IIA Norge

Helhetlig risikostyring – en veileder for risikofunksjonen 2025

Virksomhetsstyring

Kombinasjonen av prosesser og strukturer, fastsatt av styret for å informere, lede, styre og følge opp de aktivitetene virksomheten gjennomfører for å nå sine mål.

I virksomhetsstyring er risikostyring, etterlevelse og internrevisjon viktige elementer, som sammen kan bidra til god styring og verdiskapning.

Risikostyring

En prosess for å identifisere, vurdere, håndtere og følge opp potensielle endringer, hendelser eller situasjoner, for å gi rimelig grad av sikkerhet for at virksomheten kan nå sine mål på alle nivåer.

Etterlevelse

Styring og kontroll med at virksomheten overholder lover, forskrifter, kontrakter, retningslinjer, rutiner og andre krav.

Internrevisjon

En uavhengig og objektiv bekreftelses- og rådgivnings-tjeneste, som har til formål å tilføre verdi og forbedre virksomheten.

Innhold

Om denne veilederen

Behovet for å etablere en risikofunksjon oppstår i alle virksomheter, både i offentlig og privat sektor, uavhengig av virksomhetens størrelse, art og kompleksitet. Drivere for etablering av en risikofunksjon vil variere avhengig av konteksten slik som bransje og type virksomhet og organisering.

Typisk har disse drivere oppstått utfra behovet for å iverksette styring og kontroll på de områder hvor det er erfart historisk, og sannsynligvis også i fremtiden kan erfares høy risiko for vesentlige finansielle tap, skader, krenkelse av personlige rettigheter og friheter, dårlig helse og/eller tap av menneskeliv. På grunn av de potensielle sosiale og økonomiske utfall av slike hendelser er det også vanlig at eksterne tilsynsmyndigheter kommer med konkrete krav til organisering, utforming og gjennomføring av risikostyringsaktiviteter utover anbefalingene til god praksis i dette dokumentet.

I økende grad har en sett at styring av positiv og negativ usikkerhet knyttet til omskiftelige 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 risikofunksjon som et ledd i sunn virksomhetsstyring.

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

Veilederen søker også å komme med noen avklaringer og avgrensninger rundt organisering av en risikofunksjon. Dette omfatter fordeling av arbeidsoppgaver og roller mellom ulike kontroll- og bekreftelsesfunksjoner i virksomheten, for eksempel internrevisjon, risikofunksjonen og etterlevelsesfunksjonen.

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

Risikostyring foregår på alle nivåer i en virksomhet. Denne veilederen beskriver funksjonen med ansvar for helhetlig risikostyring. Prinsippene som blir beskrevet kan imidlertid også i stor grad være gyldige for de som arbeider med risikostyring innenfor et mer begrenset fagfelt eller område i en virksomhet.

Om 2025-utgaven

Veilederen ble først utgitt med tittelen «Veileder for risikostyringsfunksjonen» i 2017 på norsk og siden oversatt til engelsk. Den ble alt i 2018 oppdatert for å ta hensyn til endringer i rammeverket for COSO ERM og oppdatert ISO-standard 31000:2018. I 2020 ble det utgitt en «Good Practice Guidelines for the Enterprise Risk Management Function» som tok utgangspunkt i den engelske oversettelsen av den norske veilederen. Denne ble bearbeidet og utviklet videre av en styringsgruppe nedsatt av IIA-foreninger i de nordiske og baltiske land.

Denne utgaven bygger i sin tur videre på 2020-veilederen på engelsk, med noe utvidet innhold og tilpasset arbeid som IIA Norge har gjennomført i 2024 for standardisering av norske fagbegrep på virksomhetstyringsområdet. Det er også besluttet å ta de faglige vedleggene ut av hoved-dokumentet, og ha disse som enkeltstående temaark. Dermed kan disse etter behov enkelt oppdateres og utvides.

Bidragsytere

IIA Norge retter en stor takk til følgende medlemmer for den opprinnelige utarbeidelsen av veilederen, samt senere oppdateringer:

- Ayse B. Nordal, Nordal visjon
- Martin W. Stevens, Gjensidige
- Ole Martin Kjørstad, BDO
- Petter Kapstad, Equinor

Vi takker også representanter for IIA-foreningene i Danmark, Estland, Island, Latvia, Litauen, samt foreninger for risikostyring i Finland, Latvia og Litauen, for deres bidrag til veilederen på engelsk utgitt i 2020.

Sammendrag

Det er etter hvert utviklet seg en utbredt oppfatning om at helhetlig risikostyring er et nødvendig element i god virksomhetsstyring og verdiskapning.

Helhetlige risikostyringsaktiviteter utgjør en systematisk og objektiv måte å identifisere, analysere og evaluere risikoer på, noe som gjør det mulig både å styre risikoer innen forhåndsdefinerte rammer samt styrke kvaliteten av beslutninger som tas. For å sikre drift og gjennomføring av god risikostyring i et helhetlig perspektiv er det funnet nødvendig å ha en person eller funksjon som vies til denne oppgaven.

Denne veilederen identifiserer følgende kjernekriterier som bidrar til utforming av denne funksjon (med henvisning til avsnitt i veilederen der dette omtales nærmere):

1. Risikostyring er et lederansvar
2. Risikofunksjonen sikrer at risikostyring hensyntas i beslutninger på alle organisasjonsnivåer
3. Risikofunksjonen har god og åpen kommunikasjon med toppledelsen og styret samt med andre kontroll- og bekreftelsesfunksjoner
4. Risikofunksjonen har et mandat som er klart definert
5. Ansatte i risikofunksjonen skal organiseres uavhengig av ansvaret for den daglige driften og utvise faglig integritet
6. Risikofunksjonen skal ha tilgang til all relevant informasjon nødvendig for å utføre sine oppgaver
7. Belønningsopplegg for risikofunksjonen bør ikke inneholde et betydelig element som er avhengig av resultateffekter, som kan føre til interessekonflikter og påvirke objektiviteten til de ansatte i funksjonen
8. Belønning av de ansatte i risikofunksjonen skal være tilstrekkelig til å kunne få besatt og beholdt stillinger med den ønskede autoritet, faglig tyngde og forretningskunnskap.

