Enterprise Risk Management – Integrated Framework

Executive Summary

September 2004

Svensk översättning bearbetad av Torbjörn Wikland och accepterad av styrelsen för IIA Sweden för att skickas till COSO för godkännande

2007-01-25

Företagsövergripande riskhantering – sammanhållet ramverk

Sammanfattning för ledningen

September 2004

Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Oversight	**Representative**
COSO Chair	John J. Flaherty

American Accounting Association	Larry E. Rittenberg
American Institute of Certified Public Accountants	Alan W. Anderson
Financial Executives International	John P. Jessup
	Nicholas S. Cyprus
Institute of Management Accountants	Frank C. Minter
	Dennis L. Neider
The Institute of Internal Auditors	William G. Bishop, III
	David A. Richards

Project Advisory Council to COSO

Guidance

Toni Maki, Chair
Partner Moss Adams LLP

Mark S. Beasley
Professor
North Carolina State University

Jerry W. DeFoor
Vice President and Controller Protective Life Corporation

James W. Deloach
Managing Director
Protivity Inc.

Andrew J. Jackson
Senior Vice President of Enterprise Risk Assurance Services
American Express Company

Steven E. Jameson
Executive Vice President, Chief Internal Audit & Risk Officer Community Trust Bancorp, Inc.

John P. Jessup
Vice President and Treasurer E.I. duPont de Nemours and Company

Tony M. Knapp
Senior Vice President and Controller Motorola, Inc.

Douglas F. Prawitt
Professor
Brigham Young University

PricewaterhouseCoopers LLP

Author

Principal Contributors

Richard M. Steinberg — *Former Partner and Corporate Governance Leader (Presently Steinberg Governance)*

Frank J. Martens
Senior Manager, Client Services
Vancouver, Canada

Miles E. A. Everson
Partner and Financial Services
Finance, Operations Risk and Compliance
Leader New York

Lucy E. Nottingham
Manager, Internal Firm Services Boston

FÖRORD

För mer än tio år sedan gav the Committee of Sponsoring Organizations of the Treadway Commission (COSO) ut *Intern styrning och kontroll – ett sammanhållet ramverk (Internal Control – Integrated Framework),* för att stödja företag och andra organisationer i värderingen och utvecklingen av deras interna styr- och kontrollsystem. Detta ramverk har sedan dess införlivats som riktlinjer, regler och föreskrifter i och använts av tusentals företag för att förbättra styrningen och kontrollen av verksamheten i deras strävan att nå uppsatta mål.

De senaste åren har intresset för och fokus på riskhantering ökat. Det har blivit alltmer uppenbart att det finns ett behov av ett robust ramverk för att effektivt identifiera, värdera och hantera risker. COSO tog initiativ till ett projekt 2001 och anlitade PricewaterhouseCoopers för att utveckla ett ramverk som direkt skulle kunna användas av ledningen för att utvärdera och förbättra organisationens övergripande riskhantering.

Den tidsperiod då ramverket arbetades fram präglades av en rad uppmärksammade företagsskandaler och -misslyckanden som medförde enorma förluster för investerare, anställda och andra intressenter. I kölvatten på dessa händelser följde krav på förbättrad företagsstyrning (Corporate Governance) och riskhantering med nya lagar, regleringar och börsnoteringsregler. Behovet av ett ramverk för en företagsövergripande riskhantering, som tillhandahåller grundläggande principer och begrepp, ett gemensamt språk, tydliga anvisningar och vägledning blev alltmer angeläget. COSO anser att *Företagsövergripande*

riskhantering – ett sammanhållet ramverk (Enterprise Risk Management – Integrated Framework) fyller detta krav och förväntar sig att ramverket kommer att bli allmänt accepterat av företag och andra organisationer och särskilt av aktieägare och andra intressenter.

