Hvorfor bør styret stille tydeligere krav til risikostyringen?

AV
OLE MARTIN KJØRSTAD

Ole Martin Kjørstad er Senior Manager i BDO Advisory der han har hovedansvar for internrevisjon. Som prosjektleder har han bred erfaring fra ulike fra revisjons- og rådgivningstjenester, primært innenfor risiko- og virksomhetsstyring. Han er opptatt av at risikostyring skal være et målfokusert og reelt ledelsesverktøy, med fokus på praktiske løsninger og gode kommunikasjonsmekanismer. Ole Martin er også del av arbeidsgruppen som på vegne av IIA Norge utarbeider en Veileder for Risikostyringsfunksjonen.

Styret i en virksomhet har et lovfestet ansvar for å sørge for forsvarlig drift av virksomheten. Dette omfatter ansvaret for virksomhetens risikostyring, som til dels er definert i mer detalj av ulike organisasjoner og bransjespesifikke reguleringer. Blant annet presiserer NUES 10[1] at styret selv må danne seg en oppfatning av virksomhetens internkontroll, basert på informasjon som blir forelagt styret. Andre føringer, slik som Finanstilsynets veiledning til forskrift om risikostyring og internkontroll[2], sier først og fremst noe om rapportering fra ledelsen til styret. Dette er i seg selv bra, men verdien av slik rapportering er unektelig betinget av ledelsens evne og mulighet til å fange informasjon som er vesentlig for styret. Videre må man spørre seg om periodisk rapportering er tilstrekkelig for å sikre tidsriktig håndtering av potensielt vesentlige risiki.

Når man som styremedlem har ansvar for å sørge for forsvarlig drift har man i siste instans også ansvar for alt som skjer i virksomheten – inkludert forhold man ikke kjenner til. Når det er tilfellet, burde ikke god risikostyring handle om noe mer enn å vurdere virksomhetens risiko basert på den informasjonen man blir forelagt?

Jeg mener at et styre som skal ivareta dette ansvaret aktivt må se til at det etableres mekanismer som er egnet til å identifisere og kommunisere vesentlig informasjon til rett nivå i organisasjonen. For styrets del skal dette gi trygghet for at informasjon som er vesentlig for dem å ta stilling til blir kommunisert løpende. Med andre ord er det vel så viktig å ta et eierskap til den metodikken ledelsen og selskapet jobber etter, som å stille krav til innholdet i periodisk rapportering. Skal risikorapporteringen gi trygghet som beslutningsgrunnlag, må styrets medlemmer også føle seg komfortable med at den er så fullstendig, presis og nyansert som mulig.

Hva kjennetegner god risikostyring?

God risikostyring handler ikke om hvor mange analyser som er gjennomført eller hvor ofte man rapporterer. Det handler om mer enn å vurdere sannsynlighet og konsekvens knyttet til uønskede hendelser. God risikostyring handler om å legge til rette for at organisasjonen skal kunne ta velinformerte beslutninger og fokusere på de aktivitetene som maksimerer måloppnåelsen. Kort sagt kan man si at det handler om å skape trygghet for at virksomhetens strategi operasjonaliseres på best mulig vis samtidig som man ivaretar gjeldende interne og eksterne krav.

Dette bør som nevnt stå svært høyt på styrets agenda. Men hvordan skal man vurdere hvorvidt virksomheten har mekanismer som ivaretar dette på en god måte? Dette er lettere sagt enn gjort og vil fortone seg svært forskjellig avhengig av bransje og selskap. Jeg mener likevel det er noen nøkkelfaktorer som er generiske. Dette tegner selvfølgelig ikke et fullstendig bilde av hva som kjennetegner god risikostyring. Temaene kan imidlertid være til hjelp når man som styremedlem eller internrevisor skal vurdere hvordan risikostyringen i virksomheten er organisert og ivaretatt.

Organisering og tydelige roller med reelt mandat og ansvar

Vi har en tendens å umiddelbart tenke på metodikk for risikovurderinger og rapportering når det er snakk om risikostyring. Minst like viktig er imidlertid hvordan man organiserer arbeidet. Roller og ansvar må defineres på et vis som sikrer ivaretakelse av risikostyringsprosessen, hensiktsmessige rapporteringslinjer og nødvendig integritet i arbeidet. Dersom dette ikke er på plass, er det vanskelig å

[1] *Norsk utvalg for eierstyring og selskapsledelse (NUES) www.nues.no*
[2] *Finanstilsynet, Rundskriv 3/2009 - Veiledning til forskrift om risikostyring og internkontroll*

implementere en risikostyringsprosess som tilfører virksomheten verdi.

