

Enterprise Risk Management

– risikostyringens Hellige Gral

I de seneste 5-6 år har vi – såvel inden for som uden for den finansielle sektor – set en betydeligt stigende interesse for ”Enterprise Risk Management” (ERM) – et begreb, som kort fortalt dækker over en altomfattende proces, hvor samtlige virksomhedens risici identificeres, måles, styres og kontrolleres på langs og på tværs af forretningsområder. Ambitionsniveauet i ERM afstemmes efter ledelsens og/eller aktionærernes appetit på risiko, og belønningen for en succesrig implementering af konceptet skulle komme i form af øget konkurrencedygtighed, forbedret lønsomhed, mere ”shareholder value” – og en større robusthed over for forskellige former for ”overraskelser” af finansiell såvel som ikke-finansiell karakter.

FORFATTER



Direktør, cand.polit.
Søren Plesner
BASISPOINT

E-mail:
soren.plesner@basispoint.com

Søren Plesner er CFA Charterholder og certificeret Financial Risk Manager (FRM og PRM)

Jagten på denne risikostyringens ”hellige gral” drives af flere faktorer. For banker og sparekasser mv. er det i øjeblikket mere et spørgsmål om ”skal” end ”vil”, idet der i forbindelse med de umiddelbart forestående implementeringer af nye solvensregler, MiFID¹, hvidvaskelov mv. stilles tilsynsmæssige krav om opbygning af nye rutiner og systemer til risikostyringsprocesser, kapitalallokeringen, kundeovervågning mv. Men også markedsudviklingen – med globalisering, øget konkurrence og finansiell innovation som de vigtigste trends – motiverer i stigende grad bankdirektører mv. til at satse på forbedret risikostyring som central konkurrenceparameter.

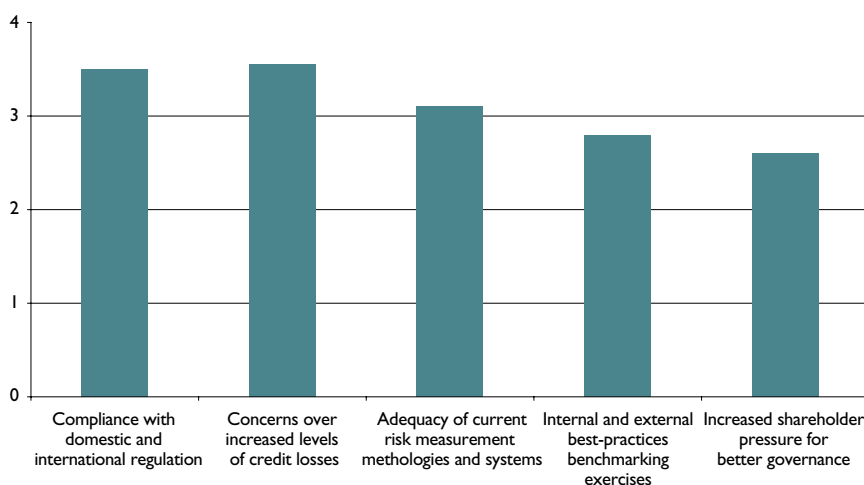
Såvel ”compliance” motivet (krav om efterlevelse) som den mere frivillige interesse for ERM bekræftes af en nylig undersøgelse, der blev gennemført af en verdensomspændende leverandør af IT-løsninger inden for risikostyring, se figur 1 og 2.

Som det fremgår, ses ”compliance with domestic and international regulation” som en væsentlig drivende faktor bag de adspurgte bankers ERM-programmer, men også mere økonomisk motiverede aspekter såsom ”Improved performance management” og forbedret prissætning af produkter vurderes som værende af stor betydning. For en nærmere beskrivelse af undersøgelsens metode og datagrundlag henvises til SAS Institute (2006).

Resultatet af ovennævnte undersøgelse skal naturligvis tages med et gran salt, for initiativtageren har jo i lighed med andre IT-leverandører, konsulentvirksomheder mv. en vis økonomisk interesse i at opmuntre til fortsat jagt på ”Gralen” – for derigennem at

Figur 1

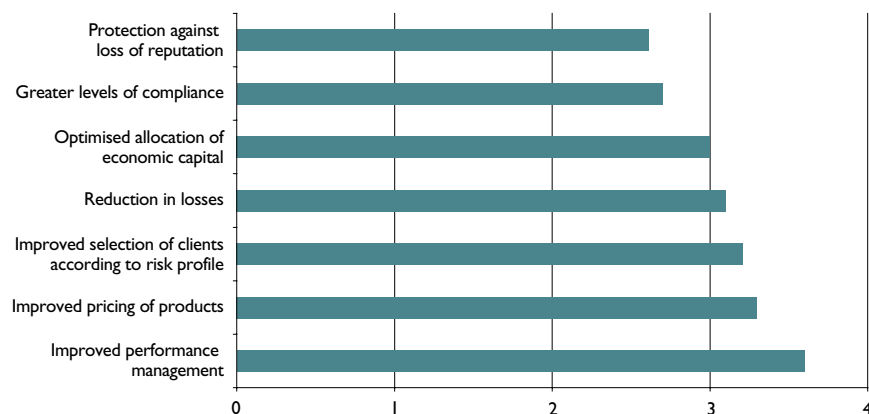
Drivkræfter bag bankers satsning på ERM



Kilde: SAS Institute

Figur 2

Potentielle gevinster ved forbedret risikostyring



Kilde: SAS Institute

fremme salget af services som "Business Process Reengineering", "integrated, end-to-end intelligence software", "Enterprise-wide Risk Management" systemer osv.

Bag alt dette fornemmer man alligevel – selv blandt de mere skeptiske – en reelt stigende erkendelse af, at et mere omfattende risikostyringsprogram – ERM eller hvad man nu ellers vil kalde det – vil være en afgørende faktor i den fremtidige kamp om markedsandele – og om aktionærers og kreditorers gunst.

