Internrevisorerna
The Institute of Internal Auditors | Sweden

COSO internal control - executive summary 2013

Intern styrning och kontroll

Av COSO auktoriserad svensk översättning

Internrevisorerna
The Institute of Internal Auditors | *Sweden*

Översättning av

Executive Summary

i uppdaterade COSO 2013

Detta projekt bemyndigades av COSO, som har till uppgift att ge idémässig vägledning genom framställningen av allomfattande ramverk och råd om intern styrning och kontroll, företagsövergripande riskhantering och begränsning av bedrägerier; allt utvecklat för att förbättra organisationers prestationsförmåga och uppsikt och reducera omfattningen av dessa organisationers bedrägerier. COSO är ett initiativ inom den privata sektorn och sponsras och finansieras gemensamt av:

- *American Accounting Association (AAA)*
- *American Institute of Certified Public Accountants (AICPA)*
- *Financial Executives International (FEI)*
- *Institute of Management Accountants (IMA)*
- *The Institute of Internal Auditors (IIA)*

Committee of Sponsoring Organizations of the TreadwayCommission

Board Members

David L. Landsittel
COSO Chair
Mark S. Beasley, Douglas F. Prawitt
American Accounting Association
Richard F. Chambers
The Institute of Internal Auditors
Charles E. Landes
American Institute of Certified Public Accountants
Marie N. Hollein
Financial Executives International
Sandra Richtermeyer, Jeffrey C. Thomson
Institute of Management Accountants

PwC—Author

Principal Contributors

Miles E.A. Everson
Engagement Leader New York, USA
Stephen E.
Soske Project Lead Partner Boston, USA
Frank J. Martens
Project Lead Director Vancouver, Canada
Cara M. Beston
Partner San Jose, USA
Charles E. Harris
Partner Florham Park, USA
J. Aaron Garcia
Director San Diego, USA
Catherine I. Jourdan
Director Paris, France
Jay A. Posklensky
Director Florham Park, USA
Sallie Jo Perraglia
Manager New York, USA

Advisory Council

Sponsoring Organizations Representatives

Audrey A. Gramling
Bellarmine University Fr.
Raymond J. Treece
Endowed Chair
Steven E. Jameson
Community Trust Bank Executive Vice President and Chief Internal Audit & Risk Officer
J. Stephen McNally
Campbell Soup Company
Finance Director/Controller
Ray Purcell
Pfizer Director of Financial Controls
William D. Schneider Sr
AT&T Director of Accounting

Members at Large

Jennifer Burns
Deloitte Partner
James DeLoach
Protiviti Managing Director
Trent Gazzaway Grant Thornton Partner
Cees Klumper
The Global Fund to Fight AIDS, Tuberculosis and Malaria Chief Risk Officer
Thomas Montminy
PwC Partner
Alan Paulus
Ernst & Young LLP Partner
Thomas Ray
Baruch College
Dr. Larry E. Rittenberg
University of Wisconsin Emeritus Professor of Accounting Chair Emeritus COSO
Sharon Todd
KPMG Partner
Kenneth L. Vander
Wal ISACA International President 2011–2012

Regulatory Observers and Other Observers

James Dalkin
Government Accountability Office Director in the Financial Management and Assurance Team
Harrison E. Greene Jr.
Federal Deposit Insurance Corporation Assistant Chief Accountant
Christian Peo
Securities and Exchange Commission Professional Accounting Fellow (Through June 2012)
Amy Steele
Securities and Exchange Commission Associate Chief Accountant (Commencing July 2012)
Vincent Tophoff
International Federation of Accountants Senior Technical Manager
Keith Wilson
Public Company Accounting Oversight Board Deputy Chief Auditor

Översättarens inledning

Det sägs ofta att svenskar inte behöver översättningar från engelska till svenska. Erfarenheten säger tyvärr något annat. Professionellt behövs ofta enhetliga översättningar av engelska begrepp. Ord som ser lika ut på svenska och engelska har helt eller delvis olika betydelser. I både offentlig förvaltning och i många företag och organisationer behövs precisa översättningar för att inte skapa oklarheter. Ett talande exempel på detta är översättningen av ”Internal Control” som t.o.m. i aktiebolagslagen felaktigt översatts till internkontroll i stället för den mer korrekta översättningen intern styrning och kontroll. Utan eftertanke kan ”control” uppfattas som bara kontroll! För att undvika sådana brister är det bra att åtminstone vissa engelska grundtexter är översatta till svenska och auktoriserade. Det är bakgrunden till att Internrevisorerna i Sverige (IIA Sweden) låtit översätta delar av COSO: s grunddokument till svenska och se till att de också blivit auktoriserade av COSO. Detta är översättningen av sammanfattningen av COSO:s ramverk (Executive Summary)[1].

