ENTERPRISE RISK MANAGEMENT R

– utfordringer med ERM-designen?

KATARINA KAARBØE er professor ved Norges Handelshøyskole (NHH). Hun har i sin forskning først og fremst vært interessert i bindeleddet mellom ledelse og styring og har publisert et antall artikler og bøker innenfor området. Kaarbøe er prosjektleder for forskningsprogrammet Beyond Budgeting ved NHH/SNF.

LARS JACOB TYNES PEDERSEN er førsteamanuensis ved Institutt for regnskap, revisjon og rettsvitenskap og styreleder for Senter for etikk og økonomi ved Norges Handelshøyskole. Han forsker på og underviser i næringslivsetikk og samfunnsansvar og er tilknyttet forskningsprogrammene Beyond Budgeting og Senter for tjenesteinnovasjon.

CHRISTIAN EIDE ANDVIK er doktorgradsstipendiat ved institutt for regnskap, revisjon og rettsvitenskap ved Norges Handelshøyskole (NHH) og er siviløkonom fra samme sted. Han forsker på virksomhets- og risikostyring i finanssektoren. Andvik er prosjektdeltaker i forskningsprogrammet Beyond Budgeting.

ANITA MEIDELL er doktorgradsstipendiat ved institutt for regnskap, revisjon og rettsvitenskap ved Norges Handelshøyskole (NHH) og er siviløkonom fra samme sted. Hun forsker på virksomhets- og risikostyring i oljesektoren. Meidell er prosjektdeltaker i forskningsprogrammet Beyond Budgeting.

SAMMENDRAG

I de siste tiårene har selskaper viet mer oppmerksomhet til å styre risiko. COSO har utviklet et rammeverk som de kaller Enterprise risk management (ERM). I denne artikkelen diskuterer vi utfordringer med ERM-design og hvilken type forskning som trengs for å svare på hvordan disse utfordringene kan håndteres. Vi vektlegger tre områder ved designen til ERM som er problematiske. For det første er individualiseringen av et selskap problematisk, fordi det fører til at det kun har én risikoappetitt. For det andre er ERM basert på en revisjonslogikk, som fører til reaktivitet. For det tredje tar designen bare hensyn til et selskap og ikke nettverket av selskap. Det er derfor viktig at vi utvikler mer kunnskap om hvordan risikostyring er designet og hva dette innebærer for helhetlig styring.

Gjennom de seneste tiårene har selskap viet mye mer oppmerksomhet til å styre risiko. Flere kriser har vært med på å bidra til nytenkning innenfor området – kollapsen til Maxwell i UK, problemene i Shell på 1990-tallet og Enron i 2001, for å nevne noen (Spira og Page 2003, Woods 2011). Power (2007) argumenterer for at det har vært en eksplosjon i ordbruken relatert til risikostyring etter 1990. *Enterprise risk management* (ERM) er et område som har vokst frem som en mer helhetlig løsning på hvordan virksomheter kan styre risiko. Det gir rom for klare endringer i ledelse og styring av selskapene for å redusere risiko, men også for å våge å ta risiko.

Det åpner for å se risikostyring på nye måter. ERM er imidlertid ikke ett avgrenset teoretisk eller praktisk fenomen, men en samlebetegnelse for et system av konsepter som skal gi veiledning i hvordan bedriften kan håndtere risiko relatert til målsettingene i selskapet.

I denne artikkelen diskuterer vi kort mulige utfordringer med ERM og hvilken type forskning som trengs for å svare på hvordan disse utfordringene kan håndteres. Risikostyring er mer enn bare en teknisk-analytisk praksis. Det innehar også bestemte verdier og idealer, særlig når det gjelder ansvarliggjøring og ansvarsfordeling i organisasjoner. De utfordringene vi tar opp i denne artikkelen, knytter seg til disse verdiene og idealene.

Internkontroll har blitt synonymt med risikostyring. I COSO 2004 ble *risk management* omdøpt til *Enterprise Risk Management*, og det ble definert slik: «[ERM] incorporates the internal control framework within it» (COSO 2004, foreword, p. v.). Ideen med å bruke ERM som et overgripende rammeverk for internkontroll impliserer at risiko er en del av bedriftens strategi. Internkontroll har i dag en mer fremskutt posisjon og høyere status. Denne endringen begynte allerede på 1980-tallet i finanssektoren og har fått en større betydning gjennom finanskrisen som oppstod 20 år senere (Woods 2011). Som følge av større regulering øker internkontrollens betydning.

