet ofte gjennom negative termer eller minimumsstandarder. Formålet med grensesystemet er at det settes klare begrensninger til hvilke aktiviteter de ansatte kan utøve, og hvilke de ikke kan utøve. Simons (1995b) hevder at hvis ledere forteller de ansatte hva de skal gjøre, vil det ikke bidra til kreative og innovative prosesser. Setter ledere derimot grenser for hva de ansatte ikke skal gjøre, vil det skape rom for kreativitet og innovasjon. Dette er mulig så lenge de ansatte holder seg innenfor de gitte rammene. Følgelig vil det bidra til å avgrense at ansatte ikke gjør noe som kan virke fristende, og som ikke samsvarer med strategi (Simons, 1995b).

Simons (1995b) deler grensesystemet inn i to: (1) *forretningsgrenser* og (2) *strategiske grenser*. Forretningsgrenser handler om samfunnets lover, virksomhetens trossystemer og bransjerelaterte regler. Hver av disse inneholder aktiviteter som vil sette en virksomhets velferd i fare. Simons (1995b) mener derfor at det er nødvendig for toppledelsen å skape grenser når usikkerheten i markedet er høy eller når den interne tilliten i virksomheten er lav. Har ikke virksomheten slike grenser, kan det være fare for høy usikkerhet blant ansatte på grunn av dårlig dømmekraft eller lite involvering fra toppledelsen. Videre trekker Simons (1995b) frem at grensesystemet vil være en forutsetning for at ledelsen kan delegere ansvar nedover i virksomheten, som videre vil frigjøre tid som kan brukes på andre strategiske formål (Simons, 1995b).

Ifølge Simons (1995b) inngår s*trategiske grenser* i ledelsens strategiske planlegging, og grensene kan være en del av det strategiske planleggingsverktøyet. Strategisk planlegging brukes ofte til å fastsette hvilke søkeaktiviteter som ikke er akseptable, og som dermed ikke bør gjennomføres. Ettersom forretningsmuligheter dukker opp raskt og uregelmessig, mener Simons (1995b) at det er viktig at toppledelsen spesifiserer rekkevidden av forretningsmulighetene som det er nødvendig å bruke ressurser på. Formålet med strategiske grenser er dermed å bidra til at virksomhetens ressurser blir brukt på en produktiv måte. Videre hevder Simons (1995b) at ettersom virksomheter operer i dynamiske markeder, vil det alltid vil være en risiko for at strategiske grenser spesifiseres feil eller at forutsetninger blir endret. Dette medfører at toppledelsen ikke alltid har mulighet til å forutse alle endringer i markedet. Ifølge Simons (1995b) er det derfor viktig at ledelsen er fleksibel og klarer å redefinere grenser, hvis det er forhold i eller rundt virksomheten som medfører at det må endres (Simons, 1995b).

Diagnostisk styringssystem

Diagnostiske styringssystemer er formelle informasjonssystemer som ledelsen bruker for å overvåke organisatoriske resultater, og korrigere avvik fra forhåndsinnstilte standarder for prestasjon i virksomheten (Simons, 1995a). Eksempler på diagnostiske styringssystemer kan være budsjett, balansert målekort, profittplan eller forhåndsdefinert Key Performance Indicators (KPI). Styringssystemet måler output variabler som representerer viktige prestasjonsdimensjoner for en gitt strategi. Simons (1995b) definerer prestasjonsdimensjoner som viktige og kritiske suksessfaktorer. Videre vil det være nødvendig med en analyse av virksomhetens strategi for å identifisere korrekte prestasjonsvariabler, både finansielle og

ikke-finansielle (Simons,1995b). Når prestasjonsvariablene blir identifisert skal styringssystemet sikre at målmekanismer styres effektivt. Gjennom periodisk oppfølging kan ledelsen måle den faktiske produksjonen mot satte standarder, og dermed gir det mulighet til justering for å oppnå større måloppnåelse (Simons, 1995b). I tillegg har styringssystemet til hensikt å bidra til å minimere ledelsens behov for konstant overvåking. Det gjør at styringen kan foregå på et lavere nivå i virksomheten og ledelsen trenger kun å involvere seg i korte perioder. Dermed kan ledelsen holde fokuset på hvorvidt virksomhetens utfall reflekterer de målene som er satt for perioden (Simons, 1995a).

Interaktivt styringssystem

Interaktive styringssystemer er formelle informasjonssystemer som brukes av ledelsen for å involvere seg i sine underordnedes beslutningsaktiviteter (Simons, 1995b). Systemene er enkle å forstå og formålet med dem er å ha personlig og regelmessig kommunikasjon med de ansatte om sentrale strategiske spørsmål (Simons, 1995a). På den måten muliggjør systemene å aktivere søk slik at ledelsen kan oppfatte strategiske usikkerheter og dermed sette en agenda for diskusjon gjennom hele virksomheten (Simons, 1995b). Gjennom interaktive styringssystemer, kan virksomheter lære og diskutere mulige strategiske forbedringer. Å gjøre styringssystemer interaktive krever imidlertid oppmerksomhet fra ansatte gjennom hele virksomheten (Simons, 1995a). Ifølge Simons (1995b) har alle interaktive styringssystemer fire definerte karakteristika: (1) informasjon generert av systemet settes øverst på agenda på ledelsesnivået, (2) hyppig og regelmessig oppmerksomhet fra ledelsen på alle nivå, (3) data som er generert av systemet blir tolket og diskutert ansikt-til-ansikt med overordnede og underordnede, og (4) systemet er en katalysator for kontinuerlig utfordringer og debatt om underliggende data, forutsetninger og handlingsplaner (Simons, 1995b). I tillegg kan interaktive styringssystemer spore strategisk usikkerhet som omhandler teknologi, kunepreferanser, reguleringer og konkurransesituasjoner.

Trossystem

Ifølge Simons (1995b) er trossystemet det eksplisitte settet med organisatoriske definisjoner som toppledelsen kommuniserer formelt og forsterker systematisk for å gi grunnleggende verdi, formål og retning for virksomheten. Disse kjerneverdiene er knyttet til virksomhetens forretningsstrategi. Trossystemet forsøker å formilde informasjon om kjerneverdiene, herunder hvordan virksomheten skaper verdi, ønsket ytelsesnivå og hvordan relasjoner

håndteres både internt og eksternt (Simons, 1995b). Simons (1995a) mener at det er viktig at trossystemet er designet bredt nok til å appellere til ulike grupper innad i virksomheten, slik at de ansatte på den måten kan forplikte seg til organisasjonsverdier og formål. Hensikten er at ansatte skal ta best mulig valg på bakgrunn av kjerneverdiene. Imidlertid har komplekse, store og desentraliserte virksomheter ikke alltid et formelt system, og dermed ikke en klar og konsistent forståelse av kjerneverdiene. På den måten blir ansatte i slike virksomheter tvunget til å gjøre antagelser om hva som er akseptabel atferd i uforutsigbare omstendigheter (Simons, 1995a). Ifølge Simons (1995a) er det viktig å kommunisere verdiene riktig for at ansatte skal forstå og handle i tråd med kjerneverdiene i virksomheten. I tillegg er det viktig at ledelsen går foran som et godt eksempel på hvordan et slikt styringssystem skal fungere. Det betyr at ledelsen må handle i tråd med kjerneverdiene, slik at de på den måten klarer å uttrykke at kjerneverdiene er godt forankret i virksomheten (Simons, 1995b).

Kritikk til rammeverket

Ifølge Simons (1995b) vil styringssystemene styrkes hvis man komplementerer og bruker dem i sammenheng med hverandre. En kombinasjon av styringssystemene vil kunne skape et dynamisk samspill som vil legge til rette for både kontroll, innovasjon og kreativitet. Det blir imidlertid rettet kritikk til rammeverket, ettersom det kan oppstå misforståelser om begrepene "positiv" og "negativ" tilknyttet kvaliteten på styringssystemene (Tessier & Otley, 2012). Grunnen til dette, er at trossystemet og interaktivt styringssystem omtales som positive styringssystemer som skal legge til rette for at ansatte opptrer kreativt. Grensesystemet og det diagnostiske styringssystemet, omtales som negative styringssystem som begrenser de ansatte gjennom uttrykte regler og planer som virksomheten skal følge (Simons, 1995b).

2.2 Risiko

Risiko kan forklares på flere måter med ulike perspektiver og er derfor et begrepet som er preget av kompleksitet (Eriksen, 2017). Ifølge Segal (2011, s. 18-19) kan risiko defineres med tre aspekter: (1) risiko er usikkerhet, (2) risiko inkluderer positiv volatilitet og (3) risiko er avvik fra det forventede. Mange forbinder risiko med noe negativt, men det er viktig å fremheve at risiko også kan ha positive effekter. Segal (2011) viser at risiko kan ha positiv effekt, noe International Organization for Standardization (ISO) også gjør: "Effect of uncertainty on objectives and an effect is a positive or negative deviation from what is

expected." (ISO, 2009). The Committee of Sponsoring Organization for the Treadway Commission (COSO) sin definisjon på risiko tar derimot ikke hensyn at risiko kan ha positive effekter (COSO, 2017). Likevel poengterer COSO (2017) at uventede hendelser kan gi positive utfall, men ser på dette som muligheten til å veie opp for risikoutfallet og ikke som en del av risiko i seg selv. COSO (2017) definerer dermed risiko som følgende: "The possibility that events will occur and affect the achievement of strategy and business objectives." I forhold til COSO (2017), mener Segal (2011) derimot at positive effekter må inkluderes i risikobegrepet. Dette for å inkludere oppveiing av risikoutfall mellom ulike virksomhetsområder og risikohendelser som oppstår samtidig, samt kostnader forbundet med volatilitet. Presenterte definisjoner på risiko kan i en helhetlig sammenheng tolkes likt og vi ønsker å poengtere at i vår utredning vil vi involvere både negative og positive effekter knyttet til definisjonen på risiko.

Ifølge Segal (2011) skiller de fleste virksomheter mellom finansiell, strategisk og operasjonell risiko. Segal (2011, s. 116) definerer de ulike risikoene som følgende:

- Operasjonell risiko: "Unexpected changes in elements related to operations, such as human resources, technology, processes and disasters."
- Finansiell risiko: "Unexpected changes in external markets, prices, rates and liquidity supply and demand. This includes market risk, credit risk and liquidity risk."
- Strategisk risiko: "Unexpexted changes in key elements of strategy formulation or execution."

2.2.1 Operasjonell risiko

Definisjonen til Segal (2011) på operasjonell risiko, tar hensyn til både negative og positive effekter operasjonell risiko kan medføre. Dermed er definisjonen nyttig å bruke som utgangspunkt for virksomheters tilnærming til operasjonell risiko. Finanstilsynet (2016, s. 4) definerer operasjonell risiko som: "Risikoen for tap som følge av utilstrekkelige eller sviktende interne prosesser eller systemer, menneskelige feil eller eksterne hendelser." Definisjonen omfatter juridisk risiko, men ikke strategisk eller omdømmerisiko som må vurderes særskilt (Finanstilsynet, 2016).

Tidligere analysesjef i Finans Norge, Are Jansrud (2017b), viser til ulike risikoklasser som alle har en sammenheng med operasjonell risiko, presenteres i Figur 2. Ifølge Jansrud (2017b)

går operasjonell risiko på tvers av kreditt-, marked-, motparts-, og likviditetsrisiko. Kredittrisiko kan ha en sammenheng med operasjonell risiko i form av svake eller sviktende interne prosesser som oppstår av en uønsket operasjonell hendelse. Det kan for eksempel være utlånstap som følge av svake kredittprosesser, feilaktig eller mangelfullt informasjonsgrunnlag. Markedsrisiko kan oppstå på bakgrunn av avvik fra rammer og rutiner som er en operasjonell hendelse. Dette kan for eksempel være tap på finansielle posisjoner som følge av bevisste og ubevisste rammebrudd. Likviditetsrisiko kan være svake eller sviktende interne prosesser som er en uønsket operasjonell hendelse. Det kan for eksempel være unødvendige høye innlånskostnader som følge av svake eller mangelfulle rutiner for likviditetsprognoser (Jansrud, 2017b). Videre viser Jansrud (2017b) at omdømmerisiko ikke er en risiko, men en konsekvens av svake operasjonelle prosesser. Det kan for eksempler være tap på grunn av kundebehandling eller IT-problemer (Jansrud, 2017b). Ifølge Finanstilsynet (2016, s. 4) er operasjonell risiko "et vidt fagfelt som griper inn på overordnet styring og kontroll samt andre risikoområder. Dette gjør det mer utfordrende å avgrense risikoområdet." Ettersom operasjonell risiko går på tvers og har en sammenheng til flere av risikoklassene, finner vi det interessant å rette fokus på operasjonell risiko videre i vår utredning.

Figur 2: Risikoklasser (Jansrud, 2017b)

2.2.2 Modul for operasjonell risiko

Finanstilsynets modul for operasjonell risiko er en veiledning for finanstilsynets vurdering av foretakenes operasjonelle risiko (Finanstilsynet, 2016). Dokumentet benyttes av

Finanstilsynet under stedlig tilsyn og i forbindelse med vurdering av foretakenes samlede risikoprofil og kapitalbehov. Vurderingsmomentene i dokumentet er basert på bestemmelser i relevante lover og forskrifter for finansforetak (Finanstilsynet, 2016). I tillegg er Baselkomiteens "Principles for the Sound Management of Operational Risk" og EBAs "Guidelines on common procedures and methodologies for the supervisory review and evaluation process", samt andre relevante internasjonale retningslinjer på området lagt til grunn. Ut over dette er vurderingsmomentene også bygget på erfaring fra tilsynsarbeidet (Finanstilsynet, 2016). Videre i vår utredning vil vi ta utgangspunkt i innholdet til finanstilsynets modul for operasjonell risiko.

2.3 Risikostyring

Risikostyring (eng. Risk Management) har vi drevet med i århundrer på ulike områder og utviklingen går langt tilbake i tid (Bragelien, 2015; Jensen, 2015). Risikostyring har lenge vært en praksis som har fokusert på tekniske risikoanalyser innenfor spesifikke områder, herunder finans, forsikring, prosjektstyring, samt helse, miljø og sikkerhet (HMS), til å inngå som en integrert del av hvordan virksomheter styres (Power, 2007; Meidell, 2017). Ifølge Wiggen (2008) blir risikostyring definert på følgende måte: "Risikostyring klargjør og knytter sammen strategi og mål, og forsterker derigjennom lederens evne til styring og kontroll". Videre definerer IIA (2021, s. 14) risikostyring som følgende: "Et virkemiddel for å styre og kontrollere usikkerhet knyttet til virksomhetens evne til å skape, beskytte og realisere verdier, samt nå sine mål." I denne sammenhengen betegnes usikkerhet som mulige ikke planlagte negative utfall, samt potensielle positive utfall (IIA, 2021).

I 2004 omdøpte COSO risikostyring til helhetlig risikostyring (eng. Enterprise Risk Management) og i denne sammenheng kom COSO ut med et rammeverk for helhetlig risikostyring (Kaarbøe et al., 2013). Helhetlig risikostyring handler om å integrere risikostyring med selskapets øvrige virksomhetsstyring og strategi (KPMG, u.å.). Risikostyring ble dermed løftet opp på et strategisk nivå i virksomheten ved å fokusere på virksomhetens strategiske målsettinger og porteføljen av risikoer på tvers av hele virksomheten (Meidell, 2017). I den oppdaterte versjonen til COSO fra 2017 (oversatt i IIA, 2018, s. 8) blir helhetlig risikostyring definert på følgende måte: "Helhetlig risikostyring er den kulturen, de egenskapene og den praksisen som organisasjoner integrer med strategi, og som de benytter når strategien settes ut i praksis. Dette for å styre risikoen når verdier skapes,

bevares og realiseres." Ifølge COSO (2017) er hensikten med helhetlig risikostyring at virksomheter skal bli bedre til å forutse ulike typer risikoer, slik at de på den måten kan være proaktive og arbeide forebyggende (COSO, 2017). Maal (2018) hevder at helhetlig risikostyring ikke er et rammeverk eller et system som virksomheter raskt kan implementere. Det er en samlebetegnelse på ulike systemer, prosesser eller rammeverk som er med på å beskrive hvordan virksomheten skal håndtere risikoer relatert til strategiske mål (Maal, 2018).

2.3.1 Risikostyring og internkontroll

COSO (2013, s. 3) definerer internkontroll som: "En prosess igangsatt og gjennomført av virksomhetens styre, ledelse og øvrige ansatte og utformet for å gi rimelig sikkerhet med hensyn til oppnåelse av drifts-, rapporterings- og etterlevelsesrelaterte målsettinger." Risikostyring og internkontroll er to begreper som ofte blir brukt om hverandre og som omfatter mye av det samme (DFO, 2021a). En årsak til dette er at definisjoner og elementer i teoretiske rammeverk for internkontroll og risikostyring, ofte er like på flere punkter. I tillegg er risikostyring på et operasjonelt nivå i virksomheten en sentral del av arbeidet med internkontroll. Ser vi på historien til begrepene, *risikostyring* og *internkontroll,* ble risikostyring i COSO sitt rammeverk fra 1992 beskrevet som et underelement av internkontroll. På slutten av 1990-tallet ble det imidlertid en endring i forholdet mellom risikostyring og internkontroll. Risikostyring fikk en mer strategisk posisjon og internkontroll ble et underelement til risikostyring (Woods, 2011; Meidell, 2017). Siden slutten av 1990-tallet har internkontrollbegrepet gradvis blitt integrert i risikostyringsbegrepet (Meidell, 2017). På slutten av 1990-tallet ble det imidlertid en endring i forholdet mellom risikostyring og internkontroll. Risikostyring fikk en mer strategisk posisjon, og internkontroll ble et underelement til risikostyring (Woods, 2011; Meidell, 2017). Siden slutten av 1990-tallet har internkontrollbegrepet gradvis blitt integrert i risikostyringsbegrepet (Meidell, 2017).

Ifølge IIA (2021) kan risikostyring knyttet til måloppnåelse omfatte hele virksomhetens internkontrollsystem. I praksis vil mange likevel oppfatte at deler av internkontrollen vil ligge utenfor risikostyring, ettersom risikostyring konsentrerer seg om virksomhetens vesentlige og risikoutsatte aktiviteter, basert på kost/nyttevurderinger. Ifølge IIA (2021) vil hele internkontrollen konseptuelt ligge innenfor risikostyring i de virksomheter som lykkes med å integrere risikostyring i virksomhetsstyringen på alle nivåer (IIA, 2021). Videre viser IIA

(2021) at risikostyring og internkontroll er overlappende når man snakker om å identifisere og håndtere risiko som påvirker måloppnåelse innenfor målkategoriene:

- Driftsrelaterte mål - målrettet og effektiv drift
- Rapporteringsrelaterte mål – pålitelig rapportering
- Etterlevelsesrelaterte mål – overholdelse av lover og regler

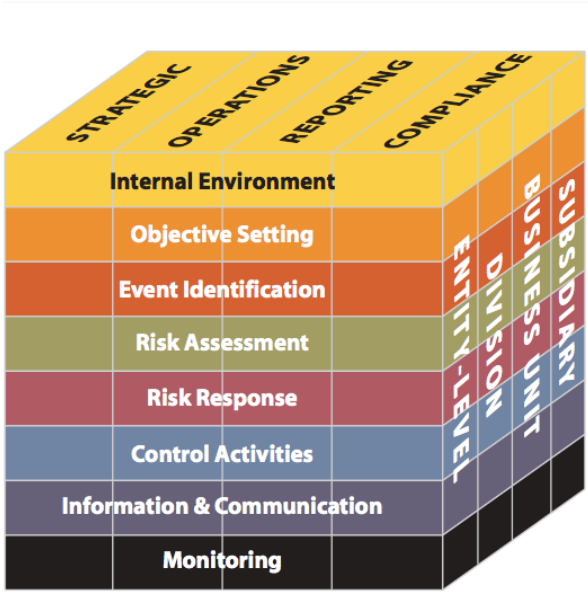
I tillegg har risikostyring et fjerde mål, overordnet mål, kalt strategisk mål som ikke er overlappende med internkontrollen. Risikovurderinger av disse overordnede målsettingene, resulterer i beslutninger om overordnede strategiske tiltak og planer og vil vanligvis ikke medføre konkrete internkontrolltiltak (IIA, 2021).

2.3.2 Standarder for risikostyring

Det er blitt utarbeidet veiledende standarder for implementering av helhetlig risikostyring. De mest brukte og anerkjente internasjonale standardene er ISO og COSO (IIA, 2018). Virksomheter står overfor risiko når de forfølger sine mål og disse to standardene er ment å hjelpe virksomheter for å ta riktig risiko, på riktig nivå. I det følgende vil vi presentere de to standardene med utgangspunkt i hvordan de kan benyttes som risikorammeverk for virksomheter.

Risikorammeverket: COSO

På verdensbasis har COSO rammeverket for helhetlig risikostyring blitt en mal for beste praksis for helhetlig risikostyring, som flere virksomheter benytter uavhengig bransje og størrelse (Power, 2007). Virksomheter benytter rammeverket for å identifisere risikoer og håndtere disse innenfor definert risikoappetitt, samt for å bidra til måloppnåelse. Rammeverket vektlegger den direkte koblingen mellom virksomhetens mål og ulike elementer av helhetlig risikostyring. Dette er illustrert i Figur 3, den tredimensjonale matrisen, en kube fra COSO sin modell i 2004 (COSO, 2004).



Figur 3: Enterprise Risk Management-rammeverk - Integrated Framework (COSO, 2004).

Den oppdaterte versjonen av rammeverket fra COSO 2017, har som formål at helhetlig risikostyring skal inngå som en del av virksomhetens DNA ved å skape en relasjon mellom risikostyring og virksomhetens arbeid med styring og strategi for å realisere mål (COSO, 2017). Som vist i Figur 4 tar rammeverket for seg 5 komponenter som gjensidig påvirker hverandre.

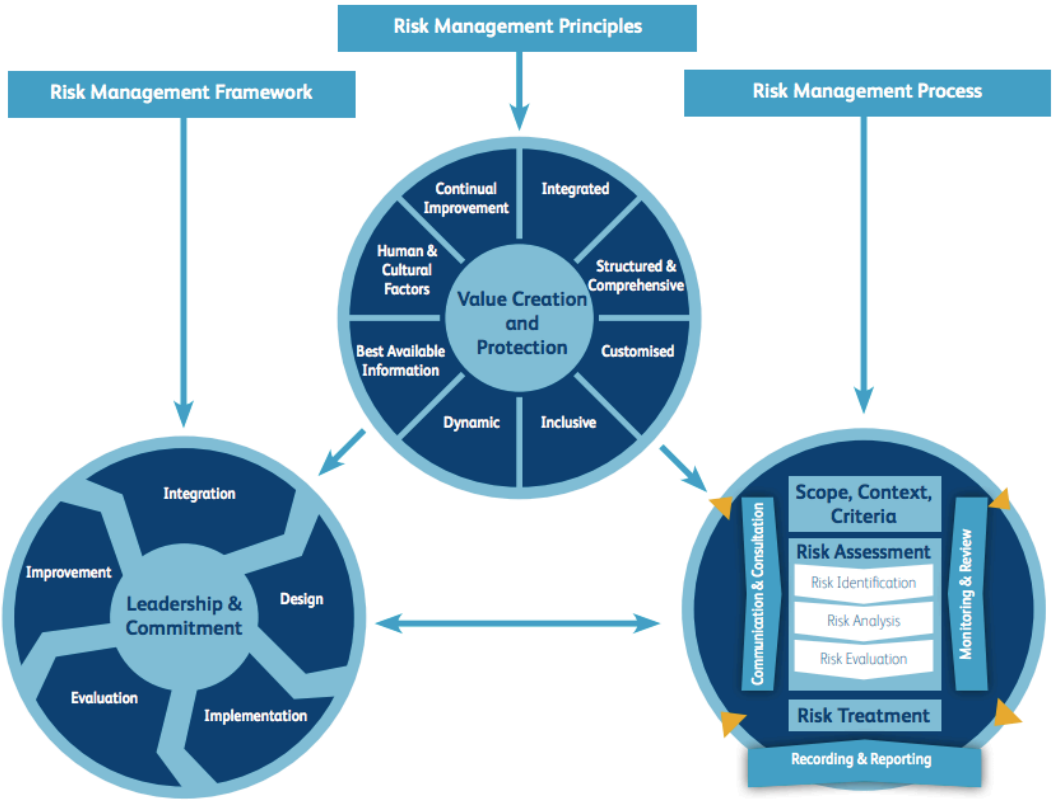
Figur 4: Enterprise Risk Management-rammeverk (COSO, 2017).

(1) *Virksomhetsstyring og kultur.* Virksomhetsstyring bidrar til etablering av organisasjonskultur, styrker betydning av helhetlig risikostyring og fastsetter ansvar for oppfølging. Kultur handler om etiske verdier, ønskelig atferd og forståelse av risiko i enheter.
(2) *Fastsettelse av strategi og mål.* Helhetlig risikostyring, strategi og fastsettelse av mål er

elementer som sammen fungerer i strategiprosessen. Risikoappetitt blir fastsatt og avstemt mot strategi, og virksomhetens mål setter strategien ut i praksis og danner samtidig grunnlag for identifisering og evaluering av risiko. (3) *Gjennomføring.* Risiko som kan påvirke oppnåelse av strategiske og operasjonelle mål må identifiseres og evalueres. Risiko prioriteres ut fra alvorlighetsgrad i forhold til risikoappetitt. Virksomheten velger deretter håndtering av risiko og benytter et porteføljesyn på hvor mye risiko virksomheten kan pådra seg. Resultatet av prosessen vil deretter rapporteres til relevante interessenter. (*4) Gjennomgang og revurdering*. Ved å gjennomgå måloppnåelse for enheter kan virksomheten ta stilling til hvor godt komponentene i den helhetlige risikostyringen virker over tid og ved endringer, samt identifisere behov for revurderinger. *(5) Informasjon, kommunikasjon og rapportering.* Helhetlig risikostyring krever en kontinuerlig prosess for å innhente og dele nødvendig informasjon som kommuniseres i hele virksomheten (COSO, 2017).

Risikorammeverk: ISO

COSO er imidlertid ikke det eneste rammeverket for å styre risiko. Den internasjonale standardiseringsorganisasjonen, ISO, har utviklet standarder for de fleste sektorer siden 1947 (Standard Norge, 2018). ISO har utviklet flere ulike standarder, og disse blir jevnlig oppdatert. I vår utredning ønsker vi å ta utgangspunkt i ISO31000, som gir oversikt over risikostyring og hvordan risikostyring skal implementeres i virksomheter (IRM, u.å.). Standarden beskriver prinsipper, rammeverk og prosesser for risikostyring som er presentert i Figur 5. Formålet med standarden er å integrere arbeidet med risikostyring i et strategisk og operasjonelt styringssystem (IIA, 2018).



Figur 5: Prinsipper, rammeverk og risikostyringsprosess i ISO31000 (IRM, u.å.)

Prinsippene beskrevet i ISO31000 skal gi virksomheter veiledning til effektiv risikostyring, dens verdi, intensjon og formål. Det er totalt 8 prinsipper i standarden presentert i Figur 5. Prinsippene gir en veiledning om hvordan risikostyring bør være designet til å arbeide med risikostyring. ISO31000 viser at risikostyring skal være integrert og strukturert, skreddersydd og dynamisk, i tillegg til å sørge for best mulig tilgjengelig informasjon. Samtidig som det skal ivareta menneskelig og kulturelle faktorer, og legge til rette for kontinuerlig forbedring (IIA, 2018). *Rammeverket* for risikostyring handler om integrering, design, implementering, evaluering og forbedring. Prinsippene og rammeverket er nært relatert ved at prinsippene skisserer hva som må oppnås og rammeverket gir informasjon om hvordan man oppnår nødvendig integrasjon (IRM, u.å.). *Risikostyringsprosessen* i ISO31000 består av (1) definere omfang, (2) kontekst og kriterier, (3) identifisere risiko, (4) risikoanalyse, (5) risikoevaluering og (6) risikohåndtering. Prosessen må imidlertid ikke følges stegvis, men kan tilpasses den enkelte situasjon. Den er også uavhengig av bransje, type og størrelse (IIA, 2018).

2.3.3 Forsvarslinjer

Innføring av helhetlig risikostyring har ført til at det har vokst frem nye roller og risikofunksjoner (Meidell, 2017). Det er viktig å definere roller og ansvar for de ulike funksjonene i virksomheten. Grunnen til dette er for å sikre effektiv ressursutnyttelse, gjennomføre tilfredsstillende kontroll av alle aktiviteter, og hindre duplisering av funksjoner og aktiviteter rettet mot risikostyring og internkontroll (IIA, 2018). Historisk har bank- og finanssektoren vært mest modne med hensyn på organisering av god virksomhetsstyring. Gjennom regulatoriske krav var de tidlig ute med implementering av en modell med tre forsvarslinjer (Liset, 2017). Modellen for "de tre forsvarslinjene" er illustrert i figur 6 (IIA, 2018). Modellen gir en oversikt over roller og ansvar for risikostyring og internkontroll på et overordnet nivå (IIA, 2018). IIA (2018) påpeker at modellen kun er et utgangspunkt og er dermed ikke et fasitsvar på hvordan man skal definere ulike roller og ansvar for de ulike funksjonene i virksomheten. Likevel er modellen et godt bidrag til å forbedre effektivitet og skape forståelse av virksomhetens helhetlige risikostyring og internkontroll, også for virksomheter der et formelt rammeverk for risikostyring eller system ikke eksisterer (IIA, 2015).

Figur 6: Tre forsvarslinjer (IIA, 2018).

Modellen skiller mellom tre linjer som er involvert i effektiv risikostyring og internkontroll. *Første forsvarslinje* eier og håndterer virksomhetens risikoer knyttet til driften, og må derfor påse at tilfredsstillende internkontroll gjennomføres (IIA, 2018). *Andre forsvarslinje* bidrar til utvikling og forvaltning av for eksempel rammeverk for risikostyring, styrings- og beslutningsprinsipper samt til videreutvikling av førstelinjes egne aktiviteter. I tillegg har de ansvar for å følge opp rapportering og opprettholde dialog med virksomheten. Støtte- og kontrollaktivitetene utføres blant annet av økonomiavdelingen, compliance[1] ansvarlig, risk manager, sikkerhets- og HMS ansvarlige, juridiske avdeling og kvalitetsstyring. Imidlertid vil disse funksjonene variere mellom virksomheter og bransjer (IIA, 2018). *Tredje forsvarslinje* utøves av internrevisjonen. Internrevisjonen gir styrende organer og toppledelsen en høyere grad av uavhengig og objektiv bekreftelse av internkontrollen i virksomheten, enn andrelinje (IIA, 2018). Videre er det viktig å være bevisst på at funksjonene i andre- og tredje forsvarslinje skal opptre uavhengig av enhetene de overvåker og kontrollerer. Det betyr at de ikke kan utføre arbeidsoppgaver som tilligger førstelinjen. I tillegg til disse tre interne forsvarslinjene, gir ekstern revisor en uavhengig bekreftelse av regnskapsrapportering (IIA, 2018).

2.4 Risikostyring og Simons rammeverk, Levers of Control

I dette delkapittelet vil vi integrere risikostyring som en del av det presenterte rammeverket for virksomhetsstyring, Simons (1995b), *Levers of Control.* Vi finner det interessant å integrere risikostyring i et rammeverk for virksomhetsstyring, ettersom det har vært et økende fokus på at risikostyring bør være en integrert del av virksomhetsstyringen (Pedersen & Ryen, 2019; Songedal & Saltermark, 2019). I det følgende vil vi integrere risikostyring innenfor hvert styringssystem som er presentert i delkapittel 2.1.1 basert på tidligere forskningslitteratur.

[1] «Compliance» innebærer etterlevelse av både eksternt og internt regelverk. I tillegg er etterlevelse et linjeansvar med ledelsen som øverste ansvarsnivå (IIA, 2015). Compliance kan oversettes til etterlevelse, men vi velger å benytte begrepet compliance videre i vår utredning.

2.4.1 Grensesystem

Ifølge Simons (1995a) avgrenser grensesystemet det akseptable aktivitetsområdet for organisasjonsdeltakerne. Grensesystemet kan ses på som spilleregler for å redusere selskapets risiko. Knytter vi dette opp til risikostyring, kan kontroll gjennom mekanismene innenfor grensesystemet bidra til å redusere nedsiderisiko. Simons (1995b) deler grensesystemet inn to typer: *(1) forretningsgrenser og (2) strategiske grenser,* som kan overføres til risikostyring.

(1) Forretningsgrenser

Organisering og ansvarsforhold

Forretningsgrenser setter grenser for hvordan man driver sin virksomhet. Ifølge Simons (1995b) er det nødvendig at toppledere skaper grenser når usikkerheten i markedet er høy eller når den interne tilliten i virksomheten er lav. Videre trekker Simons (1995b) frem at grensesystemet vil være en forutsetning for at ledere kan delegere ansvar nedover i virksomheten. Arena, Arnaboldi & Azzone (2010) hevder at delegering av ansvar for helhetlig risikostyring variere mellom virksomheter. Fra tidligere forskningslitteratur har det kommet frem flere roller som er involvert i helhetlig risikostyring i virksomheter (Arena et al., 2010; Beasley, Branson og Pagach, 2015; Mikes, 2009; Power, 2007). Beasley et al. (2015) viser til at styret og toppledelsen har det overordnede ansvaret for helhetlig risikostyring. Det er styret som har ansvar for hvordan hele prosessen for helhetlig risikostyring fungerer, mens toppledelsen har den daglige ledelsen av helhetlig risikostyring.

Utover dette er det kommet frem ytterligere to roller som er svært deltakende i virksomhetens helhetlige risikostyring, *risikoeksperter* og *risikoledere* (Arena et al., 2010; Beasley et al., 2015; Mikes, 2009; Power, 2007). Ifølge Arena et al. (2010) er det risikoekspertene som håndterer risiko innenfor spesifikke risikokategorier og som hovedsakelig er ansvarlig for den kvantitative silobaserte risikoanalysen. Mikes (2009) viser at man ofte finner risikoeksperter innenfor for eksempel kreditt- eller markedsrisiko i virksomheter. Økning av risikostyring har imidlertid ført til en fremvekst av en ny rolle. Denne rollen betegnes som risikoleder og kalles for Chief Risk Officer (CRO). CRO skiller seg fra risikoeksperter ved at de ikke nødvendigvis er eksperter i å beregne risiko, men heller fungerer som rådgivere for å støtte ledelsen i å ta ansvar for risiko (Arena et al., 2010; Power, 2007). Det er CRO som har ansvaret for å lede og integrere helhetlig risikostyring på tvers av virksomheter (Power, 2007). Kaplan & Mikes

(2016) påpeker at rollen som CRO imidlertid varierer mellom virksomheter. Beasley, Clune og Hermanson (2005) viser at det er en positiv sammenheng mellom virksomhetens implementering av helhetlig risikostyring og tilstedeværelse av CRO. Den positive sammenhengen fant de basert på data samlet inn fra 123 virksomheter i forbindelse med en studie hvor de undersøkte faktorer knyttet til implementasjon av helhetlig risikostyring i amerikanske og internasjonale virksomheter (Beasley et al., 2005). I tillegg viser Arena et al. (2010) til internrevisor og controller som også er to sentrale roller som er deltakende i virksomheters helhetlige risikostyring.

