

Vägledning

för övervakning av system för intern styrning och kontroll

INTRODUKTION JANUARI 2009

**Internal Control – Integrated Framework
Guidance on Monitoring Internal Control Systems**

Introduction

January 2009

**Vägledning för övervakning av system
för intern styrning och kontroll**

Introduktion

Januari 2009

ÖVERSÄTTNING: Torbjörn Wikland. Översättningen är granskad av Britta Isén-Nordbeck och godkänd av Internrevisorerna och COSO.

LAYOUT: Leif Zetterberg/ LZ media

TRYCK: CM-gruppen, Stockholm 2011

COPYRIGHT © 2009, The Committee of Sponsoring Organizations of the Treadway Commission (COSO).

1 2 3 4 5 6 7 8 9 0 LCN 0870517953

All Rights Reserved. No part of this publication may be reproduced, redistributed, transmitted or displayed in any form or by any means without written permission. For information regarding licensing and reprint permissions please contact the American Institute of Certified Public Accountants, licensing and permissions agent for COSO copyrighted materials.

Direct all inquiries to copyright@aicpa.org or to AICPA, Attn: Manager, Rights and Permissions, 220 Leigh Farm Rd, Durham, NC 27707. Telephone inquiries may be directed to 888-777-7707. Additional copies of this work may be obtained by visiting www.cpabiz.com.

Förord

Nu ger Internrevisorerna ut det fjärde i serien av COSO-dokument översatta till svenska. I januari 2009 publicerade COSO en särskild vägledning för den del av den interna styrningen och kontrollen som kallas »monitoring», det vill säga övervakning inklusive uppföljning och utvärdering. Den fördjupar och exemplifierar det som beskrevs redan i COSO:s första vägledning från 1992.

Orsaken till denna fördjupning är egentligen densamma som COSO:s vägledning från 2006 om hur mindre organisationer kan effektivisera sina system för intern styrning och kontroll. COSO ville då – efter 2002 års Sarbanes-Oxley-lagstiftnings hårda krav på intern styrning och kontroll – visa att intern styrning och kontroll inte måste leda till kostsamma påhängssystem. På samma sätt kan väl genomtänkt övervakning av systemen göra dem effektivare och enklare. Intern styrning och kontroll kan inte förenklas till en engångsinsats utan ska genom övervakning, uppföljning och utvärdering utsättas för löpande granskning och förändring så att den verkligen ger en rimlig försäkran om att ledningen har en god intern styrning och kontroll över organisationen. Vägledningens diskussion om övervakning av systemen ger också internrevisorer och externrevisorer många uppslag och idéer för deras granskning av den interna styrningen och kontrollen.

När nu många svenska företag och myndigheter har börjat skapa system för intern styrning och kontroll blir frågan om övervakningen av systemen allt viktigare. Då bör denna vägledning från COSO ge stöd för ett bra övervakningsarbete. Redan nu har en särskild aspekt lett till frågor och diskussion: vilken roll ska styrelsen för bolaget eller myndigheten ha för den interna styrningen och kontrollen? Det är å ena sidan uppenbart för de flesta att styrelsen inte kan bestämma detaljer i hur system för intern styrning och kontroll är uppbyggda eller fungerar. Det är å andra sidan uppenbart att frågor om dessa system inte heller helt kan överlåtas till den dagliga ledningen – de senaste årens finanskris visar att det vore för styrelsen att abdikera från sitt ansvar. För att finna en väg mellan dessa ytterligheter har i denna skrift översatts ett utdrag ur

3 ett annat COSO-dokument, publicerat i augusti 2009 (»Effektiv

uppsikt över risker på företagsövergripande nivå»). Detta dokument bygger i första hand vidare på COSO:s dokument om företagsövergripande riskhantering, ERM. Frågan om styrelsens roll är dock i stora drag densamma när det gäller intern styrning och kontroll. På liknande sätt påpekar COSO att frågor om monitoring, övervakning, i stort är desamma oavsett om de gäller intern styrning och kontroll eller ERM.

