

Styrets risiko- og kontroll-oppfølging: Hva er status etter de nye EU-kravene?



Frem til sommeren 2008 regulerte allmennaksjeloven, regnskapsloven og Norsk Anbefaling for Eierstyring og Selskapsledelse (NUES) hva styret i børsnoterte selskap skulle foreta seg i forhold til risikostyring og kontrolloppfølging. Med virkning fra juni 2008 har EU kommet med to nye direktiv som skjerper kravene.

Av Kjersti Lothe og Jonas Gaudernack



EU krever at styret skal etablere et revisjonsutvalg som overvåker virksomhetens generelle risikostyring og internkontroll. Videre skal styret avgi en redegjørelse om eierstyring og selskapsledelse, herunder hovedelementene i selskapets internkontroll og risikostyringssystemer knyttet til finansiell rapportering. Direktivene er i ferd med å implementeres i norsk rett, og mange selskap erfarer at man må etablere en bedre struktur rundt styret hvis man skal tilfredsstille kravene. Er ditt styre forberedt?

Krav i aksjelovgivningen

Hovedelementene i norske styrers ansvar for risikostyring og internkontroll kan leses ut av aksjelovgivningen § 6-12 (forvaltningsansvaret) og § 6-13 (tilsynsansvaret). I tillegg stiller § 3-4 krav til styrets overvåkning av vesentlige risikoforhold i forhold til selskapets virksomhet og kapital. Essensen i kravene er at styret har en strategi- og organiseringsoppgave hvor det bestemmes hva man vil og hvordan man skal komme dit. Deretter har styret et ansvar for å føre tilsyn med at fastsatte mål oppnåes og at risikoen og kapitalen er forsvarlig. Aksjelovgivningen sier lite

om hvilken grad av formalisering som trengs for å oppfylle et slikt tilsynsansvar.

Krav i regnskapsloven

Regnskapsloven § 3-3a krever at årsrapporten inneholder en *"beskrivelse av de mest sentrale risiko og usikkerhetsfaktorer"*. For børsnoterte foretak krever verdipapirhandelloven § 5-6.4 en tilsvarende beskrivelse i halvårsrapporten. Kravene om en beskrivelse innebærer implisitt en forventning om at den som beskriver (dvs. styret og daglig leder) har oversikt over risiko og usikkerhet.



Foto: Bård Gudim

Jonas Gaudernack, direktør, og Kjersti Lothe, senior manager, jobber begge ved PricewaterhouseCoopers' kontor i Oslo.

virksomhet. Internkontrollen og systemene bør også omfatte selskapets verdigrunnlag og etiske retningslinjer.

2. Styret bør årlig foreta en gjennomgang av selskapets viktigste risikoområder og den interne kontroll.
3. Styret bør i årsrapporten gi en beskrivelse av hovedelementene i selskapets interne kontroll og risikostyringssystemer knyttet til dets finansielle rapportering.

Krav i NUES

NUES¹ kapittel 10 omhandler styrets ansvar for risikostyring og internkontroll. Anbefalingen er en presisering, altså ikke utvidelse, av aksjelovens regler om styrets tilsynsansvar. En rimelig antakelse er dermed at anbefalingens innhold kan være relevant for alle norske styrer. Hovedessensen i anbefalingen er som følger:

1. Styret skal påse at selskapet har god intern kontroll og hensiktsmessige systemer for risikostyring i forhold til omfanget og arten av selskapets

Ut fra NUES kan vi tolke at det i styrets tilsynsansvar ligger et ansvar for å overvåke faktiske risikoforhold og relaterte kontroller. Årsaken til at det er viktig å forstå kontrollene er at det er residualrisikoen (altså gjenværende risiko etter at man har iverksatt kontrolltiltak) som er den reelle eksponeringen for selskapet. I tillegg er NUES tydelig på at styret skal overvåke kontroll- og risikostyringssystemene. Dette betyr at styret skal sørge for at de oppnår oversikt over risiko og kontroll på en robust måte: "Hva vet vi og hvordan vet vi det" – er et godt kontrollspørsmål for styremedlemmer. Selv om styret må

¹NUES er Norsk anbefaling for Eierstyring og Selskapsledelse (se www.nues.no). Børsdirektivet krever at børsnoterte foretak følger anbefalingens krav om å redegjøre for om og hvordan man følger anbefalingen.

