Universitetet i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering: 2-årig Master i Industriell Økonomi	Vår.....semesteret, 20..... Åpen / Konfidensiell
Forfatter: Idar Døssland	…… (signatur forfatter)
Fagansvarlig: Veileder(e): Ragnar Tveterås	
Tittel på masteroppgaven: Evaluering og sammenligning av ERM rammeverker Engelsk tittel: Evaluation and Comparison of ERM Frameworks	
Studiepoeng: 30	
Emneord: Enterprise Risk Management ERM ERM-rammeverk Risikostyring	Sidetall: …… + vedlegg/annet: …… Stavanger, …….. dato/år

Universitetet i Stavanger

Evaluering og sammenligning av ERM-rammeverker

Masteroppgave Industriell Økonomi

Idar Døssland

Vår 2010

Sammendrag

Opp gjennom de siste årene, og spesielt etter den globale finanskrisen, har Enterprise Risk Management (ERM) vekket stor oppmerksomhet og hatt en kraftig vekst. Behovet for veiledende standarder og rammeverk for implementering i selskaper og organisasjoner økt i takt med veksten innenfor disiplinen generelt, og dette har resultert i at flere industriinitiativer har blitt stiftet for å møte det økende behovet for veiledning og standardisering. Flere rammeverker for ERM har blitt utviklet, slik som COSOs *Enterprise Risk Management – Integrated Framework*, som ble publisert i 2004, og senest en ny internasjonal standard; ISO 31000. Disse rammeverkene har alle forsøkt å imøtekomme kravene for god ERM, men ingen har enda klart å bli godkjent som en standard som oppfyller alle krav og behov.

Denne oppgaven forsøker derfor å sammenligne eksisterende ERM-rammeverk og evaluere dem mot gjeldene behov, reguleringer og risikolitteratur. Den første delen av oppgaven gir en innføring i teorien bak Enterprise Risk Management og beskriver et referanserammeverk som benyttes i evalueringen av fire utvalgte høyprofilerte rammeverk. Funnene i denne delen gjør det klart at det er stor uenighet i bransjen om hvordan ERM i seg selv skal defineres. Den andre delen av oppgaven tar for seg de fire rammeverkene CAS *Overview of Enterprise Risk Management, COSO Enterprise Risk Management, BS 31100* og *ISO 31000* hver for seg for så å sammenligne og avsløre styrker og svakheter. Denne delen går grundigere inn i hvert av de fire rammeverkene og avslører at alle rammeverkene har betydelige svakheter, men også noe store styrker. Oppgaven presenterer et forslag for hvordan et ERM-rammeverk kan utvikles på bakgrunn av det beste fra hvert av de fire evaluerte rammeverkene, men konstaterer at det fortsatt er noen elementer som mangler før man kan presentere et fullendt rammeverk for ERM. Til slutt i oppgaven presenters forslag til videre undersøkelser innenfor emnet med fokus på teknologiske ressurser, og styring av operasjonell risiko.

Innhold

1 Innledning og motivasjon

1.1 Innledning

Denne oppgaven vurderer og evaluerer eksisterende ERM-rammeverk i henhold til gjeldende litteratur om risiko og Enterprise Risk Management. Enterprise Risk Management(ERM) er en strategisk risikostyringsdisiplin som har som mål å maksimere et selskap eller en organisasjons verdi gjennom effektiv og helhetlig styring av selskapets totale risikoportefølje. ERM-rammeverket setter rammer og retningslinjer for hvordan selskapet utfører sitt risikostyringsarbeid, og sikrer at risikostyring er en integrert del av selskapets overordnede organisasjonsstruktur og organisasjonsstruktur.

Det som kjennetegner ERM er at det fjerner fokuset fra den tradisjonelle silo-baserte risikostyringen, der risiko blir kategorisert i ulike siloer som for eksempel operasjonell risiko, finansiell risiko, ulykkesrisiko med mer. ERM forsøker å samle alle risiko-siloene ved å vurdere aspekter som gjensidige avhengigheter mellom ulike typer risiko og porteføljeeffekter.

Denne oppgaven vil evaluere og sammenligne eksisterende rammeverk for ERM med aktuell litteratur, relevante kritikere, trender og uttrykt behov fra næringslivet. Utvalget av rammeverk som er inkludert i oppgaven er basert på deres status, som igjen er basert på utgivere, brukere og omtale. Som et referansepunkt i evaluering brukes James Lams syv komponenter for et vellykket ERM-rammeverk.

1.2 Motivasjon

Denne masteroppgaven er motivert av observasjoner om at det tilsynelatende ikke finnes ett anerkjent og gjennomgående godkjent rammeverk for implementering og bruk av Enterprise Risk Management (ERM) i bedrifter og organisasjoner. Disse observasjonene er blant annet basert på kritikken fra Ali Samad-Khan som er rettet mot COSOs rammeverk og dets evne til å håndtere operasjonell risiko.

En annen motivasjon som har fått stort betydning er rollen ERM har fått som en løsning på problemene som førte til den nylige finanskrisen. Dette gjør ERM til et meget tidsaktuelt og interessant tema, med en kontinuerlig utvikling som til tider kan gjøre det vanskelig å ta til seg og forstå hele konseptet. Dette er en stor utfordring.

1.3 Oppgavens omfang og begrensninger

Det denne oppgaven prøver å belyse er styrker og svakheter ved de mest brukte og profilerte

rammeverkene og konseptene for ERM. Gjennom teoretisk gjennomgang av rammeverkene, bakgrunns- og støttelitteratur skal oppgaven identifisere hvordan ERM, og dets delkonsepter blir definert og håndtert, og hvilke utslag dette kan gi ved implementering og gjennomføring.

Oppgaven vil i høy grad være begrenset til å vurdere de eksisterende rammeverkene og konseptene tilknyttet ERM, og vil kun i liten grad kommentere nærliggende alternativer som SRM, IRM og HRM, og kun i den hensikt å gi vurderingene et bedre perspektiv.

De rammeverkene og konseptene som skal vurderes i denne oppgaven er:

- COSO: Enterprise Risk Management – Integrated Framework
- BSI British Standards: Risk Management – Code of Practice
- ISO 31000: Risk Management – Principles and Guidelines
- CAS: Overview of Enterprise Risk Management

2 Teori

2.1 Pådrivere for ERM og økt risikostyring

James Lam har i sin artikkel ”Managing Risk Across the Enterprise: Challenges and Benefits” (Ong, 2006) identifisert flere årsaker og pådrivere han mener har vært viktige for utviklingen av ERM fram mot slik vi kjenner den i dag.

Det første han nevner, og som kanskje har vært en utløsende faktor for utviklingen, er store finansielle katastrofer som enten har vært forårsaket eller har gått kraftig utover store etablerte selskaper og konserner som man i utgangspunktet antok var stabile og nesten uknekkelige. Slike hendelser inkluderer Enron-skandalen som ble avdekket i 2001, WorldCom (lønnsomhetssvindel for å kunstig drive opp aksjeprisen). Andre store skandaler som kan nevnes er de som gjelder Long-Term Capital Management, Barings Bank og Power Company of America. Interessant lesing om to av disse hendelsene kan man finne her: *The Dynamics of Organizational Collapse the Case of Barings Bank* (Drummond, 2008), *Learning from ENRON* (Deakin and Konzelmann, 2003). Slike store katastrofer har ført til at styre og ledelse i flere store selskaper i mange forskjellige industrier har lagt større og større vekt på god og effektiv risikostyring for å sikre en sikker drift av sine selskaper.

Den andre gruppen av pådrivere for ERM som nevnes av Lam er de økende kravene om kontroller, ansvarlig kapital med mer.

US Securities and Exchange Committee (SEC) var en av forgjengerne på dette området, og

senere har Basel komitéen fått stor betydning for bankindustrien med Basel II direktivet der de opprettet en direkte link mellom ansvarlig kapital og bankens underliggende kreditt-, markeds-, og operasjonelle risikoer. Med the Sarbanes-Oxley Act fra 2002 ble det opprettet lovfestede standarder for finansiell rapportering og internkontroller.

Alle disse nye lovene og retningslinjene har ført til at personer som er ansvarlige for feilhandlinger innenfor disse områdene ikke lenger bare blir straffet med bøter og andre finansielle straffer, men kan også risikere fengselsdommer. Dette tvinger selskaper til å ta et mye mer grundig grep om sin risikostyring og er dermed viktige pådrivere for utviklingen av ERM.

For å kunne håndtere de mange nye lovene og kravene har det blitt organisert flere nye industrielle initiativer med det formålet å lage nye rammeverker og standarder for blandt annet risikostyring. Dette har dannet grunnlaget for flere av de rammeverkene og konseptene som skal vurderes senere i denne oppgaven. I 1992 ga COSO (the Committee of Sponsoring Organisations of the Treadway Commission) ut et rammeverk for internkontroll(COSO, 1992), og i 1993 ga the Group of 30 ut standarder for derivater. I 2004 ga COSO så ut det rammeverket som skal vurderes senere i denne oppgaven: Enterprise Risk Management – Integrated Framework and Application Techniques (COSO, 2004).

En av de kanskje viktigste pådriverene for den videre utviklingen og suksessen til ERM er at tidlige brukere har kunnet vise til håndfaste fordeler som resultat av at de har tatt i bruk en eller annen form for ERM. Eksempler på fordeler som har blitt rapportert er forbedring av aksjepriser, oppgradering av gjeldsratinger, tidlige risikovarsler, reduksjon av tap og redusert behov for ansvarlig kapital.

