Veileder i helhetlig risikostyring for styremedlemmer:

«Spørsmål styret bør stille om risikostyringen»

IIA Norge, 15. juli 2024

Høringsutkast fra en arbeidsgruppe fra Nettverk risikostyring i IIA Norge, bestående av Esben Jensrud, Petter Kapstad, Martin Stevens og Wilhelm Kavli (sekretær)

Innledning

Styret i alle virksomheter, både i privat og offentlig sektor, har etter norsk lov ansvar for å se til at virksomheten har etablert risikostyring i henhold til anerkjent god praksis. Denne veilederen, utgitt av den ideelle foreningen IIA Norge, består av et sett med 41 sentrale spørsmål knyttet til virksomhetens risikostyring. Ved å reise spørsmål som disse kan styremedlemmer styrke styrets og ledelsens forståelse av hvordan risikostyringen av virksomheten fungerer i dag, og hvordan den kan utvikles videre.

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 fire grunnsteiner:

1) Risiko defineres nøytralt, som «usikkerhet som kan ha en positiv eller negativ innvirkning på virksomhetens evne til å nå sine mål på alle nivåer»,
2) Virksomhetens risikostyring bistår løpende beslutningsprosesser på alle nivåer, herunder ved fastsettelse, gjennomføring og oppfølging av strategiske valg,
3) Aktuelle risikoer ses samlet, for å forstå virksomhetens helhetlige risikobilde så godt at man bedre kan utnytte potensialet for verdiskapning,
4) Risikostyringen skal både bidra til at virksomheten unngår dårlige beslutninger som fører til tap, og til at den ved å styrke grunnlaget for viktige beslutninger gir 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) Risikostyring 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 i langt større grad også oppnå proaktiv styring mot økt verdiskapning.

Selv om veilederen i utgangspunktet er rettet mot virksomheter med et styre, vil den antakelig også kunne være til nytte som et verktøy for å styrke risikostyringen i andre typer virksomheter – som eksempelvis etater i offentlig sektor.

Nr.	Spørsmål	Kommentar	Referanser
A	***Styrets rolle i risikostyringen***		
A-1	*Forstår vi i styret hvilken rolle et styre skal spille i risikostyring av en virksomhet?*	Medlemmer av styret bør ha oversikt over hvilke krav lovverket stiller til styremedlemmer i en virksomhet, når det kommer til risikostyring. Videre bør styremedlemmene sette seg inn i aktuelle lovkrav som gjelder spesifikt for virksomhetens sektor og egenart.	Temaark A.6: Styrets ansvar for risikostyring [lenke kommer] Aksjeloven § 6-12 (forvaltnings-ansvaret) og § 6.13 (tilsynsansvaret) Allmennaksjeloven § 6-12 (forvaltningsansvaret) og §§ 6-13 – (styrets tilsynsansvar) «Den norske anbefalingen om eierstyring og selskapsledelse» fra NUES (bygger på G20/OECD) IIAs Trelinjemodell [lenke kommer]
A-2	*Besitter vi i styret tilstrekkelig faglig kompetanse på helhetlig risikostyring?*	Styret bør sikre seg at det har tilstrekkelig kompetanse på helhetlig risikostyring – altså det som på engelsk gjerne omtales som Enterprise Risk Management (ERM). Ved sammensetning av styret bør eierne sikre at det blant styrets medlemmer er personer med solid erfaring fra risikostyring som er egnet til å styrke styrets beslutningsgrunnlag.	(Eventuelt nytt temaark om korrelasjon?)
A-3	*Har vi i styret tilstrekkelig evne og vilje til å kritisk stille de riktige spørsmålene, og ikke gi oss før vi finner frem til gode svar?*	Styret bør ut fra en solid forståelse av sin egen rolle i virksomheten, skape seg et 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	*Forstår vi i styret verdikjeden i virksomheten, virksomhetens strategi, og hvilke risikoer som i størst grad kan påvirke verdidriverne?*	Styret bør sikre at de har fått tilstrekkelig forståelse av virksom-hetens taktiske og strategiske veivalg, og grunnlaget for disse. 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.	Temaark A.2: Igangsettelse av risikostyringsarbeid [lenke kommer]
A-5	*Når det kommer til styring av virksomhetens viktigste risikoer, utfører vi i styret det som kan forventes av oss?*	Styret bør forstå sammenhengen mellom resultat og risikokapital, og se til at balansen mellom disse er som ønsket og forventet.	Temaark A.6: Styrets ansvar for risikostyring [lenke kommer]

