

COSO – Internal Control – Integrated Framework - 1992

Executive Summary

Svensk översättning bearbetad av Torbjörn Wikland från råöversättning av PwC för auktorisering av COSO till Internrevisorernas Förening – IIA Sweden
2006-11-07

COSO - Intern styrning och kontroll – integrerat ramverk

Sammanfattning för ledningen

Ledande befattningshavare har länge sökt efter vägar att bättre styra och kontrollera de företag de leder. Åtgärder som rör styrning och kontroll etableras för att styra företaget mot vinstmål och grundläggande uppdrag och för att minimera överraskningar längs dess väg. De gör det möjligt för ledningen att hantera en snabbt förändrad omvärld ekonomiskt och konkurrensmässigt, kunders förändrade efterfrågan och prioriteringar och rekonstruktioner för framtida tillväxt. Åtgärder som rör intern styrning och kontroll främjar effektivitet, reducerar risken för att tillgångar förloras och understödjer en tillförlitlig finansiell rapportering samt efterlevnaden av lagar och regler.

Eftersom intern styrning och kontroll stödjer flera viktiga syften höjs det allt starkare röster för bättre interna styr- och kontrollsystem och rapporteringsformer för dem. Intern styrning och kontroll betraktas alltmer som en lösning på flera olika potentiella problem.

Vad intern styrning och kontroll innebär

Intern styrning och kontroll betyder olika saker för olika människor. Detta orsakar förvirring bland dem som arbetar i företag, lagstiftare, tjänstemän i myndigheter och andra. Resultat i form av missförstånd och olika förväntningar orsakar problem inom ett företag. Problemen byggs på när termen, om den inte definieras tydligt, skrivs in i lagar, förordningar och regler.

Denna rapport handlar om behoven och förväntningarna hos ledningen och andra. Den definierar och beskriver intern styrning och kontroll för att:

- etablera en gemensam definition som tillgodoser behoven hos olika intressenter.
- tillhandahålla en standard mot vilken företag och andra organisationer – stora eller små, inom den offentliga eller privata sektorn, med eller utan vinstmål – kan bedöma sina styr- och kontrollsystem och bestämma hur de ska förbättras.

Intern styrning och kontroll är definierad generellt som en process, utförd av en organisations styrelse, ledning och annan personal, utformad för att ge rimlig försäkran om att målen uppfylls inom följande kategorier:

- effektivitet och produktivitet i verksamheten
- tillförlitlig finansiell rapportering
- efterlevnad av berörda lagar och regler.

Den första kategorin riktas mot en organisations grundläggande verksamhetsmål inklusive resultat- och vinstmål och skyddandet av tillgångar. Den andra berör förberedandet av tillförlitliga publicerade finansiella lägesrapporter inklusive interimistiska och koncentrerade finansiella uttalanden och utvalda finansiella data ur sådana uttalanden såsom publicerade inkomstrapporter. Den tredje handlar om efterlevnaden av sådana lagar och förordningar som organisationen har att följa. Dessa tydliga men överlappande kategorier riktas mot olika behov och medger en bestämd fokus för att tillgodose dessa olika behov.

System för intern styrning och kontroll verkar på olika nivåer av effektivitet. Intern styrning och kontroll kan bedömas effektiva i vart och ett av de tre kategorierna, om styrelsen och ledningen har rimlig säkerhet för att:

- de förstår i vilken utsträckning organisationens verksamhetsmål uppnås
- publicerade finansiella uttalanden är tillförlitligt underbyggda
- berörda lagar och förordningar efterlevs.

Under det att intern styrning och kontroll är en process är dess effektivitet ett läge eller tillstånd i processen vid en eller fler tidpunkter.

Intern styrning och kontroll består av fem sinsemellan beroende komponenter. Dessa är härledda från det sätt som en ledning styr ett företag och är integrerade styrprocessen. Även om komponenterna kan tillämpas på alla organisationer kanske små och medelstora företag implementerar dem på ett annat sätt än stora företag. Dess styrsignaler och kontroller kan vara mindre formella och mindre strukturerade men ett litet företag kan ändå ha effektiv intern styrning och kontroll.