Risikoteknologier

Simons (1995b) påpeker at regler og krav begrenser de ansattes frihet og at grensene kommuniserer det akseptable handlingsrommet. Arena et al. (2010) viser til risikoteknologier som defineres som komplekse sett med praksis, prosedyrer og instrumenter som er vedtatt for å oppnå ledelse og kontroll for å styre risiko. For gjennomføring av helhetlig risikostyring, vil dermed risikoteknologier kunne bli betegnet som grenser hvor elementer av risikoteknologier har grensesettende effekter. Slike grensesettende effekter er risikorammeverk og risikopolicyer. Forskjellen er at risikorammeverk vil inneholde mer detaljer om utførelsen av helhetlig risikostyring, mens risikopolicyer er mer overordene regler for helhetlig risikostyring (Fraser & Simkins, 2016). Ifølge Beasley et al. (2015) og Fraser & Simkins (2016) er det hensiktsmessig å benytte risikorammeverk og risikopolicy for å formalisere helhetlig risikostyring i virksomheten. Beasley et al. (2015) viser at det er en rekke prinsippbaserte rammer for å hjelpe ledelsen i utforming og implementering av helhetlig risikostyring. Både Beasley et al. (2015) og Fraser & Simkins (2016) viser til ISO31000, og i tillegg viser Beasley et al. (2015) til COSO. Disse rammeverkene understreker den viktige rollen som den overordnede kulturen og ledelsen fra styret og toppledelsen spiller i risikostyringsprosessen (Beasley et al., 2015). Lundqvist (2014) hevder at vanlig praksis for helhetlig risikostyring i virksomheter er å ta utgangspunkt i rammeverkene, og deretter utforme sitt eget interne rammeverk for implementering av helhetlig risikostyring. Videre anbefaler Fraser & Simkins (2016) at virksomheter bør utarbeide risikopolicyer. Disse bør inneholde prinsipper om at risiko vil bli styrt helhetlig og definerer ansvaret til toppledelsen, styret og CRO (Fraser & Simkins, 2016). I tillegg hevder Jansrud (2017a) at policyer bør inneholde kvantifiserte rammer for eksponering på ulike områder og type operasjonell risiko.

(2) Strategiske grenser

Hvis vi knytter risiko til strategiske grenser, vil etablering av slike grenser være sentralt for at virksomheters aktiviteter og beslutninger skal samsvare med virksomheters strategi. Formålet med strategiske grenser er å bidra til at virksomheters ressurser blir brukt på en produktiv måte, og at toppledelsen spesifiserer rekkevidden av forretningsmuligheter som det er nødvendig å bruke ressurser på (Simons, 1995b). Risikoappetitten kan sette strategiske grenser for hvor stor risiko den ansatte i virksomheten vil ha lov å ta (COSO, 2017). COSO (2017) definerer risikoappetitt som følgende: "The organization defines risk appetite in the context of creating, preserving, and realizing value." Ifølge Mikes, Oyon & Jeitziner (2017) vil risikoappetitt for risiko kunne plasseres som en del av Simons (1995b) grensesystem. Hillson & Murray-Webster (2011) viser at risikoappetitt vil inngå som en del av virksomheters strategiske grensesystem i relasjon til helhetlig risikostyring ved at det settes grenser for akseptabelt risikonivå i virksomheten. IIA (2018) redegjør for at risikoappetitt består av "vilje" og "evne". Det omhandler nivået av usikkerhet som en virksomhet er villig, og har evne til å påta seg for å kunne gjennomføre sine aktiviteter og realisere sine mål. Risikoappetitt vil variere fra virksomhet til virksomhet, avhengig av strategi, bransje og organisasjonskultur. I tillegg vil lovkrav også påvirke virksomheters risikoappetitt. Videre tydeliggjør IIA (2018) at det er viktig at definert risikoappetitt kan operasjonaliseres. Det betyr at det bør være en rød tråd gjennom virksomhetens mål, styringsrammer, fullmakter og handlingsrom som samsvarer med den totale risikoappetitt og strategi (IIA, 2018). IIA (2018) påpeker også at risikoappetitt kan defineres kvalitativt eller kvantitativt i form av fullmakts- og eksponeringsgrenser innenfor ulike risikotyper. Ifølge Bromwiley et al. (2015) er det imidlertid lite forskning på hvorvidt virksomheter har en konsistent risikoappetitt. Likevel er det stadig flere som benytter seg av risikoappetitt som et verktøy i helhetlig risikostyring (Deloitte, 2014). Barfield (2007) tydeliggjør at det er en stor fordel å definere risikoappetitt for å sørge for at risiko blir eksplisitt.

2.4.2 Diagnostisk styringssystem

Ifølge COSO (2017) omhandler standardprosess for helhetlig risikostyring å identifisere, vurdere og håndtere risiko forbundet med strategi. I det følgende vil vi presentere former for diagnostisk styring som kan knyttes til standardprosessen for helhetlig risikostyring.

Risikoverktøy

Ifølge Arena et al. (2010) vil det være hensiktsmessig for risikoidentifisering og vurdering å ta i bruk risikoverktøy, som for eksempel risikokategoriseringsmodell eller risikomatrise.

Duijm (2015) hevder at risikomatrise blir mye brukt i operasjonell risikostyring. Risikomatrise er et enkelt verktøy for å rangere og prioritere risikoer for uønskede hendelser, samt for å ta avgjørelser om risikoer kan tolereres. En risikomatrise viser de grunnleggende egenskapene *konsekvens* og *sannsynlighet* av en uønsket hendelse, istedenfor numeriske verdier. Kombinasjoner av konsekvens og sannsynlighet blir kartlagt for å begrense antall risikokategorier. Denne kartleggingen omfatter imidlertid subjektive betraktning omkring risiko. Duijm (2015) viser til to svakheter med risikomatrise. Den første svakheten omhandler beslutningstaking om når virksomheter skal akseptere risiko basert på ulike fargenivå. Den andre svakheten omhandler hvilke risikoer virksomheter skal prioritere først ettersom virksomheter kan ha mange risikoer. Det er viktig å være klar over svakheter med matrisen, slik at man på den måten klarer å velge ut riktige risikoer basert på vurderinger (Cox, 2008; Flage & Røed, 2012; Duijm, 2015).

Eksempler på styringssystemer

Budsjett, balansert målekort og KPI er eksempler på diagnostiske styringssystemer. For å kunne vise at diagnostiske styringssystemer kan knyttes til risikostyring, er det imidlertid viktig å undersøke om hvorvidt risikoer blir inkludert i utarbeidelsen og evaluering av slike systemer. Det er blitt gjennomført tidligere forskning på integrering av risikostyring og slike diagnostiske systemer. Arena et al. (2010) og Giovannoni, Quarchioni & Riccaboni (2016) viser at virksomheter integrerer budsjett med helhetlig risikostyring. Videre viser Giovannoni et al. (2016) at ved å benytte seg av KPI-er hvor risiko blir inkludert, vil risikostyring på den måten bli et viktig agendapunkt hos styret og toppledelsen. Kaplan (2009) viser at balansert målekort er et verktøy for å integrere risikostyring med strategi og presentasjonsstyring. Power (2009) tydeliggjør videre at risiko bør inngå som en kritisk vurdering i utarbeidelse av budsjetter og planlegging, samt utforming av strategiprosessen. Beasley, Branson og Hancock (2017) viser at virksomheter finner det utfordrende å integrere risikostyring med strategisk planlegging.

Rapportering

Ifølge Wiggen (2008) er jevnlig rapportering til styret og toppledelsen viktig for at risikostyringssystemet skal overleve. Formålet med rapportering er å kunne opprettholde ønsket risikoprofil og samtidig sørge for at planlagte tiltak blir gjennomført. Chapelle (2019) viser imidlertid at en utfordring knyttet til risikorapportering er at det er vanskelig å finne den

riktige balansen mellom hvor mye informasjon man skal inkludere i rapporten. I tillegg er det en utfordring knyttet til å skille mellom informasjon som skal gå til ulike mottakere i virksomheten. Ifølge Chapelle (2019) er beste praksis å inkludere tydelig ansvar og tidsrammer for hver handlingseier med dokumentasjon og sporing, vanligvis månedlig.

2.4.3 Interaktivt styringssystem

Ifølge Simons (1995b) er det interaktive styringssystemet det formelle systemet som ledelsen bruker for å involvere seg personlig og regelmessig i sine underordnedes beslutningsaktiviteter. Systemet kan dermed knyttes til risikostyring med utgangspunkt i hvordan virksomheter kommuniserer og diskuterer risiko. Fraser & Henry (2007) hevder at relasjon og kommunikasjon mellom styret, toppledelsen og ledelsen er kritisk for en effektiv implementering av helhetlig risikostyring. Videre trekker COSO (2017) frem viktigheten av kommunikasjon knyttet til risiko.

Sheehan (2010) påpeker at som en del av det interaktive styringssystemet må ledelsen kontinuerlig samle inn informasjon og oppfordre til diskusjon om sentrale risikoer i virksomheten. Det er kritisk at toppledelsen og styret får informasjon om de viktigste risikoene for å oppnå et vellykket interaktivt styringssystem. Det er ledelsen som må sørge for at toppledelsen og styret får denne informasjonen (Sheehan, 2010). Ifølge Fraser & Henry (2007) vil diskusjon og debatt om de viktigste risikoene på alle nivåer i virksomheter bidra til økt forståelse og håndtering av risiko. Sheehan (2010) hevder at hvis styret og toppledelsen ønsker å få informasjon om risikoer i virksomheten må de sikre at ansatte har en felles forståelse om virksomhetens strategi, og forstår hvordan de kan bidra med sine tanker. I tillegg til forståelse om at virksomhetens verdisystem vektlegger informasjonsdeling (Sheehan, 2010).

Kaplan & Mikes (2016) viser til "risk talk" i arbeidet med å få risikostyring som en integrert del av daglig forretningsaktivitet. "Risk talk" blir definert som: "An organizational discourse about risk issues ranging from taskrelated problems and perceived organizational weaknesses to concerns about resource planning" (Arena, Arnaboldi & Palermo, 2017). Ifølge Power (2016) er kontinuerlig "risk talk" en nødvendig forutsetning for å skape aksept for formelle elementer i helhetlig risikostyring. Videre tydeliggjør Power (2016) at det er viktig å etablere prosesser for å bringe deltakere fra forskjellige nivåer i virksomheten sammen. "Risk talk" kan for eksempel være workshop og ansikt-til ansikt møter. Mikes & Kaplan (2014) viser at risikoworkshop er en arena hvor risiko blir diskutert. Formålet er å identifisere de viktigste

risikoene knyttet til å realisere virksomhetens mål. På den måten kan vesentlig informasjon om risikotrender fremkomme for å kunne nå virksomhetens mål (Mikes & Kaplan, 2014). Det er CRO som skal legge til rette for kontinuerlig "risk talk" gjennom workshop og ansikt-til-ansikt møter (Power, 2016; Mikes & Kaplan, 2014).

2.4.4 Trossystem

Ifølge Simons (1995b) forsøker trossystemet å formilde informasjon om kjerneverdier, herunder hvordan virksomheten skaper verdi, ønsket ytelsesnivå og hvordan enkeltpersoner forventes å håndtere relasjoner både internt og eksternt. Trossystemet virker styrende ved at virksomhetens kjerneverdier påvirker virksomhetens kultur og de ansattes holdning til å se muligheter. Hvis vi knytter dette opp til risiko, vil kjerneverdiene til virksomheten påvirke risikokulturen og risikoholdninger til ansatte.

Organisasjonskultur defineres som måten ansatte arbeider på og de holdninger og verdier som preger felleskapet som blir tydelig når kulturen er under press eller må endres (Glomseth, 2019). Risikokultur er mer spesifikt knyttet til normer, holdninger og atferd relatert til risikostyring i virksomheten (Skogum, 2021). Ifølge Power et al. (2013) definerer flere forfattere risikokultur som et element av organisasjonskulturen. Videre viser Mikes et al. (2017) at risikokultur reflekterer Simons (1995b) trossystem. Risikokultur handler dermed om hvordan ledere og ansatte handler og tenker ut ifra en risikoforståelse for å oppnå og opprettholde risikoprofilen til virksomheten i overensstemmelse med definerte mål (Wiggen, 2008). Institute of International Finance (IIF) (2009) viser til definisjon av risikokultur på en relativ lik måte. IIF (2009) definerer risikokultur som normer og tradisjoner for individer og gruppers atferd i en virksomhet som bestemmer måten de identifiserer, forstår, diskuterer og handler på bakgrunn av risikoen som virksomheten blir konfrontert med eller den risikoen de tar. Wiggen (2008) tydeliggjør at utviklingen av risikokultur gir bevisstgjøring og bygging av kompetanse relatert til risikostyring som begrep og prosess, samt tilbakemeldinger på innmeldte forhold. Videre påvirker risikokultur ledelsens og medarbeidernes beslutninger i løpet av den daglige aktiviteten og har innvirkning på risikoer de påtar seg (Financial Stability Board, 2014).

Risikoholdning er en vurdering av hvor stor risiko det er ønskelig å ta (Mellemseter & Mørch, 2006). Dermed kan risikoholdningen til den ansatte påvirkes av risikoappetitt i virksomheten. Ifølge COSO (2017) definerer virksomheters risikoappetitt som en del av prosessen med å

skape, bevare og realisere verdi. Dermed kan risikoappetitt bidra til å skape muligheter og på den måten kan man oppnå positive effekter av risiko for virksomheten. Når risikoer endrer seg og øker med omfang blir ledelsen mer opptatt av om de tar de riktige risikoene, enn om omfanget av risikoene er innenfor virksomhetens risikoappetitt. Ifølge Noreng (2002) bør en virksomhet fastsette risikoappetitt og risikokapasitet på samme måte som de individuelle investorene. En virksomhets appetitt vil variere med den strategien de har valgt, kombinert med endrede betingelser i bransjen eller markedene. Det medfører at hver virksomhet vil ha sin egen unike risikotoleranse. Den vil være forskjellig fra virksomhet til virksomhet, både på grunn av organisasjonskultur og eksterne faktorer. Videre hevder Noreng (2002) at et kritisk element i lederens ansvar er å beslutte hvor mye og hvilke risikoer virksomheten bør ta. En slik beslutning må imidlertid revurderes etter hvert som forutsetningene endres.

3.0 Forskningsmetode

Studien har blitt gjennomført som en flercasestudie av tolv virksomheter og har blitt vurdert av Norsk Senter for Forskningsdata (NSD). Med problemstilling og forskningsspørsmål som ramme har det blitt samlet inn kvalitative data fra tolv respondenter i sentrale stillinger innenfor risiko- og virksomhetsstyring. I dette kapittelet vil vi redegjøre for metodiske valg som vi har tatt i forbindelse med forskningsdesign og datainnsamling. Videre vil vi presentere hvordan datamaterialet har blitt analysert. Avslutningsvis vil vi evaluere forskningens kvalitet og forskningsprosjektets etiske vurderinger.

3.1 Forskningsdesign

Forskningsdesign er den generelle planen for hvordan man skal gå frem for å besvare forskningsspørsmålene (Saunders, Lewis & Thornhill, 2016). I vår studie har vi valgt å benytte oss av et eksplorerende design ettersom forskningsspørsmålene våre er komplekse og fremtidsrettet, og det er begrenset med tidligere forskning på området. Ifølge Selnes (1999) er et eksplorerende design anvendelig å benytte når hensikten er å fordype seg i noe man lite om. Ved å anvende et eksplorerende design gir det oss dermed mulighet til å utforske operasjonell risikostyring nærmere, slik at vi får dybdekunnskap på området. Et eksplorerende design karakteriseres som et fleksibelt design, hvilket betyr at man i praksis kan endre problemstillingen etter hvordan studien utvikler seg (Saunders et al., 2016). Ettersom vi velger å anvende et eksplorerende design er det vanlig å benytte seg av kvalitativ metode (Saunders et al., 2016). Ved å anvende kvalitativ metode bruker vi datamaterialet i form av ord fremfor tall, og vi fokuserer på dybdeforståelse i forskningen (Johannessen, Tufte, Christoffersen, 2016). På den måten gir det oss mulighet til å få frem ulike nyanser og dybdeforståelse av fenomenet vi ønsker å undersøke (Saunders et al., 2016).

3.1.1 Forskningstilnærming

I vårt forskningsprosjekt er det anvendelig å benytte en induktiv tilnærming, ettersom vi ønsker å utforske et emne og utvikle en teoretisk forklaring etter hvert som dataene blir innhentet og analysert. En induktiv tilnærming vil også være hensiktsmessig å benytte ettersom vi har valgt et eksplorerende design og kvalitativ metode (Saunders et al., 2016). Som

utgangspunkt for datainnsamlingen benyttet vi tidligere forskningslitteratur for å tilegne forståelse om temaet, i tillegg ønsket vi at situasjoner som oppstod underveis skulle være med å forme studien. På bakgrunn av dette har vi dermed ikke en ren induktiv studie, og en kombinasjon av deduktiv og induktiv vil derfor være nødvendig for å kunne trekke korrekte konklusjoner av virkeligheten (Saunders et al., 2016). Videre har det vært utfordrende å forholde seg helt objektiv til tema, uten noe form for forståelse for det vi ønsket å undersøke.

På bakgrunn av et eksplorerende forskningsdesign med en induktiv tilnærming var det hensiktsmessig å benytte et kvalitativt intensivt undersøkelsesopplegg. Grunnen var at vi ønsket å innhente mye informasjon fra få personer i deres naturlige kontekst (Saunders et al., 2016). Vi ønsket å tilegne oss en forståelse av hvordan ansatte som hadde sentrale roller innenfor risiko- og virksomhetsstyring arbeidet med operasjonell risikostyring. Hensikten var å komme frem til konkrete styringsmekanismer i virksomheter som kunne ha betydning, fremfor generelle meninger om spesifikke temaer. Denne type informasjon ville vi ikke fått tilgang til ved å benytte et kvantitativt undersøkelsesopplegg (Saunders et al., 2016).

3.1.2 Forskningsstrategi

Forskningsstrategi kan defineres som en plan for hvordan vi skal besvare våre forskningsspørsmål. Ettersom vi har en kvalitativ undersøkelse, er en av de vanligste strategiene som brukes casestudie (Saunders et al., 2016). Casestudie er en grundig undersøkelse av et emne eller fenomen innenfor dets virkelige setting (Yin, 2014; Saunders et al., 2016). På den måten fører det til rike, empiriske beskrivelser og utvikling av teori (Saunders et al., 2016). Hensikten med studien var å få en bred forståelse innenfor fagfeltet og samtidig opparbeide en god forståelse av operasjonell risikostyring i praksis. For å oppnå dette valgte vi dermed å gjennomføre en flercasestudie, hvor vi undersøkte tolv virksomheter (Yin, 2014; Saunders et al., 2016). Dette muliggjorde at vi kunne hente inn informasjon fra flere enheter og på den måten gjennomføre en omfattende datainnsamling. I tillegg bidro det til å øke muligheten for generalisering til andre lignende case (Jacobsen, 2015).

3.2 Datainnsamling

I henhold til vår utredning har vi samlet inn sekundær- og primærdata. Sekundærdata er data som vi analyserer i vår utredning, men som opprinnelig er blitt samlet inn til et annet formål,

noen ganger behandlet og lagret (Saunders et al., 2016). Primærdata er data vi selv samler inn for å undersøke våre forskningsspørsmål (Saunders et al., 2016). I det følgende vil vi derfor presentere sekundær- og primærdata som har blitt benyttet i vår utredning.

3.2.1 Sekundærdata

Sekundærdata kan være offentlig tilgjengelige rapporter og interne dokumenter fra de aktuelle virksomhetene (Saunders et al., 2016). I forkant av intervjuene ble offentlig tilgjengelige årsrapporter gjennomgått. I etterkant av intervjuene fikk vi tilsendt andre relevante dokumenter og rapporter som fungerte som et supplement til intervjuene. I tillegg ha vi benyttet eksisterende litteratur på fagfeltet.

3.2.2 Primærdata: Semistrukturerte intervjuer

For å innhente primærdata er det flere ulike typer intervjuer som man kan benytte. Intervjuer kan være sterkt formaliserte og strukturerte ved bruk av standardiserte spørsmål for hver forskningsdeltaker, eller det kan være uformelle og ustrukturerte samtaler (Saunders et al., 2016). For å innhente primærdata valgte vi å benytte semistrukturerte intervjuer. Semistrukturerte intervjuer blir også ofte referert til som kvalitative forskningsintervjuer (Saunders et al., 2016). På forhånd hadde vi utarbeidet en intervjuguide som var strukturert med sentrale spørsmål til ulike temaer med underspørsmål tilknyttet hvert tema. Dette gjorde vi for å sikre at hvert tema ble belyst (Saunders et al., 2016). Bruken av spørsmålene varierte imidlertid fra intervju til intervju, ettersom vi undersøkte ulike virksomheter innenfor ulike bransjer. I noen intervjuer ble dermed enkelte spørsmål utelatt og rekkefølgen på spørsmålene varierte (Saunders et al., 2016). Utarbeidet intervjuguider er vedlagt i vedlegg 2 og 3.

Utvalg

For å få et helhetlig inntrykk av operasjonell risikostyring i virksomheter var det avgjørende å innhente informasjon fra personer som hadde god kjennskap innenfor fagfeltet. Derfor var det hensiktsmessig å velge ut respondenter som hadde forståelse, kompetanse og erfaring innenfor risikostyring i virksomheter. I Tabell 1 er respondentene i vår utredning presentert.

VIRKSOMHET	RESPONDENT	DATO	STED	TID	ORD
PwC	Respondent 1	02.03.2021	Teams	1:09:26	7051
EY	Respondent 2	10.03.2021	Teams	50:32	5466
Sbanken	Respondent 3	09.03.2021	Teams	1:04:22	6688
Sparebanken Vest	Respondent 4	03.03.2021	Teams	46:02	4594
Sparebanken Sogn & Fjordane	Respondent 5	10.03.2021	Teams	1:03:01	6128
Storebrand	Respondent 6	10.03.2021	Teams	1:03:10	6751
Nbim	Respondent 7	03.03.2021	Teams	50:00	6104
Fiskeridirektoratet	Respondent 8	19.03.2021	Teams	47:24	3996
Bremnes Seashore	Respondent 9	11.03.2021	Teams	53:07	4866
Nye Veier	Respondent 10	11.03.2021	Teams	53:17	5636
Ruter	Respondent 11	11.03.2021	Teams	58:01	4764
BKK	Respondent 12	22.03.2021	Teams	39:52	3764

Tabell 1: Oversikt over respondenter

Videre har vi fordelt virksomhetene inn i tre kategorier: (1) konsulentselskap, (2) finansforetak og (3) fiskeri og infrastruktur, som er fremstilt i tabell 2. Innenfor konsulentselskapene intervjuet vi én respondent fra PricewaterhouseCoopers (PwC) og én respondent fra Ernst & Young (EY). Begge respondentene bistår virksomheter med problemstillinger tilknyttet risikostyring og internkontroll. Innenfor finansforetakene intervjuet vi fem virksomheter, hvor alle respondentene hadde sentrale roller innenfor risikostyring. Innenfor fiskeri og infrastruktur intervjuet vi fem virksomheter, hvor alle respondentene hovedsakelig hadde en sentral rolle innenfor avdeling for virksomhetsstyring, hvor de i ulik grad arbeidet eller ble berørt av risikostyring.

KONSULENTSELSKAP	FINANSFORETAK	FISKERI OG INFRASTRUKTUR
PwC	Sbanken	Fiskeridirektoratet
EY	Sparebanken Vest	Bremnes Seashore
	Sparebanken Sogn & Fjordane	Nye Veier
	Storebrand	Ruter
	NBIM	BKK

Tabell 2: Oversikt over bransjer

3.2.3 Gjennomføring av intervju

Nøkkelen til et vellykket intervju er nøye forberedelse og derfor er det en rekke elementer som det er nødvendig å gjøre i forkant (Saunders et al., 2016). I forberedelsene hadde vi et stort fokus på å tilegne oss kunnskap og forståelse for temaet vi skulle undersøke. Dermed brukte vi mye tid på å tilegne oss kunnskap gjennom tidligere forskningslitteratur og virksomhetenes offentlige årsrapporter. Dette arbeidet så vi i etterkant var spesielt viktig i utarbeidelse av intervjuguidene og ved gjennomføring av intervjuene. Vi opplevde at det var en stor fordel å stille godt forberedt til hvert intervju slik at vi fikk innhentet mest mulig relevant informasjon fra respondentene.

Intervjuguidene ble utarbeidet med utgangspunkt i rammeverket til Simons (1995) *Levers of Control*. Vi hadde fokus på at spørsmålene i intervjuguidene ble formulert tydelig, slik at respondentene skulle forstå spørsmålene vi stilte. I tillegg valgte vi å formulere åpne spørsmål for å unngå skjevheter og stilte oppfølgingsspørsmål for å få dypere innsikt i tematikken (Saunders et al., 2016). Intervjuguidene er vedlagt som vedlegg 2 og 3. Vedlegg 2 inneholder intervjuguide for konsulentselskapene. Intervjuguiden ble utformet på en slik måte at konsulentene kunne dele erfaringer om hvordan virksomheter driver med risikostyring og hva de ofte trenger bistand med når det kommer til operasjonell risikostyring. Vedlegg 3 inneholder intervjuguide for finansforetakene, og fiskeri og infrastruktur. Intervjuguiden ble utformet på en slik måte at vi skulle få innblikk i hvordan virksomhetene drev med operasjonell risikostyring, hva som gjøres bra og hva de fant utfordrende.

I forkant av intervjuene sendte vi ut nødvendig informasjon og samtykkeskjema til alle respondentene for å redusere usikkerhet og bekymring (Saunders et al., 2016). Samtykkeskjema er vedlagt i vedlegg 1. Alle respondentene fikk tilsendt en mail med informasjon om forskningsprosjektet, intervjutema og deres rettigheter som intervjuobjekt. På den måten fikk respondentene tid til å forbedre seg og finne frem støttende dokumenter. I tillegg til å redusere usikkerhet tilknyttet deltagelse. Det er ofte stor usikkerhet om deling av informasjon som omhandler hvordan og på hvilke måter dataen brukes (Saunders et al., 2016). Derfor ønsket vi å komme med en avklaring om den eksakte naturen til dataen vi ønsket å innhente. Innledningsvis i hvert intervju forklarte vi hva som var formålet med intervjuet, i

tillegg gjennomgikk vi samtykkeskjema, redegjorde for anonymisering og respondentens rettigheter. Hensikten var å etablere troverdighet og tillit (Saunders et al., 2016).

Ettersom vi anvendte semistrukturerte intervjuer hadde vi mulighet til å være fleksible under intervjuet og respondentene fikk mulighet til å snakke fritt innenfor en gitt kontekst. I tillegg stilte vi oppfølgingsspørsmål for å utforske temaene ytterligere, og dermed varierte både tidsbruk og antall spørsmål som ble stilt til respondentene. For å registrere data under intervjuene valgte vi å benytte oss av lydopptak og notater. Bakgrunnen for at vi valgte å ta notater var i tilfelle innspillingen ikke var vellykket. Det bidro også til at vi fikk skrevet ned egne tanker og eventuelle hendelser som ikke kom frem i lydopptaket (Saunders et al., 2016).

3.3 Dataanalyse

Dataanalyse er en grundig undersøkelse av den innsamlede dataen. Etter at intervjuene var gjennomført ønsket vi å gå i dybden for å hente ut størst mulig verdi og for å luke ut uegnet informasjon. Dette gjorde vi ved å trekke ut meninger, kategorisere og skape forståelse av informasjonen (Johannessen et al., 2016).

Med en gang vi hadde gjennomført intervjuene med de tolv respondentene utarbeidet vi en fullstendig oversikt over intervjuene, som også inkluderte kontekstuell data. Dette var viktig for å unngå at den detaljerte forståelsen av hva som ble sagt gikk tapt, og for å unngå at vi blandet data fra de forskjellige intervjuene. I tillegg til dette registrerte vi følgende kontekstuelle data: sted for intervjuet, dato, tidsbruk, bakgrunnsinformasjon om deltakerne og det umiddelbare inntrykket vi fikk av gjennomføringen. Det var i tillegg viktig å sikre deltakernes anonymitet. For å gjøre dette brukte vi en "nøkkel" som var et upersonlig kodenummer, slik at vi kunne koble deltakerne til dataene sine ved hjelp av respondent 1, respondent 2 etc. (Saunders et al., 2016).

Deretter satt vi i gang med selve dataanalysen. Det første steget handlet om å gjøre seg kjent med dataen og dette gjorde vi gjennom transkribering. Oppgaven med transkribering av lydopptakene var tidkrevende, ettersom vi ikke bare måtte registrere nøyaktig hva som ble sagt og av hvem, men vi måtte også prøve å gi en indikasjon på tonen og deltakernes ikke-verbal kommunikasjon. For å unngå at detaljert informasjon gikk tapt transkriberte vi derfor kort tid etter at intervjuene var gjennomført (Saunders et al., 2016).

Før vi begynte med koding ble det transkriberte materialet lest gjennom for å få en oversikt over de innsamlede dataene. Basert på dette utarbeidet vi en grov oversikt over hva som kunne betraktes som funn ved systematisk skjematisering. Ettersom målet med kodingen var å fange opp hvordan virksomheter arbeider med operasjonell risikostyring var det hensiktsmessig å benytte koder som definerte handlinger eller erfaringer som respondentene beskrev. Her trakk vi ut paralleller mellom data og teori som videre førte til kategorisering av dataen. Ifølge Jacobsen (2015) betyr det å kategorisere koder at informasjonen grupperes etter et sett kriterier som forsker setter. Kategoriene ble utviklet på bakgrunn av hvilke funn som var relevant til teorien. Utgangspunktet vårt var rammeverket til Simons (1995b) og dermed kodet vi etter: (1) grensesystemet, (2) diagnostisk styringssystem, (3) interaktivt styringssystem og (4) trossystem. I denne prosessen fjernet vi også deler av det teoretiske grunnlaget, samtidig som vi la til annen teori som hadde større relevans for tematikken og datamaterialet i utredningen.

Vi valgte å redegjøre for funn innenfor hver av de tre bransjene. Dermed er kapittel 4.0 empiriske funn, delt inn etter: 4.1 Finansforetak, 4.2 Fiskeri og Infrastruktur, og 4.3 Konsulentselskap. Analysekapittelet 5.0 har vi strukturert etter de tre forskningsspørsmålene. I første delkapittel gjør vi rede for operasjonelle risikoer som kan oppstå innenfor hver bransje. I andre delkapittel gjør vi rede for ulike styringsmekanismer virksomheter i de ulike bransjene benytter for å drive med operasjonell risikostyring, i tillegg sammenligner vi våre funn med eksisterende litteratur. I siste delkapittel presenterer vi styringsmekanismer som virksomheter bør benytte for å drive med god operasjonell risiko, basert på analysen fra forskningsspørsmål 1 og 2, samt tidligere forskningslitteratur.

3.4 Evaluering av forskningens kvalitet

For å vurdere forskningsmetoden er det nødvendig å evaluere kvaliteten på forskningsresultatet (Jacobsen, 2015). I det følgende vil vi dermed evaluere studiens reliabilitet og validitet. I tillegg vil det bli forklart hvordan vi har forsøkt å redusere potensielle svakheter i utredningen.

3.4.1 Reliabilitet

Reliabilitet er knyttet til nøyaktigheten av undersøkelsens data, hvilke data som brukes, måten det er samlet inn på og hvordan den bearbeides (Johannessen et al., 2016). Det handler om

hvorvidt man kan stole på datamaterialet som er samlet inn og om man vil få samme resultat dersom målingen gjentas (Saunders et al., 2016). Reliabilitet i vår utredning kan ha blitt påvirket av undersøkelsesopplegg, datainnsamling og dataanalyse (Jacobsen, 2015). For å styrke reliabiliteten har vi dermed forsøkt å gi en god beskrivelse av våre metodiske valg og det teoretiske grunnlaget for utredningen. I tillegg har vi valgt å legge ved intervjuguide (vedlegg 2 og 3). Dette for at leseren kan forstå prosessen og dermed gjøre en vurdering av valgene som er blitt tatt. Noe som imidlertid kan ha svekket forskningsprosjektets relabilitet kan ha vært at undersøkelsen er gjennomført innenfor et gitt tidsrom. Det kan ha gjort det utfordrende å tilfredsstille krav til reliabilitet, ettersom vi ikke kan garantere samme funn ved gjentatt undersøkelse på et annet tidspunkt (Johannessen et al., 2016).

Ved å benytte intervjuer som innsamlingsmetode kunne det oppstå bekymringer knyttet til reliabilitet. Ifølge Saunders et al. (2016) kan utfordringer være forsker- og respondentskjevhet, og respondent- og forskningsfeil. *Forskerskjevhet* kunne oppstå ved at vår atferd var med på å påvirke intervjuet. For eksempel kunne en fare være at vi indirekte presenterte egne meninger når spørsmålene ble stilt, noe som kunne påvirke svaret til respondenten. For å hindre dette utarbeidet vi intervjuguider i samarbeid med veileder, og gjennomførte et testintervju i forkant. I tillegg bestemte vi oss for at den ene stilte satte spørsmål fra intervjuguiden, mens den andre stilte oppfølgingsspørsmål og noterte underveis. Dette for at intervjuene skulle ha likt utgangspunkt. Videre har vi *respondentskjevhet* som kunne innebære at respondentens svar og atferd ville være påvirket av forventninger fra omgivelsene. Det kunne for eksempel være forventninger om hva sjefen ville at respondenten skulle svare. Ved hjelp av semistrukturerte intervjuer utarbeidet vi derfor spørsmål som skapte tillit, i tillegg til å stille oppfølgingsspørsmål. Videre presiserte vi i samtykkeskjema at respondenten hadde mulighet til å trekke seg og trengte ikke svare på spørsmål som respondenten var ukomfortabel med. *Respondentfeil* handler om at respondentens atferd påvirkes av indre og ytre faktorer (Saunders et al. 2016). Dette kunne for eksempel være tidspunktet vi gjennomførte intervjuet på. For å unngå dette fikk respondenten velge tidspunkt for intervjuet innenfor et tidsrom på 3 uker. På grunn av Covid-19 ble intervjuene gjennomført over Teams. Dermed var vi klar over at det kunne oppstå respondentfeil, ettersom respondenten ikke fikk velge sted for intervjuet selv. *Forskningsfeil* kunne oppstå på grunn av ulik oppfatning av spørsmål og svar. For å unngå dette gjennomførte vi semistrukturerte intervjuer med satte spørsmål. Ved uklarheter stilte vi oppfølgingsspørsmål for å avdekke usikkerhet (Saunders et al. 2016).

3.4.2 Validitet

Validitet refererer til hensikten av måling og nøyaktighet på analyse, og om funn er generaliserbare (Saunders et al., 2016). Jacobsen (2015) skiller mellom begrepsvaliditet, intern validitet og ekstern validitet.

