

Revisjonsrapport

Risikostyring ved St. Olavs hospital HF

Versjon: 4.0
Dokumentstatus: Godkjent
Forfatter: Jørgen Midtlyng
Godkjent av: Jørgen Midtlyng
Godkjent dato: 14.04.2020

Dokumenthistorikk

VERSJON	DATO	VERSJONSBESKRIVELSE
1.0	2020-02-21	Utgitt for intern kvalitetssikring
2.0	2020-03-02	Utgitt for faktaverifikasjon
3.0	2020-04-14	Oppdatert etter faktaverifikasjon. Redaksjonelle endringer i Innledning og sammendrag. Oppdatert kap. 4 vedr. datoer og faktaverifikasjon. Oppdatert kapittelreferanser i oversiktstabell for anbefalinger.
4.0	2020-04-14	Vurdert mht. u.off. Ikke grunnlag for unntak. Rapporten frigis offentlig.

Innhold

Innledning	4
Sammendrag	5
Oversikt over anbefalinger	6
1. Bakgrunn	7
2. Innretning, mål og revisjonsunderlag for revisjonen	7
3. Revisjonens funn, merknader og anbefalinger	8
3.1. Vurderinger i forstudien	8
3.2. Vurdering av regionalt rammeverk for risikostyring	8
3.3. Risikostyring	9
3.4. Pliktige risikovurderinger	11
3.5. Test av bias i risikovurdering	13
3.6. Likviditetsrisikovurdering	14
4. Gjennomføring av revisjonen	16
Appendiks A: Oversikt over revisjonsaktiviteter	17
Appendiks B: Faglig grunnlag for vurderinger og anbefalinger	18
Appendiks C: Intervjuguide vedr. mislighetsrisiko	21
Appendiks D: Forklaring til <i>bias</i> i risikovurderinger	22

Innledning

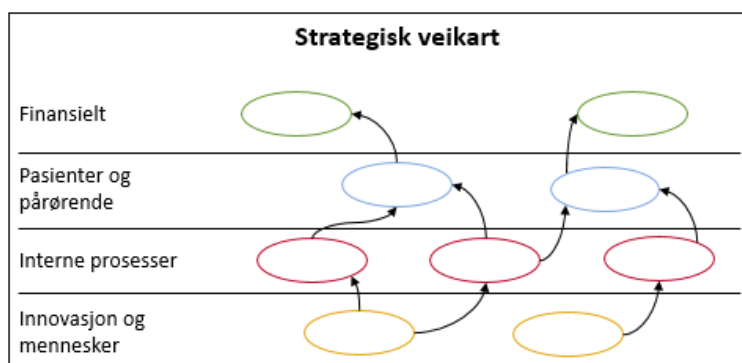
I arbeidet med denne revisjonen er lagt vekt på å oversette eiers styringskrav om risikostyring til kriterier og å vurdere helseforetakets løsninger ut fra det. Observert forbedringspunkter er også gitt på samme grunnlag.

Innledningsvis er det lagt vekt på å klargjøre hva *helhetlig risikostyring* betyr. *Helhetlig* er vanligvis brukt når risikostyringen er forankret i strategi og integrert med helseforetakenes arbeidsprosesser. Den generelle sammenhengen er imidlertid litt mer sammensatt. Systematikken er langt på vei forklart i anerkjente standarder om risikostyring (COSO ERM og NS-ISO 31000). Knytningen til strategisk retning er ikke like grundig forklart, og er derfor belyst med utgangspunkt i mikroøkonomisk teori, som belyser hvordan risikostyring er knyttet til ulike strategiske perspektiver: innovasjon og mennesker (som handler om læring og vekst), kvalitet i interne arbeidsprosesser, forholdet til brukerne/pasienter og pårørende, og finansielle størrelser. Derav begrepet *helhetlig*.

Figuren nederst på siden er ment å illustrere hvordan strategi er oversatt til strategiske prosjekter knyttet sammen gjennom strategiske veikart (Kaplan & Norton 2007), til en helhet som omfatter alle de fire strategiske perspektivene. Risikostyring knyttet til strategisk retning omfatter derfor både å styre prosjekter/tiltak etter KPI'er i denne systematikken, og å aggregere risiko til hvert strategiske perspektiv. Denne delen av revisjonen er utført med utgangspunkt i Regionalt rammeverk for risikostyring, Strategi 2030 og Helse Midt-Norges finansstrategi.

Derne er det lagt vekt på helseforetakslovens bestemmelser om partsstilling og ansvar. Partsstillingen definerer hvem som har rettigheter og plikter i forhold til styring av risiko, og ansvaret definerer hvem som bærer risiko for underliggende foretaks forpliktelser. Dette har vært spesielt viktig i vurdering av helseforetakenes arbeid med pliktig risikovurdering og -styring av IKT-investeringer. Slike investeringer gjennomføres i prosjekter organisert under regionalt helseforetak, mens plikten til risikostyring og internkontroll ligger hos de enkelte helseforetakene. Denne delen av revisjonen er utført med utgangspunkt i kontrollmiljøet for forebygging og avdekking av misligheter.

Til sist er det sett nærmere på forhold som kan påvirke og fordreie risikovurderinger, såkalt *bias*. Arbeidet er avgrenset til å se på organisasjons*bias* og er utført med utgangspunkt i arbeidet med anskaffelse, gjennomføring og drift av ny regnskaps og økonomiløsning i Helse Midt—Norge.



Sammendrag

Det er vurdert hvorvidt helseforetaket har etablert en prosess for helhetlig risikostyring, og om helseforetaket gjennomfører pliktige risikovurderinger og håndterer risiko som ikke er akseptabel. I vurderingen av helhetlig risikostyring er det sett nærmere på arbeidet med likviditetsrisiko. I arbeidet med pliktig risikovurdering er det sett nærmere på risikoanalyse i kontrollmiljøet for å forebygge og avdekke misligheter. Generelt for risikovurdering er det sett nærmere på forhold som kan fordreie vurderingene (bias) slik at beslutningstakere ikke får et mest mulig rettviseende beslutningsgrunnlag.

Internrevisjonen kan foreløpig ikke bekrefte at det regionale rammeverket for risikostyring er tilstrekkelig utviklet. Det kan heller ikke bekreftes at St. Olavs hospital HF egenhendig har utviklet og innført et helhetlig system for risikostyring som bl.a. omfatter en risikoradar.

Det som imidlertid kan bekreftes at helseforetaket har etablert et godt system for å gjennomføre risikovurderinger. På de områdene som internrevisjonen har vurdert, er det påvist at praksis for risikovurderinger varierer fra svært godt (innen beredskap) til ikke tilstrekkelig utført (mislighetsrisikovurdering).

Det regionale rammeverket inneholder grunnleggende elementer som anbefales i anerkjente standarder (rammeverk, prinsipper og prosess), men elementene er ikke fullstendig utviklet, satt i system, eller forankret i Helse Midt-Norges strategi. Med referanse til finansstrategien er det pekt på muligheten for bedre risikostyringen gjennom å gå noe lenger i å tallfeste likviditetsmessige virkninger i investeringer og å tilrettelegge for å registrere likviditetsmessig virkning av risiko i systemet for risikostyring. Med referanse til de anerkjente standardene er det pekt på muligheter for å komplettere rammeverket.

