VEILEDER FOR RISIKOSTYRINGS-FUNKSJONEN

2018

IIA Norge

Veileder for Risikostyringsfunksjonen


IIA Norge

FORORD

Dokumentet "Veileder for Risikostyringsfunksjonen" er utarbeidet av en arbeidsgruppe som jobber innen fagfeltet risikostyring i ulike bransjer. Arbeidsgruppen er en ad hoc komité i Nettverk risikostyring i IIA Norge.

IIA Norge retter en stor takk til følgende personer for utarbeidelse av veileder og innarbeidelse av høringssvar:
Ayse B. Nordal, Undervisningsbygg Oslo KF
Martin W. Stevens, Gjensidige
Ole Martin Kjørstad, Norges Bank
Petter Kapstad, Equinor

Arbeidsgruppen har hatt som mål å beskrive risikostyringsfunksjonens hensikt, ansvar og oppgaver, samt forutsetninger og suksesskriterier på tvers av bransjer. Prinsippene i veilederen kan også være nyttige for virksomheter som mangler en egen Risk Manager, men som ivaretar lignende arbeidsoppgaver under en annen stillingsbetegnelse.

Målgruppen for veilederen er virksomheter som enten ønsker å etablere en risikostyringsfunksjon eller å utvikle sin risikostyringsfunksjon videre.

Fremdriften i utarbeidelse av denne veilederen har fått betydelig drahjelp fra strukturen og utforming av "Veileder for Compliancefunksjonen" utgitt av Norges Interne Revisorers Forening (NIRF) i 2015. Det rettes en stor takk til de som arbeidet frem den veilederen.

Veilederen ble først utgitt i 2017 på norsk og siden oversatt til engelsk. Veilederen har nå blitt gjort tilgjengelig og distribuert både i Norge og gjennom IIA-foreninger i Europa. Det er ikke fremkommet tilbakemeldinger som tilsier behov for vesentlige endringer, men det er i mellomtiden utgitt nye rammeverk for COSO ERM og ISO 31000. Det er hovedsakelig på dette området at oppdateringer er laget i denne 2018 versjonen av veilederen.

INNHOLD

1 INNLEDNING

1.1 Formålet med veilederen

Behovet for å etablere en helhetlig risikostyringsfunksjon varierer avhengig av bransje og virksomhet. Typiske drivere har hittil vært behov for styring og kontroll i utfordrende omgivelser hvor det har vært høy risiko for vesentlige finansielle tap, skader eller tap av menneskeliv. Dessuten finnes det flere regulerte bransjer, herunder offentlige, der det stilles konkrete krav til organisering, utforming og gjennomføring av risikostyringsaktiviteter som vil kunne stille krav utover anbefalingene beskrevet i denne veilederen. I økende grad har en sett at styring av positiv og negativ usikkerhet knyttet til volatile omgivelser og fremtidig økonomisk utvikling gjør risikostyring til et viktig strategisk verktøy. I tråd med internasjonal utvikling etableres også norske lovkrav til opprettelse av en risikostyringsfunksjon som et ledd i sunn virksomhetsstyring.

Med denne veilederen ønsker vi å beskrive gjeldende «beste praksis» for risikostyringsfunksjoner uavhengig av bransje, regelverk og størrelse på virksomheten. Veilederen dekker ikke eventuelle lovkrav, men gir en innføring i grunnleggende prinsipper for funksjonen. Individuelle tilpasninger av risikostyringsfunksjonen vil bl.a. avhenge av virksomhetens art, størrelse, kompleksitet og organisasjonskultur.

Veilederen søker også å komme med noen avklaringer og avgrensninger rundt organisering av en risikostyringsfunksjon. Dette omfatter fordeling av arbeidsoppgaver og roller mellom ulike kontrollfunksjoner i virksomheten, for eksempel internrevisjon, risikostyringsfunksjonen og compliancefunksjonen.

Internasjonalt er det utarbeidet flere bransjespesifikke veiledere, som beskriver elementer og krav som kjennetegner en effektiv risikostyringsfunksjon, tilpasset særskilte regulatoriske krav. Noen elementer er imidlertid gjennomgående, og kombinert med erfaring fra norske virksomheter danner dette grunnlaget for veilederen.

Risikostyring foregår på mange ulike nivåer i en virksomhet. Denne veilederen beskriver funksjonen for *helhetlig risikostyring*, kjent som Enterprise Risk Management (ERM). Prinsippene som blir beskrevet er imidlertid i stor grad også gyldige for de som arbeider med risikostyring innenfor et mer begrenset fagfelt eller område i en virksomhet.

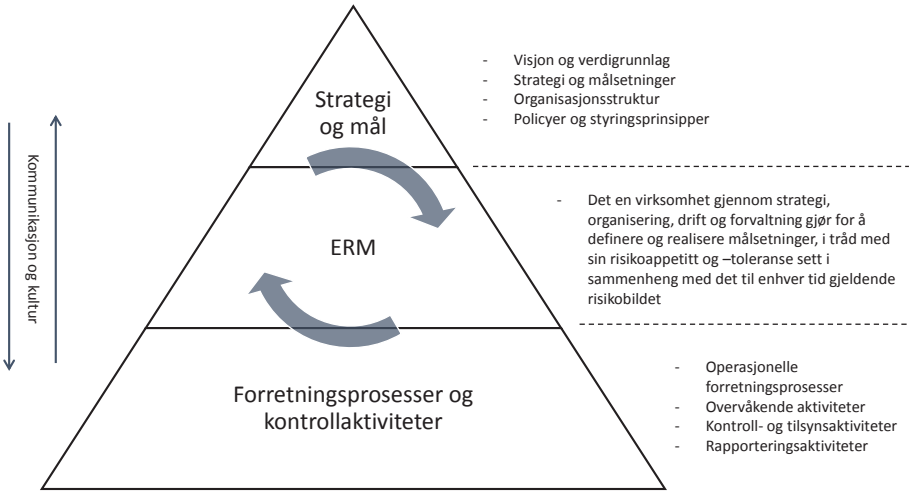
1.2 Risikobegrepet

Det å ta risiko er en naturlig del av å drive enhver virksomhet, men i beslutningsprosesser blir dette sjelden tydelig uttrykt. Begrepet *risiko* har gjerne blitt utelukkende assosiert med uønskede hendelser, og *risikostyring* blitt definert som å analysere og begrense sannsynligheten for og konsekvensen av uønskede hendelser. Dette er kun én dimensjon av det totale bildet. Det å vurdere muligheter er en like viktig komponent i helhetlig risikostyring, som det å vurdere nedsiden, da det nettopp handler om en helhet og det å evaluere risikostrategi i en portefølje av risikoer.

1.3 Helhetlig Risikostyring - Integrering med strategi og måloppnåelse

Arbeidet med risikostyring og strategi er integrerte og iterative prosesser. Målet med helhetlig risikostyring er å sikre riktig risikoeksponering, vurdert opp mot forventet/ønsket grad av måloppnåelse, i tråd med styrets og toppledelsens risikoappetitt og forretningsstrategi. Det handler om å sikre måloppnåelse gjennom utvikling av virksomheten og hensiktsmessig forvaltning av virksomhetens verdier, herunder forebygging av tap som følge av uønskede hendelser. Dette omfatter forhold på alle nivåer av virksomheten, og risikostyring må derfor være en integrert del av strategiarbeidet. En videre forutsetning for å kunne utøve god risikostyring er at det foreligger tydelig definerte mål på strategisk nivå, som målsetninger på andre nivåer i virksomheten kan knyttes opp mot. Slik kan risikovurderinger på alle nivå knyttes opp mot et målhierarki som støtter opp om virksomhetens overordnede strategi.

I praksis skal man gjennom helhetlig risikostyring sikre best mulig beslutningsgrunnlag, på ulike nivåer i virksomheten, slik at beslutninger som fattes støtter opp om overordnede målsetninger. Dernest er det viktig å ha gode mekanismer for å sikre realisering og oppfølging av de tiltak som besluttes. ERMs rolle i virksomhetsstyring er illustrert i figur 1.



