

Samordnad riskhantering på ledningsnivå – krav i Solvens 2 och nödvändigt för att erhålla hög rating

av Jörgen Olsén



Jörgen Olsén
jorgen.olsen@guycarp.com

Samordnad riskhantering på ledningsnivå (eng. Enterprise Risk Management – ERM) bedrivs med målsättningen att förstå och hantera den totala risken i verksamheten. Med hjälp av genomtänkta processer mäts riskexponeringen på strategiska ställen i organisationen och analyseras metodiskt så att en samlad bild över totalrisken tonar fram.

En lyckad ERM-process kräver ett aktivt engagemang från bolagets ledning, och processen underlättas om det finns en Chief Risk Officer med stark position i bolaget som har god förståelse för både försäkringsrisker och finansiella risker. Dessutom kan en simuleringsplattform, där verksamhetens risker kan analyseras och utvärderas, underlätta för bolaget att finna sin optimala kapitalstruktur.

Formellt ERM-arbete krävs numera av kreditvärderingsinstituten, och kommer att utgöra en av grundpelarna i Solvens 2.

I. Ökad fokusering på riskhantering

Försäkringsbolagens verksamhet ökar i komplexitet, och förbättrad riskhantering har kommit alltmer i fokus både hos ägare, tillsynsmyndigheter och kreditvärderingsinstitut. Bra riskhantering är av värde för alla dessa aktörer, även om de till viss del har skilda utgångspunkter. Ägarna vill försäkra sig om att deras kapital används så effektivt som möjligt och utnyttjas för att ge bra avkastning med kontrollerad risk. Tillsynsmyndigheterna vill skydda försäkringstagarna och se till att risken för att dessa inte ska få fullt betalt hålls på en mycket låg nivå. Kreditvärderingsinstituten, vars uppgift är att bedöma risken för att långivare inte ska få fullt betalt, letar efter förfinade instrument för att särskilja bolag

med hög och låg kreditvärdighet. Tillsynsmyndigheter och kreditvärderingsinstitut, liksom ägare, ställer därför höga krav på en effektiv försäkringsverksamhet med lämplig kontroll- och kapitalstruktur.

Artikelns disposition

I artikeln klargörs först i avsnitt II vilket ansvar för riskhantering de ledande organen i ett försäkringsbolag har. Därefter beskrivs nödvändigheten av att ta ett samlat grepp över verksamhetens totalrisk för att bedriva så ef-

Jörgen Olsén är diplomerad aktuarie inom den svenska aktuarieföreningen och arbetar med aktuariella och finansiella analyser av nordiska försäkringsbolag vid återförsäkringsmäklaren Guy Carpenter & Co. i Stockholm. Han har en doktorsexamen i matematisk statistik från Uppsala universitet.

fektiv verksamhet som möjligt. Avsnittet avslutas med en beskrivning av en simuleringsplattformens värde vid riskanalysen. Avsnitt III diskuterar tillsynsmyndigheternas krav på riskhantering i det framtida solvensregelverket Solvens 2. Avsnitt IV ger de fyra stora kreditvärderingsinstitutens (Standard and Poor's, A.M. Best, Moody's, och Fitch Ratings) syn på riskhantering och dess betydelse för bolagets kreditvärdighetsbetyg. I avsnitt V beskrivs några frågeställningar kring riskhantering som försäkringsbolagen redan nu bör arbeta med. Artikelns avslutas i avsnitt VI med en slutsats om betydelsen av riskhantering.

II. Samordnad riskhantering på ledningsnivå – ERM

Ansvar för bolagens riskhantering

Styrelsen är den grupp av personer som har utsetts att svara för bolagets organisation och förvaltning, och är ytterst ansvarig för bolagets strategi och riskhantering. *Chefaktuarien* har till uppgift att analysera den finansiella betydelsen av risk och osäkerhet inom försäkringsverksamheten. *Chefunderwritern* skall se till att bolagets riktlinjer för vilka risker som kan accepteras följs. Den *ansvariga för regelefterlevnad* (eng. compliance) har till uppgift att se till att bolaget följer lagar och föreskrifter.

På senare tid har en ny position av stor vikt för effektiv riskhantering instiftats inom många bolag – den som *CRO* (eng. Chief Risk Officer). Bolagets CRO är ansvarig för att analysera och planera för potentiella risker inom bolagets alla olika segment. CRO-funktionen skall följaktligen ha en övergripande bild av försäkringsbolagets totala riskexponering, och underlätta för styrelsen att styra verksamheten. En CRO med stark position i bolaget, och som har god förståelse för både försäkringsrisker och finansiella risker, underlättar införandet av bra riskhantering.

En av styrelsens viktiga uppgifter är att

tillsammans med ägarna utarbeta riktlinjer för försäkringsbolagets *risktolerans*. Denna toleransprofil sätter i princip konkreta siffror på hur mycket av försäkringsbolagets tillgängliga kapital som bolaget kan acceptera att förlora t.ex. vart 5:e eller 200:e år som en följd av ogynnsamma försäkringsutfall, eller på grund av en negativ utveckling för dess tillgångar. Risktoleransen styr bolagets strategi för aktivt val av risker och upprättande av underwriting-riktlinjer samt risköverföringsstrategier, och definierar därmed *riskaptiten*. Ett bolag som accepterar en minskning av det tillgängliga kapitalet med 5 procent vart 5:e år och 60 procent vart 200:e år, har troligen behov av t.ex. mer återförsäkring än ett bolag som har en högre risktolerans och kan acceptera 10 procents minskning vart 5:e och 80 procent vart 200:e år. Risktoleransen och riskaptiten kan förslagsvis bestämmas så att en önskvärd solvensgrad eller ett kreditvärdighetsbetyg inte hotas.