Kapittel 1: Helhetlig risikostyring definert

1.1 Risikobegrepet

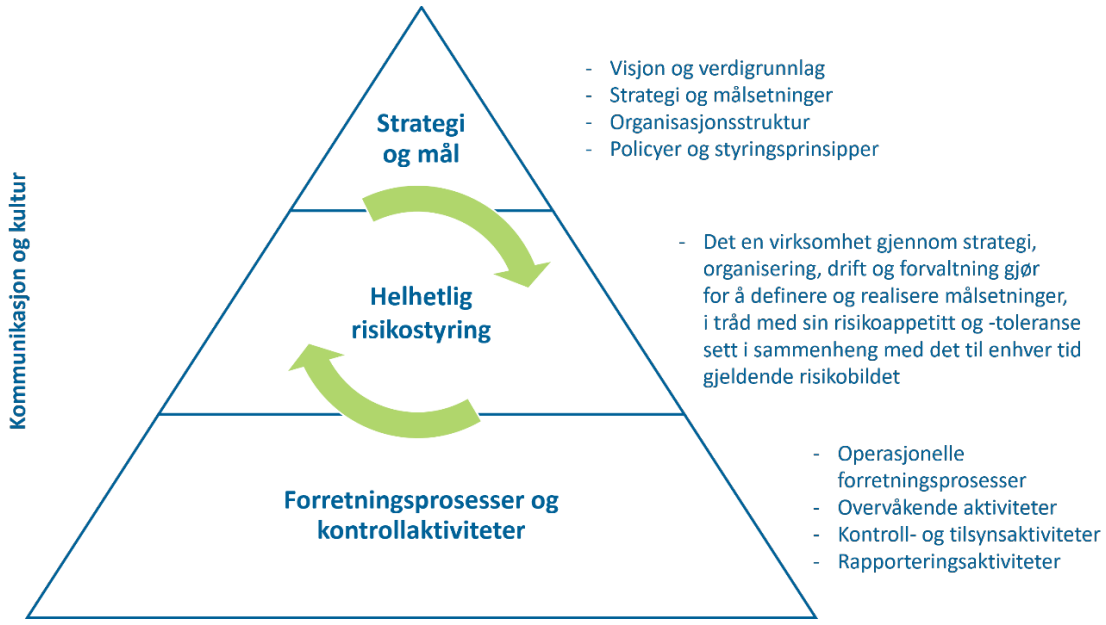
Det å ta risiko er en naturlig del av å drive enhver virksomhet, men i beslutningsprosesser blir dette sjelden tydelig uttrykt. Begrepet risiko har gjerne blitt utelukkende assosiert med uønskede hendelser, og risikostyring blitt definert som å analysere og begrense sannsynligheten for nedside og konsekvensen av uønskede hendelser. Dette er kun én dimensjon av det totale bildet. Det å vurdere muligheter – eller oppside – 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. Begrepet risiko i denne veilederen skal forstås som «usikkerhet som kan ha en positiv eller negativ innvirkning på virksomhetens evne til å nå sine mål på alle nivåer».

1.2 Helhetlig risikostyring

Risikostyring er en prosess for å identifisere, vurdere, håndtere og følge opp potensielle endringer, hendelser eller situasjoner, for å gi rimelig grad av sikkerhet for at virksomheten kan nå sine mål på alle nivåer. Dette betyr at arbeidet med risikostyring og strategi skjer gjennom integrerte og gjentagende prosesser. Det handler om å sikre både måloppnåelse gjennom utvikling av virksomheten og hensiktsmessig forvaltning av virksomhetens verdier, herunder menneskelige ressurser, omdømme og forebygging av tap eller sløseri som følge av uønskede hendelser.

Helhetlig risikostyring 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 risiko-styring 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. Den helhetlige risikostyringens rolle i virksomhetsstyring er illustrert i figur 1.



Figur 1: Forholdet mellom helhetlig risikostyring og virksomhetsstyring. Kilde: IIA Norge

1.3 Mer om risikostyring

Risikostyring består av systematiske, koordinerte, proaktive, reaktive og løpende aktiviteter som gir retning og kontroll til virksomheten i forhold til risiko.

Dette omfatter blant annet virksomhetens evne til å:

- analysere utvikling i virksomheten, dens omgivelser (intern og ekstern kontekst) og risikobildet over tid
- påvirke sannsynligheten og konsekvensen av positive eller negative hendelser
- forstå/utnytte korrelasjonen mellom ulike risikotyper
- proaktivt initiere tiltak som styrer virksomheten i ønsket retning
- reaktivt, dempe konsekvensene av negative hendelser og optimalisere konsekvensene av positive hendelser
- bygge opp en kultur som sikrer at hver ansatt kan foreta enkle eller komplekse beslutninger som bidrar til implementering av tiltak og bidrar til god risikostyring av strategiske målsetninger.

Det forutsettes også at risikostyring tar utgangspunkt i et helhetlig perspektiv på tvers av styrings- og organisasjonsenheter, funksjoner, prosesser, ansvar og risikokategorier (strategiske, finansielle, operasjonelle risikoer mv.) 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 Hvem kan nyttiggjøre seg av risikostyring

Alle eksisterende virksomheter, kommersielle så vel som offentlige, opplever usikkerhet knyttet til fremtidig utvikling, noe som er definisjonen på risiko. Valget er derfor mellom om man vil forsøke bevisst å påvirke fremtidig utvikling i en positiv retning (styre risikoen) eller la tilfeldighetene rå.

Dette gjelder selvfølgelig også på den private planen med hverdagsbeslutninger som for eksempel om man velger kasko eller ansvarsforsikring for bil, fast eller flytende rente på boliglån eller å løpe inn i vognen mens dørene lukkes for å slippe å vente til neste buss/trikk/tog. De fleste av oss vil ønske å veie opp det beste valget, ikke bare teoretisk, men også utfra tidligere erfaring, tilgjengelig informasjon og diskusjon med blant annet rådgivere, familie og venner. Man vil for eksempel kunne trekke inn i beslutningen den opplevelsen man hadde av den gang boligrenten lå på over 15 % eller den gang du var et vitne til at noen skadet seg med å forsere seg gjennom døren.

Et bevisst opplegg for sunn risikostyring er således noe som alle mennesker og virksomheter kan dra nytte av, ikke bare kommersielle selskaper og finansinstitusjoner. Det kan nevnes som eksempel det arbeidet Norges Skiforbund tok initiativ til etter 2016 i et samarbeid med risiko-styring i Equinor for å få frem risikobildet sitt med utgangspunkt i en analyse av verdidriverne sine. Bevisst styring av risikoer vil kunne bidra positivt til å sikre og skape verdier, og gjør både mennesker og virksomheter bedre rustet til å møte dagens og fremtidens utfordringer.

1.5 Forholdet mellom risikostyring, intern kontroll og virksomhetsstyring

Risikostyring er en prosess for å identifisere, vurdere, håndtere og følge opp potensielle endringer, hendelser eller situasjoner, for å gi rimelig grad av sikkerhet for at virksomheten kan nå sine mål på alle nivåer. Prosesser for styring og kontroll ofte forkortet til «internkontroll» er retningslinjer, rutiner og aktiviteter utformet og iverksatt for å styre og håndtere risiko innenfor rammen av virksomhetens risikotoleranse. Ut fra definisjonene kan man betrakte internkontroll som et element eller underprosess i helhetlig risikostyring. Dessverre kan det oppleves at begge begrepene blir tolket for snevert og adskilt fra hverandre, altså er risikostyring mer enn det å analysere og rapportere nedsiderisiko, og internkontroll handler om styring av en virksomhet og inneholder således ikke kun kontrollaktiviteter.

Denne tilnærmingen til risikostyring har fått økende aksept i de seneste årene. Et godt eksempel på dette gis i veilederen Helhetlig styring og kontroll av informasjonssikkerhet utarbeidet av Nasjonal sikkerhetsmyndighet (NSM), Direktoratet for forvaltning og økonomistyring (DFØ) og Digitaliseringsdirektoratet (Digdir) utgitt i 2021 – se figur 2.