Den översättning som gjorts av vägledningen gäller bara sammanfattningen. Den som vill ta del av COSO:s rika insamling av erfarenheter och exempel inom detta område bör ta del av hela utgåvan som finns på engelska. Det gäller även övriga vägledningar som COSO gett ut. När det nu skapats en internationell standard för riskhantering (ISO 31 000) och som COSO ännu inte anpassat sig till eller kommenterat är det viktigt att uppmärksamma denna fond av erfarenhet som COSO skapat. ISO:s standard har mest karaktär av en teoretisk struktur och behöver kompletteras med just den typ av erfarenhetsbaserade råd och tips som COSO skapat.

Översättningen är genomförd på uppdrag av Internrevisorerna (IIA Sweden) med stöd av KPMG i Sverige.

Torbjörn Wikland

Övervakning (inklusive uppföljning och övervakning)¹: En integrerad komponent i intern styrning och kontroll

Under det gångna decenniet har organisationer gjort stora investeringar i förbättrad kvalitet i sina system för intern styrning och kontroll. De har gjort investeringarna av en rad skäl, särskilt för att: 1) god intern styrning och kontroll är bra för affärsverksamheten – det hjälper organisationer att uppfylla mål för verksamheten, den finansiella redovisningen och regelefterlevnaden, och för att 2) många organisationer avkrävs rapportering om kvaliteten i den interna styrningen och kontrollen av den finansiella redovisningen och tvingar dem att utveckla särskilt stöd för deras intyganden och påståenden.

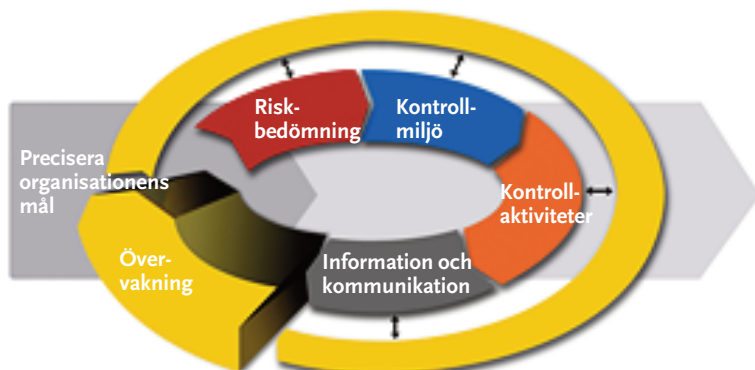
Intern styrning och kontroll utformas för att stödja organisationer i att uppnå sina mål. De fem komponenterna i COSO:s *Intern styrning och kontroll – Integrerat ramverk* (Internal Control, COSO:s ramverk – se separat översatt skrift nr 1) arbetar tillsammans för att minska riskerna för att en organisation misslyckas med att uppnå dessa mål.

COSO:s styrelse medger att ledningens försäkran om intern styrning och kontroll ofta har varit en tidskrävande uppgift som inbegriper årlig ledning av betydande omfattning och/eller granskning eller kontroll från internrevisionens sida. Effektiv övervakning kan understödja en rationalisering av försäkransprocessen, men många organisationer förstår inte fullt ut denna viktiga komponent i den interna styrningen och kontrollen. Resultatet blir att de underutnyttjar övervakningen i arbetet att stödja deras försäkran av den interna styrningen och kontrollen.

Figur 1 på nästa sida tecknar övervakningens övergripande roll och illustrerar hur en effektiv sådan tar hänsyn till den samlade effektiviteten i alla de fem komponenterna i den interna styrningen och kontrollen.

1 I grunddokumentet om Intern styrning och kontroll, utgivet 2006, översattes »monitoring» med »övervakning inkl. uppföljning och utvärdering». I detta dokument har översättningen i den följande texten förenklats till »övervakning».

Figur 1. Övervakningens roll i processen för intern styrning och kontroll



Övervakning överförd till processen för intern styrning och kontroll

COSO:s *Vägledning för att övervaka systemen för den interna styrningen och kontrollen* 2008 – COSO:s vägledning för övervakning (COSO:s 2008 Guidance on Monitoring Internal Control Systems – COSO:s Monitoring Guidance) utvecklades för att klargöra komponenten övervakning i den interna styrningen och kontrollen. Den ersätter inte den första vägledningen i COSO:s ramverk eller i COSO:s *Intern styrning och kontroll över den finansiella rapporteringen – en vägledning för mindre publika företag* 2006 (COSO:s vägledning 2006). Den snarare utvecklar de grundläggande principerna som finns i de båda dokumenten och vägleder organisationer i implementeringen av en effektiv och produktiv övervakning.