Komponenterna är:

Kontrollmiljön

Kontrollmiljön anger tonen i en organisation och påverkar kontrollmedvetenheten hos dess medarbetare. Det är grunden för alla andra komponenter för intern styrning och kontroll och erbjuder ordning och struktur. Faktorer inom kontrollmiljön innefattar integritet, etiska värden, kompetensen hos medarbetarna i organisationen, ledningens filosofi och ledarstil, det sätt på vilket ledningen fördelar ansvar och befogenheter och organiserar och utvecklar dess medarbetare samt den uppmärksamhet och vägledning som styrelsen ger.

Riskvärdering

Varje organisation möter många olika risker av externt och internt ursprung som måste värderas. En förutsättning för riskvärderingen är etablerandet av mål knutna till olika nivåer och som är internt konsistenta. Riskvärderingen är identifieringen och analysen av relevanta risker för att uppnå målen och utgör basen för att bestämma hur riskerna ska hanteras. Eftersom ekonomiska, branschmässiga, regleringsspecifika och verksamhetsmässiga villkor kommer att förändras, behövs mekanismer för att identifiera och hantera de särskilda risker som förknippade med förändring.

Kontrollaktiviteter

Kontrollaktiviteter är de riktlinjer och rutiner som bidrar till att säkerställa att ledningens direktiv genomförs. De bidrar till att säkerställa att nödvändiga åtgärder vidtas för att hantera risker för att organisationens mål inte uppnås. Kontrollaktiviteter äger rum inom hela organisationen, på alla nivåer och i alla funktioner. De innefattar en rad aktiviteter av olika slag såsom godkännanden, attester, verifikationer, avstämningar, genomgångar av verksamhetens resultat, säkrandet av tillgångarna, samt åtskillnad av tjänsteroller och uppgifter.

Information och kommunikation

Relevant information måste identifieras, fångas, och förmedlas i en sådan form och inom en sådan tidsram att de anställda kan utföra sina uppgifter. Informationssystem genererar rapporter som innehåller verksamhetsmässig och finansiell information och uppgifter om regelefterlevnaden som gör det möjligt att driva och styra företagets verksamhet. De handlar inte bara om internt genererade data utan även om information om yttre händelser, aktiviteter och villkor som är nödvändiga för välgrundade affärsbeslut och extern rapportering. Effektiv kommunikation måste även förekomma i en vidare bemärkelse och flöda nedåt, uppåt och över hela organisationen. All personal måste få ett klart budskap från den högsta ledningen att ansvaret för intern styrning och kontroll måste tas på allvar. De anställda måste förstå sin egen roll i det interna styr- och kontrollsystemet samt hur enskilda aktiviteter påverkar andras arbete. De måste ha en kanal för att kommunicera betydelsefull information uppåt. Det finns också behov av effektiv kommunikation med externa parter, såsom kunder, leverantörer, myndigheter och aktieägare.

Övervakning inklusive uppföljning och utvärdering

Interna styr- och kontrollsystem behöver övervakas, följas upp och utvärderas – en process som bestämmer kvalitén på systemets resultat över tiden. Det åstadkoms genom löpande övervakningsåtgärder och uppföljningar, separata utvärderingar eller en kombination av dessa. Löpande övervakningsåtgärder och uppföljningar äger rum under verksamhetens gång. Det inkluderar normala lednings- och övervakningsaktiviteter och andra åtgärder som personalen vidtar när de utför sina arbetsuppgifter. Omfattningen och frekvensen av separata utvärderingar beror i först hand på en värdering av risker och effektiviteten i rutinerna för de löpande övervakningsåtgärderna och uppföljningarna.

Det finns synergi och kopplingar mellan de nämnda komponenterna, som formar ett integrerat system som reagerar dynamiskt på ändrade förutsättningar. Det interna styr- och kontrollsystemet är integrerat med organisationens verksamhet och finns till av grundläggande affärs- och verksamhetsmässiga skäl. Intern styrning och kontroll blir effektivast om kontrollerna är inbyggda i organisationens infrastruktur och ingår som en väsentlig del av företaget. ”Inbyggda” kontroller stödjer initiativ för kvalitet och delegering, undviker onödiga kostnader och möjliggör snabba svarsåtgärder vid förändrade förutsättningar.

