

# Styrelsens och bolagsledningens arbete med värdeskapande riskhantering och intern kontroll

En arbetsmodell för att möta nya förväntningar och krav



# Innehåll

Inledning	3
Vilken affärsnytta ligger i att arbeta med riskhantering och intern kontroll?	5
Stöd i det praktiska arbetet – ramverk för riskhantering och intern kontroll	6
Hur hänger övergripande riskhantering och intern kontroll ihop?	7
Hur kan bolagen arbeta värdeskapande med riskhantering och intern kontroll?	8

Bilaga

# Inledning

Vi befinner oss i en spännande period där praxis inom området styrning, riskhantering och intern kontroll kommer att utvecklas för att nå den väl avvägda nivå som eftersträvas i Sverige. PricewaterhouseCoopers har såväl internationellt som i Sverige en gedigen erfarenhet av hur bolag bör utveckla sin styrning, riskhantering och interna kontroll på ett väl avvägt sätt. Oavsett hur praxis utvecklas i Sverige så är den metod som beskrivs i denna skrift något som kommer att bidra till att skapa och bevara värde för de bolag som tillämpar den.

## Svensk kod för bolagsstyrning samt lagförändringar utifrån EG-direktiv för bolagsstyrning

- Den reviderade koden omfattar sedan 1 juli 2008 en utvidgad krets av bolag, dvs samtliga noterade bolag på en reglerad marknad.
- Från och med 1 juli 2008 är det god sed på värdepappersmarknaden för svenska bolag vars aktier är upptagna till handel på en reglerad marknad att tillämpa koden och koden. Koden utgör därmed – indirekt – en del av börsens regelverk.
- De berörda bolagen bör tillämpa koden så snart som möjligt efter den 1 juli 2008, dock senast inför bolagsstämmorna 2009.
- Svensk kod för bolagsstyrning tillämpas utifrån principen ”följ eller förklara” dvs antingen följs kodens regler eller så förklarar bolaget och motiverar de avvikelser som görs.
- Införandet av EG:s 8:e direktiv, artikel 41, och lagförändringar i Aktiebolagslagen innebär bland annat krav på noterade bolag att inrätta revisionsutskott och reglering av revisionsutskottets uppgifter.
- Införandet av EG:s ändrade 4:e och 7:e bolagsdirektiv, artikel 46, och lagförändringar i Årsredovisningslagen innebär bland annat lagstadgat krav på en bolagsstyrningsrapport.
- För statliga bolag är grundprincipen att Svensk kod för bolagsstyrning kompletterar statens ägarpolitik. I vissa frågor har Regeringskansliet funnit skäl att komplettera eller tolka kodens regler.

God bolagsstyrning handlar om att säkerställa att bolag sköts på, ett för aktieägarna, så effektivt sätt som möjligt. Allmänhetens förtroende för näringslivet, liksom förtroendet mellan näringslivets olika aktörer är av grundläggande betydelse för samhällsekonomin och investeringsviljan. Dessa frågor är centrala för att trovärdigheten för en sund värdepappershandel kan utvecklas och att tillgången till riskkapital fungerar.

För att vinna marknadens förtroende ställs krav på ökad transparens och att bolagen presenterar all den information man avser att ge, till ägare och andra intressenter, på ett logiskt och organiserat sätt så att en trovärdig och öppen finansiell rapportering skapas.

En stark drivkraft till att frågan om riskhantering fått ökat genomslag är att skapa möjligheter att nå framgång i affärer genom att ta kontrollerade risker. Därmed ställs krav på att visa upp en effektiv företagsövergripande riskhantering. Riskhanteringen ska inte vara ett självändamål utan ska integreras med bolagets affärsprocess och därmed den interna styrningen och kontrollen.

Den reviderade Koden innehåller bl a regler avseende information om bolagsstyrning, bolagsstämma, valberedningar, styrelsens uppgifter, och dess storlek, sammansättning, arbetsformer samt styrelseordförandens roll. Enligt Koden framgår bl a att styrelsen ansvarar för att bolaget har en god intern kontroll och formaliserade rutiner som säkerställer att fastlagda principer för finansiell rapportering och intern kontroll efterlevs. Koden föreskriver att bolagen ska inrätta ett revisionsutskott och reglera revisionsutskottets uppgifter. Koden innehåller även krav på rapportering av bolagsstyrning och intern kontroll i en årlig bolagsstyrningsrapport.

Parallellt med den reviderade koden har EG-direktiven som berör bolagsstyrning införts i Sverige samt i de övriga länderna i Europa. Dessa innebär bl a tydligare krav på styrelser och revisionsutskott att övervaka effektiviteten i företagets riskhantering och interna kontroll.

EU har haft dessa frågor på agendan ett antal år och strävan är att uppnå en harmonisering inom Europa. Även andra intressenter (t ex investerare, ägare, analytiker och kreditratingföretag) har förväntningar på att bolagets styrelse och ledning arbetar strukturerat med dessa frågor.

Nuvarande praxis i bolagen har huvudsakligt fokus på den finansiella rapporteringen dvs den avgränsade delen av intern kontroll. Fokus är nu riskhantering och intern kontroll från ett företagsövergripande perspektiv där samarbetet mellan bolagsledning och styrelse med dessa frågor blir betydelsefullt för ett värdeskapande och effektivt arbete.

Denna skrift tar sin utgångspunkt i hur styrelser och bolagsledningar kan arbeta värdeskapande med riskhantering och intern kontroll. Den beskriver översiktligt en möjlig arbetsmodell hur styrelse och bolagsledning kan arbeta med dessa områden från ett företagsövergripande perspektiv. Vår ambition är att denna arbetsmodell ska underlätta arbetet och samtidigt underbygga rapportering om riskhantering och intern kontroll.

I bilaga till denna skrift framgår ett utdrag avseende vilka regler beträffande riskhantering och intern kontroll som finns i koden och lagförändringar utifrån EG-direktiv för bolagsstyrning.

# Vilken affärsnytta ligger i att arbeta med riskhantering och intern kontroll?

De insatser som nu krävs utifrån Koden och lagförändringar utifrån EG-direktiven och andra intressenters förväntningar och krav bör inte ses som en pålaga, utan istället byggas in i den styrmodell som bolagen redan idag arbetar efter. På så sätt bli de en hörnsten i styrningen som ger bolaget ett mer strukturerat förhållningssätt vad gäller risker. Utgångspunkten är dessutom att dessa insatser – rätt hanterade – skapar värde och nytta i bolagens verksamhet. Allt företagande handlar om att ta risker, men genom att ta rätt risker kan bolagen också i slutänden öka sin avkastning. Genom att arbeta mer strukturerat på dessa områden kan bolagen bli mer effektiva och flexibla i sin vardag. Man kan också likna det vid att bolagen etablerar en gemensam intern färdväg som gör det lättare att styra mot ett och samma mål.