I den tidlige fasen av utviklingen av ERM har finansindustrien vært en viktig pådriver, mye på grunn av at de er så utsatt for risikoer som er vanskelige å håndtere og kvantifisere (for eksempel operasjonell risiko og stor prisvolatilitet). Deregulering og økende prisvolatilitet i energiindustrien har ført til at også denne har blitt mer og mer medvirkende i utviklingen, og i tiden etter the Sabanes-Oxley Act har stadig flere industrier meldt seg på.

I sin bok *Enterprise-Wide Risk Management – Strategies for linking risk and opportunity*(DeLoach, 2000), skriver James DeLoach at det for tiden ikke finnes et perfekt ERM-rammeverk som er allment akseptert i og på tvers av industrier. Videre sier han at den situasjonen vi befinner oss i er et paradigmeskifte i strategist tenkning fra de tidligere holdningene om at risiko bare er negativt og må unngås, til en mer positiv holdning som sier

at risiko også kan by på positive muligheter. Dette innebærer at man også må endre måten bedrifter håndterer sine risikoportfolier, og som et resultat av dette har man satt i gang utviklingen av ERM-rammeverker.

The Institute of Internal Auditors Research Foundation publiserte i 2001 tall fra en undersøkelse som sa at ca 50 prosent av alle selskapene som hadde besvart undersøkelsen hevdet å i det minste ha et delvis ERM-rammeverk på plass, mens det bare var rundt 10 prosent som mente de hadde et fullstendig rammeverk på plass i selskapet sitt (Miccolis et al., 2001).

2.2 ERM i dag

2.2.1 Tall fra den globale forsikringsindustrien

Towers Perrin utførte i 2008 en global spørreundersøkelse innen forsikringsindustrien for å slå fast statusen på ERM. Undersøkelsen viser at større selskaper, selskaper som har en fortjeneste på over $10 millioner, har kommet betydelig lenger i implementering av ERM enn mindre bedrifter. Av disse står europeiske selskaper mye sterkere enn sine nordamerikanske motparter. Nøkkelen til dette viser seg å være de store, og da i særklasse de europeiske, selskapenes evne til å håndtere økonomisk kapital, noe som har vist seg som en svært stor utfordring for mange. Videre konkluderer spørreundersøkelsen at ERM, på tross av vanskeligheter med implementering, allerede påvirker beslutninger som blir tatt i selskapene. Noen av beslutningene som har hatt størst påvirkning fra ERM er de som gjelder selskapenes risikoappetitt, investeringsstrategier og produktprising. Et siste funn som presenteres i spørreundersøkelsen, og som er relevant til denne oppgaven, er at operasjonell risiko fortsatt er et svakt punkt. Dette blir forklart med at operasjonell risiko ikke kommer spesielt høyt på prioriteringslisten(TowersPerrin, 2009).

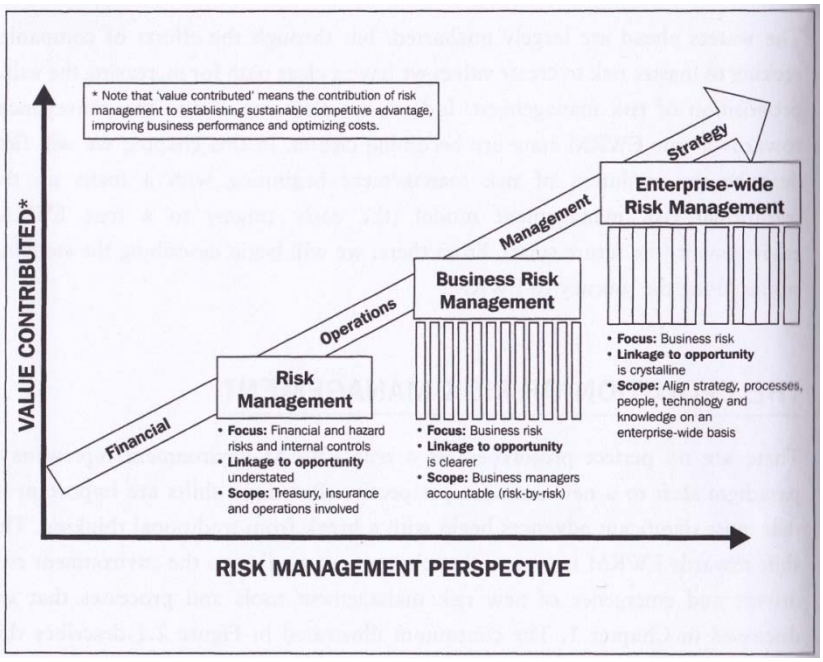
2.2.2 Hva er ERM?

Tradisjonelt sett har det vært mest vanlig å plassere bedriftenes forskjellige risikoer i ”risikosiloer”. Det vil si at markedsrisiko, kredittrisiko, operasjonell risiko med mer har blitt håndtert hver for seg og gjerne av forskjellige uavhengige enheter. Ulike risikoer kan påvirke hverandre, og porteføljeeffekter kan være lette å overse dersom man ikke har en helhetlig og integrert strategi for risikostyring. Det blir vanskelig å styre risiko i henhold til organisasjonens totale risikoappetitt, og i tillegg kan enkelte risikoer være vanskelige å klassifisere og vil dermed ”falle mellom” de etablerte siloene(Lam, 2003, Shaw, 2007).

I et forsøk på å imøtekomme slike problemer, har flere industriinitiativer gått sammen for å

utvikle Enterprise Risk Management, samt å utvikle forskjellige ERM-rammeverker. De fleste har blitt tatt svært godt imot når de har kommet ut, men har etter hvert måttet tåle en del kritikk. Som følge av dette finnes det enda ikke en vidt anerkjent industristandard som alle kan bruke som et felles referansepunkt.

De ulike organisasjonene, ekspertene og industriinitiativene har også litt forskjellige definisjoner på hva ERM er, men felles for de fleste er at de ser på et Enterprise Risk Management-rammeverk som en strategi for helhetlig risikostyring, som skal gjennomsyre bedriften eller organisasjonen på alle risikoberørte nivåer, samt legge til rette for at bedriften skal kunne avdekke muligheter i tillegg til farer. Figur 1 viser at Enterprise Risk Management, eller Enterprise-Wide Risk Management som James DeLoach kaller det, er en mer strategisk disiplin enn det tradisjonell risikostyring er.



Figur 1 - Utviklingen fra risikostyring til en strategisk prosess (DeLoach, 2000)

De mange varierende definisjonene for hva ERM egentlig er, gjør det vanskelig å evaluere forskjellige rammeverker og sammenligne dem. Spesielt med tanke på at hvert rammeverk gjerne har sin egen definisjon for hva Enterprise Risk Management er. For å gjøre et forsøk på å omgå denne problemstillingen, og unngå å bruke en definisjon som finnes i et av rammeverkene, vil arbeidet videre med denne oppgaven i stor grad basere seg på definisjonen utviklet av Joanna Makomaski(Makomaski, 2008):

Enterprise Risk Management:

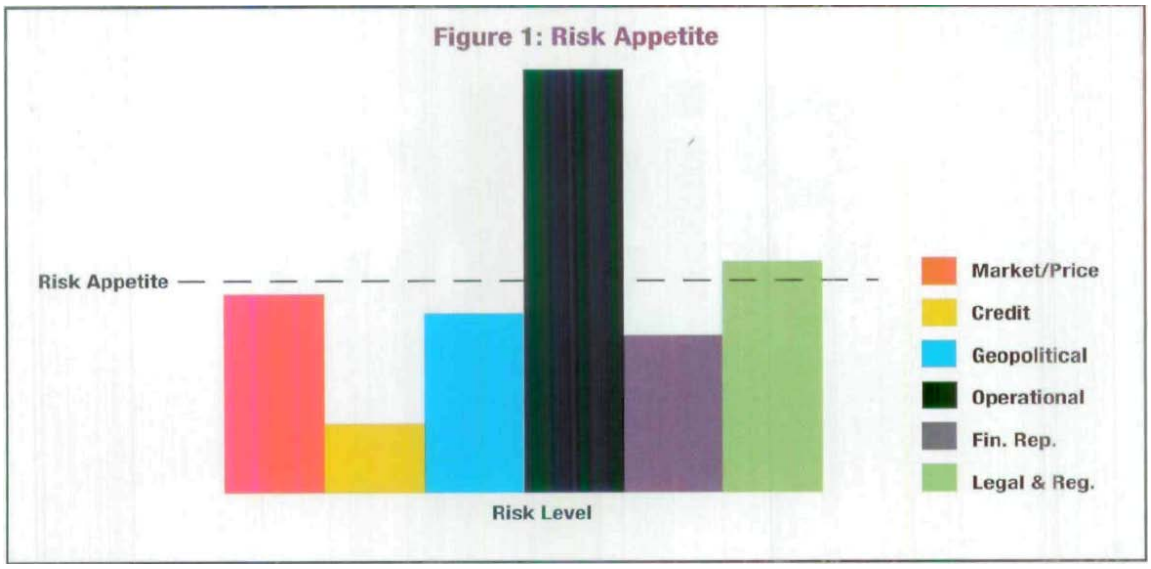
A decision-making discipline that addresses variation in company goals

Denne definisjonen ble utviklet på bakgrunn av andre definisjoners manglende evne til å forklare det definerte uttrykket uten å bruke selve ordene definisjonen skal definere. Ved å gå gjennom definisjonen ser vi at definisjonen beskriver risiko som graden av variasjon knyttet til selskapets mål. Dette støtter konseptet om at risiko ikke bare kan være negativt, ved at variasjon både kan skje i positiv og negativ retning. Definisjonen klargjør også ERMs rolle i daglige beslutningssituasjoner, et av hovedargumentene for bedrifter for å implementere ERM i sin organisasjon.