Begrepsvaliditet handler om hvorvidt det er samsvar mellom generelle fenomener som vi undersøker og måler (Jacobsen, 2015). Som forskere måtte vi finne spørsmål som kunne fungere som indikatorer på de mer teoretiske begrepene. Dette gjorde vi i konkretiseringsprosessen hvor vi undersøkte teoretiske begreper som kunne ha flere betydninger, for eksempel risiko og risikostyring, for å kunne si noe om komplekse begreper som vi ønsket svar på. Vi var imidlertid klar over at det ikke var mulig å oppnå en perfekt operasjonalisering av slike komplekse begreper. Gjennom nøyaktig og kritisk operasjonalisering kunne vi likevel få en tilnærming til begrepene. Dermed var en kritisk holdning underveis i denne prosessen nødvendig for å oppnå god validitet. I tillegg brukte vi tidligere forskningslitteratur for å sikre validitet i resultater vi kom frem til (Jacobsen, 2015).

Intern validitet handler om å finne årsakssammenhenger mellom to variabler (Saunders et al., 2016). Intern validitet omhandler hvorvidt en metode er egnet til å undersøke det den skal undersøke, eller i hvilken grad observasjonene reflekterer de fenomenene man ønsker å vite noe om (Jacobsen, 2015). For å styrke intern validitet forsøkte vi kontinuerlig å gjennomføre prosessvalidering hvor vi under hele forskningsprosjektet har vært kritiske til metoder, funn og tolkninger. Vi har også kontinuerlig stilte spørsmål om hvorvidt det er samsvar mellom virkeligheten og vår beskrivelse av denne virkeligheten (Jacobsen, 2015). Ettersom forskningsprosjektets hensikt var å undersøke operasjonell risikostyring, var det hensiktsmessig å intervjue ansatte som hadde sentrale stillinger innenfor risiko- og virksomhetsstyring. Dette kan dermed anses som en relevant forhåndskilde med nærhet til fenomenet vi undersøkte (Jacobsen, 2015). Intern validitet kan svekkes ved at andre velger ut respondenter. For å unngå dette valgte vi dermed ut respondentene selv. Det kunne imidlertid vært hensiktsmessig å undersøke flere enn en respondent innenfor hver virksomhet, da dette potensielt ville gitt mer valide funn på området vi undersøkte. Dette fordi den enkeltes subjektive mening kan svekke studiens interne validitet.

En fare for den interne validiteten kunne være misforståelser i intervjuer, og derfor var vi bevisst på dette under intervjuene og i behandlingen av datamaterialet. For å hindre

misforståelser stilte vi oppfølgingsspørsmål for å sikre riktig informasjon, i tillegg sendte vi mail for å følge opp ved usikkerhet. En annen fare ved den interne validiteten kunne være at positive effekter som oppstod i perioden egentlig oppstod på grunn av andre hendelser som inntraff på samme tidspunkt. For å sikre intern validitet undersøkte vi derfor om det kunne være andre organisatoriske endringer som var av betydning i virksomhetene den aktuelle tiden. Dette fant vi for eksempel hos Sbanken som var preget av at DnB ville kjøpe opp foretaket. Dermed måtte vi være bevisst på om dette kunne ha effekt på svarene fra respondenten.

Ekstern validitet handler om forskningen kan generaliseres og overføres til andre (Saunders et al., 2016). Vårt mål med forskningsprosjektet har vært å kunne si noe om styringsmekanismer for operasjonell risikostyring. Ved gjennomføring av kvalitativ undersøkelse er det imidlertid sjeldent at man kan generalisere funn, men at man heller utforsker og går i dybden på et fenomen (Jacobsen, 2015). Med utgangspunkt i dette er det dermed mer relevant å snakke om kontekstualisering fremfor generalisering. Derfor vil det være mottaker av informasjonen som avgjør hvorvidt resultatene kan overføres til en annen situasjon eller ikke. For å sikre ekstern validitet har vi gjort en omfattende undersøkelse med et stort utvalg fra ulike virksomheter og bransjer, som danner grunnlag for at forskningsprosjektet kan være verdifullt for andre virksomheter enn kun de vi har undersøkt. Underveis i utvelgelses- og intervjuprosessen har vi også vært klar over at vi kunne miste virksomheter som det kunne være interessant å undersøke. En annen utfordring vi var klar over var at utvalget kunne ha innslag av tilfeldige feil. Imidlertid brukte vi dette til vår fordel, og regnet med en viss usikkerhet og feilmargin (Jacobsen, 2015).

3.5 Etiske hensyn

God forskningspraksis omfatter normer og retningslinjer. Det vil være etiske retningslinjer for forskers atferd i forhold til rettighetene til de som blir påvirket av forskningen eller er involvert i forskningsprosjektet (Saunders et al., 2016). Vår forskning preges av interaksjon og kommunikasjon mellom oss og respondentene. Dermed settes det krav til en relasjon som må overholdes. I forkant av intervjuene satt vi oss derfor inn i retningslinjene av Per Nerdrum fra 1998, som ofte blir trukket frem i kvalitativ samfunnsvitenskapelig litteratur (Johannesen et al., 2016). Per Nedrum (1998) viser til tre hensyn vi som forskere må kjenne til: (1) respondentens rett til selvbestemmelse og autonomi, (2) vår plikt til å respektere respondentens privatliv og (3) vårt ansvar for å unngå skade (Johannesen et al., 2016).

Forskingsprosjektet innfridde kravene til personvernlovgivning og ble vurdert av NSD før oppstart og underveis. I tillegg sikret vi samtykke fra respondentene gjennom et samtykkeskjema, vedlegg 1. På den måten sikret vi at respondentene deltok frivillig i forskningsprosjektet og at det var mulig å trekke seg om respondenten måtte ønske det. I samtykkeskjema informerte vi også om konfidensialitet. Dette var for å sikre enighet tilknyttet data fra deres intervjuer. Samtykkeskjemaene ble gjennomgått og signert av alle respondentene i forkant av intervjuene.

Fra to respondenter fikk vi tilsendt taushetserklæring som vi måtte signere. Dette fordi respondentene skulle dele konfidensiell informasjon under intervjuet, som ikke kunne benyttes i oppgaven. Denne informasjonen ble imidlertid delt med oss for å heve vår forståelse av hvordan risikostyring fungerte i praksis internt i virksomhetene. Ved prosjektets slutt ble datamaterialet som kunne identifisere respondenter, som lydopptak og transkribering slettet. For å overholde respondentenes anonymitet ble også personlig data som alder, kjønn, navn og lignende ikke tatt med i datamaterialet. Dette fant vi nødvendig ettersom vi hadde et mindre utvalg og det var enklere å gjenkjenne respondentene, sammenlignet med et større utvalg (Jacobsen, 2015).

4.0 Empiriske funn

I dette kapittelet vil vi presentere våre empiriske funn som er samlet inn gjennom intervjuer med tolv respondenter fra ulike virksomheter. For å skape en strukturert tilnærming har vi valgt å dele kapittelet inn etter: 4.1 Finansforetak, 4.2 Fiskeri og Infrastruktur, og 4.3 Konsulentselskap. Innledningsvis i hvert delkapittel vil virksomhetene bli presentert. Deretter vil vi presentere funn tilknyttet operasjonell risiko i virksomhetene. Videre vil funn bli presentert med utgangspunkt i Simons (1995b) fire styringssystemer: grensesystem, diagnostisk styringssystem, interaktivt styringssystem og trossystem.

4.1 Finansforetak

Ifølge Finansforetaksloven (2015, §1-3) regnes finansforetak som foretak som driver virksomhet som: bank, kredittforetak, finansieringsforetak, forsikringsforetak, pensjonsforetak og holdningsforetak i finanskonsern. I vår utredning har vi fått tilgang til fem virksomheter innenfor finansforetak, hvor vi har intervjuet én respondent innenfor hver av virksomhetene. Respondentene har alle sentrale stillinger innenfor risikostyring, og blir berørt eller arbeider med operasjonell risiko. I det følgende vil vi presentere virksomhetene: Sbanken, Sparebanken Vest, Sparebanken Sogn & Fjordane, Storebrand og Norges Bank Investment Management (NBIM).

Sbanken ble startet i 2000 som den første rene nettbanken i Norge. Ved utgangen av 2020 hadde Sbanken en forvaltningskapital på 100,7 mrd. kroner og ansatte tilsvarende 334 årsverk (Sbanken, 2021). Sparebanken Vest er den tredje største sparebanken i Norge. Ved utgangen av 2020 hadde foretaket en forvaltningskapital på 221,3 mrd. kroner og ansatte tilsvarende 732 årsverk (Sparebanken Vest, 2021). Sparebanken Sogn & Fjordane er den åttende største sparebanken i Norge. Ved utgangen av 2020 hadde foretaket en forvaltningskapital på 62,661 mrd. kroner og ansatte tilsvarende 276 årsverk (Sparebanken Sogn & Fjordane, 2021). Storebrand er et norsk selskap og en ledende aktør i det nordiske markedet for pensjon, langsiktig sparing og forsikring. Storebrand hadde en forvaltningskapital på 962 mrd. kroner og 1802 årsverk ved utgangen av 2020 (Storebrand, 2021). NBIM er en avdeling i Norges Bank som forvalter Statens Pensjonsfond Utland på oppdrag fra Finansdepartementet, og forvalter verdier for mer enn 10 000 mrd. kroner. NBIM har over 500 ansatte fra 38 nasjoner,

med kontorer i Oslo, London, New York, Singapore og Shanghai (NBIM, 2019; NBIM, u.å.). Foretakene er strengt regulert og må forholde seg til myndigheter og tilsynsorgan. Som følge av finanskrisen i 2008/2009 ble det utarbeidet flere krav og veiledninger for hvordan foretakene skulle arbeide med risikostyring. Vi finner det dermed interessante å undersøke hvordan foretakene driver med operasjonell risikostyring i praksis.

4.1.1 Operasjonell risiko

I dette delkapittelet vil vi presentere empiriske funn for hvordan foretakene definerer operasjonell risiko og hvilke operasjonelle risikoer som kan oppstå i foretakene.

Funn viser at finansforetakene definerer operasjonell risiko tilnærmet likt. Vi velger å presentere Storebrand sin definisjon på operasjonell risiko ettersom den dekker alle aspekter innenfor operasjonell risiko som vi ønsker å ta for oss i vår utredning. Definisjonen er følgende: "Risiko for økonomisk tap som følge av ineffektiv, utilstrekkelig eller sviktende interne prosesser eller systemer, menneskelige feil, eksterne hendelser eller at interne retningslinjer ikke etterleves." Myndigheter og tilsynsorgan har definert ulike kategorier for operasjonell risiko for finansforetakene. Kategoriene er: internt og eksternt bedrageri, ansettelsesvilkår og sikkerhet på arbeidsplassen, kunden, produktene, skade på fysiske eiendeler, avbrudd i drift og systemer, oppgjør, levering og annen transaksjonsbehandling. Respondent 3 fra Sbanken uttrykker at de i tillegg har valgt å integrere compliance risiko innenfor operasjonell risiko. Ifølge respondent 4 fra Sparebanken Vest kan compliance risiko defineres som: "Risikoen for at man pådrar seg regulatoriske sanksjoner, økonomisk tap eller tap av omdømme som følge av manglede etterlevelse av lov og forskrift, andre eventuelle bestemmelser og/eller interne retningslinjer." Brudd på lover og regler kan hindre finansforetakene å nå sine mål, og dermed vil compliance risiko være en operasjonell risiko. Videre blir det uttrykt fra samtlige respondenter at regelverket årlig blir mer omfattende og krevende. Dermed vil endring i regelverket også kunne medføre en compliance risiko i seg selv.

Flere respondenter hevder at operasjonelle risikoer sjeldent har positive effekter, men stort sett mer negative effekter. Likevel påpeker samtlige at i enkelte tilfeller er man nødt til å ta risiko for å oppnå noe, og at operasjonell risiko ikke nødvendigvis kun medfører negative effekter. Risikotaking kan medføre positive effekter som for eksempel høyere avkastning og styrket omdømme. Respondent 6 fra Storebrand uttrykker følgende: "Gjør du ikke noe, så får du heller

ikke til noe. Det er viktig å ha forståelse om at noe kan gå galt og hvis det går galt må det være innenfor et rammeverk for hva som er håndterbart." Ifølge respondent 3 fra Sbanken er det viktig at virksomheter ikke har et "pekefingerregime" for å unngå at operasjonelle risikoer skal oppstå. Dermed hevder respondenten at virksomheter bør legge opp til at ansatte får arbeide med spennende oppgaver som kan gjøre arbeidet mer givende. Dette forutsetter imidlertid at virksomheten har et godt rammeverk på plass, og at virksomheten er flink til å delegere ansvar og myndighet.

4.1.2 Grensesystem

Grensesystemet består av to typer grenser: (1) forretningsgrenser og (2) strategiske grenser. I dette delkapittelet vil vi presentere empiriske funn for hvordan finansforetakene organiserer og definerer ansvarsforhold. Videre vil vi se på hvordan virksomhetene utarbeider risikopolicyer og risikorammeverk, i tillegg til hvilke risikoappetitt som settes for den enkelte virksomhet.

(1) Forretningsgrenser

Organisering og ansvarsforhold

Finansforetakene organiserer virksomheten for styring og kontroll av operasjonell risiko på prinsippet om tre linjer. Storebrand har valgt å kalle de tre linjene for ansvarslinjer. Ifølge respondent 6 fra Storebrand er hensikten med ansvarslinjer at førstelinje har ansvar for risikostyring, mens andrelinje er ansvarlig for at det er en god prosess med styret som har det endelige ansvaret for risikotaking. Dermed hevder respondenten at risikohåndtering blir en mer integrert del av virksomheten. I tillegg er det enklere å snakke med styret om ansvarslinjer, fordi styret er mer opptatt av ansvarsforhold. Respondentene fra Sbanken, Sparebanken Vest, NBIM og Sparebanken Sogn & Fjordane kaller de tre linjene for forsvarslinjer. Respondent 7 fra NBIM beskriver de tre forsvarslinjene på følgende måte:

> *Førstelinje består av de utførende enhetene. Det er her eierskapet både til risiko, hendelser og tiltak ligger. Andrelinje utføres av avdelingen for kontroll og etterlevelse. Det er andrelinje som påser at førstelinje gjennomfører prosesser og kontrollrutiner innenfor fastsatte rammer. Så har man internrevisjon som fungerer som tredje*

> *forsvarslinje, og vurderer kontinuerlig både første- og andrelinjes risikostyring og kontrollrutiner.*

Videre blir det uttrykt fra samtlige respondenter at andre forsvarslinje består av to uavhengige kontrollfunksjoner: *risikostyring* og *compliance (etterlevelse)*. Respondent 3 fra Sbanken uttrykker at funksjonen for risikostyring er ansvarlig for å etablere og vedlikeholde systemer og prosesser. Disse skal underbygge at virksomheten etterlever vedtatte risikostrategier, policyer og rutiner for risiko. Funksjonen utarbeider faste risikorapporter til styret, i tillegg til å rapportere ved brudd på rammer og retningslinjer. Leder for funksjonen for risikostyring er Chief Risk Officer (CRO), som er uavhengig av ledere med ansvar for risikotaking. Vedkommende deltar ikke i beslutninger som direkte relaterer seg til områder som overvåkes og rapporteres. CRO rapporterer organisatorisk direkte til daglig leder, men har en rett og en plikt til å direkte rapportere til styret dersom styret ikke får nødvendig informasjon om vesentlige risikoer via ordinær rapportering. Det kan heller ikke gis oppsigelse til CRO uten styrets samtykke. Videre forteller respondenten at Chief Compliance Officer (CCO) leder den andre delen av andre forsvarslinje som er funksjon for compliance. Funksjonen er administrativt underlagt daglig leder, men er i sitt arbeid også uavhengig av foretakets ledelse, og øvrige stabs- og kontroll funksjoner. CCO gjennomfører kontroller av etterlevelse av regler basert på styrets instrukser og rapporterer til styret om forhold av art. Respondentene fra Sparebanken Vest og Storebrand beskriver CRO og CCO på en tilnærmet lik måte. Respondent 5 fra Sparebanken Sogn & Fjordane uttrykker at de derimot ikke har et tydelig skille mellom CRO og CCO. Sparebanken Sogn & Fjordane er et mindre finansforetak med forvaltningskapital på omtrent 60 mrd. kroner. Respondenten påpeker at foretak med over 100 mrd. kroner i forvaltningskapital må ha et tydelig skille, og definerte roller mellom risikostyring og etterlevelsesfunksjonen. Ettersom Sparebanken Sogn & Fjordane har forvaltningskapital på 60 mrd. kroner, kan det være en av årsakene til at foretaket ikke har et like tydelig skille.

Videre viser samtlige av foretakene til tredje forsvarslinje som er en uavhengig internrevisorfunksjon. Respondent 3 fra Sbanken uttrykker: "Tredje forsvarslinje er på en måte en uavhengig etterkontroll, typisk ledet av en internrevisor." Videre uttrykker respondent 4 fra NBIM at internrevisor undersøker førstelinje for å se hva som er blitt gjort og hva som eventuelt skal forbedres. Ifølge respondent 4 fra Sparebanken Vest er internrevisjonens rolle å overvåke bankens samlede risiko-/kapitalstyring og internkontroll på vegne av styret, i

tillegg skal internrevisor etterprøve om rutiner og retningslinjer etterleves. Videre uttrykker respondentene at foretakene også må ha en ekstern revisor, som flere plasserer i fjerde linje. Ifølge respondent 8 fra Storebrand er det ekstern revisor som avgir revisjonsberetning i forbindelse med årsregnskapet og foretar en begrenset revisjon av kvartalsregnskapene.

Samtlige respondenter uttrykker at deres foretak har etablert *risikoutvalg* og *risikokomiteer*. Respondent 5 fra Sparebanken Sogn & Fjordane referer til finansforetaksloven som setter flere krav til hvordan finansforetakene skal organiseres. Ifølge Finansforetaksloven §13-6 fjerde ledd skal:

> *Styret skal overvåke og styre finansforetakets samlede risiko og jevnlig vurdere om finansforetakets styrings- og kontrollordninger er tilpasset risikonivå og omfang av virksomheten. Foretaket skal ha et risikoutvalg oppnevnt av styret som skal forberede styrebehandlingen. Bare styremedlemmer som ikke inngår i den faktiske ledelsen av virksomheten kan være medlem av risikoutvalget. Departementet kan i forskrift eller enkeltvedtak gjøre unntak fra plikten til å ha risikoutvalg.*

Respondent 3 fra Sbanken uttrykker at de har et risiko- og complianceutvalg som består av tre medlemmer av selskapets styre og dette utvalget er underutvalget til styret. I tillegg til utvalgets medlemmer møter leder for finans, risikostyring og compliance fast i disse møtene. Utvalget skal sørge for at risiko- og kapitalstyring i konsernet støtter opp under konsernets strategiske utvikling og måloppnåelse. I tillegg til å sikre finansiell stabilitet og forsvarlig forvaltning av eiendelene. Videre uttrykker respondenten at de har fire komiteer som er rådgivende komiteer for administrerende direktør. En av komiteene er risiko- og compliance komiteen hvor operasjonell risiko står i høysete. Det blir også uttrykt fra respondent 4 fra Sparebanken Vest at de har etablert risikoutvalg som bidra til at risiko- og kapitalstyring i konsernet støtter opp under strategisk utvikling og måloppnåelse i konsernet. I tillegg til å sikre finansiell stabilitet og forsvarlig formuesforvaltning. Videre uttrykker respondenten at de også har risikokomiteer som bistår med oppfølging og kontroll innenfor sentrale fagområder. Respondent 6 fra Storebrand uttrykker at de også har risikoutvalg og risikokomité:

> *Risikoutvalgets hovedoppgave å forbedre styrebehandlingen på risikoområdet. Utvalget skal bidra med framoverskuende beslutningsstøtte knyttet til styrets drøfting av virksomhetens risikotaking, finansielle prognoser og behandling av*

> *risikorapporteringen […] Risikokomité er et utsnitt av ledelsen i konsernledelsen, og CRO.*

Videre fremkommer det fra samtlige respondenter at de har revisjonsutvalg. Ifølge respondent 4 fra Sparebanken Vest skal revisjonsutvalget se til at Sparebanken Vest har en uavhengig og effektiv ekstern- og internrevisjon, samt regnskaps- og risikorapportering i samsvar med lover og forskrifter.

Risikopolicy

Respondent 4 fra Sparebanken Vest uttrykker at strategi er overordnet hvor man definerer ulike roller og ansvar i virksomheten, mens policyene går mer i dybden på ulike områder. Ifølge respondentene har foretakene policyer for operasjonell risiko. Policyene omhandler hvordan ansatte skal arbeide og håndtere risiko, og alle ledere er pliktig til å opplyse alle ansatte om policyene. På den måten mener respondent 4 fra Sparebanken Vest at policyene blir styrende i virksomheten.

Respondent 7 fra NBIM hevder at når virksomheter skal utforme generelle risikopolicyer for at risiko skal bli styrt helhetlig er det viktig at man starter på toppen med styret:

> *Styret må sette prinsipper som er typisk for risikostyring og som dekker all type risikostyring inkludert operasjonell risikostyring. Deretter går det delegasjon ned til CEO som har ulike policyer. CRO eller CCO har ikke policyer, men guidelines som er mer detaljert. Videre har man mer detaljerte guidelines på typisk fagnivå, og da går man konkret til verks med hva og hvordan ting bør gjøres, og dette er mer relatert til avdelingsledernivå. Til slutt er man nede på arbeidsledernivå som er prosedyrer.*

Respondent 7 fra NBIM uttrykker at dette viser nivået fra prinsipper til policyer, til guidelines til prosedyrer. Dette hevder respondenten blir mer detaljert til lenger ned man kommer. I tillegg viser samtlige respondenter at finanstilsynets modul for operasjonell risiko fungerer som en veiledning for operasjonell risiko i foretakene.

Ifølge respondent 6 fra Storebrand bruker de ikke ordet policy, men retningslinjer for flere nivåer som skal tilpasses den risikoen den skal håndtere. Derfor er Storebrand opptatt av å beskrive hva som er risiko og formulere hva som er betydningen av risikoen. Videre er de opptatt av å definere hvem som er risikoeier, risikokontroller og kontrollfunksjonen.

Respondenten uttrykker at dette sier noe om rapportering og beskrivelse av risikoen, og dette blir fastsatt av styret og vil være gjeldende for alle ledere i virksomheten.

Risikorammeverk

Det finnes en rekke prinsippbaserte rammeverk som skal hjelpe ledelsen i utforming og implementering av helhetlig risikostyring. De mest brukte og anerkjente rammeverkene kommer fra de internasjonale standardene, ISO og COSO. Respondent 4 fra Sparebanken Vest uttrykker at disse rammeverkene er et relativt nytt felt. Sparebanken Sogn & Fjordane benytter ikke COSO eller ISO, men bruker likevel mye av tankegangen. I Sparebanken Vest baserer de seg på COSO i utarbeidelsen av sitt eget interne rammeverk. Videre hevder respondent 7 fra NBIM at standardene er et fint utgangspunkt i utarbeidelsen av egne interne rammeverk, men at de fort kan bli byråkratiske. Respondenten uttrykker:

> *Det er viktig at man tilpasser standardene til virksomheten, og man må ha i bakhodet at dette må gjøres i praksis ved at det knyttes til arbeidsprosessene det er snakk om. […] Det er ikke det at standardene ikke er nyttig, men at man må prøve å trekke ut det som er mest relevant og nyttig for den standarden. Hvis man ønsker å gjøre ting på andre måter, må man argumentere for det.*

Respondent 5 fra Sparebanken Sogn & Fjordane uttrykker at finanstilsynets modul for operasjonell risiko er mer førende enn standardene i seg selv. Det blir også uttrykt av respondent 3 fra Sbanken at rammeverket for hvordan de skal styre operasjonell risiko er mer nedfelt i finanstilsynets veiledninger.

(2) Strategiske grenser

Etablering av strategiske grenser vil være sentralt for at virksomhetens aktiviteter og beslutninger skal samsvare med virksomhetens strategi. Samtlige respondenter utrykker at de har strategi for risiko. Respondent 6 fra Storebrand uttrykker at risikoappetitt er integrert i strategi for risiko og setter føring, mål og rammer. Ifølge respondent 5 fra Sparebanken Sogn & Fjordane forteller risikoappetitt noe om hvor mye risiko banken ønsker å ta. Respondenten hevder at kapitaldekning også er viktig fordi den er med på å styre og påvirke mulighetene banken har for vekst av risikoappetitt. Videre blir det uttrykt:

> *Man bør legge opp en risikoprofil og den er i mitt hode de faktiske eksponeringene som banken har. Appetitten sier noe om hvor mye eksponering vi ønsker å ta. Deretter skal eksponeringen samsvare med appetitten, at vi ikke skal ta mer risiko enn det appetitten sier vi skal ta. Videre blir det styrt av risikorammene. Dermed må banken sette risikorammer som tillater eksponering i tråd med risikoappetitten.*

Ifølge respondent 3 fra Sbanken skal styret fastsette risikoappetitt for hver risikokategori i virksomheten, og beslutte retningslinjer som operasjonaliserer risikoappetitten til virksomheten. Respondenten uttrykker:

> *Andrelinje skal opplyse styret om hva som er fornuftig risikotoleranse som de kan beslutte, og da må andrelinje operasjonalisere denne risikoen gjennom en risikopolicy over i en retningslinje som førstelinje kan forholde seg til.*

Respondenten hevder at man på den måten lager en ytre ramme som førstelinje må forholde seg til. Deretter er det andrelinje sitt ansvar å påse at førstelinje tar risiko innenfor toleransenivået. Videre utrykker respondenten at Sbanken har et lavt toleransenivå på operasjonell risiko. Respondenten viser til et eksempel på avbrudd i drift og systemer: "Hvis ikke kundene får tilgang til Sbanken sine sider, bank eller mobilbank får ikke de ansatte i Sbanken mulighet til å hjelpe kundene. Dette kan være et stort tapspotensial for oss, hvor vi kan miste kunder. Derfor har vi lav toleranse."

4.1.3 Diagnostisk styringssystem

I dette delkapittelet vil vi presentere empiriske funn for hvordan finansforetak benytter risikoverktøy og hendelsesdatabase. Videre vil vi å se på andre metoder for kvantifisering av operasjonell risiko. I tillegg til ICAAP og beregning av kapitalbehov.

Ifølge respondent 7 fra NBIM, er kjernen i rammeverket for operasjonell risikostyring arbeidet med å identifisere, vurdere og håndtere operasjonell risiko. Samtlige respondenter uttrykker at de gjennomfører løpende identifisering av risikoer i hele virksomheten. Basert på dette forsøker man å identifisere enkeltstående hendelser som kan inntreffe, og anslå et iboende risikonivå for hver enkeltstående uønsket hendelse. For å vurdere identifiserte risikoer uttrykker samtlige respondenter at de benytter risikomatrise som hovedverktøy, hvor foretaket vurderer sannsynlighet (y-aksen) og konsekvens (x-aksen). Deretter besvares det noen

spørsmål på sannsynlighet og konsekvens, og man får en score for hver enkelt risiko. Respondent 4 fra Sparebanken Vest uttrykker at hvis scoren er medium eller høy skal tiltak iverksettes. Respondenten hevder at dette imidlertid bør baseres på en helthetlig vurdering. Det fremkommer fra respondent 3 fra Sbanken at når det skal lanseres et nytt produkt, benytter Sbanken en risikomatrise:

> *Vi ønsker å se på hva som kan skje og hvilke sannsynlighet og konsekvens produktet kan medføre. Om den er grønn, gul eller rød avhenger om vi aksepterer risikoen eller ikke. Dette skal også samsvarer med banken sitt toleransenivå.*

Ifølge respondent 7 fra NBIM tar foretaket hensyn til toleransenivå for operasjonell risiko. Respondenten uttrykker:

> *Vi har definert tre typer operasjonell risiko på høyeste nivå. To er relaterte til risikofaktorer som er en stokastisk variabel med sannsynlighet og konsekvens. Konsekvens er gjort enkelt hvor det er satt grenser for finansielt- og omdømmetap. På den måten har styret tatt stilling til risikofaktornivå med hva som skal være rød, gule og grønne risikofaktorer, ved 5x5 matrise. Den siste handler om den totale finansielle eksponeringen hvor vi ser på et femårs perspektiv. Med utgangspunkt i risikofaktorene ønsker vi ikke at det skal være mer enn 20 prosent sannsynlighet for tap på mer enn 750 millioner operasjonelt i løpet av 1 år.*

Respondenten hevder at dette i praksis betyr at foretaket har tatt stilling til akseptgrenser på risikofaktorer og totalt på styrenivå. Videre påpeker respondenten at det er viktig å undersøke hvilke risikoreduserende tiltak som allerede er blitt etablert for risikofaktorer. Hvis en enkel risikofaktor eller det totale risikonivået ligger utenfor risikotoleransen satt av hovedstyret, må ytterligere tiltak iverksettes for å redusere risikoen. I tillegg hevder respondenten at det er viktig at den enkelte risikofaktor er konkret, slik at det på den måten er mulig å iverksette tiltak og relatere tidligere hendelse til den enkelte risikofaktor.

Samtlige av respondentene uttrykker at operasjonelle hendelser og tap blir registrert i en hendelsesdatabase i virksomheten. Videre hevder respondentene at foretakene iverksetter tiltak på bakgrunn av hendelser som er blitt registret i hendelsesdatabasen, i tillegg til løpende risikovurdering. Ifølge respondent 5 fra Sparebanken Sogn & Fjordane blir operasjonelle hendelser og tap periodisk gjennomgått for å avdekke vesentlige eller systematiske feil, samt

for å identifisere forbedringsområder. Videre uttrykker respondent 3 fra Sbanken at foretaket registrerer operasjonelle hendelser gjennom hele året og at dette følges opp gjennom hendelsesdatabasen i foretaket. Formålet er å sikre læring og begrense fremtidig operasjonell risiko. I tillegg hevder samtlige at ved å benytte hendelsesdatabase bidrar det til kontinuerlig rapportering til styret.

Respondent 4 fra Sparebanken Vest utrykker at i tillegg til hendelsesdatabasen, benytter de risikoindikatorer når de måler operasjonell risiko. Respondenten viser at dette for eksempel kan være driftsstabilitet, informasjonssikkerhet og kundeklager. Samtlige av respondentene viser også til slike eksempler. Videre uttrykker respondent 4 fra Sparebanken Vest at banken sjeldent benytter KPI, budsjett eller regnskap for å måle operasjonell risiko. Respondent 6 fra Storebrand hevder at en viktig del av risikostyring hos dem er å koble risiko til evnen om å nå mål. Respondenten uttrykker: "Det som binder styring og risikostyring sammen er mål. Alle er på jobb for å nå mål. Vi har ulike mål og derfor må risikostyring kobles til målene. Særlig på operasjonelle risikoer."

Finansforetakene er pliktig til å årlig gjennomføre en Internal Capital Adequacy Assessment Process (ICAAP). Det er en intern kapitalvurderingsprosess som gjennomføres for å ta stilling til foretakets kapitalbehov og det er tilsynsmyndighetene som evaluerer ICAAP. Hvis det oppstår mangelfull etterlevelse av regelverket kan Finanstilsynet fastsette individuelle kapitalkrav, kreve redusert risikonivå eller kreve forbedret styring og kontroll. Resultatet fra ICAAP brukes til å vurdere om det er behov for å justere den finansielle planen eller om det må spesifiseres tiltak for å motvirke risikomomenter som er blitt belyst i ICAAP.

Ifølge respondentene vil man i vurdering av samlet kapitalbehov ta hensyn til alle relevante risikoer foretaket er eksponert for. Kapitalbehovet for operasjonell risiko kan beregnes ved: (1) basismetoden, (2) sjablongmetoden eller (3) advanced measurement approach (AMA-metode). De ulike beregningsgrunnlagene er et risikovektet mål på foretakets eksponering for operasjonell risiko. Samtlige av respondentene hevder at basismetoden kan benyttes av alle foretak. Respondent 6 fra Storebrand og respondent 5 fra Sparebanken Sogn & Fjordane uttrykker at foretakene benytter basismetoden for å sette av kapital til operasjonell risiko. Minimumskravet til ansvarlig kapital for operasjonell risiko er i henhold til basismetoden i CRR/CRD IV-forskriften på 15 prosent av gjennomsnittlig inntekt for forretningsområdene de siste 3 årene. Ifølge respondent 5 fra Sparebanken Sogn & Fjordane benyttes den avsatte kapitalen som et utgangspunkt for toleransenivået som virksomheten setter for operasjonell

risiko. Respondent 3 fra Sbanken og respondent 4 fra Sparebanken Vest uttrykker at foretakene derimot benytter sjablongmetoden for å sette av kapital til operasjonell risiko. Sjablongmetoden stiller krav til foretakets styring og kontroll av operasjonell risiko, og overgang til å ta i bruk sjablongmetoden må varsles til Finanstilsynet. Sjablongsmetoden multipliserer hver gruppe med individuelle faktorer. De ulike gruppene har definerte faktorer, enten 12%, 15% eller 18%, og avhenger av ulike inntektstyper.

4.1.4 Interaktivt styringssystem

Ifølge respondent 6 fra Storebrand er kommunikasjon noe av det viktigste virksomheter gjør når det kommer til risikostyring. Respondenten uttrykker: "Hvis man lykkes med det får man frem at man spiller på lag." Videre mener respondenten at risiko er en fin måte å diskutere og kommunisere mellom første- og andrelinje, ettersom det er viktig å ha en felles enighet om hva som kan gå galt, hvor ofte og om det har gått galt før. Respondent 3 fra Sbanken forteller også om kommunikasjon mellom første- og andrelinje:

> *I forkant av ICAPP snakker vi i andrelinje med førstelinje om hvilke forretningsplaner vi ønsker å spille opp til styret, hvilke vekstambisjoner vi har og hva disse ambisjonene krever. Deretter spør vi førstelinje hva de tenker om det og hva de er komfortabel med.*

Videre uttrykker respondenten at de har workshop med styret hvor tanker fremlegges, samt hva som er blitt diskutert mellom linjene. Respondent 4 fra Sparebanken Vest forteller at banken gjennomfører workshop hvor alle ansatte inviteres til å delta. Respondenten uttrykker at det alltid inviterer med to ledere i virksomheten, som sier noen ord om hvordan de arbeider med operasjonell risikostyring. Respondenten uttrykker: "Det hjelper at ansatte hører fra ledere og ikke bare oss i andrelinje." Ifølge respondenten er fordelen med å benytte workshop at ansatte lærer og blir informert om operasjonelle risikoer i foretaket, og formidler det videre til sine kollegaer. Respondenten hevder at de har merket stor effekt på ansattes bevisstgjøring ved å gjennomføre workshop.

Videre uttrykker respondent 6 fra Storebrand at de også gjennomfører workshop, i tillegg til møter for gjennomgang av risiko. Respondenten hevder imidlertid at møter for gjennomgang av risiko er bedre enn workshop. En av grunnene til dette, er at tiden ledergruppen setter av til risikoworkshop et par ganger i året kun brukes til oppsummering av sist gjennomgang. Dermed hevder respondenten at ved operasjonell risiko vil innhenting av data fungere bedre med intervjubasert metode ved én til én gjennomgang og én til ledergruppen, og dermed ikke

én til mange. Videre uttrykker flere av respondentene at risiko blir informert gjennom ulike kanaler hvor man deler saker og hendelser som har oppstått i virksomhetene.