## Affärsmöjligheter fångas upp

Genom att systematiskt analysera potentiella händelser, det vill säga möjligheter och risker är ledningen i stånd att identifiera och i god tid tillvarata affärsmöjligheter vilket kan ge stora konkurrensfördelar.

## Förmåga att fatta snabba och riktiga beslut

Genom att bolaget på alla nivåer har tillgång till relevant information om möjligheter och risker underlättas beslutsfattandet. Det är vanligt att ärenden bordläggs i ledningar eller styrelser på grund av otillräcklig information. Antalet bordlagda ärenden minskar om frågan "Följer vi fortfarande tillämpliga regler och lagar om vi fattar det

beslutet?" kan besvaras genom en tydligt kommunicerad riskanalys.

## Högre effektivitet och trygghet genom riskarbetet

En företagsgemensam riskstrategi och angreppssätt för ohanterade riskområden ger möjlighet att satsa resurser på rätt risker ("prioritering"). Utifrån en överblick av nuvarande riskexponering kan riskarbetet optimeras i olika delar av organisationen, till exempel med en gemensam försäkringsstrategi.

## Samordna olika parallella initiativ

I större bolag finns ofta olika funktioner som arbetar parallellt med bolagets risker, till exempel identifikation och rapportering av risk och osäkerhetsfaktorer, arbete med Corporate Social Responsibility, internrevision, risk management och resultat av kvalitetsarbete. Många bolag har inte ett helhetsperspektiv för de olika initiativen. Här kan bolagen bli bättre på att integrera olika initiativ och säkerställa att arbetet och rapporteringsdelarna kompletterar och inte överlappar varandra.

## Öka medarbetarnas riskmedvetenhet

Genom att koppla riskhantering till individuella mål ökar medarbetarnas riskmedvetenhet. Detta gör att riskarbete drivs mer proaktivt på alla nivåer i organisationen vilket är en viktig faktor för att gemensamma mål kan uppnås.

# Stöd i det praktiska arbetet – ramverk för riskhantering och intern kontroll

Varken Koden eller lagförändringar till följd av EG-direktiven innehåller egentliga kriterier för utvärdering eller krav på användning av ett etablerat ramverk för riskhantering och intern kontroll.

Ett etablerat ramverk för riskhantering och intern kontroll underlättar dock arbetet, eftersom det tillhandahåller en gemensam nomenklatur och struktur för viktiga delar i det praktiska arbetet med riskhantering, intern kontroll, och utvärderingen av denna. Ett ramverk underlättar dessutom vid intern och extern kommunikation. Beslut om lämpligt tillvägagångssätt i det enskilda bolaget är och förblir dock en fråga för styrelse och ledning.

Det ramverk som fått den största spridningen och är internationellt erkänt är Enterprise Risk Management – Integrated Framework, lanserat 2004 av The Committee of Sponsoring Organizations of the Treadway Commission (COSO). Ramverket baseras på COSOs ramverk "Internal Controls – Integrated Framework" (lanserat 1992) genom att lyfta fram att all intern kontroll behöver utformas enligt organisationens risksituation ([www.coso.org](http://www.coso.org)).

# Hur hänger övergripande riskhantering och intern kontroll ihop?

För att kunna underlätta kommunikation och förståelse är det viktigt att ha en gemensam uppfattning om vad vi menar med riskhantering och intern kontroll och hur det hänger ihop. Det finns olika definitioner av riskhantering och den mest vedertagna är definitionen i enlighet med COSO-ramverket:

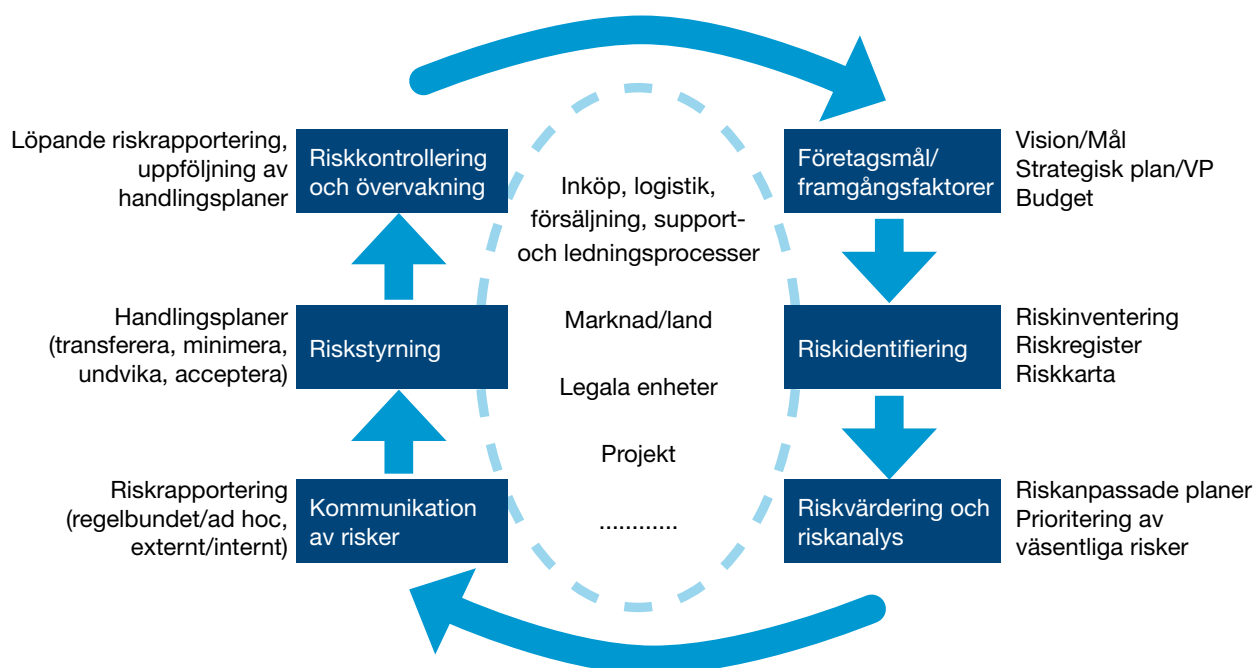
”Övergripande riskhantering (”Enterprise Risk Management”) är en process som påverkas av styrelsen, bolagsledningen och annan personal, etablerat i strategiprocesen och i hela organisationen, utformat för att identifiera potentiella händelser som kan påverka bolaget, och hantera risk inom bolagets riskaptit, för att ge en rimlig försäkran om att bolagets mål uppnås”.