Hur stödjer övervakningen organisationens styrande process?

Övervakade kontroller har en benägenhet att försämrats över tid. Övervakning, definierad enligt COSO:s ramverk, genomförs för att man ska försäkra sig om »att den interna styrningen och kontrollen fortsätter att arbeta effektivt». ² När övervakningen är riktigt utformad och förverkligad, så gynnas organisationer därför att de är mer benägna att:

2 Citat ur COSO:s ramverk

- i god tid identifiera och korrigera problem i den interna styrningen och kontrollen
- producera mer korrekt och tillförlitlig information för att användas i beslutsfattandet
- förbereda korrekta finansiella rapporter i tid
- vara beredda att leverera periodiska intyganden och påståenden om effektiviteten i den interna styrningen och kontrollen.

I förlängningen kan en effektiv övervakning leda till organisatorisk kostnadseffektivitet och reducera kostnader knutna till offentlig rapportering om intern styrning och kontroll, eftersom problem har identifierats och adresserats på ett proaktivt, snarare än ett reaktivt, sätt.

Grundläggande om effektiv övervakning

COSO:s vägledning om övervakning bygger på två grundläggande principer/nyckelpunkter som ursprungligen etablerades i COSO:s vägledning från 2006:³

- Löpande uppföljningar och/eller separata utvärderingar som gör det möjligt för ledningen att avgöra huruvida intern styrning och kontroll fortsätter att fungera över tid.
- Brister i den interna styrningen och kontrollen identifieras och kommuniceras i tid till dem som ansvarar för korrigeringar, och till ledningen och styrelsen om så är lämpligt.

Vägledningen för övervakning (The Monitoring Guidance) föreslår vidare att dessa principer uppnås bäst genom en övervakning som baseras på tre övergripande beståndsdelar:

- **Etablerandet av en bas för övervakning** som inkluderar a) ett lämpligt »ledningsklimat»⁴; b) en effektiv organisationsstruktur

³ Se nyckelpunkterna 19 och 20 i COSO:s intern styrning och kontroll över den finansiella rapporteringen – vägledning för mindre publika företag utgiven 2006 (COSO:s vägledning 2006)

7 ⁴ »Tone at the top» är uttrycket på engelska.

som knyter övervakningsroller till människor med lämplig förmåga, objektivitet och auktoritet; och c) en startpunkt eller grund för intern styrning och kontroll från vilken en löpande övervakning och separata utvärderingar kan genomföras.

- **Utforma och verkställa övervakningsrutiner** fokuserade på *tydlig information* om verkan av *nyckelkontroller* riktade mot viktiga risker knutna till organisationens mål.
- **Värdering och rapportering av resultat**, som inkluderar en gradering av allvaret i identifierade brister och rapportering av resultat från övervakningen till behörig personal och styrelsen för åtgärder i tid och uppföljning om så behövs.

Bredden av övervakande processer

Organisationer kan välja bland en stor mängd av övervakande rutiner, som inkluderar men inte utesluter andra än de följande:

- Periodiska utvärderingar och tester av kontroller genom internrevisionen.
- Löpande övervakningsprogram inbyggda i informationssystem.
- Analys av, och lämpliga uppföljningar av arbetsrapporter eller mätningar som kan identifiera avvikelser som indikerar fel i kontroller.
- Övergripande granskningar av kontroller, såsom genomgångar av överensstämmelser som en normal del av processen.
- Självutvärderingar av styrelser och ledningar rörande det »ledningsklimat»⁵ som de format i organisationerna, och effektiviteten i deras uppsiktsfunktioner.
- Förfrågningar från revisionskommittéer av interna och externa revisorer.
- Kvalitetsgranskande genomgångar av internrevisionsavdelningar.