Figur 1 Forholdet mellom ERM og virksomhetsstyring

Risikostyring kan defineres som systematiske, koordinerte og proaktive aktiviteter som er rettet mot vurdering og håndtering av usikkerhet og hendelser som kan påvirke virksomhetens strategi og måloppnåelse.

Dette omfatter blant annet virksomhetens evne til å:

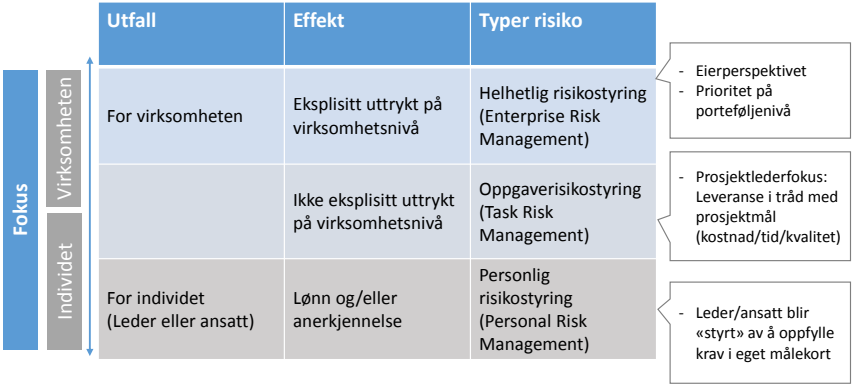
- påvirke sannsynligheten og den positive eller negative konsekvensen av hendelser
- forstå/utnytte korrelasjoner mellom ulike typer usikkerhet
- analysere utvikling i virksomheten, dens omgivelser (intern og ekstern kontekst) og risikobildet over tid
- initiere tiltak som styrer virksomheten i ønsket retning
- bygge opp en kultur som sikrer implementering av tiltak og bidrar til god risikostyring

Det forutsettes også at et helhetlig perspektiv på tvers av organisasjonsenheter, funksjoner og risikokategorier (strategiske, finansielle, operasjonelle risikoer mv.) legges til grunn, for å unngå silotenking og sub-optimalisering.

Kort sagt handler risikostyring om å fremskaffe et best mulig beslutningsgrunnlag og å legge til rette for effektiv gjennomføring og oppfølging av beslutninger. Det innebærer også å sørge for en bevisstgjøring om hva som er et akseptabelt risikonivå og nødvendig risikoeksponering.

1.4 Risikostyring på ulike nivåer

Risikostyring foregår på ulike nivåer, og avhenger av fokuset i det enkelte tilfelle. I helhetlig risikostyring er utgangspunktet på konsekvens for virksomheten. Dersom innsats rettes mot å oppnå personlige mål eller mål innenfor eget ansvarsområde vil dette kunne defineres som personlig risikostyring. Summen av personlig risikostyring i organisasjonen kan føre til sub-optimalisering, sett i lys av et overordnet virksomhetsperspektiv. Gjennomføring av oppgaverisikostyring1 bør også ta utgangspunkt i et helhetlig perspektiv, blant annet ved etablering av målsetninger og eventuelle incentivstrukturer. Disse tre ulike perspektivene: helhetlig risikostyring, oppgaverisikostyring og personlig risikostyring illustreres i figur 2.



Figur 2 Typer risikostyring[ii]

1 Med oppgaverisikostyring menes håndtering av usikkerhet i forretningsprosesser og aktiviteter, herunder prosjekter.

1.5 Forholdet mellom risikostyring, internkontroll og virksomhetsstyring

Risikostyring og internkontroll er begreper som ofte blir omtalt sammen. Ofte blir begge tolket for snevert og adskilt. Risikostyring er mer enn det å analysere og rapportere nedsiderisiko, og internkontroll handler om styring av en virksomhet og inneholder således ikke kun kontrollaktiviteter. Den amerikanske stiftelsen The Committee of Sponsoring Organizations of the Treadway Commission (COSO), har laget en definisjon av internkontroll som først ble publisert i 1992 og har fått bred aksept internasjonalt. Dokumentet kom i revidert utgave i 2013[iii]. Samme stiftelse kom også med en definisjon av helhetlig risikostyring i 2004[iv] som ble oppdatert utgave i 2017 med tittel «Helhetlig Risikostyring - Integrering med strategi og måloppnåelse».[v]

Definisjon av internkontroll	Definisjon av helhetlig risikostyring
Internkontroll er en prosess, utført av en virksomhets styre, ledelse og øvrige ansatte, utformet for å gi rimelig sikkerhet for oppnåelse av målsettinger relatert til drift, rapportering og etterlevelse[iii]	Helhetlig risikostyring er den kulturen, de egenskapene og den praksisen som organisasjoner integrerer med strategi og som de benytter når strategien settes ut i praksis. Dette for å styre risikoen når verdier skapes, bevares og realiseres[iv]

Figur 3 COSO definisjoner (tekst oversatt til norsk)

Videre lød definisjonen fra 2004 som følger: Helhetlig risikostyring er en prosess gjennomført av virksomhetens styre, ledelse og ansatte, anvendt i fastsettelse av strategi og på tvers av virksomheten, utformet for å identifisere potensielle hendelser som kan påvirke virksomheten og for å håndtere risiko slik at den er i samsvar med virksomhetens risikoappetitt, for å gi rimelig grad av sikkerhet for virksomhetens måloppnåelse [Fotnote].

Ut fra definisjonen fra kan man betrakte internkontroll som et element eller underprosess i helhetlig risikostyring. Denne underprosessen kan sies å utgjøre summen av styrings- og kontrollmekanismer.

Helhetlig risikostyring innebærer at man inntar et helhetlig perspektiv; ikke bare på virksomhetens status i øyeblikket, men også på sannsynlig positiv og negativ fremtidig utvikling. Slik er det ment å være et verktøy for balansert prioritering av ressursbruk. Derfor bør arbeidet også harmoneres med andre styringsaktiviteter, som f.eks. strategiarbeid og målstyring.

Helhetlig risikostyring bidrar til verdiskapning gjennom redusert sub-optimalisering, samt en reduksjon av usikkerheten knyttet til virksomhetens målsetninger; både de som påvirker fremtidige kontantstrømmer og ikke-finansielle målsetninger.

2 RISIKOSTYRINGSFUNKSJONEN – VIKTIGE PRINSIPPER

2.1 Funksjonens oppgaver og ansvar

I veilederen benyttes betegnelsen «risikostyringsfunksjon». Dette behøver ikke nødvendigvis å være én person, eller en fast gruppe som ikke også har andre ansvarsområder. Det viktige er at risikostyringsarbeidet representerer en systematisk og objektiv tilnærming til å identifisere, analysere og vurdere risiko, samt utforme og implementere tiltak som skal sørge for at risikoen håndteres innenfor definerte risikorammer. I tillegg skal arbeidet kunne gi faglig bistand ved utforming av strategi- og utviklingsplaner.

I en virksomhet er det styret eller øverste organ som «påser at» virksomheten har etablert forsvarlig risikostyring og internkontroll. I henhold til NUES[vii] omfatter dette bl.a. følgende:

- Å påse at selskapet har god internkontroll og hensiktsmessige systemer for risikostyring som er tilpasset omfanget av foretakets virksomhet. Internkontrollen og systemene omfatter også virksomhetens verdigrunnlag og etiske retningslinjer.
- Årlig å foreta en gjennomgang av selskapets viktigste risikoområder og internkontrollen.
- Å gi en beskrivelse av hovedelementene i foretakets internkontroll og risikostyringssystemer i årsberetningen.

Øverste leder har overordnet operativt ansvar for risikostyringen. I sitt daglige arbeid skal øvrige ledere sørge for forsvarlig risikostyring og internkontroll innenfor sine ansvarsområder, i tråd med organisasjonens målsetninger.

