



Styreveileder Risikostyring 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.



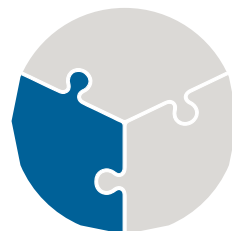
Risikostyring

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, prosedyrer og andre krav.



Internrevisjon

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



«Spørsmål styret bør stille om risikostyringen»

En veileder for medlemmer av styret i norske virksomheter

I alle norske virksomheter som har et styre, har dette etter norsk lov ansvar for å se til at virksomheten har etablert risikostyring i henhold til anerkjent god praksis. Dette gjelder virksomheter i både privat og de i offentlig sektor.

Denne veilederen består av et sett med sentrale spørsmål knyttet til virksomhetens risikostyring. Settet med spørsmål utgjør en helhet, og bør leses i sammenheng. Samlet vil de være egnet til å styrke styrets og ledelsens forståelse av hvordan risikostyringen av virksomheten fungerer i dag, og hvordan den kan utvikles videre.

Hva kjennetegner «Helhetlig risikostyring»?

Veilederen tar utgangspunkt i anerkjent god praksis for «Helhetlig risikostyring». Dette er det som på engelsk er kjent som Enterprise Risk Management (ERM), i henhold til rammeverket «COSO ERM (2017)». Denne formen for risikostyring bygger på tre grunnsteiner:

- 1) Risiko defineres nøytralt, som «usikkerhet som kan ha en positiv eller negativ innvirkning på virksomhetens evne til å nå sine mål»,
- 2) Aktuelle risikoer ses samlet, for å forstå virksomhetens helhetlige risikobilde så godt at man bedre kan utnytte potensialet for verdiskapning,
- 3) Risikostyringen skal innrettes mot å styrke grunnlaget for viktige beslutninger på alle nivåer av virksomheten, og på den måten gi grunnlag for økt verdiskapning.

Dette synet står til motsetning til et mer tradisjonelt syn på risikostyring, der:

- 1) Risiko utelukkende anses som noe som kan få et negativt utfall for virksomheten, slik at formålet med risikostyringen blir å unngå negative overraskelser som kan svekke virksomhetens resultater,
- 2) Risikostyringen bygger på en periodisk øvelse som går ut på å sette opp en samlet oversikt over aktuelle negative risikoer for virksomheten, vurdere om virksomheten har disse under kontroll, og der kontrollen anses utilstrekkelig, iverksette tiltak for å redusere risikoen.

Den mer tradisjonelle måten å betrakte risikostyring på har en klar verdi, og kan bidra til å styrke styringen av operasjonelle prosesser og unngå unødvendige tap. Men med helhetlig risikostyring kan virksomheter også oppnå proaktiv styring mot økt verdiskapning. For alle aktive virksomheter er det ikke et spørsmål om å ta risiko, men om å velge å få mest mulig ut av det risikobildet man står overfor. Som det så fint heter på engelsk «No Risk – No Reward»!



Krav til risikostyring i virksomheter er regulert i en rekke ulike lover og forskrifter, rettet mot forskjellige typer av virksomheter. Hovedprinsippene, både når det gjelder innrettingen av risikostyringen og styrets ansvar for denne, er imidlertid langt på vei de samme. IIA Norge tror derfor det kan være nyttig med en overordnet, klarspråklig veileder i helhetlig risikostyring for styremedlemmer, på tvers av organisasjonsform, sektor og bransje.

Selv om veilederen i utgangspunktet er rettet mot styremedlemmer, vil den også kunne være til nytte for andre aktører i virksomhetsstyringen, som toppledelsen, linjeledelsen og risikofunksjonen. Videre vil den vil kunne være til hjelp i arbeidet med å styrke risikostyringen i virksomheter som ikke har et styre – som eksempelvis etater i offentlig sektor.

Veiledere er utarbeidet av IIA Norges nettverk for risikostyring, ved en arbeidsgruppe som besto av Petter Kapstad (Equinor), Martin Stevens (Gjensidige), Esben Jensrud (risikoveteran) og Wilhelm Kavli (IIA Norge / sekretær).