COSO:s dokument, ramverket om intern styrning och kontroll uppdaterades och gavs ut i maj 2013. Det ursprungliga ramverket gavs ut 1992 och har nu på vissa punkter förändrats som delvis framgår av nedanstående översatta dokument. I huvudsak är dock ramverket detsamma som tidigare. Uppdateringen handlar i huvudsak om förtydliganden. En mer detaljerad genomgång av förändringarna finns i en bilaga till huvuddokumentet men som inte översatts här. Det finns tre aspekter på COSO: s uppdatering och utgivning som bör uppmärksammas:

Huvuddokumentet med uppdateringen 2013 är mer lättillgängligt och lättläst jämfört med det ursprungliga dokumentet från 1992. Det kan därför rekommenderas för läsning. Som framgår på annan plats kan det beställas från USA i både pappersform och digitalt[2]. Översättningen nedan gäller således bara sammanfattningen och kan tjäna både som självständig beskrivning av ramverket och en introduktion till huvuddokumentet.

Ett viktigt särdrag i COSO: s ramverk är dess inriktning på att ge en helhetsbedömning av en organisations interna styrning och kontroll. I samband med uppdateringen av ramverket har COSO givit ut ett mer utförligt stöd för att göra en sådan helhetsbedömning, Illustrative Tools for Assessing Effectiveness of a System of Internal Control. Det kan beställas i samband med beställningen av huvuddokumentet eller separat via COSO: s hemsida.

Många företag som använder och stödjer sig på COSO: s ramverk har samtidigt särskilt fokus på den finansiella rapporteringen. COSO har nu givit ut ett särskilt dokument som illustrerar hur frågor om den finansiella rapporteringen kan behandlas och ger samtidigt många exempel på hur frågor om intern styrning och kontroll kan hanteras. Dokumentet heter Internal Control over external Financial Reporting: A Compendium of Approaches and Examples. Det ingår också vid en beställning av huvuddokumentet från COSO.

Torbjörn Wikland
Ansvarig inom Internrevisorerna
för översättningen

[1] Detta är den femte översättningen av COSO-dokument som internrevisorerna tagit initiativ till – se vidare deras hemsida www.theiia.se.
[2] Se vidare COSO: s hemsida www.coso.org.

Förord

1992 lät the Committee of the Sponsoring Organizations of the Treadway Commission publicera sitt *Internal Control – Integrated Framework* (det ursprungliga ramverket). Det ursprungliga ramverket har vunnit brett erkännande och används i stor utsträckning världen runt. Det är erkänt som ett ledande ramverk för att utforma, implementera och förvalta intern styrning och kontroll och bedöma den interna styrningen och kontrollens effektivitet.

Under de tjugo åren sedan det ursprungliga ramverket började gälla har företagsvärlden och den operativa miljön förändrats dramatiskt, blivit alltmer komplex, teknologiskt präglad och global. Samtidigt har intressenter blivit mer engagerade i att få till stånd ökad transparens och ansvarstagande för integriteten i system för intern styrning och kontroll, som stödjer organisationers verksamhetsbeslut och styrning.

COSO har nöjet att presentera det uppdaterade *Internal Control – Integrated Framework (Ramverket)*. COSO tror att *Ramverket* möjliggör för organisationer att verkningsfullt och effektivt utveckla och upprätthålla system för intern styrning och kontroll som kan öka sannolikheten för att organisationens mål uppnås och anpassas till förändringar i verksamheten och den operativa miljön.

Den erfarne läsaren kommer att finna mycket som är välkänt i *Ramverket*, som bygger på vad som visat sig användbart i den ursprungliga versionen. Den håller fast vid den grundläggande definitionen av intern styrning och kontroll och de fem komponenterna i intern styrning och kontroll. Kravet att ta hänsyn till de fem komponenterna för att bedöma effektiviteten i ett system för intern styrning och kontroll är i grunden oförändrat. *Ramverket* fortsätter också att understryka vikten av ledningens bedömning när det gäller att utforma, implementera och förvalta intern styrning och kontroll och att värdera effektiviteten i ett system för intern styrning och kontroll.

Samtidigt innehåller *Ramverket* förbättringar och förtydliganden som är avsedda att underlätta användningen och tillämpningen. En av de mer betydelsefulla förbättringarna är formaliseringen av grundläggande begrepp som introducerades i det ursprungliga ramverket. I det uppdaterade *Ramverket* är dessa begrepp nu principer, som är knutna till de fem komponenterna och som erbjuder klargöranden för användaren att utforma och implementera system för intern styrning och kontroll och att förstå kraven för effektiv styrning och kontroll.