Analys av enskilda riskkategorier avslöjar inte hela bilden

Att förstå bolagets riskexponering och försöka optimera kapitalstrukturen genom att analysera produkter eller riskkategorier var för sig är svårt. Privatportföljen, analyserad i enskildhet, kan få ett jämnare resultat med utökad återförsäkring, och en separat analys av företagsportföljen kan leda till samma slutsats. För hela försäkringsbolaget är det dock möjligt att samma resultatutjämnning kan uppnås, fast till ett bättre pris, med en återförsäkringslösning som täcker både privat- och företagsprodukterna.

En separat analys av försäkringsriskerna kan visa att värdet av de diskonterade tekniska avsättningarna är väldigt känsligt för förändringar i ränteläget, och att minska risken med hjälp av räntederivat kan verka lämpligt. Men om tillgångarna är investerade i välmatchade obligationer kan det visa sig att portföljen i sin helhet är helt okänslig för ränteförändringar.

Total riskprofil behövs

Exemplen ovan visar att ledningen, aktuarierna och bolagets CRO måste förstå dynamiken mellan organisationens alla risker. Effekten av en alternativ struktur på återförsäkringsprogrammet bör kunna mätas, resultatet av att föra över risk till kapitalmarknaderna kvantifieras, betydelsen av att välja högre eller lägre kreditvärdighet på sina motparter belysas, samt ett kapitaltillskott från ägarna som kan underlätta en aggressivare kapitalplaceringsstrategi värderas.

Grunden till att finna den bästa kapitalstrukturen för bolaget är då att alla individuella risker (av icke försumbar storlek) mäts, och att samvariationen mellan olika risktyper förstås till form och styrka. Verkliga händelser (skador, reservförändringar, block av försäkringsrisker som har givit tidigare förluster) behöver analyseras för att man skall förstå de risker som bolaget står inför. Det är mycket möjligt att bolaget är exponerat för en del risker som inte beaktas inom mer standardiserade analysmodeller. Först när dessa analyser gjorts är det möjligt att aggregera risker från olika produktområden (företag, privat, ...) och riskkategorier (försäkringsrisker, marknadsrisker, kreditrisker, operativa risker) till en totalrisk. Ur denna holistiska modell av verksamheten framträder en bild av hur mycket total risk som finns i portföljen, samt hur mycket värde och volatilitet olika produkter bidrar med.

ERM – ett ramverk för bolagsvid riskhantering

Processen för att skapa en riskprofil som spänner över hela verksamheten kräver först och främst omfattande stöd och aktivt engagemang från styrelse och ledning. Däremot finns full förståelse för alla enskilda risker troligen endast långt ute i verksamheten. *Samordnad riskhantering på ledningsnivå* (eng. Enterprise Risk Management – ERM) kräver alltså

både att verksamhetens risker analyseras nedifrån enskilda risker och upp till bolagsnivå, samt att stöd och prioritet för arbetet kommer från ledningen, och förstås och accepteras genom hela organisationen.

Just kravet på ledningens holistiska, d.v.s. sammanhållna produkt-, riskkategori- och bolagsvida analys, är det koncept som karakteriserar samordnad riskhantering på ledningsnivå – ERM. Angreppssättet ska kontrasteras mot ”klassisk” riskhantering, som naturligtvis är en värdefull utgångspunkt vid riskhanteringsarbetet, där risker och risköverföringsstrategier analyseras separat för olika verksamhetsgrenar eller riskklasser, utan att vägas samman till en totalrisk.

Simuleringsplattform som strategiskt hjälpmedel

Försäkringsprodukternas komplexitet med kopplingen till både försäkringshändelser och utvecklingen på finansmarknaden, samt den omfattande verktygslåda av risköverföringsstrategier som finns att välja bland, innebär att det är svårt för en styrelse att direkt resonera sig fram till den optimala kapitalstrukturen. Då även små risker, var för sig oväsentliga men kanske starkt korrelerade, tillsammans kan få förödande konsekvenser måste försäkringsbolagens verksamhet kvantifieras med statistiska metoder, och analysen kan underlättas med hjälp av en simuleringsprogramvara.¹ En simuleringsplattform bör kunna analysera försäkringsrisker, marknadsrisker, kreditrisker och operativa risker i en integrerad miljö, och ta hänsyn till olika risköverföringsstrategier, samt drivas av ekonomiska scenariogeneratorer.² För att underlätta förståelse och transparens för externa parter är det viktigt att det för varje simuleringsomgång är möjligt att i efterhand i detalj studera alla händelser som påverkat bolagets resultat och kassaflöden.

I takt med att interna modeller för beräkning av ekonomiskt kapital utvecklas kommer bo-

lagets huvudsakliga riskexponeringar täckas, och riskjusterade avkastningsberäkningar och kapitalallokering kunna utföras. Verksamhetens resultat bör då sammanfattas med ett flertal probabilistiska och finansiella rapporter med nyckeltal för att stödja ledningens strategiska beslutsfattande rörande inom vilka verksamhetsgrenar bolaget bör expandera respektive minska sitt engagemang.³ För att förbättra sina verksamheter har många försäkringsbolag på eget initiativ redan börjat bygga upp ERM-system.

