Spørsmål et styre bør stille for å forstå hvordan en virksomhet styrer sine risikoer

IIA Norge

Spørsmål et styre bør stille for å forstå hvordan en virksomhet styrer sine risikoer

OM ANSVAR FOR RISIKOSTYRING

Å inneha et verv i et styre eller innen et kontrollorgan i en virksomhet er et betydelig ansvar, og kan også medføre et betydelig *personlig* ansvar.

Formålet med denne veilederen, er gjennom et sett med spørsmål, å gi en bedre forståelse av hva som er de viktigste risikoene som påvirker selskapet og hvordan de håndteres.[1]

Det er sjeldent tilstrekkelig bare å se på et resultat og en balanse for å forstå hva som virkelig påvirker en virksomhets bunnlinje. Å forstå en virksomhets risikoprofil og hvordan virksomheten styrer denne, er en vinkling som kan være til stor hjelp for å få enda bedre forståelse av virksomheten. I denne sammenheng oppfattes risiko som et fremtidig potensial for gevinst eller tap (jf. definisjonen brukt i ISO-standarden[2]).

Alle virksomheter lever av å ta én eller flere former for risiko. Det er derfor viktig å forstå sammenhengen mellom risiko og verdi/resultat. To tilsynelatende like resultater kan ha sitt utgangspunkt i svært forskjellig risikoprofil. For å bedømme hvor godt et resultat er, er det derfor avgjørende at man forstår hvilken risiko virksomheten har tatt for å oppnå dette.

Risikobegrepet i denne sammenheng omfatter kortsiktige risikoer, gjerne med ett års tidshorisont. Kanskje enda viktigere omfattes strategiske risikoer, nemlig risikoer selskapet tar eller vil møte, som en konsekvens av sin strategi eller større endringer i geopolitiske forhold, markeder eller regulatoriske forhold.

I moderne risikostyring er det vanlig å referere til «helhetlig» risikostyring som en metode for å forstå og styre virksomhetens risiko helhetlig og ikke bare fragmentert. Denne formen for risikostyring benevnes ofte som ERM (Enterprise Risk Management). Det er mange fordeler med ERM sammenlignet med å styre enkeltrisikoer hver for seg, uten å se hvordan disse samlet sett påvirker virksomheten.

1 For ytterligere informasjon om Risikostyringens formål og praktisk utførelse, se Veileder for risikostyringsfunksjonen utgitt av IIA Norge i 2017.

2 ISO 31000:2009 - Risk Management – Principles and Guidelines (foreligger også i norsk utgave).

OM DE TRE FORSVARSLINJENE I EN GOVERNANCEMODELL

Det er viktig å definere roller og ansvar for de ulike funksjonene på en tydelig måte. Dette bidrar til effektiv ressursutnyttelse, tilfredsstillende kontroll av alle aktiviteter, hindrer duplisering av oppgaver og funksjoner (inkludert aktiviteter knyttet til risikostyring og internkontroll). Videre er dette med på å tydeliggjøre grensesnittene innad i virksomhetenes helhetlige risikostyring og internkontroll.

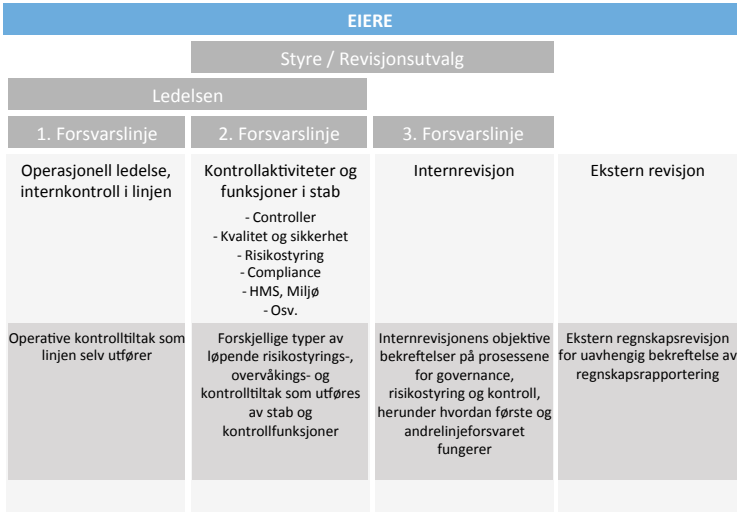
Risikostyringsfunksjonen, Compliance og øvrige andrelinjeforsvarsfunksjoner har ansvarsområder og/eller arbeidsoppgaver som grenser til hverandre. Selv om disse funksjonene er uavhengige av hverandre, er det viktig at det er god kommunikasjon mellom funksjonene for å effektivisere ressursbruken. Det kan også vurderes å samle funksjonene organisatorisk, for å styrke faglig samarbeid og gjennomføringsevne. Modellen med «de tre forsvarslinjene» (se illustrasjon under) beskriver styrings- og kontrollstrukturen i en virksomhet, herunder roller og ansvar knyttet til risikostyring og internkontroll på et overordnet nivå. Selv i virksomheter der et formelt rammeverk eller system for risikostyring ikke eksisterer, kan modellen bidra til å forbedre forståelsen av virksomhetens helhetlige risikostyring og internkontroll.