4.1.5 Trossystem

Ifølge respondent 6 fra Storebrand er risikokultur det som kjennetegner dem. Videre uttrykker respondenten: "Risikokultur omhandler de som tar risiko og det handler om å gjøre det som er best for virksomheten og kundene. I tillegg handler det om å etterleve lover og regler." Samtlige av respondentene hevder at risikokulturen i deres virksomhet har blitt betydelig bedre de siste årene. For å bygge en god risikokultur hevder flere at det er viktig med åpenhet og læring av feil. Respondent 4 fra Sparebanken Vest hevder at banken er opptatt av åpenhet og har en kultur for å lære av feil. Et eksempel på en klassisk operasjonell hendelse skjedde i februar 2021 i Sparebanken Vest, hvor en ansatt sendte ut en SMS om én kunde sitt lån til 4000 andre kunder. Ifølge respondenten medførte hendelsen at banken i ettertid var mer opptatt av å lære av hendelsen, enn å peke på den ansvarlige.

Videre påpeker flere av respondentene at foretakene har målsetting om å skape en sunn og god risikokultur. Respondent 3 fra Sbanken uttrykker at de ønsker å ha en sunn risikokultur basert på åpenhet, transparens og kompetanse, og at de stadig utfordre sine metoder, prosesser og rutiner for å forbedre seg. Respondent 5 fra Sparebanken Sogn & Fjordane uttrykker at de har målsetting om en god bedriftskultur. Ifølge respondenten kjennetegnes en god bedriftskultur ved kunnskap om risikostyring og forståelse av hvilke risikoer som er drivere for banken sin inntjening. På den måten handler det om å integrere risikokultur som en del av bedriftskulturen. Dette blir også påpekt av flere respondenter.

4.2 Fiskeri og infrastruktur

I vår utredning har vi fått tilgang til fire virksomheter og et direktorat innenfor fiskeri og infrastruktur, hvor vi har intervjuet én respondent innenfor hver. Respondentene har alle sentrale stillinger innenfor virksomhetsstyring, og blir berørt eller arbeider med operasjonell risiko. I det følgende vil vi presentere virksomhetene: Bremnes Seashore, BKK, Ruter og Nye Veier. I tillegg vil vi presentere Fiskeridirektoratet som er underlagt Næring- og Fiskeridepartementet.

Innenfor fiskeri har vi valgt å undersøke Bremnes Seashore og Fiskeridepartementet. Sjømatnæringen i Norge er kjennetegnet av lange tradisjoner og er blant de viktigste næringene i landet. Historisk har lønnsomheten variert, men i nyere tid har sjømatselskaper opplevd stor vekst. Sjømatnæringen er Norges tredje største eksportnæring, etter olje-/gass- og metallindustrien (Seashore, u.å.). Vi finner det derfor interessant å undersøke Bremnes Seashore som er en av Norges ledende leverandører av oppdrettslaks. Fiskeridirektoratet har ansvar for fiskeri- og havbruksforvaltningen i Norge. Direktoratet er offentlig eid, og fungerer som et rådgivende og utøvende organ for Nærings- og Fiskeridepartementet. Det er interessant å inkludere Fiskeridirektoratet i vår utredning fordi direktoratet skal sikre rammevilkår for lønnsom og bærekraftig fiskeri- og havbruksnæring, samt maritimt basert næringsliv (Fiskeridirektoratet (u.å.). Dermed vil deres arbeid og retningslinjer påvirke fiskerinæringen, og derav Bremnes Seashore. Det er i tillegg interessant å undersøke risikostyring i et offentlig organ, og hvilke krav og retningslinjer de må forholde seg til.

Infrastruktur er den underliggende strukturen som trengs for å få samfunnet til å fungere effektivt, der bygging og vedlikehold av infrastruktur krever store ressurser. Ofte har infrastruktur stor betydning for helse og miljø, noe som gjør at bransjen er strengt regulert og det er et kontinuerlig fokus på risikostyring. Det er derfor interessant å undersøke virksomhetene BKK, Ruter og Nye Veier som er innenfor denne bransjen. BKK er det største energiselskapet på Vestlandet og en av Norges største distributør av elektrisk energi. BKK eies av Statskraft, Bergen kommune og 16 andre kommuner på Vestlandet (BKK u.å.). Administrasjonsselskapet Ruter eies av Oslo kommune (60%) og Viken fylkeskommune (40%). Alle offentlige tilskudd til kollektivtrafikken i Oslo og Viken, unntatt statlig tilskudd til NSB, skal kanaliseres gjennom Ruter. Selskapet eier imidlertid ingen transportmidler selv. Dette utføres av ulike operatørselskap som kjører på kontrakt for Ruter (Ruter u.å.). I motsetning til Ruter som er ansvarlig for kollektivtrafikken, er det Nye Veier som skal planlegge, bygge, drifte og vedlikeholde trafikksikre hovedveier. Nye Veier ble opprettet i 2016 og er et heleid statlig aksjeselskap med et styre utpekt av Samferdselsdepartementet (Nye Veier, u.å.).

4.2.1 Operasjonell risiko

I dette delkapittelet vil vi presentere empiriske funn for operasjonelle risikoer som oppstår i virksomhetene. I tillegg ønsker vi å se på hvordan Fiskeridirektoratet driver med operasjonelt arbeid.

Nye Veier blir eksponert for ulike operasjonelle risikoer gjennom anbudsprosesser og utbyggingsaktiviteter. Respondent 10 fra Nye Veier uttrykker at operasjonelle risikoer kan omhandle alt som har med fremdrift i prosjekter, HMS, samfunnsansvar og seriøsitet. Videre uttrykker respondenten:

> *I vårt arbeid med risikostyring har vi fokus på risiko helt fra starten av når vi skal finne leverandører. Da kvalifiserer vi leverandører ved å sjekke om de har risikostyringssystemer, og på den måten kan vi se om de er i stand til å håndtere risikoene i prosjektet. […] Så har vi risiko internt, hvor vi hele tiden er ute etter hva som er risikoene og mulighetene i prosjektene vi gjennomfører. Det handler om å ha kontroll på kvalitet, HMS og hele tiden ha kontroll over de store risikoene i prosjektene.*

Ifølge respondent 12 fra BKK oppstår ofte operasjonelle risikoer ute i felt, ved uønskede hendelser tilknyttet farlige forhold i forbindelse med arbeidsoperasjoner. Videre uttrykker respondenten at informasjonssikkerhet også er en viktig del av deres arbeid ettersom de sitter på mye informasjon om sine kunder. BKK har sensorer i alle hus som går på strømforbruk, og håndtering av denne informasjon er derfor strengt regulert. Ifølge respondent 9 fra Bremnes Seashore kan det oppstå utforutsette hendelser på sjøen og den mest sentrale interne risikoen er i hovedsak personskade. I tillegg er Bremnes Seashore opptatt av omdømme og hvilket bilde samfunnet har på bransjen. Respondenten uttrykker: "Det er en risiko vi tar på høyeste alvorlig. Vi jobber aktivt med omdømme og vurderer alt opp mot omdømme." I Ruter kan operasjonelle risikoer være trengsel ombord, ruteendring eller tilfredshet med kollektivtilbudet. Respondent 11 i Ruter uttrykker: "Hvis vi bommer på behovet for kundene kan det redusere tilfredshet." Videre hevder respondenten at også Covid-19 er en sentral operasjonell risiko hovedsakelig på grunn av smittefrykt. I tillegg kan tilbudet bli påvirket om eierne ikke bidrar med finansiering.

Fiskeridirektoratet skal sikre at virksomheter tar hensyn til næringsinteresser og miljø gjennom operasjonelt arbeid med havressursforvaltning som består av regulering og kontroll.

Respondent 8 fra Fiskeridirektoratet mener at de har god fiskerikontroll ut mot næringene, men at direktorat ikke er like god på kontroll internt i direktoratet.

4.2.2 Grensesystem

Grensesystemet består av to typer grenser: (1) forretningsgrenser og (2) strategiske grenser. I dette delkapittelet vil vi presentere empiriske funn for hvordan fiskeri og infrastruktur organiserer og definerer ansvarsforhold. Videre vil vi se på hvordan virksomhetene og direktoratet utarbeider risikopolicyer og risikorammeverk, i tillegg til hvilke risikoappetitt som settes for hver enkelt virksomhet og direktorat.

(1) Forretningsgrenser

Organisering og ansvarsforhold

Respondent 8 fra Fiskeridirektoratet uttrykker at på operativt nivå har de etablert to grupper som jobber på tvers av regionene med risikostyring, som har fokus på vurdering, håndtering og risikoreduserende tiltak. I tillegg har de ressurser utenom som følger opp de tiltakene som blir anbefalt fra gruppene. Regjeringen valgte i 2020 å bevilge mer ressurser til Fiskeridirektoratet for å heve kompetansen og kapasiteten. Respondenten uttrykker:

> *Når vi utvikler risikostyringsmodeller har vi i utgangspunktet ikke ressurser som har kompetanse på det. Dermed har det vært en selvlært tilnærming. Tanken er derfor at vi nå skal rekruttere på hovedkontoret og i regionen, for å styrke kompetansen på risikostyring.*

Videre hevder respondenten at risikostyring er et fagfelt i seg selv og derfor vil direktoratet styrke formalkompetansen, slik at det blir tatt riktige valg når det utvikles modeller for fiskerikontroll. Ifølge respondent 11 fra Ruter har de et miljø for virksomhetsstyring og er i startfasen av etablering for et miljø for risikostyring. Ruter etablerte nylig en ny rolle som skal ha hovedansvar for risikostyring og internkontroll. Respondenten hevder at formålet med dette er å integrere helhetlig risikostyring som en del av virksomhetsstyringen.

Respondent 10 fra Nye Veier uttrykker at de har en fagansvarlig for risikostyring i virksomheten. Vedkommende er ansvarlig for utvikling av metoder for risikostyring, rapportere til CFO, støtte med KPI, følge opp prosjekter, samt gjennomføring av internkontroll utover risikorutiner. Videre har hvert prosjekt egne prosjektsjefer som har ansvar for å se til at prosjektene håndterer risiko og at status på dette kontinuerlig blir rapport opp til ledergruppen.

I tillegg har virksomheten sentrale roller, HR og HMS, som også har ansvar for å følge opp prosjektene. I 2016 opprettet styret i Nye Veier et revisjonsutvalg som er et saksforbedrende organ for styret. Revisjonsutvalget skal støtte styret i utøvelsen av sitt ansvar innenfor risikostyring, internkontroll og etterlevelse av retningslinjer for etikk og samfunnsansvar.

I BKK har de organisert roller og ansvarsforhold etter "de tre forsvarslinjene". Respondent 12 fra BKK uttrykker:

> *Linjeledelsen er førstelinje. Stab, ansvarlig for risiko eller ledelsen finner man i andrelinje, og internrevisjon i tredjelinje. Så har man ekstern revisor som er i fjerdelinje. Ledelsen våker over første- og andrelinje, også har du styret som våker over andre- og tredjelinje. Eierne forholder seg til fjerdelinje.*

I Bremnes Seashore fungerer organiseringen litt på samme måte som "de tre forsvarslinjene". Respondent 9 fra Bremnes Seashore uttrykker: "Hvis man snur på det og det går oppover, fungerer det litt på samme måte. Grunnen er at internansvarlig kontrollerer avdelingene, avdelingene kontrollerer seg selv og så har vi eksterne som kontrollerer oss." Videre uttrykker respondenten at administrerende direktør er øverste ansvarlig for risikostyring i alle ledd i virksomheten. I tillegg forteller respondenten at de har HMS-sjef og internkontroll ansvarlig. Den som er ansvarlig for internkontroll skal følge opp avdelingene, mens den enkelte avdelingsleder skal sørge for at risikovurderinger blir gjennomført i avdelingen. Videre har ansatte ansvar for egen sikkerhet, men også for sine kollegaers sikkerhet. Respondenten hevder: "På den måten går det hele veien fra administrerende og ned, med en del fordreringer ut til de ulike avdelingene."

Risikopolicy

Ruter har utarbeidet policyer for risikostyring og interkontroll. Respondent 11 fra Ruter uttrykker: "Policyene er skrevet ned og banket inn i styret, og dermed blir disse styrende for virksomheten." Dette blir også uttrykt av samtlige respondenter. I BKK har de policyer for risiko, men det er innenfor HMS at policyene er mest velutviklet. I tillegg er BKK en virksomhet med tilgang på mye informasjon. Respondent 12 fra BKK hevder at for å bli bedre på risikostyring er det viktig å systematisere, forstå og bruke denne informasjon i utvikling av policyer. Ifølge respondent 9 fra Bremnes Seashore er policyene bygget opp av flere småelement, i tillegg til overordnende filosofier og verdier som tar høyde for sikkerhet, rømning av fisk, trygg mat og miljø. Videre forteller respondenten at de har et overordnet

dokument som forklarer mer i detalj hvordan de skal arbeide med risikoanalyse, og da spesifikt metodisk.

I Fiskeridirektorat legger det nasjonale strategiske dokumentet føringer for direktoratet. Ifølge respondent 8 fra Fiskeridirektoratet er det i dette dokumentet policyen blir årlig utformet, basert på erfaringer og nye tilnærminger. I Nye Veier har de beslutningspunkter som baserer ser på ulike sjekklister for å tilse at de har kontroll. Respondent 10 fra Nye Veier uttrykker at det er viktig å ha en plan og aksept før man tar en beslutning. I tillegg har Nye Veier retningslinjer for kontraktsform hvor de benytter NS8407 Norsk Standard kontrakt, som omtaler risikoer og risikohåndtering. I tillegg blir det spesifisert når Nye Veier bærer risiko og når entreprenøren bærer risiko.

Risikorammeverk

Fiskeridirektoratet reguleres av økonomiregelverket til staten. Respondent 8 fra Fiskeridirektoratet uttrykker at staten setter føring for hvordan direktoratet skal arbeide med risikostyring. Dermed følger direktoratet ISO31000. Respondent 12 fra BKK hevder at alle virksomheter tar utgangspunkt i ISO bevisst eller ubevisst. Det fremkommer fra respondenten at BKK etterlever ISO, men at de ikke er ISO sertifisert. Nye Veier krever at deres leverandører er ISO9001 sertifisert, som betyr at leverandørene er kvalitetssikret for arbeidet. Ifølge respondent 10 fra Nye Veier er leverandørens forståelse av risiko et viktig element i evaluering, og dermed sikrer Nye Veier seg dette gjennom å kreve sertifisering. Videre følger Nye Veier COSO i sitt arbeid med risikostyring. Dette blir også uttrykket fra respondent 11 fra Ruter. I Bremnes Seashore benytter de seg ikke av ISO eller COSO. Ifølge respondent 8 fra Bremnes Seashore er de pålagt å følge andre standarder. Respondenten uttrykker: "Global Gap er en av de største standardene vi benytter, i tillegg til andre standarder på mattryggheten og bærekraft." Respondenten hevder at når virksomheten skal ut i markedet er det viktig å være sertifisert i henhold til standarder, som igjen blir vurdert av et eksternt selskap.

(2) Strategisk grenser

Ifølge respondent 11 fra Ruter brukes begrepet "risikotoleranse" istedenfor "risikoappetitt". Respondenten uttrykker: "Vi tolerer en type risiko i større eller mindre grad, men vi har ikke appetitt for det." Ruter har tre typer toleranse: lav, medium og høy risikotoleranse, og på operasjonell risiko opererer de med lav toleranse. Respondent 10 fra Nye Veier uttrykker at akseptabelt risikonivå handler om hvor stor risiko Nye Veier skal ta:

> *Det handler om hvor mye forsikring vi skal ha. Vi har byggherrestyrte forsikringer som betyr at vi har forsikringen og ikke entreprenøren. Vi har også garantiforsikring for å sikre at hvis vi går konkurs, så har vi en garanti. Dette er en del av risikotenkingen totalt.*

Fiskeridirektoratet setter årlige rammer for operativt og strategisk arbeid. Ifølge respondent 8 fra Fiskeridirektoratet handler Statens Direktoratregelverk om effektivitet. Respondenten hevder at det derfor ikke handler om lønnsomhet når de arbeider i forvaltning, men om hvordan ressursene skal bli brukt mest mulig effektivt. Ifølge respondent 9 fra Bremnes Seashore må de forholde seg til lovverk fra myndigheter, spesielt mattilsynet og Fiskeridirektoratet. Respondenten uttrykker at det derfor defineres grenser for hva som er akseptabelt og ikke, innenfor personvern, fiskevelferd, trygg mat, ytre miljø, verdier og omdømme. Videre uttrykker respondenten: "Hver ansatt signerer en kontrakt der de erklærer at man har en plikt til å bidra på det helhetlige som går på sikkerhet. Så har vi definert tydelige grenser på det som går på avvik basert på risikoanalyse." Respondent 12 fra BKK påpeker at ettersom de har en monopolrolle er det derfor flere regler de må etterleve. Respondenten uttrykker: "Endringer i reguleringer er noe vi prøver å påvirke, følge med på og ikke minst forstå. For dette kan være risiko i seg selv."

Respondenten 11 fra Ruter uttrykker at innovative miljøer kan oppleve at risikostyring er en hemsko som gjør at man ikke når satte mål. Respondenten hevder at problemet oppstår når man overfører innovasjon til drift hvor det faktisk treffer kunden, fordi compliance risiko kan hindre innovasjon. Dette kan for eksempel være personvern, som kan kvele en del av insentivene. Respondenten uttrykker:

> *Mange mener at risikostyring står som en motpol til innovasjon og utvikling. Jeg mener derimot at risikostyring sørger for at de innovasjonene som vi gjør faktisk lar seg gjennomføre. Grunnen er at vi har identifisert risikoer og justerer dem, så vi klarer å levere.*

Respondenten påpeker at det dermed er viktig å gjøre risikovurderinger selv i et innovasjonsmiljø, ettersom man må kunne forholde seg til blant annet compliance og finansiell risiko. Respondenten mener at virksomheter dermed må sette en høyere toleranse for enkelte risikoer fordi det vil være noen risikoer man må være villig til å ta for å oppnå en ønsket tilstand. På bakgrunn av dette hevder respondenten virksomheter må sette en høyere toleranse for innovasjon.

4.2.3 Diagnostisk styringssystem

I dette delkapittelet vil vi presentere empiriske funn for hvordan fiskeri og infrastruktur benytter risikoverktøy, Sikker jobbanalyse (SJA) og hendelsesdatabase. Videre vil vi presentere Monte Carlo simulering, i tillegg til andre metoder for kvantifisering av operasjonell risiko.

Ifølge respondent 9 fra Bremnes Seashore er virksomheter pålagt å gjennomføre risikoanalyser på grunn av krav fra myndigheter og ulike standarder. Risikomatrise kan benyttes som et verktøy i risikoanalyser. Samtlige respondenter uttrykker at risikomatrise, kalt 5x5 matrise, benyttes for å identifisere og vurdere operasjonelle risikoer. Matrisen baserer seg på tre fargekategorier: rød, gul og grønn. Ved hjelp av matrisen vurderer virksomheter sannsynlighet og konsekvens av risikoer som kan oppstå.

Det blir imidlertid uttrykt av respondent 11 fra Ruter at de i liten grad benytter risikomatrise. Ifølge respondenten har Ruter likevel et mål for 2021 at matrisen skal tas mer i bruk. Hensikten er å avdekke flere risikoer i prosjekter og avdelinger som kan være virksomhetsovergripende. Respondent 8 fra Fiskeridirektoratet uttrykker at på operativt nivå benyttes risikomatrise. Det fremkommer imidlertid at dette arbeidet er krevende fordi man må gjøre en skjønnsmessig vurdering av data og informasjon som kommer ut fra matrisen. Videre viser samtlige respondenter at en utfordringer som oppstår i risikovurderinger er at det blir kategorisert for mange risikoer. Dermed finner flere det utfordrende å synliggjøre risikoer som er viktig. Respondent 10 fra Nye Veier uttrykker:

> *Det som er utfordrende med risikostyring i alle virksomheter er at listen over risikoer blir for lang og du får ikke nok oppmerksomhet på noen av dem [...] Derfor fokuser vi alltid i styringsgruppen på de 10 viktigste risikoene og de som har størst konsekvens hos oss.*

Bremnes Seashore benytter SJA for å vurdere risiko i arbeidsoperasjoner. Ifølge respondent 9 fra Bremnes Seashore er SJA en forhåndsdefinert vurdering som alle ansatte må gjennomføre i forkant av arbeidsoperasjoner. Respondenten uttrykker at de røde og gule momentene fra 5x5 matrisen blir inkludert i SJA. Bakgrunnen er at ansatte skal ha et tydelig fokus på risikobildet av virksomheten. Videre hevder respondenten: "Vi ser at mange virksomheter setter foten ned på risikoer som er røde, men det gjør ikke vi. Grunnen er at vi ønsker en objektiv vurdering

av alle risikoer og derfor ønsker vi ikke å manipulere risikobildet." Respondent 12 fra BKK uttrykker at de også benytter SJA:

> *Når man er ute i felt og arbeider med farlige ting som strøm, stilles det krav til utførelse av SJA. For denne type arbeid er det utarbeidet maler og instrukser, som vi arbeider kontinuerlig og intensivt med. Det må også defineres hvem som er ansvarlig for sikkerheten, både inne på nettsentralen og ute i felt.*

Respondent 10 fra Nye Veier uttrykker at de systematisk følger opp elementer som avdekkes i risikovurderinger. Respondenten forteller at de benytter scenarioanalyser for å predikere hvor det kan gå galt. For å gjøre dette benytter Nye Veier seg av Monte Carlo simulering i risikovurderinger. Monte Carlo simulering blir benyttet for å simulere utfallets sannsynlighet som hver enkelt risiko har for å inntreffe, hvor langt risikoen er på vei og eventuelle konsekvenser risikoen kan medføre. Dette baseres på gjennomført risikomatrise og historisk hendelsesdata. Respondenten hevder at målet er å definere tiltak som gjør at de unngår at risikoen oppstår.

Samtlige respondenter hevder at det er viktig å registrere og føre statistikk over ulike typer hendelser som kan oppstå i virksomheter. Respondent 12 fra BKK uttrykker: "Det blir ført statistikk over ulike typer hendelser og basert på dette kategoriserer vi hvilke som skal ha størst fokus." Ifølge respondenten har BKK et kontinuerlig fokus på prosessforbedring, men virksomheten kan likevel bli bedre på rapportering og læring. Respondent 9 fra Bremnes Seashore uttrykker at hendelser og observasjoner ikke alltid blir registrert. Derfor oppstår det ofte utfordringer knyttet til oppfølging av hendelser i arbeidsoperasjoner. Respondenten forteller: "Våre ansatte er løsningsorienterte. Derfor er de flinke til å løse farer og utfordringer som kan oppstå. De er imidlertid ikke like flinke til å registrere det som har skjedd, noe som gjør at vi ikke får erfaringsutvikling og formidlet det videre."

Videre viser samtlige respondenter at virksomheter benytter måleparameter, som for eksempel KPI for å tilse måloppnåelse. Respondent 10 fra Nye Veier uttrykker at de benytter KPI på innholdet i tilbud og avtaler, for å måle at man er på riktig vei i forhold til den satte risikoutviklingen. Respondent 12 fra BKK forteller at virksomheten har integrert risiko i KPI, og at disse kontinuerlig blir overvåket. Under hver KPI har BKK flere parametere. Dette kan for eksempel være statistikk som gir en indikator på hva som skjer, og dermed kan være en forklaringsvariabel til den KPI-en. Respondent 11 fra Ruter uttrykker at de benytter signaler i

risikovurderinger. Ifølge respondenten kan dette være at det ikke er budsjettert like mye til risikostyringsfunksjonens mål i kommende budsjett.

4.2.4 Interaktivt styringssystem

Ifølge respondent 8 fra Fiskeridirektoratet møtes grupper som arbeider operativt med risikostyring ukentlig for å diskutere risikoer som er blitt identifisert. Respondenten uttrykker: "Vi har forum på ulike nivåer hvor risiko blir diskutert." Det blir også uttrykt fra respondent 11 fra Ruter at de har forum for risikostyring hvor risiko blir diskutert. Videre uttrykker respondent 10 fra Nye Veier at de har etablert "tool-box", som fungerer som et verktøy for å diskutere risiko. Dette er også integrert i ledermøter hvor de viktigste risikoer og deres utvikling blir gjennomgått en gang i måneden. Ifølge respondent 12 fra BKK har de et stort fokus på risiko i morgenmøter for å utarbeide læringsark som blir kommunisert ut. Respondenten hevder dette er viktig ettersom ansatte arbeider ute i felt og er involvert i hendelser.

Respondent 9 fra Bremnes Seashore forteller at de har arbeidet mye med kommunikasjon i virksomheten. De siste årene har de benyttet Workplace på Facebook, etablert et internt kommunikasjonsverktøy og utviklet en egen hendelsesdatabase. Hensikten er at ansatte skal dele erfaringer og lære av tidligere hendelser. Respondenten uttrykker: "Til mer vi kommuniserer fra oss og ut, til bedre blir det." Videre uttrykker flere respondenter at de gjennomfører workshop hvor ansatte blir involvert. Respondent 9 fra Bremnes Seashore hevder at involvering av ansatte er den viktigste faktoren for å lykkes. Virksomheten har merket stor effekt av at ansatte får delta på workshop, ettersom dette muliggjør at ansatte får komme med innspill og ta del i vurderinger.

4.2.5 Trossystem

Ifølge respondent 10 fra Nye Veier er risikokulturen i deres virksomhet god. Respondenten uttrykker:

> *Vi ser på sammenhenger mellom det å ha kontroll på risiko, og det å nå mål og resultater. Vi er vant til å tenke sånn hele tiden så alle prosjektene har fokus på dette. Det handler hele tiden om å vurdere hva er utfallet og hva er sannsynligheten med den beslutningen man tar. Vi har et slikt mindset. Det nytter ikke å bare ha et system, hvis man ikke har et mindset.*

Respondent 9 fra Bremnes Seashore uttrykker at risikokulturen i virksomheten har endret seg de siste syv årene. Tidligere var det mindre fokus på bruk av utstyr, og "skulle bare" mentaliteten var dermed mer fremtredende. De siste årene har Bremnes Seashore arbeidet systematisk og målrettet for å endre den tidligere kulturen. Respondenten hevder at dette har ført til færre ulykker fordi ansatte har blitt flinkere til å benytte utstyr ute i felt. Ifølge respondent 12 fra BKK har de en god risikokultur innenfor HMS, men innenfor økonomi og ytre miljø kan de bli bedre. Videre hevder respondenten: "Innrapportering er et viktig virkemiddel for å skape god risikokultur og at man faktisk gjør noe med det som blir innrapportert. Det er en viktig kulturbjelke og bør komme øverst på agendaen."

Respondent 8 fra Fiskeridirektoratet uttrykker at det tar lang tid å bygge en god risikokultur i direktoratet. I tillegg påpeker respondenten at direktoratet ikke har et like tydelig fokus på arbeidet med risikostyring og dermed er de fremdeles på et utviklingsnivå. Likevel har de et ønske om å gjøre risikotaking mer systematisk for direktoratet som helhet. Respondent 11 fra Ruter hevder at deres risikokultur heller ikke er god nok. Ifølge respondenten er utfordringen at risiko kun er noe man er opptatt av på høyere nivå og at det dermed ikke er blitt forankret i hele virksomheten. Respondenten uttrykker at de derfor arbeider med å bevisstgjøre hele virksomheten slik at det skapes en god risikokultur. Videre uttrykker respondenten: "For å oppnå en god risikokultur må risikovurderinger gjøres hos alle ansatte i virksomheten og ikke bare på et høyere nivå."

4.3 Konsulentselskap

Vi har fått tilgang til to av de største konsulentselskapene i Norge, PwC og EY, hvor vi har intervjuet én respondent innenfor hvert selskap. Respondentene har ekspertise på risikostyring og bistår andre virksomheter med konsulenttjenester innenfor risikostyring og internkontroll. Vi har valgt å inkludere konsulentselskapene i vår utredning for å få et fullstendig og ærlig bilde på hva virksomheter finner utfordrende, og hva de gjør bra.

4.3.1 Operasjonell risiko

I dette delkapittelet vil vi presentere empiriske funn for hvordan konsulentene definerer operasjonell risiko og deres erfaring på hvilke operasjonelle risikoer virksomheter blir

eksponert for. I tillegg vil vi presentere deres syn på operasjonell risiko og risikostyring i virksomheter.

Ifølge respondent 2 fra EY er operasjonell risiko et vidt fagfelt som griper inn på overordnet styring og kontroll, og andre risikoområder. Respondenten definerer operasjonell risiko som følgende:

> *En uønsket hendelse som kan ha økonomisk påvirkning eller påvirkning på omdømme. Den uønskede hendelsen kan oppstå fra et sammenbrudd av interne prosesser, menneskelige feil, systemfeil eller andre hendelser forårsaket av tredjeparter eller andre eksterne faktorer.*

Respondent 1 fra PwC uttrykker at operasjonelle risikoer som virksomheter står overfor avhenger av virksomheters natur. Det omhandler hvilket marked virksomheten operer innenfor, hvilke underleverandører de bruker og hvilke prosesser de driver med. Ifølge respondenten vil industrielle virksomheter ofte være mer eksponert for HMS hendelser, enn i finansforetak hvor ansatte sitter på kontor. Det som er felles for alle virksomheter er risiko forbundet med IT og Cyber-sikkerhet, i tillegg til regulatoriske endringer som for eksempel personvern.

Respondent 1 fra PwC hevder at operasjonell risiko har flere negative effekter enn investerings- og markedsrisiko. Dermed handler operasjonell risiko om å håndtere usikkerhet slik at man med større sannsynlighet klarer å drifte virksomheten på en sikker og god måte fremover. Respondenten uttrykker at hensikten med operasjonell risikostyring er å systematisk identifisere risikoer i hele virksomheten og iverksette risikoreduserende tiltak for å forhindre unødvendig tap. Derfor mener respondenten det er viktig at operasjonell risikostyring er et verktøy for å prioritere ressurser, balansere kostnader tilknyttet risiko og iverksette risikoreduserende aktiviteter.

Ifølge respondent 1 fra PwC har risikostyring kommet høyere på agendaen til styret og toppledelsen de siste årene. Hovedsakelig på grunn av hendelser som blant annet finanskrisen i 2008/2009 og oljeprisfallet i 2014. Videre uttrykker respondenten at Covid-19 også er et godt eksempel på dette: "Svært få selskapet var forberedt på Covid-19 og de man trodde var forberedt har man tidvis opplevd ikke har vært det." Det blir påpekt fra begge respondentene at hendelser som finanskrisen, oljeprisfallet og Covid-19 har ført til at risikostyring, og spesielt operasjonell risikostyring er satt høyere på agendaen.

4.3.2 Grensesystem

Grensesystemet består av to typer grenser: (1) forretningsgrenser og (2) strategiske grenser. I dette delkapittelet vil vi presentere empiriske funn for hvordan konsulentene opplever at virksomheter organiserer og definerer ansvarsforhold. I tillegg til hvordan konsulentene mener virksomheter bør utarbeide risikopolicyer og risikorammeverk, samt hvorfor virksomheter bør sette risikoappetitt.

(1) Forretningsgrenser

Organisering og ansvarsforhold

Respondent 1 fra PwC uttrykker at modellen for "de tre forsvarslinjene" er en standard, og at ikke alle selskaper benytter seg av den direkte. Respondenten påpeker imidlertid at det er prinsippene i den som er viktig:

> *Ofte er det førstelinje som driver aktiviteter ut mot markedet, mens andrelinje støtter og gjør kontrollaktiviteter for å støtte førstelinje. Tredjelinje vurderer hele oppsettet for styret og kalles ofte for internrevisor. Videre har man fjerdelinje som er ekstern revisor og som reviderer for myndighetene.*

Respondenten uttrykker at hva som inngår i første- og andrelinje derimot ikke er et entydig svar på. Det er derfor viktig å se på totaliteten i selskapet, i tillegg til å se på hvordan aktivitetene henger sammen. På bakgrunn av dette hevder respondenten at man bør tegne opp et kart på hva som er første-, andre- og tredjelinje i virksomheten. Ifølge respondent 2 fra EY er modellen for "de tre forsvarslinjene" et godt utgangspunkt for organisering og fordeling av ansvarsroller. Videre hevder respondenten at det er god markedspraksis å bruke modellen for å definere risikoappetitt og ved implementering av dette nedover i virksomheten.

Respondentene uttrykker at hvem som har det overordnede ansvaret for risikostyring i virksomheten avhenger av type virksomhet. Ifølge respondent 1 fra PwC vil det innenfor bank og finans og andre større selskaper ofte være CRO som har det overordnede ansvaret for risikostyring. Respondenten mener at CRO typisk har det overordnede ansvaret for operasjonell risiko ved å gjennomføre analyser og overvåke rammeverk som er satt for operasjonell risikostyring. Videre uttrykker respondenten at virksomheter også kan ha en compliance funksjon, hvor CCO har det overordnende ansvaret for funksjonen. CCO arbeider

ofte mer kvalitativt med prosessorientert risikostyring og skal sørge for etterlevelse av lover og regler. Respondent 2 fra EY uttrykker at CCO også har ansvar for å utarbeide policyer innenfor compliance, som kan ha stor betydning for operasjonelle risikoer virksomheten påtar seg. Det blir imidlertid uttrykt av respondentene at størrelse og kompleksitet på virksomheten vil ha betydning for etablering av CRO og CCO rolle. Videre blir det utrykt av respondent 1 fra PwC at det vil variere om CRO skal plasseres i første- eller andre forsvarslinje:

> *Man har faktiske situasjoner hvor man har operasjonelle risikoressurser også i førstelinje. De har da ofte et mer rådgivende og støttende ansvar opp mot de som sitter i førstelinje, enn kontroll- og etterlevelseansvar. En CRO funksjon kan i en del tilfeller ses på som en førstelinje, mens noen ganger vil det ligge i grensesnittet mellom første og andrelinje. Compliance er derimot en klarere andrelinjefunksjon.*

Respondent 1 fra PwC uttrykker at beveger man seg over på statlig og kommunal sektor opererer man ofte med en funksjon som kalles for virksomhetsstyring. Respondenten hevder at risikostyring ofte legges innenfor denne funksjonen av virksomheten. Deretter har man et spekter imellom, som kan være alt fra industriselskaper til tjenesteleverandører. Respondenten uttrykker: "Der har jeg erfaring med at risikofunksjonen ofte blir lagt under CFO eller økonomiavdelingen."

Risikopolicyer

Respondentene hevder at det er viktig at styret fastsetter overordnende prinsipper for risikostyring. Dette er de øverste kravene som styret mener at virksomheten skal forholde seg til i forhold til styring av risiko. Respondent 1 fra PwC uttrykker:

> *Det bør omfatte alle typer risiko og av den grunn bør prinsippene skrives på et høyt nivå. Videre mener jeg at alle i selskapet bør ha tilgang til alle prinsippene til styret. Så mener jeg at disse prinsippene må være ganske overordnet fordi det skal dekke relativt mye. Rent sånn hensiktsmessig så er det ikke bra at de blir for detaljerte i sine krav, for da blir det vanskelig for virksomheten å forholde seg til dem. I prinsippene bør det også fremgå hva som er grensene for risikoappetitten til styret.*

Videre hevder respondent 2 fra EY at det er viktig å skille policydokument fra rutiner. Ifølge respondenten skal policydokumentet sette de overordnede styringsprinsippene for å sørge for hvordan man skal håndtere operasjonell risiko, og de underliggende rutinene skal operasjonalisere dette. Videre uttrykker respondenten: "På den måten har virksomheten mer

generelle rutine- og prosessbeskrivelser, samt diverse underliggende dokumenter som skal svare på hvordan styringsprinsippene skal implementeres i praksis." Prinsipper, styringsdokumenter, rutiner og hva som er egnet for virksomheten avhenger imidlertid av størrelse og kompleksitet.