Organiseringen av IKT-investeringer er vurdert å være spesielt utsatt for fordreining av risikovurdering, eller såkalt organiasjonsbias. Det gjelder spesielt når både prosjektgjennomføring og drift innenfor helseforetakenes ansvarsområder gjennomføres og ledes på regionalt nivå, og det oppstår personidentiske roller gjennom flere prosjektfaser, i systemeierskap og regional eierrolle. Dette kan utilsiktet sette personer i krevende etiske situasjoner, og det kan reises spørsmål ved om helseforetakene har tatt tilstrekkelig hensyn til bias og slikt sett gjennomført plikten til risikostyring og internkontroll på en tilstrekkelig måte. Dette kan forbedres gjennom å komplettere rammeverket som nevnt ovenfor.

Internrevisjonen vil trekke fram positivt at det er etablert en tertialvis rapporteringsrutine for risiko. De underliggende vurderingene gir et visst bilde på risikosituasjonen og et grunnlag for å håndtere risiko. Videre er det identifisert god dokumentstruktur for styringsdokumenter om risiko. Det er også allerede etablert et system for KPI'er i statusrapporteringen som etter internrevisjonens vurdering godt lar seg integrere med strategisk forankrede KPI'er.

Internrevisjonen har gitt 20 anbefalinger som er samlet i egen tabell med referanser til kapittel hvor anbefalingen er diskutert. Internrevisjonen vurderer at revisjonsmålet er nådd.

Oversikt over anbefalinger

Nr.	Anbefalinger til St. Olavs hospital HF	Kap.
1	Bygg videre på Rammeverk for risikostyring i Helse Midt-Norge. Roller og ansvar samt rammeverkets anvendelsesområder bør videreføres og videreutvikles.	3.2
2	Ta utgangspunkt i modeller for verdiskapning og verdifangst for å knytte rammeverk for risikostyring til pasientbehandlingen, finansstrategien og de finansielle rammene.	3.3.2
3	Bidra til å knytte rammeverket til strategi og strategiske mål.	3.2
4	Bestem strategiske KPI'er med utfallsrom og terskler	3.2
5	Bidra til å velg normativ og kvalitetssikret standard for risikostyringen.	3.2
6	Bidra til å forenkle begrepsavklaringene i rammeverket.	3.2
7	Prosesen for risikostyring i rammeverket må kompletteres.	3.2
8	Sikre at det blir etablert risikoradar	3.3.2
9	Struktur i EQS ID 9399 Metode for risikovurdering anbefales opprettholdt og videreutviklet.	3.3.2
10	Knytning mellom risikoområder og konsekvensgradering (EQS ID 9399) samt skala for sannsynligheter og konsekvensgradering (hjelpeskjema nr. 2) anbefales opprettholdt og videreutviklet.	3.3.2
11	Etabler årlig risikoanalyse for å vedlikeholde kontrollmiljø for å forebygge og avdekke misligheter	3.4.2
12	Bidra til å konkretisere retningslinjer i antikorrupsjonsprogrammet vedr. risikovurdering for å styrke kontrollmiljøet mot misligheter.	3.4.2
13	Etabler skriftlig kommunikasjon vedr. 0-toleranse for misligheter	3.4.2
14	Etabler kategori for mislighetsrisiko i meldesystemet	3.4.2
15	Oppdater stillingsbeskrivelser for kontrollere til å omfatte vurdering av mislighetsrisiko.	3.4.2
16	Bidra til å etablere en oppmerksomhet omkring forekomst og virkning av bias i Helse Midt-Norges rammeverk for risikostyring og i de etiske retningslinjene.	3.5.2
17	Ta hensyn til bias i egne risikovurderinger	3.4.2
18	Bidra til å sikre at økonomistyringsmodellen i Helse Midt-Norge ivaretar den lovmessige pliktstrukturen i forhold til risikostyring og internkontroll	3.4.2
19	Bidra til å undersøke om det er mulig å etablere likviditetsrapporter i regnskaps- og økonomiløsningen.	3.6.2
20	Bidra til mer bruk av finansiell informasjon i arbeid med gevinstrealisering	3.6.2

1. Bakgrunn

Eiers krav til de regionale helseforetakene om å etablere systemer for risikostyring har lang historikk. Kravet ble første gang stilt i 2008¹ og er siden da gjentatt flere ganger. Internrevisjonen i Helse Midt-Norge undersøkte status i 2015 og fastslo at det var behov for å videreutvikle felles og helhetlige systemer og at ledelsens kunnskap om risikostyring må styrkes. Det regionale styrets fattet vedtak om å intensivere arbeidet med vekt på overordnede retningslinjer, opplæring og årlig rapportering².

Overordnede retningslinjer, opplæring og årlig rapportering ble utviklet og iverksatt i perioden 2016 – 2018. Rapporteringen har kommet i gang med tertialvis regelmessighet.

Internrevisjonen i Helse Midt-Norge fikk oppdraget i forbindelse med styrets behandling av sak 73/16. Risikostyring ble tatt inn i Helse Midt-Norges revisjonsprogram i 2017 med planlagt gjennomføring i 2018. Revisjonen ble startet i 2019.

2. Innretning, mål og revisjonsunderlag for revisjonen

Risikobegrepet brukes i flere sammenhenger og revisjonen har undersøkt hvordan St. Olavs Hospital HF arbeider med:

- Risikostyring. Det er lagt vekt på knytningen til mål og strategi
- Risikovurderinger som en naturlig del av styringsprosessen
- Likviditetsrisikovurdering
- Forhold som kan fordreie risikovurderinger (bias)
- Pliktige risikovurderinger

Revisjonen tar sikte på å nå følgende mål:

- Evaluere rammeverket og helseforetakets praksis i forhold til relevante normer, lovkrav og eierstyring relatert til risikostyring.
- Evaluere prosessene for å oversette operasjonell risiko til eventuell strategisk risiko
- Evaluere helseforetakets oppmerksomhet mht. feilkilder i innsamling og tolkning av data

I samråd med ledelsen ved helseforetaket er det avtalt å se på bruk av risikotyper og risikoradar.

Internrevisjonen har gjennomgått et stort antall lokale, regionale og nasjonale dokumenter for å kartlegge rammebetingelser, styringskrav, og hvordan arbeidet med risikostyring har utviklet seg ved St. Olavs hospital HF og i Helse Midt-Norge RHF. Disse dokumentene framgår av internrevisjonens arbeidsdokumenter (Appendiks A). Vesentlige dokumenter er referert i denne rapporten.

¹ Protokoll fra foretaksmøte i Helse Midt-Norge RHF, 23. januar 2008.

² Styreprotokoll Helse Midt-Norge RHF 5. november 2015 (sak 93/15)

3. Revisjonens funn, merknader og anbefalinger

3.1. Vurderinger i forstudien

Gjennom forstudien kom internrevisjonen fram til at det regionale rammeverket og rapporteringen har mangler i forhold til anbefalinger om risikostyring i anerkjente standarder (COSO ERM og NS-ISO 31000). Det ble også relativt tidlig klart at helseforetakenes gjennomføring ikke var systematisk nok, men årsaken var ikke fullt ut forstått.

3.2. Vurdering av regionalt rammeverk for risikostyring

Det regionale rammeverket inneholder begrepsavklaringer, roller og ansvar, anvendelsesområder, prosess, opplæring og evaluering. Dette er delvis i tråd med anbefalinger i standardene (COSO ERM og NS-ISO 31000).