Det finns ett direkt samband mellan de tre kategorierna av mål, som gäller vad en organisation strävar att uppnå och komponenterna, som gäller vad som krävs för att uppnå målen. Alla komponenterna är relevanta för varje målkategori. Om man betraktar en enskild kategori – t.ex. effektiviteten och produktiviteten i verksamheten – måste alla fem komponenterna vara

närvarande och fungera effektivt för att man skall kunna dra slutsatsen att den interna styrningen och kontrollen över verksamheten är effektiv.

Definitionen på intern styrning och kontroll – med dess bakomliggande grundbegrepp av en process, utförd av människor, för att ge rimlig säkerhet tillsammans med målkategoriseringen och komponenterna samt kriterierna för effektivitet med anknytande diskussioner – som utgör detta ramverk för intern styrning och kontroll.

Vad kan man uppnå med intern styrning och kontroll?

Intern styrning och kontroll kan hjälpa en organisation att uppnå sina resultat- och lönsamhetsmål och förhindra resursförluster. Den kan bidra till att säkerställa tillförlitlig finansiell rapportering. Det kan också hjälpa företaget att efterleva lagar och förordningar och därmed undvika förtroendeskadorna och andra konsekvenser. Sammantaget kan intern styrning och kontroll hjälpa en organisation att nå dit den vill och undvika fallgropar och överraskningar längs dess väg.

Vad kan man inte uppnå med intern styrning och kontroll?

Olyckligtvis har en del personer större, och orealistiska, förväntningar. De söker absoluta besked i tron att:

- intern styrning och kontroll kan säkerställa en organisations framgång – dvs. att den kommer att säkerställa att grundläggande affärs- och verksamhetsmål uppfylls eller åtminstone säkerställer överlevnaden.

Även effektiv intern styrning och kontroll kan endast bidra till att en organisation uppnår dessa mål. Den kan ge ledningen information om organisationens framsteg eller brist på framsteg för att uppnå dess mål. Däremot kan intern styrning och kontroll inte förändra en i sig dålig chef till en bra chef. Förändringar i regeringens politik eller program, konkurrenternas åtgärder eller ekonomiska förutsättningar kan vara utanför ledningens kontroll. Intern styrning och kontroll kan inte säkerställa framgång eller ens överlevnad.

- intern styrning och kontroll kan säkerställa den finansiella rapporteringens tillförlitlighet och efterlevnad av lagar och förordningar.

Denna uppfattning är också ogrundad. Ett internt styr- och kontrollsystem, oavsett hur väl utformat och fungerande det är, kan endast ge ledningen och styrelsen rimlig – inte absolut – säkerhet att organisationen uppnår sina mål. Sannolikheten att man uppnår sina mål påverkas av de begränsningar som präglar alla interna styr- och kontrollsystem. De inbegriper sådana realiteter som att bedömningar i beslutsfattandet kan vara felaktiga, och att driftavbrott kan inträffa kan inträffa på grund av enkla fel eller misstag. Dessutom kan kontroller kringgå om två eller flera personer arbetar i maskopi och det är möjligt för ledningen köra över systemet. En ytterligare begränsande faktor är att utformningen av ett intern styr- och kontrollsystem måste återspegla det faktum att resurserna är begränsade och att nyttan med kontroller måste sättas i relation till kostnaderna för dem.

Även om således intern styrning och kontroll kan bidra till att en organisation uppnår sina mål är det inget universalmedel.

Roller och ansvarsfördelning

Var och en inom en organisation har ansvar för intern styrning och kontroll.