ERM kan forstås som et svar på en større etterspørsel etter god risikostyring. ERM, influert av internkontroll, er svært preget av regnskaps- og revisjonsnormers syn på kontroll, hvor det er skarpt fokus på prosessbeskrivelser og bevis. Ifølge Power (2007) er den regulerende myndighetens hensikt med ERM for det første at selskapene skal unngå de feil som ble gjort gjennom den tidligere silobaserte risikostyringen. ERM skal i stedet være helhetlig og integrerende. For det andre var det et ønske om at risiko ikke kun skulle forstås som noe negativt, men også som noe positivt. Ideen var at siden bedrifter tar beslutninger under usikkerhet, er det viktig å være bevisst på hvilke risikoer som er relevante, og å kunne styre disse.

I de siste årene har det imidlertid blitt stilt spørsmål ved hvorvidt operasjonell risiko og intern kontroll stimulerer til intelligent risikostyring. Bidrar de til forståelsen av selskapets risikosituasjon, eller fører de bare til en form for «normalisering av avvik» i et nettverk av prosedyrer og rutiner (Power 2009)? Bekymringen er at risikostyring kan gi en falsk trygghet og opplevelse av at risiko går an å styre, og at selskapet faktisk gjør det.

Power (2009) argumenterer for at ERM-designen er problematisk på tre måter. For det første er individualiseringen av et selskap problematisk, fordi det fører til at det kun har én risikoappetitt. For det andre er det problematisk at ERM baseres på en revisjonslogikk. For det tredje er det problematisk å se risiko kontekstualisert i det aktuelle selskapet, og ikke i et nettverk av selskap. I det følgende drøfter vi disse tre utfordringene som Power (2009) tar opp.

SELSKAPET SOM ETT INDIVID MED ÉN RISIKOAPPETITT

Risikoappetitt er en hovedkomponent i ERM-designen, siden en av de kritiske utfordringene for ledergrupper er å bestemme hvor stor risiko virksomheten kan og skal utsettes for i prosessen med å skape verdier. Det betyr at organisasjonen forstås som ett individ – *the enterprising actor*. Organisasjonen fremstilles som én risikotakende entreprenør som har god kjennskap til sin egen appetitt for risiko. Ideen er at organisasjonen gjennom ERM skal tilegne seg informasjon og på bakgrunn av denne agere og styre seg selv. Til tross for at ERM gir uttrykk for organisasjonen som en intelligent aktør med egne intensjoner, er den en veldig mekanisk og reaktiv aktør. Den reagerer på historiske data og gjør tilpasninger ut fra disse.

Når risikoappetitt forstås som input til ERM, kan ERM fungere som en type termostat som regulerer seg selv ut fra hvilken temperatur det er. Flere forskere hevder imidlertid at en organisasjon representerer flere ulike grupperinger som har ulik appetitt for risiko (Power 2009, Hood 1996). En organisasjon er oppbygd av flere ulike aktørgrupper som ofte trekker i forskjellige retninger. Det kan føre til motsetninger eller konflikter mellom grupper og funksjoner i organisasjonen.

Begrepet *risikoappetitt* har blitt utbredt, til tross for at vi fortsatt vet veldig lite om hva det faktisk er, og hvilke implikasjoner det har. Konseptet har sitt utspring i regnskapslogikken som ligger bak COSO og intern kontroll, og gir et kontrollperspektiv på hva risikostyring er. I beste fall kan denne statiske designen gi organisasjonen en gjennomsnittsbetraktning av holdninger og verdier av operasjonelle og etiske risikoer. Siden ERM kun har ett mål for hvert risikoområde, blir de ulike aktørgruppenes risiko lagt sammen til et gjennomsnitt, eller så blir det ikke hensyn tatt.

REVISJONSLOGIKK

En del av ERM-utviklingen har gått ut på å skape et mer gjennomsiktig system, ikke bare for selskapet, men også for regulerende myndigheter og for hele samfunnet. Ideen har vært at ERM-designen skal skape en kontrollmekanisme som kan følges tilbake i tid – en revisjonslogikk. Gjennomsiktighet er en av grunnpilarene i designen. Dette har ført til en regelbasert *compliance*-modell som kan ha gitt lederen en falsk følelse av trygghet.

Finanskrisen var med på å flytte fokuset fra denne regelbaserte modellen til et mer kritisk perspektiv på ulike fremtidsscenarioer. Det hevdes at det har vært anlagt et altfor reaktivt og bakoverskuende perspektiv. Woods (2011) viser i sine studier at lederne i bankene og regulerende myndigheter trodde at finansregnskapene og internkontrollen var effektiv, men det viste seg at utfordringen lå i dårlig ledelse og forståelse av den mer helhetlige forretningsrisikoen. Woods refererer til Skypala (2008), som beskriver hvordan selskapene som gikk under i løpet av finanskrisen, håndterte den overordnede styringen som en samling av regler i stedet for å se mer fremover (Woods 2011).