Selve ansvaret for virksomhetens risikostyring og internkontroll kan ikke delegeres bort fra styret og daglig leder. Det operative ansvaret for selve prosessen er imidlertid en krevende oppgave i seg selv. Dette ansvaret må derfor være reelt og ligge på tilstrekkelig høyt nivå i virksomheten. Videre bør det være direkte rapporteringskanaler til toppledelsen og til styret. Uten disse kanalene vil man kunne begrense verdien av løpende rapportering. Tett dialog er avgjørende for at arbeidet skal kunne skje i tråd med styrets og ledelsens forventninger. Dersom avstanden blir for stor øker sannsynligheten for at fokuset til funksjonen ikke fullt ut støtter virksomhetens målsetninger.

Mange virksomheter har ikke rom for en dedikert Risk Manager. I slike tilfeller er det viktig at det likevel vies tilstrekkelig ressurser og oppmerksomhet til rollen. Dette handler vel så mye om hvordan ledelsen følger opp arbeidet, som hvilken stillingsbrøk som formelt blir allokert. Dersom resultatet av arbeidet som gjøres ikke brukes som et reelt beslutningsunderlag, er det lite trolig at arbeidet blir viet mye oppmerksomhet. Dette forutsetter så klart at informasjon som tilflyter styret og ledelsen er matnyttig. Av nettopp denne grunn er det viktig at styret og toppledelsen legger nødvendige føringer for hva de ønsker å få ut av risikostyringsarbeidet. Ofte blir det for raskt fokus på rapportering oppstrøms, uten at det er brukt tilstrekkelig tid på føringer og prinsipper for hvordan informasjon sammenstilles og rapporteres på ulike nivåer. Dersom styret og ledelsen ikke gir slike føringer, kan de heller ikke forvente at rapporteringen er tilpasset deres ønsker og behov.

Foto: Olivier Le Moal/Shutterstock

Et mål med risikostyring er å allokere ressurser best mulig i virksomheten. Den som har øverste ansvar for risikostyringsarbeidet bør derfor ha dette for hele virksomheten, for å unngå suboptimale beslutninger. Dette forutsetter at ansvaret ligger hos en som har tilstrekkelig kompetanse og kapasitet til å ha overblikk over virksomhetens samlede aktiviteter. Videre må den ansvarlige ikke ha insentiver som knytter egeninteresse tettere til resultatet i enkelte deler av virksomheten.


Foto: ImageFlow/Shutterstock

Omforent metodikk og prinsipper for rapportering

Skal risikostyringen gi verdi er et viktig premiss at informasjon om risiko systematiseres på et vis som gjør det mulig for styret og ledelsen å bruke dette som beslutningsgrunnlag. Dette forutsetter at beslutningstagere raskt kan tolke informasjonen og forstå hva som ligger bak. Skal man få til dette må det rapporteres etter prinsipper som er like for alle i virksomheten. I tillegg må det jobbes etter en felles metodikk som skaper forutsigbarhet og integritet i rapporterte data.

Identifikasjon og kvantifisering av risiko

Rapporteringsform har liten verdi dersom det underliggende arbeidet ikke er godt. Det som gjør rapporteringen verdifull, er strukturen man jobber etter for å identifisere og evaluere risiko. Måten man fanger informasjon og kvantifiserer risiko er derfor avgjørende. Hvordan man konkret kvantifiserer risiko skal jeg ikke gå nærmere inn på i denne artikkelen. Det finnes ingen universell fremgangsmåte som passer for alle. En bank beregner for eksempel kredittrisiko anderledes enn en anleggsvirksomhet rangerer HMS-risiko, og mange bransjer har egne standarder og normer for hvordan risikovurderinger skal gjøres. Den vanligste presentasjonen av risiko er en matrise som viser produktet av sannsynlighet og konsekvens. Bak dette kan det imidlertid også ligge indikatorer eller beregninger som dikterer hva som utgjør de ulike nivåene i matrisen.