Begreppet ”risk” definieras följaktligen som möjligheten att en händelse inträffar som negativt kan påverka bolagets förmåga att uppnå sina mål. Definitionen omfattar alla typer av risker, till exempel strategiska, finansiella, operativa och risker relaterade till krav på efterlevnad av tillämpliga lagar och regler.

Riskhanteringsprocessen kan generellt liknas vid ett kretslopp (se figur nedan) som utgörs av flera sammankopplade moment. Dessa utförs och utformas i praktiken genom olika metoder eller dokument.

Det är viktigt att komma ihåg att värdeskapande riskarbete börjar med att definiera bolagets mål. Bolagets affärsplan och strategi utgör därmed utgångspunkter för effektivt och relevant risk- och internkontrollarbete.

Basen för effektiv riskhantering och intern kontroll är kontrollmiljön, som innefattar den kultur som styrelse och bolagsledning kommunicerar och verkar utifrån. Kontrollmiljön definieras av styrelsens och ledningens riskbenägenhet som återspeglas i bolagets övergripande målsättning och strategi. Utifrån en analys av risker samt hur dessa kan hota att målen infrias, bestäms sedan om riskerna med hjälp av lämpliga åtgärder och kontroller, ska transfereras, reduceras, undvikas eller övervakas. Bolagets risksituation behöver regelbundet följas upp för att kunna utvärdera riskstrategins effektivitet. Det kan därför från tid till annan bli nödvändigt att justera bolagets målsättningar om de bidrar till för hög riskexponering för bolaget.



# Hur kan bolagen arbeta värdeskapande med riskhantering och intern kontroll?

Utvecklingen under senare år såväl i Sverige som utomlands har visat på betydelsen av att bolagen har god intern kontroll. Riskhantering och intern kontroll från ett företagsövergripande perspektiv behöver därför komma upp på styrelsernas/revisionsutskottens agendor. Samarbetet mellan bolagsledning och styrelse blir betydelsefullt. Det är viktigt att tydliggöra ledningens ansvar för genomförande samt styrelse och revisionsutskottets ansvar för övervakning och utvärdering.

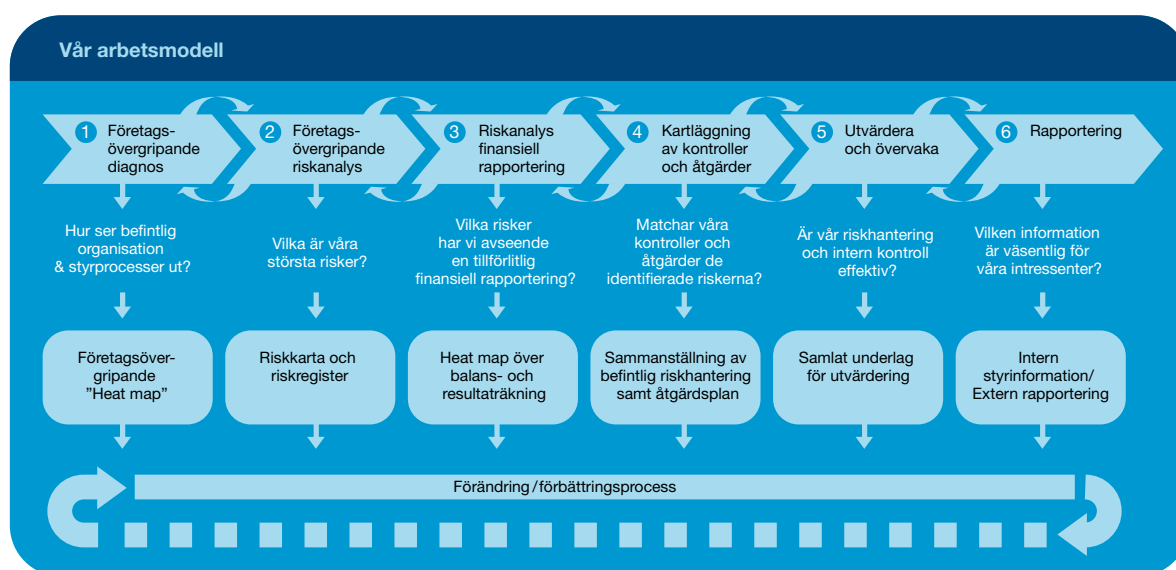
Styrelser och revisionsutskott behöver bli tydligare kravställare på relevant information från bolagsledningen och kontinuerligt ompröva informationsbehovet utifrån bolagets rådande risksituation – eftersom styrelser och revisionsutskott ska bilda sig en egen uppfattning om den interna kontrollens effektivitet – och kunna veta att rätt risker kontrolleras.

Riskhantering och intern kontroll är inget nytt. Alla bolag har någon form av intern kontroll, utformad på olika sätt med olika grad av formalisering, men oftast är den fragmenterad. Det praktiska arbetet bör således ta sin utgångspunkt i väsentlighetsbegreppet och samtidigt beakta de goda initiativ som redan utförs i det dagliga arbetet i verksamheten.

Vår arbetsmodell nedan illustrerar en metod för hur ett bolag i praktiken kan arbeta för att utifrån ett riskperspektiv kunna uppnå en lämplig nivå på den interna kontrollen. Arbetsmodellen är tillämplig för bolag som vill komma i gång snabbt och nå konkreta resultat på kort tid.

PricewaterhouseCoopers synsätt främjar en "top-down" och riskbaserad ansats där stor vikt läggs vid styrelsens och ledningens riskbedömning. Utvärdering av styrkan i företagsövergripande kontroller, exempelvis förekomst av lämpliga policies och riktlinjer, är en viktig utgångspunkt för att identifiera väsentliga områden för vidare fördjupad analys inom bolaget.

Arbetsmodellen nedan illustrerar en tänkt logisk följd för att bidra till att skapa och bevara värde i bolaget. Översta raden är arbetssteget, mellersta raden visar vilken fråga detta arbetssteg besvarar, tredje raden visar vad som blir resultatet av respektive arbetssteg. I figuren illustreras även att förändringar och förbättringar görs löpande under arbetet, samt att det kan vara nödvändigt att återvända till ett tidigare arbetssteg beroende på utfallet.