Risikostyringsfunksjonen skal bistå organisasjonen i arbeidet med å iverksette og implementere effektive prosesser for å identifisere, vurdere og håndtere risiko. I tillegg har risikofunksjonen et selvstendig ansvar for å overvåke risikobildet, og å flagge utviklingstrender for eksisterende risikoer og potensielt utfall av nye trusler/muligheter.[viii]

Risikostyringsfunksjonen har ansvar for å følge opp fremdriften i det samlede risikostyringsarbeidet, og for å bistå linjeledere i å formidle relevant risikoinformasjon oppover og ut i virksomheten. Funksjonen:

- Bidrar med risikostyringsteknikker og vurderinger i forbindelse med strategifastsettelse og målformulering.
- Operasjonaliserer retningslinjer for risikostyring, definere roller og ansvar og fastsette mål for gjennomføring av arbeidet.
- Utarbeider et rammeverk for risikostyring for hele virksomheten, og eventuelt for bestemte prosesser, funksjoner eller avdelinger i virksomheten.
- Fremmer risikostyringskompetansen i hele virksomheten.
- Etablerer en felles risikostyringsterminologi (f.eks. med hensyn til risikokategorier og begreper for sannsynlighet og konsekvens).
- Velger modell / verktøy for identifisering, rangering, vurdering og oppfølging av risiko inklusivt nye risikoer[vii]. Det skal bestrebes så langt det kan gjøres å kvantifisere risikoer, for dermed å gi et felles og forståelig grunnlag for prioritering og beslutninger.

- Bistår ledelsen i utvikling av *risikorapportering* og følge opp risikorapporteringsprosessen, herunder å etablere et system for tidlig varsel eller trigger-system for brudd på virksomhetens risikoappetitt eller risikorammer.
- Har løpende kommunikasjon med øverste leder og styret ut fra en selvstendig kvalifisert vurdering av strategigjennomføringen og risikostyringen.

Risikostyringsfunksjonen legger til rette for- og følger opp implementering av:

- Hensiktsmessige risikostyringsprinsipper hos ledelsen og bistå risikoeierne[xi] med å definere den planlagte risikoeksponeringen.
- Kommunikasjon av risikorelatert informasjon i hele virksomheten, herunder avgi ekspertvurderinger.
- Rapporteringslinjer som sikrer at risikorelatert informasjon når riktig instans på riktig tidspunkt og kommuniseres på en tilgjengelig og balansert måte til beslutningstagere. Risikostyringsfunksjonen bør tidlig involvere seg for å påse at risikovurderinger er hensyntatt i alle vesentlige beslutninger, samt når det er nødvendig, påvirke og utfordre beslutninger som gir opphav til vesentlig risiko.

I tillegg skal risikostyringsfunksjonen overvåke at nevnte prosesser etterleves og reagere dersom det avdekkes forhold som ikke er tilstrekkelig håndtert.

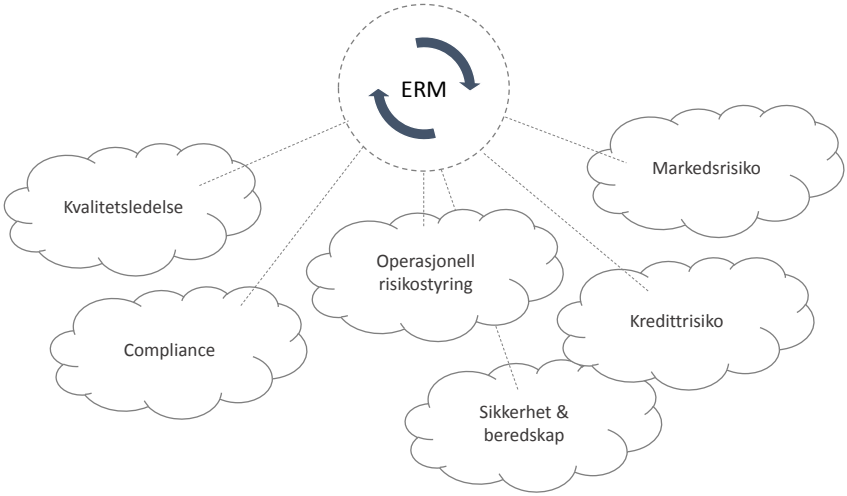
Utover den sentrale risikostyringsfunksjonen (som del av andrelinje-forsvaret), har noen organisasjoner etablert en separat etterlevelsesfunksjon (compliance) til å følge opp risiko for brudd på lover, forskrifter og retningslinjer (herunder mislighetsrisiko). Etterlevelsesfunksjonen rapporterer vanligvis direkte til toppledelsen. Det er en forutsetning at etterlevelses- og risikostyringsfunksjonene jobber tett sammen, særlig i forbindelse med juridisk risiko, omdømmerisiko, etablering av risikokultur og oppfølging av etiske retningslinjer.

Andre spesifikke oppfølgings- og overvåkingsfunksjoner kan være innenfor områdene helse, miljø og sikkerhet (HMS), innkjøp og kvalitet/ kontinuerlig forbedring. I denne sammenheng bemerkes at den oppdaterte standarden om kvalitetsledelse ISO 9001: 2015 i større grad enn tidligere (ISO 9001: 2008) krever en risikobasert tilnærming ved oppbygning av et effektivt kvalitetsledelsessystem.

Risikostyring omhandler styring av både finansiell og operasjonell risiko, som f.eks. risiko knyttet til interne prosesser, systemer, menneskelig atferd og øvrige aspekter ved virksomheten. Andre aktuelle risikoer kan være knyttet til etterlevelse av lover, regler og etiske standarder (compliance-risiko), miljørisiko mv. samt håndtering av eksterne risikoforhold, som for eksempel politisk risiko, makroøkonomiske forhold eller katastrofescenarier.

Kort sagt handler helhetlig risikostyring om å benytte en systematisk tilnærming for å legge til rette for at virksomheten samlet gjennom organisering, forretningsprosesser, kontrollaktiviteter og beslutninger kan realisere sine målsetninger.

En viktig oppgave for risikostyringsfunksjonen er derfor å påse at målsetninger er tilstrekkelig kommunisert mellom de ulike kontrollmiljøene og forankret i disse (se figur 4). Videre er det viktig å sørge for at informasjon fra disse miljøene tas hensyn til og inkluderes som del av det helhetlige risikostyringsarbeidet.



Figur 4 Eksempel på ERMs koordinering og styring av ulike risikoområder

2.2 Risikoappetitt

Risikoappetitt er det nivå av usikkerhet en virksomhet er villig og har evne til å påta seg for å kunne gjennomføre sine aktiviteter og realisere sine mål. Risikoappetitt kan defineres kvalitativt eller kvantitativt i form av fullmakts- og eksponeringsgrenser innenfor ulike risikotyper. Risikoappetitten vil variere fra virksomhet til virksomhet avhengig av strategi, bransje og organisasjonskultur. I tillegg vil lovkrav, eksempelvis aksjelovens krav for minimum egenkapital, påvirke risikoappetitten.

Det er viktig at en definert risikoappetitt kan operasjonaliseres. Det bør gå en rød tråd gjennom virksomhetens ulike mål, styringsrammer, fullmakter og handlingsrom som samsvarer med den totale risikoappetitten og strategien. I virksomheter der risikoappetitten er vanskelig å kvantifisere, er det spesielt viktig å utarbeide gode føringer for hvilke beslutningstagere som kan avgjøre hva som er riktig nivå av risiko basert på de kvalitative vurderingene som foreligger.
Risikoappetitten har både et "vilje" og et "evne" aspekt. Begrepet må ikke forveksles med det beslektede begrepet «risikokapasitet», som kan defineres som en absolutt grense på hva en organisasjon kan ta av risiko.

2.3 "Risk gaps"

"Risk gaps" er ofte brukt som et uttrykk som beskriver misforhold som kan oppstå mellom faktisk risikoeksponering og forventet avkastning (herunder samfunnsmessige gevinster). Dette kan spesielt oppstå i tilfeller der sannsynlighet for en gitt hendelse er lav, men konsekvensen er stor. En viktig oppgave for risikostyringsfunksjonen er å identifisere slike gap og sørge for at disse er kommunisert til ledelsen og styret.

