

Risikostyring i staten

Håndtering av risiko i mål- og resultatstyringen



Risikostyring i staten

Håndtering av risiko i mål- og resultatstyringen

Forord

Kan du som leder svare på følgende spørsmål:

- Hvilke faktorer er avgjørende for måloppnåelse i min virksomhet?
- Hvordan kan jeg identifisere nye og endrede risikoer?
- Hvilke av disse risikoene er vurdert som vesentlige i forhold til måloppnåelse for min virksomhet?
- Hvordan kan jeg etablere hensiktsmessige styrings- og kontrollmekanismer som balanserer risiko, kontroll og kost/nytte ved ulike tiltak og kontrollaktiviteter?
- Hvordan kan jeg vite at disse styrings- og kontrollmekanismene fungerer effektivt og som forutsatt?

Dette metodedokumentet har til hensikt å gjøre deg bedre i stand til å svare på disse spørsmålene. Det beskriver en metode for hvordan du på en strukturert måte kan benytte risikostyring og intern kontroll som et verktøy for å gi rimelig sikkerhet for at virksomheten oppnår sine målsettinger.

Regelverket for økonomistyring i staten stiller krav om risikostyring og intern kontroll i statlige virksomheter. I regelverket gis det ikke nærmere anvisning om hvordan dette skal utformes eller gjennomføres i virksomhetene. Senter for statlig økonomistyring (SSØ) har derfor utarbeidet et metodedokument for risikostyring og intern kontroll i staten. Dokumentet skal bidra til å veilede virksomhetene i hvordan dette kan gjennomføres innenfor de rammer som regelverket for økonomistyring i staten setter.

Utarbeidelsen har skjedd i form av et prosjekt ledet av seniorrådgiver Bente Nyrud Gobel (SSØ). Partner Stein-Ragnar Noreng (KPMG) har bistått prosjektleder under hele utarbeidelsen. I tillegg har følgende eksterne rådgivere bidratt i prosessen: Manager Lars-Erik Fjørtoft (Deloitte), senior manager Gunnar Hoff (Deloitte), statsautorisert revisor Knut Løken, professor og statsautorisert revisor Flemming Ruud, PhD (Handelshøyskolen BI, Universitet Zurich og Universitet St. Gallen) og manager Stein-Ove Songstad (Deloitte).

I tillegg har en referansegruppe vært en viktig del av prosjektet. Den har bestått av følgende representanter fra statlige virksomheter: Seniorrådgiver Nils Hjelle (Skattedirektoratet), revisjonsdirektør Ingjerd Juel Ingeborgrud (Rikstrygdeverket), seniorrådgiver Sverre Lunde (UIO, fra 1. august 2005 Helse- og omsorgsdepartementet), avdelingsdirektør Internrevisjonen Ingrid Nolic (Aetat), revisjonsdirektør Teis Stokka (Skattedirektoratet), revisjonssjef Sveinung Svanberg (UIO) og leder av internrevisjonsenheten Trine Tengbom (Forskningsrådet). Styringsgruppen for prosjektet har bestått av Marianne Andreassen (direktør SSØ) og seniorrådgiver Emma C. Jensen Stenseth (Finansdepartementet). Riksrevisjonen har vært observatør både i styringsgruppen og referansegruppen med henholdsvis ekspedisjonssjef Hans Conrad Hansen og avdelingsdirektør Ola Hollum.

Med dette metodedokumentet ønsker vi å framheve de positive verdiene i arbeidet med risikostyring og intern kontroll og betydningen av dette for bedret målstyring og resultatoppnåelse. SSØ vil videreutvikle metodikken basert på de erfaringer som gjøres i virksomhetene. På våre nettsider www.sfso.no vil du finne ytterligere informasjon om og eksempler i tilknytning til risikostyring og intern kontroll.

Oslo, 8. desember 2005

Innholdsfortegnelse

Sammendrag	6
1 Innledning	12
1.1 Ansvar for risikostyring og intern kontroll.	14
1.1.1 Virksomhetens interne styring	14
1.1.2 Departementets styring av virksomheter	15
1.2 Formålet med metodedokumentet.	15
2 Håndtering av risiko i mål- og resultatstyringen	16
2.1 Tre kategorier av målsettinger	17
2.2 Risikostyring og intern kontroll – en prosess	17
2.3 Dokumentasjon	19
3 Metode for håndtering av risiko i mål- og resultatstyringen	21
3.1 Formålet med dokumentasjon av risikostyringen	22
3.2 Strategi for integrering av risikostyring i mål- og resultatstyringen.	23
3.3 Prosess for risikostyring integrert i mål- og resultatstyringen.	24
3.4 Prosess for risikostyring på overordnet nivå	25
3.4.1 Identifisering av virksomhetens overordnede mål	26
3.4.2 Identifisering av kritiske suksessfaktorer	27
3.4.3 Identifisering av risikoer	28
3.4.4 Vurdering og prioritering av risikoer	31
3.4.4.1 Nærmere om vurdering av sannsynlighet og konsekvens	31
3.4.4.2 Vurdering og prioritering av risikoene på overordnet nivå	34
3.5 Prosess for utarbeidelse av risikokart på lavere organisasjonsnivåer	37
3.6 Risikoanalyse av operative prosesser	38
3.7 Risikoanalyse av prosjekter	40
3.8 Tiltak og kontrollaktiviteter som følge av vurderingene	40
3.9 Oppfølging av risikoene	47
3.9.1 Hensikten med oppfølging av risikoene	47
3.9.2 Praktiske måter å følge opp risikoer på	47
3.9.3 Bruk av kontrollere og internrevisjon	49
3.10 Risikostyringens begrensninger	49
Stikkordregister	50
Vedlegg A - Bestemmelser om intern kontroll i økonomiregelverket	52

Sammendrag

Kan du som leder svare på følgende spørsmål:

- Hvilke faktorer er avgjørende for måloppnåelse i min virksomhet?
- Hvordan kan jeg identifisere nye og endrede risikoer?
- Hvilke av disse risikoene er vurdert som vesentlige i forhold til måloppnåelse for min virksomhet?
- Hvordan kan jeg etablere hensiktsmessige styrings- og kontrollmekanismer som balanserer risiko, kontroll og kost/nytte ved ulike tiltak og kontrollaktiviteter?
- Hvordan kan jeg vite at disse styrings- og kontrollmekanismene fungerer effektivt og som forutsatt?

Dette metodedokumentet har til hensikt å gjøre deg bedre i stand til å svare på disse spørsmålene. Det beskriver en metode for hvordan du på en strukturert måte kan benytte risikostyring og intern kontroll som et verktøy for å gi rimelig sikkerhet for at virksomheten oppnår sine målsettinger. I arbeidet med metodedokumentet er det tatt utgangspunkt i et anerkjent internasjonalt rammeverk (COSO ERM, 2004). Den framgangsmåten som skisseres er tilpasset det statlige økonomiregelverket og statlige behov. Virksomheten kan likevel velge å bruke andre framgangsmåter som ivaretar økonomiregelverkets krav.

Håndtering av risiko i mål- og resultatstyringen

Mål- og resultatstyring er det overordnede styringsprinsipp i statlig forvaltning. En god mål- og resultatstyring forutsetter at virksomhetsledelsen kjenner og aktivt håndterer de utfordringer eller usikkerheter som kan påvirke måloppnåelse negativt. Økonomiregelverket inneholder gjennomgående krav om at all styring, oppfølging, kontroll og forvaltning i staten skal tilpasses virksomhetens egenart samt risiko og vesentlighet. I tillegg er kravene til intern kontroll i økonomiregelverket også krav til risikostyring. I dokumentet benyttes primært betegnelsen «risikostyring» og ikke «risikostyring og intern kontroll» om denne prosessen.

I etatsstyringen skal departementet sikre at underliggende virksomheter har etablert en forsvarlig risikostyring og intern kontroll. Virksomhetens ledelse skal sørge for at det er etablert en forsvarlig risikostyring og intern kontroll i virksomheten, og påse at den fungerer på en tilfredsstillende måte. Grunntanken i dokumentet er at metodikken og begrepsapparatet skal kunne benyttes av alle statlige virksomheter, både i departementenes styring av underliggende virksomheter og i den enkelte virksomhets interne styring, også departementenes interne styring. Metodedokumentet konsentrerer seg imidlertid hovedsakelig om den interne styringen.

I henhold til økonomiregelverket skal alle virksomheter sikre tilstrekkelig styringsinformasjon og forsvarlig beslutningsunderlag tilpasset virksomhetens egenart og risiko og vesentlighet. Regelverket inneholder i tillegg flere eksplisitte dokumentasjonskrav med relevans for dokumentasjon av risikostyring og intern kontroll som en integrert del av mål- og resultatstyringen. God dokumentasjon vil normalt også være et viktig bidrag i en kontinuerlig forbedring av risikostyringen og dermed av mål- og resultatstyringen som helhet.

Hva er risikostyring i staten og hva skal oppnås med den?

Økonomiregelverkets krav til risikostyring og intern kontroll i statlige virksomheter kan oppsummeres i beskrivelsen under.

Risikostyring og intern kontroll er en prosess integrert i mål- og resultatstyringen som:

- Er utformet for å kunne identifisere, vurdere, håndtere og følge opp risiko slik at risikoen er innenfor akseptert nivå.
- Gjennomføres av virksomhetens ledelse og øvrige ansatte.
- Anvendes i fastsettelse av strategi og planer og på tvers av virksomheten for å gi rimelig grad av sikkerhet for virksomhetens oppnåelse av sine målsettinger.

Av økonomiregelverket utledes tre kategorier av målsettinger som virksomheten skal oppfylle:

- Mål og resultatkrav.
- Pålitelig regnskapsrapportering og økonomiforvaltning.
- Overholdelse av lover og regler.

Målsettingene skal oppnås innenfor de rammene som tildelte bevilgninger og eventuelle andre disponible ressurser setter.

Definisjon av risiko: Det at forhold eller hendelser kan inntreffe og påvirke oppnåelse av målsettinger negativt. En risiko skal vurderes i forhold til *sannsynligheten* for at den inntreffer, og den forventede *konsekvensen* den vil medføre dersom den inntreffer. Resultatet av disse vurderingene angir hvor *høy* den enkelte risiko er. Det danner grunnlaget for å prioritere hvilke risikoer som anses som *vesentlige* i forhold til å kunne påvirke oppnåelsen av målsettinger negativt på ulike nivåer og som det derfor må legges vekt på videre i risikostyringsprosessen.

Definisjon av risikotoleranse: Et akseptert nivå på risiko for ikke å nå den enkelte målsetting. Risikotoleranse tar utgangspunkt i den risiko, i et vidt perspektiv, som en virksomhet kan akseptere i arbeidet med å realisere sitt formål/sin visjon, og som ligger til grunn for virksomhetens strategier og relaterte målsettinger. Strategiene og målsettingene, som i sin tur styrer fordelingen av ressurser, avklares i samråd med overordnet organ.

Når ledelsen vurderer en risiko til å være utenfor risikotoleransen, vil det være behov for å iverksette ytterligere tiltak og kontrollaktiviteter for å redusere risikoen til et akseptert nivå. På grunn av usikkerhet omkring framtiden, begrensede ressurser og begrensninger forbundet med enhver aktivitet vil det normalt ikke være mulig å redusere risikoen helt til null.

Tiltak og kontrollaktiviteter: Tiltak og kontrollaktiviteter skal bringe gjenværende risiko i samsvar med akseptert nivå. Tiltakene innarbeides i handlingsplaner eller lignende, og kontrollaktivitetene skal sikre at tiltakene blir utført på en effektiv måte og til rett tid. Kontrollaktiviteter består vanligvis av to hovedelementer – en beskrivelse av kontrollaktiviteten og hvordan den skal gjennomføres samt den faktiske gjennomføringen av aktiviteten.

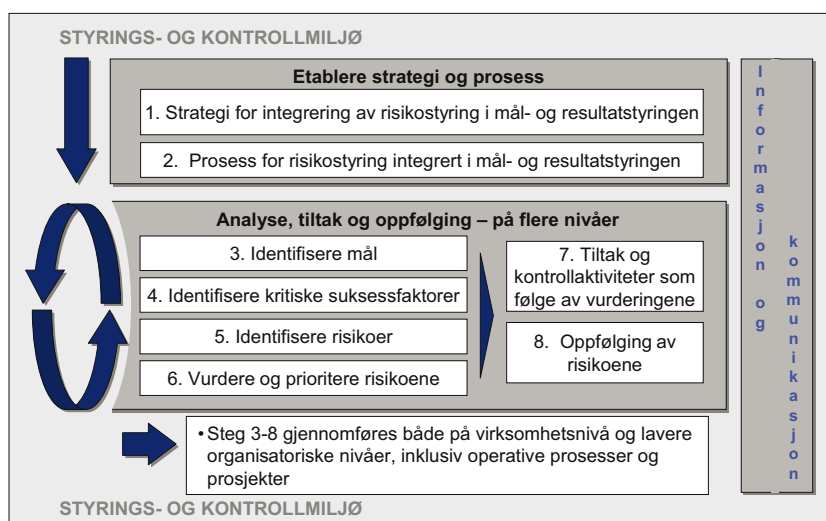
Valg av tiltak og kontrollaktiviteter: Valg av tiltak og tilhørende kontrollaktiviteter skal skje på bakgrunn av en vurdering av kostnad i forhold til nytte.