Ramverket har förbättrats genom att utvidga målkategorin finansiell rapportering till att innefatta andra viktiga former för rapportering såsom icke-finansiell och intern rapportering. Ramverket återspeglar också överväganden utifrån många förändringar i företagsvärlden och den operativa miljön under de senaste årtiondena som innefattar:

- *Förväntningar om tillsyn över styrningen*
- *Globaliseringen av marknader och verksamheter*
- *Verksamheters förändringar och större komplexitet*
- *Krav på och komplexiteten i lagar, regler, regleringar och standarder*
- *Förväntningar om kompetens och ansvarsutkrävande*
- *Användningen av, och tilltron till, framväxande tekniker*
- *Förväntningar som rör att förhindra och upptäcka bedrägerier*

Denna sammanfattning tillhandahåller en överblick på hög nivå avsedd för styrelser,

verkställande ledningar och andra högre befattningshavare. Det publicerade *Ramverket med bilagor* redogör för Ramverket, genom att definiera intern styrning och kontroll, beskriva förutsättningarna för effektiv intern styrning och kontroll inklusive komponenter och relevanta principer och ge vägledning till alla nivåers ledningar för att användas i utformningen, implementeringen och förvaltningen av intern styrning och kontroll och i värderingen av dess effektivitet. Bilagorna inom *Ramverket med bilagor* tillhandahåller ytterligare referensmaterial, men är inte tänkt som en del av *Ramverket*. T*he Illustrative Tools for Assessing Effectiveness of a System of Internal Control* tillhandahåller mallar och scenarier som kan vara användbara i tillämpningen av *Ramverket*.

Utöver *Ramverket* har *Internal Control over External Financial Reporting: A compendium of Approaches and Examples* samtidigt publicerats för att erbjuda tillvägagångssätt och exempel som illustrerar hur komponenterna och principerna beskrivna i *Ramverket* kan tillämpas för att förbereda externa finansiella uttalanden.

COSO har tidigare givit ut *Guidance on Monitoring Internal Control Systems*[3] för att hjälpa organisationer att förstå och tillämpa övervakande aktiviteter inom ett system för intern styrning och kontroll. Även om den vägledningen gjordes i ordning som stöd för att tillämpa det ursprungliga *Ramverket,* är COSO övertygad om att den vägledningen har liknande tillämplighet på det uppdaterade *Ramverket*.

COSO kan framöver komma att ge ut andra dokument för att erbjuda stöd i tillämpningen av *Ramverket*. Emellertid kommer varken the *Internal Control over External Financial Reporting: A Compendium of Approaches and Examples, Guidance on Monitoring Internal Control Systems* eller någon annan tidigare eller framtida vägledning utgöra en ersättning för *Ramverket*.

Bland andra publikationer utgivna av COSO finns *Enterprise Risk Management – Integrated Framework*[4] *(Ramverket för ERM). Ramverket för ERM* och *Ramverket* är avsedda att vara komplementära och den ena tränger inte undan den andra. Även om dessa ramverk är olika och erbjuder olika fokus så överlappar de varandra. *Ramverket för ERM* innefattar intern styrning och kontroll med stora delar av texten från det ursprungliga Internal Control – Integrated Framework återgiven. Följaktligen förblir *Ramverket för ERM* levande och passande för att utforma , implementera, vidmakthålla och värdera företagsövergripande riskhantering.

Slutligen vill COSO tacka PwC och det rådgivande utskottet för deras bidrag i utvecklandet av *Ramverket* och anknutna dokument. Deras allsidiga hänsynstagande till bidrag från många intressenter och deras insikt medverkade till att se till att kärnan i det ursprungliga *Ramverket* har blivit kvar, förtydligad och förstärkt.

David L. Landsittel
COSO: s ordförande

[3] Introduktionen finns som auktoriserad översättning till svenska: ”Vägledning för övervakning av system för intern styrning och kontroll” Internrevisorerna 2009.
[4] Sammanfattningen finns som auktoriserad översättning till svenska: ”Företagsövergripande riskhantering – sammahållet ramverk”. Internrevisorerna 2007.

Sammanfattning

Intern styrning och kontroll hjälper organisationer att uppnå viktiga mål och bibehålla och förbättra prestationsförmågan. COSO: s Internal Control – Integrated Framework (Ramverket) möjliggör för organisationer att verkningsfullt och effektivt utveckla system för intern styrning och kontroll som anpassas till en förändrad företagsamhet och operativ miljö, reducera risker till accepterade nivåer och stödjer sunt beslutsfattande och styrning av organisationen.

Att utforma och implementera ett effektivt system för intern styrning och kontroll kan vara en utmaning: att styra ett sådant system effektivt och produktivt varje dag kan göra var och en modlös. Nya och snabbt förändliga verksamhetsmodeller, ökad användning och beroende av IT, ökande regleringskrav och granskning, globalisering och andra utmaningar kräver av varje system för intern styrning och kontroll att det är lättrörligt och anpassligt till förändringar i affärsmässiga, operativa och reglerande miljöer.

Ett effektivt system för intern styrning och kontroll kräver mer än noggrann efterlevnad av policies och rutiner: det kräver att omdöme används. Ledningen och styrelsen[5] använder omdömet för att avgöra vad som är tillräcklig kontroll. Ledningen och annan personal använder omdömet varje dag för att välja ut, utveckla och genomföra kontroller över hela organisationen. Ledningen och internrevisionen, liksom övrig personal, använder omdömet när de övervakar och värderar effektiviteten i systemet för intern styrning och kontroll.