Innholdet under hver tema konkretiserer til en viss grad hva som gjelder for Helse Midt-Norge. Begrepsavklaringene er omfattende og kan bidra til klarheter framfor avklaring. Temaet som beskriver prosess har overskriften «Gjennomføring av risikostyring», mens innholdet kun omfatter risikovurdering.

Internrevisjonen legger merke til at det regionale rammeverket knytter begrepsavklaringene til definisjoner i Veileder for risikostyring utgitt av Senter for statlig økonomistyring, med videre henvisning til NS-ISO 31000 og NS 5814. Begge disse standardene er anvendelige standarder for risikostyring og risikovurderinger henholdsvis, men det er ikke dekning for å knytte rammeverkets definisjoner til definisjoner standardene. Dette bidrar til å svekke systematikken.

Videre refererer rammeverket til styringsmål og ikke til Helse Midt-Norges strategiske mål. Det er en vesentlig forskjell fra anbefalingene i de anerkjente standardene, hvor strategisk retning er et hovedpoeng.

I innledningen til det regionale er det gitt føringer om at arbeidet med et felles rammeverk for risikostyring for hele regionen skal bygge på eksisterende strukturer og ikke bli for omfattende og komplisert i startfasen. Internrevisjonen har vurdert at disse føringene har gitt noen utilsiktede konsekvenser ved å fjerne fokus fra de grunnleggende forutsetninger for å få risikostyringen til å fungere systematisk, gitt gjennom anbefalingene i COSO ERM og NS-ISO 31000.

Internrevisjonen har vurdert at det ikke er hensiktsmessig å analysere det regionale rammeverket videre nå. Det er heller ikke hensiktsmessig å legge det til grunn som referanse for vurderingen av risikostyringen ved St. Olavs hospital HF. Hovedårsaken er at rammeverket mangler knytningen til strategi, framstår som ufullstendig og følgelig heller ikke er egnet som underlag for opplæring i risikostyring. Det er derfor ikke mulig for internrevisjonen bygge en bekreftelse om systematisk risikostyring på det regionale rammeverket i sin nåværende form.

Anbefalingen fra internrevisjonen til St. Olavs Hospital HF er:

- å bidra til at rammeverket for risikostyring i Helse Midt-Norge integreres med strategi og strategiske mål. Internrevisjonen har gjort rede for hvordan det kan gjøres med utgangspunkt i fag og forskning (Appendiks B).
- å bidra til at det bestemmes strategiske KPI'er som legges til grunn for *risikotyper*, og som monitoreres og rapporteres som del av risikostyringen. Utfallsrom og terskler for hver risikotypene må defineres i forhold til grønn/gul/rød (trusler) og lys blå/blå/mørk blå

(muligheter). Tersklene vil være ulike for HF og RHF og bør diskuteres med styret, som er øverste myndighet for å akseptere risiko. Se for øvrig RHF-styresak 15/16 om KPI'er for HMN.

- å bidra til å velge normativ og kvalitetssikret referanse for risikostyringen. Begge standardene COSO ERM og ISO 31000 vil etter internrevisjonens vurdering fungere. Det viktigste er å velge en av dem. Eventuell bruk av NS 5814 bør knyttes til *vurderingstrinnet* i en prosess for risikostyring.
- å bidra til å bygge videre på eksisterende rammeverk med de kommentarene som er gitt ovenfor. Begrepsavklaringene bør forenkles. Prosessen bør kompletteres. Roller og ansvar samt rammeverkets anvendelsesområder kan videreføres.

3.3. Risikostyring

3.3.1. Revisjonskriterier

Internrevisjonen har tatt utgangspunkt i at effektiv styring er *proaktive handlinger* for å nå *mål*. Effektiv styring krever også at helseforetaket har a) etablert *representative KPI'er* for sine *strategiske mål*, og b) at målene er strukturert etter *samfunnsøkonomiske prinsipper*. Videre er det vesentlig å ha oversikt over interne og eksterne forhold som kan påvirke måloppnåelsen. En slik oversikt omtales ofte som *risikoradar*.

Mest mulig rettvise risikovurderinger forutsetter at helseforetakene er oppmerksomme på bias. Bias opptrer i mange former, og internrevisjonen har avgrenset undersøkelsen til å se på organisasjonsmessig bias.

Alle anerkjente standarder om risikostyring legger vekt på betydningen av å ha etablert prinsipper, rammeverk og prosess. Internrevisjonen har derfor lagt vekt på å undersøke om dette er etablert systematisk:

Rammeverk

Rammeverkets funksjon er sikre at risikostyringen integreres i de vesentlige aktivitetene og funksjonene. Risikoradar og monitorering av viktige forhold internt og eksternt er eksempel på komponenter i rammeverket. «Tonen fra toppen», mål og strategiutforming, roller og ansvar, ressursallokering, kommunikasjon, evaluering er andre eksempler. De to anerkjente standardene COSO ERM og ISO 31000 benytter litt ulik terminologi og struktur ift. rammeverkets bestanddeler, men fyller i prinsippet samme funksjon.

Prinsipper

Prinsippenes funksjon er å veilede helseforetakenes ansatte i hva som karakteriserer effektiv risikostyring, hva hensikten og formålet med risikostyring er og hvordan den skaper verdi for helseforetakene. Også her har de anerkjente standardene ulik terminologi og struktur, men begge rammeverkene fyller funksjonen.

Prosess

Prosessens funksjon er å sikre at rammeverket og prinsippene oversettes til aktiviteter og gjennomføres i praksis. Som nevnt ovenfor varierer de anerkjente standardene litt i terminologi og struktur, men begge fyller funksjonen.

3.3.2. Vurdering, funn og anbefalinger.

Det er tatt hensyn til vurderingene og anbefalingene for det regionale rammeverket for risikostyring i kapittel 3.1.

Hoveddokumentet som legges til grunn er *EQS ID 9399 Metode for risikovurdering*. Dette dokumentet gjør rede for terminologi, enkelte risikoområder, ansvar og arbeidsbeskrivelse. I tillegg refererer dokumentet til ulike hjelpeskjema og forklarende dokumenter:

- Hjelpeskjema nr. 1 Kartlegging
- Hjelpeskjema nr. 2 Risikodiagram og akseptkriterier.
Inneholder definerte utfallsrom for P og C. God struktur, som bør utvides.
- Hjelpeskjema 2B til bruk ved enklere vurderinger
- Hjelpeskjema nr. 3 Handlingsplan
- Eksempler på aktuelle risikovurderingsområder – drift
Omfatter underområder til områdene nevnt i hjelpeskjema 2.
- Arbeidstilsynets liste - finn farekilden HMS
- Innføring i risikovurdering

Disse dokumentene mangler på samme måte som det regionale rammeverket knytning til strategiske mål og en systematisk tilnærming til rammeverk, prinsipper og prosess. Dermed understøtter de ikke eiers krav om å etablere en mer helhetlig risikostyring.

Forbedringsforslagene gitt i kapittel 3.2 er etter internrevisjonens vurdering viktige for å komme videre på dette området. I tillegg anbefales det å bidra til at risikoradar etableres som krav i det regionale rammeverket, og at St. Olavs hospital HF selv etablerer risikoradar.