Modellen skiller mellom tre grupper (eller linjer) som inngår i effektiv risikostyring og internkontroll:

- Funksjoner som eier og administrerer risiko (førstelinjen)
- Funksjoner som fører tilsyn med risiko (andrelinjen)
- Funksjoner som gir uavhengig bekreftelse (tredjelinjen)

I markedet er det flere virksomheter som bygger bro mellom disse tre viktige komponentene innen virksomhetsstyring: Governance, Risikostyring og Compliance (samlet: GRC) for å sørge for at disse funksjonsområdene arbeider samstemt og mest mulig effektivt.

I tråd med dette har vi i dette dokumentet først delt våre spørsmål om virksomhetsstyring opp i tråd med disse tre komponentene: Governance, Risikostyring og Compliance og deretter har vi et sett med spesifikke spørsmål i forhold til risikostyring rettet inn mot henholdsvis forretningsrisiko og operasjonell risiko.



GOVERNANCE

- Hvordan er selskapets risikostyringsfunksjon organisert? Er det overlatt til den enkelte linjeenhet og kun det, eller finner man også en ERM-funksjon som ivaretar helheten i virksomheten.

  Bakgrunn: For å forstå om selskapet styrer sin virksomhet basert på et helhetlig bilde av de risikoer selskapet er eksponert for eller kun deler av dette.

- Hvordan rapporterer de risikoansvarlige i virksomheten? Kun til administrasjonen eller til styret, risiko-/revisjonsutvalget, eller begge deler?

  Bakgrunn: Dersom styret skal kunne stole på robustheten i risikostyringen er det en forutsetning at det er høy grad av faglig integritet hos de som har ansvar for funksjonen samt at det er rom for direkte kommunikasjon til styret hvis risikostyringsfunksjonen ikke skulle dele administrasjonens syn i en kritisk situasjon/sak etc.

- Er virksomhetens risikostyring og internkontrollprosesser tilpasset virksomhetens mål og policyer?

  Bakgrunn: Det er viktig at både policyer og prosesser er avstemt mot strategi og tilhørende risikoer.

- Er tilstrekkeligheten av ressurser innenfor risikostyring regelmessig vurdert opp mot behov og sammenligning med tilsvarende virksomheter?

  Bakgrunn: Det er viktig for styret å forstå om virksomhetens har vurdert om ressursene er i tråd med omfang og ambisjoner som er nødvendige i risikostrategien.

RISIKOSTYRING

- Hvordan er kompetansen og den faglige integriteten til de risikoansvarlige vurdert? Finnes det systematisk opplæring/utviklingsmuligheter innenfor risikostyring for ledere og risikostyringsmedarbeidere?

  Bakgrunn: Det er viktig for styret å forstå om virksomheten utvikler tilstrekkelig kompetanse på dette fagområdet.

- Hvilke tiltak har toppledelsen iverksatt for å bygge opp under en sunn risikokultur? Er risikoeierskap klart delegert?

  Bakgrunn: Det er viktig at det ikke oppmuntres til ansvarsfraskrivelse eller en usunn risikoadferd, for eksempel gjennom bonus og belønningssystemer som gir sub-optimale insentiver.

- Deler Risikostyring og internrevisjon informasjon regelmessig?