Vi har satt spørsmålene inn i en enkel tabell, fordelt på fem temaer:

- A. Styrets rolle i risikostyringen
- B. Virksomhetens mål for risikostyringen
- C. Virksomhetens risikobilde
- D. Virksomhetens metode for risikostyring
- E. Virksomhetens risikofunksjon

A	<i>Styrets rolle i risikostyringen</i>	
A-1	<i>Forstår vi i styret hvilken rolle et styre skal spille i risikostyring av en virksomhet?</i>	Medlemmer av styret bør ha oversikt over hvilke krav lovverket stiller til styremedlemmer i en virksomhet når det gjelder risikostyring – herunder god forståelse av styrets forvaltnings- og tilsynsansvar. Videre bør styremedlemmene sette seg inn i aktuelle lovkrav som gjelder spesifikt for virksomhetens sektor og egenart.
A-2	<i>Besitter vi i styret tilstrekkelig faglig kompetanse på risikostyring?</i>	Styret bør sikre seg at det har tilstrekkelig kompetanse på helhetlig risikostyring – altså det som på engelsk gjerne omtales som <i>Enterprise Risk Management</i> (ERM). Ved sammensetning av styret bør eierne sikre at det blant styrets medlemmer er personer med solid praktisk erfaring fra risikostyring som er egnet til å styrke styrets beslutningsgrunnlag.



A-3	<i>Har vi i styret evne og vilje til å stille konstruktivt kritiske spørsmål, og ikke gi oss før vi finner frem til gode svar?</i>	Med utgangspunkt i solid forståelse av sin rolle i virksomheten, bør styret skape seg rom for å stille de enkle kritiske spørsmålene, skape og vedlikeholde en kultur for saklig kritisk dialog om virksomheten og risikobildet, og etablere et opplegg for løpende evaluering av styrets eget arbeid.
A-4	<i>Forstår vi i styret verdikjedene i virksomheten, virksomhetens strategi, og hvilke risikoer som i størst grad kan påvirke verdidriverne?</i>	Styret bør få seg forelagt en godt gjennomarbeidet visualisering av virksomhetens verdikjede, til støtte for vurderingen av virksomhetens viktigste risikoer. For å bedre forstå risiko er det avgjørende at styret forstår de største strategiske og operasjonelle verdidrivere, og hvilke risikoer som kan påvirke virksomhetens produksjon. Dette vil gi styret grunnlag for å få tilstrekkelig forståelse av virksomhetens taktiske og strategiske veivalg, og bakgrunnen for disse. Gjennom dette arbeidet bør styret få forståelse for sammenhengen mellom resultat og risikokapital, og se til at balansen mellom disse er som ønsket og forventet.
A-5	<i>Sørger styret for at virksomhetens risikovurderinger styrker grunnlaget for styrets og ledelsens beslutninger?</i>	Styrets medlemmer bør oppleve at risikovurderingene styrker grunnlaget for strategiske og andre viktige beslutninger. Der risikovurderinger er utilstrekkelige, mangelfulle eller mangler helt, bør styret etterspørre dekkende vurderinger av risikoene knyttet til slike beslutninger.
B	Virksomhetens mål for risikostyringen	
B-1	<i>Gir virksomheten uttrykk for en utfyllende og enhetlig forståelse for hvordan risikostyring skal bidra til verdiskapning?</i>	Styret bør sikre seg at risikostyringen bidrar til verdiskapningen i selskapet, og ikke kun blir et verktøy for å styre klar av potensielt negative hendelser og forhold. Det som kjennetegner helhetlig risikostyring, er nettopp at virksomheten innretter risikostyringen mot å utnytte mulighetene for å skape verdier. Styret bør forsikre seg om at det løpende gjøres en god vurdering av balansen mellom risiko og forventet avkastning / verdiskapning, som er forelagt styret for reell behandling.