Ramverket hjälper ledningen, styrelsen, externa intressenter och andra som interagerar med organisationen i deras respektive uppgifter som rör intern styrning och kontroll utan att vara alltför normativ. Den gör det genom att erbjuda förståelse för vad som utgör ett system för intern styrning och kontroll och insikter i när intern styrning och kontroll genomförs effektivt.

För ledningen och styrelsen erbjuder *Ramverket*:

- *En möjlighet att tillämpa intern styrning och kontroll på varje organisation oavsett bransch eller legal struktur och på nivåerna hela organisationen, verksamhetsenhet och funktion.*
- *Ett principbaserat tillvägagångssätt som erbjuder flexibilitet och tillåter omdöme vid utformningen, implementeringen och genomförandet av intern styrning och kontroll – principer som kan tillämpas på hela organisationen, verksamhets- och funktionsnivåer.*
- *Krav för ett effektivt system för intern styrning och kontroll genom att beakta hur komponenter och principer finns på plats och fungerar och hur komponenterna arbetar tillsammans.*
- *En möjlighet att identifiera och analysera risker och att utveckla och genomföra lämpliga riskåtgärder inom accepterade nivåer och med ett större fokus på åtgärder mot bedrägerier.*
- *En möjlighet att utvidga tillämpningen av intern styrning och kontroll utanför den finansiella rapporteringen till andra former av rapporterings-, verksamhets- och regelstyrda mål.*
- *En möjlighet att eliminera ineffektiva, överflödiga eller oproduktiva kontroller som ytterst lite bidrar med att reducera risker för att uppnå organisationens mål.*

[5] Ramverket använder termen styrelse, vilket omfattar det styrande organet inklusive styrelsen, förvaltande organ, partner, ägare och övervakande organ.

För organisationens externa intressenter och andra som interagerar med organisationen erbjuder tillämpningen av Ramverket:

- *Större tilltro till styrelsens uppsikt över system för intern styrning och kontroll*
- *Större tilltro till att organisationens mål uppnås*
- *Större tilltro till organisationens förmåga att identifiera, analysera och svara på risker och förändringar i de affärs- och verksamhetsmässiga miljöerna*
- *Större förståelse för kraven på ett effektivt system för intern styrning och kontroll*
- *Större förståelse för att användningen av omdöme gör det möjligt för ledningen att eliminera ineffektiva, överflödiga och ickeproduktiva kontroller.*

Intern styrning och kontroll är inte seriell process utan en dynamisk och integrerad process. Ramverket är tillämpbart på alla organisationer; stora medelstora, små, vinstdrivna och icke vinstdrivna och offentliga organ. Varje organisation kan emellertid välja att implementera intern styrning och kontroll olika. Som exempel kan mindre organisationers interna styrning och kontroll vara mindre formell och strukturerad men ändå utgöra en effektiv intern styrning och kontroll.

Resten av denna sammanfattning innehåller en översikt av intern styrning och kontroll inklusive en definition, målkategorier, beskrivning av de nödvändiga komponenterna och tillhörande principer och kraven på ett effektivt system för intern styrning och kontroll. Den innehåller också en diskussion kring begränsningar – skälen för att inget system för intern styrning och kontroll kan vara perfekt. Slutligen erbjuder den synpunkter på hur olika aktörer kan använda *Ramverket*.

Definition av intern styrning och kontroll

Intern styrning och kontroll definieras på följande sätt:

Intern styrning och kontroll är en process utförd av en organisations styrelse, ledning och annan personal, utformad för att ge en rimlig försäkran om uppnåendet av mål som rör verksamheten, rapporteringen och följdsamhet gentemot lagar och regler.

Denna definition återspeglar några grundläggande begrepp. Intern styrning och kontroll är:

- *Inriktad på uppnåendet av mål inom en eller flera kategorier – verksamhet, rapportering och följdsamhet gentemot lagar och regler*
- *En process som består av pågående uppgifter och aktiviteter – ett medel för ett mål, inte ett mål i sig*
- *Utförd av människor – inte endast något om policy och rutinbeskrivningar, system och former, utan om människor och de handlingar de vidtar på varje nivå i en organisation för att påverka intern styrning och kontroll*
- *En möjlighet att ge en rimlig försäkran – men inte en absolut försäkran till en organisations högsta ledning och styrelse*
- *Anpassningsbar till organisationsstrukturen – flexibel i användningen på hela organisationen eller ett särskilt dotterbolag, en avdelning, verksamhetsenhet eller verksamhetsprocess*

Denna definition är medvetet bred. Den fångar viktiga begrepp som är grundläggande för hur organisationer utformar, implementerar och genomför intern styrning och kontroll och erbjuder en utgångspunkt för tillämpning bland organisationer som verkar i olika organisatoriska strukturer, branscher och geografiska regioner.