Ett av flera resultat av utvecklingen i USA är Sarbanes-Oxley Act, en lag som antogs 2002. Liknande lagstiftning har införts eller övervägs i andra länder. Denna lag tillgodoser ett sedan länge framfört krav ~~på~~ att börsnoterade företag ska ha interna styr- och kontrollsystem vars effektivitet företagsledningen har intygat och en oberoende revisor bekräftat. *Intern styrning och kontroll – ett sammanhållet ramverk (Internal Control – Integrated Framework)* fortsätter att klara tidens prövningar och utgör en brett accepterade standards för att uppfylla de rapporteringskrav som ställs.

Företagsövergripande Riskhantering – ett sammanhållet ramverk (Enterprise Risk Management – Integrated Framework) bygger vidare på intern styrning och kontroll och tillhandahåller ett mer robust och utförligare fokus på det bredare ämnet företagsövergripande riskhantering. Avsikten med Företagsövergripande riskhantering – ett sammanhållet ramverk är inte att ersätta ramverket för intern styrning och kontroll utan att integrera det med ramverket för intern styrning och kontroll. Företag kan studera ramverket för företagsövergripande riskhantering både för att tillgodose sin interna styrning och kontroll och för att gå vidare till en mer fullödig riskhanteringsprocess.

En av de mest kritiska utmaningarna för ledningen är att bestämma hur mycket risk organisationen är beredd att acceptera och accepterar i praktiken när den strävar efter att skapa värden. Denna rapport vill göra det lättare för dem att möta dessa utmaningar.

John J. Flaherty
Ordförande COSO

Tony Maki
Ordförande COSO Advisory Council

SAMMANFATTNING FÖR LEDNINGEN

Den underliggande förutsättningen för en företagsövergripande riskhantering är att varje organisation finns till för att skapa värde för dess intressenter. Alla organisationer möter osäkerhet, och utmaningen för ledningen är att bestämma hur mycket osäkerhet som kan accepteras när den strävar efter att öka värdet för intressenterna. Osäkerhet innebär både risker och möjligheter med potential att både urholka och öka värdet. Företagsövergripande riskhantering ger ledningen möjlighet att på ett effektivt sätt hantera osäkerhet och därtill hörande risker och möjligheter och därmed öka möjligheterna att skapa värde.

Maximalt värde uppnås när ledningens strategi och mål är att åstadkomma optimal balans mellan tillväxt och vinstmål och relaterade risker, och använda resurserna effektivt och produktivt för att uppnå företagets mål. Företagsövergripande riskhantering innefattar att:

- *koppla samman riskaptit och strategi* – ledningen ska ta hänsyn till organisationens riskaptit när strategiska alternativ ska utvärderas och när mål ska fastställas och mekanismer utvecklas för att hantera berörda risker
- *fatta bättre beslut om riskåtgärder* – företagsövergripande riskhantering ska tillhandahålla den struktur som krävs för att kunna identifiera och välja bland alternativa riskåtgärder, dvs. undvika, reducera, dela eller acceptera riskerna,
- *minska risken för överraskningar och förluster i verksamheten* – organisationer får bättre möjligheter att identifiera tänkbara händelser och genomföra åtgärder, reducera överraskningarna och de kostnader och förluster som kan följa.
- *identifiera och hantera risker som är sammansatta och som skär rakt igenom hela företaget* – varje företag möter otaliga risker som berör olika delar av organisationen. Företagsövergripande riskhantering underlättar effektiva åtgärder mot sammankopplade följdverkningar och integrerade åtgärder mot sammansatta risker.
- *ta tillvara gynnsamma möjligheter* – genom att analysera ett stort antal potentiella händelser är ledningen i stånd att identifiera och i god tid ta tillvara affärsmöjligheter och andra gynnsamma möjligheter.
- *Förbättra kapitalanvändningen* – god information om vilka risker som kan uppstå ger företagsledningen möjlighet att effektivt bedöma det övergripande kapitalbehovet och fördela kapitalet på bästa sätt.

De nämnda möjligheterna för en företagsövergripande riskhantering stödjer ledningen att nå organisationens verksamhets- och vinstmål och undvika resursförluster. Företagsövergripande

riskhantering är ett stöd för effektiv rapportering, efterlevnad av lagar och förordningar och för att företagets rykte inte skadas med de konsekvenser det kan innebära. Kort sagt hjälper företagsövergripande riskhantering organisationen att nå dit den vill och undvika fallgropar och överraskningar längs med vägen.