Dette vil vi nu undersøge nærmere i det følgende. Der indledes med en gennemgang af den udvikling, der har ført frem til den øgede interesse for ERM. Derefter præsenteres og diskuteres den såkaldte COSO ERM model, der beskriver mål for og elementer i et generelt ERM-system. Endelig diskuteres det, om – og givet fald hvordan – der kan skabes værdi gennem ERM, og vi ser på de praktiske problemer, der er forbundet med implementeringen af et sådant system.

Vejen mod ERM

Blandt mere modne bankfolk tales der ofte med en vis vemod om dagene med "3-8-5" banking. Det var dengang, man kunne tage mod indlån til 3% og låne ud til 8% – og sætte kursen mod golfbanen kl. 5 om eftermiddagen! Renterne var lave og stabile, valutakurser lå fast og konkurrencen i banksektoren var begrænset. Dette var før globaliseringens og Internettets tid, og "risikostyring" stod ikke højt på dagsordenen.

Introduktionen i slutningen af 1980'erne af det første "Basel" regelsæt for beregning af risikokapital ændrede ikke meget herpå. Ganske vist skulle der nu beregnes og afsættes kapital til afdækning af kreditrisiko – og implicit også operationelle risici – men reglerne var meget lidt risikofølsomme og indeholdt ikke meget incitament til mere aktiv risikostyring. Tværtimod blev der i mange banker brugt flere penge og kræfter på at omgå de nye regler, da dette hurtigere og nemmere kunne føre til kapitalbesparelser, end hvis man skulle bruge tid og penge på at udvikle og forfine metoder til måling og styring af risici. Regelsættet blev siden hen udbygget med krav om kapitaldækning af "markedsrisici", men disse blev placeret i en selvstændig "silo", hvor de blev målt og styret helt adskilt fra kreditrisikoen.

Det var under disse betingelser ikke særligt glamourøst at være "risk manager", da det eneste "synlige" resultat af succesrig risikostyring var, at der *ingenting* skete! Når effekten ikke kunne måles direkte på bund-

linien, blev risikostyring behandlet som et "cost center", en besværlig, påtvungen betingelse for at drive forretning.

I løbet af 1990'erne skete der imidlertid noget, der efterhånden på ganske afgørende vis skulle ændre forudsætningerne for succes og overlevelse i den finansielle verden. Globaliseringen holdt sit indtog, og de finansielle markeder blev liberaliseret. Teknologisk udvikling gjorde fysisk afstand uvæsentlig og skabte forudsætningerne for en hastig finansiell innovation. Brugen af swaps, kreditderivater mv. eksploderede og muliggjorde siden hen introduktionen af nye, komplekse forretninger såsom "Collateralized Debt Obligations" og "Synthetic Securitizations". Denne udvikling har ført til en ny og mere effektiv arbejdsdeling og en skarpere prissætning på de finansielle markeder, men også til mutation og integration af de finansielle risici! Hybride risikoforformer såsom "modpartsrisiko", et ubehageligt, dynamisk miks mellem markeds- og kreditrisiko, er tiltaget i betydning. Endvidere betyder kompleksiteten af de nye forretningsformer, som ofte involverer mange afdelinger på tværs af eksisterende forretningsprocesser, at bankerne i dag er udsat for operationelle risici i et betydeligt større omfang end tidligere. En fejl, uautoriseret handel eller systemnedbrud i ét led af kæden kan føre til alvorlige problemer og store – i værste fald livstruende – tab for banken.

I kølvandet på denne udvikling opstod der efterhånden en erkendelse af, at den traditionelle "silo-opdelte" tilgang til risikostyringen ikke var egnet til at møde disse nye udfordringer. På det mere akademiske plan begyndte man at tale om "holistisk", eller "integreret" risikostyring, og da markedsføringsfolkene tog over, blev ideen – eller myten – om "Enterprise Risk Management" så født. Her skulle "silo-tilgangen" erstattes af et system, hvor forfølgelse af bankens/virksomhedens strategiske målsætning og risikostyring gik op i en højere enhed, og hvor samtlige risici kunne sættes på en fælles-nævner i form af "Økonomisk Kapital" og styres ud fra en *helhedsvurdering* af bankens solvens og konkurrencemæssige situation.

BASEL II – "the missing link"

De største, internationale banker var hurtigt med på ERM ideen og satte betydelige ressourcer ind på at udvikle systemer til allokering af "økonomisk kapital" og beregning af "risk adjusted performance".

Men både herhjemme og internationalt var mange bankdirektører fortsat skeptiske over for konceptet, der blev set som konsulentbranchens forsøg på at sælge gammeldags dyder som sund fornuft, godt kundekendskab og "rettidig omhu" i en ny og mere eksklusiv indpakning. Endvidere ville opbygningen af et komplet ERM-system som skitseret kræve omfattende indgreb i eksisterende arbejdsprocesser og udskiftning af IT-systemer – investeringer, der på det tidspunkt ikke var påkrævet for at leve op til gældende lovgivning, og som derfor kunne være svære at retfærdiggøre over for aktionærer mv.

I januar 2001 skete der så igen noget, der på afgørende vis skulle sætte skub i udviklingen inden for risk management industrien. Basel-komiteen barslede med et 600 sider stort oplæg til et komplet nyt regelsæt for beregning af bankers risiko-kapital, efterfølgende bedre kendt som "Basel II". Formålet med det nye regelsæt var, i lyset af den ovenfor beskrevne udvikling, dels at afhjælpe nogle af de åbenlyse mangler i det eksisterende regelsæt, dels at anspore banker til bedre risikostyring, kvantitativt såvel som kvalitativt. Regelsættet foreligger nu efter flere års høringer og "Quantitative Impact Studies" i sin (foreløbigt!) endelige form og skal efter planen træde i kraft i begyndelsen af 2007 – i EU-landene i form af det såkaldte Kapitalkravsdirektiv, CRD.