Figur 2: Sammenhengen mellom styring og kontroll, risikostyring og overordnet virksomhetsstyring.
Kilde: Digitaliseringsdirektoratet

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 helhetlig risikostyring ment å være et verktøy for balansert prioritering av ressursbruk.

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. Derfor bør arbeidet også harmoneres med andre styringsaktiviteter, som for eksempel strategiarbeid og målstyring.

1.6 Dynamisk risikostyring

Begrepet «dynamisk risikostyring» har i senere tid blitt et mye brukt begrep. Dette skal ikke forveksles med en egen disiplin innen risikostyring, men ses på som et prinsipp som skal bidra til tidsriktig håndtering av usikkerhet. Vi velger derfor å omtale det i veilederen som et eksempel på god praksis.

Med dynamisk risikostyring menes i denne veilederen, at de aktivitetene som etableres for å identifisere og styre risiko, skal være tilpasset det faktum at det å drive en virksomhet ikke er statisk. Dersom man skal kunne agere tidsriktig på usikkerhet, kan man ikke utelukkende basere seg på prosesser som periodisk gir et øyeblikksbilde av virksomhetens risikoeksponering. Som nevnt flere steder i veilederen, handler risikostyring om mer enn en risikovurdering som gjennomføres med en viss frekvens, for eksempel årlig. Skal man styre risiko på en dynamisk måte, må hensyn til risiko integreres i den daglige beslutningstakingen og i måten man måler, kommuniserer og rapporterer om måloppnåelse.

Kort oppsummert, så handler det om å etablere prosesser og mekanismer som gjør virksomheten i stand til å tidsriktig respondere på – eller utnytte risiko. Dette handler i stor grad om å sørge for at førstelinjen har tilstrekkelig verktøy til å kunne respondere tidsriktig på risiko, fremfor kun å fokusere på andrelinjens mulighet til å presentere et risikobilde. Eksempler på aktiviteter som støtter opp om dynamisk risikostyring kan være:

- Tilpassede metoder og rutiner for å vurdere risiko i forbindelse med investeringsbeslutninger eller i forkant av beslutningspunkter i prosjektprosesser
- Etablering og løpende overvåking av nøkkelrisikoindikatorer, med tilhørende prosesser for å respondere når ulike nivåer av indikatorene utløses
- En banks kredittprosess, med prinsipper for å vurdere tilsagn om kreditt og løpende oppdatering av bankens porteføljeeksponering
- Situasjonsbetingede «triggere» for å gjennomføre risikovurderinger og vurdere hensiktsmessig respons, med involvering av sentrale beslutningstakere
- Løpende oppdatering av modeller for å vurdere risiko knyttet til mulige investeringer, som ledd i å utnytte muligheter når risikopremien anses å være best mulig
- Integrasjon av risiko i rapportering om måloppnåelse, for å gi beslutningstakere tidsriktig informasjon om den usikkerheten som er assosiert med virksomhetens måloppnåelse.

Hvordan man lykkes med å etablere gode prosesser som bidrar til å gjøre risikostyringen dynamisk vil variere vesentlig med virksomhetens art, kompleksitet og ambisjoner. Det er imidlertid flere fellesnevnere som er viktige å ta hensyn til, for å støtte opp om en mest mulig dynamisk styring av risiko. Som for eksempel:

- Mulighet for å kunne ekstrahere informasjon om risiko på en tidsriktig og intuitiv måte, eksempelvis gjennom å kombinere interne og eksterne data
- Tilstrekkelig forståelse for virksomhetens risikoappetitt, -toleranse og kapasitet
- Tydelig fordeling og forankring av roller og ansvar i virksomhetens beslutningsprosesser.

I tillegg er det avgjørende med et godt arbeidsforhold mellom første- og andrelinjefunksjoner i oppfølging og overvåking av risiko. En god andrelinje skal kunne støtte førstelinjen i å etablere gode prosesser for å respondere best mulig og tidsriktig på risiko. Samtidig skal andrelinjen kunne demonstrere overfor sine interessenter, hvordan virksomhetens internkontroll sørger for slik tidsriktig respons.

1.7 Om begrepene GRC og IRM

På samme måte som internkontroll og risikostyring kan anses å være gjensidig avhengige av hverandre, er de også avhengige av virksomhetens organisering og styringsprinsipper. Etterlevelse er også et sentralt element i dette universet. Derfor omtales disse fagdisiplinene gjerne samlet, under paraplyen «Governance, Risk and Compliance» (GRC). Når man snakker om helhetlig risikostyring, er det viktig å ha et bevisst forhold til hvordan disse domenene henger sammen i en virksomhet. Dette er områder som hverken bør eller kan drives i siloer.

Det er viktig at vi evner å se på virksomhetens helhet når vi jobber med risikostyring. Dette er tydeliggjort i «Veileder for virksomhetsstyring» utgitt av IIA Norge i 2021. I sistnevnt veileder er «Risikostyring» en av de 17 komponenter i virksomhetsstyring og et ledd i gjennomføring av den.

I markedet i dag blir ordet GRC også brukt i en snever betydning på systemtekniske løsninger som muliggjør registrering av risikovurderinger, kontrolldata og testresultater på tvers av funksjoner som IT-sikkerhet, risiko og etterlevelse. En annen betegnelse av det samme som er også i bruk er «Integrated Risk Management» (IRM). Sistnevnt skal ikke forveksles med ERM og helhetlig risikostyring.

Kapittel 2: Roller og ansvar for risikostyring

2.1 Om roller og ansvar

I denne veilederen benyttes betegnelsen «risikofunksjonen» for den som har det faglige ansvaret for den helhetlige risikostyringen. Dette behøver ikke nødvendigvis å være én person, eller en fast gruppe som ikke har andre ansvarsområder. Det viktigste er at det helhetlige risikostyrings-arbeidet representerer en systematisk og objektiv tilnærming til å identifisere, analysere og vurdere risiko, samt utforme og gjennomføre tiltak som skal sørge for at risikoen håndteres innenfor definerte risikorammer. I tillegg skal arbeidet kunne bidra i virksomhetens finansielle rapportering.

2.2 Styret

I en virksomhet er det styret eller øverste organ som «påser at» virksomheten har etablert forsvarlig risikostyring og internkontroll. I henhold til Norsk utvalg for eierstyring og selskaps-ledelse (NUES) omfatter dette blant annet 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.

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 og risikotoleranse.

2.3 Daglig leder og linjeledere

Daglig 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 virksomhetens målsetninger.