2.4 Styrets ansvar og kommunikasjon med styret

Styret er ansvarlig for at virksomheten drives i samsvar med gjeldende lover og forskrifter, og for å påse at en sunn risikostyring er etablert i virksomheten. I "Norsk anbefaling for eierstyring og selskapsledelse" finnes dette uttrykt på følgende måte: "Styret skal påse at selskapet har god internkontroll og hensiktsmessige systemer for risikostyring i forhold til omfanget og arten av selskapets virksomhet" [vi]. Styret bør stille tydelige krav til risikostyringsarbeidet for å sikre at alle risikoer som påvirker måloppnåelsen håndteres tilfredsstillende. I tillegg må styret fastsette virksomhetens risikoappetitt/toleranse[2].

Det er gunstig at leder av risikostyringsfunksjonen har en direkte rapporteringsmulighet til styret. Dette kan organiseres ulikt, for eksempel ved at leder av risikostyring rapporterer til styret, eventuelt til en risiko- eller revisjonsutvalg etablert under styret. Hensikten med en slik rapportering er å sikre, ved behov, muligheten for uavhengig rapportering til styret om virksomhetens risikoforhold.

2.5 Forankring i ledelsen

Øverste leder har ansvar for å etablere og gjennomføre forsvarlig risikostyring og internkontroll med et tydelig mandat, på bakgrunn av de retningslinjer og den risikoappetitt styret fastsetter. Dette ansvaret gjelder også når risikoappetitten er vanskelig å kvantifisere. I virksomheter med mål som ikke er finansielt kvantifiserbare, må man like fullt kunne knytte usikkerhet til en skala som sier noe om potensiell effekt på grad av måloppnåelse. Eksempel på slike mål kan være et offentlig mandat eller samfunnsoppdrag, eller risikotoleranse knyttet til en virksomhets omdømme.

Risikostyringsfunksjonens organisering, ansvar, arbeidsoppgaver og fullmakter bør fastsettes i en funksjonsbeskrivelse som vedtas av virksomhetens ledelse. Den bør blant annet beskrive:

- Organisatorisk plassering, samhandling og grensesnitt mot andre kontrollfunksjoner og mot linjen.
- Mandat og ressurser som balanserer med ansvarsområder, oppgaver og fullmakter.
- Tilgang til informasjon.
- Rapporteringsansvar.

2 Grensen for hvor mye risiko virksomheten er villig til (appetitt) eller evner (toleranse) å ta.

2.6 Risikostyring, ledelse og beslutningstaking

Risikostyring og beslutninger henger sammen. Ved alle større strategiske beslutninger bør det stilles krav til å utarbeide ulike scenarioer, ved at ledelsen stiller spørsmål om utfall og alternativer ved sentrale beslutninger, ettersom usikkerheten kan være stor. Figur 5 beskriver forholdet mellom risikostyring og beslutninger, når risikostyring brukes aktivt.

Beslutningstaker	Utfallsegenskaper	Utfall
Intern beslutningstaker F.eks: Å drikke en kopp kaffe	Deterministisk	Kjent og sikker – kaffekoppen er tom
Intern beslutningstaker F.eks: Estimering av antall fremtidige studenter i kommune X	Stokastisk påvirket av tilfeldigheter	Sannsynlighetsfordeling av utfallet er kjent / kan estimeres
Intern beslutningstaker F.eks: Introdusere et helt nytt produkt i et marked	Stokastisk	Sannsynlighetsfordelingen er ukjent
Ekstern beslutningstaker – oppfattet gjennom «what if» scenarioer («known unknowns») F.eks: Opptøyer	Kaskade-, snøballeffekter, «fat tailed distribution»	«Grey Swan»
Ekstern beslutningstaker – ukjent hendelse kommer overraskende («unknown unknowns») F.eks: 9/11	Sannsynligheten kan ikke beregnes med teknikkene vi besitter i dag. Blir ikke oppdaget gjennom «what if» scenarioer	«Black Swan» 

Figur 5 Beslutninger og utfall

Denne figuren er en oversettelse av opprinnelig versjon som finnes I "Y. Ayse B. Nordal, Risk Management Practices, Decision Making and Corporate Governance, Book of Proceedings", International May Conference on Strategic Management, University of Belgrade, May 2015.

Virksomheter, institusjoner og individer blir påvirket av både egne og andres beslutninger. Det som er felles for disse er at det er knyttet usikkerhet til utfallet av en beslutning. Det er svært få beslutninger som har «sikre» utfall, dvs. er deterministiske. Et eksempel på et deterministisk utfall kan være beslutningen om å drikke en kopp kaffe. Under normale forhold kan vi forutsette at kaffekoppen vil være tom hvis vi beslutter å drikke kaffen.

Men både normale forhold og deterministiske utfall er sjeldenheter. I mange tilfeller tar beslutningstageren i en virksomhet en avgjørelse, og estimerer usikkerheten på bakgrunn av sannsynlighetsfordelinger utarbeidet på basis av historiske data, sammenlignbare data eller egen erfaring om variabler som kan påvirke utfallet. Som et eksempel kan vi tenke oss en beslutningstager i kommune X, som skal bestemme hvor mange elevplasser som trengs i kommunen de kommende årene. Vedkommende kan studere historiske data, og for eksempel vurdere effekten av befolkningsutvikling, innflytting og utflytting, vil ha på behovet for elevplasser. På basis av dette er det mulig å estimere en sannsynlighetsfordeling for effekten av de kjente faktorene, som har vist seg å være vesentlige hittil.

For en rekke beslutninger er det ikke mulig å kjenne til faktorene som kan påvirke utfallet, og dermed heller ikke mulig å utarbeide sannsynlighetsfordelinger. Et eksempel kan være en virksomhet som prøver et helt nytt produkt i et helt nytt marked. Det foreligger ikke historiske data eller sammenlignbare tall som grunnlag for en slik tilnærming. Virksomheten kjenner nemlig ikke til sannsynlighetsfordelingen til relevante faktorer.

Som tidligere nevnt vil en virksomhet påvirkes også av beslutninger som de ikke tar selv. Noen av disse kan anses som «grå svaner». Virksomheten kan tenke seg at et utfall er mulig, og kan forekomme nå eller om 100 år[3]. Virksomheten kan forberede seg til slike hendelser med scenarioøvelser som inngår i beredskapsplanleggingen.

Men virksomheten kan påvirkes også av hendelser hvor selve utfallet ikke er mulig å forestille seg med vanlig scenariotenkning. Litteraturen om «Svarte svaner» beskriver disse hendelsene. Hendelsen, utfallet og relevante variabler er fullstendig ukjente for virksomheten.

3 ORGANISERING OG AVGRENSNING MOT ANDRE FUNKSJONER

3.1 De tre forsvarslinjene

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.

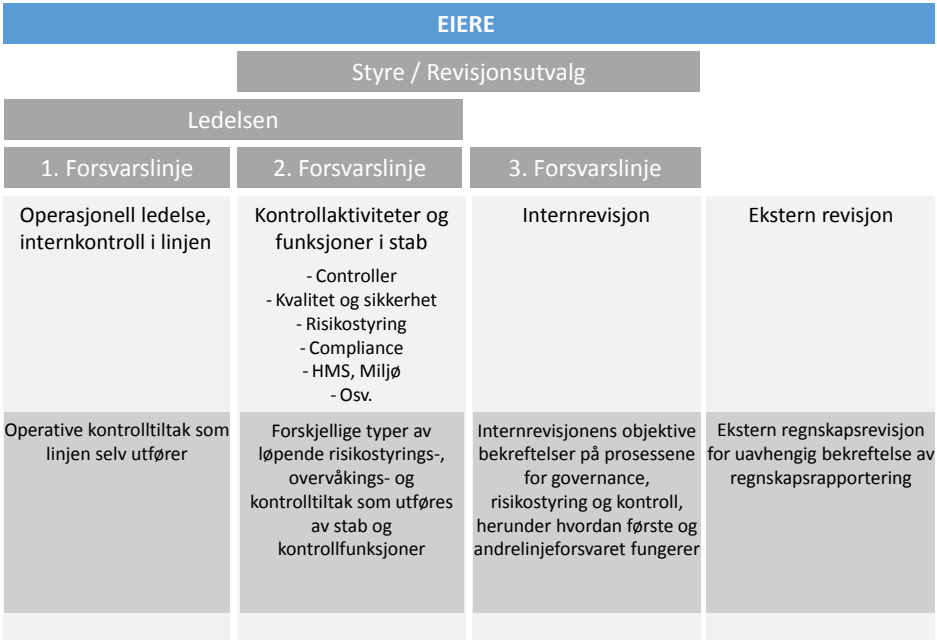
Risikostyringsfunksjonen, Compliance og øvrige andrelinjeforsvarsfunksjoner har ansvarsområder og/eller arbeidsoppgaver som grenser til hverandres områder. Selv om disse funksjonene er uavhengige av hverandre er det viktig at det er god kommunikasjon mellom disse funksjonene for å effektivisere ressursbruken. Det kan også vurderes å samle funksjonene organisatorisk, for å styrke faglig samarbeid og gjennomføringsevne.