Fra økonomiregelverket kan følgende hovedelementer i risikostyring og intern kontroll stilles opp, som alle påvirker hverandre:

- **Styrings- og kontrollmiljø.**
- **Identifisering av mål.**
- **Identifisering av risikoer.**
- **Vurdering og prioritering av risikoer.**
- **Tiltak og kontrollaktiviteter som følge av vurderingene.**
- **Informasjon og kommunikasjon.**
- **Oppfølging.**

Metoden for risikostyring som gjennomgås i dokumentet er basert på disse hovedelementene, og beskriver dem nærmere.

Metode for håndtering av risiko i mål- og resultatstyringen



Risikostyring integrert i mål- og resultatstyringen kan illustreres som vist i figuren ovenfor. Figuren illustrerer åtte steg i prosessen. Stegene beskrives nærmere i tabellen på neste side. Steg 1 og 2 gjennomføres ved første gangs integrering, og gjentas ved senere revideringer av hvordan prosessen gjennomføres i den aktuelle virksomheten. Steg 3 til 8 gjennomføres så ofte som ledelsen beslutter i sin strategi for integreringen. Steg 3 til 8 gjennomføres både på virksomhetsnivå og på lavere organisatoriske nivåer samt for operative prosesser og prosjekter. God risikostyring forutsetter et sunt styrings- og kontrollmiljø og god informasjon og kommunikasjon. Dette danner grunnpilarene i en god risikostyring.

Styrings- og kontrollmiljøet omfatter kulturen i organisasjonen som bør påvirke de ansattes holdning til risikostyring positivt, slik at organisasjonen oppnår en sikker og forsvarlig drift. Uavhengig av organisatorisk nivå er det viktig at ledere går foran som et godt eksempel for de ansatte i organisasjonen. En rekke faktorer former styrings- og kontrollmiljøet. Viktige faktorer er: Det aksepterte nivå på risiko, ledelsens holdning til og interesse for effektiv risikostyring, hvordan ledelsen vektlegger måloppnåelse, integritet, etiske verdier og tilstrekkelig kompetanse på de ulike ledelsesnivå og hos organisasjonens øvrige medarbeidere, organisasjonsstrukturen, måten ledelsen tildeler ansvar og myndighet på, og hvordan ledelsen sikrer at alle ansatte forstår virksomhetens målsettinger.

God informasjon og kommunikasjon er nødvendig på alle nivåer i en organisasjon for å identifisere, vurdere, håndtere og følge opp risiko, og på annen måte styre virksomheten mot måloppnåelse. Dette omfatter ledelsens organiserte informasjon som gjør det mulig for de ansatte å gjennomføre sitt arbeid i tråd med det ansvaret de er tildelt. Videre omfattes også uformell kommunikasjon oppover, nedover og på tvers av den formelle organisasjonsstrukturen. Det er viktig at det er god kvalitet på virksomhetens styringsinformasjon. Den må være relevant, tidsriktig, korrekt og tilgjengelig for alle som har bruk for den. Videre må informasjon og kommunikasjon bidra til at risikovurderinger på ulike nivåer i organisasjonen ses i sammenheng.

ETABLERE STRATEGI OG PROSESS

STEG 1. Strategi for integrering av risikostyring i mål- og resultatstyringen

Hva bør ledelsen gjøre og hvorfor?	Hvordan kan dette gjøres?
Utarbeide en tydelig strategi. Dette vil bidra til en klar forståelse for hensikten med risikostyringen, hvilken verdi den vil ha i forhold til de oppgaver virksomheten er pålagt og hvordan risikostyringen skal integreres i mål- og resultatstyringen.	Strategien bør blant annet ta for seg hensikten med risikostyringen, ledelsens rolle, policy for risikostyring, implementeringsfaser og milepæler, eventuelt behov for endringsledelse og kompetanseutvikling.

STEG 2. Prosess for risikostyring integrert i mål- og resultatstyringen

God risikostyring er *integrert* i virksomhetens mål- og resultatstyring. Det betyr at den er et linjeansvar, og at den utføres samtidig med andre styringsprosesser. For eksempel er det viktig at risikovurderinger gjøres samtidig med andre planleggingsprosesser. På et *overordnet nivå* er det naturlig å gjennomføre risikovurderinger som en del av strategi- og planleggingsprosesser, og på *lavere organisasjonsnivåer* i forbindelse med utarbeidelse av virksomhetsplaner og lignende. På mer operative nivåer vil det være naturlig at det gjennomføres risikovurderinger og iverksettes ulike tiltak og kontrollaktiviteter i forbindelse med utforming av *operative prosesser*. Slike vurderinger bør utføres periodisk og når det skjer vesentlige endringer i mål, organisasjon eller andre interne og eksterne forhold. Risikostyring er også svært relevant i *prosjekter* som en virksomhet gjennomfører.

Hva bør ledelsen gjøre og hvorfor?	Hvordan kan dette gjøres?
Etablere en prosess for risikostyring integrert i mål- og resultatstyringen. Dette vil øke verdien av risikostyringen og bidra til effektiv ressursbruk. Når risikostyringen fullt ut er integrert i virksomhetens mål- og resultatstyring, vil ledelsen som en del av styringsinformasjonen ha informasjon fra risikovurderinger også på lavere nivåer i organisasjonen som grunnlag for den overordnede risikovurderingen.	Det bør utarbeides en oversikt over virksomhetens samlede aktiviteter og prosesser. Det bør foretas en vurdering av hvilke aktiviteter og prosesser som er viktigst å prioritere i implementeringsarbeidet og hvilke som kan tas på et senere tidspunkt. På bakgrunn av denne prioriteringen bør det utarbeides en implementeringsplan. Den overordnede samlede risikoanalysen bør gjennomføres før det foretas risikoanalyser innenfor de enkelte virksomhetsområdene («top-down» tilnærming). Det bør skapes en sammenheng mellom risikovurderinger på et overordnet nivå og lavere nivåer.

ANALYSE, TILTAK OG OPPFØLGING – PÅ FLERE NIVÅER

I det følgende beskrives stegene (3-8 i figuren) i en strukturert prosess for risikostyring. Framgangsmåten er hensiktsmessig både på overordnet nivå for virksomheten som helhet og på lavere organisatoriske nivåer, inklusiv operative prosesser og prosjekter.

STEG 3: Identifisere mål	
Hva bør ledelsen gjøre og hvorfor?	Hvordan kan dette gjøres?
<p>Gjennomgå de mål som virksomheten styres mot for å se om de er konkrete og tilstrekkelig klart formulerte. Målene må tilpasses for alle nivåer i organisasjonen.</p> <p>Det er nødvendig med klare mål for å kunne vurdere risikoen for ikke å nå disse målene.</p>	<p>Ved implementering av risikostyring må virksomhetens målsettinger innenfor de tre kategoriene gjennomgås for å se om de er konkrete nok og tilstrekkelig klart formulerte.</p>
STEG 4: Identifisere kritiske suksessfaktorer	
Hva bør ledelsen gjøre og hvorfor?	Hvordan kan dette gjøres?
<p>Identifiseres og systematisere de forhold som er viktigst å lykkes med for å nå målene.</p> <p>Å identifisere kritiske suksessfaktorer i forbindelse med måloppnåelse gjør det enklere å identifisere risikoen. Bevisste og godt formulerte kritiske suksessfaktorer tar også hensyn til de muligheter virksomheten har til å forbedre sine prestasjoner.</p>	<p>Ved implementering av risikostyring bør de forhold som er viktigst å lykkes med for å nå målene, identifiseres og systematiseres slik at de knyttes opp mot de mål de bidrar til å oppfylle. Styringsparametere kan, foruten å være resultatindikatorer, brukes til å vise framdriften og statusen i de forhold som er kartlagt som kritiske for å lykkes med måloppnåelsen.</p>
STEG 5: Identifisere risikoer	
Hva bør ledelsen gjøre og hvorfor?	Hvordan kan dette gjøres?
<p>Identifisere og kartlegge risikoer som kan true virksomhetens måloppnåelse.</p> <p>Ledelsen må ha et bevisst forhold til hvilke risikoer som kan true måloppnåelsen før det kan tas stilling til om de håndteres tilfredsstillende eller ikke på vurderingstidspunktet.</p>	<p>Ved å systematisere mål samt hvilke forhold som er kritiske å lykkes med for å nå målene (steg 3 og 4), skaffer ledelsen seg et godt grunnlag for å definere hvilke risikoer som truer disse forholdene. Risikofaktorer knyttet til den enkelte kritiske suksessfaktor kan identifiseres på mange ulike nivåer, og danner et «risikohierarki».</p>
STEG 6: Vurdere og prioritere risikoene – utarbeide risikokart	
Hva bør ledelsen gjøre og hvorfor?	Hvordan kan dette gjøres?
<p>Vurdere risikoene med hensyn til sannsynlighet for og forventet konsekvens av at de inntreffer. Vurdering av om en risiko er høy eller lav gjøres i forhold til det målet den truer oppfyllelsen av.</p> <p>Disse vurderingene vil gi en oversikt (et risikokart) over hvilke risikoer som håndteres godt nok allerede, og hvilke som ikke håndteres godt nok. Sammenfattet gir dette et bilde av sannsynligheten for at det aktuelle målet ikke nås, og hvor alvorlig dette avviker fra målet forventes å bli hvis ikke ytterligere tiltak iverksettes.</p>	<p>Vurdering og prioritering kan gjøres på ulike måter. For eksempel vurderinger hvor alle i den aktuelle ledergruppen deltar, vurderinger foretatt av den eller de lederne som i praksis håndterer risikoen på de ulike områder i virksomheten, eller virksomhetslederens vurdering som bygger på innspill fra andre ledere. Vurderingen må baseres på ledelsens risikotoleranser. For å kunne vurdere risikoen på et overordnet nivå, er det nødvendig at ledelsen har en oppfatning av hvordan risikoen på lavere nivåer håndteres.</p>

STEG 7: Tiltak og kontrollaktiviteter som følge av vurderingene

Risikovurderinger vil, uavhengig av hvilket nivå de er gjennomført på eller om de er knyttet til et prosjekt eller en operativ prosess, lede til ulike typer beslutninger om hvordan risikoen bør håndteres. Beslutninger omkring håndtering av risiko kan generelt deles inn i fire kategorier. Disse kategoriene er å unngå, redusere, dele eller akseptere risiko. Skillet mellom sannsynlighet og konsekvens i risikovurderingene vil være til hjelp når ledelsen skal vurdere hvilken håndtering som vil ha størst effekt.

Hva bør ledelsen gjøre og hvorfor?	Hvordan kan dette gjøres?
<p>Vurdere og fatte beslutning om hvordan risikoene skal håndteres for å bringe risikoen innenfor et akseptabelt nivå.</p> <p>Iverksette de nødvendige tiltak og kontrollaktiviteter for å sikre at risikohåndteringen blir utført på en effektiv måte. Det må følges opp at kontrollaktivitetene gjennomføres som forutsatt.</p>	<p>Prioritering av nye tiltak og kontrollaktiviteter må gjøres på bakgrunn av den effekten alternative tiltak må antas å ha for å redusere en uønsket risiko, og i hvilken grad tiltakene er gjennomførbare basert på en kost/ nytte vurdering. Ledelsen må også ha en oppfatning av om de vedtatte tiltakene vil være tilstrekkelige til å redusere risikoen til et akseptabelt nivå innenfor en akseptabel tidsramme.</p>

STEG 8: Oppfølging av risikoene

Hva bør ledelsen gjøre og hvorfor?	Hvordan kan dette gjøres?
<p>Følge opp risikostyringen, og vurdere om den fungerer over tid. Ledelsen bør fastsette og konkretisere hvordan den skal skaffe seg tilstrekkelig oversikt over hvordan risikostyringen praktiseres i virksomheten. Dette oppnås gjennom løpende oppfølgingsaktiviteter, evalueringer eller en kombinasjon av de to.</p> <p>En god oppfølging av risikoer vil gi ledelsen god styringsinformasjon og muligheten til å iverksette nødvendige tiltak på et tidlig tidspunkt. Ledelsens oppfølging har også en betydelig preventiv verdi.</p>	<p>Det kan være effektivt å implementere oppfølging via styringsparametere som sier noe om hvordan risikoene håndteres. Også operasjonelle forhold kan måles ved bruk av styringsparametere. I tillegg kan oppfølgingen skje på andre måter, for eksempel ved systematisk gjennomgang i møter, samtaler rundt driftsproblemer, rapporter, stikkprøver og drøfting av feilsituasjoner som oppstår og i form av egnevalueringer fra ledere.</p> <p>Evalueringer kan også foretas på et mer objektivt grunnlag av personer som har større avstand til det som skal evalueres, for eksempel en internrevisjon.</p>

Risikostyringens begrensninger

Uansett hvor godt risikostyringen planlegges og gjennomføres, kan den bare gi ledelsen og overordnet organ rimelig sikkerhet for at virksomheten vil oppnå sine målsettinger. Det er blant annet begrensninger i tilknytning til uklare målformuleringer, ulik oppfatning av mål og/eller risikotoleranser samt svakheter i menneskelig dømmekraft.

I tillegg representerer det en begrensning at beslutninger om tiltak og kontrollaktiviteter må bygge på en kost/nytte vurdering. Videre kan det være at tiltakene og kontrollaktivitetene ikke gjennomføres som forutsatt på grunn av ubevisste eller bevisste feil.

1 Innledning

Departementer og statlige virksomheter skal ivareta mange og viktige oppgaver i samfunnet. Mål- og resultatstyring skal sikre at de overordnede politiske målene blir brutt ned til konkrete mål som virksomhetsledere kan styre etter. Både eksterne og interne rammebetingelser påvirker de mulighetene virksomhetene har til å innfri de krav og forventninger de er stilt overfor. Utfordringer eller usikkerheter som kan påvirke måloppnåelse negativt, omtales gjerne som risikoer. En god mål- og resultatstyring forutsetter derfor at virksomhetsledelsen kjenner og aktivt håndterer disse risikoene. Risikostyring og intern kontroll integrert i mål- og resultatstyringen skal bidra til at virksomheten når sine mål.