2.2.3 Viktige begreper

Risikoappetitt

Et viktig og grunnleggende begrep innenfor ERM er risikoappetitt. Risikoappetitt er den mengde risiko som et selskap er villig til å ta for å oppnå den avkastningen det forventer å få(Shaw, 2007). Finansmarkedene evaluerer selskapenes avkastninger og sammenligner dem med den mengden risiko de påtar seg for å oppnå denne avkastningen. Dersom forholdet mellom avkastning og risiko blir sett på som hensiktsmessig går verdien på selskapet opp, og vice versa(Shaw, 2007).



Figur 2 kilde: (Shaw, 2007)

Figur 2 viser en risikoappetittgraf. Dette er et eksempel på hvordan et selskap kan sammenligne forskjellige kategorier av risiko, og vurdere om de faller innenfor risikoappetitten. På figur 2 kan vi tydelig se at mengden operasjonell risiko er alt for stor i forhold til selskapets risikoappetitt. Men det, som i følge Jack Shaw, lett blir oversett av mange direktøren, er den andre risikoen som har stort avvik fra risikoappetitten. Den er rett og

slett for lav. Mange vil si at lavest mulig risiko er alltid er det beste, men det er også noe som heter ”no pain, no gain”, eller i risikoindustrien: no risk, no reward. Så for å maksimere selskapets verdi på finansmarkedet, som vanligvis er et selskaps overordnede mål, må selskapet forsøke å ligge så nærme risikoappetitten som mulig. Verken for langt over, eller for langt under(Shaw, 2007).

Dette resonnementet kan også brukes til å forklare en påstand som er en gjenganger i ERM-litteratur: Ikke all risiko er negativ.

Risikodimensjoner

Senere i denne oppgaven vil du lese at det mange forskjellige oppfatninger og definisjoner av risiko. For å oppklare dette skriver Shaw at risiko i realiteten består av seks dimensjoner som alle må tas hensyn til:

1. Sannsynligheten for en relevant trend eller hendelse
2. Størrelsen på effekten av trenden eller hendelsen
3. Graden av usikkerhet i estimatet av sannsynligheten
4. Graden av usikkerhet i estimatet av størrelsen på effekten
5. Muligheten til å påvirke trenden eller hendelsens sannsynlighet
6. Muligheten til å påvirke størrelsen på utfallet

Så i stedet for å bruke en generell definisjon på risiko, kan alle disse dimensjonene tas med i betraktning når en skal vurdere hvor stor en risiko er(Shaw, 2007).

2.3 Krav til et godt ERM-rammeverk

Enterprise Risk Management er ikke en ny måte å klassifisere og beregne risiko på, eller en ny type risiko i seg selv, men en strategi eller et rammeverk for å håndtere alle de ulike typene risikoer en organisasjon møter, slik at de kan opprettholde en balansert risikoportefølje. Så hvilke hvilke krav stilles til et godt ERM-rammeverk? Hva er det som gjør et rammeverk tilfredsstillende? Vi begynner med definisjonen på et rammeverk:

Framework:

1. A structure for supporting or enclosing something else, especially a skeletal support used as the basis for something being constructed.
2. An external work platform; a scaffold.
3. A fundamental structure, as for a written work.
4. A set of assumptions, concepts, values, and practices that constitutes a way of viewing reality.

Kilde: www.thefreedictionary.com

Et ERM-rammeverk skal altså definere grensene for hva som hva som skal være med og hva som ikke skal være med i ERM-programmet. ERM-rammeverket skal ikke være en detaljert kokebok som beskriver alt ned til minste teskje med bakepulver.

I følge Alexandra Psica, forfatter av artikkelen *Auditing ERM Frameworks*, er det ideelle ERM-rammeverket skreddersydd for den enkelte bedrifts objektiver, iboende risiko og risikotoleranse. Rammeverket skal hjelpe bedriften å forutse potensielle konsekvenser av fremtidige hendelser, gjøre endringer for å minimere uønsket risiko, håndtere negative utfall dersom en hendelse inntreffer og oppfatte og utnytte muligheter som kan gi økt vekst. Rammeverket skal sikre beslutningstakere nødvendig informasjon i god tid til å ta riktige avgjørelser innenfor den bestemte risikotoleransen for å styre bedriften mot dens objektiver (Psica, 2008).

Flere av rammeverkene som undersøkes i denne oppgaven er standardiserte rammeverk som er utformet med den hensikt at de skal tilfredsstille flest mulig bedrifter og hjelpe dem med å implementere ERM i deres organisasjon. For å kunne leve opp til ønsket om et skreddersydd rammeverk er det derfor viktig at disse rammeverkene tilbyr fleksible løsninger slik at de enklest mulig kan tilpasses den enkelte bedrift.

I boken *Enterprise Risk Management – From Incentives to Controls* presenterer James Lam det han mener er et godt ERM-rammeverk. Det brytes ned til syv nøkkelkomponenter som skal fungere som en helhet(Lam, 2003):

Tabell 1: Lams 7 komponenter for et vellykket ERM-rammeverk

Komponent	**Beskrivelse**
Felles styresett	• Felles prosesser og kontroller for måling og styring av risiko. • Felles risikopolitikk/holdninger, risikoappetitt, vokabular og tapstoleranse for hele organisasjonen. Styrets ansvar: • Definere organisasjonsstruktur og ansvarsfordeling mellom risikostyringspersonell, inkludert CRO[1]. • Forme risikokultur gjennom ord, handlinger og incentiver • Legge tilrette for organisatorisk læring, inkludert læring fra tidligere hendelser, kontinuerlig trening og -utvikling
Linjeledelse	• Skal ha høyt fokus i rammeverket, da linjeledere er i nær kontakt med organisasjonens verdiskapning og risikoeksponering • Forretningsplan og organisasjonens felles risikopolitikk må samkjøres ved oppstart av nye prosjekter • Prosesser for transaksjoner og investeringsanalyser må utvikles for å sikre riktig prioritering av oppmerksomhet slik at risikoer og muligheter ikke blir oversett. • Effektive og gjennomsiktige prosesser hjelper linjeledelse å forstå hvilke risikoer de kan akseptere individuelt, og hvilke som krever behandling på høyere nivå.
Porteføljeledelse	• Sikrer fullstendig oversikt over hele organisasjons risikoportefølje. • Utvikler gode porteføljemål og risikogrenser for å sikre optimal diversifisering og utbytte • Gir en direkte link mellom risikoledelse og aksjeeieres verdimaksimering
Risikooverføring	• Strategier for å redusere kostnader knyttet til redusering av uønsket risiko, i tillegg til å øke organisasjonens kapasitet til å beholde ønsket men konsentrert risiko • Sikre at risikooverføringsalternativer (som derivater, forsikringer og lignende) evalueres

[1] CRO – Chief Risk Officer

	på et felles grunnlag, slik at man kan velge det mest kostnadseffektive alternativet
Risikoanalyser	Avanserte metoder og teknikker for å: • Lette arbeidet med å kvantifisere ulike typer risiko på et mer konsistent grunnlag • Evaluere ulike risikooverføringsprodukter • Finne den mest kostnadseffektive måten å redusere risikoeksponering • Forbedre nåverdiberegninger og andre verdibaserte beslutningsverktøy ved å innarbeide risikokostnader
Teknologiske ressurser	IT-systemer for å lette arbeidet med store sammenhopninger av risiko-, portefølje-, og markedsdata.
Interessentledelse	Sikre gjennomsiktighet for viktige interessenter gjennom god rapportering. Med god rapportering menes rapporter som skreddersys til de ulike grupper av interessenter, som for eksempel styre, ansatte, rating agencies og så videre. Slik sikrer man at de ulike gruppene interessenter får akkurat de dataene som de trenger

For at et ERM-rammeverk skal fungere fullt ut som ønsket, må hver av disse syv komponentene utvikles og tilegnes tilstrekkelig vekt og oppmerksomhet, samtidig som de må fungere som et enhetlig rammeverk. Dette rammeverket vil bli brukt som referanse ved vurderingen av de andre rammeverkene senere i oppgaven.

Kort oppsummert er spørsmålene som ønskes besvart ved evalueringen og sammenligningen av de ulike rammeverkene i denne oppgaven disse:

1. Er definisjoner og terminologier i samsvar med annen risikolitteratur?
2. Tilfredsstiller rammeverket alle de syv komponentene av ERM, og er disse tilfredsstillende behandlet?
3. Er rammeverket godt egnet for tilpassning til bedrifters individuelle behov?
4. Er rammeverket utsatt for positiv elle negativ omtale/kritikk?

3 Evaluering og sammenligning

Rammeverkene som evalueres i denne oppgaven:

1. ISO 31000:2009 Risk Management – Principles and guidelines(ISO, 2009)
2. BS 31100:2008 Risk Management – Code of Practice(BSI, 2008)

3. Enterprise Risk Management – Integrated Framework(COSO, 2004)
4. Overview of Enterprise Risk Management(CAS, 2003)

3.1 ISO 31000: Risk Management – Principles and Guidelines

I november 2009 ble *ISO 31000: Risk Management – Principles and Guidelines* gitt ut av the International Organization for Standardization (ISO). Standarden ble utviklet av ISO med hjelp fra interessenter fra flere forskjellige land, blant annet flere fra Canada og Australia. Den bygger i stor grad på den mye brukte australske og new zealandske standarden AS/NZS 4360 som har blitt nevnt tidligere i oppgaven. Standardens oppbygning og sammenheng er vist i vedlegg 1.