B	*Mål for den helhetlige risikostyringen*		
B-1	*Gir virksomheten uttrykk for en enhetlig forståelse for hvordan helhetlig risikostyring skal bidra til verdiskapning?*	Styret bør sikre seg at risikostyringen bidrar til verdiskapningen i selskapet, og ikke kun er et verktøy for å holde kontroll med potensielle negative forhold og hendelser. Det som kjennetegner helhetlig risikostyring, er nettopp at virksomheten skal innrette risiko-styringen mot å utnytte mulighetene for å skape verdier.	IIA Norges «Veileder for virksomhetsstyring» IIA Norges «Helhetlig risikostyring – en veileder for risikofunksjonen (2024)» "COSO Enterprise Risk Management (2017)" og "ISO 31000:2018 'Risk management"
B-2	*Er det samsvar og sammenheng mellom virksomhetens strategi og virksomhetens risikoprofil?*	Styret bør sikre at virksomheten ser risikobildet og strategien i sammenheng, slik at endringer i risikovurderingene påvirker strategien – og omvendt.	IIA Norges «Helhetlig risikostyring – en veileder for risikofunksjonen (2024)»
B-3	*Har virksomheten satt et tydelig nivå for hvilken risikoeksponering den kan ha i forhold til verdiskapning?*	Styret bør løpende vurdere risiko/ lønnsomhet, på overordnet nivå og på de ulike forretningsområdene.	Temaark B.1: Risikoappetitt [lenke kommer]
B-4	*Har virksomheten et bevisst forhold til hva som utgjør eksistensielle og viktige risikoer for virksomheten?*	Styret bør sikre seg at toppledelsen og øvrige ledernivåer har et bevisst forhold til hvilke risikoer som kan påvirke virksomhetens eksistens, og at styret holdes informert om utviklingen i disse.	
B-5	*Har virksomheten satt et tydelig ambisjonsnivå for risikostyringen?*	Styret bør sette et tydelig ambi-sjonsnivå for risikostyringen ut fra anerkjente modenhetsmodeller og etablert god praksis for sin bransje. Videre bør styret sikre at risiko-styringen er tilstrekkelig til å gi styret grunnlag for å oppfylle sitt forvaltnings- og tilsynsansvar. Virksomhetens overordnede prosess for risikostyring bør dokumenteres gjennom et styrende dokument som avklarer roller og ansvar.	Temaark C.1: Helhetlig risikostyring - modenhetsanalyse [lenke kommer] Aksjeloven § 6-12 (forvaltnings-ansvaret) og § 6.13 (tilsynsansvaret) Allmennaksjeloven § 6-12 (forvaltningsansvaret) og §§ 6-13 – (styrets tilsynsansvar)
B-6	*Er virksomhetens strategiske målsetninger bygget på gode vurderinger av balansen mellom risiko og forventet avkastning / verdiskapning?*	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-7	*Er risikostyringen integrert i virksomhetens øvrige beslutnings- og styringsprosesser?*	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-8	*Hvordan sikrer virksomheten at alle ansatte og innleide tar en aktiv rolle for å forstå og håndtere risiko knyttet til sitt arbeidsområde?*	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.	Temaark A.1: Risikostyringsramme-verk og -standarder [lenke kommer]
B-9	*Brukes internrevisjonen som et verktøy for å sikre at virksomhetens risikostyring fungerer som forutsatt?*	I virksomheter med internrevisjon, bør styret sikre seg at denne følger opp sitt ansvar for å etablere og vedlikeholde en selvstendig vurdering av virksomhetens risikobilde. Styrets prioritering av revisjons-oppdrag skal møte styrets behov for rimelig grad av bekreftelse på styring og kontroll på ulike deler av virksomheten, basert på risikobildet. Dette kan innebære at intern-revisjonen gis i oppdrag å revidere ulike sider av virksomhetens helhetlige risikostyring.	"IIA Global Internal Audit Standards 2024", "Purpose of Internal Auditing", s. 15
C	***Risikostyringens datagrunnlag***		
C-1	*Tar vurderingene av virksomhetens viktigste risikoer utgangspunkt i en god forståelse av virksomhetens verdikjede?*	Styret bør få seg forelagt en godt gjennomarbeidet visualisering av virksomhetens verdikjede, som grunnlag for å vurdere vesentlighet-en av virksomhetens risikoer.	Temaark A.2: Fremgangsmåte ved oppbygging av risikostyringsarbeidet [lenke kommer]
C-2	*Utnytter virksomheten tilgjengelige data knyttet til virksomhetens drift og rammebetingelser som grunnlag for vurdering av risiko på en god måte?*	Styret bør forsikre seg om at det ligger bekreftede kvantitative fakta og godt begrunnede beregninger til grunn for risikovurderinger og beslutningsgrunnlag. Styret bør sikre at potensialet som ligger i korrekt, fullstendig og rettidig data om virksomhetens drift og rammebetingelser blir godt utnyttet.	
C-3	*Er det tydelig hvor de ulike delene av tallgrunnlaget er hentet fra, og hvilken usikkerhet som hefter ved disse?*	Styret bør sikre seg at det får gode redegjørelser for graden av usikkerhet knyttet til tallgrunnlaget.	
C-4	*Blir datagrunnlaget til grunn for viktige risikoer etterprøvd, og i så fall hvordan?*	Styret bør periodisk etterlyse kvalitetssikring av datagrunnlaget som ligger til grunn for de viktigste beslutninger.	
D	***Metode for risikostyring***		
D-1	*Er virksomhetens metodikk for beregning av risiko i samsvar med beste praksis?*	Styret bør forsikre seg om at virk-somhetens metode for beregning av risiko er i tråd med beste praksis, gitt virksomhetens egenart og egenskaper ved de aktuelle	Temaark B.7: Kvantifisering av risiko [lenke kommer]