Konsulent- og IT-branchen var fra starten begejstrede for Basel II forslaget. Her var netop den manglende forbindelse, "the missing link", mellem "3-8-5" banking og et højere udviklingstrin. Bankerne skulle nu til at gå på tre ben! Basel II bygger nemlig – med et stabilt banksystem som målsætning – på tre søjler med et varierende indhold af stok og gulerod. I "søjle 1" er der lagt op til betydeligt mere risikofølsomme regler for beregning af risikokapitalen, herunder et eksplicit kapitalkrav til dækning af tab fra operationelle risici. Reglerne er dog graduerede, således at banker kan vælge mellem "avancerede" eller "standard" metoder. Større banker *forventes* – i hvert tilfælde med tiden – at "vælge" de avancerede metoder, hvorimod mindre – eller mindre sofistikerede banker – kan bruge standard-metoderne, der vil kunne implementeres med begrænsende ressourceindsats.

Uanset, om der vælges "avancerede" eller "standard" metoder er der med "søjle 1" reglerne imidlertid fortsat tale om en "silo"-tilgang til risikoopgørelsen, dvs. en

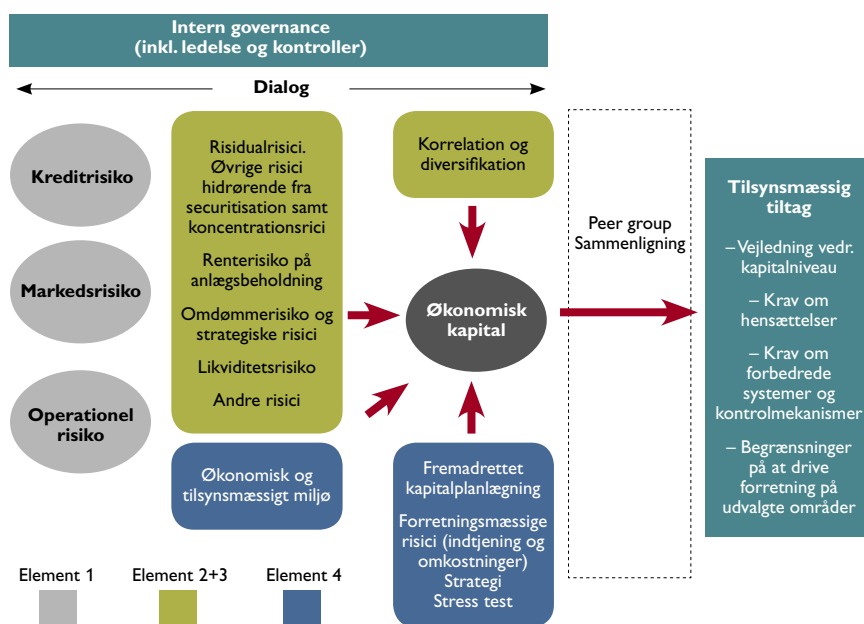
separat opgørelse af markedsrisici, kreditrisici og operationelle risici, som herefter lægges sammen for at nå frem til samlet kapitalkrav. Heri ligger der så ikke isoleret set noget incitament til en mere ”integreret” risikostyring.

De fra et ERM-perspektiv mest interessante – for bankerne potentielt mest omkostningskrævende – nyskabelser i Basel II (og CRD) er imidlertid de betydelige kvalitative krav til risikostyringen (søjle 2) – samt inddragelsen af markedsdisciplin (søjle 3).

Søjle 2 er udformet som en tilsynsproces *Supervisory Review Process (SRP)*, som har til formål at skabe en bedre sammenhæng mellem et instituts risikoprofil, risikostyring og kapital. Der er to væsentlige elementer i denne proces: ICAAP og SREP. Med ICAAP (*Internal Capital Adequacy Assessment Process*) pålægges det bankerne at sikre tilstrækkelig kapitaldækning af *samlige* (væsentlige) risici – og ikke blot de tre risikoformer, der er underlagt minimums-kapitalkravene i søjle 1. Intern (økonomisk) kapital ses her som et vigtigt styringsværktøj, og instituttet er forpligtet til at indrette ledelses-, styrings- og kontrolprocesser på at sikre en effektiv allokering heraf (”Robust Government Arrangements”). Disse ”arrangements” skal omfatte klare procedurer for identifikation, måling, styring, overvågning og kommunikation af risici. Endvidere skal der etableres passende kontrolmekanismer for at sikre, at disse procedurer afvikles som foreskrevet.

I *Supervisory Review and Evaluation Process (SREP)* skal tilsynsmyndighederne regelmæssigt bedømme kvaliteten på instituttets ICAAP og på dets ledelses-, styrings- og kontrolprocesser. Det skal dog understreges, at ICAAP ”ejes” af instituttet, og at der ikke foreskrives bestemte metoder for risikoopgørelsen i søjle 2. SRP tænkes at forløbe som en ”dialog” mellem instituttet og tilsynsmyndighederne omkring 4 elementer, se figur 3. Tilsynsmyndighederne vil foretage en skønsmæssig afvejning af de kvantitative og kvalitative komponenter i risikostyringen, når instituttets samlede kapitalbehov bedømmes. Ved denne vurdering kan der tages hensyn til eventuelle korrelations- og diversifikationseffekter mellem de forskellige risikoformer, således at instituttets samlede kapitalkrav bliver mindre en summen af de enkelte risici. Kravet er dog her, at instituttet opgør sine risici ud fra et ”holistic approach which would have to be sufficiently robust”, som det hedder i *Committee of European Banking Supervisors (2006)* – for-

Figur 3
Tilsynsprocessen i Basel II / CRD



Kilde: CBES

kortet CEBS. Hvis SREP omvendt ender med en konklusion af, at instituttets ICAAP er utilstrækkelig, kan tilsynsmyndighederne reagere ved at ”foreslå” et passende niveau for kapitalen, stille krav om forbedringer i systemer og kontrolprocedurer, eller i værste fald at fratage instituttet retten til at drive visse former for forretninger.