Denne internasjonale standarden utgir seg ikke for å være et ERM-rammeverk, og er ikke en vanlig standard som skal brukes til sertifisering. I stedet er det en veiledning til effektiv og helhetlig risikostyring for bedrifter, organisasjoner, enkeltpersoner eller nasjoner. Den skal også være like funksjonell for alle typer risiko og det skal være opp til den enkelte bedrift å tilpasse rammeverket til de typene risiko de er eksponert mot. ISO 31000 aspirerer til å bli et felles referansepunkt for framtidige risikorammeverker, og grunnstammen i standarden som skal sørge for den statusen og funksjonen som ønskes er elleve prinsipper sammen med definisjoner, terminologier og et veiledende rammeverk.

ISO 31000 har fått meget god mottagelse globalt, og da særlig i Canada der den har blitt vedtatt som nasjonal standard av the Canadian Standards Association(Rankin and Morton, 2010). Standardens fleksibilitet blir fremhevet som en av de største styrkene, noe som skal gjøre standarden egnet for bruk i alle industrier og professor Jean-Paul Louisot ved Universitetet i Paris og Sorbonne kaller det risikolederes nye mantra og et referansepunkt for framtidige ERM-rammeverk(Coccia, 2010). Et annet element som har fått positiv omtale er standardens definisjoner, terminologier og grunnleggende prinsipper(Rankin and Morton, 2010).

Standarden fremhever elleve prinsipper om risikostyring som svært viktige for vellykket risikostyring:

1. Risikostyring skaper og bevarer verdi
2. Risikostyring er integrert i alle organisatoriske prosesser
3. Risikostyring er en del av beslutningstaking
4. Risikostyring behandler usikkerheter eksplisitt
5. Risikostyring er systematisk, strukturert og hensiktsmessig

6. Risikostyring er basert på beste tilgjengelige informasjon
7. Risikostyring er skreddersydd
8. Risikostyring tar menneskelige og kulturelle faktorer med i betraktningen
9. Risikostyring er transparent og inkluderende
10. Risikostyring er dynamisk, iterativ og tilpasningsdyktig
11. Risikostyring støtter kontinuerlig forbedring av organisasjonen

Tanken er at bedrifter skal innlemme disse prinsippene i sin organisasjonskultur og ha dem som basis ved utvikling av et skreddersydd risikoprogram.

Alle er dog ikke like positive i sin omtale av den nye internasjonale standarden. I en artikkel for Society for Risk Analysis retter Matthew Leitch kraftig kritikk mot store deler av standarden (Leitch, 2010). Kritikken rettes først mot det som skal være bærebjelkene i standarden; terminologi og definisjoner. Han uttrykker sin skuffelse over at definisjonene ikke klarer å forklare det de skal definere, og at de heller vanskeliggjør begrepene enn å forenkle dem. Kanskje den viktigste definisjonen som han retter kritikk mot er den nye definisjonen av risiko:

"The effect of uncertainty on objectives"

Definisjon ISO 31000

Denne nye definisjonen har av flere blitt godt tatt i mot, og stemmer godt overens med trenden i ERM-litteratur om at man ønsker å fjerne stempelet om at risiko er noe udelt negativt. Et forklarende notat for definisjonen sier at en effekt er et avvik fra det forventede – positivt og/eller negativt. Kritikken fra Leitch dreier seg her om at det er uklart hvordan et enkelt avvik kan være både positivt og negativt på samme tid.

Jon Piercey, visepresident i australske Methodware, er heller positiv til den nye definisjonen. Han mener at det er sunt å fjerne det negative fokuset på risiko, og at det ikke lønner seg å konstant jobbe for å fjerne eller minimere risiko. Han hevder at man heller bør basere seg på prinsippet i AS/NZS 4360 om at en streben mot forretningsmessige mål alltid vil være forbundet med risiko og usikkerhet, og at det er effektiv styring av risiko som gjør det mulig å nå målene(Piercey, 2010).

Den store styrken til ISO 31000, og som også er fremhevet av den ellers svært kritiske

Matthew Leitch, er at den legger stor vekt på at risikostyring skal få større fokus, og at det skal være en vesentlig del av ledelsesprosesser på alle nivåer i organisasjonen. Dette er godt i samsvar med kravene James Lam stiller til et godt ERM-rammeverk, og bidrar til standardens verdi som grunnlag for ERM-rammeverk

Et punkt som ikke vies oppmerksomhet i ISO 31000, og som er et av de mest sentrale områdene i ERM, er håndtering av risiko på et porteføljenivå. I punkt 5 i standarden, er det skrevet at man kan ta med flere risikoer ved definering av risikokriterier, men det stopper der. Strategier for overføring av risiko, håndtering av sammenhopning av risiko samt håndtering og identifisering av porteføljeeffekter er ikke tatt hensyn til, og må antas å falle inn under for eksempel punktet om risikobehandling. Dette gjør det klart at ISO 31000 ikke er et fullverdig ERM-rammeverk, og at organisasjonen selv må utvikle den delen av rammeverket basert på kunnskap fra annen risiko- og ERM-litteratur.

Ved gjennomgang av Lams syv komponenter for ERM ser det slik ut for ISO 31000:

1. **Felles styresett:** Får mye fokus. Blir lagt stor vekt på viktigheten av risikostyring, grunnleggende prinsipper, organisatoriske prosesser, mekanismer og risikokultur. Definisjonene er dog ikke kun positivt mottatt, og bedrifter må vurdere om de definisjonene som foreligger er tilfredsstillende for deres organisasjon og risikoeksponering.
2. **Linjeledelse:** ISO 31000 bekrefter gjennom prinsipper og store deler av standarden viktigheten av at risikostyring blir praktisert på alle relevante nivåer av organisasjonen. Hvordan dette skal gjennomføres og hvordan ansvar og oppgaver skal fordeles må utvikles av bedriftene selv og tilpasses egen organisasjon og kontekst.
3. **Porteføljeledelse:** Er ikke nevnt i standarden. For å oppnå et fullverdig ERM-rammeverk, og i det hele tatt kunne bruke ERM-navnet på rammeverket må det utarbeides retningslinjer og prosesser for porteføljeledelse for å fullt ut dra nytte av helhetlig risikostyring på tvers av organisasjonens enheter og nivåer.
4. **Risikooverføring:** Er ikke kommentert i standarden, noe som i beste fall kan unnskyldes med at det faller under punktet om risikobehandling. Dette punktet er uansett lite detaljert og det er fullt ut opp til den enkelte bedrift å identifisere hvilke alternativer de har for å behandle de risikoene de er eksponert for og som krever behandling.
5. **Risikoanalyser:** Det er i standarden utarbeidet en prosess for risikovurdering som omfatter identifisering, analysering, evaluering og behandling. Dette fungerer som en

grunnleggende veiledning til rekkefølgen i prosessen. Standarden inneholder ikke egne analyser eller en oversikt av tilgjengelige analyseverktøy og det er opp til bedriftens egne risikopersonell å velge det som er mest formålstjenelig for dem.

6. **Teknologiske ressurser:** Er ikke kommentert i standarden. Nødvendigheten av dette må vurderes av den enkelte bedrift.
7. **Interessentledelse:** ISO 31000 fremhever viktigheten av å etablere interne og eksterne kommunikasjon og rapporteringsmekanismer for å sikre informasjonsflyt mellom risikopersonell og alle andre interessenter, både vedrørende ulike risikoer og om selve rammeverket.

For å oppsummere har ISO 31000 stort sett fått en svært god mottakelse. Den imøtekommer flere av (men ikke alle) Lams syv komponenter for et suksessfullt ERM-rammeverk, og er utformet slik at det skal være svært tilpasningsdyktig til bedrifters individuelle behov. Som nevnt tidligere er ISO 31000 langt fra å være et fullverdig ERM-rammeverk, og kan bare brukes som et grunnlag for utvikling av eget rammeverk, evt. til vurdering og forbedring av eksisterende rammeverk. Det som kanskje er viktigst å huske på dersom man velger å basere utviklingen av et rammeverk på ISO 31000 er at man ikke overser betydningen av å ha en god oversikt over hele organisasjonens risikoportefølje.

3.2 BS 31100:2008 Risk Management – Code of Practice

Den britiske standarden BS 31100 Risk Management – Code of Practice ble gitt ut av BSI British Standards i oktober 2008. Standarden inneholder et konseptuelt rammeverk for ERM, og er utviklet som en veiledning som bygger på den internasjonale standarden ISO 31000.

Ved utviklingen av BS 31100 ble det lagt til grunn at standarden skulle stemme overens med den da kommende ISO 31000. Som følge av dette inneholder BS 31100 nøyaktig de samme 11 grunnprinsippene, og definisjonene som er listet i *Glossary* sist i standarden er, med noen få unntak, hentet direkte fra ISO 31000. Likevel er det noen områder der den britiske standarden skiller seg fra den internasjonale.

Det første man legger merke til er at alle standardens ulike deler er grundigere forklart, og i flere tilfeller er det letter å forstå hva som menes. BS 31100 klarer på en bedre måte enn ISO 31000 å forklare det som for mange er vanskelig å forstå. At risiko kan være både negativt og positivt. BS 31100 forklarer dette med at et godt risikostyringsprogram skal gjøre det lettere å identifisere hendelser som kan ha negativ påvirkning på objektiver, samt hendelser som kan ha positiv påvirkning. Videre skal rammeverket assistere risikopersonell i å redusere

sannsynligheten for at negative hendelser inntreffer, samt redusere potensielle utfall. Tilsvarende skal rammeverket assistere risikopersonell i å øke sannsynligheten for positive hendelser, og om mulig øke potensielle utfall.