		risikoene. Denne metoden bør være dokumentert på prinsippnivå.	
D-2	*Hvis virksomheten beregner risiko-justert avkastning, er metoden som benyttes i tråd med anerkjent god praksis?*	Styret bør kunne se at den avkastningen som rapporteres hensyntar virksomhetens risikobilde. Dette bør inkluderes i dokumentasjonen av metoden for beregning av risiko.	Temaark B.7: Kvantifisering av risiko [lenke kommer]
D-3	*Er det tydelig hvilke modeller som benyttes for analyse og vurdering av datagrunnlaget, og hvilken usikkerhet som hefter ved disse?*	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.	
D-4	*Blir risikomodellen til grunn for viktige beslutninger etterprøvd, og i så fall hvordan?*	Styret bør periodisk etterlyse kvalitetssikring av modellene som ligger til grunn for de viktigste beslutninger, gjennom uavhengig tredjepartsvurdering, etterprøving av modellen mot faktisk utvikling. Der det gjøres periodisk kvalitets-sikring, bør styre få seg forelagt resultatene av disse i sin helhet.	
D-5	*Gir metoden kontroll med hvordan alternative mulige utviklinger vil påvirke virksomhetens verdiskapning, herunder det økonomiske resultatet?*	Styret bør kunne se hvordan de aktuelle fremtidige utfallene er vurdert, gitt alternative utviklinger av risikobildet. Her vil prognoser og scenarier være aktuelle metodiske verktøy.	Aksjeloven § 3-4 (krav til egenkapital og likviditet) og § 3-5 (handleplikt)
D-6	*Hvordan benyttes virksomhetens risikovurderinger som underlag for strategiske og andre vesentlige beslutninger?*	Styrets medlemmer bør oppleve at risikovurderingene styrker grunnlaget for styrets beslutninger. Styret bør etterlyse manglende eller mangelfulle vurderinger av risikoene knyttet til styrets beslutninger.	
D-7	*Er virksomhetens prosesser og organisering tilrettelagt for helhetlig risikostyring?*	Styret bør sikre seg at virksomhet-ens risikostyring er helhetlig og integrert, og ikke fragmentert og/eller rituell.	IIA Norges «Helhetlig risikostyring – en veileder for risikofunksjonen (2024)»
D-8	*Er det klart definert hvem som er eier av de ulike risikoene i virksomheten?*	Styret bør ut fra virksomhetens risikokart sikre at det er avklart hvilken person som er eier av hver av risikoene i kartet, og hva som ligger i dette eierskapet.	IIA Norges «Helhetlig risikostyring – en veileder for risikofunksjonen (2024)», kapittel 3 Temaark A.1: Risikostyringsramme-verk og -standarder [lenke kommer]
D-9	*Inneholder virksomhetens metode for risikostyring et obligatorisk trinn for evaluering og læring?*	Styret bør sikret at virksomheten har en godt fungerende læringssløyfe som del av den løpende risikostyringen.	