  Bakgrunn: Det er viktig at virksomhetenes internrevisjons- og risikostyringsfunksjon har en god og åpen dialog. Internrevisjon er gjennom internasjonale standarder (utgitt av IIA) pliktet til å forholde seg til virksomhetens risikobilde gjennom krav til å:

– *utarbeide en risikobasert internrevisjonsplan*
– *vurdere virksomhetens strategier, mål og risikoer*
– *arbeide for å forbedre prosessene for governance, risikostyring og kontroll*
– *sørge for at rapportering til toppledelse og styret også omfatter vesentlige risikoer.*

- Er det vurdert hvordan risikostyringssystemet skal integreres med øvrige deler av internkontrollsystemet og hvordan Risikostyringsfunksjonen skal samordne sitt arbeid med andre kontrollfunksjoner, for eksempel Compliance, kvalitetsrevisjon og internrevisjon?

  Bakgrunn: Det er viktig for styret å forstå om relaterte fagmiljøer samarbeider for å unngå duplisering av arbeidsinnsats, blanding av roller, utvikling av dupliserende terminologi m.m.

- Hvordan kommuniseres risikobildet til styret, både i form (kvantitativt/kvalitativt), innhold og hyppighet?

  Bakgrunn: Dette er viktig for å forstå hvor tett på styret har mulighet til å være. Er risikoinformasjonen tilstrekkelig til at styret kan agere før det uheldige skjer, eller må styret konstatere i ettertid at noe har skjedd?

- Hvordan er vesentlige nye risikoer som oppstår, samt vesentlige kontrollsvakheter, kommunisert og rapportert til ledelsen og styret?

  Bakgrunn: Det er viktig at endringer i risikobildet som skjer på bakgrunn av eksterne faktorer og svakheter som blir avdekket, kommuniseres til ledelsen og styret. Det er vanlig å ha et system for å registrere vesentlige tapshendelser og at hendelsene formidles videre til ledelsen og styret.

COMPLIANCE

- Er virksomhetens Compliancefunksjon en del av en stabsenhet som rapporterer høyt nok opp i organisasjonen? Hvis ikke, hvor rapporterer Compliance?

  Bakgrunn: Det er viktig for styret å skjønne hvor ansvaret for virksomhetens compliance ligger og om dette drives uavhengig av virksomhetens risikostyring for øvrig.

- Er compliancefunksjonen, uansett organisering, ansvarlig for å følge opp både interne og eksterne krav og retningslinjer? Hvilke krav og retningslinjer (interne og eksterne) ligger under Compliance sitt ansvarsområde?

  Bakgrunn: Det er viktig for styret å forstå omfanget av compliance, hvem som faktisk har ansvaret hvis det er delt, hva compliance har som fokus og hvordan dette kommuniseres.

STYRING AV FORRETNINGSRISIKO

- Har virksomheten en overordnet risikostrategi og hvem er ansvarlig for denne strategien?

  Bakgrunn: Det er viktig for styret å forstå om virksomheten ser på risikostyring som en strategisk og integrert del av forretningsutviklingen.

- Har virksomheten etablert en uttalt risikoappetitt som er helhetlig og kvantifiserbar?

  Bakgrunn: Det er viktig for styret å forstå både hvorvidt dette er gjort i det hele tatt og hvis det gjort, hvor mye av virksomhetens bunnlinje og risikokapital er bundet opp som følge av risikobildet.

- Hva er virksomhetens viktigste verdidrivere?

  Bakgrunn: Det er viktig for styret å forstå hvor de store verdiene genereres for å gjøre det enklere å danne seg en oppfatning av hvilke risikoer som kan påvirke verdiene, både positivt og negativt.

- Har virksomheten kvantifisert de risikoene som påvirker virksomhetens viktigste verdidrivere og er det en fornuftig sammenheng mellom allokert risikokapital og forventet verdiskaping?

  Bakgrunn: En kvantitativ forståelse sikrer et enhetlig språk som de fleste forstår. En million USD er det samme for alle, mens gult på et risikokart er mer åpen for tolkning. Et kvantitativt begrep sikrer også at man lettere ser sammenhengen mellom verdiskapning og hva man risikerer å tape for å oppnå verdiskapningen.

- Hva er virksomhetens strategi i forhold til de viktigste verdidriverne innenfor en kortere og mer strategisk horisont?

  Bakgrunn: Nyere forskning viser at mange virksomheter kun har fokus på de nærmeste månedene, mens det som virkelig gir effekt, er hva som skjer med de strategiske risikoene. Strategiske risikoer har ofte stor effekt, men får likevel liten oppmerksomhetfordi de er vanskeligere å si noe om og det kreves et visst samarbeid mellom strategienhet og risikostyring (noe som etterhvert blir mer og mer vanlig).