Tabell 2: BSI 31100 risikostyringsrammeverk:

Område	**Rammeverkets komponenter**
Fullmakter og engasjement	Styresett
Rammeverkets design for risikostyring	• Risikostyringsstrategi • Risikostyringspolicy • Risikostyringskultur • Bygging av kapasitet og kompetanse • Roller, ansvar og fullmakter • Risikoappetitt og -profil • Risiko- og konsekvenskategorisering og -måling • Risikokriterier
Implementering av risikostyring	• Risikokommunikasjon • Risikostyringsprosesser • Utvikling av risikostyringsaktiviteter
Overvåking og vurdering av rammeverket	• Risikorapportering • Implementering og vedlikehold • Overvåking, vurdering og kontinuerlig forbedring
Vedlikehold og forbedring av rammeverket	• Implementering og vedlikehold • Overvåking, vurdering og kontinuerlig forbedring

BS 31100 skillers seg også fra den internasjonale standarden ved at det retter større fokus på individuelle roller og bygging av kompetanse. Standarden synliggjør viktigheten av at det finnes systemer for at relevant personell har tilstrekkelig kunnskap om

- Selskapets styresett og bakgrunnen for dette
- Lovgivning relatert til risikostyring og metoder for å etterleve dette
- Organisasjonens risikopolicy
- Organisasjonens risikoappetitt og regler for økning
- Risikostyringsprosessen
- Hvordan identifisere, evaluere og håndtere risiko
- Verktøy og teknikker for risikostyring
- Krav til risikorapportering
- Organisasjonens tilstand vedrørende risikokapasitet
- Ulike roller og ansvar blant organisasjons ansatte

På denne måten skal bedriften sikre at alle som kan ha innflytelse på bedriftens risikoer, kan håndtere sitt ansvar på en kontrollert og informert måte. BS 31100 er også klarere enn den internasjonale standarden i å synliggjøre roller, ansvar og fullmakter. Standarden gir leseren en oversikt over hvilke roller, ansvar og fullmakter som hører til hvor, og fordeler dem mellom toppledelse, individer, risikoeiere med mer.

I likhet med ISO 31000 blir det heller ikke her viet mye oppmerksomhet til hele organisasjonens risikoportefølje. Det blir dog definert en ekstra rolle som ut fra bedriftens størrelse og behov kan vurderes å ta med. Denne rollen kalles Risk Management Oversight Body. Denne rollen skal etter den britiske standarden utføres av en risikokomité eller en komité bestående av utvalgte personer fra styret (eller tilsvarende). Risk Management Oversight Body skal bistå toppledelsen med etablering av risikoappetitt, overvåke overholdelse av organisasjonens risikopolicy, behovet for kontroller og endringer i organisasjonens risikoprofil, samt rapportere alle funn tilbake til toppledelsen. Andre oppgaver som tilfaller denne rollen er periodiske vurderinger av risikostyrings- og rapporteringsprosesser, og tilstrekkeligheten av risikostyringsressurser.

I tillegg sier standarden at bedrifter kan, dersom organisasjonens risikorammeverk er omfattende, vurdere å ansette en egen risikostyringsavdeling eller en risikodirektør (beskrevet som CRO av James Lam(Lam, 2003)). Risikostyringsavdelingen/Risikodirektøren skal arbeide under veiledning fra Risk Management Oversight Body dersom denne eksisterer. Denne rollen får da ansvaret for å, blant annet:

- håndtere risikostyring og risikoeierskap på alle nivåer i organisasjonen
- Bygge en god risikokultur, inkludert undervisning og opplæring
- Utvikle, implementere og vurdere rammeverk og risikostyringsprosesser
- Koordinere respons på risiko som berører mer enn et område av organisasjonen
- Forstå forholdet mellom hovedinteressenter
- Rapportere til toppledelse, styre og hovedinteressenter

BS 31100 inneholder en del inormative vedlegg som kort beskriver hvilke typer risiko bedrifter kan være eksponert for samt en god oversikt over ulike verktøy for risikostyring. Risikostyringsverktøyene er gruppert etter bruksområdene risikoidentifikasjon, vurdering og respons. I tillegg presenterer den en veiledning til hvordan bedrifter kan måle modenhenten av sitt risikostyringsprogram. Alle disse vedleggene er nyttige for bedrifter som vil utvikle et risikostyringsrammeverk, og vil også være nyttig for de bedriftene som allerede har et

rammeverk på plass, men ønsker å evaluere det der har.

BS 31100 Skiller seg altså ikke så mye fra ISO 31000, men gir litt grundigere beskrivelser for hvordan en bedrift bør utvikle sitt eget rammeverk for risikostyring. Standarden er utarbeidet på en måte som gjør den lett å skreddersy til bedriftenes individuelle behov. Definisjonene som var gitt i ISO 31000 har som nevnt tidligere i oppgaven måttet tåle en del kritikk, og den samme kritikken vil dermed gjelde for BS 31100. Det skal dog nevnes at standarden gir bedriftene selv ansvaret for å utarbeidet et felles risikovokabular for deres organisasjon, og at definisjonen som her er presentert i et vedlegg antas å være veiledende.

3.3 COSO: Enterprise Risk Management – Integrated Framework

"Risk Management – Integrated Framework" er utviklet av PriceWaterhouseCoopers for the Committee of Sponsoring Organizations of The Treadway Commission (COSO), og ble først publisert i 2004. Rammeverket bygger på COSOs tidligere rammeverk for intern kontroll, *"Internal Control – Integrated Framework"(*COSO, 1992). Hensikten med rammeverket er å være en grundig retningslinje for hvordan organisasjoner skal få en mer fullstendig risikostyringsprosess.

Mens AS/NZS 4360 har vært det mest utbredte rammeverket utenfor Nord-Amerika, er det COSOs rammeverk som har vært mest utbredt tatt i bruk i USA og Canada. Det skiller seg fra AS/NZS 4360 og ISO 31000 ved at det skal være et mer komplett ERM-rammeverk som skal være mer elle mindre klart for implementering i bedrifter, store som små.

Definisjonen som er lagt til grunn for rammeverket er:

"Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives"(COSO, 2004)

Allerede her merker man at COSO går mye grundigere til verks enn ISO gjør i sin standard. Denne definisjonen blir utdypet og forklart over de neste fjorten sidene rammeverket. Dette er nyttig da definisjonen i seg selv fort kan skape mer forvirring enn den hjelper oss å forstå hva ERM innbefatter. Definisjonen får blant annet kritikk fra Joanna Makomaski for det faktum at de bruker ordene som skal defineres i selve definisjonen, noe som krever at den som leser definisjonen i hvert fall har en grunnleggende kunnskap om hva risiko er(Makomaski, 2008).

Et sammendrag av utledningen gir oss litt forklaring på hva som menes med definisjonen(COSO, 2004):

1. En prosess: ERM er et kontinuerlig og gjentakende samspill mellom alle handlinger, som gjennomsyrer foretaket. Disse handlingene er gjennomgående og iboende i måten ledelsen driver sin virksomhet.
2. Gjennomført av mennesker: ERM blir satt i gang og gjennomført av ansatte i bedriften, både styre, ledelse og annet personell. Med dette menes at det gjennomsyrer holdninger og handlinger til menneskene i organisasjonen.
3. Anvendes i valg av strategi: Risikovurderinger skal tas med i beslutningsprosesser knyttet til valg av strategi og ellers i organisasjonen.
4. Hendelser som kan påvirke foretaket: Forklares med at hendelser kan ha både positiv og negativ innvirkning på foretakets oppnåelse av mål. Dette blir videre forklart med at hendelser med negativ innvirkning representerer risikoer, mens hendelser med positiv innvirkning representerer muligheter.
    - Videre blir risiko og mulighet definert som:
        - Risiko: sannsynligheten for at en hendelse vil inntreffe og negativt påvirke oppnåelse av mål
        - Mulighet: sannsynligheten for at en hendelse vil inntreffe og positivt påvirke oppnåelse av mål
5. Risikoappetitt: Den mengden risiko foretaket er villig til å ta i sin søken etter verdi.
6. Gi rimelig sikkerhet: begrunnet med at risiko er relatert til framtidige hendelser, som ikke kan forutses absolutt.

Det kanskje viktigste punktet å kommentere videre her, er COSOs definisjon og forklaring på hendelser og risiko. Dette skiller seg ut fra den generelle holdningen innenfor ERM til at risiko ikke er utelukkende negativt. I tillegg får definisjonen av risiko kritikk fra Ali Samad-Khan(Samad-Khan, 2005) for å være helt inkonsekvent definisjonen som blir brukt i risikostyringsindustrien. Som et resultat av dette hevder Samad-Khan at COSOs rammeverk er helt upassende for styring av operasjonell risiko. Dette kan forklares videre med at COSOs definisjon for risiko innebærer at de største risikoene er de som har høy sannsynlighet, kombinert med stort negativt utfall. Eksempelet han bruker for å illustrere dette går slik:

Tabell 3: Risiko

	Sannsynlighet	x	Utfall	=	Risiko
Risiko 1	10 %	x	$10,000	=	$1,000
Risiko 2	1 %	x	$50,000	=	$500

Tabellen viser at ved bruk av COSOs definisjon blir risiko 1 sett på som den største og farligste, selv om risiko 2 potensielt kan påføre betydelig større tap. Slike risikoer blir av risikoindustrien ellers sett på som fantomrisiko, altså en risiko som ikke er realistisk. Risiko 2 vil i litteratur for operasjonell risiko bli beskrevet som en halehendelse, en hendelse som har lav sannsynlighet men potensielt stort utfall. Det er slike hendelser som betraktes som svært viktige innenfor operasjonell risiko, og vil lett bli oversett ved bruk av COSOs definisjon.