Skulle ovenstående mod forventning ikke være tilstrækkeligt til at sikre en fornuftig risikostyring i bankerne, vil disse blive konfronteret med jungleloven i ”søjle 3”. Denne indeholder krav om offentliggørelse af risikostyringspolitikker, kapitaldækning mv., således at aktionærer, kreditorer og andre interessenter kan vurdere instituttets soliditet – og derudfra beslutte om – og i givet fald på hvilke vilkår – man ønsker at engagere sig økonomisk. Utilstrækkelig risikostyring og/eller kapitaldækning af risici kan dermed føre til øgede finansierings- og kapitalomkostninger og dermed forringet konkurrencedygtighed for en bank.

Behovet for en bredere risikostyringsramme

Basel II har været en væsentlig katalysator for udbredelsen af ERM-tankegangen blandt pengeinstitutter. Mange af disse har allerede investeret store summer og megen tid på at indrette systemer og processer på efterlevelse af regelsættet. Specielt de større

banker og sparekasser har valgt at gøre en dyd af nødvendigheden ved at tage skridtet fuldt ud – dvs. benytte lejligheden til at udvikle det ”totale” risikostyringskoncept. Endvidere foreligger der jo med regelsættet og de relaterede vejledninger fra CEBS, lokale tilsynsmyndigheder m.fl. en komplet ”drejebog” og checkliste for implementeringen af ”ERM” – selv om denne markedsføringsmæssige betegnelse ikke benyttes i de officielle dokumenter.

Inden for de seneste år er der imidlertid også uden for den finansielle sektor kommet øget fokus på risikostyring, ikke mindst efter Enron-kollapset i 2001 og konkursen hos WorldCom året efter. Disse og en række andre erhvervsskandaler førte i USA til vedtagelsen af den såkaldte ”Sarbanes Oxley Act” (”SOX”) – en flodhestepisk af en lov, der skulle få selv den mest tykhudede virksomhedsledelse til at interessere sig for risikostyringsprocesser og intern kontrol. Blandt de væsentligste elementer i SOX er:

- Etableringen af ”Public Company Accounting Oversight Board” (PCAOB eller blot ”Peekaboo”), en privat, non-profit organisation, der skal overvåge revisionsaktiviteterne i børsnoterede virksomheder.
- Krav om, at børsnoterede virksomheder bedømmer effektiviteten af interne

kontroller relateret til regnskabsmæssig rapportering, og at denne bedømmelse offentliggøres.

- Krav om, at virksomhedens direktion og bestyrelse personligt indestår for rigtigheden af regnskabsoplysninger mv.
- Krav om uafhængige revisionskomitéer i børsnoterede virksomheder.
- Skærpet straf for overtrædelse af værdipapirlovgivning.
- Betydeligt længere maksimal fængselsstraf og/eller bøde til virksomhedsledere, der bevidst giver vildledende regnskabsoplysninger.

SOX er det vigtigste amerikanske lovinitiativ på erhvervsiden siden New Deal og er naturligvis af mange erhvervsledere blevet set som et endog et meget kraftigt indgreb i virksomhedsstyringen. Mange – selv meget store virksomheder – overvejede simpelthen at lade sig afnotere for at slippe for det store, personlige ansvar og de betydelige omkostninger, der ville være forbundet med en efterlevelse af loven. Andre efterlyste – naturligvis under indtryk af de potentielt strenge straffe for manglende efterlevelse af loven – mere præcise retningslinier for, hvordan kontrolsystemer skulle opbygges, bedømmes og revideres, eller i det mindste en beskrivelse af ”best practice” på området.

Som respons herpå kunne PCAOB blandt andet pege på en branchestandard, ”Internal Control Integrated Framework”, udarbejdet af ”the Committee of Sponsoring Organizations of the Treadway Commission (COSO)”² i begyndelsen af 1990’erne. Som navnet antyder, var formålet med denne standard imidlertid først og fremmest at hjælpe virksomheder og andre enheder til bedre at kunne overskue og forbedre deres interne kontrolsystemer.

Den forstærkede interesse for og fokus på *risk management* som et *strategisk styrings-*

værktøj, gjorde det imidlertid klart, at der var behov for en *bredere* ramme for identifikation, vurdering og håndtering af risici.

Internationale risikostyringsstandarder

Den første egentlige, internationale standard for det, vi i dag kalder ”Enterprise Risk Management”, er den såkaldte ”Australian/New Zealand Risk Management Standard 4360 (”ANZ-4360”), som blev udgivet af ”Standards Australia and Standards New Zealand” i 1995. Denne blev populær, først og fremmest pga. af dens beskedne, fysiske omfang – oprindeligt kun 23 sider – og enkelthed. Standardsættere i andre lande, herunder UK og Japan, udviklede egne versioner af modellen, og også ISO – ”International Organisation for Standardisation” tog den til sig. Modellen er løbende blevet revideret og udvidet og foreligger nu som AS/NZS 4360:2004 – en handy håndbog på 28 sider, skrevet i klart sprog og så tilpas generel, at den passer til alle former for virksomheder. Herunder naturligvis også banker og sparekasser, for Basel II regelsættet kan snildt passes ind i standardens definition af risikostyring som ”an iterative process consisting of well-defined steps” med formålet ”to support better decision-making”, og som ”an integral part of good management practice” og ”part of an organization’s culture.”.