- Er det utarbeidet styrings- og sikringsstrategier og vurderes disse i forhold til å sikre seg mot svingninger i regnskapsrapportering eller i forhold den totale økonomiske stillingen? Tar f.eks. virksomhetens risikostyring hensyn til skatteeffekter?

  Bakgrunn: regnskapsregler for sikring kan til dels være lite fleksibel og behøver ikke å samsvare med sikring av virksomhetens overordnet økonomisk eksponering f.eks. fra etøkonomisk synspunkt bør styring av risiko foregå etter skatt fordi det gir lite mening å beskytte mere av resultatet enn det selskapet sitter igjen med etter skatt.

- Tar kommunikasjonen fra administrasjonen sikte på å være proaktiv eller reaktiv i risikokommunikasjonen?

  Bakgrunn: For å kunne forstå og påvirke den strategiske utviklingen er det viktig å få fremtidsrettet informasjon. På denne måten kan et styre i større grad være en bidragsyter og ta eierskap til viktige beslutninger i forkant.

- Har beslutningsdokumenter, både til ledelse og styret, tilstrekkelig fokus på at risikodimensjonen i beslutningen er tilstrekkelig belyst? I store saker bør både utfallsrom og sannsynlighet være en del av beslutningsdokumentet fra et risikoperspektiv.

Bakgrunn: Å få frem et mest mulig objektivt risikobilde er avgjørende for at et beslutningsunderlag skal være relevant.

- Har virksomheten store posisjoner/eksponeringer som kan gi betydelige forskjeller mellom økonomisk resultat og regnskapsresultat?

  Bakgrunn: Som en følge av regnskapsreglene kan det oppstå vesentlige forskjeller mellom et økonomisk resultat og et regnskapsresultat, for eksempel ved valutasikring av fremtidige valutainntekter eller -kostnader.

STYRING AV OPERASJONELL RISIKO

- Har virksomheten drøftet hvilke operasjonelle risikoer som har størst innflytelse på bunnlinjen?

  Bakgrunn: det er viktig å avklare og avstemme at man faktisk har en formening om hva som utgjør risikobildet og hva de ulike risikoene representerer, samt ha en omforent oppfatning av hva dette betyr for virksomheten.

- Har selskapet etablert kontinuitetsplaner / «Business Continuity Plan» (BCM) på basis av en risikovurdering?

  Bakgrunn: Det er viktig at man evaluerer verdikjeden og ser til at det finnes planer/reservedeler m.m. for så raskt som mulig å bringe verdikjeden i funksjon igjen etter en hendelse. Dette sparer virksom heten for unødig lang nedetid og vil virke positivt iforhold til forsikring og dekning i markedet.

- Finnes det katastrofescenarioer?

  Bakgrunn: Alle virksomheter bør ha tenkt gjennom hva som ville kunne defineres som en katastrofe for egen virksomhet, og hva det kan bety for bunnlinjen/verdi. Fra en slik analyse vil man kunne avsløre om man har aktiviteter som er små, men som likevel har potensiale i seg til å velte hele virksomheten selv om sannsyn-ligheten er uhyre liten. Spørsmål som reiser seg blir da - vil man ha slike aktiviteter / lønner det virkelig seg? Det er også viktig å få kartlagt slike scenarioer fordi normalt er sannsynligheten for slike hendelser så liten at de sannsynligvis aldri når opp til dokumentasjon i de overordnede risikokartene.

- Hvordan er forsikring integrert/hensyntatt i risikostyringen?

  Bakgrunn: Der man har et eget "captive" forsikringsselskap, er forsikringen avstemt mot hva som er virksomhetens overordnet behov, eller er arbeidsfeltet noe forsikringsspesialistene selv definerer? I en virk-somhet bør ansvarlig for forsikringer og risk manager arbeide tett sammen.

Denne veiledningen er utarbeidet av
Nettverk Risikostyring som er en del av IIA
Norge. 1. utgave utgitt januar 2017.

Ønsker du mer informasjon, kontakt
risikostyring@iia.no
eller se vår hjemmeside www.iia.no/ risikostyring

IIA Norge
Postboks 1417 Vika, 0115 Oslo
Besøksadresse: Munkedamsveien 3B, 3. etg.
E-post: post@iia.no
www.iia.no