III. Tillsynsmyndigheternas krav på ERM

Solvens 2 – ett regelverk under utformning

Målsättningen med Solvens 2 är ett förbättrat konsumentskydd, en moderniserad tillsyn, en fördjupad integration av den europeiska försäkringsmarknaden och förbättrad internationell konkurrenskraftighet för försäkringsbolagen. I det kommande regelverket kommer försäkringsbolag att få lov att beakta alla sorters risker de är exponerade för och hantera dessa risker så effektivt som möjligt.⁴ För närvarande förväntas solvensregelverket träda i kraft, något försenat, 2012 eller 2013, och omfatta alla försäkringsbolag och återförsäkringsbolag med en årlig premieinkomst på mer än 5 miljoner Euro.⁵ Regelverket kommer att fastställas i ett EG-direktiv, och vid utvecklingen har den europeiska kommissionen tagit hjälp av den europeiska tillsynskommittén för försäkringar och tjänstestepationer, CEIOPS.

Konceptuellt beskrivs Solvens 2 vila på tre pelare: en kvantitativ beräkningsansats för solvenskapital (pelare 1), en harmonisering av försäkringsinspektionernas tillsynsprocess och krav på försäkringsbolagens styrning och riskhantering (pelare 2), samt ett krav på ökad transparens vid offentliggörandet av den interna och externa riskrapporteringen (pe-

lare 3). Än så länge har merparten av arbetet med Solvens 2 berört den kvantitativa aspekten. Branschomfattande undersökningar (QIS1 2005, QIS2 2006, QIS3 2007) av en föreslagen europeisk standardmodell för att beräkna bolagens solvenskapital har genomförts, och nästa undersökning, QIS4,⁶ är planerad till perioden april till och med juli 2008.⁷ Först under senare delen av 2009 förväntas den europeiska standardformelns slutliga kalibrering bli känd.⁸

För att tidplanen för införandet skall hålla måste den första nivån i Solvens 2-ramverket, som beskriver solvenssystemets huvudprinciper, med ett utkast publicerat i juli 2007 antas under 2009-2010. Därefter kan en andra nivå i ramverket, som kommer att innehålla detaljerade implementeringsriktlinjer, antas under 2010. Målsättningen är att varje land sedan får åtminstone 18 månader på sig att implementera EG-direktivet i sina egna lagar, förordningar eller föreskrifter under 2011-2012.⁹ Regelverket förväntas sedan i framtiden fortsätta att förändras i takt med försäkringsmarknadens utveckling och krav på förbättrad riskhantering.

Tillsynsprocessen – Supervisory Review Process

Vid bedömningen av bolagens finansiella styrka och förmåga att uppfylla försäkringstagarnas krav, kommer tillsynsmyndigheterna även att undersöka kapaciteten att hantera och kontrollera risker kvalitativt och kvantitativt. En studie genomförd av CEIOPS har visat att just dålig styrning av bolag och olämpliga riskbeslut ofta är huvudorsaken till att försäkringsbolag hamnar i trångmål.¹⁰

Pelare 2-kraven på riskhantering och på effektivitet hos kontrollsystemen, med syftet att upptäcka försäkringsbolag som har en finansiell eller organisatorisk struktur som gör dem extra riskbenägna, börjar nu konkretiseras. Under tillsynsprocessen (*eng.* Supervisory Review Process – SRP) kommer tillsyns-

myndigheten utvärdera de metoder bolagen använder för att identifiera framtida händelser eller ekonomiska förhållanden som kan ha negativ inverkan på bolagens finansiella ställning.

Innan riktlinjerna för tillsynsprocessen är helt klara lär dock flera frågor stå på agendan i möten mellan ledningsgrupper och bolagens riskanalytiker. Vilka funktioner och ansvarsområden kommer krävas för att tillsynsmyndigheterna skall anse att bolagen har tillfredsställande riskhanteringskapacitet? Vilken omfattning, vilka risker och vilka kontrollprocesser måste finnas på plats? Vem eller vilka i organisationen är ansvariga för arbetet, och kanske inte minst viktig är frågan om vilka påföljder försäkringsbolagen kan förvänta sig om riskhanteringskapaciteten inte bedöms vara tillräcklig? Dessutom bör bolagen fundera på hur, förutom för att uppfylla tillsynsmyndigheternas krav, förbättrad riskhantering kan utveckla och effektivisera den egna verksamheten.

Riskhantering kräver definierade ansvarsfunktioner

CEIOPS och den europeiska kommissionen har nyligen, dels i utkastet till Solvens 2-ramverket samt i en separat rapport med fokus på riskhantering, givit exempel på de krav som kommer att ställas på försäkringsbolagens arbete med riskhantering och kontrollprocesser.¹¹

Fundamentalt är att ledningens roll, med det yttersta ansvaret för bolagets riskhantering och strategi, poängteras. Centralt är också att man har definierat tydliga ansvarsområden, ett antal viktiga *funktioner* inom riskhantering, regelefterlevnad, intern kontroll, och aktuariella arbetsuppgifter som bolagen måste tillsätta. För att ledningen skall kunna utföra sina uppgifter förväntas en CRO-funktion, med direkt förbindelse till bolagets styrelse, få stort inflytande. Denna CRO-funktion är separat från och komplementär till

chefaktuariens roll, även om den i princip (och särskilt för mindre bolag) skulle kunna fyllas av samma person.