B-2	<i>Har virksomheten satt et tydelig ambisjonsnivå for risikostyringen?</i>	Styret bør sette et tydelig ambisjonsnivå for risikostyringen, basert på en vurdering av virksomhetens behov. Dette skal gjøres ut fra anerkjente modenhetsmodeller og etablert god praksis innen den aktuelle bransjen. Videre bør styret sikre at det fastsatte ambisjonsnivået for risikostyringen er tilstrekkelig til at styret kan oppfylle sitt ansvar etter loven. Styret bør følge opp hvor virksomheten befinner seg i forhold til ambisjonen, og om nødvendig sikre tilstrekkelige ressurser til å nå ambisjonen. Virksomhetens overordnede prosess for risikostyring bør fastsettes i et styrende dokument som avklarer roller og ansvar.
B-3	<i>Er det samsvar og sammenheng mellom virksomhetens strategi og virksomhetens risikoprofil?</i>	Styret bør sikre at virksomheten ser risikobildet og strategien i sammenheng, slik at endringer i risikovurderingene påvirker strategien – og omvendt.
B-4	<i>Har virksomheten satt et tydelig nivå for hvor mye risiko man skal kunne ta for å få målene for verdiskapning?</i>	Styret bør løpende vurdere risiko/ lønnsomhet, på overordnet nivå og på de ulike forretningsområdene.
B-5	<i>Har virksomheten et bevisst forhold til hva som utgjør strategisk viktige risikoer for virksomheten?</i>	Styret bør sikre seg at toppledelsen og øvrige ledernivåer har et bevisst forhold til hvilke risikoer som kan ha avgjørende påvirkning på virksomheten, og at styret holdes informert om utviklingen i disse. Styret bør sikre seg at toppledelsen har dekkende planer for å sikre løpende drift. Styret bør se til at konsekvenser av geopolitisk utvikling, aktuelle katastrofesenarioer og andre potensielt viktige risikoer som ligger utenfor rammen av de alminnelige forventningene til fremtiden blir vurdert og eventuelt dekket.
B-6	<i>Er risikostyringen integrert i virksomhetens øvrige beslutnings- og styringsprosesser?</i>	Styret bør sikre at risikostyringen ikke blir lagt som en tilleggsprosess, men tvert imot ligger som del av grunnlaget for, og oppfølgingen av, alle viktige beslutninger i virksomheten.



B-7	<i>Sikrer virksomheten at alle ansatte og innleide tar ansvar for å forstå og håndtere risiko knyttet til sitt arbeidsområde?</i>	Styret bør regelmessig be om status på virksomhetens holdningsarbeid rettet mot alle i virksomheten, og hvilke tiltak toppledelsen iverksetter for å sikre en god risikokultur.
B-8	<i>Brukes internrevisjonen som et verktøy for å sikre at virksomhetens risikostyring fungerer som forutsatt?</i>	I virksomheter med internrevisjon, bør styret sikre seg at internrevisjonen gjør en selvstendig vurdering av virksomhetens risikobilde. Styrets prioritering av revisjonsoppdrag skal møte styrets behov for rimelig grad av bekreftelse av styring og kontroll på ulike deler av virksomheten, basert på risikobildet. Dette kan innebære at internrevisjonen gis i oppdrag å se på ulike sider av virksomhetens helhetlige risikostyring.
B-9	<i>Legger virksomhetens prosesser og organisering godt til rette for helhetlig risikostyring?</i>	Styret bør sikre seg at virksomhetens risikostyring er helhetlig og integrert, og ikke fragmentert og/eller rituell.
B-10	<i>Er det klart definert hvem som er eier av de ulike risikoene i virksomheten?</i>	Styret bør sikre at det er avklart hvilken person som er eier av hver av risikoene i virksomhetens risikokart, og hva som ligger i dette eierskapet.
C	Virksomhetens risikobilde	
C-1	<i>Er det satt opp en egnet struktur på virksomhetsstyringen, som sikrer styret god og uhildet informasjon om risikobildet?</i>	Styret bør se til at virksomheten er satt opp med en virksomhets-styringsstruktur som legger til rette for at risikofunksjonen kan formidle et uhildet bilde av både strategisk og operasjonell risiko til styret.
C2	<i>Legger virksomheten godt til rette for at styret kan følge med på risikobildet, og risikoer knyttet til hver enkelt av beslutnings-sakene som legges frem for styret?</i>	Styret bør sikre seg tilstrekkelig grunnlag for å følge opp endringer i risikobildet gjennom periodisk behandling, supplert med ekstraordinær behandling ved uforutsette hendelser som påvirker risikobildet i vesentlig grad. Risikoene knyttet til hver enkelt av styrets beslutningssaker bør forklares på en måte som gir styret reell forståelse for hva de innebærer.