Som altid er det imidlertid de *amerikanske* standardsættere og deres forkærlighed for voluminøse rapporter, der sætter den internationale dagsorden. I 2001 iværksatte COSO et projekt, der i 2004 resulterede i rapporten ”Enterprise Risk Management – Integrated Framework” – en 246 siders sag, der i brede vendinger beskriver mål og midler i et ERM-system. Kritikere mener, at rapporten er alt for stor – alene ”Executive Summary” er næsten på størrelse med hele AS/NZS 4360. Men på trods af dette – eller måske netop *på grund af* dette, for her er der jo virkelig tale om ”gefundenes Fressen” for konsulentbranchen – er COSO rammen i dag den mest udbredte standard for ERM.

COSO definerer ERM som ”.. 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). En fri oversættelse/fortolkning er vist i boks 1.

Ifølge COSO skal ERM gøre det muligt at:

- Skabe sammenhæng mellem en virksomheds risikoappetit og strategi.
- Understøtte ledelsens beslutninger vedrørende risikostyringstiltag.
- Reducere risikoen for operationelle ”overraskelser” og tab som følge af disse.
- Identificere og håndtere sammensatte og komplekse risici på tværs af organisationen.
- Sikre en optimal allokering og udnyttelse af kapital.

Også her synes ”Basel II” at passe fint ind. Men hvor Basel-regelsættet først og fremmest har til hensigt at sikre et stabilt banksystem, så er der i COSO ERM modellen en direkte forbindelse mellem de mål, som virksomheden stræber efter at nå, og Enterprise Risk Management. Denne forbindelse illustreres som en tredimensional matrix, eller ”ERM kasse”, se figur 4, med fire målsætningskategorier (de lodrette kolonner, ”låget”), otte risikostyringskomponenter (de vandrette rækker, ”forsiden”) og fire organisatoriske niveauer (den tredje dimension, ”siden”). Kassen skal illustrere idéen bag ERM, nemlig evnen til at fokusere på alle aspekter af en virksomheds risikostyring og strategiske og operationelle målsætninger på kryds og tværs af organisation og forretningsområder.

Skjuler risikostyringens hellige gral sig så inde i denne kasse?

Måske, men for at åbne den skal alle otte risikostyringselementer fungere effektivt og bindes sammen med et informationsflow som vist i figur 5. Og for at dette skal lykkes, er der, som vi skal se på nedenfor, en række praktiske problemer, som skal løses.

Indholdet af og sammenhængen mellem de otte COSO-elementer kan kort beskrives som følger:

1. *Internt miljø*
Omfatter ”bløde” værdier som omgangstone, risikooptattelse, risikooappe-

Boks 1

Definition på Enterprise Risk Management

”Enterprise Risk Management er en proces, hvorigennem virksomhedens bestyrelse, ledelse og andet personale udvikler og forfølger strategier på tværs af virksomheden, og hvor potentielle begivenheder, som kan have negativ – eller positiv – indflydelse på mulighederne for at nå disse mål sideløbende søges identificeret, kvantificeret og styret i overensstemmelse med virksomhedens risikoappetit.

tit, kompetencer og etiske værdier. Det interne miljø bestemmer virksomhedens risikokultur. Denne danner basis for de øvrige elementer, og har naturligvis stor indflydelse på, om ERM kan implementeres med succes

2. Fastlæggelse af mål

Det er naturligvis nødvendigt med klart formulerede målsætninger inden for alle fire kategorier strategi, drift, rapportering og compliance, hvis banken/ virksomheden skal kunne identificere risici og events, som kan påvirke disse mål positivt og negativt. ERM skal sikre, at ledelsen er i stand til at opstille disse mål, og at de valgte mål er i overensstemmelse med virksomhedens risikokultur og risikoappetit. For banker og sparekasser vil målsætningskategorierne "Rapportering" og "Compliance" være mere eller mindre dikteret af, hvilket "Basel II" ambitionsniveau, der vælges – samt af anden form for lovgivning, f.eks. MiFID. På det strategiske og operationelle plan vil målsætningen f.eks. ofte være konkretiseret som et "target" afkast på risikokapitalen (RAROC) inden for de forskellige områder, evt. suppleret med absolutte begrænsninger på det absolutte risikoniveau.

3. Identifikation af events

Interne og eksterne "events", som kan have indflydelse på en virksomheds målopfyldelse, skal være identificeret. Der skal sondres mellem risici og muligheder. Muligheder kobles tilbage til elementet "fastlæggelse af mål", mens risici kobles til "Styringstiltag".

4. Risikomåling

For at kunne gennemføre de nødvendige styringstiltag, må risici først kvantificeres. "If you can't count it, you can't control it", som det hedder. Såvel sandsynlighed for tab og disses konsekvens må vurderes. Risici skal vurderes med hensyntagen til deres indbyrdes sammenhæng (korrelation). Såvel "iboende" risici som residualrisici skal måles. De "iboende" risici er risici, som virksomheden som følge af dets forretningsaktiviteter ville være udsat for, hvis der ikke var etableret kontrolmekanismer eller ikke var blevet gennemført styringstiltag. Med residualrisici menes de risici, som er tilbage, efter at styringstiltag er iværksat. I en bank

kanne dette f.eks. være de likviditetsrisici og juridiske risici, der opstår, når de af "søjle 1" omfattede risici afdækkes med derivater e.l. For institutter underlagt Basel-regelsættet behandles residualrisici i "søjle 2", se figur 3. Målemetoderne kan både være kvantitative (f.eks. "Value-at-Risk" for markedsrisiko i en bank eller "Earnings-at-Risk" i en virksomhed) og kvalitative – eller et miks heraf (f.eks. erfaringsbaserede estimater af potentielle tab relaterede til "Key Performance Indicators").