Lämpligheten hos de styrande funktionerna

Vid tillsynsprocessen kommer det att säkerställas att bolagets styrande funktioner tillsatts med personer med lämplig bakgrund (*eng.* Fit and Proper). För dessa ledande positioner krävs det förutom formella kvalifikationer, även ett gott anseende och integritet så att bolagets bästa intressen inte åsidosätts.¹² Förutom styrelse bör lämplighetskraven även innefatta exempelvis CRO, chefaktuarie¹³ och den ansvarige för regelefterlevnad. CRO-funktionen kräver översikt och förståelse för bolagets samtliga risker, samt förmågan att kommunicera dessa till styrelsen. För CRO tycks erfarenhet av att bedöma försäkringsrisker och dess samvariation, kunskap om finansiella risker och inte minst god förståelse för det utbud av risköverföringsstrategier som finns att välja bland vara en lämplig bakgrund. Kravet på kapacitet för olika funktioner kommer dock enligt *proportionalitetsprincipen* att stå i relation till bolagets storlek och komplexiteten på dess verksamhet, för att kravet inte skall bli för betungande för små bolag.¹⁴

Ett högt krav på lämplig kunskap bör rimligen även ställas på tillsynsmyndigheternas anställda, med tanke på de nya Solvens 2-relaterade uppgifterna, nämligen att bedöma försäkringsbolagens riskhantering och utvärdera bolagens interna modeller. Då behovet i försäkringsbranschen av personer med sådan detaljkunskap som tillsynsmyndigheternas anställda som aktivt deltagit vid utformningen av Solvens 2 besitter är stort, är det möjligt att tillsynsmyndigheterna står inför en krävande uppgift att rekrytera, och framför allt behålla, denna kompetens.

De granskningsförfaranden som försäkringsbolagen bör förbereda sig på framöver är redan en realitet inom bankvärlden. Finans-

inspektionen i Sverige granskade under sommaren 2007 investmentbanken Carnegie. Granskningen avsåg delvis just en lämplighetsundersökning av kontrollrutiner och riskmedvetenhet inom bankområdet. Finansinspektionen fann stora brister i styrning och kontroll av verksamheten, konstaterade ottydlig ansvarsfördelning och att väsentliga granskningsuppgifter hade lagts på personer som saknat erforderlig kompetens för uppgiften.¹⁵ De riktade kritik mot att kontroll- och riskhanteringsaktiviteterna inom banksektorn inte har ökat i samma omfattning som verksamhetens komplexitet. En följd av granskningens resultat är att Finansinspektionen meddelat att de avser att granska motsvarande områden hos nio andra banker och värdepappersföretag.

Egen risk- och solvensbedömning (ORSA) – hjärtat i riskhanteringen

Som en mycket viktig del av riskhanteringen förväntas bolagen, med beaktande av sin egen riskprofil, göra en egen risk- och solvensbedömning (*eng.* Own Risk and Solvency Assessment – ORSA). ORSA-processen tvingar bolaget att internt åstadkomma, och för tillsynsmyndigheten redovisa, en helhetssyn på sina risker och göra en framåtblickande bedömning.¹⁶ ORSA-processen kräver naturligtvis att bolagen har kapacitet att upptäcka och mäta de risker de står inför, både sådana som beaktas i den europeiska standardformeln och andra bolagsspecifika risker.

En effekt av ORSA-processen är att försäkringsbolaget skulle kunna finna att dess riskprofil gör användandet av den europeiska standardmodellen olämplig, och att de anser att en egen riskmodell bättre fångar och mäter bolagets riskexponering. De försäkringsbolagen kommer därefter troligen att vilja använda sin egen bolagsriskspecifika modell, kalibrerad till tillsynsmyndighetens säkerhetsnivå, för att beräkna sitt behov av regulativt solvenskapital. Att ersätta den europeiska standardmodellens solvensberäkning med en in-

tern modell kommer dock att kräva tillsynsmyndighetens godkännande. Förutom kraven att en intern modell ska ta hänsyn till alla viktiga riskkategorier, vara korrekt kalibrerad, kunna jämföra kapitalkrav för individuella riskkategorier mot standardmodellen, och vara tillfredsställande dokumenterad, kommer bolagens egen tillförsikt till den interna modellen att undersökas. I *användningstestet* kontrolleras att resultatet från den interna modellen även används av ledningen i det löpande operativa riskhanteringsarbetet. Detta krav på styrelsens engagemang i, och förståelse för, resultaten från bolagets interna modell känns sunt. Ett minimikrav för att externa parter skall lita på resultatet bör vara att bolaget visar egen tillit till modellen.

Efter att försäkringsbolaget har ansökt om att en intern modell skall godkännas, skall tillsynsmyndigheten godkänna eller avslå denna ansökan inom sex månader. Även efter att en intern modell godkänts för solvensberäkning skall bolaget under de följande två åren också utföra en beräkning av solvenskapitalkravet beräknat enligt standardmodellen.¹⁷

IV. Kreditvärderingsinstitutens krav på ERM

Utanför Europa har det ökande kravet på samordnad riskhantering på ledningsnivå huvudsakligen drivits av kreditvärderingsinstitutet. Alla de fyra stora instituten (Standard and Poor's, A.M. Best, Moody's, Fitch Ratings) har, anförda av Standard and Poor's, det senaste året offentliggjort riktlinjer för hur de kommer bedöma bolagens ERM-förmåga. Riskhanteringskapaciteten kommer att påverka bedömningen av kreditvärdigheten, och i överensstämmelse med tillsynsmyndigheternas bedömningsgrunder fokuserar idag kreditvärderingsinstitutens ERM-kriterier på bolagens riskhanteringskultur. En kunnig och involverad ledning med en välkommunicerad klar syn på bolagets riskaptit och risktolerans

efterfrågas. Dessutom poängteras vikten av att en solid intern modell för beräkning av ekonomiskt kapital används och införlivas med det löpande riskhanterings- och beslutsarbetet, speciellt om de högsta ERM-betygen eftersträvas. Institutens ERM-kriterier påminner i hög grad om varandra, och Standard and Poor's bedömningskriterier ges nedan mest utrymme.