Mål- og resultatstyring er det overordnede styringsprinsipp i statlig forvaltning. Dette er nedfelt i bevilgningsreglementet¹, og i de grunnleggende styringsprinsippene i økonomiregelverket² (se rammen under). I økonomiregelverket for øvrig følges prinsippet opp og utdypes. Økonomiregelverket omhandler etat- og virksomhetsstyringen i staten i et bredt perspektiv, og dreier seg ikke bare om økonomistyring.

Reglement for økonomistyring i staten

§ 1 Formål

Reglement for økonomistyring har som formål å sikre at

- a) statlige midler brukes og inntekter oppnås i samsvar med Stortingets vedtak og forutsetninger
- b) fastsatte mål og resultatkrav oppnås
- c) statlige midler brukes effektivt
- d) statens materielle verdier forvaltes på en forsvarlig måte

§ 4 Grunnleggende styringsprinsipper

Alle virksomheter skal

- a) fastsette mål og resultatkrav innenfor rammen av disponible ressurser og forutsetninger gitt av overordnet myndighet
- b) sikre at fastsatte mål og resultatkrav oppnås, ressursbruken er effektiv og at virksomheten drives i samsvar med gjeldende lover og regler, herunder krav til god forvaltningsskikk, habilitet og etisk atferd
- c) sikre tilstrekkelig styringsinformasjon og forsvarlig beslutningsgrunnlag

Departementet skal i tillegg fastsette overordnede mål og styringsparametere for underliggende virksomheter, jf. § 7.

Styring, oppfølging, kontroll og forvaltning må tilpasses virksomhetens egenart samt risiko og vesentlighet.

¹«Bevilgningsreglementet» fastsatt av Stortinget 26. mai 2005 (erstatte det tidligere Bevilgningsreglementet fastsatt av Stortinget 19. november 1959 (med senere endringer) fra 1. januar 2006).

²«Økonomiregelverket» benyttes i metodedokumentet som samlebetegnelse for «Reglement for økonomistyring i staten» (i dokumentet forkortet til Reglementet eller «R»), fastsatt ved kronprinsregentens resolusjon 12.12.2003 og Bestemmelser om økonomistyring i staten (i dokumentet forkortet til Bestemmelsene eller «B»), fastsatt av Finansdepartementet 12.12.2003.

Økonomiregelverket inneholder krav om at styring, oppfølging, kontroll og forvaltning skal tilpasses virksomhetens egenart samt risiko og vesentlighet (jf. siste setning i § 4 i boksen på forrige side). Tilpasningskravet gjelder både i styring og kontroll i det enkelte departement, i departementets styring og kontroll av underliggende virksomheter (etatsstyringen) og i styring og kontroll i den enkelte virksomhet. I tillegg krever regelverket eksplisitt at alle virksomheter skal etablere intern kontroll tilpasset risiko og vesentlighet (B 2.4 jf. R § 14).

Disse gjennomgående kravene i økonomiregelverket innebærer at vurdering av risiko og vesentlighet skal ligge til grunn for å utforme det samlede styrings- og kontrollopplegget.³ Forsvarlig håndtering av risiko er nødvendig for alle departementer og underliggende virksomheter, uansett område og størrelse. Viktige utfordringer er å integrere slike vurderinger i styringsprosessene, å se klare sammenhenger mellom mål, risiko og tiltak, samt å ta stilling til akseptabelt nivå på risiko.

Kravene til intern kontroll i økonomiregelverket er også krav til risikostyring. Kravene sier eksplisitt at den interne kontrollen skal være innebygd i virksomhetens interne styring, og øke sannsynligheten for oppnåelse av virksomhetens mål ved at man identifiserer risikoer og tiltak for å redusere risikoene. De andre elementene som kravene til intern kontroll omfatter, representerer alle komponenter i god risikostyring.

I dette metodedokumentet benyttes «risikostyring og intern kontroll» som betegnelse på den prosessen som omfatter å identifisere, vurdere, håndtere og følge opp risiko som en del av mål- og resultatstyringen i staten. «Risikostyring og intern kontroll» blir dermed en samlebetegnelse på det som i økonomiregelverket dekkes av begrepet «intern kontroll», og de gjennomgående kravene om å tilpasse all styring, oppfølging, kontroll og forvaltning til risiko og vesentlighet, også i departementenes styring av underliggende virksomheter. I kapittel 2.2 gis en nærmere beskrivelse av prosessen og komponentene i risikostyringen ifølge det statlige økonomiregelverket. For enkelhets skyld benytter dokumentet i noen sammenhenger begrepet «risikostyring» alene og ikke «risikostyring og intern kontroll» for å beskrive denne prosessen. Dette gjelder særlig i metodedelen i kapittel 3.

Ansvar for risikostyring og intern kontroll ligger hos virksomhetens ledelse.⁴ Metodedokumentet søker å gjøre dette ansvaret enklere å forvalte ved å beskrive hvordan virksomheten på en strukturert måte kan identifisere, vurdere, håndtere og følge opp risiko.

Økonomiregelverket forutsetter at virksomhetene iverksetter aktiviteter for å tilpasse og bygge inn en tilfredsstillende håndtering av risiko i sin mål- og resultatstyring, både i planlegging, gjennomføring og oppfølging.

³ Se R §§ 4, 10 og 16, B 1.2, 1.3, 1.5.2, 1.5.3, 2.2, 2.4, 2.5.3, 2.5.5, 2.6, 4.3.6, 5.4.2.2, 6.5, 7.4, og 8.5.

⁴ Bestemmelsene benytter begrepet "virksomhetens ledelse" blant annet i forbindelse med omtale av myndighet og ansvar for virksomhetens interne styring (kapittel 2). Begrepet ledelse omfatter i denne sammenheng både virksomhetslederen og eventuelt styre for virksomheten. Det foreliggende metodedokumentet benytter begrepet «virksomhetslederen» i enkelte sammenhenger, uten at det innebærer noen realitetsforskjell fra Bestemmelsene. Det henvises for øvrig til kapittel 1.1 om ansvarsforhold.

I arbeidet med dette metodedokumentet er det valgt å ta utgangspunkt i COSO Enterprise risk management rammeverket (COSO ERM).⁵ Metodedokumentet skisserer en framgangsmåte tilpasset det statlige økonomiregelverket og statlige behov. Kapittel 3 inneholder veiledning og eksempler på et helhetlig opplegg for risikostyring. Virksomheten kan likevel velge å bruke andre framgangsmåter som ivaretar økonomiregelverkets krav.

De eksisterende styringsprosessene som risikostyring og intern kontroll skal integreres i, vil i stor grad være unike for den enkelte virksomhet – avhengig av virksomhetens egenart (samfunnsrolle, størrelse, kompleksitet osv.). Metodedokumentet beskriver derfor ikke fullt ut hvordan risikostyring og intern kontroll kan integreres i den enkelte virksomhets styring og i etatsstyringen. SSØ ønsker imidlertid å legge ut eksempler fra ulike statlige virksomheter på www.sfs.no.

1.1 Ansvar for risikostyring og intern kontroll

1.1.1 Virksomhetens interne styring

Virksomhetens ledelse

Virksomhetens ledelse skal sørge for at virksomheten har etablert en forsvarlig risikostyring og intern kontroll, og påse at den fungerer på en tilfredsstillende måte. Dette følger bl.a. av Reglement for økonomistyring i staten (R) §§ 4 og 14 og Bestemmelser om økonomistyring i staten (B) kapittel 2. Øverste administrative ledelse har samme ansvar for departementets interne styring som ledelsen i en underliggende virksomhet.

En leder i en statlig virksomhet har ansvar for å fastsette mål og resultatkrav i samsvar med eller avledet av de målene og resultatkravene som er satt av overordnet organ, og sørge for at disse nås. Virksomhetslederen skal med utgangspunkt i virksomhetens målsettinger og aktuelle risikoer på ulike nivåer sørge for å etablere en forsvarlig risikostyring og intern kontroll i henhold til økonomiregelverket. Virksomhetslederen skal sørge for at risikostyring og intern kontroll blir etablert, gjennomført, fulgt opp og dokumentert på en tilstrekkelig og effektiv måte – som en integrert del av mål- og resultatstyringen. Det er virksomhetslederens ansvar å sørge for at overordnet organ er tilstrekkelig orientert om hovedtrekkene i virksomhetens risikostyring og interne kontroll.

Virksomhetslederen er sentral for å etablere et godt styrings- og kontrollmiljø på alle nivåer. Det er viktig at lederen legger til rette for god kommunikasjon internt i organisasjonen, og for et åpent samspill med overordnet organ om disse forholdene.

En god intern styring forutsetter at lederen fordeler myndighet (fullmakter) og ansvar i form av instruksjer. Disse dokumentene reflekterer ansvaret for å etablere, gjennomføre, følge opp og dokumentere risikostyring og intern kontroll i henhold til økonomiregelverkets krav. Departementene

⁵ COSO er en forkortelse for The Committee of Sponsoring Organizations of the Treadway Commission, en arbeidsgruppe bestående av fem organisasjoner som har engasjert seg i å strukturere hvordan organisasjoner kan etablere egnede effektive styrings- og kontrollstrukturer. De fem organisasjonene er American Institute of Certified Public Accountants, American Accounting Association, The Institute of Internal Auditors, Institute of Management Accountants og Financial Executives Institute. I 1992 publiserte COSO et rammeverk for intern kontroll som i dag trolig er det mest aksepterte utgangspunktet som finnes internasjonalt for utvikling av intern styring og kontroll. I 2004 utga COSO «Enterprise Risk Management – Integrated Framework» som integrerer det opprinnelige COSO rammeverket, men utvider perspektivet ved å utvikle risikostyringsperspektivet. Rammeverket er oversatt til norsk i regi av Norges Interne Revisorers Forening. Se <http://www.nirf.org/> for nærmere informasjon om «Helhetlig risikostyring – et integrert rammeverk».

skal fastsette instruksjoner innenfor rammen av økonomiregelverket både for departementet og underliggende virksomheter (jf. R § 3 og B 1.2 og 2.2). Underliggende virksomheter skal fastsette instruksjoner for egne aktiviteter innenfor rammen av instruksjonen fra overordnet departement (jf. R § 3 og B 1.2 og 2.2).

Øvrige ledere og ansatte

Øvrige ledere skal med utgangspunkt i virksomhetens målsettinger sørge for en forsvarlig risikostyring og intern kontroll innenfor sine ansvarsområder integrert i mål- og resultatstyringen.

Alle ansatte i virksomheten har dessuten et selvstendig ansvar for å sørge for at det daglige arbeidet gjennomføres med den nødvendige kvalitet, på en mest mulig hensiktsmessig måte og i samsvar med gjeldende regler og rutiner.

1.1.2 Departementets styring av virksomheter

Departementet skal påse at dets underliggende virksomheter har etablert en forsvarlig risikostyring og intern kontroll. Dette bidrar til å sikre tilstrekkelig styringsinformasjon og et forsvarlig beslutningsgrunnlag tilpasset virksomhetens egenart samt risiko og vesentlighet. Dette følger bl.a. av Reglementet §§ 4 og 15 og Bestemmelsene kapittel 1.

Departementet står fritt til å finne en praktisk og oversiktlig form for hvordan dette skal gjøres. Men virksomhetens ansvar for håndtering av risiko i mål- og resultatstyringen skal fremkomme i ansvars- og myndighetsbeskrivelsen. Departementet skal sikre seg at virksomheten med utgangspunkt i valgte mål og strategier har etablert en prosess for håndtering av risiko i mål- og resultatstyringen og at denne prosessen gjennomføres, følges opp og dokumenteres i henhold til økonomiregelverkets krav. Dette skal legge til rette for departementenes styring, oppfølging og kontroll av virksomhetene.

1.2 Formålet med metodedokumentet

Dette metodedokumentet skal veilede virksomhetene i hvordan risikostyring og intern kontroll kan gjennomføres innenfor de rammer som regelverket setter. Den primære målgruppen er ledere på ulike nivåer i virksomhetene og de personer som bistår lederne i å tilrettelegge risikostyring og intern kontroll.

Grunntanken er at metodikken og begrepsapparatet skal kunne benyttes av alle statlige virksomheter, både i departementenes styring av underliggende virksomheter og i den enkelte virksomhets interne styring, også departementenes interne styring. Metodedokumentet konsentrerer seg imidlertid hovedsakelig om den interne styringen.

Gjennomgangseksempelen som er innarbeidet, tar utgangspunkt i den enkelte virksomhets interne styring og viser konkret hvordan den metoden som beskrives kan anvendes i praksis. Eksempelen tar for seg målet om høy brukertilfredshet i en forvaltningsvirksomhet. Ikke alle statlige forvaltningsorgan ivaretar oppgaver som gjør dette til et direkte relevant eksempel. Eksempelen er likevel valgt fordi det vil være gjenkjennelig for mange virksomheter.

I metodedokumentet benyttes et begrepsapparat som er faglig anerkjent på området risikostyring og intern kontroll, jf. økonomiregelverket og COSO ERM. I stikkordregisteret finnes henvisning til hvor i dokumentet de forskjellige begrepene er forklart.

2 Håndtering av risiko i mål- og resultatstyringen

Statlige virksomheter utfører allerede ulike former for vurdering av risiko og av hva som må gjøres for å redusere risikoen. Det er viktig at virksomhetene nyttiggjør seg de vurderinger og prosesser som allerede er etablert. En mer strukturert tilnærming til å identifisere, vurdere, håndtere og følge opp risiko i hele virksomheten kan likevel bringe en ny og viktig dimensjon inn i den etablerte etat- og virksomhetsstyringen.