Fortsatta framsteg i teknologi och ledningsteknik borgar för att intern styrning och kontroll och anknutna övervakningsprocesser

⁵ Se not 1

kommer att förändras över tiden. De grundläggande idéerna om övervakning, såsom de beskrivs i COSO:s vägledning för övervakning, är emellertid utformade för att kunna vara giltiga över lång tid.

Om att använda COSO:s vägledning för att utveckla övervakningen

Ledningen kan starta övervakningsprocessen med att uppmuntra människor med ansvar för styrning och kontroll att läsa COSO:s vägledning för övervakning och att överväga hur man bäst realiserar övervakningen eller om den redan har etablerats inom vissa områden. Vidare bör personal med lämplig kompetens, auktoritet och resurser ges i uppdrag av ledningen att ta itu med följande fyra fundamentala frågor:

1. Har vi identifierat de relevanta riskerna för våra mål, till exempel riskerna knutna till att ta fram korrekta, tidsanpassade och fullständiga finansiella uttalanden?
2. Vilka kontroller är »nyckelkontroller»⁶ som bäst stödjer en slutsats om effektiviteten i den interna styrningen och kontrollen inom dess riskområde?
3. Vilken sorts information kommer att övertygande tala om för oss om kontrollerna fortsättningsvis fungerar effektivt?
4. Utför vi idag övervakning som inte utnyttjas effektivt i utvärderingen av den interna styrningen och kontrollen och som därför resulterar i fortsatt onödigt och kostsamt utnyttjande?

Ledningen och styrelsen bör förstå tankarna bakom effektiv övervakning och hur detta stödjer deras intressen. När styrelsen lär sig

6 COSO:s definition av nyckelkontroll: Nyckelkontroller är sådana som, när de utvärderas, ger stöd för en rimlig slutsats om förmågan hos hela systemet för intern styrning och kontroll att uppnå de underliggande målen. De kan verka inom en eller alla av COSO:s fem komponenter. Nyckelkontrollen har ofta en eller båda av följande karakteristika: 1) Om de inte fungerar kan de allvarligt påverka målen för vilka utvärderaren är ansvarig, och kanske inte upptäcks i tid av andra kontroller, och/eller 2) Deras sätt att fungera kan förhindra andra kontroller från att inte fungera eller upptäcka att andra kontroller inte fungerar innan de blir allvarliga hot mot organisationens mål.

mer om övervakning kommer den att utveckla den kunskap som behövs för att fråga ledningen, kopplat till vilket område som helst som rör de viktiga riskerna: »Hur vet ni att den interna styrningen och kontrollen fungerar?»

COSO:s vägledning för övervakning (COSO Monitoring Guidance) är utformad för att hjälpa organisationer att besvara dessa och andra frågor i de sammanhang som utgör deras egna unika omständigheter – omständigheter som kommer att förändras över tid. När de fortsätter att uppnå effektivitet i övervakningen, kommer organisationerna troligtvis ha möjlighet att ytterligare förbättra processen genom att använda verktyg såsom datorstödd kontinuerlig övervakning och avvikelserapporter anpassade till sina verksamhetsprocesser.

Vägledningen täcker också andra begrepp som är viktiga för en effektiv och produktiv övervakning såsom:

- vilka karaktäristika som kännetecknar en utvärderares objektivitet
- den tidsperiod och de omständigheter där en organisation kan förlita sig på lämpligt utformad *indirekt information* – när den används tillsammans med löpande eller periodisk *direkt information* – för att fastställa om den interna styrningen och kontrollen förblir effektiv
- att fastställa om informationen som används i övervakningen är tillräcklig och anpassad för att resultaten på ett adekvat sätt stödjer slutsatser om den interna styrningen och kontrollen
- olika sätt som organisationen kan göra övervakningen mer produktiv utan att reducera dess effektivitet.

COSO:s vägledning för övervakning (COSO Monitoring Guidance) omfattar tre volymer. Volym I presenterar de grundläggande principerna för effektiv övervakning och förklarar kopplingen till COSO:s ramverk. Volym II förmedlar mer detaljerat principerna som beskrivs i volym I och ger vägledning till dem som är ansvariga för att genomföra en effektiv övervakning. Volym III innehåller exempel på effektiv övervakning.