2.4 Mål for risikostyring

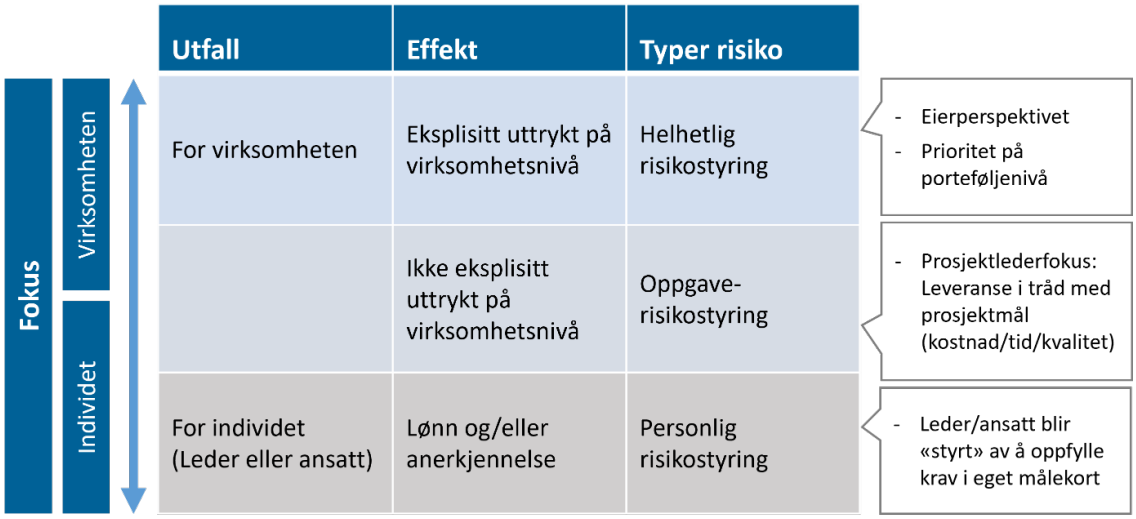
Ledere skal sikre at risikostyringsprosessen er fullt integrert på tvers av alle organisasjonsnivåer og er i tråd med virksomhetens mål, strategi og kultur. Risikostyringsaktiviteter i en virksomhet vil foregå på mange ulike nivåer, avhengig av fokuset i det enkelte tilfelle.

> "Dealing with risk is part of governance and leadership, and is fundamental to how an organization is managed at all levels." — ISO 31000:2018 introduction

I helhetlig risikostyring er utgangspunktet mål for virksomheten som helhet. 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 virksomheten kan føre til suboptimalisering, sett i lys av et overordnet virksomhetsperspektiv.

Gjennomføring av oppgaverisikostyring 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 3.



Figur 3: Typer risikostyring. Kilde: IIA Norge

2.5 Leder av risikofunksjonen

Leder av risikofunksjonen benevnes ofte med den engelske betegnelsen «Chief Risk Officer» (CRO). Det behøver ikke alltid være en egen lederstilling og ansvaret kan ivaretas av en annen stilling, men i denne veilederen brukes leder av risikofunksjonen som benevnelsen for denne rollen.

Lederen skal bistå virksomheten i arbeidet med å iverksette og gjennomføre effektive prosesser for å identifisere, vurdere og håndtere risiko. I tillegg har lederen et selvstendig ansvar for å overvåke risikobildet, og å flagge utviklingstrender for eksisterende risikoer og det potensielle utfallet av nye trusler/muligheter.

Lederen av risikofunksjonen har ansvar for å følge opp fremdriften i det samlede risikostyringsarbeidet, og for å bistå linjeledere i å formidle relevant risikoinformasjon til driftsenheter, toppledelsen og styret samt til eksterne parter der dette er påkrevd. 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 oppbygging og vedlikehold av risikostyringskompetansen i hele virksomheten.
- Etablerer en felles risikostyringsterminologi (for eksempel med hensyn til risikokategorier og begreper for sannsynlighet og konsekvens).

- Velger metodikk for identifisering, rangering, vurdering og oppfølging av risiko inklusivt nye risikoer. Det skal bestrebes så langt det kan gjøres å kvantifisere risikoer, for derved å gi et felles og forståelig grunnlag for prioritering og beslutninger.
- Bistår ledelsen i utvikling av risikorapportering og følger opp risikorapporteringsprosessen, herunder å fastsette nøkkelrisikoindikatorer (KRI-er), fastsetter et system for tidlig varsel eller trigger-system for brudd på virksomhetens risikoappetitt eller risikorammer.
- Har løpende kommunikasjon med ledelsen, daglig leder og styret ut fra en selvstendig kvalifisert vurdering av strategigjennomføringen og risikostyringen.

Risikofunksjonens leder legger til rette for- og følger opp implementering av:

- Hensiktsmessige risikostyringsprinsipper hos ledelsen
- Bistand til risikoeiere med å definere den planlagte risikoeksponeringen.
- Kommunikasjon av risikorelatert informasjon i hele virksomheten, herunder ekspertvurderingsuttalelser.
- Rapporteringslinjer som sikrer at risikorelatert informasjon når riktig instans på riktig tidspunkt og kommuniseres på en tilgjengelig og balansert måte til beslutningstagere.

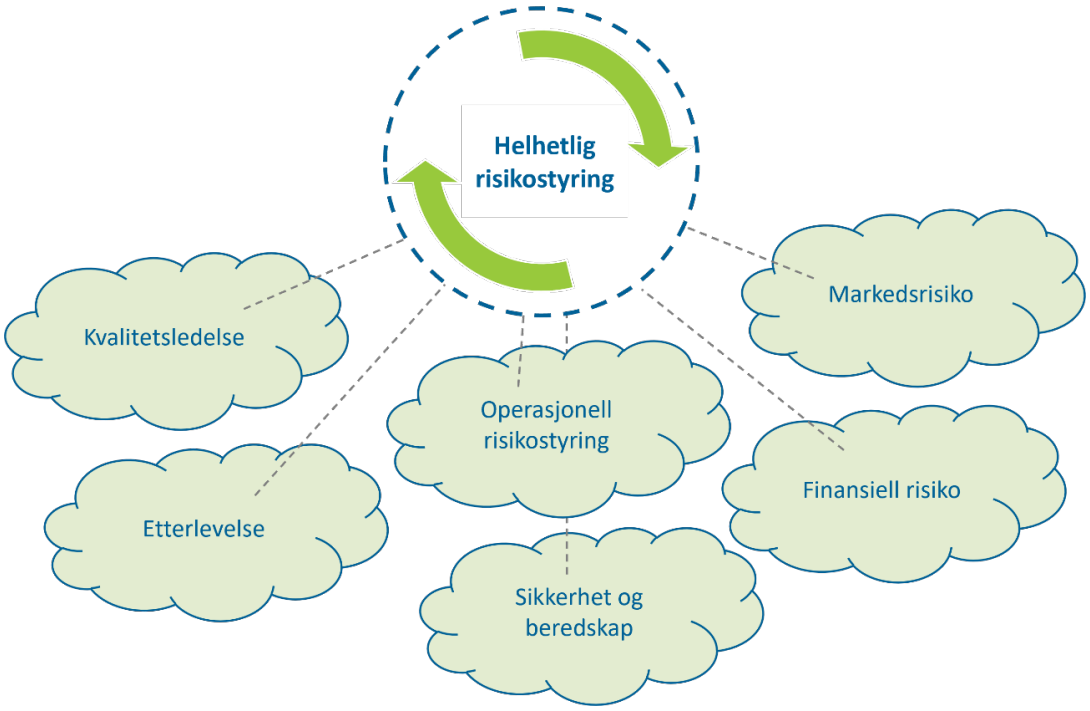
Lederen skal være opptatt av å påse at risikovurderinger er hensyntatt i alle vesentlige beslutninger, samt når det er nødvendig, påvirke og utfordre beslutninger som gir opphav til betydelig risiko. Lederen skal overvåke at risikostyringsprosessene etterleves, og reagere dersom det avdekkes forhold som ikke er tilstrekkelig håndtert.