Enterprise Risk Management – Integrated Framework definerer 8 komponenter som til sammen utgjør ERM. Disse er i realiteten hendelsesforløpet i ERM slik COSO ser det:

1. Internt miljø
2. Målsetting
3. Hendelsesidentifisering
4. Risikovurdering
5. Risikorespons
6. Kontrollaktiviteter
7. Informasjon og kommunikasjon
8. Overvåking

Punkt 1 går på holdninger og filosofi blant styre, ledelse og ansatte vedrørende risikostyring, og fremmer de samme verdiene som James Lams første komponent, felles styresett. COSO framhever at det er ledelsens ansvar å utvikle og vedlikeholde en god risikokultur. Punkt 2 Mål må eksistere før det kan være noe risiko forbundet med det, og ERM skal sikre at det eksisterer prosesser som kan hjelpe ledelsen å gjøre risikovurderinger av potensielle mål, sikre at beste alternativer blir valgt og at dette skjer innenfor selskapets overordnede mål og risikoappetitt. Punkt 3 dreier seg om prosesser og verktøy for å identifisere mulige hendelser, for så å definere dem som potensielt negative (risiko), positive (muligheter), eller begge deler. Sammen med Punkt 4, risikovurdering, utgjør dette det som tilsvarer Lams femte komponent, risikoanalyser. Punkt 5 gjelder ulike strategier for å hanskes med risiko, slik som akseptering, redusering og deling av risiko. Ledelsen velger strategier eller kombinasjoner av disse som

passer best overens med organisasjonens toleranser og risikoappetitt. Kontrollaktivitetene i punkt 6 skal sikre at de strategiene som ble vedtatt i punkt 5 blir effektivt utført og gir ønskede resultater. God informasjon og kommunikasjon (punkt 7) skal sikre at riktig og tilpasset informasjon blir sendt til riktige mottakere i god tid, slik at alle har den informasjonen de trenge for å ta gode og velinformerte beslutninger. I tillegg skal det sikre at alle har sine roller og ansvar klart for seg. Dette dekker store deler av komponent syv i Lams modell, interessentledelse. Den siste komponenten, overvåking, har en svært viktig funksjon i at den kontinuerlig skal vurdere selve rammeverket og sørge for kontinuerlig forbedring og tilpasning til endringer i omgivelsene. Dette skal sikre at rammeverket er tilpasningsdyktig og robust.

Komponent to i Lams modell, linjeledelse, får mye oppmerksom het i COSOs Intergrated Framework. Administrerende direktører får sitt ansvar vedrørende ERM grundig beskrevet som den som har det overordnede eierskapsansvar for en enhets ERM-program. Det er i mange tilfeller han som er best posisjonert for å ha porteføljeoversikt over alle enhetens risikoer. Rammeverket støtter også enkelte selskapers ønske om en egen risikodirektør[2] med hovedansvar for organisasjonens ERM-program. Videre legges det stor vekt på viktigeheten av god ansvarsfordeling og inkludering av ledelse og personell på alle nivåer, noe som samsvarer godt med Lams andre komponent. Likevel bærer mye av rammeverket preg av å være et ”top-down” rammeverk der hovedansvaret ligger på toppledelse og styre og deres evner til å ”hente” informasjon fra lavere nivåer i organisasjonen.

ISO 31000 fikk, som nevnt tidligere i oppgaven, kritikk for å ikke ta hensyn til porteføljeeffekter. COSOs rammeverk har i tillegg til et avsnitt om gjensidig avhengige risikoer, et avsnitt om porteføljeoversikt[3]. Med en oversikt over hele risikoporteføljen kan ledelsen vurdere om gjenværende risiko, etter risikobehandling i alle organisasjonens enheter er gjennomført, stemmer overens med organisasjonens totale risikoappetitt. Med et slikt overblikk blir ledelsen i stand til å vurdere om ekstra risikoreduseringstiltak må iverksettes dersom total risikoeksponering er høyere enn risikoappetitten. Dersom risikoeksponering i enkelte enheter er for høye, mens de er lavere enn akseptabelt i andre enheter, kan risiko overføres til mer risikoaverse enheter for å sikre en balansert portefølje. Til slutt kan ledelsen velge, dersom den totale risikoeksponeringen ligger langt under total risikoappetitt, å

[2] Chief Risk Officer (CRO)

[3] side 59 COSO 2004. Enterprise Risk Management - Integrated Framework. The Committee of Sponsoring Organizations of the Treadway Commission.

oppfordre enkelte enheter å akseptere større risikoer i ønskede områder for å øke enhetens vekst.

Enterprise Risk Management – Integrated Framework er mye mer omfattende og detaljert enn de tidligere nevnte standardene ISO 31000 og BS 31100. Dette gjør COSO's rammeverk til et aktuelt alternativ for de som ønsker et mer eller mindre ferdigutviklet rammeverk for deres organisasjon, men vil gjøre det vanskeligere å skreddersy rammeverket til deres individuelle behov.

3.4 CAS: Overview of Enterprise Risk Management

Overview of Enterprise Risk Management(CAS, 2003) ble utviklet av Casualty Actuarial Society(CAS) og utgitt i 2003. Det er utviklet med hovedfokus på å støtte opplæring av CAS' egne medlemmer innen risikostyring. Oversikten inneholder flere deler, men det er del tre og fire som blir gjennomgått i denne oppgaven:

- ERM-definisjoner og konseptuelt rammeverk
- ERM-språk, -modeller, -verktøy og –måling

"ERM is the discipline by which an organization in any industry assesses, controls, exploits, finances, and monitors risks from all sources for the purpose of increasing the organization's short- and long-term value to its stakeholders"

Definisjon fra CAS(CAS, 2003)

Denne definisjonen stemmer godt overens med den som er lagt til grunn for denne oppgaven, (jmfr. Punkt 2.2), og i og med at det Overview of Enterprise Risk Management går grundigere til verks og definerer nøkkelegrepene under ERM, beveger vi oss videre til selve rammeverket.

Tabell 4: ERM rammeverk CAS

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

Tabellen over er hentet fra det konseptuelle rammeverket og viser hvordan CAS ser for seg at risikostyring må gjøres i separate funksjoner i noen sammenhenger men at man i andre sammenhenger må se på alle typer risiko som en stor helhet.

Ved etablering av kontekst skal både ekstern, intern og risikokontekst vurderes. Vurdering av ekstern kontekst innebærer at selskapet skal vurdere sitt forhold til omgivelsene og utføre en SWOT-analyse[4]. Vurdering av intern kontekst innebærer en forståelse av selskapet overordnede mål, strategier for å nå målene og prestasjonsindikatorer. Ved vurdering av risikokontekst skal selskapet identifisere hvilke risikokategorier det er eksponert for og som må inkluderes i ERM-rammeverket.

Ved å følge CAS'rammeverk skal man nå identifisere og evaluere risikoer for hver av de definerte kategoriene. Dette kan forsvares med at ulike typer/kategorier av risiko beregnes på ulike måter og krever spesialister på sitt felt, men fallgruven her er at man lett kan overse risikoer som ikke lar seg kategorisere(Shaw, 2007).

Det neste steget, risikointegrering, samler alle kategoriene igjen for å vurdere

[4] SWOT: Strenghts – Weaknesses – Opportunities - Threats

porteføljeeffekter og gjensidige avhengigheter mellom ulike risikotyper. Dette er det eneste rammeverket som vurderes i denne oppgaven som direkte tar opp utfordringen med porteføljeeffekter.

Etter at man har prioritert mellom risikoer og vurdert hvilke som bør reduseres, utnyttes, overføres eller beholdes skal hele risikoprofilen og de valgte strategiene overvåkes og evalueres før informasjon fra dette steget blir brakt tilbake til steg en, kontekst, og hele prosessen starter på nytt i en evig syklus. På denne måten skal organisasjonen sikre at den oppfatter utviklingen i risikoporteføljen og får sikret at man har gjort riktige valg.

Rammeverket i *Overview of Enterprise Risk Management* er ikke veldig detaljert og grundig beskrevet men skal fungere som en innføring i hvordan et ERM-rammeverk kan se ut. Det er likevel interessant å se hvordan de tar hensyn til porteføljeeffekter på en måte som ingen av de andre rammeverkene gjør.

I del fire av dokumentet beskrives ulike verktøy og modeller som kan brukes til å måle organisasjonens prestasjoner samt risikomålinger slik at man ved å bruke ERM kan linke disse sammen og dermed identifisere hva som påvirker organisasjonens prestasjoner. Dette omfatter flere vanlige måleverktøyer, som Weighted Average Cost of Capital (WACC) og Value at Risk (VaR), og det blir her også tatt hensyn til halehendelser ved Tail Value at Risk (Tail VaR).

For å oppsummere så inneholder Overview of Enterprise Risk Management mye av det som er etterlyst i ERM-sammenheng men som glimrer med sitt fravær i de tidligere presenterte rammeverkene. Dette dokumentet fokuserer på de tekniske delene av ERM og forklarer dette på en ganske tilfredsstillende måte. Det som mangler her, og som det blir satt mye større fokus på i de andre rammeverkene er den organisatoriske delen av ERM. Hvordan ERM skal bygges inn i organisasjonen, ansvar skal fordeles og holdninger og risikokulter skal utvikles blir ikke beskrevet i CAS' konseptuelle rammeverk, og det blir derfor ikke en fullgod løsning for de som er ute etter et rammeverk som passer til sin organisasjon.