Händelser innebär både risker och möjligheter[1]

Händelser kan ha negativ eller positiv inverkan eller bådadera. Händelser med negativ inverkan representerar risker som kan förhindra värdeskapande eller undergräva befintliga värden. Händelser med en positiv inverkan kan undanröja en negativ inverkan eller innebära gynnsamma möjligheter. Sådana möjligheter innebär att en händelse kan inträffa som positivt påverkar strävan att nå målen, skapa eller bevara värden i organisationen. Ledningen kanaliserar tillbaka de gynnsamma möjligheterna till företagets strategi- och målsättningsprocess och utarbetar planer för att tillvarata dessa möjligheter.

Definition av företagsövergripande riskhantering

Företagsövergripande riskhantering (*Enterprise Risk Management*) handlar om risker och gynnsamma möjligheter som påverkar skapandet eller bibehållandet av värden och definieras på följande sätt:

Företagsövergripande riskhantering är en process som genomförs av en organisations styrelse, ledning och annan personal, och som genomförs i ett strategiskt sammanhang och över hela företaget, utformad för att identifiera potentiella händelser som kan påverka organisationen och hantera risker inom ramen för dess riskaptit och ge rimlig försäkran om att organisationens mål uppnås.

Denna definition återspeglar några grundläggande begrepp. Företagsövergripande riskhantering:

- är en löpande process, som genomsyrar hela organisationen
- genomförs av människor på varje nivå i organisationen

[1] Riskbegreppet i COSO: s rapport är främst kopplat till händelser med negativ inverkan. I andra riskanalyserande rapporter innefattar riskbegreppet mer entydigt händelser med såväl negativ som positiv inverkan. *Översättarens anm.*

- används i det strategiska arbetet
- används över hela organisationen, på varje nivå och i varje enhet och innefattar att riskerna optimeras över hela organisationen.
- är utformad för att identifiera potentiella händelser som, om de inträffar, påverkar organisationen, och för att hantera risker inom ramen för dess riskaptit
- kan ge en rimlig försäkran till organisationens ledning och styrelse
- är anpassad för att nå mål i en eller flera skilda men överlappande målkategorier

Denna definition är med avsikt brett utformad. Den fångar nyckelbegrepp som är grundläggande för hur företag och andra organisationer hanterar risker och utgör en bas för tillämpning oavsett organisation, bransch och sektor. Den fokuserar direkt på att nå uppsatta mål i en enskild organisation och utgör basen för att definiera en effektiv företagsövergripande riskhantering.

Att nå uppsatta mål

Inom ramen för en organisations fastställda syfte eller vision fastställer ledningen strategiska mål, väljer strategi och preciserar en uppsättning mål för verksamhetens olika delar. Detta ramverk för företagsövergripande riskhantering är anpassat för att nå organisationens mål och delas in i fyra kategorier:

- *Strategiska mål* – mål på hög nivå, nära knutna till och som stödjer dess syfte
- *Operationella mål* – effektivt och produktivt utnyttjande av dess resurser
- *Rapporteringsmål* – tillförlitlig rapportering
- *Efterlevnadsmål* – efterlevnad av gällande lagar och regler

Denna kategorisering av organisationens mål medger fokusering på olika aspekter av företagsövergripande riskhantering. Dessa tydliga men överlappande kategorier - ett mål kan hamna inom fler än en kategori - berör olika organisationsbehov och kan falla inom olika befattningshavares ansvarsområden. Kategoriseringen medger också en precisering av vad som kan förväntas inom varje målkategori. Ytterligare en kategori som används av vissa organisationer, nämligen säkerställande av resurser, beskrivs också.