Många organisationer torde förbättra effektiviteten och produk-

tiviteten i sina system för intern styrning och kontroll genom att använda de tankar som utvecklas i denna vägledning. COSO:s vägledning för övervakning är utformad för det syftet, dvs. för att hjälpa organisationer (1) att identifiera effektiv övervakning där den redan finns och använda den på maximalt bästa sätt och (2) identifiera mindre effektiv övervakning, som kan förbättras. I båda fallen kan systemet för intern styrning och kontroll effektiviseras och därmed öka sannolikheten för att organisationens mål kan uppnås.

Effektiv uppsikt över risker på företagsnivå: Styrelsens roll

(Utdrag ur COSO:s dokument *Effective Enterprise Risk Oversight: The Role of the Board of Directors*. Augusti 2009)

Styrelsen i ett företag spelar en avgörande roll för att se till att det finns ett företagsövergripande förhållningssätt till riskhantering. Eftersom företagsledningen är ansvarig inför styrelsen är styrelsens fokus på effektiv uppsikt över risker avgörande för att ange tonen och klimatet för en effektiv riskhantering i strategiskt arbete, för formulering av mål på hög nivå och för godkännande av stora resurstilldelningar.

COSO:s *Företagsövergripande riskhantering – sammanhållet ramverk*⁷ lyfter fram fyra områden som bidrar till styrelsens uppsikt över företagsövergripande riskhantering:

- **Förstå företagets riskfilosofi och medverka till att fastställa företagets riskaptit.** Riskaptit är den risknivå, generellt uttryckt, som en organisation vill acceptera i förvaltandet av intressenternas insatser. Eftersom styrelsen representerar synpunkterna och önskemålen hos företagets nyckelintressen bör ledningen ha en aktiv diskussion med styrelsen för att etablera en ömsesidig förståelse för organisationens övergripande riskaptit.

⁷ COSO:s egen sammanfattning av detta dokument har utgivits på svenska som nr 2 i Internrevisorernas skriftserie med översatta COSO-dokument. Se www.internrevisorerna.se

- **Känna till i vilken utsträckning ledningen har etablerat en effektiv företagsövergripande riskhantering för organisationen.** Styrelsen bör ställa frågor till ledningen om de befintliga riskhanteringsprocesserna och utmana ledningen att visa upp effektiviteten i dessa processer vad gäller identifiering, värdering och hantering av organisationens mest betydelsefulla företagsövergripande riskexponeringar.
- **Granska företagets riskportfölj och jämföra den med företagets riskaptit.** Effektiv uppsikt över riskerna från en styrelses sida betingas av styrelsens förmåga att förstå och värdera en organisationens strategi i förhållande till riskexponeringar. Tid som styrelsen avsätter på dagordningen och informationspunkter som integrerar strategi och verksamhetsinitiativ med företagsövergripande riskexponeringar, stärker styrelsens förmåga att säkerställa att riskexponeringar motsvaras av den övergripande riskaptiten.
- **Bli underrättad om de viktigaste riskerna och huruvida ledningen hanterar dem ordentligt.** Risker utvecklas ständigt och efterfrågan på robust information är stor. Regelbunden uppdatering från ledningens sida till styrelsen av nyckelriskfaktorer är avgörande för en effektiv övervakning från styrelsens sida av riskexponeringar för att bevara och öka intressenternas insatser.

Styrelser utnyttjar ofta styrelsekommittéer för att fullfölja en del av sin uppsikt över riskerna. Användningen av och fokus för kommittéerna varierar från ett företag till ett annat, även om vanliga kommittéer är revisionskommittéer, nominerings-/bolagsstyrelsekommittéer, ersättningskommittéer, som var och en riktar uppmärksamheten på delar av den företagsövergripande riskhanteringen. Även om uppsikten över riskerna, liksom strategin, är styrelsens fulla ansvar kan en del företag inleda processen genom att be de berörda kommittéerna att ta upp översikten av risker inom sina områden och fokusera på strategiska riskfrågor i diskussionen med hela styrelsen.