2.6 Ansvar for helhetlig risikostyring

Risikostyring omhandler styring av både finansiell og operasjonell risiko, som for eksempel 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 (etterlevelsesrisiko), 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, virksomhetsprosesser, kontrollaktiviteter og beslutninger kan realisere sine målsetninger.

En viktig oppgave for risikofunksjonens leder 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 koordinering og styring av ulike risikoområder. Kilde IIA Norge

2.7 Andre funksjoner for risikostyring

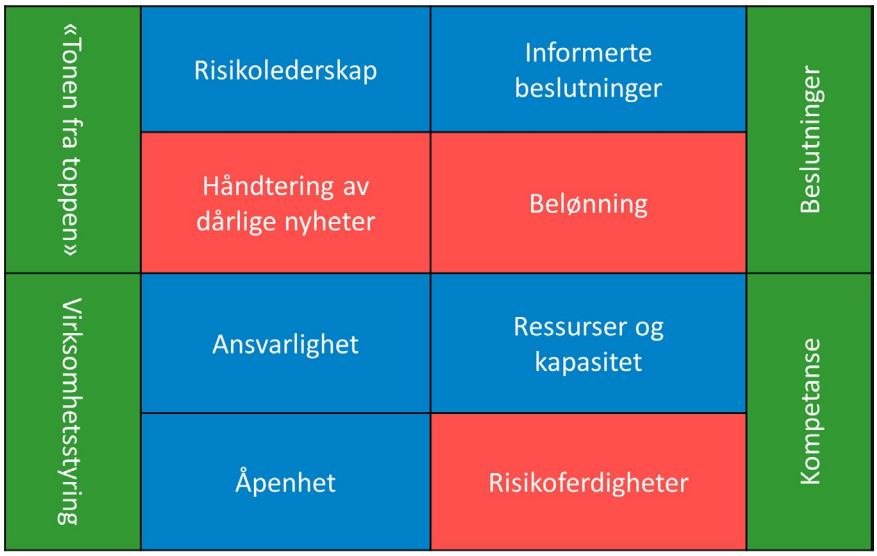
En virksomhet kan ha andre spesifikke oppfølgings- og overvåkingsfunksjoner for eksempel innenfor områdene helse, miljø og sikkerhet (HMS), innkjøp og kvalitet/ kontinuerlig forbedring. I denne sammenheng bemerkes at den oppdaterte ISO-standarden om kvalitetsledelse (ISO 9001:2015) i større grad enn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

Kapittel 3: Viktige temaer i risikostyring

3.1 Risikokultur

Risikokultur er et begrep som fikk eksplosiv utbredelse i media etter finanskrisen i 2008. Begrepets popularitet skyldes en erkjennelse av at det ikke var nok å ha skriftlige etiske retningslinjer og formelle risikostyringsstrukturer i finansinstitusjoner om man ikke klarer å omsette teori til praksis. Det er imidlertid et begrep som er godt kjent fra internkontroll teori, herunder COSO Internkontroll og COSO Risikostyring under navnet «kontrollmiljø», deretter «internt miljø» og til slutt «virksomhetsstyring og kultur». I ISO 31000:2018 Risikostyring er et av prinsippene som må hensyntas for å skape og beskytte virksomhetens verdi definert som «menneskelige og kulturelle faktorer».

Risikokultur beskriver felles holdninger til risikostyring i en virksomhet som i sin tur påvirker enkeltmenneskets adferd med hensyn til risikostyring. Som eksempel vises modellen til «Institute of Risk Management» i figur 5, som identifiserer åtte aspekter med risikokultur. De fem blå er på overordnet styringsnivå, og de tre røde har med menneskelig utvikling å gjøre.



Figur 5: Modell for risikokultur. Kilde: *Institute of Risk Management* (IRM)

Det er ønskelig å bygge en sunn risikokultur i virksomheten, noe som vil kjennetegnes med en positiv holdning til risikostyring og anvendelse av strukturert risikostyringsarbeid.

3.2 Anvendt og tilpasset metodikk

En risikofunksjon vil ha ansvar for å velge et tilpasset rammeverk/standard som virksomheten skal anvende for å styre risikoer og å oppnå gode forretningsmessige beslutninger. Man kan for eksempel velge å ta utgangspunkt i COSO ERM eller i ISO 31000:2018. Et generisk rammeverk/standard vil alltid måte tilpasses den virksomheten som skal anvende den og eventuelle eksterne krav fra myndigheter, bransjen eller andre. Metodikken bør vurderes minst årlig for å tilpasse den utviklingen i egen virksomhet og markedet samt endrede krav fra myndighetene.

3.3 Risikoappetitt, risikokapasitet og risikotoleranse

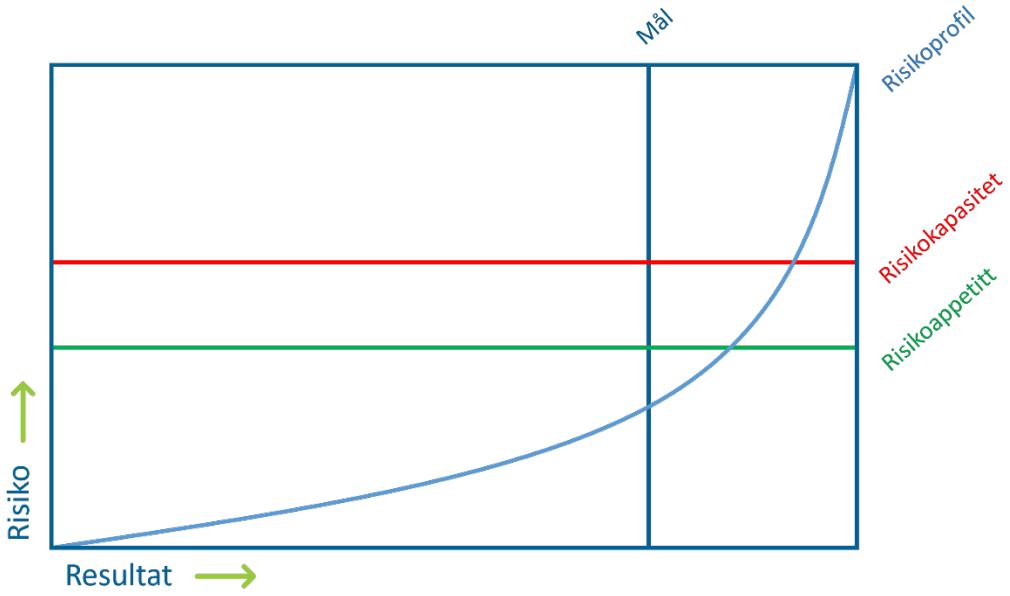
Risikoappetitt er definert som «den type og mengde risiko virksomheten er villig til å akseptere

for å gjennomføre sine strategier og nå sine mål». Risikoappetitten er således det nivået man ønsker og er villig til å ta for å oppnå mål, mens begrepet «risikokapasitet» er et uttrykk for det nivået av usikkerhet man har evnen til å håndtere og risikotoleranse er definert som «den variasjon i resultater en virksomhet er villig til å akseptere for å nå sine mål».