Standard and Poor's

Standard and Poor's utkom i november 2005 med riktlinjer för bedömning av försäkringsbolagens ERM-kapacitet. Bedömningsgrunderna har efter återkoppling från branschen förfinats,¹⁸ och under 2006 betygsattes 241 försäkringsbolag över hela världen och gavs ERM-betyget svag, tillräcklig, stark eller utmärkt. ERM är endast en av åtta kategorier som Standard and Poor's bedömer vid sin kreditvärderingsprocess, men trots det krävs starkt eller utmärkt ERM-betyg för att bolagets totala kreditvärdighet skall kunna få betyget stark eller utmärkt.

Bedömningskriterierna hos Standard and Poor's är uppbyggda kring fem pelare där försäkringsbolagets riskhanteringskultur, riskkontrollprocess, beredskap för nya och extrema riskhändelser, kapacitet att mäta risker och kvantifiera ekonomiskt kapital, samt dess strategiska riskhantering undersöks.

Försäkringsbolagets *kultur*, där stor vikt läggs på styrelsens och ledningens delaktighet och framåtanda i ERM-arbetet anser Standard and Poor's vara mest betydelsefullt. Faktiska beslutsvägar inom organisationen, riskhanteringsavdelningens bemanning, organisation och behörighet, samt den generella riskmedvetenheten inom bolagets alla delar undersöks. Stor vikt läggs vid att bolagets ledning definierat organisationens risktolerans, vilket troligen kräver en analys med hjälp av interna modeller. I riskkulturen ingår även en undersökning av hur väl och tydligt ledningens budskap kommuniceras, förstås

och accepteras i organisationens olika delar.

Önskvärda egenskaper vid *riskkontrollprocesserna* är att beakta alla betydelsefulla risker i kontrollaktiviteterna, samt att vara försäkrad om att kontrollmekanismerna verkligen begränsar skador till att ligga inom intervallen i den accepterade risktoleransen. Dessutom undersöker Standard and Poor's vilka konsekvenserna blir inom organisationen om föreskrifter inte följs.

Nya risker är risktyper som är okända idag och därför inte kan mätas med vanliga metoder. Riskerna kan t.ex. uppstå på grund av förändringar i miljön, och en förutseende organisation förväntas planera även för det okända. *Extremriskhantering* behandlar organisationens reaktion vid katastrofhändelser som naturkatastrofer eller terroristattacker. Förutom att undersöka vilka planer som är upprättade för att affärsverksamheten skall kunna drivas vidare, bedöms även bolagets tillgång till likvida medel i stressade situationer.

Vid bedömningen av bolagets kapacitet att *mäta risker och kvantifiera ekonomiskt kapital* läggs tyngdpunkten på hurvida alla huvudsakliga risktyper identifierats och kvantifierats, samt hurvida formen och styrkan på samvariationen mellan risker har förståtts.¹⁹ En effektiv riskanalys kräver onekligen tillgång både till välstrukturerad och lättillgänglig data, och ett kraftfullt och anpassningsbart simuleringsverktyg där alla betydelsefulla risktyper, och orsak-verkan-interaktion mellan risktyper kan undersökas. I takt med att försäkringsbolagen inser hur viktig den interna modellen kommer att bli i verksamheten, som hjärtat i det kvantitativa riskhanteringsarbetet och som underlag vid planering, prissättning och belöningsystem, kommer mer resurser att krävas för analys- och simuleringsarbetet.

Försäkringsbolag med stark *strategisk riskhantering* använder den interna modellen för ekonomiskt kapitalberäkning när bolagets riktning stakas ut, och kan antas få en konkurrensfördel vid styrning av verksamheten genom

försäkringsmarknadens olika cykler. En förutsättning för kvantitativ strategisk riskhantering är dock att risker inom organisationen mäts och att lönsamhetsmåten, förutom förväntat resultat för olika försäkringsprodukter, även sätts i relation till hur stor del av bolagets kapital som måste allokeras till respektive produkt. Riskjusterade avkastningskrav bör alltså beräknas för hela portföljen, och strategiska beslut om att utöka eller minska engagemanget bör baseras på hurvida en produkt bidrar med mer värde till portföljen än dess kapitalbindningskostnad.

Det som karaktäriserar ett bolag med starkt ERM-betyg är alltså att styrelse och ledning är engagerade i ERM-arbetet och har definierat och kommunicerat risktolerans och önskvärd riskprofil till organisationen. Det kräver en holistisk syn på verksamhetens risker och därmed möjlighet att både mäta risker från individuella områden samt kapacitet att aggregera samman dem till bolagsnivå. Dessutom är bolag med stark ERM väl förberedda för nya risker som kan uppkomma i verksamheten, och tar strategiska beslut att växa eller dra sig tillbaka från olika segment med hjälp av riskjusterade avkastningsmått. Om bolagets ERM endast bedöms som tillräcklig är det fullt möjligt att olika riskgrupper var för sig kan mätas, men att det holistiska angreppssättet saknas. Svag ERM karaktäriseras av svårigheter att mäta och hantera även enskilda risker, samt en brist på kontrollprocesser. För betyget utmärkt ERM krävs i princip att bolaget anses vara en av ledarna inom riskhanteringsområdet. Bland de 241 bolag som betygssattes 2006 gavs 5 procent betyget svag, 82 procent tillräcklig, 10 procent stark och 3 procent utmärkt.

Standard and Poor's vill försäkra sig om att försäkringsbolaget visar ett långsiktigt engagemang för samordnad riskhantering på ledningsnivå, vilket deras typiska frågor vid ERM-uppföljningar visar. När ERM-betyget skall uppdateras undersöks exempelvis om

ERM-kapaciteten har förbättrats sedan sist, hur riskprofilen förändrats, om bolaget ändrat sin risktolerans, modifierat den önskvärda riskprofilen och hur risköverföring används för att uppnå den, samt hur de har kommunicerat detta inom organisationen.

