

REVIDERTE RETNINGSLINJER FOR RISIKOSTYRING I HELSE NORD –

1. Innledning

Dokumentet erstatter *Retningslinjer for risikostyring Versjon 2.0* av 20. januar 2015, og gir overordnede retningslinjer for organisering og gjennomføre risikostyringen i Helse Nord.

Formålet med aktiv risikostyring er å forbedre organisasjonens evne til å oppnå fastsatte mål.

Retningslinjene tar utgangspunkt i rammeverket utgitt av COSO¹ i 2017, *Helhetlig Risikostyring – Integrering med strategi og måloppnåelse (Enterprise Risk Management – Aligning Risk with Strategy and Performance)*, men henter også inspirasjon fra andre dokumenter og rammeverk, særlig *ISO 31000:2018 Risikostyring Retningslinjer*.

2. Nærmere om risikostyring

2.1 Definisjon av risikostyring

COSO definerer risikostyring som:

«Den kultur, evne og praksis/anvendelse, integrert med fastsetting av strategi og måloppnåelse, som organisasjoner baserer seg på for å styre risiko når verdier skapes, opprettholdes og realiseres.»

ISO 31000:2018 definerer risikostyring som:

«Koordinerte aktiviteter for å rettlede og kontrollere en organisasjon med hensyn til risiko.»

Fellestrekket er *hensikten*; å rettlede og kontrollere mht. risiko.

COSOs definisjon tar også med elementer/egenskaper som må være på plass og hva de må integreres med, for at risikostyringen skal bidra til å skape og realisere verdier.

2.2 Definisjon av risiko

COSO definerer risiko som «en hendelse kan inntreffe og påvirke oppnåelse av strategiske og forretningsmessige mål.»

ISO definerer risiko slik: *Usikkerhetens innvirkning på mål.*

¹ Committee of Sponsoring Organizations of the Treadway Commission

ISO tilføyer at: «En virkning er et avvik fra det forventede. Den kan være positiv, negativ eller begge deler og kan ta for seg, skape eller resultere i muligheter og trusler.»

COSO knytter risikoen opp mot hendelser, ISO mot usikkerhet generelt. Begge lar begrepet risiko fange opp så vel positive som negative effekter på måloppnåelsen, dvs. «oppside-risikoen» er også med.

3. Prosess/Grunnleggende modeller

COSO-rammeverket kan illustreres slik figur 1 viser: 5 trinn på veien fra formål, visjon og kjerneverdier via strategiutvikling, formulering av virksomhetsmål, gjennomføring, og fram til forbedret måloppnåelse.

5 komponenter med 20 elementer som bør være tilstende, utgjør en god helhet rundt virksomhetsstyring. Det vises til vedlegg A for beskrivelse av de 20 elementene.



Figur 1: Rammeverk for helhetlig risikostyring – Kilde: COSO

ISO har tilsvarende budskap og presiserer bl.a. at «risikostyringsprosessen bør være en integrert del av ledelse og beslutningstaking og være integrert i organisasjonens struktur, drift og prosesser. Den kan anvendes på strategisk nivå, operasjonelt nivå, programnivå eller prosjektnivå.»

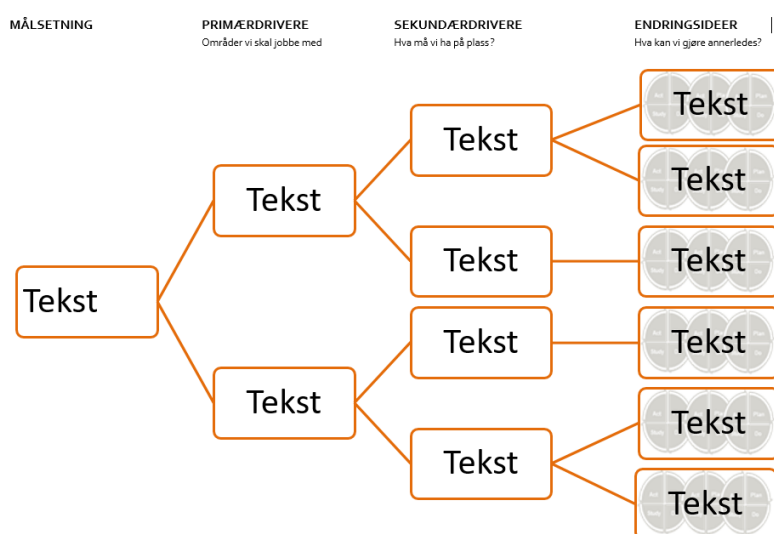
4. Risikostyring i Helse Nord

Risikostyring tar utgangspunkt i definerte strategier og mål.

Styringsmålene fra eier, gitt i oppdragsdokument og foretaksmøteprotokoll, er overordnet i målhierarkiet.