Risikoappetitt kan defineres enten kvalitativt eller kvantitativt i form av fullmakts- og eksponeringsgrenser innenfor ulike risikotyper. Risikoappetitt vil variere fra virksomhet til virksomhet avhengig av strategi, bransje og risikokultur. 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. «Risikoappetitt» er det nivået man ønsker og er villig til å ta for å oppnå mål. Risikokapasitet er et uttrykk for det nivået av usikkerhet man har evnen til å håndtere. Risikotoleranse er det øvrige nivået man er villig til å ta – se eksempel-illustrasjon i figur 6.



Figur 6 Illustrasjon av sammenhengen mellom risikoappetitt og risikokapasitet. Kilde: COSO ERM 2017

3.4 Risikogap

Risikogap, på engelsk «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 risikofunksjonens leder er å identifisere slike gap og sørge for at disse er kommunisert til ledelsen og styret.

3.5 Strategisk risikostyring

Det er utført analyser av vesentlige verdinedganger i børsnoterte selskaper for eksempel i forhold til fire forskjellige typer risikoer:

1. Strategisk
2. Ekstern
3. Operasjonell
4. Etterlevelse

Konklusjonen fra to amerikanske og en norsk undersøkelse var at vesentlig verdifall i børsnoterte selskapene var hovedsakelig forårsaket av strategisk risiko. I USA var vesentlig verdifall forårsaket av strategisk risiko beregnet i undersøkelsen utgitt i 2012 til 81 % av tilfeller (Booz & Co.), og beregnet til 86 % i en senere undersøkelse i 2015 (Harvard Business Review). I Norge foretok Hermann Christensen i 2018 en lignende undersøkelse der strategisk risiko utgjorde 63 % av verdifallet med ekstern risiko som nummer to faktor. De fleste av oss vil også huske selskaper som for eksempel Kodak og NOKIA som ekstreme eksempler av selskaper som ikke klarte å omstille strategien i tide med betydelig negativ påvirkning på selskapets egenkapital.

Vi lever i dag i en verden med blant annet hurtig teknologisk utvikling og menneskeskapte klima-endringer. Derfor er det viktig at risikostyringsteknikker anvendes og vil kunne gi verdi også i forbindelse med utarbeidelsen av strategien. Typer av teknikker utover fagekspertise innenfor sannsynlighetsberegninger vil kunne være bistand til scenarioanalyser samt analyse av nye og fremvoksende risikoer. Noen virksomheter kombinerer strategiarbeid med risikofunksjonen.

3.6 Beslutningstaking og kvantifisering av risiko

Det tas mange store og små beslutninger på alle nivåer i en virksomhet som vil påvirke virksom-hetens utvikling og resultater. De fleste slike beslutninger vil medføre en grad av usikkerhet. Beslutninger kan basere seg på intuisjon og erfaring. Men ved viktige beslutninger som kan få betydelige konsekvenser for virksomhet, er det forventning om en større grad av analysearbeid og drøftelser for og imot beslutningen.

Risikofunksjonen vil normalt besitte selskapets fremste ekspertise på statistiske beregning og modellering. I så fall vil det være naturlig at funksjonen bidrar med sin kunnskap i kvantifisering av ulike mulige utfall. Det er da nødvendig å først identifisere data til grunnlag for vurderingen.

Situasjonen vil da i utgangspunktet være en av disse tre:

1. Virksomheten har tilstrekkelig data tilgjengelig
2. Virksomheten har ikke tilstrekkelig data tilgjengelig
3. Virksomheten har data tilgjengelig, men det er grunn til å stille spørsmål ved om disse utgjør et relevant grunnlag for å vurdere fremtidig utvikling

Der virksomheten har dataserier om virkelig utvikling over tid, og det ikke er stor tvil om at historisk utvikling mest sannsynlig kan gjenta seg også i fremtiden, kan man utvikle prognoser basert på normalfordelinger – såkalt «Value at Risk».

Der virksomheten mangler historiske data, eller man mener at den historiske dataen ikke reflekterer en sannsynlig fremtidig utvikling, må dataserier konstrueres. Dette gjøres ved å skjelne til sammenlignbare situasjoner, eller ved å justere den historiske dataen etter de nye

forholdene. Det vil gjøre det mulig å kjøre normalfordelinger og «Value at Risk»-prognoser.

Der man ikke har en dataserie, men har en formening om ytterpunktene i en normalfordeling, kan man bruke såkalt «Monte Carlo»-simulering for å skape data til grunnlag for analyse. Denne metoden konstruerer et kunstig datagrunnlag til erstatning for et empirisk, ved simulering gjennom en såkalt slumptallsgenerator. «Monte Carlo»-simulering kan med fordel brukes for å lage modeller av effekten av hendelser med lav sannsynlighet og høy konsekvens, som for eksempel resultat av katastrofer.

Der virksomheten ikke har en klar formening om fremtidig utvikling, kan man legge et scenario til grunn for risikovurderingen. Dette kan være aktuelt for å øke forståelsen av hvordan mulig geo-politisk eller teknologisk utvikling vil kunne påvirke produkter og/eller markedet. Det er normalt å begrense seg til 3-4 scenarioer og for hver av disse lage dataserier som beskrevet ovenfor.

En virksomhet kan gjerne bruke scenarioer for å prøve ut soliditeten i strategien, og se hvordan strategien kan endres for å holde virksomheten på rett kjøl. Fordelen med å tenke det utenkelige, det vil si kartlegge virkningen av forhold som ligger utenfor den ordinære forretningsutvikling, er at forståelsen av virksomhetens sårbarheter økes. Da blir det mulig å senere tolke tegnene på sårbarheter, og endre strategien tidsnok.

Risikofunksjonen besitter ingen krystallkule, men den har teknikker som kan bistå virksomheten med styrket grunnlag for beslutninger som tas. Det vil alltid være usikkerhet knyttet til risiko-funksjonens analyser, og de underliggende hovedforutsetninger skal alltid redegjøres for.

Den risikoen ingen kan være forberedt på er utviklinger som kommer ut av det blå, som ingen hadde fantasi til å forestille seg. Disse hendelser kalles gjerne «sorte svaner», på engelsk «black swans». Skulle en «sort svane»-situasjon oppstå, vil arbeidet med å kartlegge og analysere slike scenarioer vise seg å være et viktig bidrag til virksomhetens beredskap.

3.7 Best tilgjengelig informasjon

Kvantifisering av risikobilde innebærer en beregning av sannsynlige fremtidige utfall basert på en formening om sannsynligheten for at tilfellet skal inntreffe. Tallene vil derfor måtte basere seg på de beste estimater basert på blant annet historikk og sammenlignbare situasjoner modifisert med et tungt innslag av ekspertvurderinger. Det vil alltid være en avveining mellom presisjons-grad og tid/kostnad til anskaffelse av data sett opp mot formålet med bruken. Noen ganger vil det være tilstrekkelig å benytte seg av en vurdering basert på ekspertenes mageølelse. Ved å innhente vurderinger fra flere enn en ekspert kan pålideligheten av risikoberegningen øke.