Når det er sagt vil internrevisjonen få fremheve at dokumentlista ovenfor samlet sett inneholder gode enkeltelementer:

- Strukturen med hoveddokument og de relaterte hjelpedokumenter vurderes å være til god hjelp for ansatte som skal arbeide med risikovurdering. Den vil også bidra godt til å definere kompetanse, gjennomføre opplæring og kontinuerlig forbedring. Dette er vesentlig. Strukturen anbefales opprettholdt.
- Dokument EQS ID 9399 knytter risikoområder til konsekvensgradering. Dokument *Hjelpeskjema nr. 2 Risikodiagram og akseptkriterier* definerer skala for sannsynligheter og konsekvensgradering. Disse definisjonene er vesentlige og anbefales opprettholdt og videreutviklet. Konsekvensgraderingen bør videreutvikles slik at den minimum reflekterer helseforetakets strategiske prioriteringer.
- Dokumentet *Innføring i risikostyring* tar opp temaet verdier. Selv om sammenhengen er avgrenset til risikoen for tap av verdier, vurderer internrevisjonen at temaet berører selve formålet med risikostyringen – å *skape og beskytte verdier*. Her anbefales det å ta utgangspunkt i modeller for verdiskapning og verdifangst, slik at man får etablert en klar kobling til pasientbehandlingen, finansstrategien og de finansielle rammene. Temaet bør etter internrevisjonens vurdering løftes til det regionale rammeverket.

3.4. Pliktige risikovurderinger

Begrepet *risikostyring* er knyttet til virksomhetsstyringen og dermed til strategi og internkontroll. Begrepet *risikovurdering* forekommer i flere sammenhenger. I tillegg til å være en del av risikostyringsprosessen, forekommer begrepet i lovgivningen og som en del av internkontrollen. Lovgivningen har enten direkte krav til risikovurderinger, som for eksempel ved tilberedning av legemidler, eller indirekte krav gjennom plikten til internkontroll gitt gjennom §§ 6 d) og e) i Forskrift om ledelse og kvalitetsforbedring i helse og omsorgstjenesten.

Risikovurdering knyttet til misligheter er eksempel på et indirekte krav gjennom plikten til internkontroll. Helse Midt-Norge har hatt nytt regnskaps- og økonomisystem siden mars 2017 og det er derfor relevant å undersøke om risikovurdering er tatt i bruk i kontrollmiljøet mot misligheter.

3.4.1. Revisjonskriterier

Regelverket: Utgangspunktet har vært at St. Olavs hospital HF er pliktsubjekt etter loven³ og har et selvstendig ansvar for internkontroll og risikostyring på alle områder i virksomheten.

Reglement og bestemmelser for økonomistyring i staten: Direktoratet for forvaltning og økonomistyring har avgitt tolkningsuttalelse om internkontroll og særskilte risikovurderinger av misligheter i statens økonomiregelverk (april 2019). Der framgår det at risikovurderinger ikke er et vilkår for å oppfylle kravene i økonomiregelverket. Det er imidlertid under forutsetning om tilfredsstillende innebygd intern kontroll i IKT-systemene.

For å vurdere om forutsetningen er til stede har internrevisjonen har innhentet og vurdert bokføringssjekklisten for regnskapsåret 2018. Der framgår det at regnskaps- og økonomisystemet har mangler⁴ som vanskeliggjør kontrollaktivitetene. Internrevisjonen har derfor vurdert at vilkåret for å se bort fra risikovurdering ikke er til stede.

Helse Midt-Norges antikorrupsjonsprogram: Antikorrupsjonsprogrammet omfatter misligheter og krav bl.a. til kontrollsystem, retningslinjer og risikoanalyser.

Normative kilder: Følgende er lagt til grunn:

- COSO/ACFE Fraud Risk Management Guide stiller klare og eksplisitte krav til risikovurdering jf. tekst nedenfor:

The organization performs comprehensive fraud risk assessments to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks.

- Revisorforeningen publiserer tilsvarende i et erfaringsnotat utarbeidet av Økokrim⁵, at mangelfull risikoanalyse er en gjenganger og en av de grunnleggende årsakene til at bedrifter rammes av ulike varianter av økonomisk kriminalitet.
- ISA 240 om revisors oppgaver og plikter til å vurdere misligheter ved revisjon av regnskaper, stiller i punkt 17 b) krav om å etterspørre ledelsens prosess for å identifisere og håndtere risikoer for misligheter.

³ Helseforetaksloven kapittel 2 om partsstilling og ansvar.

⁴ Eksempel: mangler ved bokføringsspesifikasjon, sporbarhet og sikring mot endringer etter utstedelse.

⁵ *Beskytt bedriften mot misligheter*. Morten Bamble, Økokrim. Publisert i Revisorforeningen 2019.

3.4.2. Vurderinger, funn og anbefalinger

Det er lagt til grunn at eier kan pålegge helseforetakene i regionen å bruke samme regnskaps og økonomisystem. Eier kan også avgjøre at helseforetakene skal utkontraktere anskaffelsen til seg selv som regional tjenesteleverandør. Regionalt helseforetak kan dermed ha oppgaveansvaret for å gjennomføre anskaffelsen, tilrettelegge systemet for bokføring, drifte og vedlikeholde systemet. Eier kan imidlertid ikke overta vurderingene om hvorvidt system og rutiner er i tråd med regelverk og myndighetskrav. Det er helseforetakets ansvar.

Internrevisjonen tar et forbehold om at systemeier og den regnskapspliktige kan ha ulike vurderinger av:

- hvorvidt mangler som framgår av bokføringssjekklisten er i strid med bokføringslovgivningen,
- hvorvidt manglene svekker kontrollmiljøet,
- hvorvidt forutsetningen om tilfredsstillende innebygd intern kontroll er til stede, og
- og om det er etablert tiltak som bøter på manglene.

Informasjon om at ekstern revisor har gått god for at manglene ikke er i strid med regelverket er ikke verifisert ovenfor internrevisjonen. Det er heller ikke verifisert at den regnskapspliktige har akseptert risikoen ved et eventuelt svekket kontrollmiljø. Det er derfor tatt utgangspunkt i det som faktisk er dokumentert i bokføringssjekklista. Som nevnt ovenfor i diskusjonen av kriteriene vurderer internrevisjonen at risikovurdering er påkrevet.

I vurderingene videre har internrevisjonen benyttet sjekkliste (Appendiks C) for kontrollmiljøet utarbeidet i forbindelse med gjennomføring av internrevisjon om mislighetsrisiko i Helse Nord RHF i 2018⁶. Sjekklisten ble oversendt revidert part i forkant av intervju med anmodning om å forberede svar og dokumentreferanser for å belyse hvert enkelt punkt. Intervjuene ble utført med relevant personell ift. sjekklistens spørsmål. Dokumentreferansene ble gjennomgått i ettertid. Resultatet ble oppsummert og sjekklisten ble utsendt for faktaverifikasjon. Det er ikke gitt innsigelser til oppsummeringen, hvor det framgår at dokumentert risikoanalyse ikke er utført. Det gis derfor anbefaling om å etablere årlig risikoanalyse som et underlag for å vedlikeholde et godt kontrollmiljø for å forebygge og avdekke misligheter.

Antikorrupsjonsprogrammet omtale av risikoanalyser er på et overordnet nivå og gir få om ingen konkrete retningslinjer om risikovurdering og ansvarsforhold som møter krav i regelverket eller anerkjente standarder. Internrevisjonen anbefaler derfor at helseforetaket bidrar til å konkretisere retningslinjer om risikovurdering for å avdekke og forebygge misligheter.