Målkategorierna

Ramverket tillhandahåller tre målkategorier som tillåter organisationer att fokusera på olika aspekter av intern styrning och kontroll:

- *Verksamhetsmål – Dessa gäller effektivitet och produktivitet i organisationens verksamhet, inklusive verksamhetsmässiga och finansiella resultatmål och säkerställande av att tillgångar inte förloras.*
- *Rapporteringsmål – Dessa gäller intern och extern finansiell och icke-finansiell rapportering och kan innefatta tillförlitlighet, att komma vid rätt tidpunkt, transparens och andra villkor som satts upp av regleringsorgan, erkända standardsättande organ eller i organisationens policies.*
- *Mål för följdsamhet gentemot lagar och regler – Dessa hänför sig till att följa lagar och regleringar som organisationen måste följa.*

Komponenter i intern styrning och kontroll

Intern styrning och kontroll består av fem integrerade komponenter.

Styr- och kontrollmiljön

Styr- och kontrollmiljön[6] är den uppsättning av standarder, processer och strukturer som är grunden för genomförandet av intern styrning och kontroll i hela organisationen. Styrelsen och den verkställande ledningen anger ”tonen” i företaget vad gäller betydelsen av intern styrning och kontroll inklusive den förväntade uppförandenormen. Ledningen förstärker förväntningarna på de olika nivåerna i organisationen. Styr- och kontrollmiljön inbegriper organisationens redbarhet och etiska normer; parametrarna som möjliggör för styrelsen att fullfölja sitt övergripande styrningsansvar; den organisatoriska strukturen och tilldelningen av befogenheter och ansvar; processen för att attrahera, utveckla och behålla kompetenta individer; och entydigheten i resultatmåtten, incitamenten och belöningarna för att kunna få till stånd ett ansvarstagande för resultat och prestationer. Den så genomförda styr- och kontrollmiljön har en genomgripande effekt på hela systemet för intern styrning och kontroll.

Riskvärdering

Varje organisation möter en mångfald av risker från externa och interna källor. Risk de-

[6] Denna komponent har tidigare översatts till ”kontrollmiljön”. Eftersom ”control” i övrigt översatts till ”styrning och kontroll” har den översatta komponenten konsekvensändrats till ”Styr- och kontrollmiljön”.

finieras som en möjlighet att en händelse inträffar som motverkar uppnåendet av mål. Riskvärderingen innefattar en dynamisk och iterativ process för att identifiera och värdera risker knutna till uppnåendet av mål. Risker i hela organisationen för att dessa mål inte uppnås tar hänsyn och relateras till etablerade risktoleranser. På så vis utgör riskvärderingen grunden för att bestämma hur risken ska tas om hand.

En förutsättning för riskvärderingen är att mål upprättats, knutna till olika nivåer i organisationen. Ledningen specificerar målen inom kategorierna avseende verksamheten, rapporteringen och följdsamheten mot lagar och regler med tillräcklig tydlighet för att kunna identifiera och analysera risker till dessa mål. Ledningen tar också hänsyn till hur målen passar in i organisationen. Riskvärderingen kräver också att ledningen överväger effekter av tänkbara förändringar i den externa miljön och i sin egen verksamhetsmodell som kan leda till att den interna styrningen och kontrollen blir ineffektiv.

Kontrollaktiviteter

Kontrollaktiviteter är handlingar etablerade genom policies och rutiner som ser till att ledningens direktiv genomförs för att reducera risker för att målen inte uppnås. Kontrollaktiviteter utförs på alla nivåer i organisationen och i olika stadier i verksamhetsprocesserna och i IT-miljön. De kan vara förhindrande eller upptäckande till sin natur och kan omfatta en rad manuella och automatiserade aktiviteter såsom attester, godkännanden, verifieringar, avstämningar och återrapporteringar av verksamhetsresultat. Tvåhandsprincipen är typiskt inbyggd i urvalet och utvecklandet av kontrollaktiviteter. Där tvåhandsprincipen inte är möjlig tar ledningen fram och utvecklar alternativa kontrollaktiviteter.

Information och Kommunikation

Information är nödvändigt för att organisationen ska kunna genomföra sina ansvarsuppgifter för intern styrning och kontroll för att stödja uppnåendet av dess mål. Ledningen erhåller eller skapar och använder relevant och kvalitetssäkrad information från både interna och externa källor för att se till att de andra komponenterna fungerar. Kommunikation är den kontinuerliga, iterativa processen för att ge, dela och erhålla nödvändig information. Intern kommunikation är sättet genom vilket information sprids genom organisationen och flödar uppåt, neråt och tvärs igenom organisationen. Det gör det möjligt för personalen att få en tydlig signal från högsta ledningen att ansvar för styrning och kontroll måste tas på allvar. Extern kommunikation är tvåfaldig: den möjliggör ingående kommunikation av relevant extern information, och den ger information till externa parter som svar på krav och förväntningar.