3.8 Kommunikasjon og konsultasjon

For å bevare funksjonens objektivitet bør lederen av risikofunksjonen ikke kunne ta forretnings-messige beslutninger og disposisjoner som går ut over funksjonen. Unntaket til dette kan være dersom det er tidskritisk å lukke en eksponering for å unngå vesentlige tap og ansvarlig leder ikke kan nås. For at virksomheten skal kunne dra nytte av innsikten risikofunksjonen skaffer seg gjennom sitt arbeid er det dermed viktig at risikobildet og oppfatningen om mulighetene for å realisere positiv eller unngå negativ utvikling blir kommunisert tydelig og tidsmessig til topp-ledelsen og/eller styret.

Det vil være naturlig at lederens stillingsinstruks også innebærer en plikt til å melde raskt fra, dersom det er forhold som lederen mener kan påvirke virksomhetens resultater i vesentlig grad.

Risikofunksjonen representerer faglig kapasitet med innblikk i alle forretningsområder. Det er derfor helt naturlig at toppledelsen og styret kan nyttiggjøre seg av risikofunksjonens leder ved å innhente råd og vurderinger i forbindelse med viktige beslutningsprosesser.

3.9 Operasjonell risiko og risikorespons

Helhetlig risikostyring skal kunne identifisere potensielle risikoer som kan være kritisk til verdiskapningen i virksomheten, dette som utgangspunkt for å overvåke risikobildet og tiltak for å redusere det negative utfall av risikoer på virksomheten og styrke en positiv utvikling.

For operasjonell risiko har overvåking av risikobildet tradisjonelt betydd at man følger opp om viktige kontroller er på plass og gjennomføres. Gjennom egenvurdering av kontroll (på engelsk *Control Self-Assessment*) har 1. linjen kunnet rapportere at de nødvendige kontroller gjennomføres. Dette har vært viktig tapsforebyggende informasjon for linjeledere og et kontrollopplegg 2.- og 3.linjen kan bygge sitt arbeid videre på.

Tradisjonelt har kontrollopplegget vært utført i ettertid for eksempel gjennom stikkprøvekontroller. Med utviklingen i kunstig intelligens har mulighetene for å automatisere ytterligere slik kontroll økt. Resultatet blir at alle transaksjoner/poster overvåkes på en automatisk og mer kostnadseffektiv måte. Der beslutninger allikevel foretas etter en menneskelig vurdering kan det være aktuelt å teste et utvalg av slike beslutninger også som ledd i læring og utvikling av medarbeidere.

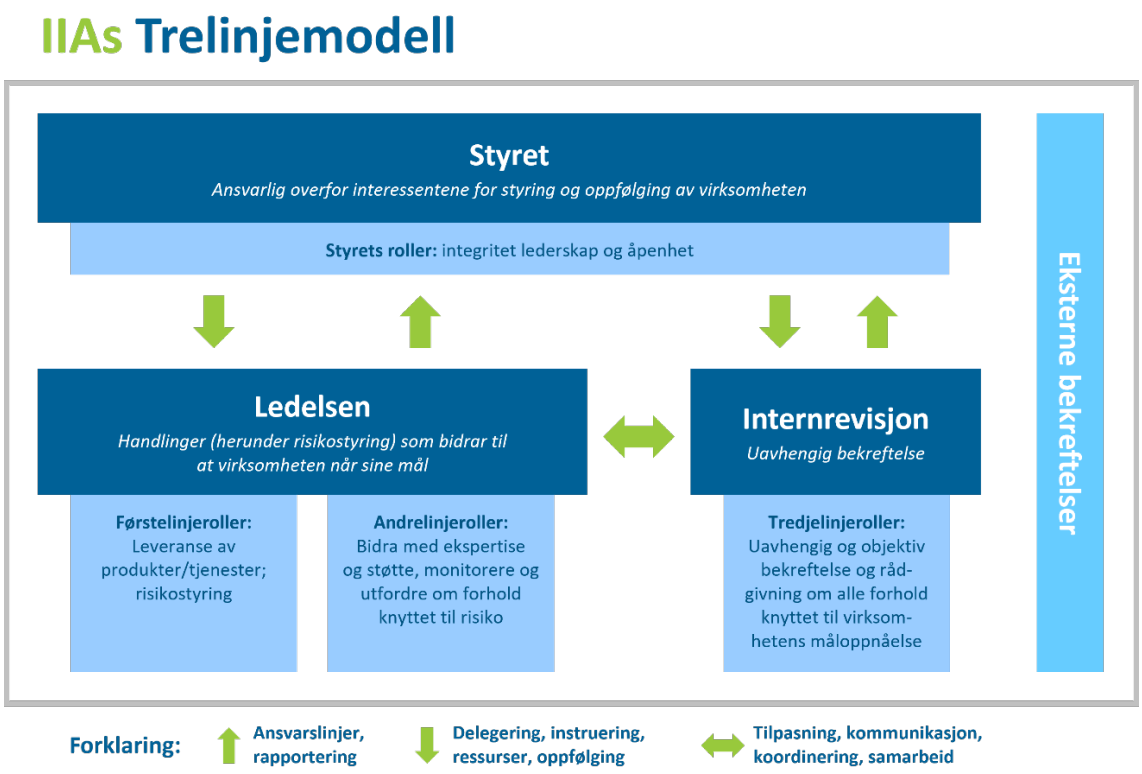
Et annet resultat av en operasjonell risikovurdering kan være at man ønsker å sette i gang nye tiltak for å redusere risikoen for feil. Dette kan for eksempel være ønsket om å erstatte en manuell med en helautomatisert prosess. I slike tilfeller er det god praksis at virksomheten tar initiativ til å følge opp gjennomføring av tiltak i henhold til både tid og budsjett samt oppnåelse av ønsket utfall. Igjen er det naturlig at status rapporteres opp i linjen og følges opp av en sentral risikofunksjon for å sikre oppnåelse av den ønskede endringen i risikobildet.

IIA Norge har utgitt et eget hefte «Operasjonell risiko – en innføring», som blant annet skisserer en modell for arbeidet med operasjonell risikostyring.

Kapittel 4: Organisering og gjennomføring av risikofunksjonen

4.1 Trelinjemodellen

Det er viktig å definere roller og ansvar for de ulike funksjonene i en virksomhet på en tydelig måte. Dette bidrar til effektiv utnyttelse av ressurser, 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 grensesnittet mellom helhetlig risikostyring og internkontroll.



Figur 7: Trelinjemodellen fra IIA. Kilde: *The IIA's Three Lines Model – An Update of the Three Lines of Defense* (as of Sept. 2024)

IIAs Trelinjemodell 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.

Risikofunksjonen er en andrelinjerolle og en av støtte- og kontrollaktivitetene i virksomheten, på lik linje med blant annet økonomiavdeling, etterlevelsesfunksjonen, IT-sikkerhetsfunksjonen og helse-, miljø- og sikkerhetsfunksjonen samt juridisk avdeling og kvalitetsstyring. Utvalg, navn og innretning på disse funksjonene vil imidlertid variere mellom virksomheter og sektorer.

Andrelinjeroller er dels proaktive, og dels reaktive. 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 definert risikoappetitt og ønsket utvikling, og sørge for at virksomheten fokuserer og reagerer på dette.