Risikorammeverk

Ifølge respondent 1 fra PwC er det to rammeverk for operasjonell risikostyring som er mest anerkjent og brukt i hele verden. Dette er ISO og COSO. Respondent 2 fra EY uttrykker: "COSO er ikke noe vi pleier å henvise til, men likevel vet jeg at mange tar utgangspunkt i standarden når de setter opp rammeverk og tilsvarende." Ifølge respondent 1 fra PwC vil typiske fallgruver ved implementering av rammeverk være at virksomheter tror det skal dekke alle former for risiko, i tillegg til at rammeverket blir for teoretisk. For å unngå slike fallgruver uttrykker respondenten: "Det er viktig å få rammeverket praktisk implementert i prosessene, snakke virksomhetens språk og fokusere på hvordan det skaper verdi. Det er noe av det viktigste i implementering av operasjonell risikostyring." Videre hevder respondenten at det er viktig å få gjort systemer på terminologibruk, samt finne vurderingsskalaer og metoder som er gode for virksomheten. I tillegg er det viktig å få det integrert i rapportering til styret og toppledelsen, slik at det blir gode diskusjoner tilknyttet risiko. På den måten mener respondenten at man får det integrert i virksomhetens prosesser. Respondenten hevder det også er viktig å få det inn i plan- og budsjettprosesser, fordi det er hensiktsmessig å starte med å tegne kommende årshjul for å få på plass et risikostyringsrammeverk.

(2) Strategiske grenser

Respondent 1 fra PwC definerer risikoappetitt som "den risikoeksponeringen som styret mener at selskapet bør jobbe innenfor". Respondent 2 fra EY definerer risikoappetitt som "type og mengde risiko som en virksomhet er villig til å akseptere." Hvilken type risiko som avgjør risikoappetitt vil imidlertid avhenge av bransjen virksomheten operer innenfor. Ifølge respondenten vil risikoappetitt bestå av *risikoevne* og *risikovilje*. Risikoevnen er grensen virksomheten kan tåle og må holde seg innenfor. Risikovilje vil være innenfor risikoevnen igjen. Respondenten uttrykker:

> *Hvis man ser for seg en sirkel med risikoevne ytterst og risikovilje innerst, så skal det være en buffer mellom evne og vilje som skal sørge for at det man styrer etter i praksis er risikovilje. For å operasjonalisere dette er det etablert risikorammer og det vil typisk være måltall eller rammer for hva man skal holde seg innenfor.*

Videre hevder respondenten at det er viktig å etablere tydelig risikoappetitt med tydelige rammer som virksomheten styrer etter i praksis og overvåker løpene. Respondent 1 fra PwC uttrykker at risikoappetitt også bør linkes opp til rapporteringskrav, slik at selskapet nærmer seg appetitten til styret.

Finanstilsynet legger også føringer for operasjonell risiko. Ifølge respondent 2 fra EY er dette føringer på hva som er god praksis opp mot størrelse, kompleksitet og type virksomhet. I tillegg har man risikoevne og regulatorisk krav, for eksempel knyttet til kapitalkrav. Respondent 2 fra EY uttrykker:

> *Da vil man gjerne se risikoevne opp mot kapitalkrav som virksomheten har. Om man skal se på hvordan det skal settes opp bør virksomheten se på betalingsposisjonen først. Dette for å forstå hva virksomheten må ha av kapital og hvordan virksomheten skal holde seg innenfor dette basert på satt risikoevne.*

4.3.3 Diagnostisk styringssystem

I dette delkapittelet vil vi presentere empiriske funn for hvordan konsulentene hevder at virksomheter bør benytte risikoverktøy og hvordan de bør rapportere operasjonell risiko. I tillegg til hvordan finansforetak skal beregne kapitalbehov for operasjonell risiko.

Respondent 2 fra EY uttrykker at ledende markedspraksis for måltall og rammer som man skal holde seg innenfor er å etablere en 5x5 matrise, med rød, gul og grønn sone. Ifølge respondenten er ledende praksis hvis man er i gul sone å predefinere tiltak med tydelige ansvarsforhold. På den måten viser det hva som skal til for å komme tilbake i grønn sone. Er man derimot i rød sone vil man se på andre eskaleringer. Da blir styret informert med en gang og det iverksettes raskere håndtering for å komme tilbake på riktig spor. Videre uttrykker respondenten at det er viktig å finne gode tiltak:

> *Noen ganger kan man si at det risikonivået er akseptabelt og da vil det ikke være behov for tiltak. Andre ganger kan tiltaket være at man skal overvåke risikoen mer fremover, med høyere frekvens enn det man vanligvis ville gjort. I noen situasjoner er man imidlertid nødt til å redusere risikoen og det er det som er krevende.*

Respondent 1 fra PwC uttrykker at en utfordringer som ofte oppstår med matrisen er at skalaen blir for grov. Dermed hevder respondenten at virksomheter kan finne det utfordrerne å sette en eksakt sannsynlighet for at risikoen vil oppstå.

Videre uttrykker respondent 2 fra EY at det er viktig å vise til gode tall i risikorapportering og en forutsetning for å klare dette er å vise til risikomatrise. Respondenten hevder at det er viktig at det ikke bare blir gjengitt nøkkeltall, men at virksomheter også klarer å beskrive vurderinger som er blitt gjort. Ifølge respondent 1 fra PwC bør virksomheter ikke benytte risikomatrise i rapportering, ettersom det kan fremstå uprofesjonelt. Respondenten hevder at god praksis heller vil være å rapportere risikoer i et listeformat hvor risikoer blir definert. Definerte risikoer bør visualiseres med en farget pil som indikerer risikonivået til den enkelte risiko og retning på pilen indikerer forventet utvikling i neste periode, ofte en tolv måneders periode. I tillegg bør det foreligge en refleksjon rundt årsak, hendelse, konsekvens og integrerende tiltak som har blitt etablert.

Respondent 2 fra EY uttrykker at når man kvantifiserer risiko bør man gjennomføre scenarioanalyse for å se hvor galt det kan gå. For å gjøre dette kan virksomheter benytte Monte Carlo simulering. Ifølge respondent 1 fra PwC benytter virksomheter utførte risikovurderinger med sannsynlighet og konsekvens i Monte Carlo simulering. I tillegg benyttes hendelsesdata som virksomheten har opparbeidet seg over tid som input i simuleringen. Respondenten påpeker at input kan variere, basert på hvor mye historisk data virksomheten besitter og hvor god kvaliteten er på risikovurderingene. Imidlertid påpeker respondenten at virksomheter må være relativt modne på risiko før man klarer å utføre en Monte Carlo simulering, og for at det skal gi noe verdi.

I henhold til kapitalkravsforskriften skal finansforetak definere kapitalbehov for operasjonell risiko. Ifølge respondent 2 fra EY er det ulike metoder for beregning av kapitalbehov: basismetoden, sjablongmetoden og AMA-metoden. Basismetoden kan alle foretak benytte. Sjablongmetoden kan foretakene benytte uten å søke til Finanstilsynet, men de må varsle om det. Derimot kan Finanstilsynet nekte for det, så i praksis hevder respondenten man kan si at det blir en søknadsprosess. Det blir uttrykt av respondenten at basismetoden og sjablongmetoden er relativt like, men at hovedforskjellen er at sjablongmetoden deler opp inntektsvariabelen i flere grupper. For å benytte AMA-metoden må foretakene derimot søke om tillatelse. Respondenten hevder at AMA-metoden er en mer avansert metode som fastsettes på bakgrunn av forventet og uventet tap med mindre kredittilsynet bestemmer annet.

4.3.4 Interaktivt styringssystem

Ifølge respondent 2 fra EY er det viktig at risiko kommuniseres og diskuteres i virksomheter. Respondenten hevder at kommunikasjon også er viktig for å få til en god risikokultur. Imidlertid påpeker respondenten at en utfordring som kan oppstå i virksomheter er at førstelinje kun har fokus på effektivitet, og dermed kan det oppstå misnøye hvis andrelinje stopper opp deres arbeid for å gjøre dem oppmerksom på risikoer som kan oppstå. Derfor mener respondenten det er viktig at førstelinje har en åpen holdning til det som kommer fra andrelinje. I tillegg hevder respondenten at et løpende samspill mellom første- og andrelinje er viktig for å redusere usikkerhet tilknyttet risikoer. Dette samspillet vil imidlertid variere mellom virksomheter.

Respondent 1 fra PwC uttrykker at det viktig å etabler ulike forum hvor risiko blir diskutert. Respondenten forteller at i risikoforum møtes relevante personer for å diskutere seg frem til risikobildet som er laget for virksomheten, basert på et utkast som er laget av risikofunksjonen i virksomheten. På den måten blir relevante problemstillinger tilknyttet risiko belyst, og det blir kartlagt hvilke endringer som må gjennomføres i virksomheten. Deretter kommer man til enighet og det tas opp til ledergruppen for godkjennelse, før det videre går opp til styret. Ifølge respondenten er det viktig å drive med målrettet trening opp til styret og andre som har et dedikert ansvar for risikovurdering og rapportering.

4.3.5 Trossystem

Respondent 2 fra EY mener at organisasjonskultur defineres som "måten virksomheten arbeider og tar beslutninger på, de målene virksomheten setter seg og atferden blant ledere og ansatte." Ser man derimot på risikokultur hevder respondenten at det er mer spesifikt knyttet til normer, holdninger og atferd relatert til risikostyring i virksomheten. Respondenten uttrykker:

> *Jeg merker forskjell på risikokultur hos de ulike kundene på helt simple ting som hvorvidt man er opptatt av å gjennomføre egne kontroller eller at man har tillit til de ansatte, og kan la andre gjøre det. Hvis man har en sterk risikokultur er det ikke like nødvendig å ha sterk overvåking og mye kontroller, for da vil den kulturen være bærevirkende for det som faktisk blir gjort i praksis.*

Respondenten hevder at et mål på god risikokultur handler om hvor transparent virksomheten er i risikorapportering og om styringsprinsippene fra styret blir forstått. Ifølge respondenten vil det imidlertid ta lang tid å bygge opp en god risikokultur, spesielt hvis man har stor utskiftning i arbeidstokken.

5.0 Analyse

I dette kapittelet vil vi gjennomføre en analyse av våre empiriske funn og trekke inn tidligere forskningslitteratur for å besvare våre tre forskningsspørsmål. I delkapittel 5.1 vil vi presentere og diskutere første forskningsspørsmål: *Hvilke operasjonelle risikoer oppstår i virksomheter?* I delkapittel 5.2 vil vi ta utgangspunkt i rammeverket til Simons (1995b) *Levers of Control*, for å besvare andre forskningsspørsmål: *Hvilke styringsmekanismer benytter virksomheter for operasjonell risikostyring?* Avslutningsvis vil vi i delkapittel 5.3 ta utgangspunkt i delkapittel 5.1 og 5.2, empiriske funn og tidligere forskningslitteratur for å besvare tredje forskningsspørsmålet: *Hvilke styringsmekanismer er avgjørende for god operasjonell risikostyring?*

I kapittel 4.0, *empiriske funn,* ble virksomhetene behandlet individuelt og kategorisert innenfor tre ulike bransjer: (1) Finansforetak, (2) Fiskeri og infrastruktur, og (3) Konsulentselskap. I dette kapittelet vil vi behandle virksomhetene innenfor hver bransje som samlet og sammenligne de tre bransjene. Det gir oss mulighet til å diskutere forskjeller og likheter på tvers av bransjene når det gjelder operasjonell risikostyring.

5.1 Operasjonell risiko

Første forskningsspørsmål "hvilke operasjonelle risikoer oppstår i virksomheter?", vil besvares med utgangspunkt i det teoretiske rammeverket presentert i kapittel 2 og empiriske funn presentert i kapittel 4. I dette delkapittelet vil vi definere operasjonell risiko, samt redegjøre for dens positive og negative effekter. I tillegg vil vi redegjøre for hvilken påvirkning operasjonell risiko har på andre risikoklasser og diskutere operasjonell risiko i lys av Covid-19.

5.1.1 Definisjon av operasjonell risiko

Finanstilsynet (2016, s. 4) definerer operasjonell risiko som "risikoen for tap som følge av utilstrekkelige eller sviktende interne prosesser eller systemer, menneskelige feil eller eksterne hendelser." Sammenligner vi definisjonen til Finanstilsynet (2016) på operasjonell risiko med våre empiriske funn fra finansforetakene er den tilnærmet lik. Trekker vi inn hvordan Storebrand definerer operasjonell risiko ser vi denne likheten: "Risiko for økonomisk tap som

følge av ineffektiv, utilstrekkelig eller sviktende interne prosesser eller systemer, menneskelige feil, eksterne hendelser eller at interne retningslinjer ikke etterleves." Myndigheter og tilsynsorgan har definert ulike kategorier for operasjonell risiko for finansforetakene. Kategoriene er følgende: internt og eksternt bedrageri, ansettelsesvilkår og sikkerhet på arbeidsplassen, kunden, produktene, skade på fysiske eiendeler, avbrudd i drift og systemer, oppgjør, levering og annen transaksjonsbehandling. Våre empiriske funn viser at finansforetakene i tillegg har valgt å integrere compliance risiko innenfor operasjonell risiko. Compliance risiko er den risikoen som oppstår som følge av manglede etterlevelse av lov og forskrift, andre eventuelle bestemmelser eller interne retningslinjer. Det kan føre til konsekvenser som regulatoriske sanksjoner, økonomisk tap eller tap av omdømme. Årsaken til at finansforetakene velger å integrere compliance risiko innenfor operasjonell risiko, er at brudd på lover og regler kan hindre foretak i å nå sine mål. Den årlige økningen i regelverk og retningslinjer er krevende å sette seg inn i og kan medføre en compliance risiko i seg selv. For å sikre at regulatoriske krav etterleves er det finanstilsynet som følger opp og veileder foretakene. Videre viser våre funn at compliance risiko kan være en av årsakene til at rollen, *Compliance,* har vokst frem i virksomheter. Dette vil utbroderes ytterligere i delkapittel 5.2.1.

Sammenlignet med finansforetakene viser våre empiriske funn at virksomhetene innenfor fiskeri og infrastruktur opererer i mer dynamiske miljøer. Operasjonelle risikoer innenfor fiskeri kan oppstå ute på sjøen, mens innenfor infrastruktur kan operasjonelle risikoer oppstå i utbygging av prosjekt eller i arbeid med elektrisitet. Innenfor fiskeri og infrastruktur vil derfor operasjonelle risikoer hovedsakelig være tilknyttet personskade og HMS, i verste fall kan dette dreie seg om fare for liv og helse. Grunnet dette er det flere virksomheter som har etablert egne roller innenfor HMS, noe som vil beskrives ytterligere i delkapittel 5.2.1. I tillegg viser våre empiriske funn fra konsulentselskapene at felles for alle virksomheter uavhengig bransje, er risiko forbundet med IT- og cybersikkerhet og regulatoriske endringer som for eksempel personvern.

Videre viser våre empiriske funn at operasjonelle risikoer sjeldent har positive effekter, men stort sett negative effekter. Dette samsvarer med COSO (2017) sin definisjon av operasjonell risiko som noe utelukkende negativt. Våre funn viser at negative effekter ved operasjonell risiko kan for eksempel være svikt i systemer, personskade eller brudd på lovverk. Imidlertid blir det påpekt at virksomheter er nødt til å ta risiko for å oppnå noe. I enkelte tilfeller kan risikotaking medføre positive effekter som høyere avkastning og styrket omdømme. Dette samsvarer med Segal (2011) som hevder at operasjonell risiko ikke bare gir negative, men

også positive effekter. På den måten vil et utelukkende fokus på negative effekter hindre virksomheter i å ta risiko og se hvilke muligheter det kan gi på lenger sikt. På bakgrunn av dette viser våre empiriske funn at virksomheter bør legge opp ansattes arbeid slik at det skapes profitt. Dette forutsetter imidlertid at man har et godt rammeverk på plass og at virksomheter er flinke til å delegere ansvar og myndighet. Hvordan virksomheter gjør dette vil utbroderes ytterligere i delkapittel 5.2 og 5.3.

5.1.2 Operasjonell risiko på tvers

Ifølge Finanstilsynet (2016, s. 4) er operasjonell risiko "et vidt fagfelt som griper inn på overordnet styring og kontroll og andre risikoområder, noe som kan gjøre det utfordrende å avgrense risikoområdet." En slik beskrivelse på operasjonell risiko finner vi i våre empiriske funn fra konsulentselskapene som hevder at operasjonell risiko er et vidt fagfelt, som griper inn på overordnet styring og kontroll og andre risikoområder. En årsak til at operasjonell risiko er et vidt fagfelt kan ses i sammenheng med Jansrud (2017b), som viser at ulike risikoklasser har en sammenheng med operasjonell risiko. Som presentert i delkapittel 2.2.1 hevder Jansrud (2017b) at operasjonell risiko går på tvers av kreditt-, marked-, motpart-, og likviditetsrisiko. Et eksempel er markedsrisiko hvor man kan tape finansiell posisjon som følge av en operasjonell hendelse, for eksempel bevisst eller ubevisst rammebrudd. På den måten finner vi at risiko som oppstår i ulike risikoklasser kan oppstå på bakgrunn av operasjonelle hendelser. Dermed kan vi konkludere med at en av årsakene til at operasjonell risiko er et vidt fagfelt, er at operasjonell risiko går på tvers av flere av risikoklasser.

Omdømmerisiko

Våre empiriske funn viser at operasjonell risiko er en uønsket hendelse som kan ha økonomisk påvirkning eller påvirkning på omdømme. Et eksempel var SMS hendelsen fra februar 2021 i Sparebanken Vest, som påvirket omdømme i en negativ retning. Et annet eksempel fra Sbanken var svikt eller avbrudd i drift og systemer. Det kunne medføre at kundene ikke fikk tilgang til nettsidene og dermed kunne det bli et tapspotensial for virksomheten. Andre eksempler finner vi innenfor fiskeri og infrastruktur hvor operasjonelle hendelser kan være ulykke på sjø, i utbyggingsprosjekt eller i forbindelse med elektrisitet. Det kan både ha økonomisk påvirkning og påvirkning på omdømme til virksomheten. På bakgrunn av dette finner vi at virksomheter setter omdømme høyt på agendaen, og noen definerer omdømme som en operasjonell risiko. Jansrud (2017b) hevder imidlertid at omdømme ikke er en

operasjonell risiko, men en konsekvens av svake operasjonelle prosesser. Det er interessant å trekke Jansrud (2017b) sin beskrivelse av operasjonell risiko i sammenheng med Finanstilsynet (2016). Finanstilsynet (2016) hevder at operasjonell risiko omfatter juridisk risiko, men ikke strategisk eller omdømmerisiko som må vurderes særskilt. Med bakgrunn i Jansrud (2017b) og Finanstilsynet (2016) er det dermed ikke riktig å si at omdømme er en operasjonell risiko, men at operasjonelle hendelser i virksomheter kan påvirke omdømme.

5.1.3 Covid-19

Historisk sett har bank- og finanssektoren kommet lengst med operasjonell risikostyring. Dette skyldes finanskrisen i 2008/2009 hvor finansforetakene ble mer regulert og risiko ble satt høyere på agendaen (Liset, 2017). Etter oljeprisfallet i 2014 ble olje- og gassnæringen mer regulert. Våre empiriske funn fra fiskeri viser at oljeprisfallet også påvirket deres næring. Trekker vi inn Covid-19 har det oppstått flere operasjonelle hendelser det siste året. Covid-19 har preget alle bransjer sammenlignet med finanskrisen og oljeprisfallet, som preget enkelte bransjer. Krisen har rammet ansatte med permitteringer og oppsigelser, i tillegg til at liv og helse har blitt satt i fare både på og utenfor arbeidsplassen. Krisen har også påvirket virksomheter i form av utsettelser av prosjekter, og redusert tilbud og etterspørsel av varer og tjenester. Dette har medført økonomisk tap og konkurser. Som et resultat av Covid-19 har virksomheter laget handlingsplaner for å håndtere operasjonelle risikoer som har oppstått, og vil oppstå. På bakgrunn av tidligere kriser vil vi anta at det vil komme nye retningslinjer og reguleringer fra myndigheter tilknyttet risiko, og spesielt operasjonell risiko som følge av Covid-19.

5.1.4 Oppsummert

Samlet viser våre empiriske funn at operasjonelle risikoer hovedsakelig gir negative effekter, men et utelukkende fokus på negative effekter kan hindre virksomheter i å se mulighetene som risiko kan gi. I noen tilfeller må virksomheter ta risiko for å oppnå noe og dette kan følgelig gi positive effekter. Videre viser forskningslitteratur og eksempler fra empiriske funn at operasjonell risiko er et vidt fagfelt og går på tvers av flere risikoklasser. Det betyr at i noen tilfeller kan operasjonell risiko tilhøre andre risikoklasser. I tillegg finner vi at omdømmerisiko ikke er en operasjonell risiko, men at operasjonelle hendelser kan påvirke omdømme. Avslutningsvis finner vi at Covid-19 har gitt en økning av operasjonelle hendelser i

virksomheter. Vi antar at et resultat av Covid-19 vil være at operasjonell risikostyring vil bli satt høyere på agendaen i fremtiden.

5.2 Styringsmekanismer for operasjonell risikostyring

Andre forskningsspørsmål "hvilke styringsmekanismer benytter virksomheter for operasjonell risikostyring?" vil besvares med utgangspunkt i det teoretiske rammeverket presentert i kapittel 2 og empiriske funn presentert i kapittel 4. Analysen vil ta utgangspunkt i Simons (1995b) fire styringssystemer: grensesystem, diagnostisk styringssystem, interaktivt styringssystem og trossystem.

5.2.1 Grensesystem

Grensesystemet fungerer som et styringssystem ved å avgrense det akseptable aktivitetsområdet til ansatte i virksomheten (Simons, 1995b). Delkapittelet vil ta utgangspunkt i Simons (1995b) to typer grenser, (1) *forretningsgrenser og (2) strategiske grenser,* som kan overføres til risikostyring.

(1) Forretningsgrenser

Ifølge Simons (1995b) er det nødvendig at toppledelsen skaper grenser når usikkerheten i markedet er høy eller når den interne tilliten i virksomheten er lav. Forretningsgrenser setter grenser for hvordan man skal drive sin virksomhet og er en forutsetning for at ledere kan delegere ansvar nedover i virksomheten. Vi skal se på hvordan virksomheter organiserer og definerer ansvarsforhold, samt roller som er sentrale for operasjonell risikostyring. Videre vil vi å se på hvordan virksomheter benytter risikoteknologier som vil ha grensesettende effekter. Slike grensesettende effekter kan være risikopolicyer og risikorammeverk som kan bidra til å oppnå ledelse og kontroll for å styre risiko.

Organisering og ansvarsforhold

Modellen "de tre forsvarslinjene" som er presentert i delkapittel 2.3.3, viser en oversikt over roller og ansvarsforhold for risikostyring på et overordnet nivå. Ifølge IIA (2018) gir modellen en god beskrivelse av kontrollstrukturen i en virksomhet, og skiller mellom tre linjer som er involvert i effektiv risikostyring. Våre empiriske funn fra finansforetakene viser at foretakene

organiserer styring og kontroll av operasjonell risiko med utgangspunkt i modellen. Det fremkommer at et av finansforetakene kaller de tre linjene for ansvarslinjer, mens resterende foretak benytter forsvarslinjer. Trekker vi inn funn fra fiskeri og infrastruktur fremkommer det at samtlige virksomheter ikke benytter modellen, men det blir hevdet at organiseringen fungerer litt på samme måte. Med utgangspunkt i våre empiriske funn kan vi konkludere med at det er variasjon i hvordan virksomhetene organiserer og definerer tydelige ansvarsforhold. Dette samsvarer med Arena et al. (2010) som hevder at delegering av ansvar for helhetlig risikostyring varierer mellom virksomheter. I det følgende vil vi redegjøre for hvordan virksomhetene organiserer roller og ansvarsforhold for operasjonell risikostyring.

Styret og toppledelsen

Ifølge Finansforetaksloven (2015, §13-6) skal styret overvåke og styre finansforetakets samlede risiko. I tillegg skal de jevnlig vurdere om finansforetakets styrings- og kontrollordninger er tilpasset risikonivå og omfanget av virksomheten. Empiriske funn fra finansforetakene viser at styret og toppledelsen har sentrale roller for risikostyring. På den måten samsvarer våre funn med Beasley et al. (2015), som viser at styret og toppledelsen har det overordnet ansvaret for helhetlig risikostyring. Trekker vi inn empiriske funn fra fiskeri og infrastruktur er det administrerende direktør som er øverst ansvarlig for alle ledd i virksomheten, og ikke styret. Dermed er det ikke nødvendigvis styret som alltid har det overordnede ansvaret for helhetlig risikostyring i virksomheter.

Risikoutvalg, revisjonsutvalg og risikokomité

Ifølge Finansforetaksloven (2015, §13-6) skal foretaket ha et risikoutvalg oppnevnt av styret, som skal forberede styrebehandlingen. Våre empiriske funn viser at finansforetakene har etablert risikoutvalg for å opprettholde kontrollen i foretakene. Det blir blant annet uttrykt at utvalget skal sørge for at risiko- og kapitalstyring i konsernet støtter opp under konsernets strategiske utvikling og måloppnåelse, og sikre finansiell stabilitet. Videre viser våre funn at flere virksomheter innenfor både finansforetak og fiskeri og infrastruktur har revisjonsutvalg. Revisjonsutvalget er et saksforbedrende organ for styret, og skal støtte styret i utøvelsen av sitt ansvar innenfor risikostyring, internkontroll og etterlevelse av retningslinjer for etikk og samfunnsansvar. Flere av virksomhetene innenfor finansforetak har risikokomiteer som skal være rådgivende komiteer for administrerende direktør, i tillegg til å bistå med oppfølging og kontroll innenfor sentrale fagområder.

Andre sentrale roller som er involvert i risikostyring

Fra tidligere forskningslitteratur er det kommet frem ytterligere roller som er involvert i helhetlig risikostyring: *risikoeksperter og risikoledere* (Arena et., 2010; Beasley et al., 2015; Mikes, 2009; Power, 2007). Fra våre empiriske funn finner vi ingen tydelige definerte roller som omhandler risikoeksperter. Dette kan skyldes at vårt hovedfokus er rettet mot operasjonell risiko, i tillegg til at risikoeksperter ofte operer i virksomheter innenfor kreditt- og markedsrisiko (Mikes, 2009). Imidlertid viser våre funn at virksomhetene har etablert roller som kan betegnes som risikoledere. Innenfor finansforetakene har samtlige av virksomhetene valgt å plassere risikoledere i andre forsvarslinje. Våre empiriske funn fra finansforetakene viser at i andre forsvarslinje er det to uavhengige kontrollfunksjoner: *risikostyringsfunksjonen* og *compliancefunksjonen,* og innenfor hver av disse finner vi sentrale risikoledere. Innenfor risikostyringsfunksjonen betegnes risikoleder for Chief Risk Officer (CRO). Dette samsvarer med Power (2007) og Arena et al. (2010), som hevder at CRO er en sentral rolle i helhetlig risikostyring. Trekker vi dette i lys av Beasley et al. (2005) vil CRO være viktig i implementering av helhetlig risikostyring. Videre viser våre funn fra finansforetakene at innenfor compliancefunksjonen er det etablert en ytterligere risikoleder, betegnes som Chief Compliance Officer (CCO). CCO har ansvar for å gjennomføre kontroller av etterlevelse av lover og regler, noe som kan være en årsak til at finansforetakene har valgt å involvere en ny rolle. Sammenligner vi våre empiriske funn med tidligere forskningslitteratur kan det tyde på at det er det kommet frem en ytterligere rolle som er involvert i helhetlig risikostyring.

Videre er et interessant funn at størrelse og kompleksitet vil ha påvirkning på om virksomheten har et tydelig skille mellom CRO- og CCO-rollen. Det fremkommer at banker med forvaltningskapital på over 100 mrd. kroner må ha et tydelig skille mellom CRO og CCO. Ettersom Sparebanken Sogn & Fjordane har en forvaltningskapital på omtrent 60 mrd. kroner har ikke banken et like tydelig skille. Det kan tyde på at forvaltningskapitalen vil ha betydning for om foretak skiller mellom CRO- og CCO-rollen. Det fremkommer et annet funn som det er verdt å bemerke seg, som omhandler hvorvidt CRO skal plasseres i første- eller andrelinje. Konsulentselskapene viser at CRO i noen tilfeller kan plasseres i førstelinje. I andre tilfeller kan CRO ligge i grensesnittet mellom første- og andrelinje, men i de fleste tilfeller plasseres CRO i andrelinje. CCO er derimot en klarere andrelinje. Samtlige av finansforetakene viser at CRO- og CCO-rollen blir plassert i andrelinje.

IIA (2018) påpeker at sentrale roller i andrelinje ikke bare utføres av CRO og CCO, men også av roller innenfor HMS, økonomiavdeling, juridisk avdeling og/eller kvalitetsstyring. Sammenligner vi våre funn fra finansforetakene med fiskeri og infrastruktur er det ikke etablert roller som CRO og CCO, men roller som er ansvarlige innenfor HMS og økonomiavdelingen. Det kan tyde på at alle virksomhetene vi har undersøkt har etablert sentrale roller for risikostyring, som samsvarer med rollene som blir beskrevet av IIA (2018). Videre er et interessant funn at alle virksomhetene har en rolle for internrevisor. Dette samsvarer med IIA (2018) og Arena et al. (2010) som viser til at internrevisor er sentral i arbeidet med risikostyring. I tillegg finner vi at samtlige virksomheter benytter ekstern revisor, som også IIA (2018) viser til er en sentral rolle.

Internkontroll

Det fremkommer at både finansforetakene og fiskeri og infrastruktur legger vekt på internkontroll i operasjonell risikostyring. En av årsakene til dette er at uventede tap ved utilstrekkelig internkontroll kan være en operasjonell risiko i seg selv. Internkontroll skal gjennomføres av hele virksomheten, inkludert styret, ledelsen og ansatte. Hensikten med internkontroll er å tilse at virksomheten når sine mål knyttet til målrettet og effektiv drift, og pålitelig rapportering og etterlevelse av lovverk med akseptabel gjenværende risiko. Videre fremkommer det av våre funn at samtlige av virksomhetene har etablert roller som er ansvarlige for internkontroll. I tillegg benytter virksomhetene internkontrollsystemer, som inneholder avviksbehandling og risikoverktøy for identifisering og vurdering av risiko. Dette samsvarer med Jansrud (2017a) som mener at styret bør utvikle og vedlikeholde robuste systemer for internkontroll med hensiktsmessige interne kontroller, som dekker operasjonell risikokontroll i hele virksomheten. I tillegg stiller myndigheter og ulike standarder krav til at alle virksomheter skal gjennomføre internkontroll. Dersom virksomhetene ikke har tilstrekkelig dokumentert internkontroll kan myndighetene gi pålegg om å rette opp dette innen en gitt frist, noe som kan føre til dagbøter. I alvorlige tilfeller kan virksomheten bli politianmeldt. Spesielt gjelder dette HMS ettersom mangelfullt HMS-system også kan gi forretningsmessige konsekvenser (IIA, 2018).

Risikoteknologier

Risikoteknologier defineres som komplekse sett med praksis, prosedyrer og instrumenter som er vedtatt for å oppnå ledelse og kontroll for å styre risiko (Arena et al., 2010). For helhetlig

risikostyring vil risikoteknologier ha en grensesettende effekt, og slike grensesettende effekter kan være risikopolicyer og risikorammeverk. Risikopolicyer inneholder overordnede regler, mens risikorammeverk inneholder detaljer om utførelsen av helhetlig risikostyring (Fraser og Simkins, 2016). I det følgende vil vi se på hvordan virksomhetene benytter risikoteknologier som styringsmekanisme for operasjonell risikostyring.

Risikopolicy

Ifølge Beasley et al. (2015) og Fraser & Simkins (2016) er det hensiktsmessig å benytte risikopolicyer for å formalisere helhetlig risikostyring i virksomheter. Våre empiriske funn viser at samtlige av virksomhetene har utarbeidet policy for operasjonell risiko, som omhandler hvordan ansatte skal arbeide og håndtere risiko. Ifølge konsulentselskapene er det viktig å starte på toppen med styret når virksomheten skal utforme policyer for at risiko skal bli styrt helhetlig. Det er styret som fastsetter de overordnende prinsippene for risikostyring, og ifølge konsulentselskapene er dette de øverste kravene som styret mener at virksomheten skal forholde seg til. Våre empiriske funn viser at prinsippene bør inneholde styrets risikoappetitt. Det er også viktig at prinsippene er overordnede og ikke for detaljerte, ettersom alle i virksomheten skal ha tilgang til og forholde seg til policyene. Videre hevder konsulentselskapene at det er viktig å skille mellom policyer og rutiner. Grunnen er at de underliggende rutinene skal operasjonalisere de overordnede policyene. I praksis betyr det at man utarbeider generelle rutinebeskrivelser, prosessbeskrivelser og underliggende dokumenter som skal svare på hvordan styringsprinsippene skal implementeres. I tillegg mener Finanstilsynet (2016) og Jansrud (2017a) at policyer bør inneholde kvantifiserte rammer. Imidlertid viser våre funn fra finansforetak at en typisk fallgruve er at policyer blir for teoretiske og at førstelinje ikke klarer å forholde seg til dem. Virksomheter er derfor opptatt av å definere hvem som er risikoeier og hvem som er risikokontroller, slik at førstelinje på den måten klarer å forholde seg til policyer som er blitt utarbeidet. Et eksempel på dette fra finansforetakene er at ansatte skal bli opplyst om policyer. Dette eksemplet viser hvordan virksomhetene arbeider med å få ansatte til å forholde seg til policy, og på den måten at policy for operasjonell risiko blir styrende i virksomheten.

Risikorammeverk

Ifølge Beasley et al. (2015) og Fraser & Simkins (2016) er det hensiktsmessig å benytte risikorammeverk for å formalisere helhetlig risikostyring i virksomheten. Risikorammeverk

skal hjelpe virksomheten å ta riktig risiko, på riktig nivå. Våre empiriske funn viser at *COSO* og *ISO* er de mest brukte og anerkjente risikorammeverkene for operasjonell risikostyring. Det fremkommer at samtlige av virksomhetene tar utgangspunkt i rammeverkene og deretter utarbeider sine egne rammeverk for risikostyring. Det kan tyde på at virksomhetene ikke benytter rammeverkene direkte, men at mye av tankegangen er tuftet på rammeverkene. Dette samsvarer med Lundqvist (2014) som viser at vanlig praksis for helhetlig risikostyring i virksomheter er å ta utgangspunkt i et av rammeverkene, og deretter lage sitt eget interne rammeverk for implementering av helhetlig risikostyring. Det fremkommer imidlertid fra finansforetakene at finanstilsynets modul for operasjonell risikostyring er mer førende enn rammeverkene, ISO og COSO. Videre viser funn fra fiskeri og infrastruktur at virksomhetene har andre standarder som de må forholde seg til. På bakgrunn av dette kan vi konkludere med at virksomheter også har andre standarder som de må forholde seg til, og som kan være mer førende enn COSO og ISO.