²Revisjonsdirektivet definerer foretak av allmenn interesse som foretak som har utstedt omsettelige verdipapirer som er opptatt til handel på et regulert marked i EØS-land, banker og andre kredittinstitusjoner, samt forsikringsselskap. Den førstnevnte gruppen vil i Norge pr. i dag utgjøre foretak med

omsettelige verdipapirer notert på Oslo Børs og Oslo Axess.

³NUES krever redegjørelse i årsrapporten mens 4-direktiv krever redegjørelse i årsberetningen. Dette vil forhåpentligvis koordineres innen årsoppgjøret.

overvåke den generelle risikostyringen og kontrollen, må man i årsrapporten kun redegjøre for den delen av systemene som er relevant for finansiell rapportering. I tillegg kommer regnskapslovens krav om å beskrive sentrale risiko og usikkerhetsfaktorer.

EU krav: 4. og 8. direktiv

EUs 4. og 8. direktiv omhandler krav til risikostyring, internkontroll og finansiell rapportering, altså mye av det samme som aksjelovene og NUES. Direktivene forventes implementert i norsk rett innen utgangen av 2008. Felles for direktivene er at de rettes mot styret for å bidra til større involvering. Direktivene gjelder selskap av allmenn interesse.²

Årsregnskapsdirektivet (4. direktiv) krever at styret i årsberetningen redegjør for eierstyring og selskapsledelse og gir

en beskrivelse av hovedelementene i selskapets internkontroll og risikostyringssystemer relatert til finansiell rapportering. Bortsett fra plassering er det altså intet nytt i forhold til eksisterende krav i NUES.³

Revisjonsdirektivet (8. direktiv) krever at det skal opprettes revisjonsutvalg. Dette er nytt som lovkrav. Utvalget skal bestå av styremedlemmer og minst én person må være uavhengig av foretaket og ekspert på revisjon/regnskap. Utvalgets oppgaver overlapper med det NUES pålegger styret:

- a. overvåke prosessen for regnskapsavlegging
- b. overvåke om virksomhetens interne kontrollsystem og risikostyringssystemer fungerer effektivt. Dersom foretaket har

etablert internrevisjon, skal overvåkingen også omfatte denne

- c. overvåke den lovpliktige revisjonen av årsregnskapet og konsolidert regnskap
- d. gjennomgå og overvåke revisor eller revisjonsselskapets uavhengighet, særlig med tanke på levering av andre tjenester enn revisjonstjenester

Det er rimelig å anta at EUs logikk er som følger: (1) revisjonsutvalg går i dybden, (2) utvalget sammenfatter for styret, og (3) styret utgir redegjørelsen i plenum.

Praktiske konsekvenser for selskap av allmenn interesse

Den første praktiske konsekvensen av de nye EU-kravene er at man må opprette





Foto: Bård Gudim

“Hvis tilsynsansvaret skal oppfylles må systemene for risiko og kontroll være såpass formaliserte at det er mulig å overvåke dem.”

revisjonsutvalg. Deretter må styret og revisjonsutvalget gjøre en vurdering av om tilsynsansvaret i henhold til aksjelovgivning, NUES og EU-kravene er oppfylt. Det er det neppe. For å utdype denne påstanden er det formålstjenelig å skissere hva som ligger i kravene.

For det første må foretaket ha et system for risikoanalyse, implementering av risikotiltak, samt tiltaksovervåkning. Deretter må systemet overvåkes av styret og revisjonsutvalget. Styret og revisjonsutvalget må også

Nye EU-krav: **Revisjonsutvalg**

- Skal velges blant styrets medlemmer og være et underutvalg av styret
- Skal kunne vise til regnskapsfaglig eller revisjonsfaglig bakgrunn hos minimum ett av medlemmene. Denne personen må også være uavhengig av foretaket

Skal overvåke:

- Effektiviteten i virksomhetens risikostyringssystem, internkontrollsystem og evt. internrevisjon
- Prosessen for finansiell rapportering
- Den lovpliktige revisjonen av årsregnskapet, og revisors uavhengighet