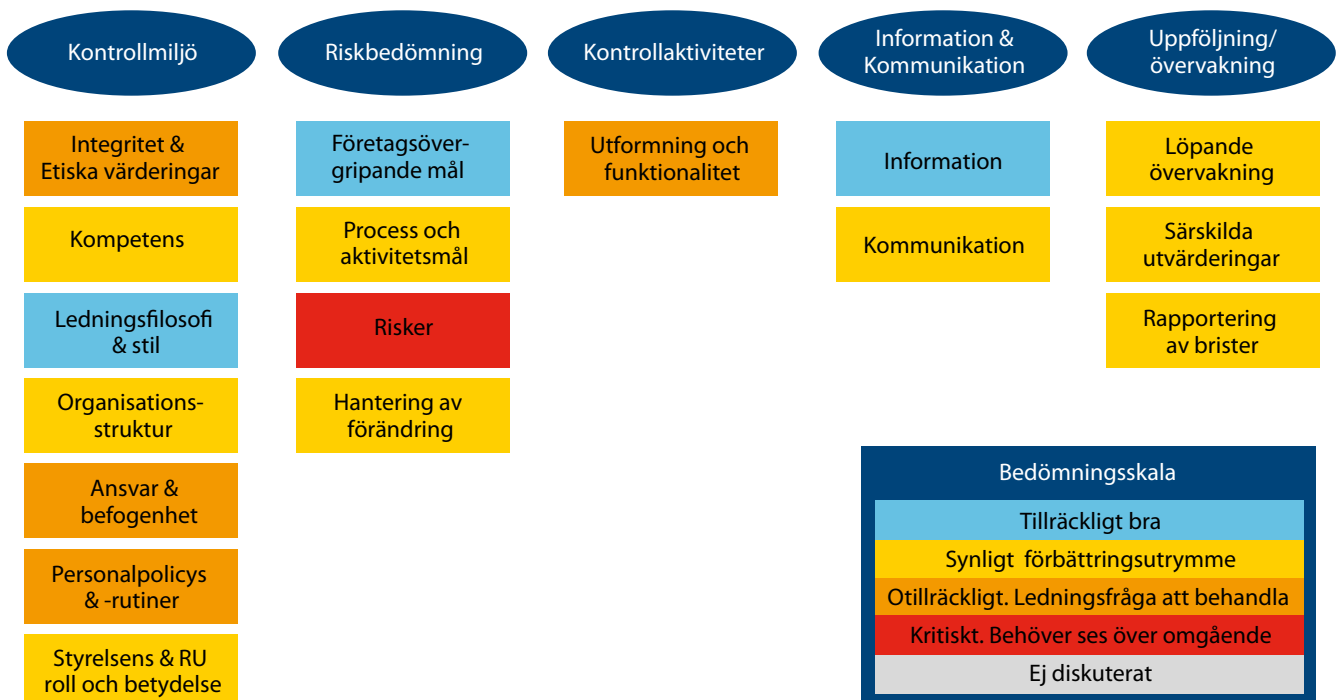
# Hur kan bolagen arbeta värdeskapande med riskhantering och intern kontroll?

## Steg 1. Företagsövergripande diagnos av riskhantering och intern kontroll

Det strukturerade arbetet med riskhantering och intern kontroll bör inledas med en företagsövergripande diagnos – en nulägesanalys – av de väsentliga komponenterna i bolagets befintliga riskhanterings- och internkontrollstruktur. Diagnosen utförs med syfte att få en förståelse för bolagets befintliga organisation, styrprocesser och relevanta företagsövergripande kontroller och deras relativa styrka. Genom diagnosen sätts bolagets styrmodell i fokus samtidigt som det fångar upp olika initiativ som pågår inom bolagets olika funktioner, roller och ansvar samt förekomst av olika styrande dokument såsom

affärsplan, policies och riktlinjer. En lämplig omfattning för diagnosen ges i COSO:s principer/fokuspunkter, där väsentliga områden inom respektive komponent beaktas. Dessa illustreras i nedanstående exempel, där resultatet från diagnosen har sammanställts i en sk "heat map", med identifierade förbättringsområden. Diagnosen utförs lämpligen i en workshop.

Diagnosen skapar även en förståelse för bolagets styrmodell och vilka funktioner inom bolaget som arbetar med riskhantering. Det är av stort värde att det fortsatta arbetet tar sin utgångspunkt i bolagets styrmodell. Ett förenklat exempel på en heat map illustreras i figuren nedan.

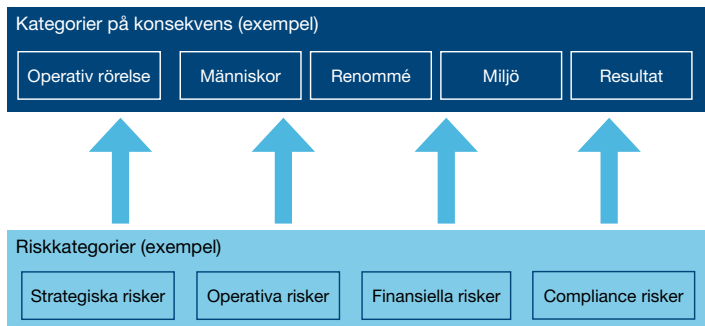


# Hur kan bolagen arbeta värdeskapande med riskhantering och intern kontroll?

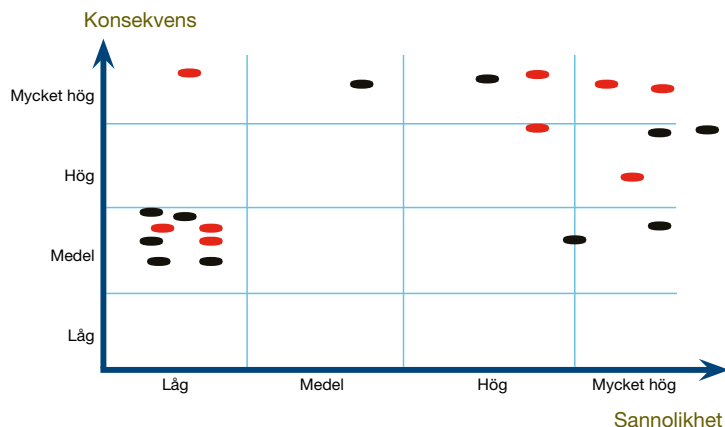
## Steg 2. Vilka risker har bolaget? Företagsövergripande riskanalys

Medan steg 1 belyser utformningen av företagets övergripande interna styrnings- och kontrollstruktur, införs i steg 2 risk- och väsentlighetsbegreppen för att kunna skilja väsentliga från mindre viktiga riskområden.