5. Styringstiltag

Ledelsen vælger, hvordan den vil reagere på risici, herunder undgå, acceptere, reducere eller overføre risiciene. Endvidere gennemføres der nødvendige tiltag for at sikre sammenhæng mellem påtagne/accepterede risici og virksomhedens risikoappetit og risikotolerance.

6. Kontrolaktiviteter

Der skal udarbejdes og iværksættes politikker og procedurer for at sikre, at de nødvendige styringstiltag (element 5) gennemføres.

7. Information og kommunikation

Relevant information bliver identificeret, kortlagt og kommunikeret ud på en måde og med en tidsramme, som gør det muligt for medarbejderne at udøve deres ansvar.

8. Overvågning

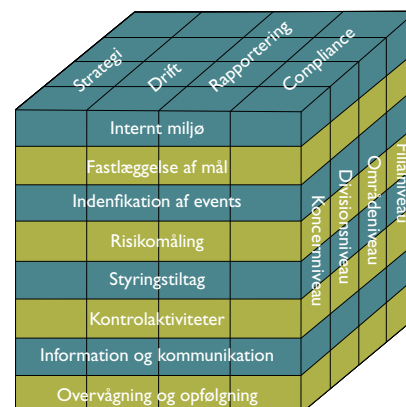
ERM-processen overvåges, og processen tilpasses om nødvendigt. Overvågning sker løbende fra ledelsens side og/eller ved lejlighedsvis separate evalueringer.

Det skal understreges, at de 8 komponenter ikke er tænkt at skulle fungere på samme måde i enhver virksomhed. Anvendelsen i for eksempel små og mellemstore virksomheder kan være mindre formel og mindre struktureret. Ikke desto mindre er det tanken, at også små banker/ virksomheder kan opnå effektiv ERM, så længe hver komponent er til stede og fungerer som beskrevet.

Kan der skabes værdi med ERM?

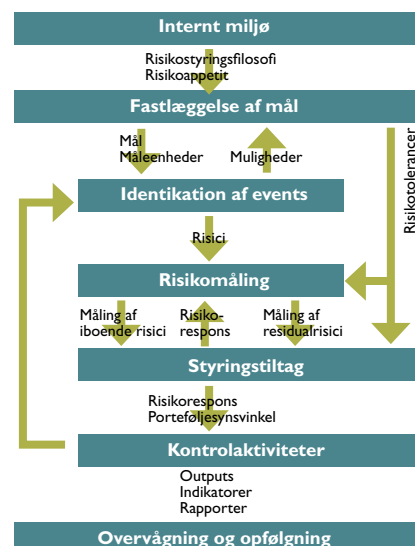
Svaret herpå er ja – men naturligvis kun, hvis man som diskuteret ovenfor får ERM til at tænde på alle otte cylindre.

Figur 4
COSO ERM modellen



Kilde: COSO (2004). Forfatterens frie oversættelse

Figur 5
Informationsflows i ERM

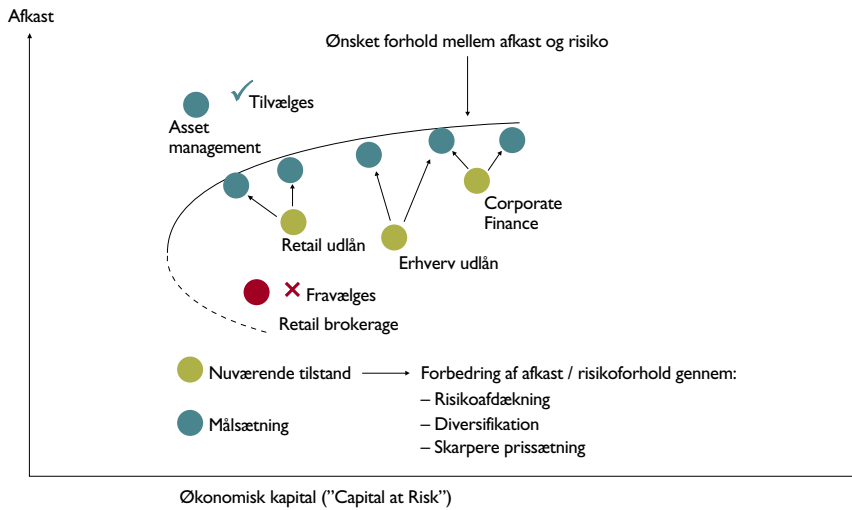


Kilde: COSO (2004)

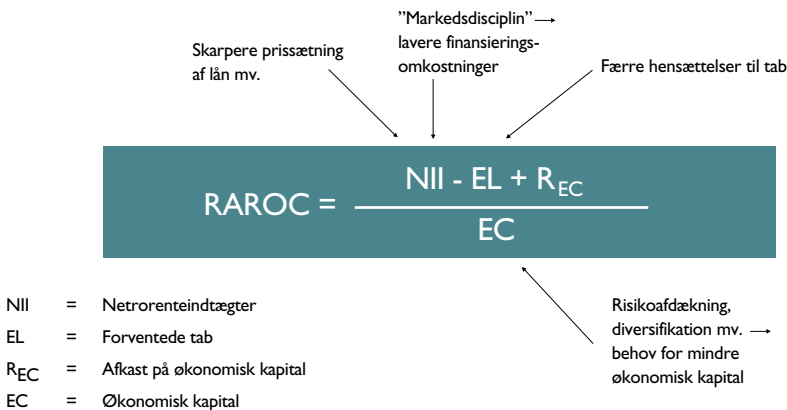
Banken/ virksomheden har selv en høj grad af kontrol over målkategorierne "rapportering" og "compliance", og et effektivt ERM-system må forventes at skabe rimelig sikkerhed for, at disse mål nås. Alene heri ligger der naturligvis en vis værdiskabelse for f.eks. banker, da efterlevelse af Basel II og andre regelsæt jo er en *nødvendig betingelse* for at drive forretning på rimeligt selvstændige vilkår.