Ledningen

Verkställande direktören eller motsvarande har det yttersta ansvaret och bör vara "ägare" av systemet. Mer än någon annan person anger verkställande direktören "tonen" i företagets ledning och som påverkar integritet och etik och andra faktorer i en positiv kontrollmiljö. I ett stort företag fullföljer verkställande direktören detta ansvar genom att visa ledarskap och ange inriktning för de högre cheferna och granska hur de styr och kontrollerar verksamheten. De högre cheferna ålägger i sin tur ansvaret för att etablera mer specifika riktlinjer och rutiner på personer med ansvar för verksamhetens olika funktioner. I ett mindre företag är verkställande direktörens, ofta ägarens, inflytande mer direkt. Oavsett detta gäller att när ansvaret är uppdelat på många områden så fungerar dessa områdeschefer i praktiken som verkställande direktörer för sitt respektive område. Särskilt stor betydelse har ekonomichefer och deras personal eftersom deras kontrollaktiviteter verkar tvärs över, uppåt och nedåt i företagets rörelsedrivande och andra enheter.

Styrelsen

Företagsledningen är ansvarig inför styrelsen, som ger riktlinjer och råd och har en granskande roll. Effektiva styrelseledamöter är objektiva, kunniga och frågvisa. De har också kunskaper om företagets verksamhet och miljö och ägnar den tid som krävs för att fullfölja sina styrelseåtaganden. En företagsledning kan utnyttja sin position för att köra över kontroller, strunta i eller undertrycka framförd information från underordnade och göra det möjligt för en ohederlig ledning att avsiktligt förvränga resultat för att sopa igen spåren efter sig. En stark och aktiv styrelse, särskilt i kombination med effektiva kommunikationskanaler uppåt och kompetenta funktioner för ekonomi, juridik och internrevision, har störst möjligheter att identifiera och korrigera ett sådant problem.

Internrevisorer

Internrevisorer spelar en viktig roll genom att utvärdera effektiviteten i styr- och kontrollsystem och bidra till den löpande effektiviteten. På grund av sin organisatoriska placering och befogenhet i ett företag kan en internrevisionsfunktion ofta spela en viktig övervakande roll.

Övrig personal

Intern styrning och kontroll är i viss utsträckning ett ansvar för var och en i en organisation och bör därför vara en uttalad eller underförstådd del av arbetsbeskrivningen för samtliga. Så gott som alla anställda producerar information som används i det interna styr- och kontrollsystemet eller vidtar åtgärder som krävs att utöva kontroll. Därutöver bör all personal ha ett ansvar för att uppåt förmedla information om problem i verksamheten, avvikelser från uppförandekoden eller andra överträdelser av givna riktlinjer eller olagliga handlingar.

Flera externa parter bidrar ofta till att organisationen uppnår sina mål. Externrevisorer, som framför en oberoende och objekt ståndpunkt, bidrar direkt genom granskningen av årsredovisningen och indirekt genom att lämna information som är till nytta för företagsledningen och styrelsen vid fullgörandet av deras uppgifter. Andra intressenter som ger användbar information för etablera en intern styrning och kontroll är lagstiftare, myndigheter, kunder och andra gör transaktioner med företaget, finansanalytiker, fondförvaltare och nyhetsmedia. Externa parter har emellertid inte ansvar för eller är en del av företagets interna styr- och kontrollsystem.

Hur är denna rapport upplagd?

Denna rapport består av fyra delar. Den första delen utgörs av denna *sammanfattning för ledningen (Executive Summary)*, en översikt på hög nivå av ramverket för intern styrning och kontroll riktat till verkställande direktören och de högre cheferna, styrelseledamöter, lagstiftare och myndigheter.

Den andra delen, *Ramverket (the Framework)*, definierar intern styrning och kontroll, beskriver dess komponenter och anger kriterier som företagsledningar, styrelser och andra kan använda för att bedöma deras styr- och kontrollsystem. *Sammanfattningen för ledningen* är inkluderad i denna del.

Den tredje delen, *Rapportering till externa parter (Reporting to External parties)*, är ett tilläggsdokument som ger råd avseende utarbetande av offentligt utgivna finansiella lägesrapporter till de företag som rapporterar eller överväger att rapportera om intern styrning och kontroll offentligt.