Företaget inventerar därför sina enskilda risker inom relevanta riskkategorier. Syftet med en riskinventering är att identifiera de viktigaste riskerna som bolaget är utsatt för, bedöma sannolikheten att de kan inträffa samt att kvantitativt eller kvalitativt värdera deras påverkan på företagets mål. Samtidigt bedöms hur effektiva befintliga kontroller och åtgärder är för att minska riskerna som till viss del redan har identifierats i steg 1. Inventeringen genomförs i workshops, intervjuer eller genom självutvärdering.



Resultat av inventeringen kan illustreras i en riskkarta som ska återspegla företagets riskexponering i dagsläget. Riskkartan är ett överskådligt dokument för en framtida uppföljning av företagets "riskbild" och bör sedan uppdateras regelbundet (se exempel nedan).



Riskkartan är ett hjälpmedel för att kunna prioritera risker som överstiger bolagets riskacceptansnivå som illustreras genom hög sannolikhet och/eller påverkan. Riskkartan underlättar därmed besluten om hur riskerna ska bemötas med olika riskstrategier (undvika, transferera, minimera, acceptera) samt ökar företagets förmåga att kunna satsa rätt resurser på rätt område.

## Steg 3. Exempel på nedbrytning av ett riskområde – riskanalys avseende den finansiella rapporteringen

Det övergripande målet med ett bolags externa finansiella rapportering är att den ska vara tillförlitlig och framtagen i överensstämmelse med god redovisningssed, tillämpliga lagar och förordningar samt övriga krav, exempelvis kraven för noterade bolag. En strukturerad och omsorgsfull riskbedömning möjliggör identifiering av de väsentliga riskerna som kan komma att påverka hur väl detta mål uppnås. I steg 1 och 2 i arbetsmodellen erhålls en första övergripande bedömning av väsentliga områden, möjliga redovisningsrisker och var möjliga brister i affärsprocesser finns.

Den fördjupade riskbedömningen avseende risk för fel i den finansiella rapporteringen bör ta sin utgångspunkt i väsentliga finansiella poster såsom balans- och resultaträkningen och väsentliga noter. Bedömningen beaktar såväl kvantitativ (väsentlighet) som kvalitativ risk (den finansiella postens komplexitet, felhistorik, risk för oegentligheter/bedrägerier etc) som ligger i var och en posterna. Vid analysen beaktas bolags-, affärsenhets- och funktionsnivå samt IT-miljön och eventuell förekomst av outsourcing av processer.

Genom att ta utgångspunkt i väsentlighet och risk inriktas således det fortsatta arbetet på de väsentliga finansiella posterna samt de mest väsentliga affärsenheterna. Exempelvis är de processer som gäller justerings- och bokslutsposter känsliga för att ledningen överskrider sina befogenheter. Redovisningsmässiga bedömningar, såsom värdering av tillgångar och skulder är ofta beroende av en noggrann analys av den ekonomiska miljön, och i vissa fall konkurrenternas agerande, och kan vara känsliga för manipulation. Det är även värt att notera att många av företagsskandalerna under det senaste årtiondet kunnat hänföras till felaktiga redovisningsmässiga bedömningar och justeringsposter.

I det förenklade exemplet högst upp på nästa sida illustreras ett sätt att väga samman olika kvantitativa och kvalitativa faktorer till en total riskexponering.

## Hur kan bolagen arbeta värdeskapande med riskhantering och intern kontroll?

**Riskanalys Finansiell Rapportering – förenklat exempel**

Post	Balans	Materialitet	Komplexitet	Felhistorik	Bedrägeririsk	Påverkan av övergripande kontroller	Total riskexponering
<b>Balansräkning 31 december 2007</b>							
<b>Omsättningstillgångar</b>							
Varulager	8 774	1	4	5	3	0	13
Kundfordringar	189 317	3	4	5	4	-1	15
Kortfristiga placeringar	681 254	4	4	1	2	-4	7
Kassa och bank	553 071	4	2	2	5	-1	12

Hög prioritet


### Steg 4. Hur hanterar ni dessa risker? Mappning av befintliga kontroller med väsentliga risker

Riskerna som har identifierats och prioriterats i steg 2 och 3 sammanställs för att kunna utvärdera att såväl övergripande som mer detaljerade åtgärder och kontrollaktiviteter utformats ändamålsenligt för att hantera väsentliga övergripande risker och risker avseende den finansiella rapporteringen.

Sammanställningen underlättar arbetet med att identifiera gap och är därmed ett stöd för att adressera väsentliga risker med lämpliga kontroller och åtgärder. Det leder till en handlingsplan för att förbättra den interna kontrollen utifrån ett riskperspektiv.

Bolaget måste klargöra vilka strategier man har för att hantera riskerna, dvs vilka risker man accepterar, vilka man kanske vill överföra till andra aktörer och vilka man vill försöka reducera.

Det är här som systemet för internkontroll kommer in, dvs alla de regler bolaget satt upp i form av styrande dokument i form av policys, riktlinjer etc. Man måste således veta vad som ska ställas mot riskerna och försäkra sig om att den interna kontrollen är rätt utformad så att riskhanteringen kan bli effektiv.

Risk		Kontrollmoment	Uppföljningsprocess	Effektivitet	Åtgärdsplan			Status
Vad heter risken?	Vad innebär risken?	Vilken kontroll/ åtgärd måste finnas eller fungera för att motverka risken?	Hur följer vi upp effektivitet och efterlevnad av kontrollmoment?	Hur bra fungerar våra nuvarande kontrollmoment idag?	Vilka åtgärder vidtar vi i år för att förbättra våra kontrollmoment?	Vem är ansvarig?	Till vem och hur ofta rapporteras våra framsteg?	

## Hur kan bolagen arbeta värdeskapande med riskhantering och intern kontroll?

Exempel på hierarki av styrande dokument:

- Policier – beskriver varför – övergripande avsikt och viljeförklaring från ledningen
- Riktlinjer – beskriver vad som ska göras för att övergripande mål i policier ska uppnås
- Anvisningar/processbeskrivningar – beskriver på vilket sätt policyns innehåll ska införas
- Rutinbeskrivningar/instruktioner – beskriver hur och av vem åtgärderna ska införas

Det är av stor vikt att de styrande dokumenten kommuniceras inom organisationen på ett tydligt sätt så att samtliga berörda personer förstår riktlinjerna och vet hur de ska förverkligas. Till detta följer sedan en väl fungerande återrapportering som säkerställer att intentionerna verkligen efterlevs.