Modellen med «de tre forsvarslinjene» (se illustrasjon figur 6) 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.

3 Slike hendelser, som f.eks. opptøyer, kan ha snøball-effekter og dermed en «fat-tailed» sannsynlighetsfordeling, der ekstreme hendelser har større sannsynlighet enn de har i normale fordelinger.

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).



Figur 6 Beskrivelse av de tre forsvarslinjene.

Første forsvarslinje eier og håndterer virksomhetens risikoer knyttet til driften og må derfor påse at tilfredsstillende internkontroll gjennomføres av medarbeidere i «linjen»; dvs. selgere, saksbehandlere og liknende funksjoner. Linjeledelsen har ansvar for å opprettholde en hensiktsmessig internkontroll hvilket innebærer eierskap til og ansvar for risikovurdering og risikohåndtering. De daglige operative kontrollaktivitetene gjennomføres vanligvis av medarbeidere i linjen, innenfor rammer fastsatt av den operative ledelsen. Det er ledelsens ansvar å etablere ulike kontroll- og oppfølgingsfunksjoner for å bidra til å bygge og/eller overvåke kontroller gjennomført av førstelinje.

Andre forsvarslinje har en rolle som er dels proaktiv og dels reaktiv. På den proaktive siden skal andrelinjen bidra til utvikling og forvaltning av for eksempel rammeverk for risikostyring, styrings- og beslutningsprinsipper samt bidra til videreutvikling av førstelinjens egne aktiviteter.
På den reaktive siden skal andrelinjen følge opp rapportering og opprettholde dialog med virksomheten. Dette med mål om å kunne identifisere forhold som avviker fra ønsket utvikling og sørge for at virksomheten fokuserer og reagerer på dette.

Støtte- og kontrollaktivitetene i andrelinjen utføres av blant annet Økonomiavdelingen, Compliance-ansvarlig, Risk Manager, sikkerhets- og HMS-ansvarlig, juridisk avdeling og Kvalitetsstyring. De spesifikke funksjonene vil imidlertid variere mellom virksomheter og sektorer.

Tredje forsvarslinje utøves av internrevisjonen som gir styrende organer og toppledelse en høyere grad av uavhengig og objektiv bekreftelse av internkontrollen i virksomheten, enn andrelinjen. Internrevisjonen kan blant annet vurdere om virksomhetens prosesser for styring og kontroll er hensiktsmessige og om internkontrollen fungerer etter sin hensikt, herunder om første og andre forsvarslinje fungerer effektivt og hensiktsmessig, og bidrar til at virksomheten når sine mål. Tredje forsvarslinje gir en uavhengig vurdering av risikostyringen til virksomhetens øverste organ.

I tillegg til disse tre interne forsvarslinjer gir ekstern revisor en uavhengig bekreftelse av regnskapsrapporteringen.

Det er viktig å være bevisst på at funksjonene i andre og tredje forsvarslinje skal opptre uavhengig av enhetene de overvåker og kontrollerer. Det vil si at de ikke skal utføre arbeidsoppgaver som tilligger førstelinjen, men kontrollere og overvåke at arbeidsoppgaver utføres i henhold til eksterne og interne regler og rutiner. Et godt utviklet risikostyringssystem, vil også være et godt grunnlag for internrevisjonens selvstendige risikovurdering.

Klare mandater og stillingsbeskrivelser er viktig for å kunne skille de ulike funksjonene og ansvarsområdene fra hverandre. Ledelsen bør vurdere å ta stilling til hvor i virksomheten disse funksjonene skal ha sin plass.

3.2 Organisatorisk plassering av risikostyringsfunksjonen

Risikostyringsfunksjonens organisatoriske plassering varierer avhengig av virksomheten og modenhetsnivået for helhetlig risikostyring i en organisasjon. Flere rammeverk anbefaler at risikostyringsfunksjonen skal rapportere til den øverste ledelsen uten at dette er nærmere spesifisert.
I noen virksomheter er ansvar for risikostyringen lagt til en separat funksjon utenom linjen, med rapportering til øverste leder. Andre steder kan den være plassert sammen med andre risiko- og kontrollfunksjoner, som i økonomiavdelingen med rapportering til økonomidirektør, eller sammen med Compliancefunksjonen. I mindre virksomheter kan ansvaret for risikostyringsarbeidet være forankret i en annen rollebeskrivelse, for eksempel økonomidirektør.

Risikostyringsfunksjonen skal utføre en aktiv rolle i å overvåke det totale risikobildet og forholdet mellom risiko og måloppnåelse/avkastning. Vedkommende skal gi klare anbefalinger og føringer til toppledelsen og styret særlig i forhold til de strategiske utfordringer.

Det er altså ikke ett riktig svar på hvor risikostyringsfunksjonen «hører hjemme» i virksomheten. Før en beslutter hvor risikostyringsfunksjonen skal plasseres, må ledelsen blant annet vurdere hva som skal være funksjonens fokusområder, hvilke miljøer risikostyringsfunksjonen har grensesnitt mot og dermed kan oppnå synergier og et faglig samarbeid med, virksomhetens behov for et fagmiljø innen risikostyring og internkontroll og hvilken organisering som best vil legge til rette for at risikostyringsfunksjonen får utøvd sitt ansvar.

3.3 Mandat, autoritet, kompetanse og ressurser

Virksomheten må peke ut en person med det overordnede ansvaret for risikostyringsfunksjonen. Den ansvarlige, og risikostyringsfunksjonen for øvrig, må blant annet forstå forretningsideen, strategien, markedet og rammebetingelsene til virksomheten. Ideelt sett kan dette kombineres med at noen av de ansatte på risikostyringsområdet har detaljkunnskaper om virksomhetens ulike prosesser, produkter og systemer. For alle stillinger bør det stilles definerte krav til erfaring og kompetanse.

Ansvaret må forankres på et tilstrekkelig høyt nivå i virksomheten, som sikrer nødvendig grad av autoritet og tilgang til sentrale beslutningstagere. Funksjonen må tildeles ressurser, rammevilkår og nødvendig mandat for å kunne holde seg oppdatert og sikre nødvendig videreutvikling av fagkompetansen. Ressursvurderingen bør legge opp til tilstrekkelig buffer for å ta ad hoc oppgaver og kunne yte kvalifisert rådgivning.

3.4 Uavhengighet og integritet

Personer som jobber i og er ansvarlig for virksomhetens risikostyringsfunksjon, skal i størst mulig grad organiseres uavhengig av den operative virksomheten. Dette hindrer ikke at risikostyringsfunksjonen informerer om og forankrer krav samt utarbeider beslutningsgrunnlag som påvirker forretningsdriften. Det er imidlertid en forutsetning at funksjonen ikke utfører eller er ansvarlig for den operasjonelle driften, eller fatter beslutninger som påvirker forretningsdriften. Personer i risikostyringsfunksjonen skal heller ikke jobbe i enheter de er satt til å overvåke.