Det er svært viktig å forstå verdien av risikostyring og intern kontroll som en integrert del av den samlede mål- og resultatstyringen. Hvis risikostyring og intern kontroll kun blir en prosess på siden av, og ikke som en del av prosessene i etat- og virksomhetsstyringen, vil verdien være begrenset for virksomheten. Dessuten kan parallelle prosesser innebære lite effektiv ressursbruk fordi beslektede tema behandles på ulike arenaer og i ulike dokumenter. Følgende figur illustrerer sammenhengen mellom virksomhetens vurdering og håndtering av risikoer og den øvrige mål- og resultatstyringen:

Figur 1: Håndtering av risiko i mål- og resultatstyringen



Uansett hvilket nivå i virksomheten risikostyring og intern kontroll utøves på, vil den alltid ta utgangspunkt i de målene som er fastsatt for det enkelte nivået, og i de strategiene som er fastsatt for å nå dem. I en strategi vil enkelte forhold være viktigere enn andre for at virksomheten skal lykkes. Her betegnes dette som kritiske suksessfaktorer.⁶ De enkelte organisatoriske nivåene må være bevisst hvilke forhold dette er, slik at de knyttes sammen med strategiene.

⁶ Begrepet «kritiske suksessfaktorer» benyttes i metodedokumentet som betegnelse på hvilke faktorer det er viktigst å lykkes med for å nå mål på ulike nivåer i virksomheten. Begrepet anvendes i den praktiske tilnærmingen for risikostyring som dette metodedokumentet beskriver, fordi det er essensielt å tydeliggjøre hva det er viktigst å lykkes med som utgangspunkt for å gjøre en god risikovurdering. Det understrekes at det ikke ligger noen føringer i retning av bestemte styringsmodeller som for eksempel balansert målstyring i dette, selv om begrepet «kritisk suksessfaktor» også benyttes i slike modeller.

Etablering av styringsparametere som viser graden av oppfyllelse av de kritiske suksessfaktorene vil, gitt at det er god sammenheng med de målene som er etablert, bidra til at den samlede styringen blir mer effektiv. På bakgrunn av den sammenheng som da etableres mellom mål, strategier, kritiske suksessfaktorer og tilhørende styringsparametere, vil det være mulig å identifisere og vurdere risikoer knyttet til måloppnåelsen. Til slutt illustrerer figuren at vurdering av om etablerte tiltak og kontrollaktiviteter er tilstrekkelige og effektive, knyttes sammen med de risikoer de er ment å redusere.

Ved å etablere sterke sammenhenger fra mål til tiltak og kontrollaktiviteter, styrkes fokuset på de forhold som er viktigst for Stortinget, departementet og virksomheten. Slik vil man kunne oppnå en raskere effekt av de initiativ som tas med en mer effektiv ressursbruk.

2.1 Tre kategorier av målsettinger

Av de grunnleggende styringsprinsippene i Reglementet § 4 (jf. omtale i kapittel 1) kan vi utlede tre kategorier av målsettinger som virksomheten må oppfylle:

- Mål og resultatkrav.
- Pålitelig regnskapsrapportering og økonomiforvaltning.
- Overholdelse av lover og regler.

Målsettingene skal oppnås innenfor de rammene som tildelte bevilgninger og eventuelle andre disponible ressurser setter.

Risikostyring og intern kontroll har som hensikt å gi rimelig sikkerhet for oppnåelse av målsettinger innen alle de tre kategoriene (se kapittel 3.10 om risikostyringens begrensninger). I regelverket understrekes dette av at målsettingene også går igjen i Reglementet § 14 og gjentas i Bestemmelsene 2.4 om intern kontroll som vist i vedlegg A til metodedokumentet.

2.2 Risikostyring og intern kontroll – en prosess

Som beskrevet i kapittel 1 krever økonomiregelverket at vurdering av risiko og vesentlighet skal ligge til grunn for å avgjøre det samlede styrings- og kontrollopplegget. Dette fremkommer av de gjennomgående kravene i økonomiregelverket om å tilpasse all styring, oppfølging, kontroll og forvaltning til risiko og vesentlighet, sett i sammenheng med kravene til intern kontroll i Reglementet § 14 og Bestemmelsene 2.4 (se vedlegg A).⁷ Kravene har et prosessperspektiv på internkontrollen ved at den skal være innebygd i virksomhetens interne styring og øke sannsynligheten for måloppnåelse ved å identifisere risikoer og tiltak for å redusere risikoene.⁸ Kravene kan oppsummeres i beskrivelsen på neste side av en prosess for risikostyring og intern kontroll i statlige virksomheter. (Videre i dokumentet benyttes som nevnt primært betegnelsen «risikostyring» og ikke «risikostyring og intern kontroll» om denne prosessen.)

⁷ Se R §§ 4, 10 og 16, B 1.2, 1.3, 1.5.2, 1.5.3, 2.2, 2.4, 2.5.3, 2.5.5, 2.6, 4.3.6, 5.4.2.2, 6.5, 7.4, og 8.5.

⁸ Det vil si at intern kontroll begrepet i økonomiregelverket omfatter langt mer av styringsaspekter enn en mer tradisjonell og snever fortolkning av begrepet til bare å omfatte konkrete interne kontrolltiltak.

Definisjoner og sentrale begreper

Risikostyring og intern kontroll er en prosess integrert i mål- og resultatstyringen som:

- Er utformet for å kunne identifisere, vurdere, håndtere og følge opp risiko slik at risikoen er innenfor akseptert nivå.
- Gjennomføres av virksomhetens ledelse og øvrige ansatte.
- Anvendes i fastsettelse av strategi og planer og på tvers av virksomheten for å gi rimelig grad av sikkerhet for virksomhetens oppnåelse av sine målsettinger.

Kategorier av målsettinger virksomheten skal oppfylle:

- Mål og resultatkrav.
- Pålitelig regnskapsrapportering og økonomiforvaltning.
- Overholdelse av lover og regler.

Målsettingene skal oppnås innenfor de rammene som tildelte bevilgninger og eventuelle andre disponible ressurser setter.

Definisjon av risiko: Det at forhold eller hendelser kan inntreffe og påvirke oppnåelse av målsettinger negativt. En risiko skal vurderes i forhold til *sannsynligheten* for at den inntreffer, og den forventede *konsekvensen* den vil medføre dersom den inntreffer. Resultatet av disse vurderingene angir hvor *høy* den enkelte risiko er. Det danner grunnlaget for å prioritere hvilke risikoer som anses som *vesentlige* i forhold til å kunne påvirke oppnåelsen av målsettinger negativt på ulike nivåer og som det derfor må legges vekt på videre i risikostyringsprosessen.

Definisjon av risikotoleranse: Et akseptert nivå på risiko for ikke å nå den enkelte målsetting. Risikotoleranse tar utgangspunkt i den risiko, i et vidt perspektiv, som en virksomhet kan akseptere i arbeidet med å realisere sitt formål/sin visjon, og som ligger til grunn for virksomhetens strategier og relaterte målsettinger. Strategiene og målsettingene, som i sin tur styrer fordelingen av ressurser, avklares i samråd med overordnet organ.

Når ledelsen vurderer en risiko til å være utenfor risikotoleransen, vil det være behov for å iverksette ytterligere tiltak og kontrollaktiviteter for å redusere risikoen til et akseptert nivå. På grunn av usikkerhet omkring framtiden, begrensede ressurser og begrensninger forbundet med enhver aktivitet vil det normalt ikke være mulig å redusere risikoen helt til null.

Tiltak og kontrollaktiviteter: Tiltak og kontrollaktiviteter skal bringe gjenværende risiko i samsvar med akseptert nivå. Tiltakene innarbeides i handlingsplaner eller lignende, og kontrollaktivitetene skal sikre at tiltakene blir utført på en effektiv måte og til rett tid. Kontrollaktiviteter består vanligvis av to hovedelementer – en beskrivelse av kontrollaktiviteten og hvordan den skal gjennomføres samt den faktiske gjennomføringen av aktiviteten.

Valg av tiltak og kontrollaktiviteter: Valg av tiltak og tilhørende kontrollaktiviteter skal skje på bakgrunn av en vurdering av kostnad i forhold til nytte (jf. R § 4 og B 2.4).

Fra gjennomgangen ovenfor og Bestemmelsene 2.4 (se vedlegg A) kan det stilles opp følgende hovedelementer i god risikostyring og intern kontroll:

Hovedelementer i god risikostyring og intern kontroll

- Styrings- og kontrollmiljø.
- Identifisering av mål og kritiske suksessfaktorer.
- Identifisering av risikoer.
- Vurdering og prioritering av risikoer.
- Tiltak og kontrollaktiviteter som følge av vurderingene.
- Informasjon og kommunikasjon.
- Oppfølging.

Metoden for risikostyring som gjennomgås i kapittel 3 er basert på disse hovedelementene, og beskriver dem nærmere.

2.3 Dokumentasjon

Alle statlige virksomheter skal sikre tilstrekkelig styringsinformasjon og forsvarlig beslutningsgrunnlag tilpasset virksomhetens egenart samt risiko og vesentlighet (R § 4). Regelverket inneholder i tillegg flere eksplisitte dokumentasjonskrav med relevans for dokumentasjon av risikostyring og intern kontroll som en integrert del av mål- og resultatstyringen, se nedenfor.

Departementet skal påse at de underliggende virksomheter utfører sine oppgaver forsvarlig og målrettet (R § 15 og B 1.5.2). Departementet skal fastsette instruks for underliggende virksomheter, og virksomhetene skal fastsette instruks for egne aktiviteter innenfor rammen av instruks fra overordnet departement (R § 3). Styringsdialogen mellom departement og virksomhet skal være dokumenterbar (B 1.3). Tildelingsbrevene skal blant annet inneholde overordnede mål, styringsparametere, tildelte beløp og krav til rapportering (R § 7 og B 1.4). Virksomhetens planer skal dokumenteres gjennom interne styringsdokumenter (B 2.3.1). I tillegg stiller Bestemmelsene 2.4 et særskilt krav om at virksomhetens ledelse skal påse at den interne kontrollen kan dokumenteres.

Regelverket regulerer ikke spesifikt hva slags dokumenter det er behov for å utarbeide, eller hvordan disse skal innrettes og bygges opp, med unntak av instruks og tildelingsbrev omtalt ovenfor og i tilknytning til visse operative prosesser i økonomistyringen.⁹

⁹ Økonomiregelverket inneholder konkrete bestemmelser om dokumentasjon i tilknytning til noen operative prosesser, blant annet av økonomisystemet (B 4.3.5), av transaksjonskontroller av utgifter og inntekter (B 2.5) og av bokførte opplysninger (B 4.4.4). Disse delene av de operative prosessene er ikke hovedfokus for det foreliggende metode-dokumentet, og slike særskilte dokumentasjonskrav omtales derfor ikke nærmere i det videre. Nærmere omtale og forklaring av regelverkets dokumentasjonskrav knyttet til ulike operative funksjoner finnes i veiledningsmateriellet Ordsøk, som finnes på www.sfsno.no.

Om form, frekvens og omfang på dokumentasjonen

Regelverket krever ikke at dokumentasjonen av risikostyring og intern kontroll skal framgå i form av egne dokumenter. Virksomheten kan derfor utforme dokumentasjon av hvordan risiko håndteres i mål- og resultatstyringen på den måten som passer best inn i virksomhetens opplegg for styring, oppfølging, kontroll og forvaltning. Dette kan for eksempel skje i form av en sammenhengende, oversiktlig og forståelig framstilling av hvordan risiko håndteres som en del av virksomhetens øvrige dokumentasjon av mål- og resultatstyringen.

Regelverket stiller heller ingen spesifikke krav til frekvens eller omfang på dokumentasjonen. Det er derfor opp til virksomheten å fastsette hva som er nødvendig for at ledere på de ulike nivåer skal være tilstrekkelig informert for å kunne ivareta sitt ansvar for å sikre og følge opp forsvarlig og målrettet drift. Normalt vil dette innebære en konsentrasjon om stadig mer vesentlige forhold jo høyere opp i styringshierarkiet informasjonen skal brukes. Virksomheten bør imidlertid samtidig ta i betraktning at selv små svakheter og feil kan bli vesentlige hvis de oppstår i et stort antall eller innebærer signal om svakheter av generell art.

Virksomheten kan også selv velge system, presentasjonsform og oppbevaringsmedium ut fra virksomhetens størrelse og kompleksitet.

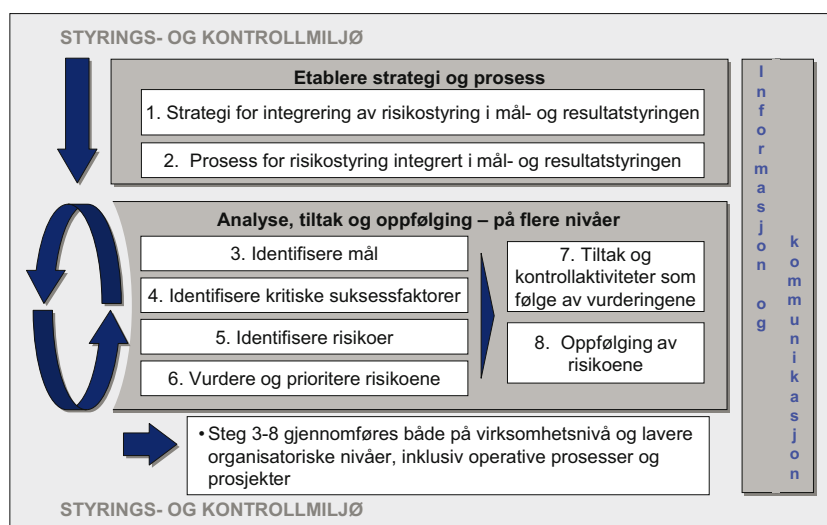
I kapittel 3.1 gjennomgås hvordan en god dokumentasjon kan være et nyttig bidrag i en kontinuerlig forbedring av risikostyring og intern kontroll og dermed av mål- og resultatstyringen som helhet.