C-3	<i>Følger styret regelmessig opp virksomhetens risikobilde?</i>	Styret bør følge opp risikobildet regelmessig og etter behov, kombinert med dypdykk på områder av vesentlig betydning. Prognoser av risikoutfall frem i tid skal måles mot egenkapital og likviditet. Styret bør se til at forsikring anses som et verktøy for å håndtere virksomhetens risikobilde, på linje med andre risikoendrende tiltak. Virksomhetens policy og praksis for forsikring bør være basert på virksomhetens risikoprofil, og integreres i risikostyringen.
C-4	<i>Har virksomheten en oppdatert oversikt over virksomhetens viktigste risikoer?</i>	Styret bør se til at virksomheten til enhver tid har god oversikt over de risikoene som har stor betydning for virksomhetens overordnede resultater på kort og lang sikt. For at styret og toppledelsen skal kunne forstå og vurdere de ulike risikoene på virksomhetsnivå, vil det være en stor fordel om risikoene gjøres reelt sammenlignbare ved at de tallfestes. Slik kvantifisering kan gjøres i kroner, eller på annen måte.
C-5	<i>Dekker virksomhetens risikostyring også midlertidige programmer og prosjekter, på linje med løpende prosesser?</i>	Styret bør sikre at risikostyring av programmer og prosjekter gjøres på linje med ordinære prosesser, og at den utføres på en måte som legger til rette for at den fungerer som en integrert del av virksomhetens helhetlige risikostyring. Styret bør forsikre seg om at ledelsen er seg bevisst risikobildet i de ulike stadiene av et prosjekt.
C-6	<i>Utnytter virksomheten potensialet som ligger i tilgjengelige data knyttet til virksomhetens drift og rammebetingelser som grunnlag for vurdering av risiko?</i>	Styret bør forsikre seg om at det ligger bekreftede kvantitative fakta og godt begrunnede beregninger til grunn for risiko-vurderinger og beslutningsgrunnlag. Styret bør sikre at potensialet som ligger i korrekt, fullstendig og rettidig data om virksomhetens drift og rammebetingelser blir godt utnyttet.
C-7	<i>Er det tydelig hvor de ulike delene av tallgrunnlaget er hentet fra, og hvilken usikkerhet som hefter ved hver av disse?</i>	Styret bør sikre seg at det får gode redegjørelser for graden av usikkerhet knyttet til tallgrunnlaget. Styret bør se til at grunnlaget for vurderingen av viktige risikoer blir etterprøvd, ved å periodisk etterspørre kvalitetssikring av data som ligger til grunn for de viktigste beslutningene i virksomheten.