Den fjärde delen, *Verktyg för utvärdering (Evaluation Tools)*, ger material som kan vara användbart vid genomförandet av en utvärdering av ett internt styr- och kontrollsystem.

Vad bör man göra?

Vilka åtgärder som man kan tänkas vidta till följd av denna rapport, beror på de inblandade parternas ställning och roller:

Företagets högre ledning

De flesta högre chefer som har bidragit till denna studie anser att de i stort sett har ”kontroll” över sina organisationer. Många sade dock att det finns områden inom deras företag – en division, en avdelning eller en kontrollkomponent som skär genom hela verksamheten – där kontrollerna är i ett tidigt utvecklingskede eller i övrigt behöver förstärkas. De gillar inte överraskningar. Denna studie föreslår att den verkställande direktören tar initiativ till en självutvärdering av styr- och kontrollsystemet. Genom att använda detta ramverk kan den verkställande direktören tillsammans med nyckelpersoner som leder operativa och finansiella funktioner rikta uppmärksamheten mot rätt område. Ett angreppssätt på frågan är att den verkställande direktören samlar affärsenheternas chefer och medarbetare i nyckelfunktioner för att diskutera en inledande bedömning av styrningen och kontrollen. Direktiv ges då för att dessa personer ska diskutera denna rapports begrepp med deras underordnade chefer och utöva tillsyn över den första bedömningsprocessen inom deras ansvarsområden och återrapportera resultaten från denna process. Ett annat angreppssätt kan inkludera en

granskning av hela företagens och affärsområdenas riktlinjer och internrevisionens revisionsplan. Oavsett vilket sätt ledningen väljer bör en inledande självutvärdering ge underlag för att bestämma om det behövs en bredare och djupare utvärdering och hur den ska genomföras. Den inledande utvärderingen bör också säkerställa att löpande övervakningsprocesser har etablerats. Den tid som åtgår för att utvärdera den interna styrningen och kontrollen utgör en investering, dock med en hög avkastning.

Styrelseledamöter

Styrelseledamöterna bör diskutera tillståndet för företagets interna styr- och kontrollsystem med företagsledningen och utöva tillsyn när så behövs. De bör inhämta uppgifter från intern- och externrevisorerna.

Övriga personal

Chefer och annan personal bör överväga hur deras styrnings- och kontrollansvar utövas i ljuset av detta ramverk och diskutera idéer med överordnade chefer hur den interna styrningen och kontroller kan förstärkas. Internrevisorer bör överväga bredden på deras inriktning mot det interna styr- och kontrollsystemet och eventuellt jämföra sitt utvärderingsmaterial med verktygen för utvärdering.

Lagstiftare och myndigheter

Regeringsmedlemmar och deras tjänstemän som skriver eller ser till att lagar efterlevs inser att det kan uppstå missförstånd och olika förväntningar i praktiska taget alla frågor de tar upp. Förväntningarna på intern styrning och kontroll varierar avsevärt i två avseenden. För det första varierar de när det gäller vad styr- och kontrollsystem kan åstadkomma. Som påpekats ovan tror vissa iakttagare att interna styr- och kontrollsystem förhindrar, eller borde, förhindra ekonomiska förluster, eller, åtminstone, att företag går omkull. För det andra, även om man är överens om vad interna styr- och kontrollsystem kan och inte kan göra och om giltigheten i begreppet "rimlig säkerhet" kan man ha skilda åsikter om vad begreppet innebär och hur det ska tillämpas. Företagsledare har uttryckt oro över hur myndigheter kommer att tolka offentliga utgivna rapporter som uppgivit "rimlig säkerhet" i efterhand och det efteråt uppges att ett misstag i kontrollen har inträffat. Innan lagstiftning och myndigheter agerar i frågor som rör ledningens rapportering om intern styrning och kontroll bör det finnas en gemensam uppfattning om ett gemensamt ramverk för intern styrning och kontroll. Detta ramverk bör kunna bidra till att uppnå en sådan gemensam uppfattning.