A.M. Best

För stora och komplexa försäkringsbolag kräver A.M. Best att ett formellt ERM-ramverk implementeras.²⁰ Precis som Standard and Poor's lägger A.M. Best där stor vikt vid bolagets kultur och riskmedvetenhet, och poängterar att olika risker måste kunna kvantifieras och aggregeras med hänsyn tagen till riskernas samvariation för att uppnå en önskvärd holistisk riskbild. För små bolag med en enkel riskprofil och flera års stabilt resultat, vanligtvis specialiserade på en försäkringsprodukt, bör traditionell riskhantering där enskilda risker analyseras i enskildhet utan att slutligen aggregeras samman till en totalrisk (d.v.s så kallad *silobaserad* riskhantering) för närvarande vara tillräcklig och inte resultera i någon nedgradering av kreditvärdigheten. A.M. Bests utkast till kriterier för ERM-bedömning tar alltså fasta på att det inte är realistiskt att kräva ett rigoröst ERM-ramverk med dess krav på strukturer, personal, statistisk kompetens och mjukvara i alla bolag. Det kan dock aldrig skada om även enklare bolag använder valda delar av ERM-ramverket inom riskhanteringsarbetet.

Till stor del överensstämmer alltså A.M. Bests krav med Standard and Poor's. Riskmedvetenhet skall omfattas i det dagliga operativa arbetet, och detta budskap skall kommuniceras från ledningen. A.M. Best vill försäkra sig om att bolaget är kapabelt att identifiera och etablera kontrollrutiner för risker, samt att de tar ett bolagsomfattande angreppssätt på risker och deras samvariation. På denna analys ska välgrundade beslut om vilken typ av risköverföring som krävs för att verksamheten skall hållas inom den önsk-

värda risktoleransen baseras.

En viktig komponent i kreditvärderingsprocessen är bolagens kapitaltillräcklighet, beräknad med hjälp av A.M. Bests faktor-baserade BCAR-modell (Best's Capital Adequacy Ratio). Det verkar som att A.M. Best framöver kommer att tillåta bolag vars ERM-kapacitet bedöms som stark att hålla en mindre mängd kapital för en viss kreditvärdighet, jämfört med ett bolag med svag ERM.

A.M. Best anser att en intern modell för beräkning av ekonomiskt kapital är en mycket viktig komponent i ett bolags ERM-arbete. I takt med att bolagens interna modeller utvecklas, kommer fler resultat från de modeller som anses hålla hög kvalitet att beaktas vid kreditvärderingsprocessen. För att en intern modell skall anses stark kräver dock A.M. Best att modellen dels beaktar enskilda risker samt att riskers orsak-verkan-interaktion kan fångas. Även handhavandet med bestämning av indataparametrar till modellen måste utföras under kontrollerade former. Dessutom, vilket inte kan nämnas för ofta i dessa sammanhang, är ett krav för att modellens resultat skall beaktas av A.M. Best att försäkringsbolaget även använder modellen vid sin egen strategiska styrning av verksamheten.

Moody's

Moody's har etablerat ett ERM-ramverk med fyra huvudkategorier.²¹ *Riskstyrningskategorien* betonar ledningens betydelse och undersöker bolagets riskaptit, ägandeskapet för olika risker samt hur kontrollfunktioner har organiserats. Moody's vill se att ledningen definierat en riskaptit för hela bolaget med konsistenta riskbegränsningar för de olika affärsenheterna som möjliggör att de eftersträvade finansiella målen nås. Resultatutvecklingen bör följas upp med regelbundna rapporter, från bolagets CRO till ledningen.

Riskhanteringskategorin tar fasta på riskkontrollprocesser, vilka begränsningar som finns för risker som bolaget tar på sig och hur

dessa begränsningar styrs med hjälp av risköverföring. Riskhanteringen skall utgå från en holistisk syn på verksamhetens risker, och Moody's ställer krav på en koppling inom verksamheten mellan riskhanteringsaktiviteter, prissättning, kapitalhantering, och strategisk planering av affärsverksamheten.

Kategorin för *riskanalys och kvantifiering* fokuserar på bevakning, mätning och rapportering av risker. Risker måste kunna aggregeras i verksamheten och analysen ta hänsyn till effekten av risköverföring. Dessutom betonas vikten av att aktuariella parametrar stress-testas och att samvariation mellan parametrar uppmärksammas.

Iriskinfrastrukturkategorin undersöks kvaliteten på försäkringsbolagets IT-system, speciellt med avseende på datalagring och den programvarulösning som bolaget använder för sin interna modell. Moody's betraktar system där alla riskklasser och försäkringsprodukter, likväl som risköverföringsstrategier, kan modelleras i en integrerad miljö som tillförlitligare än när separata system används för olika produkter och riskkategorier.

Sammanfattningsvis skiljer sig inte Moody's ERM-bedömning i någon större omfattning från övriga kreditvärderingsinstitut. En ledning med god förståelse för försäkringsbolagets totala risktolerans och ett budskap som förs ut i organisationen, en lämplig kontrollfunktionsstruktur där risker mäts, hanteras och överförs till motparter om det är lämpligt, är det som eftersträvas. Dessutom poängterar Moody's vikten av en stabil databehandlingsmiljö vilket underlättar den statistiska parameterbestämningen som de interna modellerna kräver.