Det er relevant i denne sammenhengen å bekrefte at øverste leder og ledende ansatte som internrevisjonen snakket med kommuniserer tydelig verbalt om 0-toleranse for misligheter ved St. Olavs Hospital HF. Dette er et sentralt element i kontrollmiljøet. Tilsvarende skriftlig kommunikasjon er ikke identifisert i ledelsessystemet for helseforetaket. Internrevisjonen gir derfor anbefaling om å gjøre det.

⁶ Internrevisjonsrapport 02/2018: Mislighetsrisiko i Helse Nord RHF, Internrevisjonen i Helse Nord RHF, 30.10.2018.

I intervjuene ble det vist til at helseforetaket har etablert meldesystem og varslingskanal for å håndtere etiske utfordringer og at alle klinikker samt stabsavdeling benytter kontrollere i arbeidet. Det ble opplyst at meldesystemet mangler kategori for mislighetsrisiko. Stillingsbeskrivelser for kontrollere omfatter ikke arbeid med mislighetsrisiko. Det er opplyst at varslingskanalen er operativ. Det gis anbefaling om å etablere en slik kategori for mislighetsrisiko i meldesystemet og å oppdatere stillingsbeskrivelser for kontrollere.

Internrevisjonen har identifisert risiko for bias i vurderinger av kontrollmiljøets evne til å forebygge og avdekke misligheter. Dette er organisasjonsbias som er beskrevet nærmere i kapittel 3.5. Anbefalingen er at man innarbeider en vurdering av bias i risikovurderinger.

I internrevisjonens arbeid med vurderingene var det nødvendig å gjennomgå økonomistyringsmodellen i Helse Midt-Norge for å forstå:

- hvordan helseforetakenes posisjon som pliktsubjekter i bokførings- og regnskapsarbeidet er beskrevet
- hvordan ulike pliktmessige spørsmål blir belyst, vurdert og akseptert på tvers i foretaksgruppen, og
- hvordan eventuell dissens håndteres.

Modellen gjør etter internrevisjonens vurdering ikke tilstrekkelig rede for disse forholdene og kan i sin nåværende form bidra til bias i risikovurderinger på mislighetsområdet. Det anbefales at helseforetaket bidrar til å tydeliggjøre økonomistyringsmodellen og sikre at den ivaretar den lovmessige pliktstrukturen.

I dokumentstudiene vedr. risikovurdering ble vurderingsarbeidet knyttet til beredskap gjennomgått. Dette arbeidet framstår som grundig i metode og innhold og kan fungere som eksempel når helseforetaket utvikler systemer for risikovurdering på andre områder.

3.5. Test av bias i risikovurdering

Risikovurdering utføres av mennesker og vil være utsatt for ulike former for påvirkning som gi et uriktig beskrivelse av risikoen. Eksempelene som diskuteres i COSO ERM er for eksempel inhabilitet, blanding av roller, allianser, behov for å tildekke dårlige resultater eller overdreven optimisme. Eksistensen av Helse Midt-Norges etiske retningslinjer er også vurdert som en erkjennelse av at uheldige forhold av denne typen kan forekomme og må håndteres. Internrevisjonen har lagt til grunn at bias i risikovurdering er relevant både i forhold til de etiske retningslinjene og for å oppnå mest mulig rettvise risikovurderinger. Bias som fenomen i risikovurderinger er ytterligere belyst i Appendix D.

3.5.1. Revisjonskriterier

Bias i risikovurdering er grundig behandlet i begge de anerkjente rammeverkene om risikostyring. NS-ISO 31000 anbefaler (punkt 6.4.3) at forhold som kan fordreie analysen bør vurderes, dokumenteres og kommuniseres til beslutningstakerne. COSO ERM går enda lenger og anbefaler tiltak for å mitiggere bias i ulike situasjoner. Internrevisjonen avgrensar vurderingen i denne revisjonen til å bedømme om rammeverket for risikostyring i Helse Midt-Norge belyser utfordringene med bias og om det er spesielle områder med risiko for bias.

3.5.2. Observasjoner, vurderinger og anbefalinger.

Internrevisjonen har utført dokumentstudier, intervjuer og stikkprøve i kontrollmiljøet for å forebygge og avdekke misligheter.

Rammeverket for risikostyring i Helse Midt-Norge omfatter ikke retningslinjer om å identifisere, vurdere og redusere virkningen av bias i risikovurderinger. Dokumenter i kvalitets og HMS-systemet ved St. Olavs hospital HF omfatter heller ikke noe om dette.

Internrevisjonen har også undersøkt faktiske forhold som kan øke risiko for bias. Organiseringen av arbeidet med anskaffelse, innføring og drift av nytt regnskaps- og økonomisystem i Helse Midt-Norge er lagt til det regionale helseforetaket. Regionalt helseforetak er samtidig systemeier, eier av de regnskapspliktige enhetene, og har samtidig ansvar for rapportering til regionalt styre. Dette gir en utfordrende opphopning av roller på få personer i det regionale helseforetaket. Ledere vil etter internrevisjonens vurdering være spesielt utsatt med konstant risiko for å utløse bias i risikovurderinger. Internrevisjonen vurderer at denne måten å organisere oppgavene på kan redusere det ytringsklimaet som trengs for å få fram mest mulig rettvise risikovurderinger. Oppmerksomhet på og reduksjon av bias i risikovurderinger vil kunne redusere begge disse ulempene. Det gis anbefaling om å etablere en oppmerksomhet omkring forekomst og virkning av bias i Helse Midt-Norges rammeverk for risikostyring og i de etiske retningslinjene.

3.6. Likviditetsrisikovurdering

Gjeldende finansstrategien i Helse Midt-Norge legger stor vekt på likviditetsstyring for å sikre økonomisk bærekraft. Internrevisjonen har derfor vurdert hvordan systemet for helhetlig risikostyring understøtter finansstrategien.

Likviditetsstyring på regionalt nivå er omtalt i strategiens kapittel 7.1 og omfatter:

- Forvaltning av regionens økonomisk rammer, bl.a. ved å tilrettelegge for forutsigbar og langsiktig finansiering av helseforetakenes drift og investeringer.
- Tilrettelegge for at helseforetakene har nødvendig likviditet tilgjengelig.
- Bidra til å håndtere finansiell risiko knyttet til bruk av likviditet.
- Å styre likviditetsfordelingen i foretaksgruppen ved at Helse Midt-Norge RHF har funksjon som foretaksgruppens «internbank».

3.6.1. Revisjonskriterier

Helseforetak er iht. strategiens kapittel 7.2 ansvarlig for å rapportere likviditetsutvikling og risiko knyttet til finansiell informasjon. Ansvarer innebærer å etablere interne rapporterings- og oppfølgingsrutiner for likviditetsutviklingen og å sikre god kvalitet både i tall, analyser og kvalitative tiltak. Detaljeringsgrad og hyppighet skal baseres på det enkelte foretakets risiko for overforbruk.

RHF er iht. strategien ansvarlig for:

- Å tilrettelegge for forutsigbar og langsiktig finansiering av helseforetakenes drift og investeringer.
- Tilrettelegge for at helseforetakene har nødvendig likviditet tilgjengelig.
- Bidra til å håndtere finansiell risiko knyttet til bruk av likviditet.