Dette påvirker også hvordan man innhenter informasjon om risiko. Noen har mulighet til å hente mye informasjon direkte fra kilder som regnskap og fagsystemer, mens noen virksomheter utelukkende baserer seg på kvalitative analyser. Hva som er best vil avhenge av både ambisjonsnivå og tilgjengelighet til gode data. Ofte kan en kombinasjon være mest hensiktsmessig, men dette medfører

også et behov for gode modeller for datafangst og -prosessering. Dette er ofte nødvendig for å dekke ulike aspekter som inngår i risikoanalysen. Som eksempelet i figur 1 viser, er det ofte vanlig å vurdere risiko i lys av ulike konsekvensområder.

Uavhengig av valgt metode, er det viktig at prinsippene for hvordan man kvantifiserer er tydelige og omforent. I et konsern der man rapporter på ulike nivåer, bør det benyttes skalaer som gjør at informasjonen blir relevant for de respektive nivåene. Ledere på ulike nivåer vil ha behov for informasjon med ulik detaljeringsgrad. Det som er svært vesentlig for en avdeling eller et datterselskap er ikke nødvendigvis like alvorlig for konsernet samlet sett.

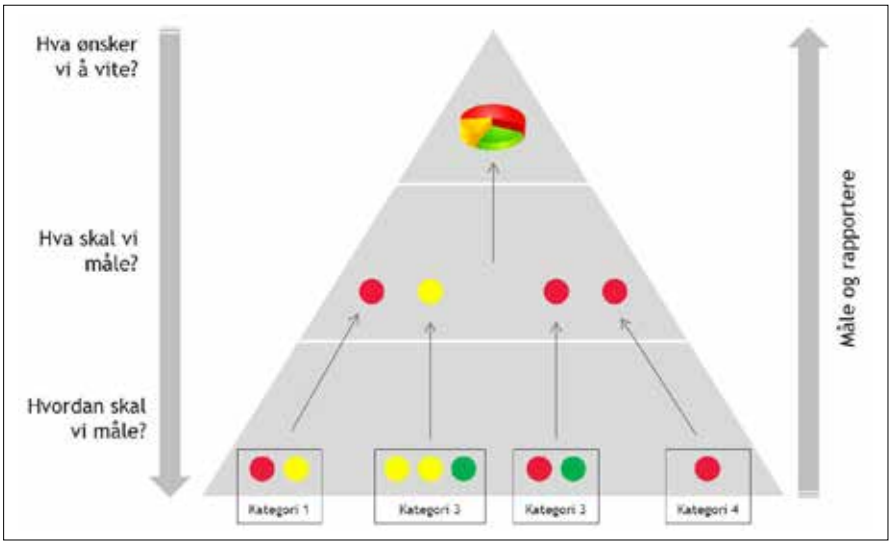
Figur 1

Presentasjon

Når det gjelder rapportering til styret og ledelsen bør man også vurdere å presentere risiko i form av et statisk sett kategorier. Til sammen bør disse kategoriene utgjøre de forholdene som er essensielle å ivareta for at virksomheten skal styres i tråd med definerte krav og målsetninger. Ved å velge en slik tilnærming kan man lettere se utviklingen i risikobildet over tid. Samtidig er det mindre risiko for at områder med et høyt antall risikoer tar uforholdsmessig mye plass i rapporteringen. Dette kan overskygge risiki som er mindre sammensatt, men potensielt mer vesentlige.

En slik tilnærming fordrer at det er definerte prinsipper for hvordan det som rapporteres under hver enkelt kategori aggregeres. Også her vil det variere hva som er mest hensiktsmessig. For noen vil det være mest interessant å se de høyeste risikoene i hver kategori, mens andre vil ha mest interesse av et vektet gjennomsnitt. Dersom man bruker sistnevnte bør rapporteringsmekanismene imidlertid være slik at mindre enkeltforhold som i seg selv kan være svært kritiske likevel blir rapportert direkte. Igjen forutsetter dette at styret og toppledelsen er involvert i utviklingen av disse prinsippene.

Figur 2 viser et enkelt eksempel på rapportering på ulike nivåer. I dette eksempelet er det den høyeste risikoen innenfor hver kategori som dikterer verdien som blir rapportert videre.