4 Oppsummering og sammenligning

Tabell 5: Oppsummering

Kriterie	**ISO**	**BSI**	**COSO**	**CAS**
Felles styresett	+	++	++	mangler
Linjeledelse	+	+	+	mangler
Porteføljeledelse	mangler	+/-	+	+
Risikooverføring	mangler	+/-	+	+
Risikoanalyser	mangler	+	+/-	+
Teknologiske ressurser	mangler	mangler	mangler	mangler
Interessentledelse	+	+	+	mangler
Definisjoner og terminologier	+/-	+/-	-	Kun definisjon av ERM
Mulighet for skreddersøm	++	++	-	+

Tabellen viser en oppsummering av de elementene som blir dekket i de ulike rammeverkene som er gjennomgått i denne oppgaven. ”+” indikerer bra dekket, ”++” indikerer meg godt dekket, ”-” indikerer dårlig dekket, ”+/-” indikerer mangelfult dekket, og ”mangler” indikerer at det ikke er beskrevet i rammeverket.

Som vi kan se ut fra tabellen er det ingen av rammeverkene som er vurdert i denne oppgaven som dekker alle kravene til et fullstendig ERM-rammeverk. Og det er store variasjoner i hva som blir lagt mest fokus på i de ulike rammeverkene. Felles styresett, eller corporate governance som det kalles i standardene, er det som tre av fire rammeverk er best beskrevet. Det er store likheter mellom ISO 31000, BS 31100 og COSOs ERM Integrated Framework på dette området, og det er tydelig at de med dett ønsker å klargjøre viktigheten av at styre og ledelse har stor eierskapsfølelse når et ERM-prosjekt blir satt i gang. Dette blir av alle rammeverken indentifisert som en kritisk faktor for suksess. En fallgrop med denne viktigheten kan være at, dersom det ikke er tydelig nok beskrevet i det veiledende rammeverket kan man risikere å vie for mye oppmerksomhet mot styret og ledelsens rolle i ERM, og på den måten glemme å inkludere risikopersonell på lavere nivåer i tilstrekkelig grad. Disse er også viktige da disse opererer nærmere risikoers kilder og utspring, og vil være de som hovedsaklig vil være først ute med å oppdage nye farer og muligheter. Etter arbeidet med denne oppgaven virker det tydelig at styre og toppledelses viktigste ansvar er å utvikle

rammeverket, fordele oppgaver, ansvar og fullmakter på mest mulig hensiktsmessig måte. Ansvaret for å ha oversikt over hele risikoporteføljen bør gis til personer som sitter i, eller nær styret og toppledelsen, slik vedkommende har god oversikt og kort rapporteringsvei både oppover og nedover i organisasjonen.

Porteføljeledelse er beskrevet som selve kjernen i ERM, og er det som skal sikre at risikostyringen foregår på jevnt nivå i hele organisasjonen, altså hele enterprisen. Det er da noe underlig at dette får så lite oppmerksomhet i både BS 31100 og ISO 31000. Spesielt med tanke på at dette er de nyeste rammeverkene av de som er vurdert i denne oppgaven. En grunn til dette er at ingen av disse to rammeverkene utgir seg for å være ERM-rammeverk, men snarere bare risikorammeverk. På den andre siden ønsker de like fullt å være en veiviser til helthetlig risikostyring i organisasjoner, og selv om ERM-ordet elle konseptet ikke er nevnt i selve rammeverkene, er likhetene med tanke på holdninger og ambisjoner veldig like. Begge standardene blir også flittig nevnt i artikler og litteratur om ERM, og det er klart at de har en relevans for disiplinen. BS 31100 og ISO 31000 er utviklet for å være et referanse- og utgangspunkt for alle framtidige risikorammeverker, og det er mulig at de med dette ønsket blir for generelle for å brukes som eneste utgangspunkt for et ERM-rammeverk.

Ved vurderingen av rammeverkene ble det undersøkt hvilke analyseverktøy som er beskrevet i rammeverkene. Funnene viser at dette er lite beskrevet i nesten samtlige rammeverker. Dette kan sannsynligvis begrunnes med at bedriftene og organisasjonene selv må velge hvilke analyser som skal benyttes på bakgrunn av hvilke risikoer de er eksponert for. I rammeverkene blir det i stedet selve risikostyringsprosessen beskrevet i grov detalj, noe som vil være tilstrekkelig for de fleste. CAS går derimot litt lenger ved at de har et vedlegg som lister opp potensielle verktøy for risikoanalyse og prestasjonsmålinger.

Det eneste som mangler i alle rammeverkene er litteratur vedrørende teknologiske ressurser. Denne komponenten av ERM ble, som nevnt tidligere i oppgaven, beskrevet av James Lam som en viktig del av et velfungerende ERM-program. Dette kan begrunnet med at å hele tiden ha full oversikt over en hel organisasjons risikoportefølje innebærer å tolke enorme mengder risikodata, og det lar seg vanskelig gjøre uten gode IT-verktøyer. Grunnen til at dette ikke er tatt med i rammeverkene som her har blitt vurdert, kan være at dette er noe som vurderes som en selvfølge. Det blir dermed opp til bedriftene selv å vurdere hvordan de i praksis skal imøtekomme slike utfordringer. En annen forklaring kan også være at det ikke finnes gode nok komplette it-løsninger for ERM og at bedriftene da uansett må utvikle disse selv. Dersom den siste forklaringen er den gjeldende ville det være til stor hjelp om et veiledende

rammeverk også kunne tilby veiledning til hvordan en komplett IT-løsning bør utvikles og hvilke oppgaver IT-løsningen minimum må kunne håndtere.

Det vanskeligste temaet i denne oppgaven har vært å forholde seg til mange ulike og til tider motstridende definisjoner og terminologier. Dette har vanskeliggjort prosessen med å vurdere rammeverkene og kan forklare mye av stridighetene innefor ERM-diskusjonen. En grunn til dette kan naturligvis være tidsforskjellen mellom når de ulike rammeverkene ble publisert. Det synes likevel fortsatt å være stor uenighet om definisjoner av sentrale begreper innenfor ERM, og dette kan også være grunnen til at svært mange var positive til at det kom en internasjonal standard som skulle samle disiplinen på et globalt plan. Det er dog ikke kun enighet om definisjonene i ISO 31000 heller, og disse vil trolig være grunnlag for videre diskusjoner og forbedringer i årene som kommer.

Et av de viktige kravene som var stilt til et ERM-rammeverk, og som ble brukt til vurderingen i denne oppgaven var at et godt rammeverk skal være tilpasningsdyktig til bedrifters individuelle behov. Dette vil være et naturlig krav til et standardisert og veiledende rammeverk, men ikke nødvendigvis for et rammeverk som utviklet for mer spesifikke behov. Noe som er felles for ISO 31000, BS 31100 og COSO, er at de alle skal være standardiserte rammeverk som skal passe like godt for store som små organisasjoner og på tvers av alle industrier. Det som følger naturlig av et slikt krav, er at jo flere detaljer som er fastsatt i rammeverket, jo mindre tilpasningsdyktig og allment anvendelig vil rammeverket være. Sett på denne måten vil den internasjonale og den britiske standarden komme bedre ut av det enn COSO. På den annen side kan man risikere at rammeverket blir så generelt at det blir vanskelig å forstå hva det faktisk sier. Det vil da være nødvendig med supplerende litteratur og kunnskap for å utvikle et komplett rammeverk som er klart for implementering i organisasjonen. Hvis man ser det fra denne synsvinkelen vil trolig COSOs rammeverk komme best ut for mange. Løsningen fra CAS med å legge ved alternativer metoder for å utføre de ulike stegene i risikoprosessen kan være en god idé for videreutvikling av de andre rammeverkene. På denne måten får man informert om mulige løsninger uten å redusere tilpasningsdyktigheten til rammeverket.

Mye av vurderingen av rammeverkene i denne oppgaven har vært basert på en sammenligning med James Lams syv komponenter for et godt ERM-rammeverk. Dette har vært grunnlaget for vurderingen av de andre rammeverkene, og kan ha hatt innflytelse på utfallet av vurderingene. Sammenligningen av rammeverkene seg i mellom skal bidra til et mer rettferdig og objektivt resultat, men man bør likevel ha dette i bakhodet når man leser

oppgaven.

Ved å ta det beste fra hvert av rammeverkene kan vi bygge et nytt rammeverk. Basert på Lams syv komponenter vil dette da se slik ut:

Tabell 6: Sammensatt rammeverk

Kriterier	**Beste Rammeverk**
Felles styresett	COSO/BSI
Linjeledelse	ISO/BSI/COSO
Porteføljeledelse	COSO/CAS
Risikooverføring	COSO/CAS
Risikoanalyser	CAS
Teknologiske ressurser	-
Interessentledelse	ISO/BSI/COSO
Definisjoner og terminologier	ISO/BSI
Mulighet for skreddersøm	ISO/BSI

Ved hjelp av denne tabellen kan man lett se hvilke rammeverk som er sterkest på hver av de syv komponentene i James Lams referanserammeverk. Tabellen tydeliggjør også fraværet av teknologiske ressurser i samtlige rammeverk.

5 Konklusjon

Motivasjonen i denne oppgaven var å sammenligne høyt profilerte rammeverk for Enterprise Risk Management, for så å finne ut om det er et som peker seg ut som det best egnede for anbefaling til bedrifter som vil etablere et Enterprise Risk Management program i sin organisasjon.

Funnene som er gjort gjennom arbeidet med oppgaven indikerer at det fortsatt ikke finnes ett ERM-rammeverk som blir sett på som en fasit i bransjen. Gitt ERMs kompleksitet vil det være svært vanskelig å utvikle et rammeverk som kan godkjennes av alle, samtidig som det er klart for implementering i en hvilken som helst bedrift. Rammeverkene som er evaluert og sammenlignet i denne oppgaven skal fungere som veiledning og et utgangspunkt som bedriftene kan utvikle rammeverket sitt fra. Bedriftene må selv kartlegge sine behov, og forstå sin kontekst. De kan så velge hvilket eller hvilke rammeverk de skal ta utgangspunkt i, og

begynne å skreddersy det ideelle rammeverket for deres individuelle behov.