3.6.2. Vurderinger, funn og anbefalinger

Internrevisjonen får opplyst at regnskaps- og økonomiløsningen ikke har støtte for å ta ut rapporter om likviditet, og at en slik løsning er ønskelig. Det gis derfor en anbefaling om å kartlegge hva som skal til for å etablere slik støtte i løsningen.

Internrevisjonen er forelagt kontantstrøm budsjett for 2020 og kontantstrøm prognose for 2021 og har også fått en forklaring på kontrollernes rolle i budsjettoppfølgingen. Det er videre innhentet underlag for langtidsbudsjett 2019 – 2030. Internrevisjonen har ikke undersøkt metodikken godt nok til å kunne avgi bekreftelser, men har likevel et godt inntrykk av at likviditetsrisiko styres så godt som forutsetningene tillater.

Det er også gjort en vurdering av arbeidet med gevinstrealisering i HMN LØ. Gevinstområdene som er besluttet og resultat per 2. tertial 2019 framgår av Figur 1. I Regional gevinstrealiseringsplan v.1.0 HMN LØ (juni 2017) framgår det bl.a:

- Programmet skal gjennomføre gevinst- og lønnsomhetsanalyse (ref. Programdirektivet).
- Gevinst- og lønnsomhetsanalysen skal oppdateres gjennom programmet.
- Første revidering (av gevinst- og lønnsomhetsanalysen) igangsettes ved oppstart av programmet.

Rapporteringen av besluttede gevinstområder jf. Figur 1 ser ikke ut til å være i tråd med finansstrategien og gevinstrealiseringsplanen fra 2017 på grunn av mangel på tallfestede finansielle virkninger. Denne situasjonen vil etter internrevisjonens vurdering svekke muligheten for finansiell risikoanalyse i forbindelse med investeringsprosjekter, og følgelig svekke muligheten til å håndtere finansiell risiko så tidlig som mulig.

Internrevisjonen vil anbefale at St. Olavs hospital HF bidrar til å se nærmere på hvordan denne utfordringen virker i kombinasjon med det regionale helseforetakets forvaltning av internbankfunksjonen (ref. Finansstrategiens punkt 7.1). Risikoen etter internrevisjonens vurdering er at pasientbehandlingen og ansattes arbeidsforhold kan bli for lett tilgjengelig som likviditetsbuffer i vedlikeholdet av internbankfunksjonen (se også RHF styresak 14/20 kap. 5). Denne risikoen kan reduseres ved å legge mer vekt på finansiell informasjon i arbeidet med gevinstrealisering, og å forbedre rammeverket for helhetlig risikostyring i tråd med vurderingene i kapittel 3.12. Forbedringsmuligheten i kulepunkt 2 i kapittel 3.12 og den samfunnsøkonomiske koblingen forklart i Appendiks B kan være sentral dersom helseforetaket ønsker å komme videre på dette området.

#	KPI/aksjon	Enhet	1. tertial	2. tertial	3. tertial	Hittil i år	2018	Mål 2019	Premissgiver innhold og oppfølging
1	Andel Kjøp i SAP	%	N/A					N/A	Lederforum LØ
2	Avtaledekning	%	52 %	60 %		56 %	43 %		Strategisk innkjøpsforum
3	Avtalelojalitet	%	94 %	99 %		97 %	84 %		Nettverk strategisk logistikk
4	Ekstern servicegrad		N/A					N/A	Nettverk strategisk logistikk
5	Intern servicegrad (fra forsyningslager)		N/A					N/A	Nettverk strategisk logistikk
6	Andel betaling med kort/faktura	%	73 %	73 %		73 %	72 %		Økonomisjefnettverk
7	Andel EHF inngående faktura	%	85 %	87 %		86 %	84 %		Økonomisjefnettverk
8	Omløpshastighet sentrallager		10,5	10,7		10,7	10,1		Nettverk strategisk logistikk
9	Andel faktura som matcher innkjøpsordre	%	27 %	28 %		28 %	28 %		Økonomisjefnettverk

*) N/A – parameter er ikke klar

Figur 1: Kapittel 2.7 Gevinstrealisering LØ – pr. tertial
(Styresak 55-19 Statusrapport 2. tertial 2019 St. Olavs hospital HF)

4. Gjennomføring av revisjonen

Revisjonens oppdragsgiver er styret i Helse Midt-Norge RHF. Oppdraget er gitt gjennom styrets godkjenning av internrevisjonens *Revisjonsprogram for 2019 – 2021*.

Revisjonslaget har bestått av:

- Jørgen Midtlyng, Revisjonsleder – Helse Midt-Norge RHF
- Ingvild Klevan, medrevisor

Representanter for revidert part har vært:

- Merete Blokkum, Direktør for virksomhetsstyring
- Grethe Aasved, Administrerende direktør

Revisjonen var tidfestet med forventet start april 2019 og forventet rapport i februar 2020.

- Forstudier og revisjonsplanlegging startet august 2019.
- Revisjonsvarsel ble sendt ut 30. oktober 2019
- Formøte med administrerende direktør og styreleder ble avholdt 28. november 2019.
- Svar på revisjonsvarsel ble etterlyst 2. desember 2019
- Revisjonskoordinator oppnevnt 13. desember 2019.
- Åpningsmøte ble avholdt 6. januar 2020
- Intervjuer ble gjennomført 9. og 28. januar 2020
- Sluttmøte ble ikke avholdt pga. situasjon med Covid-19 under utvikling.
- Rapport ble sendt ut for faktaverifikasjon den 2. mars 2020.
- Tilbakemelding på faktaverifikasjon ikke mottatt*.
- Rapporten ble frigitt med forbehold om til revidert part den 14. april 2020.

Intervju er gjennomført i St. Olavs Hospital HF sine lokaler. Arbeidet for øvrig er utført ved internrevisjonens kontor i Stjørdal.

Prosedyrer for revisjonen er dokumentert i eget styringsdokument ID 707 for internrevisjonen.

* Respons på utsendt faktaverifikasjon ble ikke mottatt innen fristen. Arbeidet med tilbakemelding på faktaverifikasjon kan ha blitt forstyrret av Covid-19 situasjon som var under utvikling i samme periode. Internrevisjonen vurderer risikoen for faktafeil i rapporten som liten og frigir rapporten, dog med et forbehold om at St. Olavs hospital HF må kunne påpeke eventuelle forhold i ettertid. Det er ikke trukket konklusjoner på områder hvor det har vært tvil. Internrevisjonen har funnet det riktig å opplyse brukere av revisjonsrapporten om denne situasjonen for å kunne åpne for eventuelle korrigeringer etter rapportens utgivelse. Eventuelle korrigeringer vil bli meddelt oppdragsgiver for revisjonen.

Appendiks A: Oversikt over revisjonsaktiviteter

ID	Type	Tema
01	DG	Innledende studier
02	DG	Finansstrategi inkl. relaterte dokumenter
03	DG	Regelverk, veiledere og rammeverk for risikostyring
04	DG	Oppfølging av styringsdokumenter 2015 - 2019
05	DG	Risikostyring som tema i styresaker
06	DG	Kontroll av utført risikostyring
07	IN	Oppsummering av intervju
08	DG	Likviditetsrisikostyring
09	DG	Kontrollmiljø og pliktig risikovurdering - misligheter

Appendiks B: Faglig grunnlag for vurderinger og anbefalinger

For å belyse hva *helhetlig risikostyring* betyr, har internrevisjonen sett nærmere på risikostyringen i et samfunnsøkonomisk perspektiv. Hensikten er å belyse litt grundigere det som går fram av regelverket, eierstyringen og de normative kilder for risikostyring (COSO ERM og NS-ISO 31000).