Utfordringen ligger i å utvikle prosesser som bidrar til interaksjon og dialog, og å unngå prosesser med fokus på kun å leve opp til en standard. Ut fra et læringsperspektiv handler det både om å ha adaptive tilpasninger og dessuten om å tenke helt nytt. Dette minner om hva mange i finanssektoren kaller stresstesting. Dette er mer utfordrende, siden det er med på å skape tvetydighet og utfordre hovedelementer i den valgte strategien og styringsmodellen.

FEIL TYPE KONTEKSTUALISERING

Behovet for å inkludere risikostyring og interne kontrollsystemer i organisasjonsprosessene er en selvsagt del i ERM-designen. Ideen er at organisasjonen gjennom ERM vil ha risikoeiere for alle prosesser og derigjennom kunne følge hvem som er ansvarlig hvis noe skjer. Til tross for det finnes det i liten grad eksplisitte beskrivelser av hvordan dette skal gjøres i reguleringen. På samme måte som for risikoappetitt er det regnskapsførerens konsept som brukes (som har en mer prinsipiell form for hvordan dette skal gjøres). Det sies veldig lite eksplisitt om hvordan dette kan gjøres på en god måte.

En av lærdommene fra finanskrisen er imidlertid at det er viktig å kontekstualisere organisasjonens virksomhet ytterligere for å kunne forutse fremtiden. For eksempel i Turnbull-rapporten (1999), som har vært utgangspunktet for konstruksjonen av ERM, er beskrivelsen av selskapet kun relatert til det enkelte selskap, og ikke til et videre nettverk av aktører. Mange hevder at finanskrisen hadde sitt utspring i at selskapene ikke forstod den koblingen de har til andre selskap i sine egne omgivelser. Et tydelig eksempel er bankkrisen i USA, der det var stor kompleksitet i relasjonene mellom bankene og de organisasjonene som var med på å bygge opp de nye bankproduktene, som til slutt førte til at flere banker og finansinstitusjoner gikk konkurs.

Utfordringen ligger ikke bare i å identifisere risiko lokalt i og rundt selskapet, men også i en mer global forstand koblet til et nettverk av aktører. Organisasjonen kan ikke ses på isolert, men i stedet er det viktig å se på både leverandører, konkurrenter, kunder og så videre. ERM må kunne ta hensyn til videre omgivelser enn bare de nærmeste. Dette gir imidlertid en enorm kompleksitet som innebærer at subjektive elementer blir del av risikostyringen.

Som tidligere nevnt hevder Power (2009) at det er tre utfordringer med designen av ERM; individualiseringen av selskapet ut fra begrepet risikoappetitt, revisjonslogikk som skaper reaktivitet, og for snever kontekst. En implikasjon av dette er at ERM ikke kun kan handle om objektivt målbare enheter – i tillegg må det tas hensyn til subjektive enheter. Det er en fare med å vektlegge det målbare altfor mye, ettersom dette kan føre til at selskapene bare fokuserer på det som er mulig å måle, i stedet for også å prøve å ta hensyn til usikkerheter som ikke kan måles, og kanskje heller ikke reduseres. Til tross for dette er det viktig at selskapene skaper bevissthet rundt disse risikoområdene og har planer for hvordan det kan slå ut for selskapet.

Risiko handler ifølge Power både om den objektive, målbare usikkerheten og den subjektive usikkerheten. Designen på ERM må da ta hensyn til balansen mellom disse to områdene. Vi mener i tråd med Power at dette er områder som vi vet altfor lite om. Hvordan kan begrepet risikoappetitt brukes på en mer konstruktiv måte som tar hensyn til flere aktørgrupper? Hvordan kan revisjonslogikken endres eller utvikles for å få en mer proaktiv beslutningsprosess? Hvordan kan designen ta mer hensyn til en videre kontekst? Disse spørsmålene er knyttet både til dem som regulerer virksomheten, og dem som gjennomfører risikoanalyser. Det gjør det også mer krevende å utvikle

kunnskap om dette fenomenet, og det er behov for å utvikle kunnskap på dette området.