Efterlevelse af lovgivning er imidlertid ikke en *tilstrækkelig* betingelse for overlevelse i en verden med hård konkurrence og krav om "shareholder value". Her kræves, at der er sammenhæng mellem forretningsidé, strategiske mål og operationelle mål – herunder effektiv drift og effektiv brug af risikokapital.

Figur 6
Værdiskabelse gennem risikostyring



Figur 7
Vejen til forbedret RAROC gennem ERM



Et effektivt ERM system kan sikre, at virksomhedens knapteste ressource – kapitalen – allokere til forretningsområder, hvor den forrentes bedst. Dette kan f.eks. ske ved til- og fravalg af forretningsområder ud fra de ”hurdle rates” for risikokorrigeret performance, der fastlægges i ”COSO ERM element 2”, eller ved at afkast/risiko-forholdet på nuværende forretningsområder forbedres gennem styringstiltagene i ”element 5”, se figur 6. Afkast/risiko-forholdet kan forbedres ved 1) reduktion af risikoen for virksomheden/forretningsområdet, 2) reduktion af kapital- og finansieringsomkostninger og 3) skarpere prissætning af produkter, f.eks. udlån. I figur 7 er det illustreret, hvordan disse tiltag kan øge RAROC – Risk Adjusted Return on Capital – som i dag er et udbredt mål for risikokorrigeret performance i banker og sparekasser.

De praktiske problemer

Når nu ideen om et ERM er så besnærende, hvorfor har så ikke alle banker og virksomheder et sådant system? Svaret herpå skal jo nok søges i de betydelige praktiske problemer og store omkostninger, der vil være forbundet med implementeringen heraf, med risikomodelering, data og IT infrastruktur som de afgørende ”roadblocks”. Dette underbygges af den tidligere omtalte undersøgelse, gennemført af SAS Institute. Her har de adspurgte banker svaret på spørgsmålene om, hvad de opfatter som de største forhindringer for implementering af systemer til styring af hhv. kreditrisiko og operationelle risici, og resultatet heraf er sammenfattet i figur 8a og 8b.

Undersøgelsens spørgsmål relaterer sig godt nok til ”siloeerne” kreditrisiko og operationelle risici, men man kan nok tillade sig at formode, at de anførte problemer i *mindst*

lige så høj grad ville gælde for det mere ambitiøse, altomfavnende ERM-system.

For så vidt angår problemer med risikomodeleringen kan man finde god hjælp i COSO-rapportens del 2, ”Application Techniques”, hvor der gives praktiske anvisninger i brugen af modellens elementer – herunder ”Risk Assessment”. Herunder peges der på en række kvalitative og kvantitative metoder, der kan bruges til opgørelse af risici i finansielle såvel som ikke finansielle virksomheder.

Værre ser det ud med data og IT infrastruktur problemerne. De fleste banker og virksomheder har af historiske årsager stadig stærkt fragmenterede systemer, og det nødvendige datagrundlag er mangelfuldt eller af en sådan kvalitet, at det ikke umiddelbart kan bruges til at opgøre risici på tværs af processer. For at opbygge et effektivt ERM-system vil det derfor være nødvendigt at udvikle eller indkøbe nye ”end-to-end”, ”skalerbare” løsninger med ”åben systemarkitektur” som muliggør ”Integrated Decision Processing” (IDP) og hvad det ellers hedder. Endvidere skal der gennemføres en hovedrengøring af data, som i rensset form placeres i et ”data warehouse”, som man så siden kan bearbejde med ”Online Analytic Processing” (OLAP) og ”data mining” teknikker.

ERM eller ej?

Ikke mindst udsigten til de ovenfor omtalte, store investeringer har afholdt mange bankdirektører mv. fra at gå ERM-vejen. Et hypotetisk argument herfor er, at de med deres erfaring, kundekendskab osv. har en udmærket idé om omfanget af risici i deres forretninger. Hertil behøves ikke avancerede modelleringsteknikker og nye systemer. Fra januar 2007 træder ”Basel II”, de nye og væsentlige mere risikofølsomme regler for beregningen af risikokapitalen, ganske vist i kraft, men disse kan jo let opfyldes ved at vælge ”standardmetoder” og et ”passende” højt kapitalberedskab.

Dette argument holder imidlertid ikke meget længere, for store danske og internationale banker har – med netop Basel II som katalysator – investeret store summer i udviklingen af sofistikerede risikostyringsmetoder med tilhørende IT-infrastruktur. Disse betydelige investeringer skal nu forrentes, bl.a. ved udnyttelse af de avancerede risikostyringsmodeller til at stille skarpere priser og gå på strandhugst blandt kunderne hos de institutter, der er mindre godt klædt på.

I lyset af denne udfordring står det mindre pengeinstitut over for valget mellem at

forsætte som hidtil – og evt. tære lidt på den gennem årene opbyggede kapitalpolstring – eller at kaste sig ud i jagten på ”Gralen”.

Dette er måske ikke så uoverstigelig en opgave, som man skulle frygte, hvis blot man griber det rigtigt an fra starten.

For det første skal der lægges et realistisk ambitionsniveau. Implementeringen af ”Enterprise Risk Management” – eller hvad vi nu skal kalde det – indebærer ikke nødvendigvis, at alle risici skal oprøres og styres i ét gigantisk system i én central risikostyringsenhed. Det er imidlertid vigtigt, at man så hurtigt som muligt får formaliseret og implementeret risikostyringspolitikker og procedurer, som kan tjene som den fælles ramme, inden for hvilke risici identificeres, måles og styres på tværs af og på alle niveauer af organisationen. Sådanne politikker og forretningsgange kan (og skal i henhold til de nye Basel-regler) på sigt udgøre ryggraden i bankens risikostyring og interne kapitalallokeringsproces – og er i øvrigt sund fornuft.