Videre fremkommer det at selv om rammeverkene er et fint utgangspunkt, kan typiske fallgruver være at rammeverkene blir for byråkratiske og teoretiske. En annen fallgruve kan være at virksomhetene ofte tror at rammeverkene skal dekke alle former for risiko. Våre funn viser at man kan hindre eller redusere fallgruvene gjennom å få rammeverkene praktisk implementert i prosessene. Det er også viktig å snakke virksomhetens språk og fokusere på hvordan det skaper verdi. Videre hevder konsulentselskapene at det er avgjørende å bruke tid på å få gjort systemer på terminologibruk, i tillegg til å finne vurderingsskalaer og metoder som er riktig for virksomheten. Det er også avgjørende å få dette integrert i rapportering til ledelsen og styret, og samtidig få det inn i plan- og budsjettprosesser.

(2) Strategiske grenser

Ifølge COSO (2017) kan risikoappetitt sette strategiske grenser for hvor stor risiko den ansatte i virksomheten vil ha lov å ta. IIA (2018) redegjør for at risikoappetitt består av "evne" og "vilje". Det fremkommer fra våre empiriske funn at risikoevne handler om grensen virksomheten kan tåle og må holde seg innenfor, og risikovilje vil være innenfor risikoevnen igjen. Videre viser empiriske funn at risikoappetitt bør integreres i strategi, slik at det på den måten setter føring, mål og rammer for virksomheten. I tillegg bør virksomheten sette appetitt for ulike risikoer som blir besluttet i retningslinjer. På bakgrunn av dette samsvarer våre funn med IAA (2018), som påpeker at virksomhetens mål, styringsrammer, fullmakter og handlingsrom bør samsvare med den totale risikoappetitten og strategien. Det er også flere av

virksomhetene som benytter risikoappetitt som et verktøy i sin helhetlige risikostyring (Deloitte, 2014). Dette kan gjøres ved kvalitative eller kvantitative metoder, som vil utbroderes ytterligere i delkapittel 5.2.2 (IIA, 2018).

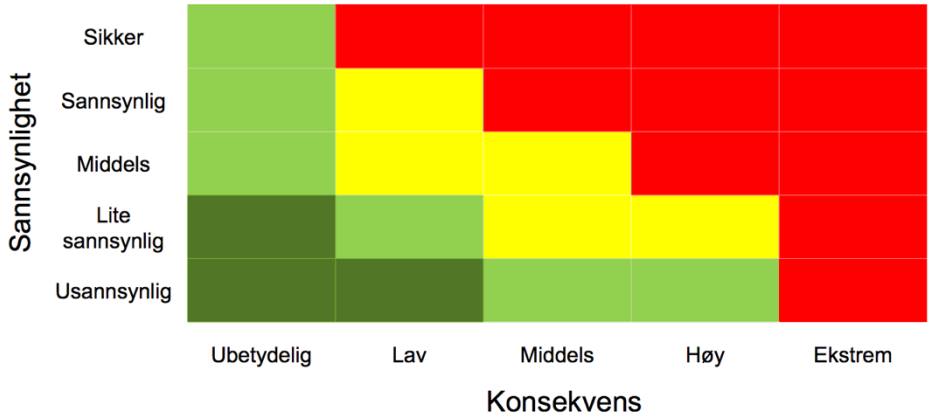
Risikoappetitt vil imidlertid variere med utgangspunkt i lovverk, samt virksomheters bransje, strategi og organisasjonskultur (IIA, 2018). Virksomheter er strengt regulert og dermed kan lovverk i seg selv sette grenser for virksomheter. Funn viser at finansforetakene blant annet må forholde seg til finanstilsynet og kapitaldekningsregelverket, som definerer grenser for foretakene. Videre fremkommer det at fiskeri må forholde seg til mattilsynet og fiskeridirektoratet, som utarbeider retningslinjer for akseptabel drift innenfor blant annet personvern, fiskevelferd, ytre miljø, verdier og omdømme. Et funn som er verdt å bemerke seg er at lovverk kan sette grenser for innovasjon. Det blir uttrykt fra virksomhetene at risikostyring står som en motpol til innovasjon og utvikling. Hovedproblemet oppstår hovedsakelig når man overfører innovasjon til drift. En av årsakene til dette er compliance risiko som kan hindre innovasjonen og kvele en del av insentivene. Det fremkommer fra funn at risikostyring ikke bare setter grenser, men at risikostyring også muliggjør at innovative idéer faktisk lar seg gjennomføre. Det forutsetter imidlertid at man gjennomfører gode risikovurderinger selv i innovasjonsmiljøer. Ved å identifisere og justere risikoer, kan virksomheter tilrettelegge for risikoer som kan oppstå. I tillegg er det avgjørende at virksomheter ikke setter en felles toleranse for risikoer, men at det settes toleranse for hver enkelt risiko. Årsaken til dette er at noen risikoer man må være mer villig til å ta, for å oppnå en ønsket tilstand. Med utgangspunkt i våre funn kan det tyde på at virksomheter bør sette en høyere toleranse for risiko knyttet til innovasjon for å muliggjøre innovasjon.

5.2.2 Diagnostisk styringssystem

COSO (2017) viser at standardprosessen for risikostyring omhandler å identifisere, vurdere og håndtere risiko forbundet med strategi. I dette delkapittelet vil vi diskutere hvordan virksomhetene benytter diagnostiske styringssystemer for å identifisere, vurdere og håndtere risiko. I det følgende vil vi undersøke hvordan virksomhetene benytter risikoverktøy og hendelsesdatabase for å identifisere og vurdere operasjonell risiko. Videre vil vi undersøke hvordan risiko blir rapportert og målt, i tillegg til hvordan finansforetakene setter kapitalbehov for operasjonell risiko.

Risikoverktøy: Risikomatrise

Konsulentselskapene hevder at ledende markedspraksis for måltall og rammer, er å etablere en risikomatrise. Ifølge Arena et al. (2010) er det hensiktsmessig å ta i bruk risikomatrise som et verktøy for å identifisere og vurdere risiko. Våre empiriske funn viser at samtlige av virksomhetene benytter seg av risikomatrise, også kalt 5x5 matrise, med rød, gul og grønn sone. Det fremkommer at risikomatrisen benyttes som hovedverktøy for å identifisere og vurdere operasjonell risiko. Dette samsvarer med Duijm (2015), som viser at risikomatrise ofte blir benyttet i operasjonell risikostyring. Et eksempel på en slik matrise er illustrert i Figur 7 (Duijm, 2015).



Figur 7: Risikomatrise (Jansrud, 2017b)

Våre empiriske funn viser at ved identifisering av enkeltstående uønskede hendelser som kan inntreffe, anslår virksomhetene et iboende risikonivå. Som Figur 7 viser er det mulig å vurdere operasjonell risiko ut fra konsekvens (x-aksen) og sannsynlighet (y-aksen). Det gjøres ved at det blir besvart noen spørsmål på sannsynlighet og konsekvens, og deretter får man en score på risikoen. Dette samsvarer med Dujim (2015) sin beskrivelse av risikomatrise. Videre viser funn at scoren fra risikomatrisen representerer en farge som gir en indikasjon på om risikoen skal aksepteres eller ikke. Dujim (2015) viser imidlertid at en svakhet tilknyttet matrisen omhandler beslutningstaking om når risikoen skal aksepteres på ulike fargenivåer. Fra funn blir det påpekt fra flere av virksomhetene at i vurderingen om risikoen skal aksepteres eller ikke, tar de stilling til virksomhetens risikoappetitt. Dette kan være med på å redusere svakheten som Dujim (2015) fremlegger.

Videre viser funn fra konsulentselskapene til hva som er ledende praksis for iverksettelse av tiltak basert på vurdering av fargenivåer i matrisen. Ledende praksis i gul sone er å predefinere

tiltak med tydelig ansvarsforhold, som viser hva virksomheten skal gjøre for å komme tilbake i grønn sone. Er man i rød sone vil det være andre eskaleringer, som for eksempel at styret blir informert slik at det iverksettes raskere håndtering for å komme tilbake på riktig spor. I de tilfeller hvor det ikke er mulig å gjøre noe mer med risikoen, hevder konsulentselskapene at tiltaket vil være å overvåke risikoen med høyere frekvens enn det man vanligvis ville gjort. Imidlertid viser våre funn at noen av virksomhetene velger å ikke iverksette tiltak mot risikoene som havner i rød sone. Årsaken til dette er at virksomhetene ønsker en objektiv vurdering av risikoen slik at virksomheten kan unngå at risikoen manipulerer risikobildet.

Når virksomhetene skal iverksette tiltak hevder flere av virksomhetene det er avgjørende at risikofaktorene er konkrete, slik at det er mulig å relatere hendelser til dem. Flere finner dette utfordrende, ettersom listen med identifiserte risikoer blir så lang at det blir vanskelig å synliggjøre de mest sentrale risikoene. Dette samsvarer med Dujim (2015), som hevder at en annen svakhet med matrisen er at virksomheter har for mange risikoer og dermed ikke klarer å prioritere hvilke som bør løses først. Med utgangspunkt i våre empiriske funn kan vi konkludere med at god praksis vil være å fokusere på de risikoene som medfører størst konsekvens for virksomheten. I tillegg er det avgjørende å predefinere tiltak med tydelige ansvarsforhold ettersom det fremkommer at det er vanskelig å forankre ansvar til de som er ansvarlig for risikoene.

Risikoverktøy: Sikker jobbanalyse (SJA)

For å vurdere risiko i arbeidsoperasjoner benytter virksomhetene innenfor fiskeri og infrastruktur, Sikker Jobbanalyse (SJA). Våre empiriske funn viser at SJA er en forhåndsdefinert vurdering som alle ansatte må gjennomføre i forkant av arbeidsoperasjoner. Det fremkommer at risikoene som ligger i gul og rød sone i risikomatrisen, blir inkludert i SJA. Hensikten med å inkludere disse risikoene i SJA er at ansatte skal være klar over risikoene som kan oppstå i arbeidsoperasjoner. Våre empiriske funn viser at konsekvenser kan reduseres fordi ansatte blir bevisst på risikoene som kan inntreffe på forhånd. Funn viser at fordelen med SJA er at man kan kommunisere og inkludere ansatte i vurderinger i forkant av arbeidsoperasjoner. En annen fordel er at SJA har som formål å avdekke risiko, og dermed er det essensielt å lære av tidligere hendelser som kontinuerlig kan inkluderes i SJA. Imidlertid finner vi at gjennomføring av SJA er et ressurskrevende arbeid, og tar mye tid (Norsk Olje og Gass, 2017). Likevel er dette arbeidet avgjørende for virksomhetene innenfor fiskeri og infrastruktur for å avdekke farlige forhold som kan oppstå, og som videre kan bidra til læring.

Hendelsesdata

Finanstilsynet (2016) viser at operasjonell risiko skiller seg fra andre risikotyper ved at den ikke er rettet mot et spesielt virksomhetsområde, men omfatter ulike kategorier av hendelser som kan påvirke flere områder. Våre empiriske funn viser at det er avgjørende at virksomhetene innenfor fiskeri og infrastruktur har en hendelsesdatabase, slik at det er mulig å føre statistikk over ulike typer hendelser. På den måten kan virksomhetene kategorisere hvilke hendelser som bør ha størst fokus. Hovedproblemet til flere av virksomhetene innenfor fiskeri og infrastruktur, er at hendelser og observasjoner i mange tilfeller ikke blir registrert. Det kan medføre at virksomhetene ikke får inn viktig erfaringsdata og dermed blir det ikke mulig å formidle viktig informasjon videre. Finansforetakene har også de siste årene begynt å registrere hendelser i hendelsesdatabase. En årsak til dette er at finanstilsynet forventer at finansforetakene skal se på taps- og hendelsesdatabasen i forbindelse med fastsettelse av rammer og måltall for styring av operasjonell risiko. En annen årsak er regulatoriske krav, for eksempel Basel, som legger føringer for at finansforetak skal benytte hendelsesdata. Ifølge Finanstilsynet (2016) bør foretakene prioritere hendelser med lav frekvens og høy konsekvens, det vil si ekstreme, men ikke usannsynlige hendelser som kan medføre store tap for virksomheten. I tillegg bør foretakene vurdere både faktiske og potensielle hendelser (Finanstilsynet, 2016).

Videre viser Finanstilsynet (2016) at foretak bør vurdere hendelser med en systematisk tilnærming til sin risikotoleranse. En teknikk som kan brukes til dette er scenarioanalyser. Empiriske funn viser at virksomheter ønsker å gjennomføre scenarioanalyser for å predikere hvor det kan gå galt. For å gjøre dette benytter noen av virksomhetene seg av Monte Carlo simulering. Ifølge Mun (2010, s. 82) er Monte Carlo simulering en tilfeldig tallgenerator som er nyttig for prognoser, estimering og risikoanalyse. På den måten kan man kvantifisere usikkerhet til en beslutningsvariabel. Våre empiriske funn viser at man ved Monte Carlo simulering baserer seg på utførte risikovurderinger ved hjelp av risikomatrise, i tillegg til hendelsesdata over tid. Imidlertid vil en utfordring ved Monte Carlo simulering være at det blir for mye historisk data. Dermed bør virksomhetene være kritiske til kvaliteten på risikovurderingene. Videre fremkommer det fra konsulentselskapene at det er avgjørende at virksomheten er ganske modne på risiko for å kunne gjennomføre Monte Carlo simulering, og for at det skal gi verdi.

Rapportering på risiko

Ettersom virksomheter står overfor påvirkning fra endrede rammebetingelser og indre og ytre forhold, er det viktig å ha kontroll over risikobildet i virksomheten. En forutsetning for å opprettholde kontroll, er jevnlig rapportering av risiko. Ifølge Wiggen (2008) er det viktig med jevnlig rapportering til ledelsen og styret for at risikostyringssystemet skal overleve. Formålet med rapportering er å kunne opprettholde den ønskede risikoprofilen til virksomheten, samtidig som man har aktiv oppfølging for å sørge for at planlagte tiltak blir gjennomført. Våre empiriske funn viser at det å anvende en hendelsesdatabase bidrar til at rapportering blir bedre i virksomheten, og at vesentlige hendelser blir løpende rapportert til styret. Videre viser funn at det er viktig å ha gode tall i risikorapporteringen, og flere hevder en avgjørende forutsetning er å vise til risikomatrisen. Det fremkommer imidlertid fra en av konsulentene at det å inkludere risikomatrise i risikorapportering kan fremstå som uprofesjonelt. Konsulenten hevder at risiko heller bør rapporteres i et listeformat, hvor risikoene er forståelige og det blir inkludert en refleksjon i rapporten om selve hendelsen, konsekvens og integrerende tiltak som er etablert for å håndtere den enkelte risiko.

Andre metoder for kvantifisering av operasjonell risiko

Simons (1995a) mener at mål og målsetting er de viktigste designparameterne for det diagnostiske styringssystemet. Det fremkommer fra empiriske funn at virksomhetene kobler risiko til evnen om å nå satte mål. Flere av virksomhetene hevder at man på denne måten kan integrere operasjonell risikostyring i virksomhetsstyringen. For å tilse måloppnåelse inkluderer flere av virksomhetene innenfor fiskeri og infrastruktur risiko i KPI-er. Våre funn viser at det blir definert tydelige KPI-er for innhold i tilbud og kontrakter for å tilse at man er på riktig vei i forhold til forespeilet risikoutvikling. I tillegg viser funn at det blir inkludert flere parametere innenfor hver KPI. Dette kan for eksempel være statistikk, som gir en indikator på hva som skjer og dermed kan være en forklaringsvariabel til den aktuelle KPI-en. Våre funn fra fiskeri og infrastruktur samsvarer dermed med Giovannoni et al. (2016), som hevder at det å benytte KPI hvor risiko er inkludert vil bidra til at risikostyring blir et viktig agendapunkt hos styret og toppledelsen. Retter vi derimot blikket til finansforetakene finner vi ikke samsvar med Giovannoni et al. (2016), ettersom funn viser at finansforetakene sjeldent inkluderer risiko i KPI-er.

Videre hevder Power (2007) at risiko bør inngå som en kritisk vurdering i utarbeidelse av budsjetter. Våre empiriske funn viser imidlertid at virksomhetene ikke definerer operasjonell risiko i budsjetter. Sammenligner vi våre empiriske funn med tidligere forskningslitteratur av

Power (2009), Arena et al. (2010) og Giovannoni et al. (2016) hvor risiko blir inkludert i KPI-er og budsjetter er det lite som samsvarer med deres forskning. Funn viser at noen av virksomheter benytter signaler fra kommende budsjetter for å se hvor mye som er budsjettert for å oppnå målsettinger innenfor sitt område. Videre viser våre empiriske funn at det vil være fordelaktig for virksomhetene å få innblikk i ikke-revisor godkjente forretningsplaner med kontaktstrømanalyser og markedsverdier, for å si noe om risikoutvikling. Årsaken til dette er at revisorgodkjente regnskap gjør at virksomhetene sitter igjen med gammel informasjon, og særlig i sykliske bransjer som for eksempel shipping og oljeindustrien.

Kapitalbehovet i finansforetakene

Finansforetakene er pliktig til å årlig gjennomføre Internal Capital Adequacy Assessment process (ICAAP) for å vurdere kapitalbehovet for operasjonell risiko. ICAAP er en intern kapitalvurderingsprosess for å ta stilling til kapitalbehovet (Finanstilsynet, 2019). Etter kapitalkravsforskriften (2006, §41) kan finansforetak anvende tre ulike metoder for beregning av kapitalbehovet for operasjonell risiko. Dette er basismetoden, sjablongmetoden og AMA-metoden. Ifølge Regjeringen (2018) er det ingen virksomheter i Norge som har tillatelse eller har søkt om å benytte seg av AMA-metoden. Fra våre empiriske funn fremkommer det at heller ingen av virksomhetene benytter denne metoden. Derimot fremkommer det at to av foretakene benytter basismetoden, mens to andre foretak benytter sjablongmetoden. Våre empiriske funn fra konsulentselskapene viser at de to metodene er relativt like. Hovedforskjellen er at sjablongmetoden deler opp inntektsvariabelen i flere grupper. Det fremkommer at ved å benytte basismetoden skal foretak multiplisere alt med 15 prosent, mens for sjablongmetoden multipliseres hver gruppe med individuelle faktorer. De ulike gruppene har definerte faktorer, enten 12 prosent, 15 prosent eller 18 prosent. Gruppene defineres av de ulike inntektstypene. Vi finner at i en vanlig bank har man ofte en overvekt av inntekt i gruppene der 12 prosent er faktoren. Dermed blir kapitalkravet noe lavere enn dersom man hadde valgt basismetoden. Ser vi på et rent matematisk eksempel, dersom alle inntekter ligger i gruppen med 12 prosent, vil kapitalbehovet vært 20 prosent lavere med sjablongmetoden kontra basismetoden. Derfor kan man holde mindre kapital i henhold til regulatoriske krav og potensielt få relativt større avkastning på egenkapitalen. Dermed er det grunnlag for å si at det er bedre å benytte sjablongmetoden. Våre empiriske funn viser imidlertid at i overgangen til å benytte sjablongsmetoden må foretak varsle finanstilsynet, mens basismetoden er noe alle foretak kan benytte seg av. Et interessant funn som er viktig å trekke frem, er at det kommer

et nytt regelverk om kapitalbehov for operasjonell risiko i ferdigstilt Basel III, som forventes å inntre Norge tidligst i 2023. Da skal alle eksisterende metoder avvikles og erstattes med en felles metode. Metoden vil i stor grad ta hensyn til proporsjonalitet, som medfører at metoden blir enklere for mindre banker. Dette vil være hensiktsmessig ettersom kapitalkravsforskriften i dag kan være krevende for mindre banker.

5.2.3 Interaktivt styringssystem

Interaktivt styringssystem er det formelle systemet som ledelsen bruker for å involvere seg personlig og regelmessig i ansatte sine beslutningsaktiviteter (Simons, 1995b). Systemet kan derfor knyttes til risikostyring med utgangspunkt i hvordan virksomheter kommuniserer og diskuterer risiko. I dette delkapittelet vil vi derfor se på hvordan risiko blir kommunisert og diskutert i virksomhetene, samt hvordan man etablerer prosesser for å bringe deltakere fra forskjellige nivåer i virksomheten sammen.

Kommunikasjon og diskusjon på ulike nivåer

COSO (2017) trekker frem viktigheten av kommunikasjon knyttet til risiko. Fraser & Henry (2007) viser at diskusjon og debatt om risiko på alle nivåer i virksomheten vil bidra til økt forståelse og håndtering av risiko. Dette samsvarer med våre empiriske funn hvor flere virksomheter hevder at kommunikasjon og diskusjon er noe av det viktigste i risikostyring. Videre viser funn fra finansforetakene at risiko er en fin måte å kommunisere og diskutere mellom første- og andrelinje i virksomheten. Det er viktig at andrelinje innhenter verdifull informasjon fra førstelinje, ettersom førstelinje besitter mye informasjon som det er viktig at andrelinje har oversikt over. Konsulentselskapene hevder at det bør være et løpende samspill mellom første- og andrelinje, for å kunne redusere usikkerhet i virksomheten. Flere av virksomhetene hevder at dette samspillet er en viktig styringsmekanisme for operasjonell risiko. Dette finner vi imidlertid vil variere mellom virksomhetene.

Videre viser Fraser & Henry (2007) at kommunikasjon mellom styret, toppledelsen og ledelsen er kritisk for en effektiv implementering av helhetlig risikostyring. Våre empiriske funn fra fiskeri og infrastruktur viser at risiko blir kommunisert på øverste nivå i virksomhetene, og at risiko alltid er integrert i ledelse- og styremøter. Ifølge Sheehan (2010) er det viktig at virksomheter generer dialog og debatt om de viktigste risikoer i virksomheter for å oppnå et vellykket interaktivt styringssystem. Dette finner vi igjen i flere av

virksomhetene, hvor det har blitt etablert forum for å generere dialog og debatt rundt risikoene som er blitt identifisert. I disse risikoforumene møtes relevante personer for å diskutere problemstillinger som er blitt belyst, i tillegg til å kartlegge hvilke endringer som bør gjennomføres. Arbeidet fra risikoforumene må godkjennes av ledergruppen, før det deretter blir delt med styret. Dette samsvarer med Sheehan (2010) som mener det er ledelsen som skal sørge for at styret og toppledelsen får informasjon om de viktigste risikoene i virksomheten.

Våre empiriske funn viser at virksomhetene benytter ulike kanaler for diskusjon og debatt tilknyttet risiko, og for å kommunisere ut viktig informasjon mellom flere nivåer i virksomheten. Videre viser funn at flere av virksomhetene har etablert interne kommunikasjonsverktøy hvor ansatte oppfordres til å dele erfaringer om operasjonelle hendelser. På den måten får ansatte mulighet til å få innblikk om tidligere hendelser, hva som gikk galt og hvordan det har blitt håndtert. Flere av virksomhetene hevder at dette er avgjørende for å bidra til kompetansedeling og læring, og for å hindre at slike hendelser vil oppstå igjen. Virksomhetene innenfor fiskeri og infrastruktur mener at dette er spesielt avgjørende innenfor deres bransje. Dette skyldes at operasjonelle hendelser som oppstår i deres bransje kan medføre mer alvorlige konsekvenser, sammenlignet med hvilke konsekvenser som vil oppstå i andre bransjer. Dermed er det avgjørende å bevisstgjøre ansatte på tidligere hendelser.

Risk talk

Ifølge Power (2016) er det viktig å etablere prosesser for å bringe deltakere fra forskjellige nivåer i virksomheten sammen. Kaplan & Mikes (2016) viser til "risk talk" i arbeidet med å få risikostyring som en integrert del av de daglige forretningsaktivitetene. Risk talk kan foregå gjennom workshop og ansikt-til-ansikt møter. Ifølge Mikes & Kaplan (2014) er risikoworkshop en arena hvor risiko blir diskutert med formål om å identifisere de viktigste risikoene knyttet til å realisere virksomhetens mål. Flere av virksomhetene gjennomfører workshop hvor ansatte blir involvert. Empiriske funn viser at involvering av ansatte er viktig for å lykkes. Ved å involvere ansatte kan det bidra til ytterligere tanker og innspill, i tillegg til å kunne identifisere flere potensielle risikoer som kan oppstå i virksomheten. Ifølge Power (2016) og Mikes & Kaplan (2014) er det CRO som skal legge til rette for risikoworkshop. Dette samsvarer med våre funn fra finansforetakene som viser at sentrale roller i andrelinje er ansvarlig for å fasilitere workshop. Videre blir det rettet noe kritikk til risikoworkshop, ettersom det blir hevdet at risikoworkshop fungerer mer som en oppsummering av hva som

ble gjennomgått fra forrige workshop. Vi finner derfor at workshop kan erstattes eller suppleres med en intervjubasert metode, hvor man har samtaler "én til én". Denne metoden kan også kalles ansikt-til-ansikt møter (Kaplan & Mikes, 2016). Fordelen ved å benytte denne metoden er at virksomheter kan avdekke flere risikoer og få dypere innsikt i virksomheters risikobilde. Denne metoden er imidlertid mer ressurs- og tidskrevende for virksomheter.

5.2.4 Trossystem

Trossystemet er det eksplisitte settet med organisatoriske definisjoner som toppledere kommuniserer formelt og forsterker systematisk for å gi grunnleggende verdi, formål og retning for virksomheter. Ifølge Simons (1995b) vil trossystemet virke styrende ved at virksomheters kjerneverdier påvirker virksomheters kultur, og de ansattes holdning til å se muligheter. Knytter vi risiko opp til dette vil kjerneverdier til virksomheter påvirke risikokultur og risikoholdninger til ansatte.

Risikokultur

Mikes et al. (2017) viser at risikokultur reflekterer Simons (1995b) trossystem. Ifølge Power et al. (2013) definerer flere forfattere risikokultur som et element av organisasjonskultur. Dette blir også underbygget av flere av virksomhetene at risikokultur er en integrert del av organisasjonskulturen. Våre empiriske funn beskriver organisasjonskultur som måten virksomheten arbeider og tar beslutninger på, samt hvordan atferden er mellom ansatte i virksomheten. Ifølge konsulentselskapene er risikokultur mer knyttet til normer, holdninger og atferd relatert til risikostyring. Fra Institute of International Finance (2009) blir risikokultur definert som normer og tradisjoner for individer og gruppers atferd i en virksomhet som bestemmer måten de identifiserer, forstår, diskuterer og handler på bakgrunn av risikoen som virksomheten blir konfrontert med eller den risikoen de tar. Vi kan dermed konkludere med at våre empiriske funn og Institute of International Finance (2009) samsvarer.

Innenfor finansforetakene er det sentralt å skape en god risikokultur i enhver evaluering, ettersom primærproduktene deres er forbundet med mye risiko. Ifølge Finansforetaksloven (2015, §13-5), underliggende forskrifter og Baselkomiteens prinsipp 1, har styret det overordnede ansvaret og bør etablere en sterk risikostyringskultur i hele virksomheten (Finanstilsynet, 2016). Våre empiriske funn fra finansforetakene viser at risikokulturen har blitt betydelig bedre de siste årene. Det er flere av virksomhetene som viser at åpenhet og

læring av feil har vært viktig for å klare dette. Et godt eksempel er SMS-hendelsen i Sparebanken Vest fra februar 2021, hvor virksomheten i etterkant gikk gjennom den operasjonelle hendelsen og brukte hendelsen for å lære av feil. En slik håndteringen finner vi igjen fra andre virksomheter, hvor flere uttrykker at de har en kultur for å lære av feil. Videre finner vi samsvar mellom virksomhetene ved at flere har målsetting om å skape en sunn og god risikokultur, og at risikokultur er basert på åpenhet, transparens og kompetanse.

Videre viser våre empiriske funn at bevisstgjøring på risikokultur i hele virksomheten er viktig for å bygge en god risikokultur. Et godt eksempel innenfor fiskeri og infrastruktur viser at for å skape en god risikokultur har innrapportering vært et viktig virkemiddel. Det at virksomheten er bevisst og faktisk gjør noe med det som blir innrapportert er en viktig kulturbjelke. Et annet eksempel finner vi fra Bremnes Seashore. Virksomheten har opplevd stor effekt på risikokulturen ved å arbeide målrettet og systematisk for å gå bort fra "skulle bare" mentaliteten, til at ansatte er mer bevisst på bruk av utstyr og sikkerhet. På den måten har de klart å endre den tidligere kulturen, og det har videre medført at det har oppstått færre ulykker ute i felt. Disse eksemplene er interessante å sammenligne med Wiggen (2008), som hevder at utviklingen av risikokultur gir bevisstgjøring og bygging av kompetanse relatert til risikostyring. Våre funn viser at bevisstgjøring er viktig for å bygge en god risikokultur, mens Wiggen (2008) hevder at god risikokultur bidrar til bevisstgjøring. Vi kan dermed konkludere med at risikokultur ikke bare bidrar til bevisstgjøring, men at bevisstgjøring også vil være en forutsetning for å bygge en god risikokultur.

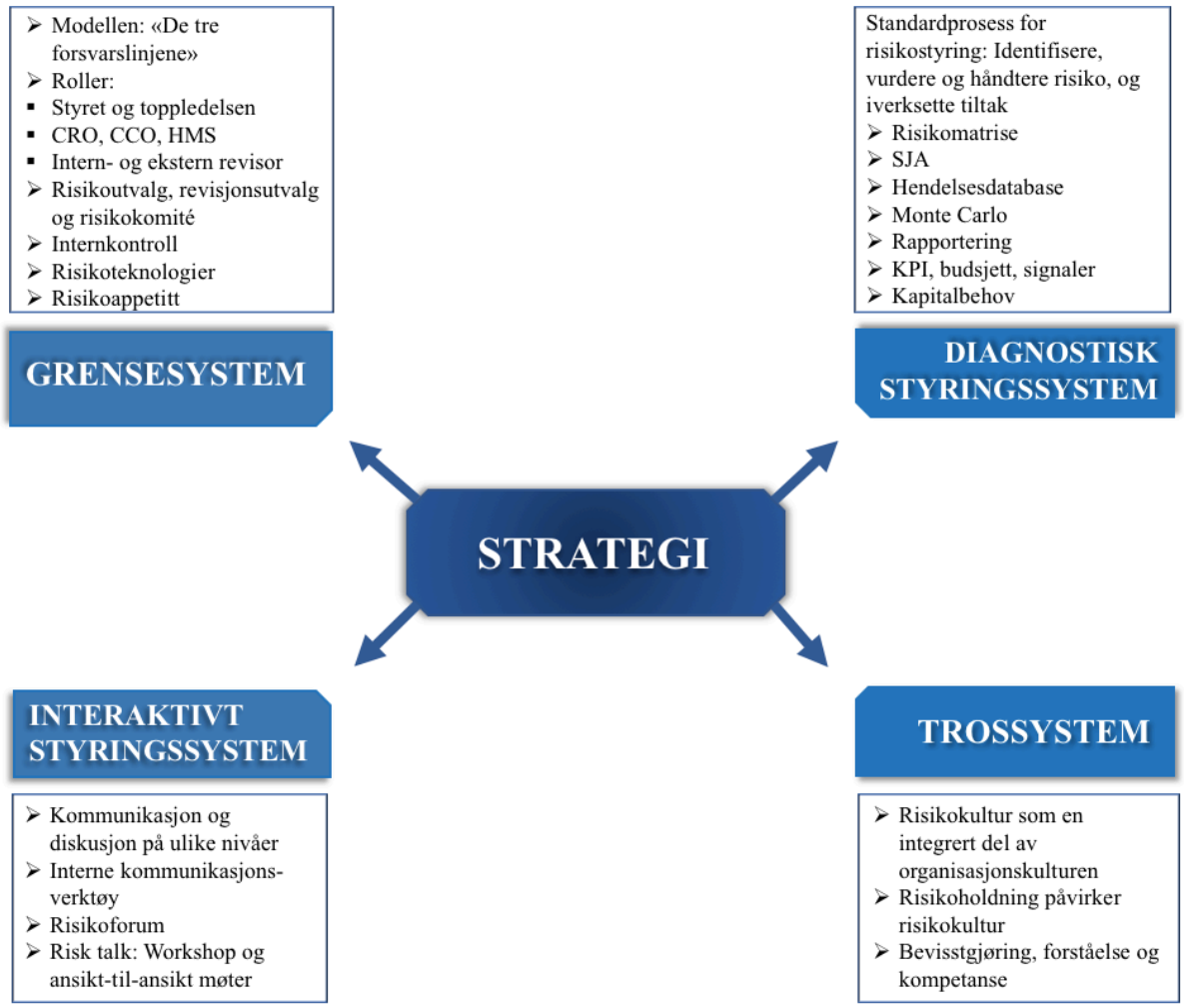
Våre empiriske funn viser imidlertid at det tar lang tid å bygge en god risikokultur. Eksemplene overfor viser til virksomheter med god risikokultur. Trekker vi inn andre empiriske funn, blir det uttrykt at noen virksomheter derimot er på et utviklingsnivå når det kommer til risikokultur. Funn viser at det er manglende kompetanse, spesielt på et høyere nivå. Dette fører til at risiko ikke blir prioritert i alle prosesser, men kun i de tilfeller det oppstår en operasjonell hendelse av betydning for virksomhetens omdømme eller økonomiske tap. Oppsummert finner vi at det er en betydelig forskjell mellom virksomheters risikokultur. Dette kan tenkes å ha en sammenheng med at enkelte virksomheter er betydelig mer modne på risikostyring og følgelig har klart å bygge opp en god risikokultur.

Risikoholdning

Våre empiriske funn viser at risikokultur er knyttet til normer, holdninger og atferd relatert til risikostyring i virksomheten, og dermed vil risikoholdning ha påvirkning på risikokulturen. Ifølge Mellemseter & Mørck (2006) defineres risikoholdning som en vurdering av hvor stor risiko det er ønskelig å ta, men dette blir imidlertid begrenset av definert risikoappetitt i virksomheten. Derfor finner vi at den enkeltes risikoholdning vil variere fra virksomhet til virksomhet, og fra ansatte til ansatte. Sammenligner vi ansatte som arbeider ute i felt innenfor fiskeri og infrastruktur vil de ha en annen risikoholdning, enn ansatte innenfor finansforetak som sitter på kontor. Det som imidlertid er felles for virksomhetene uavhengig av bransje er at det kan skapes en felles forståelse i virksomheten, ved å sette grenser for hvor stor risiko den ansatte i virksomheten har lov å ta (COSO, 2017). Våre empiriske funn viser at det er viktig at alle i virksomheten er bevisst på risikoene som virksomheten blir eksponert for, og at alle har forståelse og kompetanse for hvordan risiko skal håndteres. Dette uttrykker flere av virksomhetene vil bidra til å skape gode risikoholdninger, som videre vil være viktig for å bygge en god risikokultur. Videre mener Simons (1995a) at ledere bør gå foran som et godt eksempel på hvordan dette skal fungere. Det forutsetter at ledere må handle i tråd med kjerneverdier og normer, slik at de på den måten klarer å uttrykke at kjerneverdier er godt forankret i virksomheten (Simons, 1995a). Trekker vi dette i sammenheng med våre empiriske funn vil det være med å bidra til en felles forståelse av virksomhetens verdier og på den måten skapes det felles holdning til risiko i virksomheten.