E	Virksomhetens risikobilde		
E-1	*Er det satt opp en egnet struktur på virksomhetsstyringen, som sikrer styret god og uhildet informasjon om risikobildet?*	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.	IIA Norges «Helhetlig risikostyring – en veileder for risikofunksjonen (2024)», kapittel 2 Temaark A.1 Risikostyringsrammeverk og -standarder [lenke kommer]
E-2	*Hvordan legger virksomheten til rette for at styret kan føre tilsyn med risikobildet, og risikoer knyttet til hver enkelt av beslutnings-sakene som legges frem for styret?*	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.	
E-3	*Følger styret regelmessig opp virksomhetens risikobilde?*	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.	Temaark B.3 Risikorapportering og kommunika-sjon med styret [lenke kommer] Aksjeloven § 3-4 (krav til egenkapital og likviditet) og § 3-5 (handleplikt)
E-4	*Har virksomheten en oppdatert oversikt over virksomhetens viktigste risikoer?*	Styret bør se til at virksomheten har god oversikt over de risikoene som har stor betydning for virksom-hetens 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.	Temaark A.1: Risikostyringsrammeverk og -standarder [lenke kommer]
E-5	*Er katastrofesenarioer, med lav sannsynlighet og tilsvarende høy konsekvens, vurdert i risikostyringen?*	Styret bør se til at også relevante risikoer som ligger utenfor den forventede utviklingen blir vurdert og dekket.	Temaark B.2: Risiko og beslutningstaking [lenke kommer]
E-6	*Dekker virksomhetens risikostyring også midlertidige programmer og prosjekter på linje med løpende prosesser?*	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.	
E-7	*Er virksomhetens policy og praksis for forsikring basert på virksomhetens risikoprofil, og integrert i risikostyringen?*	Styret bør se til at forsikring anses som et verktøy for å håndtere virksomhetens risikobilde, på linje med andre risikoendrende tiltak.	

F	*Virksomhetens risikofunksjon*		
F-1	*Er fagansvaret for virksomhetens risikostyring klart definert og tydelig plassert?*	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 topplede lsens redskap. Samtidig bør funksjonen i henhold til anerkjent god praksis selv presentere og svare for sine rapporter overfor styret.	IIA Norges «Helhetlig risikostyring – en veileder for risikofunksjonen (2024)», kapittel 2 Temaark B.9: Etikk for risiko-funksjonen [lenke kommer] Temaark 3 linjemodellen
F-2	*Hvordan forstår risikofunksjonen sin rolle i virksomheten?*	Styret bør sikre at risikofunksjonen tar en proaktiv og fremoverlent rolle, som leverandør av et uhildet vurderingsgrunnlag. Funksjonen bør følge opp virksom-hetens risikoeksponering i et helhetlig perspektiv – og følge utviklingen i risikobildet i tett dialog med virksomheten.	
F-3	*Har risikofunksjonens kommunikasjon en egnet form?*	Styret bør sikre at risikofunksjonens skriftlige og muntlige rapportering til styret er utformet på en måte som er godt tilpasset styrets behov.	Temaark B.3: Risikorapportering og kommunikasjon med styret [lenke kommer]
F-4	*Har virksomheten prioritert ressurser slik at risikofunksjonen kan fylle sin rolle?*	Styret bør forsikre seg om at risikofunksjonen har tilstrekkelig systemstøtte, arbeidsressurser – samt fag- og forretningskompetanse innenfor områdene strategi, finans og driftsoperasjonene. Styret bør gjøre en analyse av sitt behov, og forsikre seg om at virksomheten har definert ambisjonsnivået, hvor virksomheten befinner seg i forhold til dette, og hvilke ressurser og kompetanse som skal til for å nå ambisjonen.	Temaark A.7: Kompetansekrav til risikofunksjonen [lenke kommer] Temaark C.1: Helhetlig risiko – modenhetsanalyse [lenke kommer]
F-5	*Har risikofunksjonen kompetanse til å realisere den ambisjonen styret har satt for virksomhetens risikostyring?*	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.	Temaark A.7 Kompetansekrav til risikofunksjonen [lenke kommer]
F-6	*Hvordan sørger virksomheten for å vedlikeholde fagkompetansen på risikostyring, og videreutvikle metoder og teknikker?*	Styret bør sikre at virksomheten har en oppdatert kompetansestrategi for risikofunksjonen, og regelmessig be om status på denne.	

F-7	*Hvordan samordner risiko-funksjonen sitt arbeid med andre styringsfunksjoner i virksomheten?*	Styret bør sikre at risikofunksjonen i større virksomheter samordner sin aktivitet med andre stabs- og støtte-funksjoner, som etterlevelse/ Compliance-funksjoner, personvern-ombud, kvalitetsrevisjon og intern-revisjon. Målet må være å optimal-isere ressursbruken og den samlede nytteverdien for virksomheten.	IIA Norges «Helhetlig risikostyring – en veileder for risikofunksjonen (2024)», punkt 2.6 (Eventuelt nytt temaark om «Legal compliance» og «Market compliance»?) - eller oppdatering av veileder for Compliance funksjonen?