Övervakande aktiviteter[7]

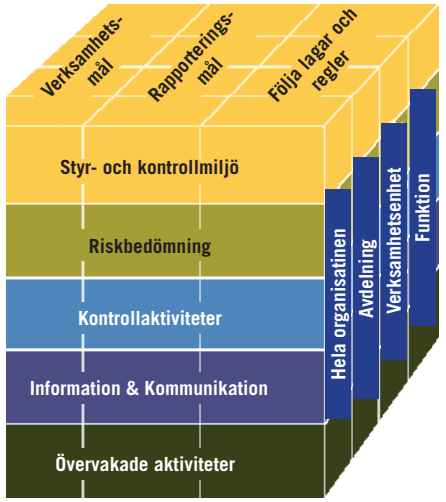
Löpande utvärderingar, separata utvärderingar eller någon kombination av de två används för att försäkra sig om att var och en av de fem komponenterna i intern styrning och kontroll finns och fungerar inklusive kontroller för att se verkan av principerna inom varje komponent. Löpande utvärderingar inbyggda i verksamhetsprocesserna på olika nivåer i organisationen ska ge information i rätt tid. Separata utvärderingar, periodiskt genomförda, kommer att variera i omfattning och frekvens beroende på värderingen av risker, effektiviteten i löpande utvärderingar och överväganden från ledningen. Utfallet utvärderas mot kriterier etablerade av reglerande organ, erkända standardsättande organ eller ledningen och styrelsen och brister förmedlas till ledningen och styrelsen när så är lämpligt.

[7] Den kallades i den tidigare versionen av ramverket för ”Monitoring” och översattes då till övervakning.

Samband mellan mål och komponenter

Ett direkt samband finns mellan *målen*, dvs. vad en organisation strävar mot att uppnå, *komponenterna*, som representerar vad som krävs för att uppnå målen, och den *organisatoriska strukturen* (operativa enheter, legala indelningar och annat). Sambandet kan åskådliggöras i form av en kub.

- *De tre målkategorierna – verksamhet, rapportering och lagar och regler – representeras av kolumner.*
- *De fem komponenterna representeras av rader.*
- *Organisationens struktur representeras av den tredje dimensionen.*



Samband mellan mål och komponenter

Ramverket lägger fram sjutton principer som representerar de grundläggande begreppen knutna till varje komponent. Eftersom dessa principer är framtagna direkt ur komponenterna kan en organisation nå en effektiv intern styrning och kontroll genom att tillämpa alla principerna. Alla principerna är tillämpliga på mål som rör verksamheten, rapporteringen samt följdsamhet mot lagar och regler. Principerna som stödjer komponenterna i den interna styrningen och kontrollen är förtecknade nedan.

Styr- och kontrollmiljön

1. *Organisationen[8] visar att den förbundit sig till redbarhet och etiska värden.*
2. *Styrelsen visar självständighet gentemot ledningen och övervakar utvecklingen av och resultaten i den interna styrningen och kontrollen.*
3. *Ledningen etablerar, under styrelsens tillsyn, strukturer, rapporteringslinjer och lämplig ansvars- och befogenhetsfördelning i strävan mot målen.*
4. *Organisationen visar att den förbundit sig till att attrahera, utveckla och behålla kompetenta individer i enlighet med dess mål.*
5. *Organisationen håller individer ansvariga för deras tilldelade befogenheter för intern styrning och kontroll i strävan mot målen.*

Riskvärdering

6. *Organisationen preciserar målen med tillräcklig tydlighet för att kunna identifiera och värdera risker som rör målen.*
7. *Organisationen identifierar risker för att målen inte uppnås i organisationens alla delar och analyserar risker som en*

[8] Utifrån ramverkets definitioner används termen ”organisation” som samlingsbegrepp för styrelsen, ledningen och annan personal såsom de beskrivs i definitionen av intern styrning och kontroll.

grund för att fastställa hur riskerna ska hanteras.

8. *Organisationen tar hänsyn till möjligheterna för bedrägerier när den bedömer riskerna för att målen inte uppnås.*
9. *Organisationen identifierar och värderar förändringar som påtagligt kan påverka systemet för intern styrning och kontroll.*

Kontrollaktiviteter

10. *Organisationen väljer ut och utvecklar kontrollaktiviteter som medför att risker för att inte uppnå mål reduceras till acceptabla nivåer.*
11. *Organisationen väljer ut och utvecklar generella kontroller över informationsteknologin för att stödja uppnåendet av målen.*
12. *Organisationen genomför kontrollaktiviteter genom policies som klargör vad som förväntas och procedurer som ser till att policies genomförs.*

Information och kommunikation

13. *Organisationen tar emot eller skapar och använder relevant kvalitetssäkrad information för att stödja en fungerande intern styrning och kontroll.*
14. *Organisationen kommunicerar information internt, inklusive mål och ansvar för intern styrning och kontroll, som är nödvändigt för att stödja en fungerande intern styrning och kontroll.*
15. *Organisationen kommunicerar med externa parter som rör frågor om hur den interna styrningen och kontrollen fungerar.*