5.2.5 Oppsummert

I dette kapittelet har vi undersøkt hvilke styringsmekanismer virksomhetene benytter for operasjonell risikostyring med utgangspunkt i det teoretiske rammeverket, Simons (1995b) *Levers of Control.* Vi finner likheter og ulikheter mellom virksomhetene, og hvilke styringsmekanismer som blir benyttet for operasjonell risiko. I Figur 8 har vi oppsummert hvilke styringsmekanismer virksomhetene vi har undersøkt benytter for operasjonell risiko.



Figur 8: Styringsmekanismer som virksomhetene benytter for operasjonell risikostyring

5.3 Avgjørende styringsmekanismer for god operasjonell risikostyring

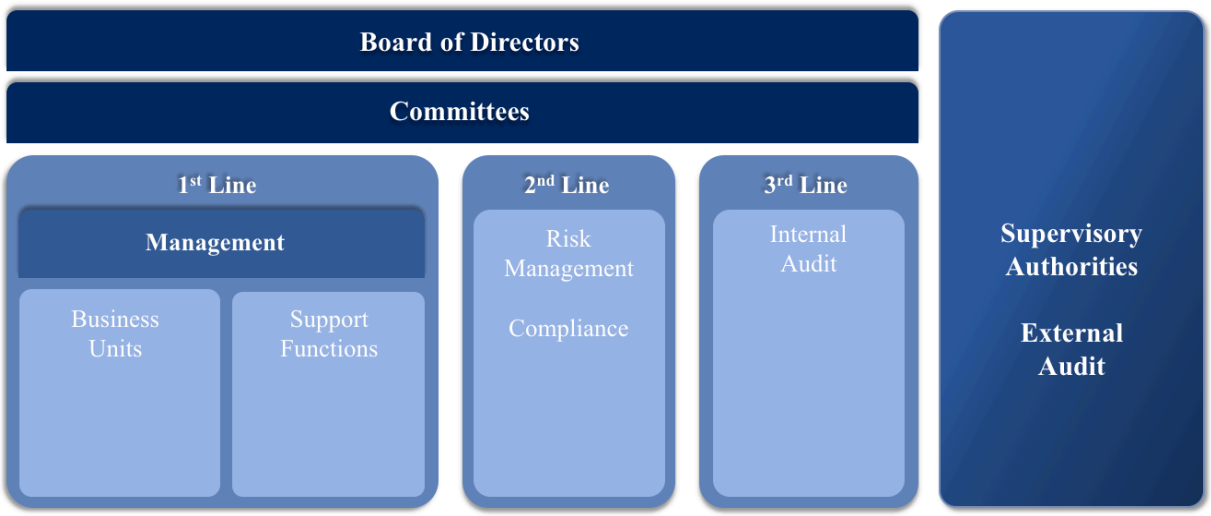
Tredje forskningsspørsmål "hvilke styringsmekanismer er avgjørende for god operasjonell risikostyring?" vil besvares med utgangspunkt i forskningsspørsmål 1 og 2, samt våre empiriske funn og tidligere forskningslitteratur. I det følgende vil vi dermed presentere styringsmekanismer som vil være avgjørende for god operasjonell risikostyring i virksomheter, uavhengig av bransje og størrelse.

5.3.1 Organisering og ansvarsforhold

Det er avgjørende at virksomheter organiserer og definerer ansvarsforhold på en slik måte at virksomheter kan drive med god operasjonell risikostyring. I det følgende vil vi presentere de tre forsvarslinjene og sentrale roller som er involvert i risikostyring i virksomheter.

De tre forsvarslinjene

Vi ønsker å presentere en modell for de tre forsvarslinjene (eng. three lines of defence), Figur 9, som virksomheter kan benytte for organisering av roller og ansvarsforhold for risikostyring på et overordnet nivå. Hensikten med å presentere denne modellen er å skape en oversiktlig og god forståelse av hvilke roller som er sentrale for risikostyring. I tillegg kan prinsippene i modellen fungere som et godt utgangspunkt for alle virksomheter uavhengig av bransje. Modellen er utviklet i samarbeid med konsulenten fra EY.



Figur 9: Three lines of defence

For å definere roller og ansvarsforhold i virksomheten kan det være hensiktsmessig å ta utgangspunkt i modellen. Selv om modellen kun er en standard og ikke benyttes av alle direkte, er likevel prinsippene i modellen viktig. Grunnen er at det er viktig å definere tydelig hvem i virksomheten som er risikoeier og hvem som skal kontrollere risikoeier. Innenfor finansforetakene er det førstelinje som er risikoeier, mens andrelinje har ansvar for å kontrollere førstelinje. Finansforetakene benytter modellen direkte, og har derfor definerte roller og ansvarsforhold mellom de tre linjene. På den måten har foretakene oversikt over

sentrale roller som er involvert i risikostyring og følgelig kontroll over ansvarsforholdet til hver enkelt. Vår undersøkelse viser at hvorvidt alle virksomheter trenger et like tydelig skille mellom linjene, er uvisst. Det som imidlertid er en avgjørende styringsmekanisme for organisering av roller og ansvarsforhold for risikostyring på et overordnet nivå er å utarbeide klare mandater og stillingsbeskrivelser, som er tilpasset virksomheten. På den måten vil det tydeliggjøre roller og ansvarsforhold som bidrar til at alle i virksomheten er sitt ansvar bevisst når det kommer til risikostyring.

Styret og toppledelsen

Styret har hovedansvar for hvordan hele prosessen for helhetlig risikostyring fungerer, mens toppledelsen står for den daglige ledelsen av helhetlig risikostyring (Beasley et al., 2015). For å opprettholde kontroll i virksomheten er det avgjørende at styret og toppledelsen har en inngående forståelse av sitt ansvar for risikostyring. Fraser & Simkins (2016) viser til en økning i styrets kompetanse om risikostyring, men at den likevel er langt fra tilstrekkelig. Flere studier avslører mangel på kompetanse på risiko, samt formål og verdi av risikostyring (Fraser & Simkins, 2016). Med utgangspunkt i dette vil en avgjørende styringsmekanisme for god operasjonell risikostyring være at styret og toppledelsen har kompetanse på risiko, og en fullstendig forståelse for hvordan virksomheten skal drive med operasjonell risikostyring.

Risikoutvalg, revisjonsutvalg og risikokomité

For å opprettholde kontroll i virksomheter er det sentralt å etablere risikoutvalg, revisjonsutvalg og risikokomité. Risikoutvalget kan være et underutvalg til styret og revisjonsutvalget kan være et saksforbedrende organ for styret. Risikokomité kan fungere som rådgiver for administrerende direktør. En av fordelene ved å etablere risikoutvalg og risikokomité er at det er andrelinje som fungerer som et rådgivende organ opp til komité og utvalg, og dermed muliggjør det at andrelinje kan presentere risikorapporter og vise til risikoanalyser som er gjennomført. Det vil bidra til økt kompetanse hos komité og utvalg, som dermed kan gi fordeler i form av kompetansedeling til styret og toppledelsen. I tillegg vil komité og utvalg kunne støtte opp under beslutninger som tas av styret og toppledelsen. Våre empiriske funn viser at noen av virksomhetene ikke har etablert slike utvalg og komiteer. For å styrke risikostyring i virksomheter vil det være avgjørende å etablerer risikoutvalg, revisjonsutvalg og risikokomité.

Andre sentrale roller som er involvert i risikostyring

En annen avgjørende styringsmekanisme for organisering og ansvarsforhold er å tydeliggjøre andre sentrale roller som er involvert i risikostyring. Dette behovet øker jo mer kritisk risikoene er i virksomheten. Empiriske funn viser at roller som CRO og CCO er involvert i risikostyring, i tillegg til roller innenfor HMS, økonomiavdeling, juridisk avdeling og kvalitetsstyring. Størrelse og type virksomhet vil avgjøre hvilke roller virksomheten ønsker å etablere. Tilsvarende påvirker det også hvilken funksjon virksomheten velger å plassere rollene innenfor. I de tilfeller virksomheten tar utgangspunkt i modellen for "de tre forsvarslinjene" vil det være naturlig å plassere rollene i andrelinjefunksjon (IIA, 2018). I andre tilfeller vil det være naturlig å heller etablerer miljøer for risikostyring, enn å plassere roller inn i en risikostyringsfunksjon. Uavhengig av hvor man velger å plassere rollene vil det likevel være viktig at det er et naturlig bindeledd mellom rollene og opp til styret og toppledelsen. Dette er en avgjørende styringsmekanisme ettersom disse rollene ofte innehar viktig informasjon som styret og toppledelsen må bli informert om.

En annen sentral rolle som er deltakende i virksomhetens risikostyring er internrevisor (Arena et al., 2010; IIA, 2018). Det er viktig å involvere internrevisor i arbeidet med risikostyring, ettersom internrevisor skal vurdere hele oppsettet for styret. Samtlige av virksomhetene plasser internrevisor i tredje forsvarslinje. IIA (2018) viser også til at tredje forsvarslinje utøves av internrevisor. En avgjørende styringsmekanisme er derfor å ha en internrevisor som gir en uavhengig vurdering av risikostyring til virksomhetens øverste organ. I tillegg er det avgjørende å ha en ekstern revisor som reviderer til myndighetene. Ekstern revisor gir en uavhengig bekreftelse av regnskapsrapportering (IIA, 2018). Det som imidlertid er viktig å poengtere er at virksomheter må være bevisst på at andre- og tredje forsvarslinje skal opptre uavhengig av enhetene de overvåker og kontrollerer. Det forutsetter at de ikke skal utføre arbeidsoppgaver som tillegger førstelinje, men kontrollerer og overvåker at arbeidsoppgaver utføres i henhold til eksterne og interne regler og rutiner. Dette er også sentralt for virksomheter som ikke benytter forsvarslinjene direkte.

Oppsummert

Oppsummert vil det være flere styringsmekanismer som er avgjørende for organisering og ansvarsforhold når det kommer til operasjonell risikostyring. En avgjørende styringsmekanisme vil være at styret og toppledelsen har fullstendig forståelse og kompetanse for hvordan man skal drive med risikostyring i virksomheten. En annen avgjørende styringsmekanisme vil være å tydeliggjøre sentrale roller som er involvert i risikostyring, i

tillegg til å utarbeide klare mandater og stillingsbeskrivelser. Til slutt vil det også være fordelaktig å etablere risikoutvalg, revisjonsutvalg og risikokomité for å opprettholde kontroll og styrke risikostyring i virksomheter.

5.3.2 Internkontroll

Det er hensiktsmessig at virksomheter gjennomfører internkontroll som en del av operasjonell risikostyring. Årsaken til dette er at operasjonell risiko kan oppstå som følge av uventede tap på grunn av utilstrekkelig internkontroll. I tillegg stilles det regulatoriske krav fra myndigheter til at virksomheter må gjennomføre internkontroll. Dermed vil en avgjørende styringsmekanisme for god operasjonell risikostyring være å ha systemer for internkontroll. Dette underbygger Jansrud (2017a), som hevder at styret bør utvikle og vedlikeholde robuste systemer for internkontroll med hensiktsmessige interne kontroller som dekker operasjonell risikokontroll i hele virksomheten. En annen avgjørende styringsmekanisme er at internkontroll gjennomføres av hele virksomheten, inkludert styret, ledelsen og ansatte. I tillegg er det avgjørende å etablere sentrale roller som er ansvarlig for internkontroll. Mange virksomheter velger også å benytte internrevisor for å være trygg på at internkontrollen fungerer (Jensen, 2015). Det er også helt avgjørende at internkontrollen er godt gjennomført og dokumentert, ettersom myndigheter kan gi pålegg hvis ikke internkontrollen er optimal.

5.3.3 Policy, rammeverk og appetitt

Virksomhetens strategi må samsvare med virksomhetens formål. Derfor er det viktig at virksomheten tar hensyn til strategi i utarbeidelse av policy og rammeverk, i tillegg til å inkludere virksomhetens risikoappetitt. Etter hvert som virksomheten blir bedre til å integrere risikostyring med strategi og måloppnåelse, vil det åpne opp muligheter for å styrke deres fleksibilitet og motstandsdyktighet.

Risikopolicyer

Risikopolicyer er hensiktsmessig å benytte for å formalisere risikostyring i virksomheter (Beasley et al., 2015; Fraser & Simkins, 2016). Dermed er en avgjørende styringsmekanisme at virksomheter utarbeider policyer for operasjonell risiko, som bør inneholde generelle prinsipper som skal bli styrt helhetlig. Det er styret som har ansvar for å fastsette prinsippene, ettersom prinsippene skal beskrive de øverste kravene som styret mener at virksomheten skal

forholde seg til. I prinsippene bør det fremgå hvem som er ansvarlig for risikostyring og hva som er virksomhetens risikoappetitt. Videre er det viktig at virksomheten skiller mellom policyer og rutiner, ettersom underliggende rutiner skal operasjonalisere de overordnede policyer. For å oppnå dette er det viktig å utarbeide rutinebeskrivelser, prosessbeskrivelser og underliggende dokumenter som skal svare på hvordan styringsprinsippene skal implementeres. Policyer bør også inneholde kvantifiserte rammer (Finanstilsynet, 2016; Jansrud, 2017a). Fraser & Simkins (2016) viser at totalt to til fire sider med beskrivelse bør være tilstrekkelig for en helhetlig risikostyringspolicy.

Risikorammeverk

En avgjørende styringsmekanisme for operasjonell risikostyring er å ta i bruk et risikorammeverk. De mest anerkjente og brukte risikorammeverkene er ISO og COSO. På verdensbasis har COSO blitt en mal for beste praksis for helhetlig risikostyring, og er et rammeverk som flere virksomheter benytter uavhengig av bransje og størrelse (Power, 2007). Andre virksomheter benytter seg av ISO31000, som inneholder prinsipper som gir veiledning til effektiv risikostyring. Det finnes også andre rammeverk og standarder som virksomheter må forholde seg til avhengig av bransje, størrelse og kompleksitet. Det vil derfor være hensiktsmessig at virksomheter utarbeider egne interne rammeverk for risikostyring, basert på eksisterende rammeverk, tilpasset den enkelte virksomhet (Fraser & Simkins, 2016; Lundqvist, 2014). Selv om flere virksomheter benytter seg av risikorammeverk, foreligger det likevel et stort potensial for mer omfattende bruk i fremtiden (COSO, 2017). Lengden som anbefales for rammeverkdokumentet er omtrent 10-15 sider for helhetlig risikostyring (Fraser & Skimkins, 2016).

Risikoappetitt

Risikoappetitt er det nivået av usikkerhet som en virksomhet har evne og er villig til å påta seg for å kunne gjennomføre sine aktiviteter og realisere sine mål (IIA, 2018). En avgjørende styringsmekanisme for virksomheter vil være at styret integrerer risikoappetitt i strategi slik at man har appetitt for ulike risikoer, og som videre blir besluttet i prinsipper og retningslinjer. Prinsippene bør dermed inneholde definert risikoappetitt for operasjonell risiko, hvor kritiske og høye risikoer i virksomheten skal reduseres gjennom implementering av ytterligere kontrolltiltak. Retningslinjer bør fastslå kritiske og høye risikoer som er uakseptable. Gjennom

dette fastsettes den faktiske risikoappetitten for operasjonell risiko (Deloitte, 2010). På den måten setter styret føring for hvilken toleranse virksomheten skal ha for operasjonell risiko.

Virksomheter bør ikke definere en helhetlig risikoappetitt for virksomheten, men mer spesifikt for den enkelte risiko. Grunnen er at man vil ha høyere toleranse for noen risikoer enn andre, som for eksempel innovasjon hvor det er viktig å ha en høyere toleranse for å muliggjøre at innovative idéer faktisk lar seg gjennomføre. Videre er det avgjørende at risikoappetitten kan operasjonaliseres, og at den er tydelig definert og formidlet i hele virksomheten. Det er også avgjørende at virksomheten kvalifiserer og kvantifiserer risikoappetitten. Finner virksomheten det utfordrende å kvantifisere er det spesielt viktig å utarbeide gode føringer for hvilke beslutningstagere som kan avgjøre hva som er riktig nivå av risiko, basert på de kvalitative vurderingene som foreligger (IIA, 2018).

Oppsummert finner vi at avgjørende styringsmekanismer for operasjonell risiko er at styret utarbeider risikopolicyer og risikorammeverk. Videre bør virksomheten etablere sitt eget rammeverk basert på eksisterende risikorammeverk, og tilpasse dette til virksomheten. I tillegg bør risikoappetitt integreres i strategi og det bør defineres tydelig risikoappetitt både kvalitativt og kvantitativt.

5.3.4 Standardprosess: identifisere, vurdere og håndtere operasjonell risiko

Standardprosessen for risikostyring omhandler å identifisere, vurdere og håndtere risiko forbundet med strategi (COSO, 2017). Med utgangspunkt i standardprosessen vil vi presentere hvordan virksomheter kan benytte risikoverktøy, rapportering og hendelsesdatabase som avgjørende styringsmekanismer for operasjonell risiko. I tillegg vil vi presentere andre metoder for kvantifisering av operasjonell risiko som kan benyttes som styringsmekanismer.

Risikoverktøy

Hvilke metoder og teknikker som er hensiktsmessig å benytte i risikostyring vil variere. Det tradisjonelle risikoperspektivet er å uttrykke operasjonell risiko som et produkt med sannsynlighet og konsekvens (Utne, 2020). For å gjøre dette benytter flere virksomheter seg av *risikomatrise* for å identifisere og vurdere operasjonell risiko. Det er imidlertid viktig å være klar over utfordringer med matrisen som omhandler når risikoen skal aksepteres eller ikke (Dujim, 2015). Det er nødvendig at virksomheter har en tydelig risikoappetitt for den enkelte risiko, som kan gjøre det enklere å avgjøre når risikoen skal aksepteres og ikke. Dette

vil også gjøre vurdering av risikoer mer objektiv for når virksomheten skal iverksette tiltak for å redusere risikonivået. Videre er en annen utfordring med matrisen at virksomheter har for mange risikoer og dermed ikke klarer å velge hvilke risikoer som skal prioriteres først (Dujim, 2015). Dermed er det avgjørende at virksomheter velger ut de mest sentrale risikoer som medfører størst konsekvens, i tillegg til å predefinere tiltak med tydelige ansvarsforhold. Disse må jevnlig følges opp og inkluderes i risikorapportering. I risikorapportering inkluderes ofte risikomatrisen, noe våre empiriske funn tilsier er uprofesjonelt. Dermed vil en *risikoliste* med et listeformat være et bedre alternativ. I risikolisten defineres alle risikoer i prioritert rekkefølge. I tillegg kan definerte risikoer visualiseres med en farget pil som indikerer risikonivået til den enkelte risiko og retningen på pilen indikerer forventet utvikling i neste periode, ofte 12 måneder. Det bør også foreligge en refleksjon rundt årsak, hendelse, konsekvens og integrerende tiltak som har blitt etablert for håndtering. Sammenlignet med en risikomatrise vil en risikoliste dermed gjøre det enklere å rapportere og forstå risikobildet av virksomheten.

Hendelsesdata

Det å registrere hendelser i en hendelsesdatabase er avgjørende i operasjonell risikostyring. Alle virksomheter, uavhengig bransje, bør ha en egen hendelsesdatabase for å muliggjøre at hendelser kan linkes til hverandre ved identifisering og vurdering av risiko. På den måten blir det enklere å vurdere sannsynlighet og konsekvens basert på tidligere hendelser som er registrert. Det forutsetter imidlertid at virksomheter oppfordrer ansatte til å kontinuerlig registrere hendelser. Videre bør virksomheter rette sin oppmerksomhet på hendelser med lav frekvens og høy konsekvens, det vil si ekstreme, men ikke usannsynlige hendelser da disse hendelsene kan medføre store tap for virksomheter. I tillegg bør virksomheter vurdere potensielle hendelser og ikke bare faktiske hendelser (Finanstilsynet, 2016). Etter hvert som virksomheter blir modne og bygger opp hendelsesdatabase kan de gjennomføre Monte Carlo simulering.

Andre metoder for å kvantifisere operasjonell risiko

Det vil være avgjørende for virksomheter å kvantifisere operasjonell risiko, men dette kan være utfordrerne. Derfor vil vi presentere andre metoder enn bare risikomatrise og hendelsesdata som virksomheter kan benytte for kvantifisering av operasjonell risiko.

En metode for å kvantifisere operasjonell risiko er å benytte KPI. Virksomheter kan benytte KPI for å identifisere operative delmål på nivå som gjør at de ansatte ser verdi av KPI. Dette kan danne rammebetingelser for andre aktiviteter i virksomheter. Det vil derfor være avgjørende at virksomheter velger riktige KPI-er for måloppnåelse. Vi ønsker også å presentere Key Risk Indikators (KRI) som virksomheter kan utarbeide og som er økende i alle bransjer. KRI er begrensninger som ledelsen kan bruke til å vise hvor risikabel en aktivitet er, for eksempel i et prosjekt eller i en investering (Vig & Hallaråker, 2006; Davies et al., 2006). KRI kan dermed fungere som "føre var" signaler, som angir hvordan risikoer sannsynligvis vil påvirke forretningsresultater. I tillegg kan KRI være nyttig til å støtte oppunder beslutninger og handlinger. Det å ta i bruk KRI vil gjøre virksomheter mer fremtidsrettet og vil kunne gi en indikasjon på handlinger som det må iverksettes tiltak til. På den måten kan dette bidra til å redusere risikoer og gi et tydeligere risikobilde for virksomheter. Det er imidlertid viktig å poengtere at KRI ikke nødvendigvis fungerer med en gang. Derfor må virksomheter prøve og feile for å bygge riktige KRI (Vig & Hallaråker, 2006).

En annen metode for å måle og overvåke operasjonell risiko kan være å integrere operasjonell risiko i budsjett. Videre bør virksomheter bli flinkere til å integrere budsjettprosessen i de øvrige planleggingsprosessene: strategi, policyer, rammeverk og andre operasjonelle styringsdokumenter. Dette fordi de fleste virksomheter i dag utarbeider budsjetter først, og deretter lager årets operasjonelle planer for virksomheter uten at disse i etterkant sammenstilles med budsjettet. Eller motsatt, at operasjonelle planer legges først og deretter utarbeides budsjettet uten at det sammenstilles (KPMG, 2017). Derfor vil det være avgjørende å integrere budsjettprosessen i øvrige planleggingsprosesser.

En tredje metode for å kvantifisere operasjonell risiko finner vi hos finansforetakene. Finansforetakene beregner kapitalbehov for operasjonell risiko og viser til operasjonelle tap i sine risikorapporter. Vi finner at sjablongmetoden er bedre enn basismetoden og AMA-metoden, ettersom man kan holde mindre kapital i henhold til regulatoriske krav og potensielt få større avkastning på egenkapitalen. Imidlertid er det enklere å benytte basismetoden ettersom denne ikke må varsles til finanstilsynet. Derfor starter ofte de fleste virksomheter med basismetoden før man eventuelt går over til sjablongmetoden. Imidlertid er det viktig å påpeke at eksisterende beregningsgrunnlag skal avvikles og erstattes med en felles metode som forventes å inntre tidligst i 2023.

Oppsummert finner vi at avgjørende styringsmekanismer for god operasjonell risikostyring er å benytte risikomatrise, risikolister i rapportering, registrering av hendelsesdata og predefinere tiltak med tydelig ansvarsforhold. I tillegg kan virksomheter kvantifisere operasjonell risiko ved andre metoder som KPI, KRI og budsjett. Finansforetakene kan i tillegg beregne kapitalbehov for operasjonell risiko. Vi finner imidlertid at virksomheter bør veie opp kvantitative indikatorer mot kvalitative, og ledelsens kvalitative vurderinger bør veie like mye som de kvantitative ved operasjonell risiko.

5.3.5 Kommunikasjon, kompetanse og kultur

En studie fra Universitet i Stavanger fra 2012 viste at ulike risikoperspektiver påvirker risikokommunikasjon, og at det kan forårsake barrierer og problemer i kommunikasjonen i virksomheter. Konklusjonen av studien var at de som innehar roller for å vurdere og ta beslutninger om risiko utførte dette uten tilstrekkelig kompetansegrunnlag (Utne, 2020). Trekker vi dette i lys av vår undersøkelse fremkommer det at virksomhetene arbeider systematisk og målrettet for å bygge opp kompetanse i virksomheten, slik at alle innehar samme forståelse av virksomhetens risikobilde. Med utgangspunkt i studien og våre funn tyder det på at noe av det mest avgjørende virksomheten gjør innenfor operasjonell risikostyring, er å kontinuerlig bygge opp kompetanse i hele virksomheten. Vi finner at avgjørende styringsmekanismer for å bygge kompetanse kan være å benytte risikoverktøy, hendelsesdatabase og annen overvåking, som kan bidra til økt forståelse av virksomhetens risikobilde. I tillegg vil det være hensiktsmessig at virksomheten implementerer et internt kommunikasjonsverktøy for å tilrettelegge for debatt og diskusjon tilknyttet risiko, og for å kommunisere ut viktig informasjon om risikoer mellom alle nivåer i virksomheten. Følgelig kan dette bidra til kompetansedeling, læring og bevisstgjøring av ansatte.

Videre kan det være fordelaktig å gjennomføre risikoworkshop for å identifisere de viktigste risikoene som er knyttet til å realisere virksomhetens mål (Mikes & Kaplan, 2014). Gjennomføring av workshop vil også bidra til å bygge kompetanse og bevisstgjøre ansatte på virksomhetens risikobilde. En forutsetning for vellykket workshop er å ha godt formulerte mål og oversikt over målene, samt en felles forståelse av virksomheten. Direktorat for Økonomistyring (2021b) hevder at selv om mål og risikoer gjerne ikke er på plass før workshop gjennomføres, er det viktig med kompetanse om hvordan mål og risiko bør formuleres. Videre finner vi at det kan være fordelaktig å benytte ansikt-til-ansikt møter for å

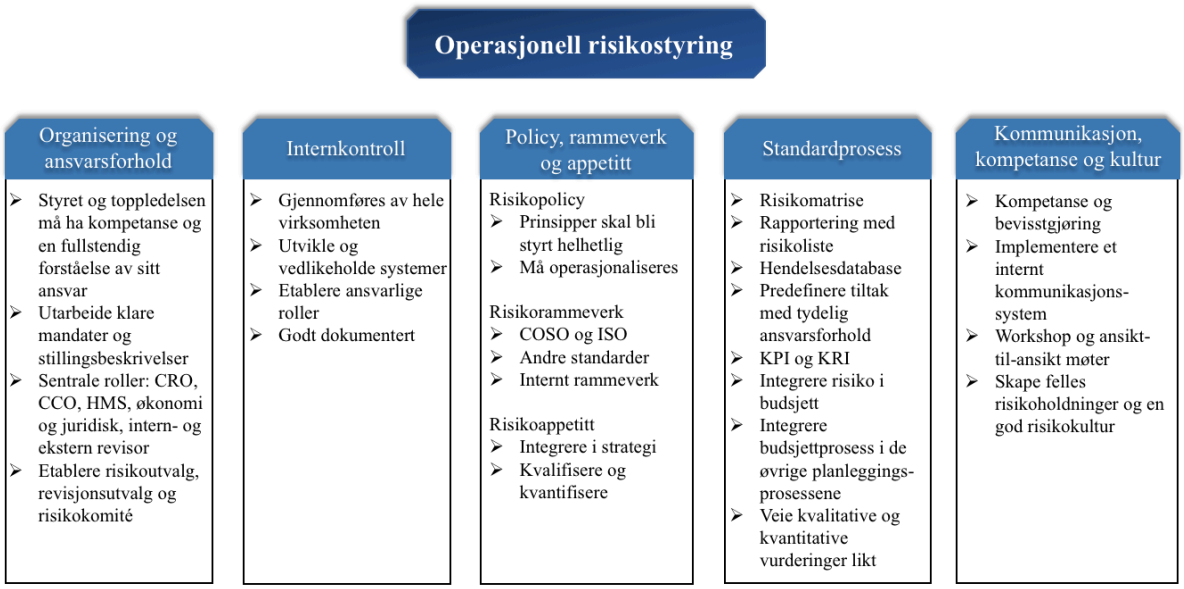
identifisere enda flere risikoer, og dette gjerne ved en intervjubasert metode. Dette er imidlertid ressurskrevende, men vil bidra til et enda tydeligere risikobilde av virksomheten.

Et annet element som er viktig for å bygge opp kompetanse i virksomheten er å definere begrepet "risiko". Begrepet defineres på ulike måter, ettersom individer og virksomheter har ulik holdning og forståelse av begrepet. I tillegg bruker virksomheter begrepet for lite og flere frykter begrepet. Årsaken til dette kan være at begrepet involverer både negative og positive effekter. Derfor er det viktig å definere begrepet "risiko" internt i virksomheten slik at alle har en felles forståelse for hva virksomheten legger i det. Videre vil det være med å bidra til å skape en felles risikoholdning. Tilsvarende vil det å bygge opp kompetanse og forståelse om risiko i virksomheten bidra til å skape en god risikokultur. I tillegg vil bevisstgjørelse av ansatte være en forutsetning for å bygge en god risikokultur. Det er avgjørende å skape en god risikokultur, ettersom den omhandler normer og tradisjoner for individer og gruppers atferd i en virksomhet. Det bestemmer hvordan ansatte identifiserer, forstår, diskuterer og handler på bakgrunn av risikoen som virksomheten blir konfrontert med eller den risikoen de tar (Institute of International Finance, 2009).

Oppsummert finner vi at noe av det mest avgjørende virksomheter gjør innenfor operasjonell risikostyring er å bygge kompetanse. For å bygge kompetanse og skape forståelse av risikobildet i virksomheter vil risikoverktøy, hendelsesdatabase, overvåking og implementering av et godt internt kommunikasjonssystem være avgjørende styringsmekanismer for god operasjonell risikostyring. På den måten kan man tilrettelegge for diskusjon og involvering i alle ledd i virksomheten. Dette vil også bidra til å skape felles risikoholdninger og en god risikokultur i virksomheten.

5.3.6 Oppsummert

I dette kapittelet har vi diskutert og redegjort for avgjørende styringsmekanismer som virksomheter kan benytte for god operasjonell risikostyring. Basert på våre empiriske funn, forskningslitteratur og tidligere analyse har vi utarbeidet en visuell fremstilling over det vi finner er avgjørende styringsmekanismer for god operasjonell risikostyring. Dette er illustrert i Figur 10. Presenterte styringsmekanismer vil bidra til god operasjonell risikostyring og på den måten kan virksomheter benytte styringsmekanismene for å redusere operasjonelle risikoer, som vi avdekket i forskningsspørsmål 1.



Figur 10: Avgjørende styringsmekanismer for god operasjonell risikostyring

6.0 Avslutning

I dette kapittelet vil vi konkludere studiens funn. Delkapittel 6.1 vil besvare vår problemstilling og delkapittel 6.2 inneholder forslag til videre forskning.

6.1 Konklusjon

Vår problemstilling er *hvordan integrere operasjonell risikostyring i virksomhetsstyringen?* Vi søker å besvare problemstillingen ved å besvare våre tre forskningsspørsmål.

6.1.1 Første forskningsspørsmål: Hvilke operasjonelle risikoer oppstår i virksomheter?

Basert på våre empiriske funn og tidligere forskningslitteratur har vi undersøkt hvilke operasjonelle risikoer som oppstår i tolv virksomheter. Innenfor fiskeri og infrastruktur vil operasjonelle risikoer som oppstår hovedsakelig være tilknyttet personskade, HMS og i verste fall fare for liv og helse. Innenfor finansforetakene vil operasjonelle risikoer som oppstår være svikt i prosesser, eksterne hendelser eller brudd på lover og regler, som kan medføre økonomiske tap eller regulatoriske sanksjoner. Studiens funn viser dermed at hvilke operasjonelle risikoer som oppstår i virksomhetene vil avhenge av bransje, størrelse og kompleksitet. Operasjonelle risikoer som er felles for alle virksomhetene uavhengig av bransje, er personvern og IT- og cyber sikkerhet. I tillegg har Covid-19 medført en økning av operasjonelle hendelser i alle virksomhetene.

Videre viser funn at operasjonell risiko er et vidt fagfelt og går på tvers av flere risikoklasser. Et funn som skiller seg ut, er omdømmerisiko som ikke er en operasjonell risiko, men at operasjonelle hendelser kan påvirke omdømme. Retter vi blikket mot effekter av operasjonelle risikoer finner vi at det utelukkende gir negative effekter. Studiens funn viser imidlertid at et utelukkende fokus på negative effekter hindre virksomheter i å se muligheter som risikoer kan gi. For å oppnå positive effekter forutsetter det at virksomheter etablerer styringsmekanismer, som diskutert og redegjort for i forskningsspørsmål 2 og 3.

6.1.2 Andre forskningsspørsmål: Hvilke styringsmekanismer benytter virksomheter for operasjonell risikostyring?

Med utgangspunkt i våre empiriske funn og det teoretiske rammeverket, Simons (1995b) *Levers of Control,* har vi undersøkt hvilke styringsmekanismer virksomhetene benytter for operasjonell risikostyring. Som et resultat av drøftelsen i forskningsspørsmål 2 har vi videreutviklet det teoretiske rammeverket, presentert i Figur 8.

Innenfor *grensesystemet* finner vi at organisering og ansvarsforhold for risikostyring på et overordnet nivå vil være avhengig av bransje og størrelse. Finansforetakene benytter modellen for "de tre forsvarslinjene". Fiskeri og infrastruktur benytter ikke modellen direkte, men studiens funn viser at organiseringen fungerer i stor grad på samme måte. Tilsvarende varierer det hvem som har det overordnende ansvaret for risikostyring i virksomhetene. Funn viser at det som oftest er toppledelsen og styret som har det overordnede ansvaret, i andre tilfeller er det administrerende direktør. Videre er andre sentrale roller som er involvert i risikostyring; CRO, CCO, HMS-ansvarlig og/eller økonomiavdeling, samt intern- og ekstern revisor. Flere av virksomhetene har også etablert utvalg og komité for å opprettholde kontroll for risikostyring. I tillegg gjennomfører virksomhetene internkontroll. Funn fra studien viser at virksomhetene har implementert internkontrollsystemer og etablert sentrale roller for internkontroll.

For å formalisere helhetlig risikostyring utarbeider virksomhetene risikopolicyer og risikorammeverk. Risikopolicyer omhandler hvordan ansatte skal arbeide og håndtere risiko, mens risikorammeverk skal hjelpe virksomhetene å ta riktig risiko, på riktig nivå. Studiens funn viser at virksomhetene utvikler egne risikorammeverk basert på eksisterende rammeverk som for eksempel COSO og ISO. Imidlertid kan det være andre standarder som er mer førende. Videre integrerer virksomhetene risikoappetitt i strategi som setter føring, mål og rammer. I tillegg er noen av virksomhetene mer regulert enn andre og dermed kan lovverk i seg selv sette grenser.

Videre benytter virksomhetene *diagnostiske styringssystemer* for å identifisere, vurdere og håndtere operasjonell risiko. Samtlige av virksomhetene benytter risikomatrise for å identifisere og vurderer operasjonell risiko. Risikomatrisen og virksomheters risikoappetitt skal bidra i vurderingen om risikoen skal aksepteres eller ikke. Skal virksomhetene iverksette tiltak er det avgjørende at risikofaktoren er konkret, slik at det er mulig å relatere hendelser til

den enkelte risikofaktoren. I forlengelsen av dette er det flere av virksomhetene som har etablert hendelsesdatabase. Studiens funn viser hovedsakelig at det er innenfor fiskeri og infrastruktur at hendelsesdata blir benyttet. I senere tid har også finansforetakene begynt å registrere hendelser. Risikomatrise og hendelsesdatabase har vært et viktig bidrag til virksomheters løpende rapportering til styret. I tillegg benytter virksomhetene andre metoder for å kvantifisere operasjonell risiko, som for eksempel KPI og budsjett. Finansforetakene vurderer også kapitalbehov for operasjonell risiko.