Det er viktig å være bevisst på at funksjonene i andre- og tredjelinjen 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.

4.2 Samarbeid mellom andrelinjefunksjoner

Utover leder av den sentrale risikofunksjonen (som andrelinjerolle) ledet, har et økende antall virksomheter etablert en separat funksjon eller funksjoner til å følge opp risiko for brudd på lover, forskrifter og retningslinjer (herunder mislighetsrisiko). Etterlevelsesfunksjonen (på engelsk «compliance function») vil ikke alltid være organisert som en eller flere lederstillinger og ansvaret kan ivaretas av en annen stilling, men i denne veilederen brukes leder av etterlevelsesfunksjonen som benevnelsen for denne funksjonen.

Etterlevelsensfunksjonens leder rapporterer vanligvis direkte til toppledelsen. Det er en forutsetning at lederne av henholdsvis etterlevelsesfunksjonen og risikofunksjonen jobber tett sammen, særlig i forbindelse med juridisk risiko, risiko for misligheter og sosial dumping, varslingsrutiner, omdømmerisiko, etablering av risikokultur og oppfølging av etiske retningslinjer.

Lederne av etterlevelsesfunksjonen og risikofunksjonen samt øvrige andrelinjefunksjoner 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.

4.3 Samarbeid mellom andre- og tredjelinjen

Funksjonene i andre-. og tredjelinjen har til felles at de ikke har ansvar for den daglige driften. Begge funksjoner har som mål at virksomheten de er ansatt i skal utvikle seg på en vellykket og bærekraftig måte.

Globale standarder for internrevisjon krever at «lederen av internrevisjonen skal utarbeide en plan for internrevisjonen som støtter virksomhetens måloppnåelse». Planen skal bygge på en vurdering av virksomhetens strategier, målsetninger og risikoer. I denne forbindelsen vil internrevisjonen måtte forstå risikoene som virksomheten står ovenfor. En viktig kilde i denne prosessen vil være dokumentasjonen utarbeidet av risikostyrings- og etterlevelsesfunksjoner.

For å lette kommunikasjonen med toppledelsen og styret er det viktig at risikostyrings-, etterlevelses- og internrevisjonsfunksjonene benytter seg av et felles språk og terminologi så langt dette lar seg gjøres.

Et tillitsforhold mellom 2.- og 3.-linjen vil innebære at internrevisjon kan fokusere sin innsats på de områdene der oppfølging fra risikostyrings- og etterlevelsesfunksjoner er svakest. Ved at

internrevisjonens leder utfordrer både lederen for risikofunksjonen og leder for etterlevelses-funksjonen i utførelsen av deres roller og oppgaver, vil det være med på å styrke kvaliteten på disse fagområdene.

4.4 Viktige vurderinger ved organisering av risikofunksjonen

Risikofunksjonens organisatoriske plassering varierer avhengig av virksomheten og modenhets-nivået for helhetlig risikostyring (se nærmere modenhetsmodellen - ERM modenhet i en virksomhet). Flere rammeverk anbefaler at risikofunksjonen skal rapportere til den øverste ledelsen uten at dette er nærmere spesifisert.

For å sikre velfungerende risikostyring vil det være viktig at sentrale så vel som lokale risiko-funksjoner er plassert på «seniorledelses»-nivå, at personell har tilstrekkelig erfaring kombinert med faglig, personlig og profesjonell autoritet.

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

Det finnes altså ikke ett riktig svar på hvor risikofunksjonen «hører hjemme» i virksomheten. Før en beslutter hvor risikofunksjonen skal plasseres, må ledelsen blant annet vurdere:

- hva som skal være funksjonens fokusområder
- hvilke miljøer risikofunksjonen har grensesnitt mot og dermed kan oppnå synergier og et faglig samarbeid med
- virksomhetens behov for et fagmiljø innen risikostyring og internkontroll
- hvilken organisering som best vil legge til rette for at risikofunksjonen får utøvd sitt ansvar.

Det er gunstig at risikofunksjonens leder har en direkte rapporteringsmulighet til styret eller til et risiko- eller revisjonsutvalg etablert under styret. Hensikten med en slik rapportering er å sikre, ved behov, muligheten for uavhengig og fullstendig rapportering til styret om virksomhetens risikoforhold.

4.5 Mandat, autoritet, kompetanse og ressurser

Virksomheten må peke ut en leder med det overordnede ansvaret for risikofunksjonen. Lederen og eventuelt øvrige medarbeidere i risikofunksjonen 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.

4.6 Toppledelsens ansvar

Daglig leder har ansvar for å etablere og gjennomføre forsvarlig risikostyring og internkontroll med en policyerklæring, 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.

Lederens organisatoriske plassering, ansvar, arbeidsoppgaver og fullmakter bør fastsettes i stillingsinstruks til leder av risikofunksjonen samt mandat for risikofunksjonen som godkjennes av daglig leder. Disse dokumentene 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.

4.7 Uavhengighet, objektivitet og integritet

Personer som jobber i og er ansvarlig for virksomhetens overordnet risikofunksjon, skal som andrelinjefunksjon opptre uavhengig av enhetene de overvåker og kontrollerer. Dette hindrer ikke at lederen av risikofunksjonen skal kunne informere om og forankre krav samt utarbeide 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 risikofunksjonen skal heller ikke jobbe i enheter de er satt til å overvåke.

Enkelte og særlig små virksomheter vil ikke ha mulighet til å opprette en egen og uavhengig risikofunksjon. Det vil i slike tilfeller være viktig at funksjonsbeskrivelsen adresserer problemstillingen. En rolleblanding kan forringe risikofunksjonens objektivitet.

Virksomheten bør stille til rådighet tilstrekkelige ressurser til å ha en velfungerende og objektiv risikofunksjon. Funksjonen må kunne støtte seg på linjen for å løse oppgaver så lenge dette ikke strider mot krav til uavhengighet.

De ansatte som arbeider i risikofunksjonen, 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 risikofunksjonen skal respektere og bidra til virksomhetens legitimitet og etiske mål. Forutsetninger for å sikre legitimitet og integritet inkluderer et mandat som er forankret i styret og toppledelsen som tydeliggjør risikofunksjonens ansvar og oppgaver, og at organisering, informasjonstilgang og rapportering støtter oppunder mandatet.

4.8 Forståelse av kontekst og tilgang til informasjon

Risikofunksjonen må ha tilgang til nødvendig informasjon om virksomhetens drift og beslutninger. Dette kan med fordel defineres i funksjonsbeskrivelsen/mandat, og omfatter tilgang til blant annet datasystemer, styringsdokumenter, fysisk eiendom, personell og dokumenter fra styrende organer. For å kunne foreta forsvarlig oppfølging og overvåking, må risikofunksjonen ha rett til å delta på interne møter ved behov.

4.9 Belønningspolitikk og incentivmodell

Virksomheten må ha etablert en belønningspolitikk og incentivmodell som bidrar til å sikre funksjonens uavhengighet. Belønning og incentivmodell for risikofunksjonen 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 faglig tyngde.

4.10 Rapportering

Uavhengig av hvordan den formelle organiseringen er lagt opp, bør risikofunksjonen 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.

4.11 Utkontraktering av funksjonen

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