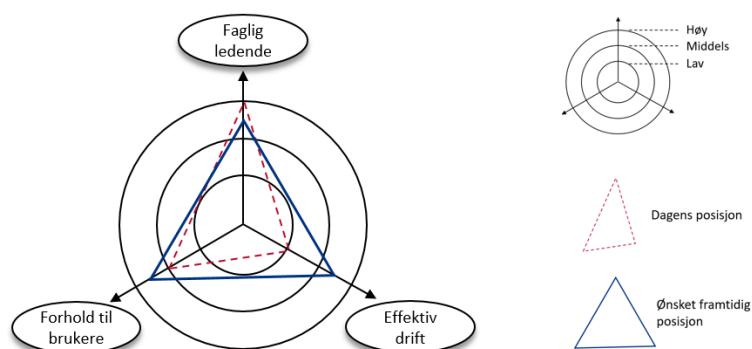
Både regelverket, statlig veiledere om risikostyring, COSO ERM og NS-ISO 31000 knytter styring av risiko til verdiskapning. Velfungerende prosesser for risikostyring settes videre i sammenheng med å fastlegge strategi for å oppnå mål bestemt gjennom veloverveide beslutninger. Disse kildene er også omforent om at risikostyring må være en integrert del av virksomhetsstyringen og at ledelsens forpliktelse til risikostyringen er avgjørende for resultatet.

Det er lagt til grunn at mål, strategiutforming og risikostyring er forankret i:

- størrelsen av og vilkårene i Stortingets bevilgninger
- overordnede målsetninger og føringer bestemt i regelverket, og
- den nasjonale helsepolitikken.

Dette er utgangspunktet når helseforetakene gjør avveininger og etablerer strategier for å møte krav og forventninger til kvalitet og pasientsikkerhet på en side, og styring av likviditet på den andre.

Internrevisjonen har satt dette i sammenheng med litteratur⁷ som viser at strategiutvikling i hovedsak er prioritering og avveining på tre områder: å være faglig ledende, å drive virksomheten effektiv, og hvilken relasjon man ønsker å ha til brukerne. Sammenhengen er illustrert i Figur 2.



Figur 2: Figuren illustrerer hvilke prioriteringer og avveininger virksomheter i realiteten gjør når de posisjonerer seg strategisk. Prioriteringene og avveiningene oversettes til strategiske prosjekter.

⁷ The discipline of market leaders, Wiersema, Treacy 1997

Litteraturen setter videre prioriteringer og avveininger i sammenheng med utvikling av strategiske prosjekter med klare målformuleringer i form av tallfestede og ikke-tallfestede virkninger^{8,9}.

Undersøkelser viser imidlertid (ref. Figur 3) at hovedårsaken til feilslått strategigjennomføring er mangel på tydelige milepæler og mål knyttet til styring av de strategiske prosjektene. *Målbare mål* er derfor en viktig forutsetning for risikostyring og vellykket strategigjennomføring. Dette er også konsistent med statens veileder for gevinstrealisering², COSO ERM og NS-ISO 31000.



Figur 3: Faktorer som er forbundet med feilslått strategigjennomføring (n=288)
 Kilde: BCG – Changing Change management (2012) og Prof. Daniel Simonovich, INSEAD.

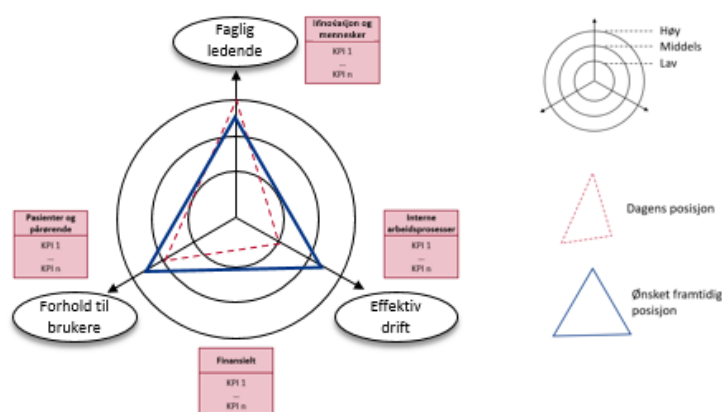
Det kan derfor underbygges faglig at overveide og målbare mål i strategiske prosjekter har sammenheng med virkningsfull risikostyring. Mål må være egnet til å styre strategiske prosjekter fra oppstart og overlevering i tråd med det som er planlagt. Slike mål omtales videre i denne rapporten som *key performance indicators* (KPI).

Figur 4 viser hvordan prioriteringer og avveininger jf. Figur 2 oversettes til generiske KPI-typer:

- KPI-typer knyttet til *Forskning, innovasjon og kvalifikasjoner* vil stå sentralt i arbeidet med å opprettholde eller å utvikle faglig ledende posisjon.
- KPI-typer knyttet til *Interne arbeidsprosesser* vil ha stor betydning i utviklingen av mer effektiv drift.
- KPI-typer knyttet til pasienter og pårørende vil stå sentralt i utviklingen av forholdet til *brukerne*.
- I tillegg vil finansielle KPI-typer være nødvendige på grunn av begrenset finansiering og krav om økonomisk bærekraft.

⁸ Veileder: *Gevinstrealisering – planlegging for å hente ut gevinster av offentlige prosjekter*, DFØ 2014.

⁹ Veileder i *Samfunnsøkonomiske analyser*, DFØ 2018.

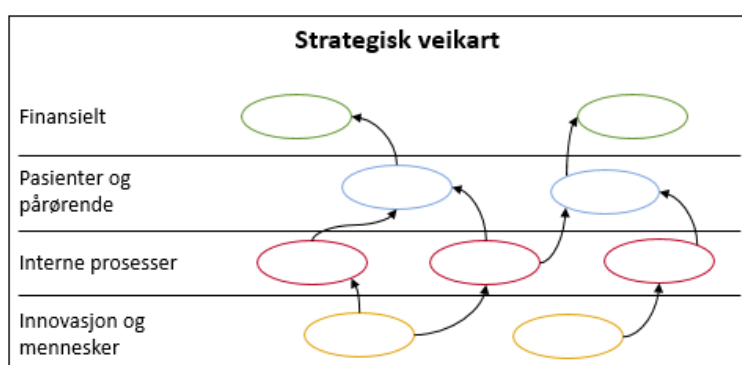


Figur 4 illustrerer sammenhengen mellom prioriteringer og avveininger i strategiutviklingen og KPI'er som er egnet til å føre strategiske prosjekter fram til planlagte mål.

Sammenhengen vist i Figur 4 utnyttes videre til å etablere et strategisk veikart som vist i Figur 5. Strategisk veikart bør benyttes for å kunne håndtere iboende avhengigheter mellom strategiske prosjekter. Eksempelvis vil et innovasjonsprosjekt ha spesifikke KPI'er og samtidig kunne påvirke tallfestede og/eller ikke-tallfestede virkninger for KPI'er under de øvrige strategiske hovedområdene. Internrevisjonen vil derfor være opptatt av at rammeverket for risikostyring omfatter:

- bevisste og faglig forankrede valg av risikotyper
- at valgte risikotyper reflekterer valgte KPI'er og omfatter alle hovedområdene i et faglig forankret strategisk veikart.