Fitch Ratings

Fitch Ratings framhäver att de explicita ERM-kraven på ett holistiskt angreppssätt och med fokuseringen på riskers samvariation är ett stort steg framåt vid försäkringsbolagets riskhantering. Även Fitch Ratings har definierat

ett antal kategorier vid sin formella ERM-bedömningsprocess: riskstyrning, risktolerans, riskbevakning, rapportering, modeller för ekonomiskt kapital, och riskoptimering.²² Grundläggande är dock styrelsens engagemang i ERM-arbetet och att ledningen får hjälp av en stark CRO med seniort ansvar som tillåts vara aktivt involverad i bolagets större affärsuppgörelser.

Fitch Ratings har själva investerat avsevärda resurser i den kvantitativa aspekten av ERM. De har utvecklat en egen stokastisk modell, Prism,²³ för att beräkna försäkringsbolags ekonomiska kapitalbehov. Utgående från publik information (som är speciellt lätt-tillgänglig för försäkringsbolagen i USA) används modellen vid Fitch Ratings kreditvärderingsprocess. För försäkringsbolag som kommunicerar resultat från sin interna beräkning av ekonomiskt kapital kommer resultatet från Prism att användas som måttstock.

Fitch Ratings framstår som det kreditvärderingsinstitut som har störst kvantitativ styrka, vilket även avspeglar sig i att de anser att försäkringsbolagens interna modeller för beräkning av ekonomiskt kapital är hjärtat i ERM-arbetet. Institutet anser att möjligheten att beräkna ekonomiskt kapital, på bolagsnivå, är ett krav för att kunna jämföra den riktiga kostnaden av att behålla en risk i bolaget med att utnyttja en risköverföringsstrategi.

V. Ta tempen på din egen organisation

Omfattningen på tillsynsmyndigheternas och kreditvärderingsinstitutens krav på ledningens aktiva engagemang i ERM-arbetet, samt betydelsen som läggs vid att använda en holistisk intern modell för beräkning av ekonomiskt kapital, gör det värdefullt att undersöka hur det ser ut i den egna organisationen idag.

En VD eller styrelseledamot i ett försäkringsbolag kan lämpligen ställa sig följande frågor: Har vi tydliggjort bolagets risktoleran-

ser, och på vilka grunder? Är linjechefer och andra anställda tillräckligt engagerade i riskkontrollarbetet? Har vi bestämt lämpliga riktlinjer för underwritingen inom bolagets olika produktlinjer, givet vår önskvärda totala riskprofil, och är dessa riskbegränsningar konsistenta? När reviderade vi senast dessa riktlinjer, och hur har verksamheten utvecklats sedan dess? Hur långt har arbetet kommit med att kvantifiera försäkringsrisk, marknadsrisk, kreditrisk och operativ risk? Har CRO koordinerat arbetet mellan riskkategorierna och analyserat riskerna i en integrerad simuleringsmiljö? Har resultaten jämförts med kapitalkraven från CEIOPS QIS3-modell, och skiljer sig vår erfarenhet av kapitalkraven under standardmodellen från övriga bolag i branschen? Har vi tillräcklig förståelse för de interna modellerna som aktuarierna och finansanalytikerna arbetar med? Har modellutvecklarna förstått vilka resultatmått från de interna modellerna vi behöver för att ta strategiska beslut för verksamheten? Har vår CRO-funktion tillräckligt god överblick och stark position i bolaget? Är vi nöjda med innehållet i riskrapporterna och hur ofta vi får dem? Hur lång tid skulle det ta för oss att bygga upp de nödvändiga ERM-strukturerna i verksamheten för att uppfylla kreditvärderingsinstitutens nuvarande krav, och på vilket sätt skulle en framtida nedgradering av bolagets betyg från t.ex. Standard and Poor's påverka vår verksamhet?

Detta är alla svåra frågor som försäkringsbolagens ägare, ledning och anställda just nu borde arbeta med.

VI. Slutsats

ERM-arbetet är en *kontinuerlig process* där verksamhetskritiska risker identifieras, bedöms och kvantifieras, varefter bolaget implementerar en integrerad strategi med målsättningen att hantera och, i förekommande fall, överföra risker till motparter på ett sådant

sätt att bolagets värdeskapande förmåga maximeras.

Försäkringsbolagens riskhanteringsförmåga har alltid granskats av kreditvärderingsinstitut och tillsynsmyndigheter, men nu formaliseras kraven. Med den nuvarande ERM-mognaden i branschen är det tydligt att fokuseringen ligger på styrelsens och ledningsgruppens attityd, engagemang och aktiva involvering i riskhanteringsarbetet. Det är mycket viktigt att ledningen har en övergripande syn på verksamhetens alla risker och förstår riskers samvariation. Slutligen lägger alla parter stor vikt vid att den holistiska interna modellen för att beräkna ekonomiskt kapital även används för strategiska beslut rörande verksamhetens riktning.

Erkännanden

Ett stort tack för klargöranden och värdefulla synpunkter som förbättrat artikeln, såväl språkligt som struktur- och faktamässigt, riktas till Frank Aichert, Erik Alm, Bengt Von Bahr, Olof Fält, Arne Sandström, Elisabeth Sundström, och Claes Thimrén.

Noter

- ¹ För att få en balanserad bild av nyttan och möjligheterna med kvantifiering av bolags-specifika risker och simulering av hela verksamheten bör man även lyfta fram processens svårigheter. Att exempelvis finna historiska skador, samt att omsätta dessa till bolagets nuvarande försäkringsverksamhet, riskexponering, återförsäkringsprogram och ersättningsnivåer kräver en omfattande analys där förståelse för den egna verksamheten måste kompletteras med statistisk expertis.
- ² Inom Guy Carpenter använder vi sedan många år tillbaka simuleringsplattformen MetaRisk för att analysera och optimera skadeförsäkringsverksamhet, med speciell fokusering på optimal återförsäkring.
- ³ Guy Carpenter 2007a, avsnitt 2.2, innehåller en genomgång av olika riskmått och principer för kapitalallokering.