Enkelte små virksomheter vil ikke ha mulighet til å opprette en egen stilling til å arbeide med risikostyring. Det vil i slike tilfeller være viktig at funksjonsbeskrivelsen adresserer problemstillingen. En rolleblanding kan forringe risikostyringsfunksjonens uavhengighet. Utgangspunktet må være at virksomheten skal stille til rådighet tilstrekkelige ressurser til å ha en velfungerende og uavhengig risikostyringsfunksjon. Funksjonen kan støtte seg på linjen for å løse oppgaver så lenge dette ikke strider mot krav til uavhengighet.

De ansatte som arbeider i risikostyringsfunksjonen må i tillegg til en relevant fagkompetanse ha høy faglig integritet. I tillegg må lederen ha tilstrekkelig autoritet og erfaring til å ta ansvar for utvikling og formidling av risikostyringsrammeverket. Den faglige integriteten er avgjørende for å oppnå tillit til funksjonen og funksjonens nytteverdi. Integritet synliggjøres gjennom rettskaffenhet, omhu og ansvarlighet i arbeidet. Integritet kan ødelegges gjennom partisk, uetisk eller ulovlig handling. Ansatte i risikostyringsfunksjonen skal respektere og bidra til organisasjonens legitimitet og etiske mål. Forutsetninger for å sikre legitimitet og integritet inkluderer et mandat som er forankret i styret og toppledelsen som tydeliggjør risikostyringsfunksjonens ansvar og oppgaver, og at organisering, informasjonstilgang og rapportering støtter oppunder mandatet.

3.5 Tilgang til informasjon

Risikostyringsfunksjonen må ha tilgang til nødvendig informasjon om virksomhetens drift og beslutninger. Dette kan med fordel defineres i funksjonsbeskrivelsen, og omfatter tilgang til bl.a. datasystemer, styringsdokumenter, fysisk eiendom, personell og dokumenter fra styrende organer. I tillegg må risikostyringsfunksjonen ha rett til å delta på interne møter ved behov, for å kunne foreta forsvarlig oppfølging og overvåking.

3.6 Belønningspolitikk og incentivmodell

Virksomheten må ha etablert en belønningspolitikk og incentivmodell som bidrar til å sikre funksjonens uavhengighet. Belønning og incentivmodell for risikostyringsfunksjonen skal ikke inneholde resultatavhengige komponenter som kan føre til interessekonflikter og påvirke objektiviteten til personer i funksjonen. Videre skal belønningen være på et nivå som gjør det mulig å besette funksjonen med personer som innehar nødvendig kompetanse og tyngde.

3.7 Rapporteringskrav til stillingen

Uavhengig av hvordan den formelle organiseringen er lagt opp, bør risikostyringsfunksjonen ha løpende rapporteringsplikt til styret og toppledelsen etter en frekvens som overordnende organer fastsetter. Videre bør det tilrettelegges for ad-hoc kommunikasjon med styret ved behov.

For å sikre velfungerende risikostyring vil det være viktig at sentrale så vel som lokale risikostyringsfunksjoner er plassert på "senior ledelses"-nivå, at personell har tilstrekkelig erfaring kombinert med faglig, personlig og profesjonell autoritet.

3.8 Outsourcing av funksjonen

Dersom virksomheten velger å outsource hele eller deler av risikostyringsfunksjonen, må ledelsen sørge for at alle de grunnleggende kravene til en risikostyringsfunksjon er ivaretatt. Det gjøres oppmerksom på at enkelte lover vil kunne innskrenke muligheten for outsourcing. Slik outsourcing er mest vanlig i startfasen av etableringen av helhetlig risikostyring, inntil organisasjonen tilegner seg et felles språk, risikokultur og et velfungerende rammeverk for risikostyring.

4 FREMGANGSMÅTE VED OPPBYGGING AV RISIKOSTYRINGSARBEIDET I ORGANISASJONEN

4. 1 Rammeverk og standarder

Det er to standarder/rammeverk som har oppnådd internasjonal aksept. Disse er:

1. ISO 31000:2018 – Risk Management – Guidelines[xi]

ISO 31000 Risikostyring – Retningslinjer er en internasjonal standard som er oppdatert i 2018. Den oppdaterte versjonen er foreløpig ikke oversatt til norsk. Den beskriver prinsipper, rammeverk og prosesser for risikostyring. Disse komponentene kan allerede være etablert i virksomheten, men det kan være behov for å skreddersy og forbedre dem for at risikostyringen skal være effektiv, hensiktsmessig og konsistent.

Prinsippene omfatter verdiskaping og -bevaring, og sier at risikostyring skal være integrert, strukturert og fullstendig, skreddersydd, inklusivt, dynamisk, sørge for best tilgjengelig informasjon, ivareta menneskelige og kulturelle faktorer samt legge til rette for kontinuerlig forbedring. Rammeverket for risikostyring består av: integrering, design, implementering, evaluering og forbedring. Risikostyringsprosessen består av følgende: definere omfang, kontekst og kriterier, identifisering av risiko, risikoanalyse, risikoevaluering og risikohåndtering. Prosessen skjer innenfor overordnede krav til kommunikasjon og rådføring, dokumentasjon og rapportering samt overvåking og oppfølging.

Det overordnede formålet med ISO 31000 er å integrere risikostyringsarbeidet i et strategisk og operasjonelt ledelsessystem. I den nye utgaven blir ledelsens rolle understreket, og verdiskapning og verdibevaring får en sentral plass som risikostyringsprinsipp.

Det gjelder å ha en disiplinert beslutningsprosess knyttet til forhold som påvirker risiko og lønnsomhet, som bidrar til at virksomheten oppnår de forventede resultater. Standarden gjelder uavhengig av næring, type og størrelse på virksomheten.

2. COSO: «Helhetlig risikostyring - Integrering med strategi og måloppnåelse» 2017[v]

I kapittelet 1.5 ovenfor, om forholdet mellom risikostyring og internkontroll, blir det forklart at COSO utarbeidet et rammeverk for ERM som i utgangspunktet bygget videre på prinsippene i rammeverket på internkontroll. Formålet med publikasjonen i 2004 var å hjelpe irksomhetene å bedre beskytte og styrke sine interessenters verdier. Den underliggende filosofien var at "verdier maksimeres når ledelsen setter strategi og mål for å finne en optimal balanse mellom mål for vekst, avkastning og relaterte risikoer, og utnytter ressursene for å nå enhetens mål."
Det kom en oppdatering av COSO ERM i 2017 som understreker hvor viktig det er å vurdere risiko både i strategiprosessen og i arbeidet med å fremme måloppnåelse. Executive Summary finnes oversatt til norsk og er utgitt av IIA Norge.

Det fastslås at risiko ikke skal ses utelukkende som en begrensning eller utfordring i fastsettelse og gjennomføring av strategi. Tvert imot, så er risiko en nødvendig konsekvens av den forandringen eller de målene man ønsker å oppnå. Virksomhetens håndtering av risiko danner således grunnlag for strategiske muligheter og åpner for utvikling av viktige særpreg ved virksomheten.

Rammeverket fastsetter fem komponenter som utgjør helhetlig risikostyring:
1. Virksomhetsstyring og kultur
2. Fastsettelse av strategi og mål
3. Gjennomføring
4. Gjennomgang og revurdering
5. Informasjon, kommunikasjon og rapportering

Disse fem komponentene støttes av et sett med 20 prinsipper. Disse prinsippene dekker alt fra overordnet virksomhetsstyring til oppfølging og overvåking. De er håndterbare i omfang, og de beskriver forskjellige fremgangsmåter som kan benyttes i ulike organisasjoner uansett størrelse, type eller sektor. COSO fremholder at overholdelse av prinsippene kan gi ledelsen og styret rimelig grunn til å forvente at organisasjonen forstår risikoene knyttet til strategien og virksomhetens mål, og søker å styre disse.

4.2 Utforming av rammeverk i praksis

En fellesnevner på eksisterende standard og rammeverk er en definisjon av at risikostyring omfatter metoder og prosesser som brukes av organisasjoner til å styre risikoer og utnytte muligheter.