### Steg 5. Utvärdering och övervakning av riskhantering och intern kontroll – vad är nuläget och vad bör förbättras?

Förändrings-/förbättringsarbete av riskhanteringsprocessen är nödvändigt. Riskhantering och intern kontroll bör uppdateras i takt med att företagets omständigheter förändras (t ex pga nya marknader eller nya produkter). Bolagets riskexponering påverkas kontinuerligt och nya lokala och globala riskscenarier blir relevanta och som därför behöver övervakas (t ex nya politiska utvecklingar, pandemier, konjunktursvängningar).

Ett effektivt stöd i förändringsarbetet är sammanställningen som har skapats i steg 4. Utifrån ett riskperspektiv identifieras viktiga riskområden dess hantering och därmed om kontrollerna behöver övervakas eller förbättras.

Olika risker kräver olika typ av uppföljning. Syftet med detta arbetssteg är att utvärdera hur väl riskstrategierna som har definierats i steg 4 efterlevs i organisationen.

Styrelserna och revisionsutskotten måste sannolikt bli en tydligare kravställare i framtiden. De måste sätta upp ett ramverk över vilket typ av rapportering, som de kommer att behöva, dvs givet att ledamöterna nu ska bilda sig en tydligare uppfattning om hur företagets system för riskhantering och intern kontroll fungerar. Styrelsen och revisionsutskottet bör ställa sig frågan om det inom bolaget finns tillräckliga underlag för att övervaka och utvärdera att de kontroller som ska hantera riskerna verkligen fungerar?

Redan idag får styrelser någon typ av rapportering i dessa frågor, men nu måste man säkra att denna rapportering ger en tillräckligt heltäckande bild av hur det ser ut. Med heltäckande menas att styrelsen kan se att företaget har rimlig kontroll över de risker som är viktiga. Det blir ett slags "riskregister", med återrapportering till styrelsen på de t ex 10-15 mest väsentliga riskerna. Denna återrapportering ligger sedan till grund för de årliga analyser och utvärderingar som styrelsen gör kring riskhanteringen och som ska säkerställa att organisationen har fokus på rätt saker. Det blir således underlag för styrelsens interna slutsats om hur riskhantering – och internkontrollsystemet fungerat under det senaste räkenskapsåret.

Några exempel på metoder för att övervaka och utvärdera att kontroller som ska hantera risker verkligen fungerar kan vara:

- Control Self Assessment – CSA (självutvärdering av kontrollaktiviteter). Vid CSA bör så hög grad av objektivitet eftersträvas som möjligt t ex genom att någon oberoende till den som utfört kontrollen bekräftar att den utförts.
- Business Performance Reviews – löpande uppföljning av den operativa verksamheten inklusive uppföljning av lämpliga Key Performance Indicators (KPI) – riskhantering och intern kontroll bör därför vara en stående punkt på agendan.
- Controlling (effektiva system och metoder för uppföljning och kontroll av bolagets verksamhet och ekonomiska ställning mot de fastställda målen)
- Särskilda utredningar och granskningar samt särskild uppföljning för att säkerställa att rapporterade brister åtgärdas.
- Särskild testning (ett särskilt testprogram utarbetas där någon annan än den som utför kontrollen testar att kontrollerna utförts som det var tänkt).
- Styrelseutskottens arbete – t ex Revisionsutskottets arbete med att för styrelsens räkning kvalitetssäkra den finansiella rapporteringen.
- Internrevisioner (i de fall särskild granskningsfunktion – internrevision – finns etablerad kan deras uppdrag omfatta att särskilt granska efterlevnad av intern kontroll).

## Hur kan bolagen arbeta värdeskapande med riskhantering och intern kontroll?

Ett sätt att summera bolagets mognadsnivå vad gäller den interna kontrollen är att mäta in sig i enlighet med PricewaterhouseCoopers Internal Controls Maturity Framework, se figur nedan.

Inom olika områden befinner sig bolaget sannolikt på olika nivåer enligt denna skala, vilket är fullt naturligt beaktat väsentlighet och risk.

Genom att använda PricewaterhouseCoopers "Internal Control Maturity Framework" erhålls en gemensam skala för bedömning som även skapar underlag för identifiering av förbättringsområden. Att fastställa ambitionsnivå för det enskilda bolaget är och förblir dock en fråga för styrelse och ledning.

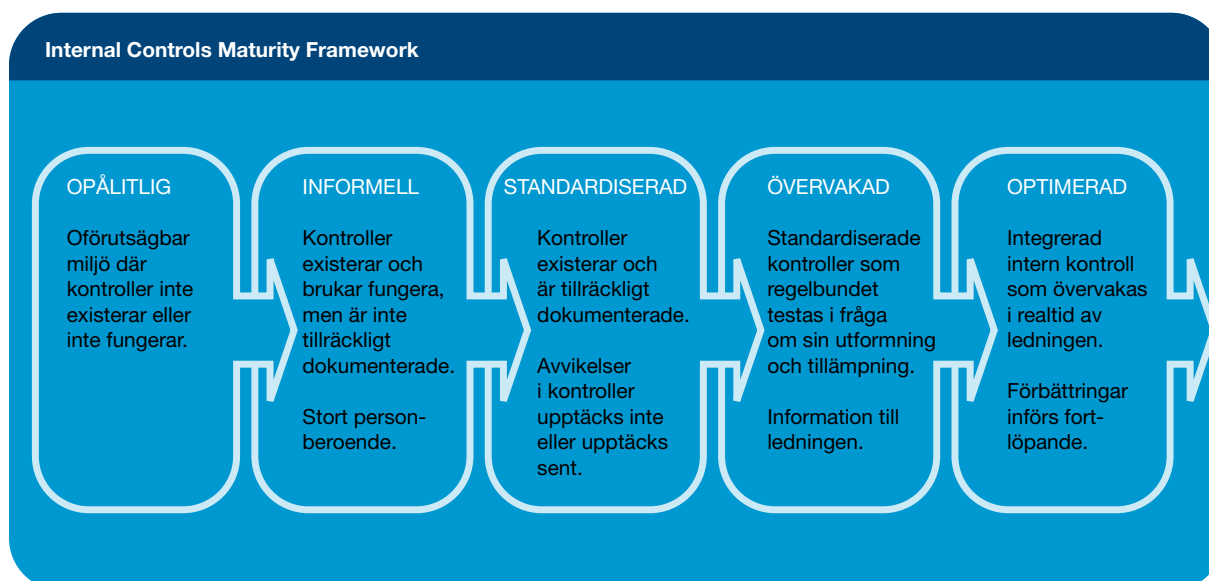
### Utvärdering av behovet av en särskild granskningsfunktion (internrevision)

I bolag som inte har en särskild granskningsfunktion (internrevision) ska, enligt Koden, styrelsen årligen utvärdera behovet av en sådan funktion och i sin beskrivning av de väsentliga inslagen i bolagets system för riskhantering och interna kontroll motivera sitt ställningstagande. Således ska styrelsen utvärdera värdet av särskild granskning av den interna kontrollen. Som utgångspunkt i denna utvärdering kan följande fråga ställas:

"Finns särskilda omständigheter beaktat bolagets specifika verksamhet eller andra förhållanden som gör att en särskild granskningsfunktion (internrevision) bör inrättas?"