Det *interaktive styringssystemet* knyttes til risikostyring med utgangspunkt i hvordan virksomhetene kommuniserer og diskuterer risiko. Samtlige av virksomhetene ønsker at risiko skal bli kommunisert og diskutert på alle nivåer i virksomheten. Årsaken til dette er at bevisstgjøring på alle nivå og formidling om at alle har like mye ansvar for risiko ikke kommer tydelig nok frem i virksomhetene. For å involvere ansatte på alle nivåer i virksomheten blir det etablert risikoforum, risikoworkshop og ansikt-til-ansikt møter. Flere av virksomhetene har i tillegg etablert interne kommunikasjonssystemer. På den måten arbeider virksomhetene kontinuerlig for å bevisstgjøre ansatte. Innenfor *trossystemet* er virksomhetene opptatt av å bygge en god risikokultur som er basert på åpenhet, transparens og kompetanse. Det tar imidlertid lang tid å bygge opp en god risikokultur og flere av virksomhetene er fremdeles på et utviklingsnivå. Funn fra studien viser at det er manglende kompetanse, spesielt på et høyere nivå. Dette fører til at risiko ikke blir prioritert i alle prosesser, men kun i de tilfeller det oppstår en operasjonell hendelse av betydning for virksomhetens omdømme eller økonomiske tap. I tillegg viser funn fra studien at risikoholdning påvirker risikokulturen. Dermed er det viktig å skape en felles forståelse av virksomheters verdier, slik at det på den måten skapes en felles holdning i virksomheten.

6.1.3 Tredje forskningsspørsmål: Hvilke styringsmekanismer er avgjørende for god operasjonell risikostyring?

Med utgangspunkt i drøftelsen fra forskningsspørsmål 1 og 2, og tidligere forskningslitteratur har vi kommet frem til hvilke styringsmekanismer som er avgjørende for god operasjonell risikostyring. Som et resultat av drøftelsen i forskningsspørsmål 3 utarbeidet vi en visuell fremstilling, presentert i Figur 10.

En avgjørende styringsmekanisme omhandler organisering og ansvarsforhold. Styret og toppledelsen bør ha en fullstendig forståelse og kompetanse for hvordan man skal drive med

god operasjonell risikostyring i virksomheten. I tillegg er det viktig å tydeliggjøre andre sentrale roller som er involvert i risikostyring, og utarbeide klare mandater og stillingsbeskrivelser. Det vil være avgjørende å etablere risikoutvalg, revisjonsutvalg og risikokomité for å opprettholde kontroll og styrke risikostyring i virksomheten. En annen avgjørende styringsmekanisme for god operasjonell risikostyring er internkontroll. Det er viktig at internkontrollen er godt dokumentert og blir gjennomført av alle i virksomheten.

Videre er avgjørende styringsmekanismer for god operasjonell risikostyring å utarbeide risikopolicyer og risikorammeverk, samt definere virksomhetens risikoappetitt. I tillegg er det avgjørende å identifisere, vurdere og håndtere operasjonell risiko ved hjelp av risikovektøy og hendelsesdatabase. Det er imidlertid viktig at virksomhetene veier opp kvantitative indikatorer mot kvalitative, og ledelsens kvalitative vurderinger bør veie like mye som de kvantitative ved operasjonell risiko. For å rapportere risiko er det hensiktsmessig å rapportere i et listeformat hvor risikoer blir forstått og det foreligger en refleksjon om selve hendelsen, konsekvens og integrerende tiltak.

Andre avgjørende styringsmekanismer for god operasjonell risikostyring omhandler kommunikasjon, kompetanse og kultur. En forutsetning for å lykkes er at ledelsen legger til rette og involverer alle ledd for diskusjon og kommunikasjon om sentrale risikoer som kan oppstå. Videre vil det å benytte risikoverktøy, hendelsesdatabase, overvåking og implementering av et godt internt kommunikasjonssystem være avgjørende for å bygge kompetanse og forståelse av risikobildet i virksomheten. I tillegg vil det være fordelaktig å gjennomføre workshop og ansikt-til-ansikt møter, ettersom det vil være med å bidra til bevisstgjørelse av alle ansatte i virksomheten. Gjennomgående viser studiens funn at operasjonell risikostyring må inkluderes i alle prosesser og på alle nivåer i virksomheten. På den måten vil det bidra til å skape felles risikoholdninger og en god risikokultur i hele virksomheten.

6.1.4 Problemstilling: Hvordan integrere operasjonell risikostyring i virksomhetsstyringen?

For å konkludere og svare på vår problemstilling, *hvordan integrere operasjonell risikostyring i virksomhetsstyringen?* finner vi at operasjonell risikostyring integreres med virksomhetsstyring gjennom (1) organisering og ansvar, (2) internkontroll, (3) policy, rammeverk og appetitt, (4) standardprosess og (5) kommunikasjon, kompetanse og kultur.

Innenfor hvert av disse elementene har vi i denne utredningen presentert ulike styringsmekanismer som virksomheter kan benytte for å integrere operasjonell risikostyring i virksomhetsstyringen, oppsummert i Figur 10.

Vår utredning bidrar med en visuell fremstilling som presenterer avgjørende styringsmekanismer for god operasjonell risikostyring, Figur 10. Til helhetlig risikostyring og operasjonell risikostyring bidrar utredningen med en flercasestudie av tolv virksomheter. I tillegg bidrar utredningen med økt kunnskap om hvordan operasjonell risikostyring kan integreres med virksomhetsstyringen, som også vil kunne anvendes av praktikere som ønsker å integrere operasjonell risikostyring i virksomhetsstyringen.

6.2 Videre forskning

For å få en bedre forståelse av operasjonell risikostyring som en integrert del av virksomhetsstyringen kunne det vært interessant å utforske studiens tematikk ytterligere. I denne sammenheng oppfordrer vi til forskning som går ytterligere i dybden på operasjonell risikostyring integrert i virksomhetsstyringen. Ved å benytte flercasestudie har vi ikke hatt mulighet til å gå i dybden på hver enkelt virksomhet og bransje. Dermed oppfordrer vi til å studere en bransje eller en virksomhet for å utforske fenomenet ytterligere.

Det er også interessant å gjøre en studie på Covid-19 for å se hvilke effekter Covid-19 har hatt på operasjonell risikostyring. I tillegg til hvilke nye reguleringer og retningslinjer som er blitt etablert som følge av krisen. Dette med bakgrunn av at Covid-19 har medført økning av operasjonelle hendelser, som har ført til at operasjonell risikostyring er blitt satt høyere på agendaen. Videre oppfordrer vi til å gjennomføre en studie på det nye regelverket som ferdigstilles i Basel III om kapitalbehov for operasjonell risiko, som forventes å inntre Norge tidligst i 2023. Her skal alle eksisterende metoder avvikles og erstattes med kun en felles metode, som i stor grad hensyntar proporsjonalitet og vil gjøre det enklere for mindre banker. Dermed er det interessant å kunne se hvilke effekter dette vil ha, spesielt på mindre banker.

Litteraturliste

Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of enterprise risk management. *Accounting, Organizations and Society*, *35*(7), 659-675.

Arena, M., Arnaboldi, M., & Palermo, T. (2017). The dynamics of (dis) integrated risk management: A comparative field study. *Accounting, Organizations and Society*, *62*, 65-81.

Barfield, R. (2007). Risk appetite–How hungry are you. *The journal: Special risk management edition*, 8-13.

Beasley, M. S., Branson, B., & Hancock, B. (2017). The state of risk oversight: an overview of enterprise risk management practices. Survey report, AICPA and North Carolina State University.

Beasley, M., Branson, B., & Pagach, D. (2015). An analysis of the maturity and strategic impact of investments in ERM. *Journal of Accounting and Public Policy*, *34*(3), 219-243.

Beasley, M. S., Clune, R., & Hermanson, D. R. (2005). Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. *Journal of accounting and public policy*, *24*(6), 521-531.

Board, F. S. (2014). Guidance on supervisory interaction with financial institutions on risk culture: a framework for assessing risk culture. *April*, *7*, 1.

Bragelien, I. (2015). Risikostyring. *Magma, 8*(2015), 14-16.

BKK (u.å.) *Temaside.* https://www.bkk.no/temaside/ab07b13b-561d-4341-b546-6222f3b5247c

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. *Long range planning*, *48*(4), 265-276.

Chapelle, A. (2019). *Operational risk management: Best practices in the financial services industry*. John Wiley & Sons.

Coso, I. I. (2004). Enterprise risk management-integrated framework. *Committee of Sponsoring Organizations of the Treadway Commission*, *2*.

COSO (Committee of Sponsoring Organizations of the Treadway Commission). (2013) *Internkontroll – et integrert rammeverk.* https://www.finansmarkedsfondet.no/contentassets/b0a3fc4ee0e74a879b0fad979c2d2d34/sluttrapport_rammeverk-for-intern-styring-og-kontroll-nirf_2013-2014.pdf

COSO (Committee of Sponsoring Organizations of the Treadway Commission). (2017) *Enterprise Risk Management - Integrating with Strategy and Performance.* https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-andPerformance-Executive-Summary.pdf

Cox Jr, L.A. (2008). What's wrong with risk matrices?. *Risk Analysis: An International Journal*, *28*(2), 497-512.

Davies, J., Finlay, M., McLenaghen, T., & Wilson, D. (2006). Key risk indicators–their role in operational risk management and measurement. *ARM and RiskBusiness International, Prague*, 1-32.

Deloitte. (2010). *Uavhengig attestasjonsoppdrag for Norges Banks representantskap vedrørende risikostyringen i Norges Bank Investment Management. Oppdraget omfatter en gjennomgang av utforming og implementering av organisasjonsstruktur og rammeverk for styring av operasjonell risiko.* https://www.norges-bank.no/contentassets/c80274266a8f496cbebad44b2045cd04/attestasjonsprosjekt_rapport.pdf

Deloitte. (2014). Risk appetite frameworks. *How to spot the genuine article.* https://www2.deloitte.com/content/dam/Deloitte/au/Documents/risk/deloitte-au-risk-appetiteframeworks-0614.pdf

Direktoratet for forvaltning og økonomistyring (2021a). *Sammenheng mellom risikostyring og internkontroll*. https://dfo.no/fagomrader/risikostyring/sammenhengen-mellom-risikostyring-og-internkontroll

Direktorat for forvaltning og økonomistyring (2021b). *Hva er en risikoworkshop?* [Lysarkpresentasjon]. https://dfo.no/fagomrader/risikostyring/verk%C3%B8y-til-risikostyring

Duijm, N. J. (2015). Recommendations on the use and design of risk matrices. *Safety science*, *76*, 21-31.

Eriksen, J. (2017). *Krise- og beredskapsledelse: teamtrening*. Cappelen Damm akademisk.

Finansforetaksloven. (2015). *Lov om finansforetak og finanskonsern* (LOV-2015-04-10-17). Lovdata. https://lovdata.no/lov/2015-04-10-17/§1-3

Finansforetaksloven (2015). *Lov om finansforetak og finanskonsern* (LOV-2015-04-10-17). Lovdata. https://lovdata.no/lov/2015-04-10-17/§13-5

Finansforetaksloven (2015). *Lov om finansforetak og finanskonsern* (Lov-2015-04-10-17). Lovdata. https://lovdata.no/lov/2015-04-10-17/§13-6

Finanstilsynet (2019). *IAAP-rapport.* https://www.finanstilsynet.no/rapportering/fellesrapporteringer/icaap-rapport/?parent=1974

Fiskeridirektoratet (u.å.). *Om oss.* https://www.fiskeridir.no/Om-oss

Flage, R., & Røed, W. (2012, June). A reflection on some practices in the use of risk matrices. In *11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference* (pp. 881-891).

Fraser, I., & Henry, W. (2007). Embedding risk management: structures and approaches. *Managerial Auditing Journal*.

Fraser, J. R., & Simkins, B. J. (2016). The challenges of and solutions for implementing enterprise risk management. *Business horizons*, *59*(6), 689-698.

Giovannoni, E., Quarchioni, S., & Riccaboni, A. (2016). The role of roles in risk management change: The case of an Italian bank. European Accounting Review, 25(1), 109-129.

Glomseth, R. (2019). Hva er organisasjonskultur, og hvorfor bry seg med den? *Magma, 2*(2019)*,* 11-14.

Hagness, K., Vatne, M., & Nordheim, K. (2014). Effektiv virksomhetsstyring. *Magma-Econas tidsskrift for økonomi og ledelse, 4*(2014), 34-38.

Hayne, C., & Free, C. (2014). Hybridized professional groups and institutional work: COSO and the rise of enterprise risk management. *Accounting, Organizations and Society*, *39*(5), 309-330.

Hillson, D., & Murray-Webster, R. (2011). Using risk appetite and risk attitude to support appropriate risk-taking: a new taxonomy and model. Journal of Project, Program & Portfolio Management, 2(1), 29-46.

IIA. (2015). *Veileder for compliancefunksjonen.* https://iia.no/wp-content/uploads/2019/09/2017-Veiledning-for-Compliancefunksjonen.pdf

IIA (2018). *Veileder for risikostyringsfunksjonen.* https://iia.no/wp-content/uploads/2019/09/2018-Veileder-for-Risikostyringsfunksjonen.pdf

IIA (2019). *Veileder for virksomhetsstyring.* https://iia.no/wp-content/uploads/2021/03/Veileder-virksomhetsstyring-1.-utgave-ENDELIG.pdf

IIA (2021). *Veileder for virksomhetsstyring.* https://iia.no/wp-content/uploads/2021/03/Veileder-virksomhetsstyring-1.-utgave-ENDELIG.pdf

Institute of International Finance (IIF). (2009). *Reform in the Financial Services Industry: Strengthening Practices for a More Stable System,* Report of the IIF Steering Committee on Implementation (SCI).

International Organization for Standardization (ISO). (2009). *ISO31000: 2009 Management – Principles and Guidelines.* https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en

IRM (u.å). *A Risk Practitioners Guide to ISO 31000: 2018.* http://www.demarcheiso17025.com/document/A%20Risk%20Practitioners%20Guide%20to%20ISO%2031000%20%96%202018.pdf

Jacobsen, D. I. (2015). *Hvordan gjennomføre undersøkelser? – Innføring i samfunnsvitenskapelig metode.* (3.utg). Oslo: Cappelen Damm.

Jansrud, A. (2017a). *Operasjonell risiko: Måling, styring og kontroll.* [Lysbildepresentasjon] https://www.finansnorge.no/contentassets/2351118c435d4a77a3057eb1ebe4a684/12-operasjonell-risiko-maling-og-styring.pdf

Jansrud, A. (2017b.) *Operasjonell risiko.* [Lysarkpresentasjon] https://www.finansnorge.no/globalassets/presentasjoner/2017/operasjonell-risiko-norges-bank.pdf

Jensen, Ø. (2015). Risiko og ansvar. *Magma, 4*(2015), 17-19.

Johannessen, A., Tufte, P. A., & Christoffersen, L. (2016). *Introduksjon til samfunnsvitenskapelig metode* (5.utg.). Oslo: Abstrakt forlag AS

Johansen, I. S. (2016). *Modul for operasjonell risiko.* https://www.finanstilsynet.no/contentassets/4fd11f06085f47c5bd9756a2e42e563f/modul-for-operasjonell-risiko---evaluering-av-styring-og-kontroll-og-eksponering.pdf

Kaarbøe, K., Pedersen, L. J. T., Andvik, C. E., & Meidell, A. (2013). Enterprise Risk Management: utfordringer med ERM-designen?. *Magma, 16*(6), 37-40.

Kapitalkravsforskriften (2006). *Forskrift om kapitalkrav for forretningsbanker, sparebanker, finansieringsforetak, holdingsselskaper i finanskonsern, verdipapirforetak og forvaltningsselskaper for verdipapirfond mv.* (FOR-2006-12-14-1506). Lovdata. https://lovdata.no/LTI/forskrift/2006-12-14-1506/§41-1

Kaplan, R. S. (2009). Conceptual foundations of the balanced scorecard. *Handbooks of management accounting research*, *3*, 1253-1269.

Kaplan, R. S., & Mikes, A. (2016). Risk management—The revealing hand. *Journal of Applied Corporate Finance*, *28*(1), 8-18.

KPMG (u.å.). *Risikostyring.* https://home.kpmg/no/nb/home/tjenester/radgivning/risikotjenester/risikostyring.html

KPMG (2017). *Hvordan budsjettere når økonomisystemet ikke strekker til?* https://home.kpmg/no/nb/home/nyheter-og-innsikt/2017/01/hvordan-budsjettere-naar-okonomisystemet-ikke-strekker-til.html

Langfield-Smith, K. (1997). Management control systems and strategy: a critical review. *Accounting, organizations and society*, *22*(2), 207-232.

Liset, P. (2017). *Compliance – hva er god praksis?* https://blogg.pwc.no/styringogkontroll/compliance-hva-er-god-praksis

Lundqvist, S. A. (2014). An exploratory study of enterprise risk management: Pillars of ERM. *Journal of Accounting, Auditing & Finance*, *29*(3), 393-429.

Maal (2018). *Helhetlig risikostyring: Lyst på en sniktitt på fremtidens styringsverktøy?*. https://blogg.pwc.no/styringogkontroll/helhetlig-risikostyring-lyst-til-%C3%A5-titte-inn-i-hva-som-er-fremtidens-styringsverkt%C3%B8y

Malmi, T., & Brown, D. A. (2008). Management control systems as a package—Opportunities, challenges and research directions. *Management accounting research*, *19*(4), 287-300.

Meidell, A. (2017). Utviklingen av helhetlig risikostyring i relasjon til internkontroll og revisjon. *Praktisk økonomi & finans*, *33*(01), 135-149.

Mellemseter, S. E., & Mørch, T. (2006). Risikostyring i praksis. *Magma*, *4*(2006), 40-47.

Mikes, A. (2009). Risk management and calculative cultures. Management Accounting Research, 20(1), 18-40.
Mikes, A. & Kaplan, R. (2014). Towards a Contingency Theory of Enterprise Risk Management. Harvard Business School.

Mikes, A., Oyon, D. & Jeitziner, J. (2017). Risk management: Towards a behavioral perspective. *The Routledge Companion to Behavioral Accounting Research. Oxford: Routledge. doi*, *10*, 9781315710129-29.

Mun, J. (2010). *Modeling risk: Applying Monte Carlo risk simulation, strategic real options, stochastic forecasting, and portfolio optimization* (Vol. 580). John Wiley & Sons.

Noreng, S. R. (2002). Enterprise Risk Management. *Magma, 1*(2002).

Norges Bank Investment Management (2019). *Om oss.* *https://www.nbim.no/no/organiseringen/om-oss/*

Norges Bank Investment Management (u.å.). https://www.nbim.no/no/

Norsk olje & gass (2017). *090 - Norsk olje og gass Anbefalte retningslinjer for felles modell for sikker jobb analyse (SJA)*. https://www.norskoljeoggass.no/contentassets/d1dea04d994c4c56bd2639f5696c4274/090---anbefalte-retningslinjer-for-felles-modell-for-sikker-jobb-analyse.pdf

Nye Veier (u.å.) *Om oss.* https://www.nyeveier.no/om-oss/

Pedersen, K. E., & Ryen, M. E. (2019). *Bruk av risikostyring for gevinstrealisering i digitaliseringsprosjekter: en kvalitativ casestudie av et digitaliseringsprosjekt i et stort internasjonalt energiselskap* (Master's thesis).

Power, M. (2007). Organized uncertainty: Designing a world of risk management. Oxford University Press on Demand.

Power, M. (2009). The risk management of nothing. *Accounting, organizations and society*, *34*(6-7), 849-855.

Power, M. (2016). Riskwork: Essays on the organizational life of risk management. Oxford University Press.

Regjeringen (2018). *Utfyllende bestemmelser om kapitalkrav for banker (CRR)- vurdering av AMA-metode (operasjonell risiko)*. https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2018/nov/utfyllende-bestemmelser-om-kapitalkrav-for-banker-crr---vurdering-av-ama-metode-operasjonell-risiko/id2619726/

Ruter (u.å.) *Selskapsinformasjon.* https://ruter.no/om-ruter/selskapsinformasjon/

Saunders, M, N, K., Lewis, P. & Thornhill, A. (2016). *Research methods for business students*. London: Pearson Education.

Sbanken (2021). *Årsrapport 2020.* https://ml-eu.globenewswire.com/Resource/Download/ee96baab-e576-46ee-9c21-e405eca9529d

Seashore (u.å.) *Om oss.* https://www.seashore.no/om-oss/

Segal, S. (2011). Corporate value of enterprise risk management. *Hoboken (NJ): Wiley*.

Selnes, F (1999) *Markedsundersøkelser.* (4.utg). Otta: Tano Aschehoug.

Sheehan, N. T. (2010). A risk-based approach to strategy execution. Journal of business strategy, *31*(5), 25-37.

Simons, R. (1995a). Control in an age of empowerment. *Harvard Business Review*, *73*(2), 80-88.

Simons, R. (1995b). *Levers of Control: How managers use innovative control systems to drive strategic renewal.* Harvard Business Press.

Songedal, S. H., & Saltermark, K. (2019). *Integrasjon av helhetlig risikostyring med andre virksomhetsstyringssystemer: en flercasestudie av fem organisasjoner* (Master's thesis).

Sparebanken Sogn & Fjordane (2021). *Årsrapport 2020*. https://cdn.sanity.io/files/5rz6wn2n/production/e0eac88f48c51f7760b464eca476d7c1971a0472.pdf

Sparebanken Vest (2021). *Årsrapport 2020.* https://www.spv.no/om-oss/investor-relations/rapporter

Standard Norge (2018). *ISO-standarder.* https://www.standard.no/standardisering/iso-standarder/

Storebrand ASA. (2021). *Årsrapport 2020.* https://www.storebrand.no/om-storebrand/eierstyring-og-selskapsledelse/arsrapporter/_/attachment/inline/b3fdfebb-5892-47a0-819f-3e03e7a8ef84:e86181f71f8e76c8083319db5af69ee729e71991/2020-arsrapport-storebrand-asa.pdf

Tessier, S., & Otley, D. (2012). A conceptual development of Simons' Levers of Control framework. *Management Accounting Research*, *23*(3), 171-185.

Utne, R. (2020) *Risikokommunikasjon og systemisk risiko - et heksebrygg av sorte svaner, grå neshorn og kokende frosker.* https://www.prosjektutsyn.no/wp-content/uploads/2020/04/Fagnotat-risikokommunikasjon.pdf

Vig, J. & Hallaråker, T. (2006). *ERM-guiden.* https://risikoledelse.com/erm-handbok/erm-handbok-1/risiko/1-3/

Wiggen, T. M. (2008). Hva er risikostyring? DNV.

Woods, M. (2011). *Risk management in organizations*. Routledge.

Yin, R. K. (2014). *Case Study Research: Design and Methods* (5. utg.). Thousand Oaks, California: SAGE publications

Vedlegg 1: Samtykkeskjema

Samtykkeskjema

Kontaktinformasjon:

Vilde Isabelle Sævdal
E-post: vilde.sævdal@student.nhh.no
Tlf: 916 85 166

Benedikte Amalie Stokke
E-post: benedikte-amalie.stokke@student.nhh.no
Tlf: 417 58 235

Veileder Øyvind Thomassen
E-post: Ovind.Thomassen@nhh.no
Tlf: 55 95 94 71

Jeg deltar frivillig i forskningsprosjektet utført av Vilde Isabelle Sævdal og Benedikte Amalie Stokke fra Norges Handelshøyskole (NHH). Vi vil gjennomføre personlige intervjuer for å skape forståelse rundt risikostyring som en integrert del av virksomhetsstyring, og undersøke hva som er beste praksis for risikostyring.

1. Deltakelsen innebærer å bli intervjuet i ca. 45-60 minutter av masterstudenter fra NHH. Det vil bli skrevet notater under intervjuet.
2. Min deltakelse i dette prosjektet er frivillig. Jeg kan trekke meg og avslutte deltakelsen til enhver tid uten konsekvenser.
3. Om jeg føler meg ukomfortabel under intervjuet, har jeg rett til å ikke svare på spørsmålet.
4. Jeg tillater at det blir tatt lydopptak av intervjuet.
5. Jeg forstår at jeg ikke vil bli identifisert med navn i rapporter som bruker informasjon fra intervjuet, og at min konfidensialitet som deltaker i studien forblir sikker. Bruk av innsamlet data vil bli behandlet konfidensielt og i samsvar med personvernregelverket.
6. Navn og kjønn vil ikke inkluderes i skriftlig form. Dataene i den skriftlige formen vil kunne bli brukt i videre forskning ved Norges Handelshøyskole. Deltakerne vil ikke direkte bli gjenkjent i publikasjonen, men selskapet vil kunne være identifiserbart.
7. All data vil bli slettet ved studiets slutt, 01.06.2021.
8. Jeg har lest og forstått forklaringen som er gitt meg. Jeg har fått alle spørsmål besvart på en tilfredsstillende måte, og jeg deltar frivillig i denne studien.
9. Jeg har fått kopi av samtykkeerklæringen.

Navn (blokkbokstaver):

Sted og dato: Signatur:

Vedlegg 2: Intervjuguide I

Intervjuguide for konsulentselskapene

DEL 1: INTRODUKSJON

- Kort presentasjon om oss og prosjektet
- Informere om konfidensialitet og anonymitet
- Forespørsel om lydopptak
- Bekreftelse på at samtykkeskjema er signert

DEL 2: INNLEDENDE SPØRSMÅL

1. Kan du fortelle litt om hvordan du arbeider med risikostyring?
2. Hva legger du i operasjonell risikostyring?
3. Kan du fortelle om ulike typer risiko som virksomheter blir eksponert for?

DEL 3: HOVEDDEL

Tema 1: Grensesystemet

Organisasjonsstruktur

4. Hvem er det som typisk har det overordnede ansvaret for risikostyring i virksomheter?

- Hva mener du er beste måte å organisere de ulike rollene for risikostyring (1, 2 og 3 linje)?
- Kan du skissere opp et typisk hierarki for risikostyring i virksomheter?
- Er det egne stillinger/fulltidsstillinger for risikostyring i virksomheter eller en birolle hos ansatte?
- Hvor viktig er det å ha en CRO-funksjon som ivaretar risikostyring?
    - Hvilke andre risikofunksjoner kan virksomheter ha?

Policyer

5. Basert på dine erfaringer: Hvordan utformer virksomheter generelle prinsipper (risikopolicyer) for at risiko skal bli styrt helhetlig?

- Hva er din anbefaling for å lage rutiner og prosedyrer for å styre risiko?
- Hvordan fastsetter man disse policyene og hvordan er de utfylt?
- Hvordan er disse nedfelt i et dokument og bruker virksomheter dette?
- Hvordan operasjonaliserer virksomheter prinsipper?

Rammeverk

6. Basert på dine erfaringer, hvilke risikorammeverk anbefaler du at virksomheter bruker?

- Hva mener du er viktig når virksomheter tar i bruk rammeverk?
- Hva er typiske fallgruver som kan oppstå når man benytter rammeverk?
- Har du sett noen positive effekter ved å ta i bruk slike rammeverk?

Risikoappetitt

7. Hvordan definerer virksomheter tydelige grenser for hva som er et akseptabelt risikonivå?

- Hvilken type risiko er det som typisk utgjør risikoappetitten i virksomheter?
- Hvilke lovverk påvirker risikoappetitten?

Tema 2: Diagnostisk styringssystem

Risikoprosessen

8. Hvordan *identifiserer* virksomheter risiko?

- Hva er det viktig å ta hensyn til når man identifiserer risiko?
- Hva er typiske fallgruver når man identifiserer risiko?

9. Hvordan *vurderer* virksomheter risiko?

- Skilles det mellom kvantitative og kvalitative vurderinger?
- Hvordan vurderes risikofaktorer?
- Hvilke verktøy benyttes?

- Hvilke data brukes for vurdering? Hendelsesdata og/eller kun vurdering av oppstått risiko?

10. Hvordan *håndterer* virksomheter risiko?
    - Eks. akseptere, unngå, forfølge, redusere eller dele risiko?
11. Hvor viktig er oppfølging i etterkant av denne prosessen?

- Hvordan mener du at man bør følge opp risikoprosessen?
- Hvilke kontrolltiltak er det viktig å benytte? Hvordan styres disse tiltakene?

Rapportering av risiko

12. Hvordan pleier man å rapportere risiko og til hvem?

- Hvordan blir operasjonell risiko integrert i rapportering?
- Hvordan fremstilles risikoene visuelt i rapportene?
- Hvordan inkl. risiko i f.eks. KPI-er, budsjetter, balansert målekort, prognoser etc.?

Tema 3: Interaktiv styringssystem

Kommunikasjon og diskusjon

13. Hvordan bør risiko kommuniseres og diskuteres i virksomheter?

- Mellom ulike nivåer, ansatt til ansatt og leder til ansatt?
- På hvilke arenaer foregår slike diskusjoner?
- Hva mener du virksomheter kan blir bedre på når det gjelder kommunikasjon og diskusjon av risiko?

Tema 4: Trossystemet

Organisasjonskultur, risikokultur og risikoholdning

14. Hvordan opplever du at risikokulturen er i ulike virksomheter?
15. Hvordan skaper man en god risikokultur og hvorfor er det viktig for virksomheter?
16. Hvordan er ledere og ansatte sin holdning til risiko når de tar beslutninger og gjennomfører arbeidsoppgaver?

Tema 5: Risikostyring i praksis

17. Basert på dine erfaringer, hva er det virksomheter gjør bra og hva sliter de mest med når det kommer til risikostyring?
18. Hva trenger virksomheter hovedsakelig bistand med fra deg når det kommer til risikostyring?
19. Hvordan opplever du at virksomheter har integrert risikostyring i virksomhetsstyringen?
20. Hva mener du er viktig å tenke på når man integrerer risikostyring i virksomhetsstyringen?
21. Hva mener du er beste praksis for operasjonell risikostyring? Er det noen elementer som er viktigere enn andre?
22. Hvordan tror du virksomheter kommer til å drive med operasjonell risikostyring i fremtiden?
23. Har Covid-19 hatt noe innvirkning på fokuset på risikostyring?

DEL 4: Avsluttende kommentar

24. Er det noe du vil legge til?
25. Har du noen spørsmål til oss?

Vedlegg 3: Intervjuguide II

Intervjuguide for finansforetak og fiskeri og infrastruktur

DEL 1: INTRODUKSJON

- Kort presentasjon om oss og prosjektet
- Informere om konfidensialitet og anonymitet
- Forespørsel om lydopptak
- Bekreftelse på at samtykkeskjema er signert

DEL 2: INNLEDENDE SPØRSMÅL

1. Kan du fortelle litt om hvordan din virksomhet arbeider med risikostyring?
2. Hva legger du i operasjonell risikostyring?
3. Kan du fortelle om ulike typer risiko som din virksomheter kan bli eksponert for?

DEL 3: HOVEDDEL

Tema 1: Grensesystemet

Organisasjonsstruktur

4. Hvem er det som har det overordnede ansvaret for risikostyring i virksomheten?
- Hvordan har dere organisert rollefordeling for risikostyring?
- Kan du skissere opp et typisk hierarki for risikostyring i virksomheten?

Policyer

5. Hvordan utformer dere generelle prinsipper (risikopolicyer) for at risiko skal bli styrt helhetlig?
- Har dere rutiner og prosedyrer for å styre risiko?
- Hvordan fastsettes disse policyene og hvordan er de utfylt?
- Er det nedfelt i et dokument, og blir dette brukt?
- Har dere noen prinsipper som virksomheten har operasjonalisert?

Rammeverk

6. Har dere et risikorammeverk internt og hvilket rammeverk er det basert på?
- Hva mener du er viktig når man tar i bruk rammeverk?
- Har du opplevd noen positive effekter ved at virksomheten har tatt i bruk rammeverk?

Risikoappetitt

7. Hvordan definerer virksomheten tydelige grenser for hva som er et akseptabelt risikonivå?
- Hvilken type risiko er det som typisk utgjør risikoappetitten i virksomheten?
- Har dere grenser for operasjonell risiko?
- Hvilke lovverk påvirker risikoappetitten virksomheten?

Tema 2: Diagnostisk styringssystem

Risikoprosessen

8. Hvordan *identifiserer* dere ulike typer risiko?
- Hva er det viktig å ta hensyn til når man identifiserer risiko?
- Hva er typiske fallgruver når man identifiserer risiko?

9. Hvordan *vurderer* virksomheten risiko?
- Skilles det mellom kvantitativ og kvalitativ vurdering?
- Hvordan vurderes risikofaktorer?
- Hvilke verktøy benyttes?
- Hvilke data brukes for vurdering? Hendelsesdata og/eller kun vurdering av oppstått risiko?

10. Hvordan *håndterer* virksomheten risiko?

- Prioriterer dere risiko som grunnlag for å velge risikotiltak? Eks. akseptere, unngå, forfølge, redusere eller dele risiko?

11. Hvordan følger dere opp håndtering og generelt prosessen for risikostyring?

- Hvordan følges tiltakene opp? Hvordan styres disse tiltakene?
- Har dere noen kontrolltiltak som benyttes for å redusere/håndtere risiko?
- Blir det utarbeidet noen dokumenter i arbeidet med risikostyring?

Rapportering av risiko

12. Har dere jevnlig risikorapportering og hvem er det som har ansvar for rapportering?
13. Hvordan blir operasjonell risiko integrert i rapportering?
14. Hvordan fremstiller dere risikoene visuelt i rapportene?
15. Inkluderer dere risiko i f.eks. KPI-er, budsjetter, balansert målekort, prognoser etc?

Tema 3: Interaktivt styringssystem

Kommunikasjon og diskusjon

16. Hvordan kommuniseres og diskuteres risiko i virksomheten?

- Mellom ulike nivåer, ansatt til ansatt og leder til ansatt?
- På hvilke arenaer foregår slike diskusjoner?
- Hva mener du virksomheten kan blir bedre på når det gjelder kommunikasjon og diskusjon av risiko?

Tema 4: Trossystemet

Organisasjonskultur, risikokultur og risikoholdning

17. Hvordan opplever du at risikokulturen er i din virksomhet?
18. Hvordan arbeider dere med å skape en god risikokultur?
19. Hvordan er ledere og ansatte sin holdning til risiko når de tar beslutninger og gjennomfører arbeidsoppgaver?

Tema 5: Risikostyring i praksis

20. Basert på dine erfaringer, hva synes du virksomheten gjør bra når det kommer til risikostyring?
21. Hva synes du er mest utfordrende når det kommer til risikostyring?
22. Hvordan opplever du at dere har integrert risikostyring i virksomhetsstyringen?
23. Hva mener du er viktig å tenke på når man integrerer risikostyring i virksomhetsstyringen?
24. Hva mener du er beste praksis for operasjonell risikostyring? Er det noen elementer som er viktigere enn andre?
25. Hvordan tror du virksomheter kommer til å drive med operasjonell risikostyring i fremtiden?
26. Har Covid-19 hatt noe innvirkning på fokuset på risikostyring?

DEL 4: Avsluttende kommentar

27. Er det noe du vil legge til?
28. Har du noen spørsmål til oss?