Figur 2

Risikoappetitt og -aksept

En god risikovurdering skal ta utgangspunkt i virksomhetens krav og målsetninger, og evaluere hvorvidt dagens strategi og internkontroll i tilfredsstillende grad ivaretar disse. For at virksomheten skal kunne gjennomføre slike vurderinger, må styret og ledelsens risikoappetitt være definert. Risikoappetitten sier noe om hvor mye risiko virksomheten er villig til å ta for å nå sine målsetninger.

Virksomheter som driver med kapitalforvaltning kan definere og operasjonalisere sin risikoappetitt i form av investeringsmandater. I de fleste virksomheter er det imidlertid svært vanskelig å kvantitativt definere føringer som sier hvor mye risiko ulike ledere kan forplikte virksomheten til. I disse tilfellene kan en systematisk tilnærming til risikoaksept, i form av tydelige akseptkriterier, være et godt hjelpemiddel for å overvåke at virksomhetens aktiviteter er innenfor styret og ledelsens risikoappetitt.

Når man definerer slike kriterier må man huske at målet er at risikoeksponeringen skal stå i stil med de målsetningene som er satt for virksomheten. Dersom man sier at det skal være automatikk i at risiko over et visst nivå ikke er akseptabel og derfor må reduseres kan man skape uheldige ringvirkninger. Det kan skape motstand mot selve metodikken og bidra til å skape distanse mellom risikostyrings- og strategiarbeidet. Videre kan det bidra til insentiver for å underrapportere reelle forhold. Jeg mener derfor at kriteriene som settes ikke bør være absolutte, men heller tydelig si

noe om hvem som kan akseptere ulike nivåer av risiko. For eksempel bør det være definerte nivåer som linjeleder kan akseptere før vurderingen heves til daglig leder og eventuelt direkte til styret. På denne måten blir rapporteringen også en mulighet for de med et operasjonelt ansvar til å «få aksept» fra ledelsen og styret for den risikoen som er assosiert med deres ansvarsområde. Slik kan man skape mer effektiv transparens mellom strategiske valg og de ulike risikoene valgene innebærer. Dersom en strategisk beslutning medfører vesentlig risikoeksponering i en begrenset del av virksomheten kan et slikt regime øke sannsynligheten for at informasjon raskt tilflyter styret og ledelsen. Ved å synliggjøre risikoeksponeringen som følger av virksomhetens ulike aktiviteter, mener jeg også at man kan oppnå et sterkere resultat- og oppgaveeierskap i organisasjonen.

Figur 3

Systematisk oppfølging og evaluering av utviklingstiltak

Det er en grunn til at det heter risikostyring og ikke bare risikoanalyse. Arbeidet som gjøres for å identifisere og analysere risiko er til for å gi et bedre grunnlag for å prioritere ressurser til de viktigste tiltakene og mest verdiskapende utviklingsaktivitetene – se eksempel på styringssystem i figur 3. Dersom virksomheten ikke evner å implementere og følge opp de initiativene som besluttes på bakgrunn av identifisert risiko, vil arbeidet heller ikke gi den ønskede effekten.

En god metodisk tilnærming til risikostyring inkluderer derfor tydelige prinsipper for hvordan man følger opp utviklingsarbeid i virksomheten. Metodikken bør også legge opp til en vurdering av ressursene et tiltak krever opp mot den forventede effekten. I tillegg til tydelig delegering av ansvar bør alle tiltak forankres på det nivået som er nødvendig for å sikre at tilstrekkelige ressurser faktisk blir allokert. Dette for å at tiltak skal få nødvendig fokus, hindre at ressurser brukes på tiltak som ikke realiseres og sikre at tiltak som ikke anses hensiktsmessige heller ikke igangsettes.

Foto: ESB Professional/Shutterstock

Når et tiltak er vedtatt implementert bør det være en fast systematikk i hvordan fremdrift følges opp, og ikke minst hvordan effekten av tiltaket evalueres når det er ferdigstilt. En slik systematikk skal gi styret trygghet for at nødvendige utviklingstiltak faktisk blir gjennomført og at effekten blir evaluert. Denne tryggheten mener jeg er et premiss for effektiv ivaretagelse av styrets tilsynsansvar.