For det andet skal man ikke lade sig skræmme af udsigten til kæmpe-investeringer i ny IT infrastruktur. En vigtig forudsætning for effektiv ERM er ganske vist, at man har et system, der gør det muligt at skabe et samlet overblik over bankens engagementer, positioner mv., for uden denne mulighed vil man kæmpe i blinde. Et sådant system kan imidlertid i vidt omfang opbygges på grundlag de data, som ligger i de eksisterende systemer, når blot disse ”destilleres” og evt. suppleres med anden relevant information – og den sunde fornuft, der aldrig bør gå af mode. Og når man nu alligevel er i gang med at gennemgå og justere arbejdsgange og systemer med henblik på efterlevelse af MiFID, hvidvaskningsdirektiv mv., kan man jo lige så godt gøre det ordentligt fra starten. Denne proces vil i sig selv med stor sikkerhed føre til betydelige forbedringer af risikostyringen – ”*the process itself almost always leads to improvements*”.

Der kan dog naturligvis ikke gives nogen garanti for, at anstrengelserne fører til, at man en dag står med risikostyrings ”hellige gral” i hænderne – for det kan jo være, at skeptikerne har ret i, at den slet ikke findes.

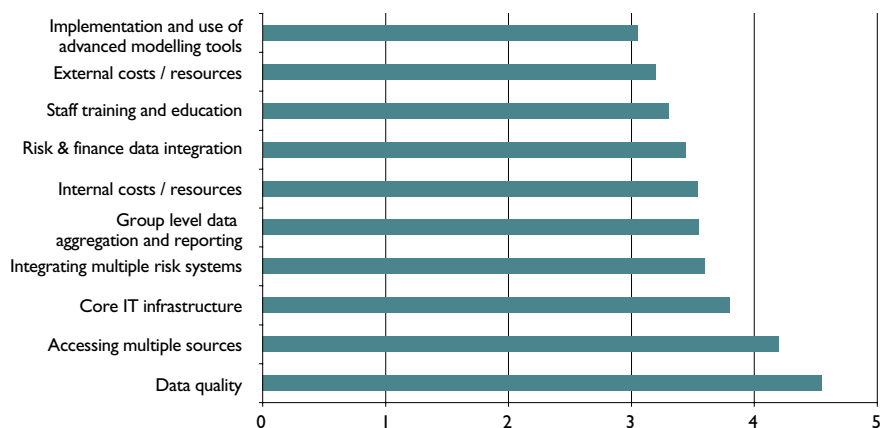
Men så kan man jo altid leve af at holde myten i live.

Noter

- 1) MiFID står for ”Markets in Financial Instruments Directive” og er en udløber af den ”Financial Services Action Plan”, der skal gøre EU

Figur 8a

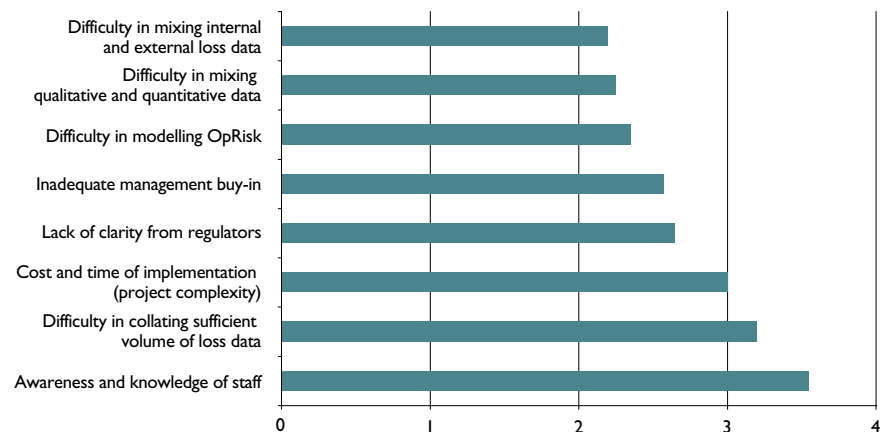
Væsentlige forhindringer for implementering af system til styring af kreditrisici



Kilde: SAS Institute

Figur 8b

Væsentlige forhindringer for implementering af system til styring af operationelle risici



Kilde: SAS Institute

- til verdens mest konkurrencedygtige økonomiske zone. I december ventes den nye ”minibørsreform” – den danske version af EU-direktivet MiFID – vedtaget i Folketinget.
- 2) The Committee of Sponsoring Organizations of the Treadway Commission (COSO) er en privat, non-profit organisation, der blev etableret i 1985 af 5 amerikanske revisionsorganisationer. Komitéen er opkaldt efter sin første formand, James C. Treadway.

Litteratur

- Andersen, Michael og Anders Grosen, 2005. Konkurrencemæssigt opbrud på pengeinstitutmarkedet – hvad betyder de nye Basel II-regler? *Finans/Invest* 6/05.
- CEBS, 2006: *Guidelines on the Application of the*

Supervisory Review Process. Committee of European Banking Supervisors.

- COSO, 2004: *Enterprise Risk Management – Integrated Framework*. The Committee of Sponsoring Organizations of the Treadway Commission.
- Plesner, Søren, 1995: Fra ”3-8-5 banking” til global markedsplads. *Finans/Invest* 7/95.
- Plesner, Søren, 2001: Finansiell risikostyring i en global økonomi. *Finans/Invest* 6/01.
- Plesner, Søren, 2002: Økonomisk kapital – fundamentet i moderne bankdrift. *Finans/Invest* 4/02.
- Plesner, Søren, 2005: Trends på de internationale finansmarkeder 6/05.
- SAS Institute, 2006: *Enterprise Risk Management in the Financial Services Industry – International Benchmark Survey*. SAS Institute.