Eftersom de mål som avser tillförlitlig rapportering och efterlevnad av gällande lagar och regler ligger inom organisationens styrning och kontroll kan företagsövergripande riskhantering förväntas ge rimlig försäkran om att dessa mål uppnås. Uppnåendet av strategiska och operativa mål beror dock av externa händelser som inte alltid styrs eller kontrolleras genom organisationens egna åtgärder. För dessa mål ger en företagsövergripande riskhantering en rimlig försäkran om att ledningen, liksom styrelsen i sin övervakande roll, i tid görs medvetna om i vilken utsträckning företaget når uppställda mål.

Den företagsövergripande riskhanteringens komponenter

Företagsövergripande riskhantering består av åtta sammankopplade komponenter. De utgår från det sätt som en ledning driver ett företag och är integrerade i ledningsprocessen. Dessa komponenter är:

- *Den interna miljön* – Den interna miljön innefattar det arbetsklimat som finns i organisationen och som bestämmer utgångspunkten för hur organisationens medarbetare ser på och förhåller sig till risker. Den inkluderar ledningens riskhanteringsfilosofi och riskaptit, integritet och etiska värderingar, och den miljö i vilken de verkar.
- *Formulerandet av mål* – Mål måste finnas innan ledningen kan identifiera potentiella händelser som påverkar uppnåendet av målen. Företagsövergripande riskhantering säkerställer att ledningen har etablerat en process för att sätta mål och att de valda målen stödjer och knyter an till organisationens syften och motsvarar organisationens riskaptit.
- *Identifiering av händelser* – Interna och externa händelser som kan påverka en organisations möjligheter att nå sina mål måste identifieras och preciseras som risker och möjligheter. Möjligheterna kanaliseras tillbaka till ledningens processer för att utforma strategier och mål.
- *Riskbedömning* – Risker analyseras, med utgångspunkt från deras sannolikhet och konsekvenser, för att få ett underlag för hur de ska hanteras. Risker bedöms både före och efter hantering, dvs. både som ursprungliga och återstående risker.

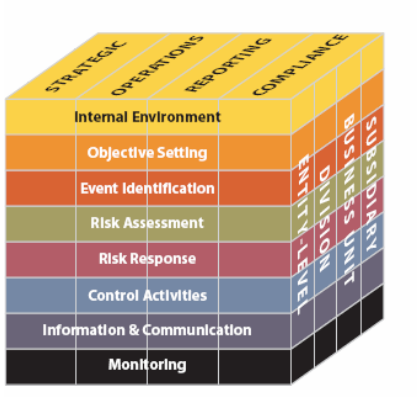
- *Riskåtgärder* – Ledningen väljer vilka åtgärder som ska vidtas – dvs. undvika, acceptera, reducera eller dela risken – och anpassar åtgärderna så att de stämmer överens med organisationens risktolerans och riskaptit.
- *Kontrollaktiviteter* – Riktlinjer och rutiner fastställs och genomförs för att säkerställa att riskåtgärderna genomförs på ett effektivt sätt
- *Information och kommunikation* – Relevant information identifieras, samlas in och förmedlas i en form och inom en tidsram som gör det möjligt för de anställda att utföra sina åtaganden. En effektiv kommunikation kan även uppstå i en vidare mening genom att den flödar ner i, tvärs över och uppåt i organisationen.
- *Övervakning, inklusive uppföljning och utvärdering* – Hela den företagsövergripande riskhanteringen övervakas och modifieras när det behövs. Övervakning sker genom löpande ledningsaktiviteter inklusive uppföljningar, separata utvärderingar, eller bådadera.

Företagsövergripande riskhantering är inte i strikt mening en seriell process där en komponent endast påverkar den nästkommande. Den är en process med verkan i flera riktningar och som upprepas iterativt, och där praktiskt taget varje komponent kan påverka och påverkar de andra.

Sambandet mellan mål och komponenter

Det finns ett direkt samband mellan de mål som ett företag strävar efter att nå och komponenterna i den företagsövergripande riskhanteringen, där komponenterna representerar vad som behövs för att nå dem. Sambandet är avbildat i en tredimensionell matris, i form av en kub.