Ett exempel på sådana omständigheter kan vara att bolaget har en särskild riskexponering som medför att, även om den interna kontrollen i "linjen" fungerar tillfredsställande, bolaget inte har "råd" med de konsekvenser som kan uppkomma vid eventuella brister. Detta förhållande gäller för vissa bolag med särskilt publikt intresse. Till exempel för finansiella bolag har staten genom Finansinspektionen reglerat att en särskild granskningsfunktion ska finnas i syfte att ge en oberoende utvärdering av den interna kontrollen så att styrelsen kan vidta lämpliga åtgärder.

Ett annat exempel är ett bolag som av olika skäl inte har en tillräckligt formell och tydlig struktur för intern kontroll och som saknar tillräckliga rutiner för uppföljning av densamma. I ett sådant fall kan en särskild granskningsfunktion både fungera som en drivkraft för vidare uppbyggnad av rutiner och samtidigt ge styrelse och ledning en oberoende utvärdering av den interna kontrollen.



# Hur kan bolagen arbeta värdeskapande med riskhantering och intern kontroll?

## Steg 6. Intern och extern rapportering av riskhantering och intern kontroll

Nedan illustreras hur bolagens arbete med riskhantering och intern kontroll byggs in i den årscykel som bolagen redan idag arbetar utifrån. Det blir en utgångspunkt för att definiera viktiga milstolpar (t ex styrelsemöten, strategisk och operativ planering samt rapportering) och illustrerar när strukturerad information om risk och kontroll behöver vara tillgänglig för att fungera som ett effektivt stöd för att från ett riskperspektiv kvalitetssäkra styrning och rapportering inom bolaget.

Genom att tillämpa den möjliga arbetsmodellen skapas även ett underlag för den externa rapporteringen och där visa att riskhantering och intern kontroll är en integrerad del av verksamhetsstyrningen.

Enligt Koden och Årsredovisningslagen ska bolagen upprätta en bolagsstyrningsrapport samt enligt Årsredovisningslagen ska bolagen bl a beskriva väsentliga risker och osäkerhetsfaktorer. Av regelverken framgår vad en bolagsstyrningsrapport bör innehålla, bl a ska styrelsen i ett särskilt avsnitt beskriva bolagets riskhantering och interna kontroll avseende den finansiella rapporteringen.

Styrelsen beskriver därmed övergripande de väsentliga inslagen i bolagens system för riskhantering och interna kontroll med utgångspunkt i bolagets styrmodell. Underlag till beskrivningarna erhålls från de tidigare arbetsstegen i denna arbetsmodell. Beskrivningarna bör vara pedagogiska och bolagsanpassade och knyta an till övriga delar i årsredovisningen.

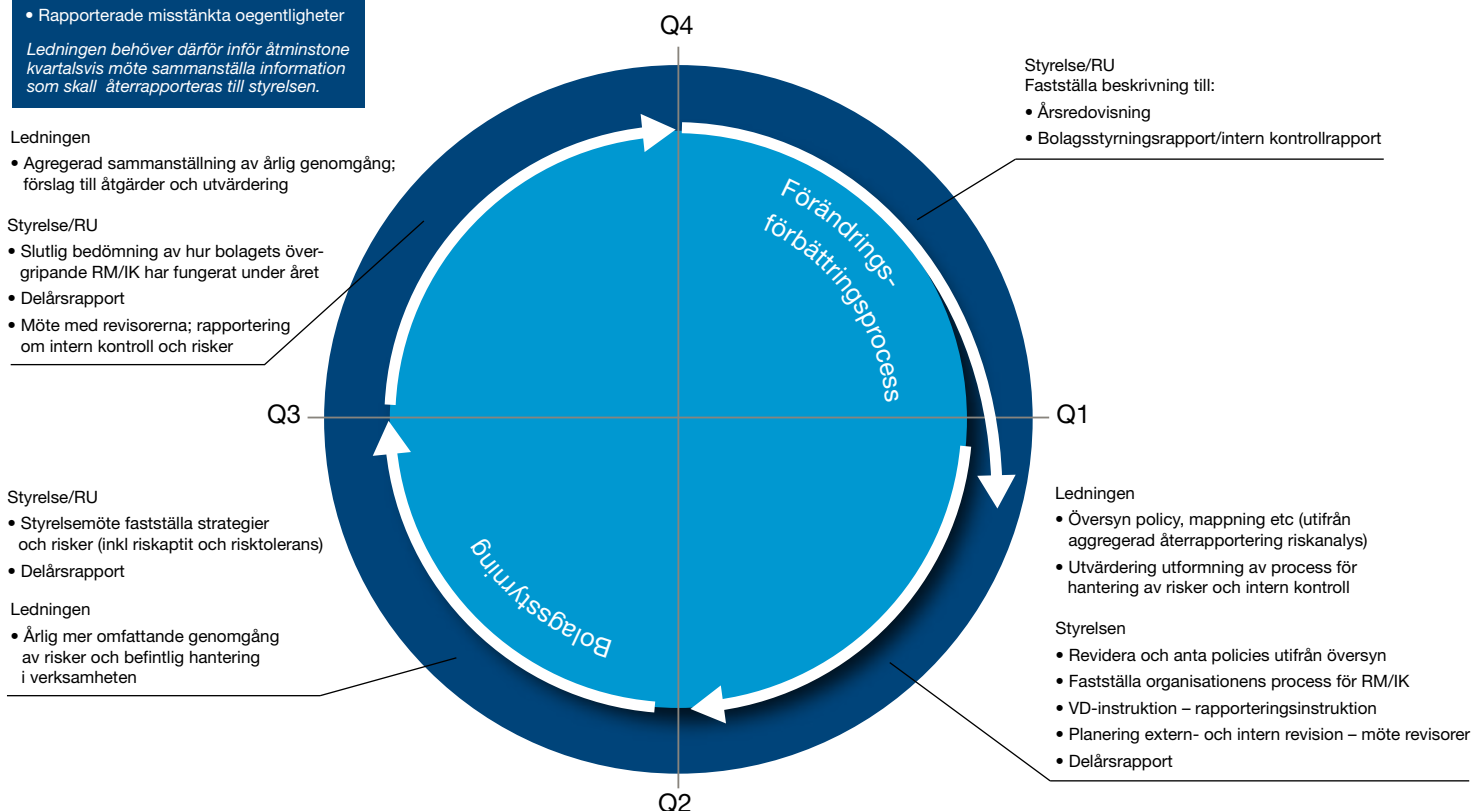
**Återkommande punkter i styrelsens/RUs agenda:**