Helse Nord's «*Regional Utviklingsplan 2035*» er et annet utgangspunkt for å vurdere risiko. Oppdragsdokument til helseforetakene er inndelt etter samme logikk som Regional Utviklingsplan.

I tråd med metodikken for forbedringsarbeid oppfordres det til å utarbeide «driverdiagram²», se figur 2. Driverdiagram visualiserer sammenhengen mellom forbedringsarbeidets mål og de endringer og tiltak en tror vil ha effekt på målet.



Figur 2: Driverdiagram – Kilde Pasientsikkerhetsprogrammet I Trygge Hender

Primære og sekundære drivere kan sammenliknes med kritiske suksess-faktorer, og er et naturlig utgangspunkt for overordnet risikovurdering i helseforetakene.

Risikovurdering skal også gjøres i forkant av vesentlige endringer i drift, organisering eller gjennomføring av prosjekt.

² Driverdiagram: visualiserer sammenheng mellom forbedringsarbeidets mål og endringer og tiltak en tror kan ha effekt på målet. Referanser: Pasientsikkerhetsprogrammet «I trygge hender»: *Forbedringsguiden*. Institute for Healthcare Improvement. *QI Essentials Toolkit: Driver Diagram*.

Risikostyringen skal gjennomføres i samsvar med COSO-rammeverket og omfatte følgende:

Styrets ansvar

Styret har en sentral rolle i beslutninger på strategisk nivå, og må vurdere foretakets strategiske risiko.

Ansvarer innebærer bl.a. å ta stilling til om foretakets mål og prioriteringer er i samsvar med, og dekkende for lovkrav og målene eier har fastsatt, og om de er egnet til å bidra til å skape, opprettholde og realisere foretaksgruppens verdier.

Styret bør også ha siste ord i spørsmål om foretakets risikotoleranse, inklusive prioriteringene mellom målsettinger, se punktet *Konkrete målsettinger*.

Temaene skal behandles av styret minimum én gang per år.

Styrets rapportering til eier skal orientere om risikostyrings-arbeidet i foretaket. Rapportene skal særlig gjøre rede for de risikoene som er viktigst å håndtere akkurat nå, og som derfor har sterkest fokus («Topp 5 risiko» e.l.).

Konkrete mål

Mål og «drivere» for måloppnåelse må konkretiseres og operasjonaliseres nærmere. Tiltakene som er listet opp under målområdene i Regional Utviklingsplan er relevante å se til for å identifisere sekundære drivere og indikatorer for måloppnåelse.

Prioritere målene

Det er ikke nødvendigvis slik at alle målsettingene må risikovurderes hvert år. Det viktigste er en vurdering av hvor foretaket har størst risiko. Normalt er 2-5 målsettinger per målområde tilstrekkelig å risikovurdere og følge opp.

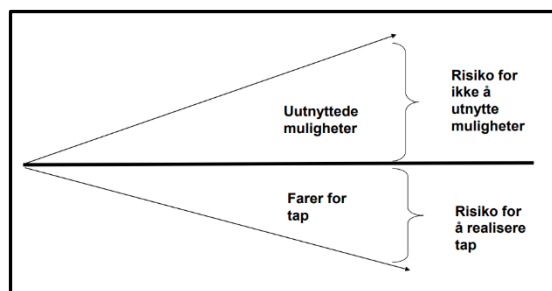
Tidsperspektivene som angis i Regional Utviklingsplan 2035 og prioriteringene som fremgår av øvrige plandokumenter som økonomisk langtidsplan og årlig oppdragsdokument, gir viktig input til den årlige prioriteringen.

Slik prioritering er reelt sett å beslutte hvilken risikotoleranse/risikovillighet foretaket skal ha. Å nedprioritere en målsetting er et valg om å leve med situasjonen slik den er. Å sette fokus på en målsetting/prioritere den, er et valg om å ville avklare om risikoen er akseptabel og/eller om tiltak må settes i verk.

Organisering av risikostyringsarbeidet

Foretaket skal dokumentere hvordan risikostyringen organiseres og gjennomføres, i samsvar med retningslinjene. Her skal bl.a. følgende fremgå:

- A. *Hvem som har det daglige ansvaret for risikostyringen i foretaket*
Ansvaret bør være på høyt nivå i organisasjonen, og helst hos en person som i liten grad har ansvar for daglige driftsoppgaver. Dette for å ivareta prinsippet om «armlengdes avstand».
- B. *Hvordan målsettinger som inngår i risikostyringen velges ut og prioriteres*
- C. *Hvem som skal delta i vurderingene, og hvordan vurderingen skal gjennomføres*
Medarbeiderne som kjenner aktivitetene best og som skal iverksette eventuelle oppfølgingstiltak i etterkant må involveres. For mange involverte kan gå på bekostning av effektiviteten.
- D. *Oppfølging etter risikovurdering*
Foretaket skal ha klare rutiner for hvordan man beslutter å iverksette tiltak, hvordan ansvar fordeles og hvordan foretaket følger opp at tiltakene blir iverksatt og har ønsket effekt. Herunder involvering av ledergruppe o.a.
- E. *Oppside-risiko*
Tradisjonelt har risikostyringsarbeidet vært mest opptatt av å unngå at noe går galt. Risikostyring har i mindre grad vært vurdering av å ta i bruk åpenbare muligheter for betydelig gevinst og forbedring. Foretaket bør derfor beskrive hva som kan gjøres for å bidra til holdninger som sikrer at risikostyringen legger til rette for å «gripe mulighetene». Oppside- og nedsiderisiko kan illustreres jf fig. 3:



Figur 3: Illustrasjon oppside- og nedsiderisiko

- F. *Verktøy, maler og matriser*
Foretakene har oppfordres til å ta i bruk felles risikovurderingsverktøy, distribuert fra Helse Nord RHF. Andre verktøy kan også benyttes.
- G. *Rapportering*
Helseforetakene skal beskrive rutinene for rapportering til eget styre og andre interne organ. Risikovurderingen skal være en del av tertialrapporteringen til Helse Nord RHF. I særskilte tilfeller vil det være naturlig at styret i helseforetak løfter risikorapporteringen til Helse Nord RHF hyppigere enn dette.

H. *Årshjul/fremdriftsplan for risikostyringen*

Foretaket skal utarbeide en forklarende oversikt over hva som skal gjøres, når og hvem som har ansvaret.

Vedlegg A: Komponenter og prinsipper

Virksomhetsstyring og kultur

1. **Styret fører tilsyn med risiko** – Styret fører tilsyn med strategien og utøver sine virksomhetsstyringsforpliktelser som støtte for ledelsen i arbeidet med å gjennomføre strategien og nå virksomhetens mål.
2. **Etablerer driftsstrukturer** – Organisasjonen etablerer driftsstrukturer i arbeidet med å gjennomføre strategien og nå virksomhetens mål.
3. **Definerer ønsket kultur** – Organisasjonen definerer den atferd som karakteriserer enhetens ønskede kultur.
4. **Er opptatt av og viser forpliktelse til kjerneverdier** – Organisasjonen er opptatt av og viser forpliktelse til enhetens kjerneverdier.
5. **Rekrutterer, utvikler og beholder medarbeidere med ønskede egenskaper** – Organisasjonen er opptatt av å bygge menneskelig kapital som er i samsvar med strategien og virksomhetens mål.

Fastsettelse av strategi og mål

6. **Analyserer omgivelsene virksomheten opererer i** – Organisasjonen vurderer potensielle virkninger omgivelsene kan ha på risikoprofilen.
7. **Definerer risikoappetitten** – Organisasjonen definerer risikoappetitten som en del av prosessen med å skape, bevare og realisere verdi.
8. **Evaluerer alternative strategier** – Organisasjonen evaluerer alternative strategier og den potensielle innvirkning disse kan ha på risikoprofilen.
9. **Formulerer virksomhetens mål** – Organisasjonen vurderer risiko når den på ulike nivåer etablerer virksomhetens mål, som er i samsvar med strategien og støtter opp om den.

Gjennomføring

10. **Identifiserer risiko** – Organisasjonen identifiserer risiko som påvirker gjennomføringen av strategien og oppnåelse av virksomhetens mål.
11. **Vurderer alvorligheten av risiko** – Organisasjonen vurderer hvor alvorlig risikoen er.
12. **Prioriterer risikoer** – Organisasjonen prioriterer risikoer som grunnlag for beslutninger om hvordan disse skal håndteres.
13. **Iverksetter risikohåndtering** – Organisasjonen identifiserer og velger hvordan risikoen skal håndteres.
14. **Utvikler porteføljesyn** – Organisasjonen utvikler og evaluerer et porteføljesyn på risiko.

Gjennomgang og revurdering

15. **Evaluerer vesentlige endringer** – Organisasjonen identifiserer og evaluerer endringer som i vesentlig grad kan påvirke strategien og virksomhetens mål.
16. **Gjennomgår risiko og måloppnåelse** – Organisasjon gjennomgår enhetens måloppnåelse og vurderer risiko.
17. **Tilstreber forbedring av den helhetlige risikostyringen** – Organisasjonen tilstreber kontinuerlig forbedring av den helhetlige risikostyringen.

Informasjon, kommunikasjon og rapportering

18. **Drar nytte av informasjonssystemer** – Organisasjonen drar nytte av enhetens informasjons- og teknologisystemer for å understøtte den helhetlige risikostyringen.
19. **Kommuniserer risikorelatert informasjon** – Organisasjonen bruker kommunikasjonskanaler til å understøtte den helhetlige risikostyringen.
20. **Informerer om risiko, kultur og måloppnåelse** – Organisasjonen informerer om risiko, kultur og måloppnåelse på flere nivåer og på tvers av enheten.