- ⁴ Enligt pressreleasen från offentliggörandet av utkastet till EG-direktiv den 10 juli 2007. Tillgängligt online via <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/1060&format=HTML&aged=0&language=EN&guiLanguage=en>.
- ⁵ 5 miljoner Euro är beloppet i förslaget till direktiv. Siffran kan naturligtvis ändras under kommande förhandling innan den slutliga versionen av direktivet fastställs.
- ⁶ CEIOPS hemsida för QIS-arbetet: <http://www.ceiops.org/content/view/118/124>.
- ⁷ Olsén 2007 beskriver filosofin bakom det riskbaserade solvensregelverket Solvens 2, och betydelsen av att delta i QIS-undersökningarna.
- ⁸ KOM 2007b, fråga 19.
- ⁹ KOM 2007a. KOM 2007b, fråga 41.
- ¹⁰ KOM 2007b, fråga 15.
- ¹¹ CEIOPS 2007; KOM 2007a.
- ¹² KOM 2007a, artikel 42; KOM 2007b, fråga 26.
- ¹³ Kraven på en diplomerad aktuarie är harmoniserad i de europeiska länderna. Den europeiska aktuarieorganisationen Groupe Consultatif definierar vilka kunskapskrav som skall ställas på en aktuarie, varpå aktuarieföreningarna i de europeiska länderna ställer motsvarande krav i regler, vilket också leder till att den lokala aktuarieutbildningen på motsvarande sätt harmoniseras.
- ¹⁴ KOM 2007a, artikel 28; KOM 2007b, fråga 29.
- ¹⁵ Finansinspektionen 2007.
- ¹⁶ KOM 2007a, artikel 44; KOM 2007b, fråga 27.
- ¹⁷ KOM 2007a, artikel 109.
- ¹⁸ Standard and Poor's 2006; 2007a; 2007b.
- ¹⁹ Guy Carpenter 2007a, avsnitt 3.3, diskuterar hur samvariation kan mätas som linjär korrelation eller mer förfinat med copulateknik.
- ²⁰ A.M. Best 2007.
- ²¹ Moody's 2007.
- ²² Fitch Ratings 2006.
- ²³ Prism-modellen finns beskriven på <http://www.fitchratings.com/prism>.

Litteraturlista

- A.M. Best 2007: Draft: Risk Management and The Rating Process for Insurance Companies, A.M. Best 5 mars 2007. Tillgänglig från <http://www.ambest.com>.

- CEIOPS 2007: Risk Management and Other Corporate Issues, CEIOPS 17 juli 2007. Tillgänglig från <http://www.ceiops.org>.
- Finansinspektionen 2007: Pressmeddelandet ”Fivarner Carnegie, ger straffavgift på 50 miljoner kr och byter ut VD och styrelse”. Publicerat 28 september 2007 på <http://www.fi.se>.
- Fitch Ratings 2006: Enterprise Risk Management for Insurers and Prism’s Role, Fitch Ratings 26 september 2006. Tillgänglig från <http://www.fitchratings.com>.
- Guy Carpenter 2007a: Paul Brehm et al, *Enterprise Risk Analysis for Property & Liability Insurance Companies – A Practical Guide to Standard Models and Emerging Solutions*, Guy Carpenter & Company, LLC, New York 2007. Mer information finns på <http://ERMbook.guycarp.com>.
- Guy Carpenter 2007b: Internal Models – A Winning Solution for Solvency II, Guy Carpenter & Company, LLC, 2007. Tillgänglig från www.guycarp.com.
- KOM 2007a: Förslag till EUROPAPARALAMENTETS OCH RÅDETS DIREKTIV om upptagande och utövande av försäkrings- och återförsäkringsverksamhet – Solvens II, Europeiska Gemenskapernas Kommission, 10 juli 2007. Tillgänglig på olika språk via ’Com (2007) 361’-länken på http://ec.europa.eu/internal_market/insurance/solvency_en.htm.
- KOM 2007b: Solvency II: Frequently Asked Questions (FAQs), Europeiska Gemenskapernas Kommission, 10 juli 2007. Tillgänglig via ’Frequently Asked Questions (FAQ)’-länken på http://ec.europa.eu/internal_market/insurance/solvency_en.htm.
- Moody’s 2007: Risk Management Assessment: Non-life Insurance Companies, Moody’s mars 2007. Tillgänglig från <http://www.moodys.com>.
- Olsén 2007: Jörgen Olsén, Riskbaserade solvensregelverk enligt Solvens 2-metodiken – Hur det fungerar och varför försäkringsbolagen måste förbereda sig redan nu, Nordisk Försäkringstidskrift 2007:(1) 3-15.
- Standard and Poor’s 2006: Insurance Criteria: Refining The Focus Of Insurer Enterprise Risk Management Criteria, Standard and Poor’s 2 juni 2006. Tillgänglig från www.standardandpoors.com.
- Standard and Poor’s 2007a: Enterprise Risk Management At Firms Noticed By Its Absence As Time Goes By, Standard and Poor’s 23 februari 2007. Tillgänglig från www.standardandpoors.com.
- Standard and Poor’s 2007b: A Roadmap For Evaluating Financial Institutions’ ERM Practices, Standard and Poor’s 3 maj 2007. Tillgänglig från www.standardandpoors.com.