3 Metode for håndtering av risiko i mål- og resultatstyringen

Dette kapitlet omhandler en prosess for håndtering av risiko i mål- og resultatstyringen basert på et anerkjent internasjonalt rammeverk og tilpasset kravene i økonomiregelverket. Den metoden som beskrives her, representerer en av flere mulige framgangsmåter. Metoden ligger godt innenfor de krav som økonomiregelverket stiller. Virksomheten kan velge å benytte andre framgangsmåter som ivaretar økonomiregelverkets krav, jf. beskrivelsen av disse kravene i kapittel 1 og 2. Virksomheten bør dokumentere den valgte metoden.

Figuren nedenfor illustrerer de åtte stegene i prosessen. Steg 1 og 2 gjennomføres ved første gangs integrering av risikostyring i mål- og resultatstyringen, og gjentas ved senere revideringer av hvordan prosessen skal gjennomføres i den aktuelle virksomheten. Steg 3 til 8 gjennomføres så ofte som ledelsen beslutter i sin strategi for integreringen. De gjennomføres både på virksomhetsnivå og på lavere organisatoriske nivåer samt for operative prosesser og prosjekter.

Figur 2: Risikostyring integrert i mål- og resultatstyringen



Fra figuren over og gjennomgangen foran kan følgende hovedelementer i god risikostyring stilles opp, som alle påvirker hverandre:

- Styrings- og kontrollmiljø.
- Identifisering av mål og kritiske suksessfaktorer.
- Identifisering av risikoer.
- Vurdering og prioritering av risikoer.
- Tiltak og kontrollaktiviteter som følge av vurderingene.
- Informasjon og kommunikasjon.
- Oppfølging.

Et godt styrings- og kontrollmiljø og god informasjon og kommunikasjon danner grunnpilarene i en god risikostyring og blir omtalt separat under. Temaet blir også behandlet senere i dokumentet integrert i behandlingen av de øvrige elementene i risikostyringen.

Styrings- og kontrollmiljø

God risikostyring forutsetter et sunt styrings- og kontrollmiljø. Et sunt styrings- og kontrollmiljø vil motivere til målrettet innsats og styring. Styrings- og kontrollmiljøet omfatter kulturen i organisasjonen som bør påvirke de ansattes holdning til risikostyring positivt, slik at organisasjonen oppnår en sikker og forsvarlig drift. Uavhengig av organisatorisk nivå er det viktig at ledere går foran som et godt eksempel for de ansatte i organisasjonen.

En rekke faktorer former styrings- og kontrollmiljøet. Viktige faktorer er:

- Det aksepterte nivået på risiko.
- Ledelsens holdning til og interesse for effektiv risikostyring.
- Hvordan ledelsen vektlegger måloppnåelse, integritet, etiske verdier og tilstrekkelig kompetanse på de ulike ledelsesnivå og hos organisasjonens øvrige medarbeidere.
- Organisasjonsstrukturen.
- Måten ledelsen tildeler ansvar og myndighet på.
- Hvordan ledelsen sikrer at alle ansatte forstår virksomhetens målsettinger.

Informasjon og kommunikasjon

God risikostyring forutsetter god informasjon og kommunikasjon. Informasjon og kommunikasjon er nødvendig på alle nivåer for å identifisere, vurdere, håndtere og følge opp risiko, og på annen måte styre virksomheten mot måloppnåelse. Dette omfatter ledelsens organiserte informasjon som gjør det mulig for de ansatte å gjennomføre sitt arbeid i tråd med det ansvaret de er tildelt. Videre omfattes også uformell kommunikasjon oppover, nedover og på tvers av den formelle organisasjonsstrukturen. Informasjonen og kommunikasjonen må bidra til at risikovurderinger sees i sammenheng på ulike nivåer i organisasjonen.

Virksomhetens systemer for styringsdata produserer rapporter med ulike typer finansiell og annen informasjon som bidrar til å gjøre det mulig å drive og ha kontroll med virksomheten. Styringsdata må innhentes, bearbeides og formidles på en måte og til tidspunkter som gjør de ansvarlige i stand til å utføre sine oppgaver. Det er viktig at det er god kvalitet på virksomhetens styringsinformasjon. Den må være relevant, tidsriktig, korrekt og være tilgjengelig for alle som har bruk for den.

3.1 Formålet med dokumentasjon av risikostyringen

Formål med dokumentasjonen

God dokumentasjon vil normalt være et viktig bidrag i en kontinuerlig forbedring av risikostyringen. I det følgende beskrives formålene med og nytteverdien for ledelsen av å dokumentere risikostyringen. Med den frihet og fleksibilitet som er gitt til å velge form, frekvens og omfang på dokumentasjonen (se kapittel 2.3), skal ledere innenfor sine ansvarsområder sørge for at formålene med dokumentasjonen ivaretas. Dokumentasjonen bør gi en sammenhengende, oversiktlig og forståelig framstilling av hvordan risiko håndteres i mål- og resultatstyringen. Både medarbeidere, ledere (se kapittel 3.9) og overordnet myndighetsnivå vil ha behov for å vurdere kvaliteten i risikostyringen. En tilfredsstillende dokumentasjon er nødvendig for at dette skal være mulig. Dokumentasjonen bør tas inn i virksomhetens øvrige dokumentasjon av mål- og resultatstyring, og utformes på den måten som passer best inn i den enkelte virksomhets opplegg for dette.

Dokumentasjon av risikostyringsprosessen

Formålet med dokumentasjonen av risikostyringsprosessen er å vise:

- Hvordan risikostyringen er lagt opp og integrert i mål- og resultatstyringen.
- Hvilke vesentlige vurderinger som er foretatt, slik at det er mulig å konstatere at virksomheten har vurdert risikoer og tiltak og kontrollaktiviteter for å håndtere risikoen på alle vesentlige aktivitetsområder.
- Hvordan ledere på forskjellige nivåer har deltatt i prosessen.

Dokumentasjonen bør normalt inneholde en sammenfatning av konklusjonene som kan legges fram for overordnet organ som et ledd i styringsdialogen.

Dokumentasjon av tiltak og kontrollaktiviteter for å håndtere risikoene

Formålet med dokumentasjonen av tiltakene og kontrollaktivitetene er å:

- Gi ledere på alle nivåer oversikt over hvordan målrettet drift er forutsatt forsvarlig sikret.
- Være med å gi grunnlag for å vurdere gjenværende risiko, og behovet for ytterligere tiltak og kontrollaktiviteter.
- Spesifisere tiltak og kontrollaktiviteter som lederne på de forskjellige områdene skal sørge for at blir gjennomført og fulgt opp gjennom året.

For å dekke dette formålet vil det normalt være tilstrekkelig at det for alle vesentlige områder foreligger en kortfattet, oppdatert og oversiktlig dokumentasjon av de tiltak og kontrollaktiviteter som skal gjennomføres. Oversikten bør vise hvem som har ansvar for gjennomføringen, og når den skal skje. I den grad det ikke reduserer muligheten for oversikt, kan det være hensiktsmessig å henvise til andre og mer fylldige beskrivelser.

Ved endring eller etablering av tjenester, produkter og rutiner av vesentlig betydning bør en slik oversikt foreligge før aktiviteten igangsettes.

Dokumentasjon av oppfølging av risikoene

Formålet med å dokumentere oppfølgingen av risikoene er å sikre at ledelsen på de ulike nivåer får:

- Tilstrekkelig informasjon om den løpende gjennomføringen av risikostyringen, slik at ledelsen har rimelig trygghet for at tiltakene og kontrollaktivitetene fungerer som forutsatt.
- Tilstrekkelig informasjon om økt risiko som følge av at tiltakene og kontrollaktivitetene ikke fungerer som forutsatt, slik at etablering av ytterligere tiltak og kontrollaktiviteter kan vurderes.

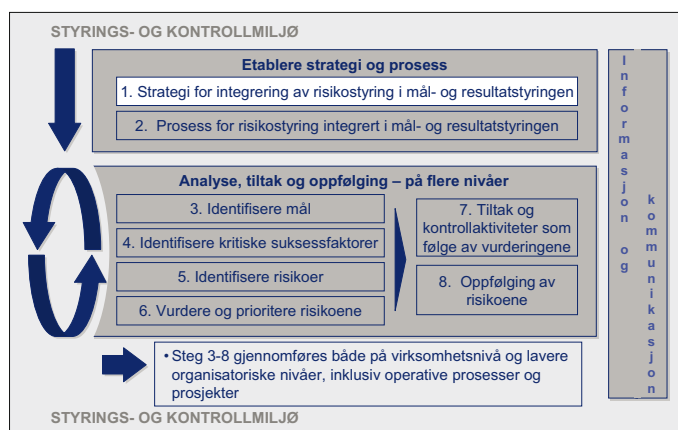
Virksomhetens ledelse skal påse at risikostyringen fungerer tilfredsstillende. Dette innebærer normalt et strukturert og dokumentert opplegg for oppfølging som omfatter ledere på alle nivåer i organisasjonen. Dette er nødvendig for å kunne gripe inn når tiltak svikter eller viser seg for svake.

3.2 Strategi for integrering av risikostyring i mål- og resultatstyringen

Ledelsen bør utarbeide en tydelig strategi som bidrar til en klar forståelse for hensikten med risikostyringen. Den bør vise hvilken verdi risikostyringen vil ha i forhold til de oppgavene virksomheten er pålagt, og hvordan risikostyringen skal integreres i mål- og resultatstyringen.

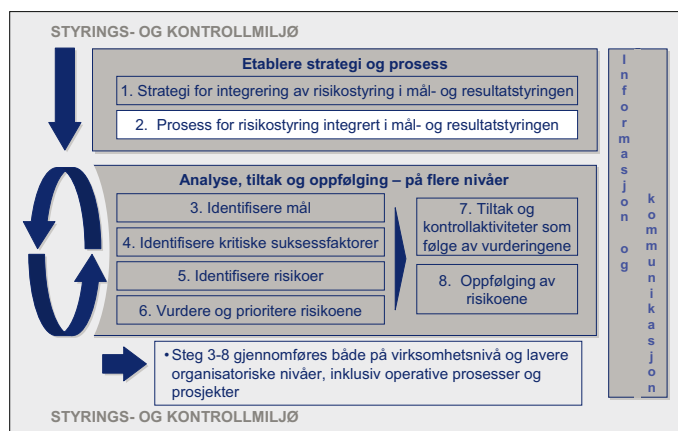
Strategien bør ta for seg følgende forhold:

- Hensikten med risikostyringen som en del av mål- og resultatstyringen.
- Ledelsens rolle i implementeringen og den løpende gjennomføringen.
- Hvordan virksomheten skal utarbeide policy for risikostyringen og hovedpunkter for innholdet i en slik policy.
- Implementeringsfaser og milepæler; hvor langt virksomheten skal komme år 1, og hvor lang tid det skal ta før risikostyringen er helt integrert med øvrig virksomhetsstyring og omfatter hele virksomheten.
- Hvilket behov ledelsen ser for endringsledelse og kompetanseutvikling i forbindelse med implementeringen.
- Hvilket behov det er for å arbeide med organisasjonskulturen knyttet til styring av risiko.
- Hvordan en tilretteleggerfunksjon (dedikert ressurs) kan utnyttes som ledelsens «forlengede arm» i det praktiske arbeidet med å integrere risikostyringen i mål- og resultatstyringen.



3.3 Prosess for risikostyring integrert i mål- og resultatstyringen

God risikostyring er integrert i virksomhetens mål- og resultatstyring. Det betyr at den er et linjeansvar, og at den utføres samtidig med andre styringsprosesser. Det bør utarbeides en oversikt over virksomhetens samlede aktiviteter og prosesser. Deretter bør det vurderes hvilke aktiviteter og prosesser som er viktigst å prioritere i implementeringsarbeidet, og hvilke som kan tas på et senere tidspunkt. På bakgrunn av denne prioriteringen bør det utarbeides en implementeringsplan.



For eksempel er det viktig at risikovurderinger gjøres samtidig med andre planleggingsprosesser. På et *overordnet nivå* er det naturlig at slike risikovurderinger utføres som en del av strategi- og planleggingsprosesser. Se kapittel 3.4 om prosess for risikostyring på overordnet nivå. På *lavere organisasjonsnivåer* er det naturlig at vurderingene gjennomføres i forbindelse med utarbeidelse av virksomhetsplaner og lignende. Se kapittel 3.5 om prosess for utarbeidelse av risikokart på lavere nivåer.

Den overordnede samlede risikoanalysen bør gjennomføres før det foretas risikoanalyser innenfor de enkelte virksomhetsområdene («top-down» tilnærming). For større virksomheter kan det likevel være nyttig at det gjennomføres overordnede risikoanalyser innenfor hvert virksomhetsområde før en samlet risikovurdering for den totale virksomheten gjennomføres. Det bør skapes en sammenheng mellom risikovurderinger på et overordnet nivå og lavere nivåer.

Generelt bør risikovurderinger gjøres på det tidspunkt og på den arena der merverdien vil være størst for virksomhetens styring. For eksempel vil en virksomhet kunne ha stor nytte av å gjøre en risikovurdering som:

- Tar utgangspunkt i foreløpige styringssignaler fra overordnet organ – og som samtidig kan gi grunnlag for innspill til de endelige styringssignalene.
- Skaper grunnlag for å gi foreløpige styringssignaler til underordnet nivå.