Nye EU-krav: **Styrets Redegjørelse**

- Skal offentliggjøres årlig som en egen og klart atskilt del av styrets årsberetning. Innholdet tilsvarer rettledningen som følger av NUES
- Skal vurderes av selskapets eksterne revisor med hensyn på konsistens mot revisjonen av årsregnskapet. Revisor skal ikke avgi en eksplisitt erklæring over effektiviteten i internkontrollen (som Sarbanes-Oxley reglene krever)

Skal inneholde:

- En uttalelse om foretakets eierstyring og selskapsledelse, og hvilket rammeverk foretaket følger på området
- En beskrivelse av hovedelementene i selskapets risikostyringssystemer og internkontroll over foretakets finansielle rapportering

overvåke faktiske risikoforhold og kontrolltiltak. Videre må det gjøres rede for de faktiske risikoforholdene i årsrapporten og halvårsrapporten. Til slutt må hovedelementene i selskapets internkontroll og risikostyringssystemer relatert til finansiell rapportering beskrives i årsrapporten/årsberetningen.

Hvis tilsynsansvaret skal oppfylles må systemene for risiko og kontroll være såpass formaliserte at det er mulig å overvåke dem. Det bør videre være en viss formalisering rundt styrets og revisjonsutvalgets overvåkning, slik at de kan underbygge at de har oppfylt sine plikter og at redegjørelsen er basert på forsvarlig saksbehandling. I praksis bør styret gjennom en instruks til daglig leder bestemme hvordan de vil at systemet skal se ut og overvåkes, samt hvordan styret vil ha informasjon. Det er også rimelig å anta at revisor vil vurdere design og implementering av systemet, da styrets og selskapets overvåkning

av risiko og kontroll vil være relevant for revisjonen.

I praksis bør man derfor få på plass skriftlige retningslinjer for risikoanalyse, risikohåndtering og tiltaksovervåkning, og styrets, revisjonsutvalgets og daglig leders rolle bør beskrives i et instruksverk. På denne måten blir det mulig å faktisk føre tilsyn og å underbygge innholdet i en redegjørelse.

Praktiske konsekvenser for andre selskap

NUES- og EU-kravene gjelder tilsynelatende bare selskap av allmenn interesse. Vanlige norske AS/ASA har derfor ikke krav på seg til å opprette revisjonsutvalg og utgi en redegjørelse om risiko og kontrollsystemene over finansiell rapportering. Begge deler kan imidlertid gjøres og må kunne sies å være beste praksis. Når det gjelder tilsynsansvaret er derimot bildet mer

komplisert. NUES angir at anbefalingen er en presisering av aksjelovgivningens tilsynsansvar, ikke en utvidelse. Derfor bør nok styremedlemmer i vanlige norske AS/ASA se på de nye reglene for å få bedre innblikk i hva som ligger i styrets tilsynsansvar, samt vurdere om ansvaret er oppfylt.

For ytterligere informasjon, kontakt:

jonas.gaudernack@no.pwc.com 952 60 769
kjersti.lothe@no.pwc.com 952 60 184

Forslag til god internkontroll

Risikoanalyse

- Rammeverk for risikoanalyse (risikomodell, vurderingsskala, begrepsapparat, malverk etc)
- Prosess for risikovurdering (identifikasjon, analyse og kommunikasjon til styret)

Etablering og implementering av risikotiltak/kontroll

- Retningslinjer for etablering av tiltak/kontroller (hvem beslutter, dokumentasjon, malverk)
- Struktur for kommunikasjon og evt opplæring i tiltak (f.eks intranett, håndbøker)
- Systematikk for å vedlikeholde/oppdatere/sanere styrende dokumenter

Oppfølging av risikotiltak/kontroll

- Systematikk for identifikasjon av tiltak/kontroller som skal overvåkes

- Systematikk for identifikasjon og overvåkning av kontrollbevis (dvs informasjon som viser om tiltak fungerer/svikter)
- Retningslinjer for kommunikasjon av avvik til ledelse/styre, samt oppfølging av avvik

Anbefalt grad av formalisering

- Formell styreinstruks, med retningslinjer for innhold i styrets arbeidsplan, sakspapirer og styrereferater
- Formell instruks til daglig leder, med retningslinjer for hvordan styrets overordnede retningslinjer for risikostyring og internkontroll skal iverksettes, samt hvordan styret skal holdes orientert for å kunne overvåke prosessen
- Formaliserte nøkkelkontroller på ledelsesnivå
- Formaliserte nøkkelkontroller på transaksjonsnivå