Sammenhengene diskutert ovenfor kan være et utgangspunkt for videre refleksjon om hvordan Helse Midt-Norge velger å knytte begrepet *helhetlig risikostyring* til et strategisk og samfunnsøkonomisk innhold.



Figur 5 viser at det er avhengigheter mellom de strategiske KPI-typene. I et system for helhetlig risikostyring er det et poeng at avhengighetene er reflektert som risikotyper i rammeverket for risikostyring. Helheten blir større dersom KPI-typene også reflekteres i arbeidet med gevinstrealisering.

Appendiks C: Intervjuguide vedr. mislighetsrisiko

1. Kontrollmiljø

Styrets og ledelsens forventninger om styring av mislighetsrisiko, og deres vektlegging av integritet og etiske verdier, er avklart og kommunisert.

- a) Styrevedtatte etiske retningslinjer foreligger og omfatter temaer som er vesentlige for forebygging av misligheter.
- b) Foretakets ledelse kommuniserer gjennom ord og handlinger at de er opptatt av etikk.
- c) Foretakets fullmaktstruktur (ansvar og myndighet) er egnet for forebygging, avdekking og håndtering av misligheter.
- d) Det er klart formidlet fra ledelsen at misligheter eller mistanke om misligheter følges opp, og hvilke følger dette normalt får.
- e) Foretaket har etablert varslingskanal i samsvar med gjeldende regelverk.

2. Risikovurdering

Foretaket gjennomfører risikovurderinger for å identifisere spesifikke mislighetsrisikofaktorer, vurdere sannsynlighet for og konsekvens av disse, og beslutte hvordan uakseptabel risiko skal håndteres.

- a) Risikoer for misligheter inngår i foretakets opplegg for systematiske risikovurderinger
- b) Mislighetsperspektiver inngår i risikovurderinger i investerings- og byggeprosjekter.
- c) Det utarbeides tiltaksplaner med ansvarsfordeling og tidsfrister når risikovurderinger har avdekket uakseptabel mislighetsrisiko.

3. Forebyggende tiltak

Foretaket utvikler og iverksetter forebyggende kontrolltiltak for å redusere risikoen for at misligheter inntreffer.

- a) Ansatte gjøres kjent med etiske retningslinjer.
- b) Ansatte får opplæring og trening i emner relatert til etikk og misligheter, som er tilpasset egen rolle og oppgaver.
- c) Adgangen til å ha bierverv er regulert.
- d) Foretaket har rutiner for å innhente/få registrert informasjon om bierverv.
- e) Foretaket har rutiner for å sikre at det ikke gjøres innkjøp i strid med inngåtte avtaler.
- f) Nærstående parter kartlegges når større anskaffelser/investeringer gjennomføres.
- g) Det er etablert kontrolltiltak som sikrer overholdelse av fullmaktstrukturen.
- h) Forebyggende tiltak iverksettes, i samsvar med tiltaksplan fra risikovurderinger.

4. Avdekkende kontroller

Foretaket utvikler og iverksetter kontroller som er egnet for å avdekke avvik og misligheter så fort som mulig.

- a) Det gjennomføres jevnlige kontroller for å verifisere at fullmaktstrukturen etterleves.
- b) Det gjennomføres jevnlige kontroller for å verifisere at det ikke foreligger uønskede koplinger som følge av bierverv eller nærståendeforhold.
- c) Det gjennomføres jevnlige kontroller for å verifisere at regelverket for offentlige anskaffelser etterleves.
- d) Det gjennomføres relevante telle- og eksistenskontroller.
- e) Det gjennomføres kontrolltiltak for å identifisere og håndtere transaksjoner med forhøyet mislighetsrisiko.
- f) Avdekkende kontroller, i samsvar med tiltaksplan fra risikovurderinger og ved kjente svakheter i forebyggende tiltak, gjennomføres.
- g) Budsjettoppfølgingen er egnet til å avdekke avvik som kan skyldes misligheter.

5. Håndtering

Foretaket utvikler og iverksetter tiltak som er egnet for hensiktsmessig håndtering av mistenkte eller avdekkede misligheter.

- a) Rutiner for hvordan mulige/avdekkede mislighetssaker skal følges opp, er utarbeidet.
- a) Mulige/avdekkede mislighetssaker blir håndtert i samsvar med regelverk og foretakets rutiner.

6. Oppfølging

Foretaket utvikler og utfører løpende evalueringer for å fastslå om komponentene i mislighetsrisikostyringen er til stede og fungerer, og svakheter kommuniseres til rett tid til de med ansvar for å treffe korrigerende tiltak.

- b) Ledere følger opp arbeidet med etikk og misligheter innen eget ansvarsområde.
- c) Ledelsen gjennomfører årlig gjennomgang/evaluering av arbeidet med etikk og misligheter.
- d) Det iverksettes forbedringstiltak ved uakseptable svakheter og mislighetsrisiko.
- e) Det er avklart hva som skal formidles til styret knyttet til misligheter og mislighetsrisiko.

Appendiks D: Forklaring til *bias* i risikovurderinger

Begge internasjonalt anerkjente rammeverk for risikostyring diskuterer innvirkningen av ulike former for *bias* i risikovurderingen. *Bias* utarter seg på mange måter og har ingen direkte entydig norsk oversettelse. Partiskhet og forutinntatthet er et eksempel på norske oversettelser, men disse begrepene er ikke fullt ut dekkende for den engelske betydningen av begrepet.

Rammeverket COSO Enterprise Risk Management diskuterer begrepet med hensyn til organisasjonsmessige forhold som vist nedenfor:

Bias in decision-making has always existed and always will. It is not unusual to find within an entity evidence of dominant personalities, overreliance on numbers, disregard of contrary information, disproportionate weighting of recent events, and a tendency for risk avoidance or risk taking. So the question is not whether bias exists, but rather how bias affecting decisions relating to enterprise risk management can be managed. The board is expected to understand the potential organizational biases that exist and challenge management to overcome them»

NS-ISO 31000 Risikostyring – retningslinjer diskuterer begrepet i en litt videre betydning:

Risikoanalysen kan påvirkes av alle forskjeller i meninger, fordommer, oppfatninger av risiko og bedømmelser. Andre forhold som påvirker, er kvaliteten på informasjonen som brukes, antakelser og utelatelser som gjøres, alle begrensninger i metodene og hvordan de utføres. Disse påvirkningene bør vurderes, dokumenteres og kommuniseres til beslutningstakerne.

I diskusjonen omkring risikoanalyse og *bias* i en 3-linje internrevisjon er det også naturlig å belyse hvordan *bias* diskuteres i forbindelse med styrearbeid. Styreutdanningen Executive Board Programme i regi av Scandinavian Executive Institute i samarbeid med INSEAD benytter artikkelen *The Hidden Traps in Decision Making*, John S. Hammond, Ralph L. Keenay and Howard Raiffa, HBR 2007 for å belyse utfordringene med *bias* i styrets vurderinger.

De er for øvrig mye litteratur tilgjengelig som diskuterer særtrekk og virkninger av *bias* i risikovurdering og beslutninger. Internrevisjonen har vurdert at referansene gitt ovenfor er dekkende og hensiktsmessig med hensyn til revisjonstemaet.