Övervakande aktiviteter

16. *Organisationen väljer ut, utvecklar och genomför löpande och/eller separata utvärderingar för att försäkra sig om att komponenterna i den interna styrningen och kontrollen finns på plats och fungerar.*
17. *Organisationen utvärderar och kommunicerar brister i den interna styrningen och kontrollen i god tid till berörda som har ansvar för att vidta korrigerande åtgärder. De berörda inkluderar högsta ledningen och styrelsen när så är lämpligt.*

Effektiv intern styrning och kontroll

Ramverket slår fast kraven för ett effektivt system för intern styrning och kontroll. Ett effektivt system ger rimlig försäkran huruvida en organisation uppnår sina mål. Ett effektivt system för intern styrning och kontroll reducerar risken till en acceptabel nivå att inte nå organisationens mål som kan relateras till en, två eller tre målkategorierna. Det kräver att:

- *Var och en av de fem komponenterna och berörda principer finns och fungerar. Att de finns gäller fastställandet att komponenterna och berörda principer existerar i utformningen och genomförandet av systemet för intern styrning och kontroll för att uppnå preciserade mål. Att de fungerar gäller fastställandet att komponenterna och berörda principer fortsätter att finnas till i verksamheten och ledningen av systemet för intern styrning och kontroll för att uppnå preciserade mål.*
- *De fem komponenterna verkar tillsammans på ett integrerat sätt. Att verka tillsammans gäller fastställandet av att de fem komponenterna tillsammans reducerar risken till en acceptabel nivå att inte nå ett mål. Komponenterna ska inte övervägas åtskilt; i stället ska de verka tillsammans som ett integrerat system. Komponenterna är beroende av varandra genom en mångfald av relationer och samband dem emellan, särskilt på det sätt som principer interagerar med och över komponenter.*

När en större brist existerar som gäller huruvida en komponent eller berörd princip finns och fungerar eller som gäller om komponenterna verkar tillsammans på ett integrerat sätt, kan inte organisationen dra slutsatsen att den har tillgodosett kraven för ett effektivt system för intern styrning och kontroll.

När ett system för intern styrning och kontroll har fastställts vara effektivt har den högsta ledningen och styrelsen en rimlig försäkran, vad gäller tillämpligheten inom hela organisationen, att organisationen:

- *För till stånd en effektiv och produktiv verksamhet där externa händelser inte sannolikt har någon betydande inverkan på om målen uppnås eller där organisationen rimligt kan förutse karaktären och tiden för externa händelser och reducera effekten till en acceptabel nivå*
- *Förstår i vilken utsträckning verksamheten kan skötas effektivt och produktivt när externa händelser kan ha en betydande inverkan på om målen uppnås eller där organisationen rimligt kan förutse karaktären och tiden för externa händelser och reducera effekten till en acceptabel nivå*
- *Förbereder rapporter i enlighet med berörda regler, regleringar och standarder eller enligt organisationens preciserade rapporteringsmål*
- *Följer berörda lagar, regler, regleringar och externa standarder*

Ramverket kräver omdöme i utformningen, implementeringen och genomförandet av intern styrning och kontroll och i värderingen av dess effektivitet. Användandet av omdöme, inom gränser som etablerats genom lagar, regler, regleringar och standarder, ökar ledningens förmåga att fatta bättre beslut om intern styrning och kontroll men kan inte garantera perfekta resultat.

Begränsningar

Ramverket medger att medan intern styrning och kontroll ger rimlig försäkran om att nå organisationens mål, så finns det begränsningar. Intern styrning och kontroll kan inte förhindra dåligt omdöme eller dåliga beslut eller att externa händelser kan leda till att organisationen misslyckas att uppnå sina verksamhetsmål. Med andra ord, även ett effektivt system för intern styrning och kontroll kan ställas inför ett misslyckande. Begränsningar kan vara resultatet av:

- *Brister i anpassningen av målen som etablerats som en förutsättning för intern styrning och kontroll*

- *En verklighet där mänskligt omdöme i beslutsfattandet är bristfälligt eller partiskt*
- *Sammanbrott som kan inträffa på grund av mänskliga tillkortakommanden sådant som enkla misstag*
- *Att ledningen har möjlighet att "köra över" den interna styrningen och kontrollen*
- *Att ledningen, annan personal och/eller tredje part kan gå förbi kontroller genom hemligt samarbete*
- *Externa händelser utanför organisationens kontroll*

Dessa begränsningar utesluter att styrelsen och ledningen kan få en absolut försäkran om att målen för organisationen kan nås – dvs. intern styrning och kontroll kan ge rimlig men inte absolut försäkran. Oavsett dessa inneboende begränsningar bör ledningen vara medveten om dem när den väljer ut, utvecklar och genomför kontroller som minimerar dessa begränsningar där så är praktiskt möjligt.