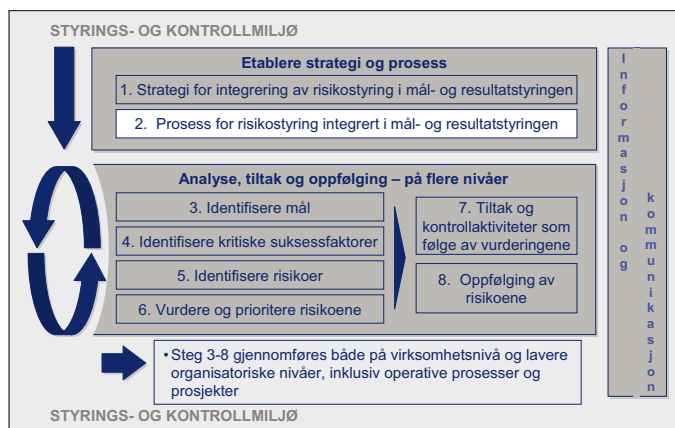
En annen og mer indirekte nytteverdi kan dessuten være at den strukturerte risikovurderingen i noen grad erstatter en ustrukturert og/eller ubevisst risikovurdering som likevel ville funnet sted – noe som bidrar til mer effektiv ressursbruk.

På mer operative nivåer vil det være naturlig at det gjennomføres risikovurderinger og iverksettes ulike kontrolltiltak i forbindelse med utforming av *operative prosesser*. Slike vurderinger bør utføres periodisk og når det skjer vesentlige endringer i mål, organisasjon eller eksterne forhold. Se kapittel 3.6 om risikoanalyse av operative prosesser.

Risikostyring er også svært relevant i *prosjekter* som en virksomhet gjennomfører. Dette gjelder spesielt i prosjekter med betydelig omfang eller usikkerhet. Se kapittel 3.7 om risikoanalyse av prosjekter. I kapittel 3.8 omhandles tiltak som følge av vurderingene og i kapittel 3.9 oppfølging av risikoene. Kapittel 3.10 omhandler risikostyringens begrensninger.

3.4 Prosess for risikostyring på overordnet nivå

Formålet med en overordnet risikovurdering av virksomheten er å etablere en omforent beskrivelse av virksomhetens risikoer som virkemiddel for bedre prioriteringer, og dermed gi høyere måloppnåelse. For å oppnå dette må virksomheten etablere en prosess som sikrer at alle viktige risikoer på dette nivået identifiseres og vurderes i forhold til den påvirkning de kan ha på virksomhetens måloppnåelse.



Prosesen bør involvere ledere som påvirker valg av mål og strategi, og som har et overordnet ansvar for måloppnåelse. Det betyr som regel at flere ledere involveres i en slik vurdering. Det er flere elementer som må være på plass når risikovurderingen gjennomføres. Tydelige mål og kritiske suksessfaktorer må være identifisert, og lederne må ha tilstrekkelig kunnskap om hvordan disse faktorene håndteres.

I en prosess for strukturert risikostyring vil det være behov for at ledelsen jevnlig diskuterer risiko. Frekvensen kan variere, men den bør neppe være sjeldnere enn i sammenheng med årlige strategier og prioriteringer. I tillegg bør den løpende oppfølgingen av virksomheten inkludere vurderinger av om risikoene håndteres som forutsatt.

I tillegg til den strukturerte prosessen for overordnet risikostyring, foregår det normalt formelle og uformelle risikovurderinger i ledermøter. Sakslisten i ledergruppemøtene inneholder ofte saker som

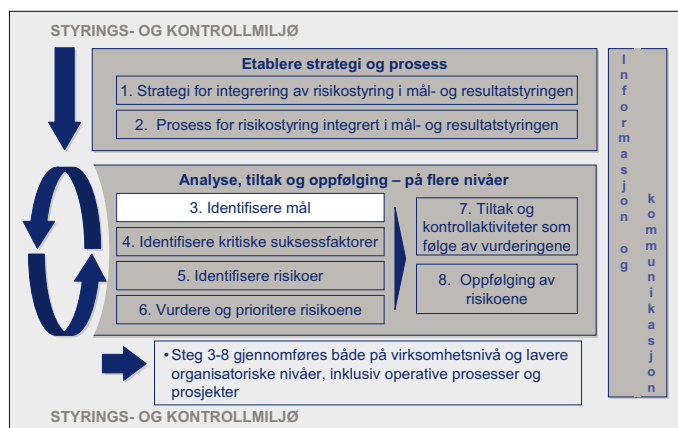
gjelder arbeidet med å nå virksomhetens mål. Det kan være saker om iverksettelse av nye tiltak på noen områder, betydelige problemer eller utfordringer som oppstår på andre områder osv. Alle slike saker har med vurdering og håndtering av risiko å gjøre. Når ledergruppen behandler slike saker, skjer det som oftest i form av diskusjoner og beslutninger om hva som skal gjøres med sakene. Det er viktig at ledere i slike drøftinger bevisst behandler risikoproblematikk. Dette gir trygghet for at det over tid etableres felles holdninger til virksomhetens risikotoleranse. Ledernes håndtering av overordnede risikoer utenom tidspunktene for strukturerte prosesser, bør også inkluderes i virksomhetens beskrivelse av hvordan risikoer skal behandles.

I kapittel 3.4.1 – 3.4.4 beskrives trinnvis stegene (3-6 i figur) i en strukturert prosess fram mot å etablere et overordnet risikokart for virksomheten.

3.4.1 Identifisering av virksomhetens overordnede mål

For å kunne evaluere risikoer knyttet til måloppnåelse, er det en forutsetning at virksomheten har etablert klare mål. Det er viktig å identifisere alle målene virksomheten styrer mot, uavhengig av om de er fastsatt i målbare størrelser, verbalt formulert eller en kombinasjon av disse. Denne prosessen kan bidra til å konkretisere målene og dermed gi grunnlag for å forbedre kvaliteten i mål- og resultatstyringen.

De overordnede målene bør systematiseres, og vurderes med hensyn til om de er de riktige målene og om de er klart og tydelig formulert. Dette er et arbeid som virksomhetens ledelse må gjennomføre. Normalt etableres og formuleres mål i forbindelse med strategi- og planleggingsprosesser. Uansett må målene være klarlagt før risiko kan identifiseres og vurderes.



Virksomhetens målsettinger vil normalt knytte seg til følgende hovedgrupper:

- Mål og resultatkrav.
- Pålitelig regnskapsrapportering og økonomiforvaltning.
- Overholdelse av lover og regler.

Gjennomgangseksempel - utgangspunkt overordnet mål

I de følgende kapitlene blir metodikken illustrert ved hjelp av et gjennomgående eksempel som tar utgangspunkt i ett av de overordnede målene for virksomheten i eksempelet:

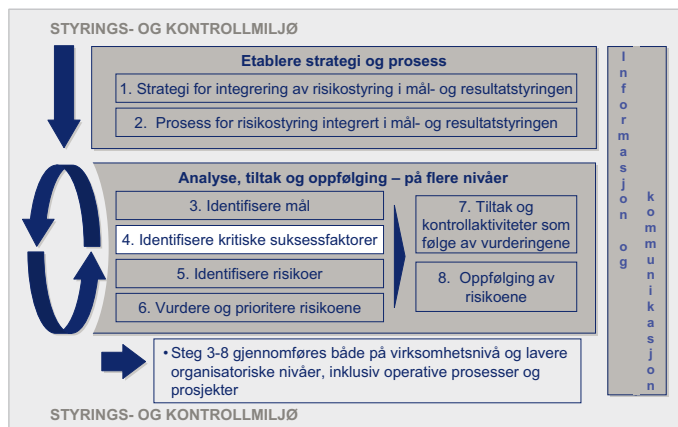
Vi skal oppnå høy brukertilfredshet hos brukerne av våre forvaltningstjenester.

Kommentarer til bakgrunnen for målfastsettelsen:

Virksomheter som leverer forvaltningstjenester til brukere, kan oppleve at brukeren er misfornøyd med rekkevidden av den lovfestede rettigheten. Eksempelet omhandler kun virksomhetens forvaltning av den lovfestede rettigheten. Brukertilfredsheten er derfor utelukkende knyttet til forvaltningsorganets håndtering av de lovfestede rettighetene og ikke om brukere opplever mangler ved selve rettigheten.

3.4.2 Identifisering av kritiske suksessfaktorer

Etter at virksomhetens overordnede mål er kartlagt og systematisert, bør de forhold som det er viktigst å lykkes med for å nå målene, kartlegges. Slike viktige forhold benevnes i mange sammenhenger som *kritiske suksessfaktorer*, og kjennetegnes av at det kan hindre oppnåelsen av ett eller flere mål dersom man ikke lykkes med dem. Når høy brukertilfredshet er et overordnet mål, vil for eksempel rask og riktig saksbehandling bidra til brukertilfredshet. Bevisste og godt formulerte kritiske suksessfaktorer tar også hensyn til de muligheter virksomheten har for å forbedre sine prestasjoner. En godt gjennomført risikostyring vil være sterkt knyttet til forhold som er viktige for at virksomheten skal lykkes. Dermed vil den i alle sine faser fange opp både de muligheter virksomheten har og de risikoer som begrenser dens evne til å utnytte disse mulighetene.



De kritiske suksessfaktorene som knytter seg til overordnede mål, bør identifiseres og systematiseres slik at de knyttes opp mot de mål de bidrar til å oppfylle. Dette er en del av den overordnede styringen av virksomheten. Virksomhetens leder og lederne av de ulike virksomhetsområdene må derfor involvere seg i arbeidet med å identifisere og systematisere de kritiske suksessfaktorene.

På et overordnet nivå er det viktig å ikke være for detaljert når kritiske suksessfaktorer beskrives. Dette vil kunne føre til at vesentlige forhold blir borte i operasjonelle detaljer. Mer detaljert beskrivelse vil gjøres i den eller de delen(e) av organisasjonen hvor den praktiske utøvelsen av aktiviteten finner sted.

Mål- og resultatstyringen inkluderer styringsparametere for blant annet å kunne måle resultatoppnåelse. Med utgangspunkt i de etablerte målsettinger, kan ledelsen identifisere slike målekriterier for resultater, med fokus på kritiske suksessfaktorer. Foruten å være resultatindikatorer, kan styringsparametrene også brukes til å vise framdriften og statusen i de forhold som er kartlagt som kritiske for å lykkes med måloppnåelsen.

Gjennomgangseksempel – kritiske suksessfaktorer

Virksomheten har vurdert hvilke forhold det er særlig viktig å lykkes med for å kunne oppnå det overordnede målet om høy brukertilfredshet. Disse forholdene har virksomheten benevnt som kritiske suksessfaktorer.

Følgende kritiske suksessfaktorer er fastslått for dette målet:

- 1 God kunnskap om lovfestet rettighet blant egne saksbehandlere.
- 2 God informasjon til brukerne om deres rettigheter og praktisk fremgangsmåte for å oppnå rettighetene.
- 3 Enkle standardiserte søknadsskjema som er lett tilgjengelige for brukeren.
- 4 Riktig saksbehandling.
- 5 Rask saksbehandling.
- 6 Rask iverksettelse av vedtak.
- 7 Rask klagebehandling.

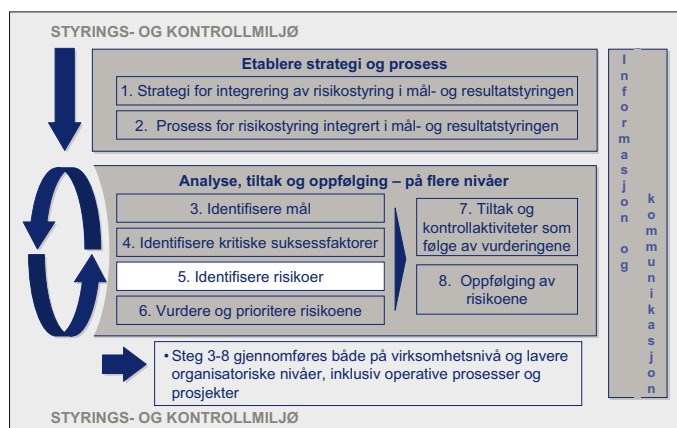
3.4.3 Identifisering av risikoer

Når virksomhetens ledelse har konkretisert klare mål og identifisert kritiske suksessfaktorer, er det skapt et godt grunnlag for identifisering av risikoer, risikovurdering og prioritering av risikoreduserende tiltak.

Når ledelsen har identifisert kritiske suksessfaktorer på et overordnet nivå, har de samtidig identifisert risikoer på samme nivå. Når de forhold som det er viktig å lykkes med er identifisert, følger det implisitt at det er viktig at man ikke mislykkes med disse forholdene. Dersom det er viktig med rask og riktig saksbehandling for å oppnå høy brukertilfredshet, kan man slutte at det motsatte vil kunne ha en negativ effekt på mulighetene til å oppfylle målet. De kritiske suksessfaktorene «riktig saksbehandling» og «rask saks-

behandling» kan derfor gjøres om til risikoer ved å formulere dem som «risiko for at det ikke er riktig saksbehandling» og «risiko for at det ikke er rask saksbehandling».