Återrapporering riskhantering och intern kontroll, inkluderar:

- Återrapporering riskhantering och intern kontroll; Status uppföljning
- Utvärdering om ändrad riskbild/IK som föranleder åtgärd
- Rapporterade misstänkta oegentligheter

*Ledningen behöver därför inför åtminstone kvartalsvis möte sammanställa information som skall återrapporeras till styrelsen.*

### Riskhantering och Internkontroll





## Exempel på regler i koden och lagförändringar utifrån EG-direktiv beträffande riskhantering och intern kontroll

Nedan återges ett utdrag av regler som återfinns i koden samt som lagändringar utifrån EG-direktiv (extrakt av 4:e, 7:e samt 8:e direktivet) beträffande revisionsutskott, riskhantering och intern kontroll samt information om bolagsstyrning: (regler återges i förkortad form – för helheten av regeltext hänvisas till respektive lag samt till koden)

### Svensk kod för bolagsstyrning – utdrag av regler

Enligt ingress till kapitel 3 framgår att ”styrelsen ska förvalta bolagets angelägenheter i bolagets och samtliga aktieägares intresse”.

- 3.1 I styrelsens uppgifter ingår bland annat att fastställa verksamhetsmål och strategi, se till att det finns en tillfredsställande kontroll av bolagets efterlevnad av lagar och andra regler som gäller för bolagets verksamhet, se till att erforderliga etiska riktlinjer fastställs för bolagets uppträdande (se vidare Koden).

Enligt ingress till kapitel 10 i Koden framgår att ”Styrelsen ansvarar för att bolaget har god intern kontroll och formaliserade rutiner som säkerställer att fastlagda principer för finansiell rapportering och intern kontroll efterlevs samt att bolagets finansiella rapportering är upprättad i överensstämmelse med lag, tillämpliga redovisningsstandarder och övriga krav på noterade bolag.”

- 10.1 Styrelsen ska inrätta ett revisionsutskott (se vidare Koden).
- 10.2 Revisionsutskottet ska bl a ansvara för beredningen av styrelsens arbete med att kvalitetssäkra bolagets finansiella rapportering (se vidare Koden).
- 10.5 Styrelsen ska årligen lämna en beskrivning av de viktigaste inslagen i bolagets system för intern kontroll och riskhantering avseende den finansiella rapporteringen.
- 10.6 I bolag som inte har en särskild granskningsfunktion (internrevision) ska styrelsen årligen utvärdera behovet av en sådan funktion och i sin beskrivning av den interna kontrollen motivera sitt ställningstagande.

Enligt ingress till kapitel 11 framgår att ”styrelsen ska årligen i en bolagsstyrningsrapport och på sin webbplats informera aktieägare och kapitalmarknad om hur bolagsstyrningen i bolaget fungerar och hur bolaget tillämpar Svensk kod för bolagsstyrning”.

- 11.1 Bolaget ska upprätta en bolagsstyrningsrapport som ska fogas till bolagets årsredovisning.
- 11.2 Externt rapporteringskrav att i ett särskilt avsnitt i bolagsstyrningsrapporten återge styrelsens beskrivning av riskhantering och intern kontroll avseende den finansiella rapporteringen.

### Aktiebolagslagen / Årsredovisningslagen

- ABL Enlig den svenska aktiebolagslagen (kap 8) ansvarar styrelsen för bolagets organisation och förvaltningen av bolagets angelägenheter. Styrelsen ska se till att bolagets organisation är utformad så att bokföringen, medelsförvaltningen och bolagets ekonomiska förhållanden i övrigt kontrolleras på ett betryggande sätt. Styrelsen ska vidare i skriftliga instruktioner ange arbetsfördelningen mellan å ena sidan styrelsen och å andra sidan den verkställande direktören och de andra organ som styrelsen inrättar. Styrelsens ansvar och tillsynsskyldighet kan inte överlåtas på någon annan. Styrelsen ska fortlöpande bedöma bolagets och, om bolaget är moderbolag i en koncern, koncernens ekonomiska situation.
- ABL Lagförändring kap 8 Aktiebolagslagen – ett nytt avsnitt om revisionsutskott införs. Av lagen framgår att noterade bolag som huvudregel ska ha ett revisionsutskott samt reglering av revisionsutskottets uppgifter.
- ÅRL Lagförändring kap 6 Årsredovisningslagen – avseende lagstadgat krav på bolagsstyrningsrapport.
- ÅRL Kap 6 § 6 punkt 3 Förvaltningsberättelsen ska bl a innehålla företagets framtida utveckling inklusive en beskrivning av väsentliga risker och osäkerhetsfaktorer.

[www.pwc.com/se](http://www.pwc.com/se)

PricewaterhouseCoopers i Sverige är marknadsledande inom revision, redovisning, skatt och affärsrådgivning med 3 400 medarbetare och kontor på 125 orter runt om i landet. Med erfarenhet och unik branschkunskap utvecklar vi värden för våra 60 000 kunder vilka utgörs av globala företag, svenska storföretag och organisationer, mindre och medelstora, främst lokala företag samt den offentliga sektorn.

PricewaterhouseCoopers i Sverige drivs som en självständig och oberoende juridisk enhet. Vi ingår i det globala nätverket PricewaterhouseCoopers som är världens största nätverk inom revision, skatte- och affärsrådgivning. Vi delar våra kunskaper, erfarenheter och lösningar med 155 000 medarbetare i 153 länder för att utveckla nya perspektiv och praktiska råd.

Kontaktpersoner:

Katja Severin Danielsson  
[katja.severin.danielsson@se.pwc.com](mailto:katja.severin.danielsson@se.pwc.com)  
tel 08-555 334 25

Ansgar Toscha  
[ansgar.toscha@se.pwc.com](mailto:ansgar.toscha@se.pwc.com)  
tel 08-555 330 74