Videre funn tyder på at ISO 31000 kommer til å bli et populært rammeverk i årene som kommer, gitt dets enkle struktur, status som internasjonal standard, og svært gode muligheter for individuell tilpasning. Den mest åpenbare anbefalingen basert på denne oppgaven er likevel at man ikke avskriver noen alternativer før de er nøye vurdert. Flere av rammeverkene kan med fordel kombineres, da et rammeverk ofte dekker ulike deler av ERM på en bedre måte enn et annet. BS 31100 som ble utarbeidet og utgitt før ISO 31000, men som er basert på et tidligere utkast av den internasjonale standarden, kan med fordel brukes som et informativt supplement til ISO 31000. COSOs rammeverk har fortsatt mange tilhengere, men funnene i oppgavene tyder på at den har begynt å bli utdatert. Dersom man likevel ønsker å benytte rammeverket vil det derfor være anbefalt å vurdere rammeverket opp mot den nye internasjonale standarden og oppdatert risikolitteratur, for så å gjøre nødvendige justeringer. Det beste alternativet ut fra de rammeverkene som er tatt med i denne oppgaven vil være å sette sammen et rammeverk med utgangspunkt i det beste fra alle de vurderte rammeverkene, for så å supplere med oppdatert risikolitteratur.

6 Forslag til videre undersøkelser

Etter de siste årenes finansielle problemer og kriser er risikostyring et brennhett tema. Alt tyder på at dette er en trend som vil fortsette, og det vil være store muligheter for videre undersøkelser innen for denne disiplinen.

Et område som ofte stikker seg fram når det er snakk om manglende utvikling innenfor ERM er gode IT-verktøy som kan assistere i gjennomføringen av et ERM-program. Selv om det finnes løsninger som kan ta for seg deler av ERM, som for eksempel konsentrerer seg om enkelte kategorier av risiko, finnes det i skrivende stund ingen komplette it-løsninger som er laget for ERM i butikkhyllene. Interessant lesing kan være *Taking ERM to the Next Level(Liebowitz, 2007)*, og *Managing All Your Enterprise's Risks(Avsnitt: A solution to the ERM technology problem)(Shaw, 2007)*. Her kan du lese om RIMS' The Risk Maturity Model, og Causal Modeling.

Videre er definisjoner og terminologier et sentralt tema som er svært utsatt for diskusjoner og er helt klart et kapittel som ikke er ferdig. Da gjerne med fokus på operasjonell risiko som i følge undersøkelsen fra Towers Perrin fortsatt er et svakt punkt for ERM(TowersPerrin, 2009).

Referanser

BSI 2008. Risk Management - Code of Practice. BSI British Standards.

CAS 2003. Overview of Enterprise Risk Management. Casualty Actuarial Society.

COCCIA, R. 2010. International standard seen as framework for ERM programs. *Business Insurance,* 44**,** 1.

COSO 1992. Internal Control - Integrated Framework.

COSO 2004. Enterprise Risk Management - Integrated Framework. The Committee of Sponsoring Organizations of the Treadway Commission.

DEAKIN, S. & KONZELMANN, S. J. 2003. *Learning from ENRON,* Cambridge, ESRC Centre for Business Research, University of Cambridge.

DELOACH, J. W. 2000. *Enterprise-wide risk management : strategies for linking risk and opportunity,* London, Financial Times Prentice Hall.

DRUMMOND, H. 2008. The dynamics of organizational collapse the case of Barings Bank. *Routledge international studies in money and banking 46.* New York: Routledge.

ISO 2009. ISO 31000 Risk Management - Principles and Guidelines. 286 Sussex Street, Sydney NSW 2000 AUSTRALIA: SAI Global Limited.

LAM, J. 2003. *Enterprise risk management : from incentives to controls,* Hoboken, N.J. ; [Chichester], Wiley.

LEITCH, M. 2010. ISO 31000:2009—The New International Standard on Risk Management. *Risk Analysis,* 9999.

LIEBOWITZ, M. 2007. Taking ERM to the Next Level. *Risk Management (00355593),* 54**,** 44-44.

MAKOMASKI, J. 2008. So What Exactly Is ERM? *Risk Management (00355593),* 55**,** 80-81.

MICCOLIS, J. A., HIVELY, K. & MERKLEY, B. W. 2001. *Enterprise risk management : trends and emerging practices,* Altamonte Springs, Fla., Institute of Internal Auditors Research Foundation.

ONG, M. K. 2006. *Risk management : a modern perspective,* Amsterdam ; London, Elsevier Academic ;.

PIERCEY, J. 2010. Impact of ISO 31000 on existing ERM programs. Available: http://www.methodware.com/assets/Documents/whitepapers/Impact-of-ISO-31000-on-Existing-ERM-Programs.pdf [Accessed February 2010].

PSICA, A. 2008. Auditing ERM Frameworks. Available: http://www.entrepreneur.com/tradejournals/article/178351539.html.

RANKIN, E. & MORTON, D. 2010. Creating a Common Language. *Canadian Underwriter,* 77**,** 50-53.

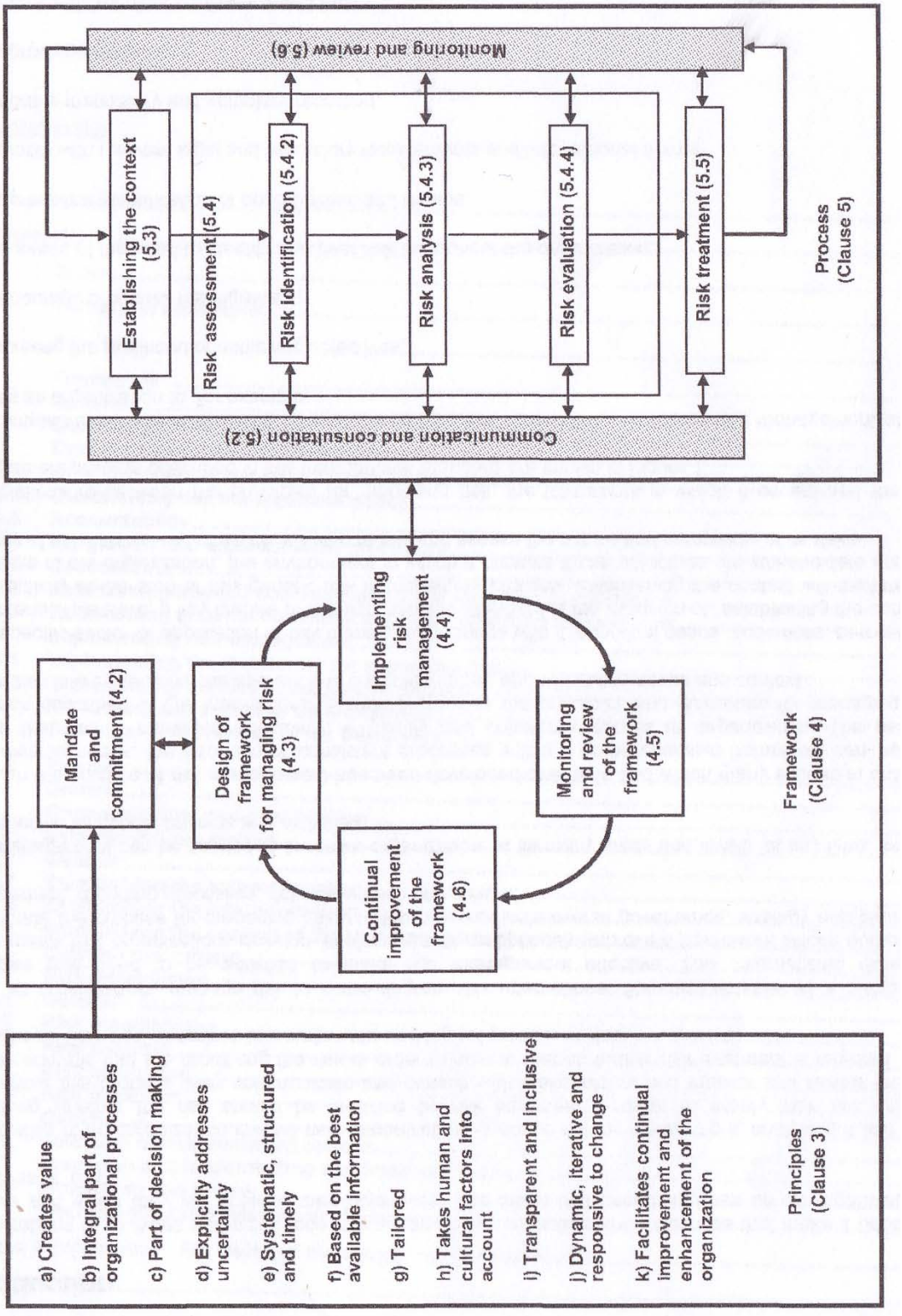
SAMAD-KHAN, A. 2005. Why COSO is flawed. *Operational Risk,* 6**,** 24-28.

SHAW, J. 2007. Managing All of Your Enterprise's Risks. *Risk Management (00355593),* 54**,** 38-44.

TOWERSPERRIN. 2009. Embedding ERM - A Tough Nut to Crack. Available: http://www.towersperrin.com/tp/getwebcachedoc?webc=GBR/2009/200901/2008_Global_ERM_Survey_12809.pdf.

Vedlegg

VEDLEGG 1



Sammenhengen mellom prinsipper, rammeverk og prosess i ISO 31000 (ISO, 2009)