Samordning med andre styringsaktiviteter

De fleste virksomheter har i ulik grad allerede etablert ulike mekanismer for ledelses- og styrerapportering. Noen har kanskje implementert balansert målstyring eller andre arbeidsmetoder som overvåker virksomhetens forretnings- og støtteaktiviteter. Risikostyringsarbeidet bør koordineres og samkjøres med slike aktiviteter. Å se på

dette som helt separate funksjoner vil være sløsing med ressurser ettersom fokuset ofte i stor grad vil overlappe. Både risiko- og målstyring handler tross alt om hvordan man fanger informasjon om forhold som påvirker usikkerhet knyttet til topp- og bunnlinjen i virksomheten. Dette skal igjen være grunnlaget for å se hvordan denne usikkerheten best håndteres.

Riktig bruk av støtteverktøy

Alle kan være enige om at enkel tilgang til fullstendig informasjon ved beslutninger samt strukturert oppfølging av utviklingstiltak i en virksomhet er bra. Begge deler er imidlertid lettere sagt enn gjort og krever administrative ressurser. Det krever innsats, eierskap og involvering fra flere parter. For at bedre risikostyring ikke skal være synonymt med økt administrasjon, er det viktig å bruke tilgjengelige verktøy på best mulig vis. For mange vil dette innebære å bruke eksisterende rapporteringsverktøy og -systemer mer effektivt. Noen vil også kunne dra nytte av å anskaffe et eget system som støtter opp om risikostyringsaktivitetene.

Det utvikles flere slike systemløsninger i dag. Noen av disse er dedikerte risikostyringsverktøy, mens andre er bygget med tanke på blant annet kvalitetsledelse. Det finnes også løsninger som i stor grad er skalerbare og skal kunne dekke alle fagområder under paraplyen GRC (Governance, Risk & Compliance). Dersom et system skal videreformidle informasjon til styret og ledelsen som gir noen reell verdi, må det legge til rette for at informasjon blir registrert og behandlet korrekt. Videre bør man sørge for at systemet er egnet til å automatisere oppfølging av enkle administrative oppgaver, slik som å holde oversikt over roller og ansvar for risikovurderinger samt sende påminnelser om statusoppdateringer for pågående tiltak.

Dette stiller krav til brukervennlighet og ofte mulighet for integrasjon med andre systemer. Ved en anskaffelse bør man derfor være svært bevisst på hvordan ulike interessenter i virksomheten skal benytte systemet. Systemet bør være praktisk innrettet og ikke innebære at informasjon som allerede registreres i ett system mål registreres dobbelt. Som bruker bør det være enkelt å få oversikt over status på oppgaver som man selv har ansvar for eller som omhandler eget ansvarsområde i virksomheten.

Foto: ImageFlow/Shutterstock

Risikostyring – styret og ledelsens verktøy for en mer robust virksomhet

God risikostyring handler altså om mye mer enn det å gjøre gode risikoanalyser. Det handler om å legge til rette for effektiv informasjonsflyt, tydeliggjøring av roller og ansvar, gode beslutningsmekanismer, riktig prioritering av ressurser og felles forståelse for virksomhetens målsetninger, krav og verdier. Et godt system for risikostyring representeres av summen av de aktivitetene som legger til rette for dette. Styret bør derfor aktivt søke informasjon fra ledelsen om hvordan arbeidet er organisert og følges opp, fremfor kun å etterspørre periodisk orientering om risikobildet. Gjennom dette kan styret oppnå trygghet for at relevant informasjon raskt tilflyter rett nivå og vurdere om etablerte prosesser for å identifisere, evaluere og håndtere risiko er gode nok.

For styret og toppledelsen bør risikostyring være et verktøy som skaper trygghet for at virksomheten organiseres og drives på en måte som støtter opp om definerte mål og krav. De må være komfortable med at måten det jobbes på er egnet til å fange opp, håndtere og kommunisere forhold på rett nivå i organisasjonen.

Det er dette, og ikke risikoanalysen eller rapporteringen i seg selv som skaper en mer robust organisasjon. Nettopp derfor bør styret stille tydeligere krav til krav til risikostyringen.

> Både risiko- og målstyring handler om hvordan man fanger informasjon om forhold som påvirker usikkerhet knyttet til topp- og bunnlinjen i virksomheten.