Professionella organisationer

Regelskapande och andra professionella organisationer som erbjuder vägledning avseende ekonomisk styrning, revision och närliggande ämnen bör se över sina standarder och vägledningar i ljuset av detta ramverk. Om skillnader i begrepp och terminologi undanröjs kommer samtliga parter att gynnas.

Utbildningsinstitutioner

Detta ramverk borde bli föremål för akademisk forskning och analys för att se var man kan göra framtida förbättringar. Förutsatt att denna rapport blir accepterad som en gemensam bas

för förståelse, borde dess begrepp och termer införlivas i läroplaner för universitet och högskolor.

Vi anser att denna rapport erbjuder ett antal fördelar. Med rapporten som grundval för ömsesidig förståelse, kommer samtliga parter att kunna tala samma språk och därmed kommunicera effektivare. Företagsledare kommer att var i stånd att bedöma styr- och kontrollsystem mot en standard och förbättra systemen och styra sina företag mot fastställda mål. Framtida forskning utgå från en etablerad bas. Lagstiftare och myndigheter kommer att kunna få en ökad insikt om intern styrning och kontroll, dess fördelar och begränsningar. Om samtliga parter använder sig av ett gemensamt ramverk för intern styrning och kontroll kommer dessa fördelar att förverkligas.

Purchasing Information

COSO publications are available through the American Institute of Certified Public Accountants (www.aicpa.org) . For further information about COSO products or to order, contact AICPA at 888-777-7077 or visit the [CPA2BIZ web site](#).

Internal Control – Integrated Framework, 2 Vols. Click to Purchase Internal Control Issues in Derivatives Usage – An Information Tool, [Product number 990010](#)

Copyright © 1985-2004 The Committee of Sponsoring Organizations of the Treadway Commission. All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of the Committee of Sponsoring Organizations of the Treadway Commission is strictly prohibited. All trademarks used or referred to in this Web site are the property of their respective owners.

Enterprise Risk Management – Integrated Framework

Executive Summary

September 2004

Svensk översättning bearbetad av Torbjörn Wikland efter råöversättning E&Y för auktorisering av COSO till Internrevisorernas Förening – IIA Sweden

2006-11-07

Företagsövergripande riskhantering –

Integrerat ramverk

Sammanfattning för ledningen

September 2004

Copyright © 2004 by the Committee of Sponsoring Organizations of the Treadway Commission.

All rights reserved. For information about reprint permission and licensing please call (201) 938-3245. A permission request form for emailing requests is available at www.aicpa.org/copyright.htm. Otherwise, requests should be submitted in writing and mailed to Permissions Editor, AICPA, Harborside Financial Center, Plaza Three, Jersey City, NJ 07311-3881.

Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Oversight

Representative

COSO Chair

American Accounting Association

American Institute of Certified Public Accountants

Financial Executives International

Institute of Management Accountants

The Institute of Internal Auditors

John J. Flaherty

Larry E. Rittenberg

Alan W. Anderson

John P. Jessup

Nicholas S. Cyprus

Frank C. Minter

Dennis L. Neider

William G. Bishop, III

David A. Richards

Project Advisory Council to COSO

Guidance

Toni Maki, Chair

Partner Moss Adams LLP

Managing Director

Protivity Inc.

Mark S. Beasley

Professor

North Carolina State

University

Andrew J. Jackson

Senior Vice President of

Enterprise Risk

Assurance Services

American Express

Company

John P. Jessup

Vice President and

Treasurer E.I. duPont de

Nemours and Company

Jerry W. DeFoor

Vice President and

Controller Protective Life

Corporation

Steven E. Jameson

Executive Vice President,

Chief Internal Audit &

Risk Officer Community

Trust Bancorp, Inc.

Tony M. Knapp

Senior Vice President and

Controller Motorola, Inc.