Et *rammeverk* for risikostyring involverer typisk:
- Identifikasjon av interne og eksterne forhold som påvirker virksomhetens målsetninger.
- Fastsettelse av risikoappetitt og risikostyringspolicy.
- Utforming av risikostyringsfunksjon/-organisasjon og ansvarsområder.
- Etablering av interne og eksterne kommunikasjons- og rapporteringsstrukturer.
- Tildeling av ressurser til funksjonen.

Med utgangspunkt i dette er det behov for å etablere en prosess for risikostyring som gjerne vil bestå av:
- Identifikasjon av bestemte hendelser og forhold av betydning for virksomhetens måloppnåelse (trusler og muligheter).
- Analyse og vurdering av hendelser og forhold ut ifra sannsynlighet og konsekvens eller en modellering av fremtidige utfall gjennom anvendelse av andre statistiske metoder.
- Valg av håndteringsstrategi, implementering og oppfølging av gjennomføringen (herunder måling av effekt).

Ved å identifisere og proaktivt vurdere trusler og muligheter kan virksomheter beskytte og skape verdier for sine interessenter, herunder eiere, ansatte, kunder, tilsynsmyndigheter og samfunnet generelt. Det omfatter ytre risiko (knyttet til regelverk, omdømme osv.), strategisk risiko (en iboende del av beslutningsprosessen), finansiell risiko, etterlevelsesrisiko og operasjonell risiko. Som følge av bl.a. globaliseringen av næringslivet, har smitteeffekten mellom virksomheter og markeder (systemisk risiko) og avhengigheter mellom ulike risikoer blitt viktige elementer som må håndteres i risikostyringsprosessen.

Som en sentral del av styringsstrukturen i en virksomhet bidrar helhetlig risikostyring til å beskytte verdier og til å bedre beslutningsprosessen ved å fastsette akseptable nivåer for risikoappetitten og ved å forankre risikostyring i virksomhetens planleggings- og ledelsesprosesser. Når risikostyring er forankret, blir den en del av virksomhetens kultur.

Grunnlaget for en solid risikostyring er at alle deler av organisasjonen er ansvarlige for å håndtere risikoer innenfor sine områder. Men risikostyring skal gjennomføres etter en integrert, helhetlig tilnærming slik at man sikrer at den er i samsvar med målsetninger og strategi i virksomheten som helhet.

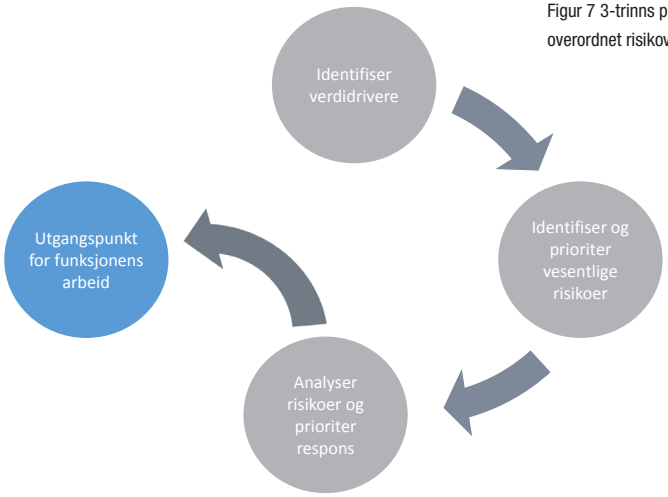
Hovedpunkter relatert til risikostyring:

- Virksomheten definerer sin risikostrategi og -appetitt. Øverste leder utpeker en leder for risikostyringsfunksjonen. Risikoeiere[viii] blir identifisert for alle vesentlige risikoer.
- Risikoeierne fastsetter meningsfulle og målbare målsetninger og kontrollmekanismer som anerkjennes i hele virksomheten.
- En sentralisert risikostyringsfunksjon har ansvaret for etablering og vedlikehold av risikostyringsprosessene. Den gir virksomheten et formelt risikostyringsrammeverk og tilpassede opplæringsprogrammer til å forbedre risikostyringskulturen og fremme et felles risikospråk og begrepsbruk i hele virksomheten.
- Toppledelsen gjennomgår jevnlig rapporter om utviklingen i vesentlige risikoer og om gjennomføringen av risikohåndteringsplanene. Ledelsen forsyner løpende styret og eventuelt revisjonsutvalget med relevant, fullstendig og tidsriktig informasjon.
- Kritiske, nye og fremvoksende risikoer («emerging risks»)[vii] blir løftet til det rette ledelsesnivået så snart de er identifisert.

4.3 Overordnet risikovurdering i tre trinn

En virksomhet som aldri tidligere har foretatt en overordnet risikovurdering kan gjøre dette gjennom en enkelt tre-trinns prosess (se illustrasjon figur 7):

1. Identifisere og definere virksomhetens verdidrivere. Det vil si, spørre seg «hvorfor eksisterer denne virksomheten, og hva påvirker måloppnåelsen i positiv og negativ retning?» I denne sammenheng kan verdi være et vidt begrep. Det kan omfatte eksempelvis liv og helse eller oppfyllelse av et offentlig mandat, like fullt som kostnader og verdsettelse i kroner og øre.
2. Identifisere, evaluere og analysere vesentlig usikkerhet som kan påvirke verdidriverne. Dette omfatter både de elementene som kan føre til bedre utfall enn forventet og et dårligere utfall. Det skal vurderes hvilke av disse risikoer som anses som vesentlige og som skal styres aktivt. For alle risikoer bør det vurderes om de skal styres (aktivt håndtere og følge opp), deles (dele risikoeksponering med en annen part eller gjennom forsikring) eller unngås (endre operativ drift eller fullt ut forsikre en risiko). Som del av det å styre en risiko, kan bevisst økt risikoeksponering også være et alternativ.
3. Usikkerheten kan kvantifiseres i form av sannsynlighet og konsekvens, og bør være med på å danne grunnlag for arbeidsoppgavene til Risikostyringsfunksjonen (se 4.4). Ved bruk av en slik skala, må det tydelig defineres hva som menes med de ulike nivåene av sannsynlighet og konsekvens. Herunder må konsekvensskalaen defineres for relevante kategorier, eksempelvis økonomi, måloppnåelse, HMS og omdømme. Sannsynlighet må kunne vurderes også for usikkerhet som ikke historisk kan beregnes, gjennom en kvalitativ vurdering av hvor sannsynlig det er at en situasjon oppstår fremover i tid. Virksomhet som ikke måler sin måloppnåelse i kroner og øre, bør definere intervaller for konsekvens som knyttes opp mot grad av konsekvens for sine mål/mandater.



Figur 7 3-trinns prosess for overordnet risikovurdering

4.4 12-trinns plan for å opprette en risikostyringsfunksjon i en virksomhet

For de som vurderer å implementere risikostyring i sin virksomhet foreslår vi følgende fremgangsmåte:

1. Utarbeid mandat og stillingsbeskrivelse for funksjonen, og definer rollen i virksomheten samt rapporteringslinjer. Se til at en risikostyringsfunksjon har støtte og forankring i selskapets ledelse og styre.
2. Ansett eller utpek leder for risikostyring med egnet erfaring og kompetanse og sørg for at det gis rom for å bygge opp en funksjon som har nødvendig integritet.
3. Fastsett policy for implementering av risikostyring, herunder rammeverk som skal anvendes, fremgangsmåte, ansvar og rapportering. Vurder behov for å kjøpe/utvikle et støttesystem for risiko- og virksomhetsstyring for å kunne lette arbeidet med å etablere virksomhetens risikoprofil og styre risikoene.
4. I ERM-funksjonen bør man dekke alle typer risiko, herunder usikkerhet i strategi og beslutningstagning, operasjonelle og finansielle risikoer, politisk risiko, regulatoriske risikoer mv. Funksjonen bør også fokusere på tiltak for risikohåndtering ved uønskede hendelser, eksempelvis gjennom forsikringsordninger og «business continuity management».
5. Styret og ledelsen definerer risikoappetitten og beskriver hvordan virksomheten skal sikre at risikoer blir innenfor fastsatte rammer og eventuelle øvre- og nedregrenser.
6. Kommuniser implementeringsplan i virksomheten og foreta risikovurderinger. Bestem prinsipper for styring og måling av risiko.
7. For å kunne ta vare på og ikke minst rekruttere medarbeidere til risikostyringsarbeidet bør det være på plass en karrierestige som tydelig viser at dette er en profesjon med bestemte krav både til utdanning og erfaring, og som viser hvilke utviklingsmuligheter som finnes.
8. I de største virksomhetene kan det være hensiktsmessig å etablere Risk Managers i linjen i tillegg til en sentral funksjon som skal ivareta helheten (ERM-funksjon).
9. Foreta regelmessig kommunikasjon over status på risikokultur, risikoeksponering, risikoappetitt, risikovurderinger og eventuelt nye risikoer[vii] og endringer i eksisterende risikoer.
10. Risikokommunikasjon skal i størst mulig grad være proaktiv og det er viktig at alle risikoer har en eier.
11. Det må etableres en arbeidsform som sikrer at sentral risikostyringsenhet arbeider tett med strategi- og linjefunksjonene.
12. Gjennomfør årlig rapportering til styret og legg plan for aktiviteter for påfølgende år.

4.5 Årsaker til at etablering av helhetlig risikostyring blir mislykket

Over tid har man høstet erfaring både nasjonalt og internasjonalt på hva som fungerer og ikke fungerer. Noen av årsakene som har vist seg å ha størst negativ betydning er etter vår mening:

- Uklar visjon, manglende verdigrunnlag og dårlig formulerte strategier og mål hindrer samordning og fokusering i virksomheten.
- Manglende kobling mellom strategiske mål og risikostyring.
- Uklart mandat og dermed manglende forståelse i risikostyringsfunksjonen og organisering av ansvarsfordeling.
- Risikostyringsansvarlig mangler generell risikostyringskompetanse, strategisk forståelse og helhetlig bilde og klarer ikke å påta seg rådgiver- og utfordrerrollen.
- Risikostyringsansvarlig mangler forståelse av forretningen.
- Begrepene er ikke forstått eller blir misforstått.
- Manglende eierskap til systemverktøy.
- Det benyttes verktøy uten å vurdere svakheter og begrensninger.
- Det blir ikke viet tilstrekkelig oppmerksomhet til utvikling og forankring av en risikokultur. Det blir ikke oppmuntret til diskusjon, eller stimulert til ærlighet og åpenhet for å få en god vurdering av risiko -"ingen skal bli hengt for å fortelle sannheten".
- Manglende prioritering av vesentlige risikoer.
- Manglende forståelse/ kunnskap om samvariasjon mellom risikoer.
- Manglende styring/oppfølging av IT-risiko.Manglende fokus på endring i risikobilder og nye risikoer[vii].
- Virksomheten er ikke overbevist om nytten av risikostyringsarbeidet og det blir derfor manglende forankring.
- Organisering og ansvar er uklart mellom risikoansvarlig og risikoeiere[viii].
- Personlig risikostyring skjer på bekostning av helhetlig risikostyring.
- Arbeid utført av de forskjellige kontrollfunksjoner er lite samkjørt.
- Det oppstår usunn konkurranse/ profesjonskrig mellom risk manager og beslektede funksjoner, f.eks. kvalitet-, compliance- og internrevisjonsfunksjonene.
- Mangelfullt gjennomførte risikovurderinger der forutsetningene for analysen ikke er beskrevet, noe som fører til at ledelsen ikke stoler på risikobildet som presenteres.
- Manglende kvalitetssikring i analyser/vurderinger.
- Manglende helhetlig tanke rundt rapportering gir ulike formater på risikovurderingene som vanskeliggjør aggregering til et høyere nivå.

Husk det er til syvende og sist ikke form som teller, men innhold!
Nettverk risikostyring i IIA Norge har planer om å utvikle ytterligere fagdokumenter som kan vise praktisk tilnærming til risikostyringsoppgaver samt avholde kurs/seminar innenfor fagområdet – se nærmere websiden til IIA Norge www.iia.no og egen webside for Nettverk risikostyring.

IIA Norge utgir 2 ganger årlig SIRK et fagblad for områdene Styring – Internrevisjon – Risiko – Kontroll. Det kan abonneres på papirutgaven hos IIA Norge og pdf versjon kan lastes ned fra websiden til IIA Norge.

Fotnoter

[i] Ordet "Compliance" brukes som betegnelse for funksjonen for kontroll av etterlevelse (av lover, forskrifter og internt regelverk) – se også egen veileder fra Norges Interne Revisorers Forening (NIRF) "Veileder for compliancefunksjonen" utgitt 2015.

[ii] http://onlinelibrary.wiley.com/doi/10.1111/risa.12375/full

[iii] Internkontroll- et integrert rammeverk – mai 2013 tilgjengelig fra IIA Norge (tidligere NIRF)

[iv] Helhetlig risikostyring – et integrert rammeverk september 2004 – utgitt IIA Norge (tidligere NIRF) oktober 2005

[v] Helhetlig risikostyring - Integrering med strategi og måloppnåelse (Sammendraget oversatt til norsk av IIA Norge i 2018). Original på engelsk «Enterprise Risk Management – aligning risk with strategy and performance» - utgitt juni 2017 http://www.coso.org/

[vii] Norsk anbefaling for eierstyring og selskapsledelse utgitt av Norsk utvalg for eierstyring og selskapsledelse (NUES) 30. oktober 2014

[viii] Nye risikoer brukes som norsk oversettelse av det som omtales på engelsk som "emerging risk"

[ix] En risikoeier har ansvar for resultateffekten knyttet til den aktuelle risikoen

[x] Nassim Nicholas Taleb, The Black Swan 2007, Random House

[xi] Utgitt av "standard.no" på norsk

IIA NORGE

IIA Norge, tidligere kjent som Norges Interne Revisorers Forening (NIRF) – er interesseorganisasjonen for alle som arbeider med eller har interesse av fagområdene internrevisjon, virksomhetsstyring, risikostyring, compliance og kontroll. Foreningen skal gi sine medlemmer et solid faglig fundament og styrke kunnskapen i norske virksomheter om styring, kontroll og internrevisjon.

IIA Norge er et nasjonalt institutt av det globale The Institute of Internal Auditors (IIA). Foreningen ble etablert i Norge i 1951 og er med sine over 800 medlemmer den største internrevisjonsforeningen i Norden. IIA Norge deler profesjonens grunnleggende prinsipper – etiske regler og internasjonale standarder for profesjonell utøvelse av internrevisjon – med mer enn 180 000 medlemmer i 165 land.

IIA Norge gir foreningens medlemmer og fagmiljøet generelt tilbud om faglige nettverk, kompetanseutvikling, sertifiseringsordninger, litteratur, metoder og verktøy innenfor disse fagområdene. Besøk www.iia.no for mer informasjon om foreningen.

Foreningens motto er «Fremskritt gjennom deling av kunnskap».

Nettverk risikostyring i IIA Norge har planer om å utvikle ytterligere fagdokumenter som kan vise praktisk tilnærming til risikostyringsoppgaver samt avholde kurs/seminar innenfor fagområdet – se nærmere websiden til IIA Norge www.iia.no og egen webside for Nettverk risikostyring, www.iia.no/risikostyring.

IIA Norge utgir 2 ganger årlig SIRK et fagblad for områdene Styring – Internrevisjon – Risiko – Kontroll. Det kan abonneres på papirutgaven hos IIA Norge og pdf-versjon kan lastes ned gratis fra websiden til IIA Norge.


IIA Norge

IIA Norge
Postboks 1417 Vika, 0115 Oslo
Besøksadresse: Haakon VIIs gate 9, 6. etasje
E-post: post@iia.no
www.iia.no.

IIA Norge

Veileder for risikostyringsfunksjonen