D	Virksomhetens metode for risikostyring	
D-1	<i>Er virksomhetens metodikk for beregning av risiko i samsvar med god praksis?</i>	Styret bør forsikre seg om at virksomhetens metode for beregning av risiko er i tråd med god praksis, gitt virksomhetens egenart og egenskaper ved de aktuelle risikoene. Denne metoden bør være dokumentert på prinsippnivå. Hvis virksomheten beregner risikojustert avkastning, bør styret kunne se at den avkastningen som rapporteres hensyntar virksomhetens risikobilde. Dette bør inkluderes i dokumentasjonen av metoden for beregning av risiko.
D-2	<i>Er det tydelig hvilke modeller som benyttes for analyse og vurdering av datagrunnlaget, og hvilken usikkerhet som hefter ved disse?</i>	Styret bør se til at de får god informasjon om hvilke modeller som benyttes og hvordan. Uansett hvor god modellen er, og hvor godt den benyttes, vil det alltid hefte usikkerhet knyttet til de beregningene som kommer ut av analysene. Styret bør periodisk etterlyse kvalitetssikring av modellene som ligger til grunn for de viktigste beslutninger, gjennom uavhengig vurdering eller tredjepartsvurdering, etterprøving av modellen mot faktisk utvikling. Der det gjøres periodisk kvalitetssikring, bør styret få seg forelagt resultatene av disse i sin helhet.
D-3	<i>Gir metoden kontroll med hvordan alternative mulige utviklinger vil påvirke virksomhetens verdiskapning, herunder det økonomiske resultatet?</i>	Styret bør kunne se hvordan de aktuelle fremtidige utfallene er vurdert, gitt alternative utviklinger av risikobildet og foreslåtte tiltak. Her vil prognoser og scenarier være aktuelle metodiske verktøy.
D-4	<i>Inneholder virksomhetens metode for risikostyring et obligatorisk trinn for evaluering og læring?</i>	Styret bør sikre at virksomheten har en godt fungerende læringssløyfe som del av den løpende risikostyringen.



E	Virksomhetens risikofunksjon	
E-1	<i>Er fagansvaret for virksomhetens risikostyring klart definert og tydelig plassert?</i>	Styret bør sikre at virksomheten har en risikofunksjon med mandat, integritet, kompetanse og kapasitet som tillater en helhetlig risikostyring. I henhold til trelinjemodellen skal risikofunksjonen være toppledelsens redskap. Samtidig bør funksjonen i henhold til anerkjent god praksis selv presentere og svare for sine rapporter overfor styret.
E-2	<i>Har risikofunksjonen rett forståelse av sin rolle i virksomheten?</i>	Styret bør sikre at risikofunksjonen tar en proaktiv og fremoverlent rolle, som leverandør av et uhildet vurderingsgrunnlag. Funksjonen bør følge opp virksomhetens risikoeksponering i et helhetlig perspektiv – og følge utviklingen i risikobildet i tett dialog med virksomheten.
E-3	<i>Har risikofunksjonen kompetanse og kapasitet til å realisere den ambisjonen styret har satt for virksomhetens risikostyring?</i>	Styret bør sikre at funksjonen er satt opp med solid fagkompetanse på moderne risikostyring, tilpasset virksomhetens sektor og egenart. Det er her avgjørende med evne til å tilføre verdi gjennom å styrke grunnlaget for både strategiske og taktiske beslutninger – på alle nivåer i virksomheten. Styret bør se til at virksomheten vedlikeholder fagkompetansen på risikostyring, og videreutvikler metoder og teknikker. Man bør ha en oppdatert kompetansestrategi for risikofunksjonen, og styret bør årlig be om status for denne. Styret bør forsikre seg om at virksomheten har prioritert tilstrekkelige ressurser til funksjonen, slik at den har god systemstøtte, nødvendige arbeidsressurser – samt fag- og forretningskompetanse innenfor områdene strategi, finans og driftsoperasjoner.
E-4	<i>Har risikofunksjonens kommunikasjon en egnet form?</i>	Styret bør sikre at risikofunksjonens skriftlige og muntlige rapportering til styret er utformet på en måte som er godt tilpasset styrets og toppledelsens behov.



E-5	<i>Samordner risikofunksjonen sitt arbeid med andre styringsfunksjoner i virksomheten?</i>	Styret bør sikre at risikofunksjonen i større virksomheter samordner sin aktivitet med andre stabs- og støttefunksjoner, som etterlevelse/ <i>compliance</i>-funksjoner, personvernombud, kvalitetsrevisjon og internrevisjon. Målet må være å optimalisere ressursbruken og den samlede nytteverdien for virksomheten.
------------	--	---