James W. Deloach

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 integrerat ramverk (Internal Control – Integrated Framework)*, för att stödja företag och andra organisatoriska enheter i värderingen och förbättrandet av deras interna styr- och kontrollsystem. Detta ramverk har sedan dess införlivats som riktlinjer, regler och föreskrifter i och används 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 och 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 anlätade 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 dess kölvatten 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 integrerat 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 skall ha interna styr- och kontrollsystem vars effektivitet företagsledningen har intygat och en oberoende revisor bekräftat. *Intern styrning och kontroll – ett integrerat 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 integrerat 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 integrerat 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 använder resurserna effektivt och produktivt för att uppnå företagets mål. Företagsövergripande riskhantering innefattar att:

- *koppla samman riskaptit och strategi* – ledningen skall ta hänsyn till organisationens riskaptit när strategiska alternativ skall utvärderas och när mål skall fastställas och mekanismer utvecklas för att hantera berörda risker
- *fatta bättre beslut om riskåtgärder* – Företagsövergripande riskhantering skall ge 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 bli följden.
- *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 sammansatt risker.
- *ta tillvara gynnsamma möjligheter* – Genom att gå igenom hela skalan av 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 hjälper ledningen att nå organisationens verksamhets- och vinstmål och undvika resursförluster. Företagsövergripande riskhantering är ett stöd för effektiv rapportering och 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 möjligheter¹

Händelser kan ha negativ eller positiv inverkan eller bådadera. Händelser med en 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. Med sådana möjligheter förstås att en händelse inträffar 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

¹ Riskbegreppet i COSO: s rapport är främst kopplat till händelser med negativ inverkan. I andra riskrelaterade dokument innefattar riskbegreppet händelser med såväl negativ som positiv inverkan. *Översättarens anm.*

- genomförs av människor på varje nivå i organisationen
- 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 utformad för att nå mål i en eller flera åtskilda men överlappande kategorier

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 organisationen 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 riskhanteringskomponenter

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 och 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 kan påverka 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.

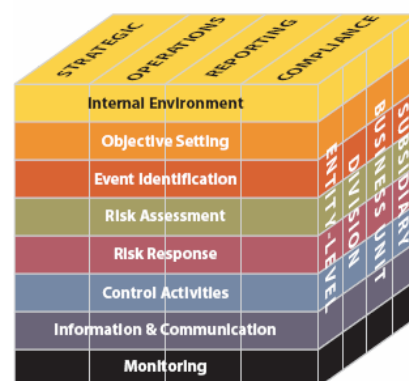
- *Riskåtgärder* – Ledningen väljer vilka åtgärder som ska vidtas – dvs. undvika, acceptera, reducera eller dela risken – och anpassar åtgärderna så att de stämmer överens med organisationens risktolerans och riskaptit.
- *Kontrollaktiviteter* – Riktlinjer och rutiner fastställs och genomförs för att säkerställa att riskåtgärderna förverkligas 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 förmedlas 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 riktigt 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 påverkas av 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 riskkapit.

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 följs.

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 beslutsfrågor, när beslut om riskåtgärder och införande av kontroller måste ta hänsyn till avvägningen av kostnaderna mot de fördelar de medför, haverier kan inträffa på grund av mänskliga brister såsom enkla fel och misstag, kontroller kan kringgåas genom bedrägligt förfarande av två eller flera personer och ledningen har möjlighet att köra över beslut i den företagsövergripande riskhanteringen. 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 mer robusta begrepp och verktyg för ledningen. Intern styrning och kontroll definieras och beskrivs i "*Intern styrning och kontroll – ett integrerat 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 integrerat 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, ekonomin, internrevisor och andra har vanligtvis viktiga stödjande uppgifter. Andra anställda inom organisationen är ansvariga för att riskhanteringen utförs i enlighet med upprättade direktiv och protokoll. Styrelse bidrar med en viktig övervakande roll i den företagsövergripande riskhanteringen och är medveten om och godkänner organisationens riskbenägenhet. Många 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 någon 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 parter och intressenters befattning och roll:

- *Styrelse* – Styrelsen bör diskutera 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 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 tänkbare 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 vara i stånd att bedöma sitt företags övergripande riskhanteringsprocess mot en standard och förbättra processen och styra deras företag mot fastställda mål. Framtida forskning kan utgå från en redan 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.