På samme måten som mål og kritiske suksessfaktorer inngår i et *målhierarki*, vil også risikoer inngå i et *risikohierarki*. Dette innebærer at risikofaktorer knyttet til den enkelte kritiske suksessfaktor kan identifiseres på mange ulike nivåer. For eksempel kan en rekke forhold påvirke muligheten for rask saksbehandling. Det kan være for liten saksbehandlerkapasitet, lite rasjonell IT-støtte eller konkrete hendelser som brudd i telefon- og datalinjer. Felles for alle disse underliggende risikoforholdene, er at de påvirker mulighetene for rask saksbehandling, og at betydningen av dem derfor må vurderes opp mot denne suksessfaktoren. Prosessen med å identifisere risikoer kan også bidra til å finne fram til kritiske suksessfaktorer som ikke tidligere er identifisert.



Tabellen nedenfor illustrerer hvordan både kritiske suksessfaktorer og risikoer kan henge sammen på ulike nivåer. Jo lengre ned i hierarkiet man kommer, jo mer blir de kritiske suksessfaktorer og tilhørende risikoer knyttet til bestemte tiltak som må være på plass for å lykkes.

Tabell 1: Eksempel på risikohierarki

«Risiko for at det ikke er rask saksbehandling»		
Nivå	Kritiske suksessfaktorer	Risiko
1	Vi må ha en rask og effektiv saksbehandling.	Risiko for at vi ikke har en rask og effektiv saksbehandling.
2	Vi må ha tilstrekkelig med saksbehandlere-ressurser.	Risiko for at vi ikke har tilstrekkelig med saksbehandlerressurser.
3	Vi må ha et lavest mulig sykefravær.	Risiko for at vi har et for høyt sykefravær.
4	Vi må ha ergonomisk tilpassede arbeidsstasjoner.	Risiko for at vi har arbeidsstasjoner som skaper belastningsskader for våre ansatte.

En kritisk suksessfaktor og risiko på et nivå henger gjerne sammen med flere kritiske suksessfaktorer og risikoer på nivået under. Illustrasjonen over viser ikke hvordan hierarkiet spres ut i pyramideform jo lavere nivå man kommer på. En slik spredning fører til at omfanget øker betydelig fra nivå til nivå.

For å kunne vurdere risikoen på et overordnet nivå, er det nødvendig at ledelsen har en oppfatning av hvordan risikoen på lavere nivåer håndteres. Når risikostyringen fullt ut er integrert i virksomhetens mål- og resultatstyring, vil ledelsen ha informasjon fra risikovurderinger på lavere nivåer i organisasjonen som grunnlag for den overordnede risikovurderingen. Denne styringsinformasjonen, både den formelle og uformelle, bør gi ledelsen det nødvendige grunnlaget for selvstendige vurderinger knyttet til overordnede risikoforhold. På bakgrunn av denne informasjonen skal lederne vurdere virksomhetens muligheter til å nå de målene som er satt eller – sagt på en annen måte – risikoen for at de ikke når målene.

Dersom ledelsen mener at den ikke har tilstrekkelig informasjon om virksomhetens prestasjoner og dermed heller ikke organisasjonens evne til å nå de fastsatte målene, må ledelsen skaffe seg slik informasjon før den overordnede risikovurderingen gjennomføres. I påvente av at risikostyringen skal implementeres i hele virksomheten, kan dette gjøres ved at det innhentes informasjon om virksomhetens nåværende evne til å lykkes med kritiske suksessfaktorer på neste nivå. Informasjonen kan inkludere status om etablerte og relevante styringsparametere, verbale beskrivelser av hvordan kritiske suksessfaktorer og risikofaktorer håndteres nå, og hvilke utfordringer som knytter seg til å nå de målene som er satt framover.

Risikoer som ikke fanges opp i framgangsmåten som er beskrevet

En god planleggingsprosess skal inkludere vurdering av både eksterne og interne forhold som virksomheten må være oppmerksom på. Slike eksterne faktorer kan for eksempel være knyttet til politiske, sosiale, teknologiske eller økonomiske forhold. Det er flere anerkjente metoder for å identifisere eksterne og interne forhold som påvirker målfastsettelse. En av disse er den såkalte SWOT-analysen (SWOT står for Strengths, Weaknesses, Opportunities, Threats). Metodene omtales ikke ytterligere i dokumentet.

Mål, kritiske suksessfaktorer og planer skal også gjenspeile de vurderinger ledelsen foretar av slike forhold. Det kan likevel være at enkelte viktige forhold ikke tydelig framgår av de målene som er satt eller ikke er identifisert i planleggingsprosessen. Risikostyringen vil kunne være et sikkerhetsnett for å fange opp slike forhold. I praksis vil dette kunne gjøres ved at det i forbindelse med risikovurderinger på alle nivåer også vurderes om det eksisterer risikoer som ikke er fanget opp ved hjelp av kartleggingen. Dette kan gjelde risikoer som knytter seg til enkelthendelser med for eksempel krise- eller katastrofelignende konsekvenser. Det er derfor viktig at ledere på alle nivåer også inkluderer slike risikoer i sine risikovurderinger.

Gjennomgangseksempel – identifisering av risikoer

Virksomheten har identifisert hvilke risikoforhold som knytter seg til de ulike kritiske suksessfaktorene som er definert. Det er foreløpig ikke vurdert om den enkelte risiko er høy eller lav, men kun konstatert at dette kan være aktuelle risikoer sett fra et overordnet nivå.

Kritisk suksessfaktor	Risiko
1. God kunnskap om lovfestet rettighet blant egne saksbehandlere.	1. Risiko for at våre saksbehandlere ikke har tilstrekkelig kunnskap om brukernes lovfestede rettigheter.
2. God informasjon til brukerne om deres rettigheter og praktisk fremgangsmåte for å oppnå rettighetene.	2. Risiko for at informasjonen til brukerne ikke er god nok når det gjelder innholdet i rettigheten og praktisk fremgangsmåte for å oppnå rettigheten.
3. Enkle standardiserte søknadsskjema som er lett tilgjengelige for brukeren.	3. Risiko for at våre søknadsskjemaer er for kompliserte og vanskelig tilgjengelig for brukeren.
4. Riktig saksbehandling.	4. Risiko for at det gjøres feil i saksbehandlingen slik at brukeren oppnår mindre eller større rettighet enn han/hun har krav på.
5. Rask saksbehandling.	5. Risiko for at vi har ineffektive prosedyrer for saksbehandling som forsinker saksbehandlingen unødige.
6. Rask iverksettelse av vedtak.	6. Risiko for at vi ikke iverksetter vedtakene tilstrekkelig raskt etter at de er fastsatt.
7. Rask klagebehandling.	7. Risiko for at vi har ineffektive prosedyrer for behandling av klager på vår saksbehandling.

Risikovurderinger knyttet til styringsparametere

Virksomhetene skal i henhold til økonomiregelverket fastsette styringsparametere som en del av mål- og resultatstyringen. Slike styringsparametere kan være både kvalitative og kvantitative. De kan være avledet av kritiske suksessfaktorer ved at de er vurdert å gi god informasjon om hvordan disse blir håndtert av virksomheten. Styringsparametere kan si noe om hvilke resultater som er oppnådd, hva som er gjort for å oppnå disse eller status på enkeltområder i virksomheten. I noen tilfeller vil det være begrensninger i informasjonsverdien til en styringsparameter ved at den alene ikke gir tilstrekkelig informasjon om hvordan kritiske forhold utvikler seg.

Dersom styringsparametere er etablert med sterk knytning til mål og eventuelt kritiske suksessfaktorer, kan risikovurderingene ta utgangspunkt i disse. Det vil si at man vurderer risikoene for ikke å nå fastsatt størrelse på måleenheten for de enkelte styringsparametere. I de tilfeller hvor styringsparametere ikke har tilstrekkelig sammenheng med målene, eller disse ikke dekker hele virksomheten, vil en slik framgangsmåte ikke være god nok. Risikoen knyttet til virksomhetens måloppnåelse vil da ikke bli tilstrekkelig kartlagt og vurdert, og formålet med risikostyringen vil ikke kunne oppnås.

3.4.4 Vurdering og prioritering av risikoer

Risikovurderingene må knyttes direkte opp mot de mål og kritiske suksessfaktorer som er etablert. Vurdering av om en risiko er høy eller lav må alltid gjøres i forhold til det målet den truer oppfyllelsen av. Dersom en slik tilknytning ikke etableres, kan risikovurderingen bli vilkårlig.

Oversikten over virksomhetens risikoer på et overordnet nivå og ledelsens bevissthet om hvordan disse håndteres i organisasjonen, danner viktige utgangspunkt for å utarbeide et såkalt risikokart på et overordnet nivå.

I risikokartet angis graden av sannsynlighet for at den aktuelle risikoen inntreffer i den aktuelle perioden. Man angir dessuten den forventede konsekvensen risikoen medfører dersom den inntreffer. Det tas hensyn til dagens etablerte tiltak i vurderingen.

Resultatet av vurderingen gir et bilde av sannsynligheten for at det aktuelle målet ikke nås, og hvor alvorlig dette avviker fra målet forventes å bli hvis ikke ytterligere tiltak iverksettes. Dette resultatet vil ha sin naturlige plass i styringsdialogen og må derfor koordineres med denne.

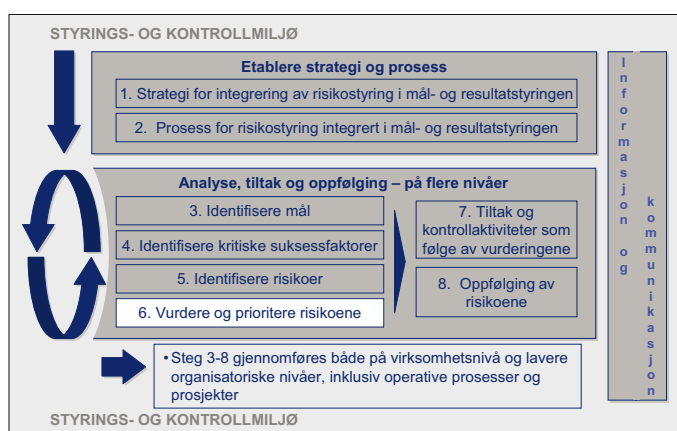
Utarbeidelse av risikokart bør gjøres samtidig med vesentlige planleggings- og strategiprosesser. Slike vurderinger underveis i disse prosessene kan øke bevisstheten omkring ulike konsekvenser av de strategiske valgene som gjøres.

3.4.4.1 Nærmere om vurdering av sannsynlighet og konsekvens

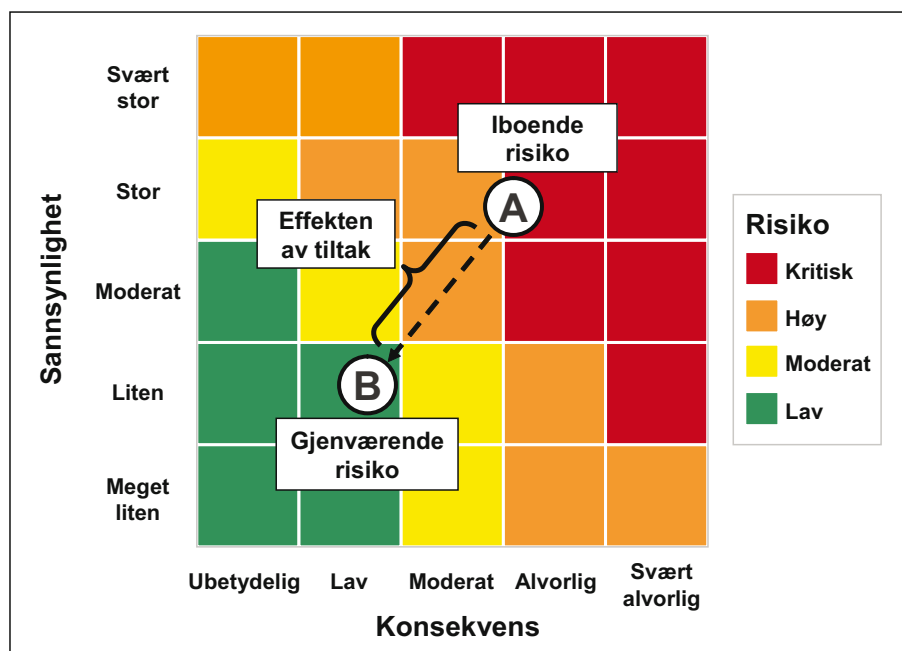
Det er en anerkjent metode å gradere risiko ved hjelp av en kombinasjon av sannsynligheten for at risikoen inntreffer og konsekvensen av at den inntreffer. Mange kan oppleve det som noe unaturlig å skulle splitte sine vurderinger på denne måten. I det daglige er vi mest vant til å konkludere direkte om et forhold har høy eller lav risiko. Fallskjermhopping vurderer noen å være for risikabelt fordi konsekvensen vil kunne være katastrofal hvis skjermen ikke åpner seg. Andre vurderer det som lite risikabelt fordi sannsynligheten for at ting skal gå feil er svært liten når alle sikkerhetsprosedyrer følges. I tillegg kan man ha ulik aksept for å ta risiko. Dette er i kapittel 2 omtalt som risikotoleranse.

Iboende og gjenværende risiko

Hvor høy en risiko er, kan vurderes uten at en tar hensyn til de ulike tiltakene og kontrollaktivitetene som er etablert for å redusere den. Dette kan for eksempel være å vurdere risikoen for at virksomheten ikke er i stand til å tiltrekke seg nødvendig ny kompetanse, uten å ta hensyn til alle de tiltak og kontrollaktiviteter som er iverksatt for å få dette til. Denne risikoen kan benevnes som *iboende risiko*. Alternativt kan en ta hensyn til de tiltakene og kontrollaktivitetene som er iverksatt når man vurderer risiko. En slik risiko kan benevnes som *gjenværende risiko*.