De fyra målkategorierna – strategiska, operationella, rapporterings- och efterlevnadsmål, återfinns i de vertikala kolumnerna, de åtta komponenterna i de horisontella raderna och organisationens olika enheter utgör den tredje dimensionen. Denna bild återspeglar förmågan att fokusera på helheten i en organisations företagsövergripande riskhantering eller dess målkategorier, komponenter,



organisationsenheter eller delar av dem.

Effektivitet

Att fastställa om en organisations företagsövergripande riskhantering är ”effektiv” sker som resultat av en bedömning av om de åtta komponenterna anses finnas på plats och fungera effektivt. Således är komponenterna ett kriterium på en effektiv företagsövergripande riskhantering. För att komponenterna ska finnas på plats och fungera ordentligt får det inte finnas några väsentliga svagheter och riskerna måste ha tagits om hand inom ramen för organisationens riskaptit.

När den företagsövergripande riskhanteringen bedöms vara effektiv i var och en av de fyra målkategorier kan företagsledning och styrelse med rimlig säkerhet fastställa att de förstår i vilken utsträckning företagets strategiska och operationella mål uppnås och att bolagets rapportering är tillförlitlig samt att gällande lagar och förordningar efterlevs .

De åtta komponenterna kommer inte att fungera på samma sätt i alla organisationer. I t.ex. mindre och medelstora organisationer kan tillämpningen vara mindre formell och ha en lösare struktur. Trots detta kan den företagsövergripande riskhanteringen i mindre organisationer fortfarande vara effektiv så länge alla komponenter finns på plats och fungerar ordentligt.

Begränsningar

Även om företagsövergripande riskhantering erbjuder viktiga fördelar, finns det också begränsningar. Utöver de faktorer som diskuterats ovan kan begränsningar uppstå när det mänskliga omdömet fallerar i beslutsfattandet, när beslut om att åtgärda risker och införa kontroller måste innefatta avvägning av kostnader mot nytta, när haverier kan inträffa på grund av mänskliga brister såsom enkla fel och misstag, när kontroller kan kringgås genom bedrägligt förfarande av två eller flera personer och när ledningen har möjlighet att köra över beslut om riskhantering. Dessa begränsningar utesluter att en styrelse och ledningen med absolut säkerhet kan fastslå att organisationen når sina uppställda mål.

Innefattar intern styrning och kontroll

Intern styrning och kontroll är en integrerad del av den företagsövergripande riskhanteringen. Detta ramverk för företagsövergripande riskhantering innefattar intern styrning och kontroll och skapar mera robusta begrepp och verktyg för ledningen. Intern styrning och kontroll definieras och beskrivs i *”Intern styrning och kontroll – ett sammanhållet ramverk” (Internal Control – Integrated Framework).* Eftersom ramverket har klarat tidens prövningar och är grunden för nuvarande regler, förordningar och lagar, så förblir detta dokument definitionen på och ramverket för intern styrning och kontroll. Det är bara delar av texten i *“Intern styrning och kontroll – ett sammanhållet ramverk”* som återges i detta ramverk, men hela ramverket används som referens i detta dokument.

Roller och ansvar

Alla anställda i en organisation har något ansvar för den företagsövergripande riskhanteringen. Verkställande direktören är ytterst ansvarig och bör åta sig ägarskapet. Andra ledande befattningshavare stödjer organisationens riskhanteringsfilosofi, ser till att riskhanteringen är i linje med dess riskaptit och hanterar riskerna inom sina ansvarsområden och håller dem inom gränserna för etablerade risktoleranser. Ansvariga ledare för riskhantering, ekonomi, internrevision och andra har vanligtvis viktiga stödjande uppgifter. Andra anställda inom organisationen är ansvariga för att riskhanteringen utförs i enlighet med upprättade direktiv och fattade beslut. Styrelse bidrar med en viktig övervakande roll i den företagsövergripande riskhanteringen och är medveten om och godkänner organisationens riskbenägenhet. Flera externa intressenter såsom kunder, återförsäljare, affärspartners, externrevisorer, myndigheter och finansanalytiker, erbjuder ofta värdefull information för genomförandet av en företagsövergripande riskhantering, men de har inget ansvar för, eller är en del av organisationens företagsövergripande riskhantering.