Att använda *Intern styrning och kontroll – Sammanhållet ramverk*

Hur denna rapport kan användas beror på vilka roller intresserade parter har:

- **Styrelsen** – *Styrelsen bör med den högsta ledningen diskutera läget i organisationens system för intern styrning och kontroll och ha tillsyn över systemet när så behövs. Högsta ledningen är ansvarig för intern styrning och kontroll och inför styrelsen och hela styrelsen måste etablera sina policies och förväntningar på hur dess medlemmar ska ha tillsyn över organisationens interna styrning och kontroll. Styrelsen måste underrättas om riskerna för att organisationens mål inte uppnås, värderingarna av brister i den interna styrningen och kontrollen, ledningens vidtagna åtgärder för att reducera sådana risker och brister och hur ledningen värderar effektiviteten i organisationens system för intern styrning och kontroll. Hela styrelsen bör utmana ledningen och om nödvändigt ställa tuffa frågor och söka få inspel och stöd från internrevisorer, externrevisorer och andra. Kommittéer under styrelsen kan ofta stödja styrelsen genom att ta itu med några av dessa tillsynsaktiviteter.*
- **Den högsta ledningen** – *Den högsta ledningen bör värdera organisationens system för intern styrning och kontroll i relation till* Ramverket *och fokusera på hur organisationen tillämpar de sjutton principerna till stöd för komponenterna i den interna styrningen och kontrollen. Där ledningen har tillämpat 1992 års upplaga av* Ramverket *bör den först granska den gjorda uppdateringen av den versionen (som framhålls i Appendix F till* Ramverket*) och överväga följderna av dessa uppdateringar vad avser organisationens system för intern styrning och kontroll. Ledningen kan överväga att använda* Illustrative Tools *som del i denna inledande jämförelse och som en löpande utvärdering av den övergripande effektiviteten i organisationens system för intern styrning och kontroll.*
- **Övrig ledning och personal** – *Ledningar och personal i övrigt bör granska förändringarna i denna version och värdera följderna av dessa förändringar vad avser organisationens interna styrning och kontroll. Dessutom bör de överväga hur de utför sina ansvarsuppgifter i ljuset av* Ramverket *och diskutera med högre ansvariga uppslag för att stärka intern styrning och kontroll. Mer precist bör de överväga hur befintliga kontroller påverkar de berörda principerna inom de fem komponenterna för intern styrning och kontroll.*
- **Internrevisorer** – *Internrevisorer bör granska sina internrevisionsplaner och hur de tillämpades i 1992 års upplaga av* Ramverket. *Internrevisorerna bör också granska de gjorda förändringarna i detalj i denna version och överväga möjliga följder av dessa förändringar i granskningsplaner, utvärderingar och varje slag av rapportering om organisationens system för intern styrning och kontroll.*
- **Oberoende revisorer** – *Inom några lagskipningsområden, är oberoende revisorer engagerade i att revidera eller undersöka effektiviteten i en klients interna styrning och kontroll i finansiell rapportering utöver att revidera organisationens finansiella uttalanden. Revisorer kan värdera organisationens system för intern styrning och kontroll i relation till* Ramverket *och fokusera på hur organisationen har valt ut, utvecklat och genomfört kontroller som påverkar principerna inom komponenterna för intern styrning och kontroll. Revisorer kan, på liknande sätt som ledningen, använda* Illustrative Tools *som del i denna utvärdering av den övergripande effektiviteten i organisationens system för intern styrning och kontroll.*
- *Andra professionella organisationer – Andra professionella organisationer som ger råd om verksamhet, rapportering och följdsamhet mot lagar och regler kan granska sina standarder och vägledningar i jämförelse med* Ramverket. *I den mån olikheter i begrepp och termer elimineras gynnar de alla parter.*
- *Utbildare – Under förutsättning att* Ramverket *uppnår bred acceptans bör dess begrepp och termer återfinnas i universitetens studiekurser.*

En kort ordlista med använda nyckelbegrepp på engelska och deras översättning till svenska:

Internal Control	Intern styrning och kontroll
Control Environment	Styr- och kontrollmiljö
Risk Assessment	Riskvärdering eller riksbedömning
Control Acitivities	Kontrollaktiviteter
Monitoring Acitivities	Övervakande aktiviteter
Operations	Verksamhet
Compliance	Följdsamhet gentemot lagar och regler
Entity	Organisation
Integrity	Redbarhet eller integritet
Enterprise Risk Management	Företags- eller organisationsövergripande riskhantering
Internal auditor	Internrevisor
Risk Management	Riskhantering
Risk Response	Riskåtgärd

En mer utförlig ordlista med förklaringar på engelska finns i Appendix A i det engelska huvuddokumentet.

Internrevisorerna
The Institute of Internal Auditors | *Sweden*

INTERNREVISORERNAS FÖRENING
Strandvägen 7 A
SE-114 56 Stockholm, Sweden
e-post: info@internrevisorerna.se
www.internrevisorerna.se

Grafisk produktion och omslagsfoto: Ulf Bengtsson/cbcom