Ved NHH har vi derfor startet et prosjekt som del av forskningsprogrammet Beyond Budgeting for å studere risikostyring i olje- og banksektoren. I oljesektoren har vi valgt Statoil, og i banksektoren har vi valgt DNB. Begge selskapene er valgt ut fordi de er store, komplekse selskap som befinner seg i en kontekst som er veldig regulert. Dette innebærer at de er selskap som ligger langt fremme når det gjelder styring av risiko.

Statoil startet sitt arbeid med Enterprise Risk Management i 1996, og risikostyring er i dag en integrert del av virksomhetsstyringen i selskapet. Selv om risikoappetitten ikke er eksplisitt tallfestet i Statoil, er det likevel en forståelse for hva som er akseptabel og ikke-akseptabel risiko innenfor ulike områder. I vårt prosjekt i Statoil vil vi blant annet studere hva ulike deler av organisasjonen legger i begrepene risiko og risikostyring, og hvordan risikoappetitten styres når ledere fatter beslutninger. Vi er blant annet interessert i å avdekke eventuelle forskjeller mellom ulike nivå og mellom ulike enheter, og hvordan dette påvirker den totale risikostyringen i selskapet.

Helt siden starten har formålet i ERM-enheten sentralt i Statoil vært å bruke ERM til å skape verdier for selskapet og eierne. ERM har i mindre grad vært brukt som et verktøy for internkontroll. Vi ønsker å studere nærmere hvordan Statoil totalt sett balanserer bruken av risikostyring til å skape verdier på den ene siden og til styring og kontroll på den andre siden. I denne sammenhengen vil vi også se på hvordan Statoil løfter blikket for også å vurdere risikoer i omgivelsene de opererer i.

Som Norges største bank har DNB mye erfaring med risikostyring. Kvantitative modeller for modellering av kredittrisiko er raffinert gjennom en årrekke med forskning og utveksling av praktiske erfaringer mellom internasjonale aktører. Bankene opererer i en bransje hvor statlige tilsyn og internasjonale reguleringer legger stramme føringer for selskapsatferd, og selv om bankene har jobbet mye med risikostyring, ble vi i 2008 vitne til en gigantisk kollaps i de finansielle markedene.

Nesten daglig kan vi lese om økte kapitalkrav for norske banker og implementeringen av Basel III og CRD IV. Ved inngangen til 2013 opprettet DNB risikostyring som et eget støtteområde i konsernet, og lederen for dette området møter i konsernledelsen sammen med konserndirektør for finans. I 2012 etablerte konsernet et rammeverk for risikoappetitt som trådte i kraft samtidig som den nye organiseringen. Argumentet for implementeringen av det nye rammeverket begrunnes med utfordringene ved å gi et holistisk og balansert bilde av konsernets risikoeksponering. Det er en implisitt anerkjennelse av at eksisterende mekanismer er for lite integrert i styringen av konsernet, og rammeverket skal tjene som en hjelp i operasjonaliseringen av selskapets retningslinjer vedrørende risiko.

I vårt prosjekt med DNB ønsker vi å studere hvordan risikoappetitt som et styrende rammeverk implementeres. Vi vil undersøke hvorfor DNB gjør de valgene de gjør knyttet til risikostyring, hvem som er involvert i beslutningene, og hvordan det nye rammeverket påvirker risikostyringen. Hvorfor man har valgt å skille risikostyring ut som et eget område, er også av stor interesse.

I denne artikkelen har vi diskutert sentrale utfordringer knyttet til ERM som risikostyring. Vi har videre diskutert kunnskapsbehovet på dette området, og belyst pågående forskningsprosjekter i NHH-miljøet som sikter mot å bidra til å fylle dette kunnskapsgapet. På denne måten vil vi kunne komme nærmere utviklingen i risikostyring i praksis og samtidig bidra til å utvikle forståelsen av begrepets innhold. M

REFERANSER

Hood, C. 1996. *United Kingdom: From second-chance to near-miss learning. In Lessons from experience: Experiential learning in administrative reforms in eight democracies*, red. J.P. Olsen and B.G. Peters, 36–70. Oslo: Scandinavian University Press.

Power, M. 2007. *Organized Uncertainty – Designing a World of Risk Management*. Oxford: Oxford University Press.

Power, M. 2009. The risk management of nothing. *Accounting, Organizations and Society, 34*: 849–855.

Skypala, P. 2008. Time to reward good corporate governance. *www.ft.com* [lesedato 18.11.].

Spira, L. og M. Page. 2003. Risk management: the reinvention of internal control and the changing role of internal audit. *Accounting, Auditing and Accountability Journal, 16*(4):640–661.

Woods, M. 2011. *Risk Management in Organizations – An integrated case study approach*. New York: Routledge.