Rapportens uppbyggnad

Denna rapport är uppdelad i två volymer. Den första volymen innehåller *Ramverket* och *Sammanfattningen för ledningen*. *Ramverket* definierar företagsövergripande riskhantering och beskriver principer och begrepp, som ger vägledning för befattningshavare på alla nivåer i företag och andra typer av organisationer, för att utvärdera och öka effektiviteten i den företagsövergripande riskhanteringen. *Sammanfattningen för ledningen* ger en överblick på hög nivå och riktar sig till verkställande direktörer och andra ledande befattningshavare,

styrelsemedlemmar och myndigheter. Den andra volymen, *Metoder för tillämpning (Application Techniques),* ger metodmässiga illustrationer som kan vara användbara för att tillämpa olika delar av ramverket.

Användningen av rapportern

Föreslagna åtgärder som kan vidtas med utgångspunkt från rapporten beror på berörda parters och intressenters befattningar och roller:

- *Styrelse* – Styrelsen bör diskutera det aktuella läget i organisationens företagsövergripande riskhantering med den verkställande ledningen och vid behov övervaka den. Styrelsen bör se till att den underrättas om de mest betydande riskerna och de åtgärder som ledningen vidtar och hur den säkerställer en effektiv företagsövergripande riskhantering. Styrelsen bör överväga om den kan få ytterligare underlag från internrevisorer, externrevisorer och andra
- *Den högsta verkställande ledningen* – Denna rapport föreslår att den verkställande direktören bedömer organisationens förmåga till företagsövergripande riskhantering. Ett tillvägagångssätt kan vara att verkställande direktören samlar ansvariga för affärsenheter och nyckelpersoner ur funktionsenheter för en inledande bedömning av förmågan till och effektiviteten i den företagsövergripande riskhanteringen. Oavsett tillvägagångssätt bör en inledande bedömning avgöra huruvida en bredare och djupare utvärdering behövs och hur en sådan i så fall ska utformas.
- *Övrig personal* – Chefer och övrig personal bör granska hur de utför sina förpliktelser i ljuset av detta ramverk och diskutera med högre chefer tänkbara idéer för att förbättra den företagsövergripande riskhanteringen. Internrevisorer bör överväga om fokuseringen på företagsövergripande riskhantering är tillräckligt bred.
- *Myndigheter* – Detta ramverk kan främja en gemensam syn på företagsövergripande riskhantering inklusive dess möjligheter och dess begränsningar. Myndigheter kan hänvisa till ramverket för att etablera förväntningar, antingen genom regler eller riktlinjer, eller genom att utföra granskningar av de organisationer de övervakar.
- *Professionella organisationer* – Regelbildande och andra professionella organisationer som ger vägledning i frågor om ekonomistyrning, revision och liknande ämnesområden bör se över standards och rekommendationer i ljuset av detta

ramverk. Om skillnader i begrepp och terminologi kan elimineras gynnar detta alla berörda parter.

- *Utbildningsinstitutioner* – Detta ramverk kan bli ett ämne för akademisk forskning och analys för att undersöka möjligheter till framtida förbättringar. Under förutsättning att denna rapport accepteras som en gemensam grund för förståelse bör de begrepp och den terminologi som används i rapporten ta sin plats i akademiska läroplaner.

Med denna grund för ömsesidig förståelse kommer alla parter och intressenter kunna tala med ett gemensamt språk och kommunicera mer effektivt. Företagsledare kommer att kunna bedöma sitt företags övergripande riskhanteringsprocess mot standards och förbättra processen och styra deras företag mot fastställda mål. Framtida forskning kan utgå från en etablerad bas. Lagstiftare och myndigheter kommer få ökad förståelse för företagsövergripande riskhantering inklusive dess fördelar och begränsningar. När alla parter använder ett gemensamt ramverk för företagsövergripande riskhantering kommer dessa fördelar att förverkligas.