Figur 3: Risikokart som viser iboende og gjenværende risiko



Figur 3 illustrerer et risikokart for risikoen for ikke å tiltrekke seg nødvendig kompetanse, hvor A representerer iboende risiko og B gjenværende risiko etter å ha tatt hensyn til effekten av alle tiltak og kontrollaktiviteter som er iverksatt.

Fordelen med å vurdere gjenværende risiko på et overordnet nivå, er at ledelsen får informasjon om risiko gitt de tiltakene og kontrollaktivitetene som allerede er iverksatt. Dette samsvarer med det som ledergrupper normalt forholder seg til når de diskuterer og vurderer om det skal foretas endringer i noen deler av virksomheten. Et risikokart basert på en vurdering av gjenværende risiko utgjør derfor et viktig beslutningsgrunnlag når ledelsen skal vurdere videre håndtering av risikoen.

En sentral utfordring er å vurdere risiko med utgangspunkt i hvordan tiltak og kontrollaktiviteter faktisk etterleves og virker – og ikke med utgangspunkt i hvordan de er ment å virke eller ideelt sett skulle ha virket. Se nærmere om hvordan ledere kan skaffe seg informasjon om hvordan tiltak og kontrollaktiviteter etterleves og virker i kapittel 3.9 oppfølging av risikoer.

I det følgende utdypes sannsynlighet og konsekvens i et gjenværende risikoperspektiv. Det vil si der en vurderer risikoen når en har tatt hensyn til effekten av tiltak og kontrollaktiviteter som er iverksatt (ikke iboende risiko).

Vurdering av sannsynlighet

Når gjenværende risiko skal plasseres langs sannsynlighetsaksen i et risikokart, gjøres en vurdering av hvor sannsynlig det er at risikoen inntreffer når man tar hensyn til de tiltakene og kontrollaktivitetene som er iverksatt for å redusere sannsynligheten.

Det betyr at ledelsen når den vurderer sannsynligheten for at risikoen for ikke å tiltrekke seg nødvendig kompetanse inntreffer, tar hensyn til alle de tiltak og kontrollaktiviteter som er iverksatt for å redusere nettopp denne sannsynligheten. Dette kan være alt fra annonsering i riktige medier, profilering av virksomheten mot miljøer der interessant kompetanse befinner seg til lønnsbetingelser. Vurderingen av (gjenværende) sannsynlighet vil da synliggjøre hvor gode ledelsen vurderer disse tiltakene og kontrollaktivitetene til å være når det gjelder å tiltrekke nødvendig ny kompetanse.

Vurdering av konsekvens med bruk av konsekvensskala

Når gjenværende risiko skal plasseres langs konsekvensaksen i risikokartet, gjøres en vurdering av hvor alvorlig konsekvensen forventes å bli hvis risikoen inntreffer. I vurderingen tar man hensyn til de tiltakene og kontrollaktivitetene som er iverksatt for å redusere konsekvensen av at risikoen inntreffer.

Med konsekvens menes hvilke følger risikoen kan få i forhold til de mål virksomheten har satt seg hvis den inntreffer. Ledelsen kan også ha etablert konkrete tiltak og kontrollaktiviteter med det formål å redusere konsekvensene av en risikofaktor. For eksempel vil konsekvensen av å ikke tiltrekke seg nødvendig kompetanse kunne være redusert på ulike måter. Det kan være ved at det er inngått avtale om innleie av riktig kompetanse når virksomheten selv mangler den, og/ eller ved at eksisterende arbeidskraft har fått opplæring/studier osv.

En konsekvensskala kan inndeles i *ubetydelig*, *liten*, *moderat*, *alvorlig* og *svært alvorlig konsekvens*. Graderinger av konsekvensen av en risiko vil inneholde større eller mindre grad av skjønn fra de ledere som foretar graderingene. En bør unngå at to personer med samme oppfatning av hvilken konsekvens et forhold kan få, klassifiserer den ulikt. Dersom to ledere mener at høyere sykefravær kan føre til at ventetiden for behandling av saker øker til tre måneder, må begge klassifisere dette med samme grad av konsekvens. Det bør med utgangspunkt i risikotoleransen etableres en felles konsekvensskala som er akseptert av virksomhetslederen. Det innebærer at det beskrives hvilke konsekvenser av risikoer som betraktes å være i de ulike kategoriene. Dette vil redusere mulighetene for at den ene lederen i eksempelet klassifiserer tre måneders ventetid som en lav konsekvens og den andre klassifiserer dette som en alvorlig konsekvens.

Fordi risikoene skal vurderes opp mot virksomhetens mål og den betydningen de har for virksomhetens muligheter til å kunne nå målene, er det naturlig at en konsekvensskala beskriver ulike konsekvenser av å ikke nå det målet som er fastsatt. Dersom målet for ventetid er satt til to uker, så bør konsekvensskalaen beskrive hvilke konsekvenser som er å betrakte som ubetydelige, lave, moderate, alvorlige og svært alvorlige for dette målet. Det kan for eksempel være at ledelsen vurderer at en ubetydelig konsekvens av risikoen for sykefravær er at ventetiden øker til 2,5 uker, en lav konsekvens er økning til tre uker, en moderat konsekvens er fire uker osv. Slik bør en konsekvensskala bygges opp, og inkludere alle virksomhetens overordnede mål.

Når det i virksomhetsstyringen er etablert styringsparametere for å følge opp virksomhetens resultatoppnåelse, kan det etableres grenser for når styringsparametere på et gitt tidspunkt skal klassifiseres som for eksempel grønn, gul eller rød for å markere avstand fra fastsatte mål. Når det etableres en konsekvensskala, bør den samsvare med de vurderingene som er lagt til grunn ved etableringen av eventuelle grenser for styringsparametrene.

Gjennomgangseksempel – konsekvensskala

I forbindelse med at ledelsen fastsatte målet om å oppnå høy brukertilfredshet, fastsatte ledelsen også med utgangspunkt i sin risikotoleranse kriterier for hvor alvorlig den vil betrakte eventuelle avvik fra dette målet. På denne måten har ledelsen lagt rammen for at organisasjonen kan gjennomføre risikovurderinger basert på de samme konsekvenskriterier.

Ledelsen har fastsatt følgende kriterier for hvordan den vil betrakte eventuelle avvik fra målet om høy brukertilfredshet. Kriteriene knytter seg til klager i forbindelse med forvaltningen av brukerrettigheten og ikke til klager på selve innholdet i rettigheten:

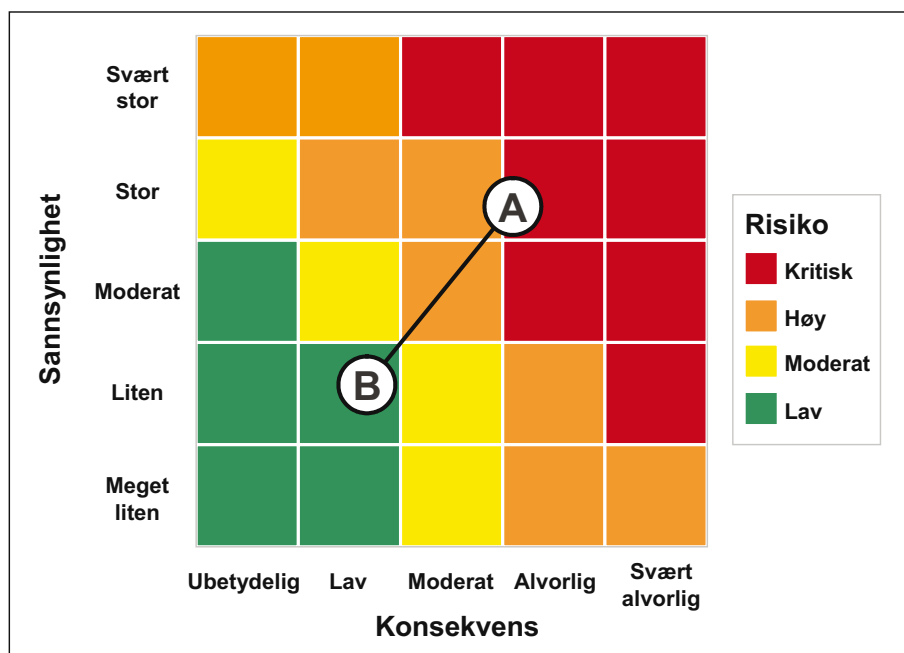
Ubetydelig konsekvens	Liten konsekvens	Moderat konsekvens	Alvorlig konsekvens	Svært alvorlig konsekvens
Noen få enkelttilfeller av brukerklager.	Færre enn 5 % av brukerne klager på virksomhetens forvaltning av brukerrettigheten.	Mellom 5 % og 10 % av brukerne klager på virksomhetens forvaltning av brukerrettigheten.	Mellom 10 % og 25 % av brukerne klager på virksomhetens forvaltning av brukerrettigheten.	Mer enn 25 % av brukerne klager på virksomhetens forvaltning av brukerrettigheten.

3.4.4.2 Vurdering og prioritering av risikoene på overordnet nivå

Risikokartets nære tilknytning til de vurderinger og beslutninger som ligger til grunn for strategier og prioriteringer, fører til at de samme lederne som er involvert i vurdering og beslutning av strategier og prioriteringer, bør delta i utarbeidelsen av risikokartet.

En vedtatt strategiplan bør alltid inneholde en beskrivelse som viser hvilken risiko virksomhetsledelsen mener det er forbundet med de overordnede strategiske målene, og hvordan risikoen skal håndteres i de valgte strategier for å nå målene. Risikovurderingene bør derfor legges til grunn samme tidsperspektiv som selve planleggingsdokumentet. Beskrivelsen kan for eksempel gis i form av et risikokart.

Figur 4: Risikokart i forbindelse med valgt strategi for å nå et mål



Figur 4 illustrerer et risikokart hvor A representerer risikoen ved en valgt strategi for å nå et mål. Punkt B illustrerer hvor risikoen antas å flytte seg dersom strategien også inneholder tiltak som er illustrert ved streken mellom A og B. Slike tiltak kan for eksempel være knyttet til kompetanseutvikling, teknologiutvikling, forenkling, økt ressursbruk, bedre måling og oppfølging osv.

Virksomhetens ledelse har ansvar for å velge prosess for integrering av risikostyring i mål- og resultatstyringen (jf. kapittel 3.3), og dessuten bestemme hvem som skal involveres i den overordnede risikovurderingen. Vurdering og prioritering av risikoer på overordnet nivå kan gjøres på ulike måter, for eksempel:

- Vurderinger hvor alle i ledergruppen deltar.
- Vurderinger foretatt av den eller de lederne som i praksis håndterer risikoen på de ulike områder i virksomheten.
- Virksomhetslederens vurdering som bygger på innspill fra dem som er nevnt i punktene ovenfor.

Virksomhetslederen har det endelige ansvaret overfor overordnet myndighet. Virksomhetslederen kan derfor overprøve vurderingen på bakgrunn av sin egen innsikt og sitt eget skjønn uavhengig av hvem som har gitt innspill til vurderingen. Dersom virksomhetslederens vurderinger avviker vesentlig fra øvrige lederes vurderinger, bør dette begrunnes av virksomhetslederen.

Gjennomgangseksempel – vurdering og prioritering av risikoene

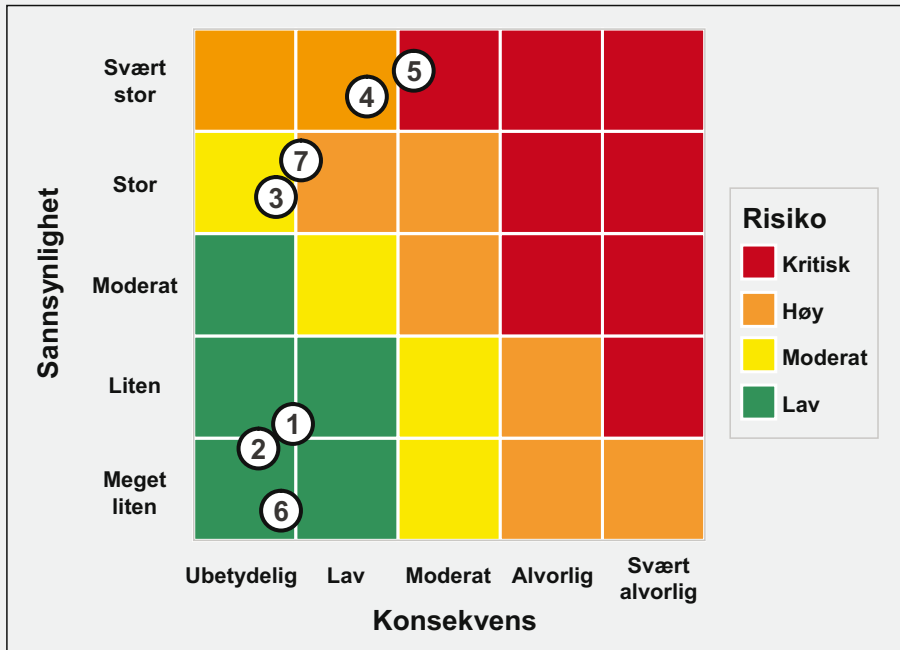
Virksomheten har vurdert i hvilken grad den er eksponert for de risikoene som er identifisert knyttet til å kunne oppnå høy brukertilfredshet. Den har lagt til grunn den fastsatte risikotoleransen ved vurderingen av de enkelte risikoene.

Ledelsen har basert seg på følgende informasjon om risikoene i sin risikovurdering:

Risiko	Beskrivelse av nåsituasjonen
1. Risiko for at våre saksbehandlere ikke har tilstrekkelig kunnskap om brukernes lovfestede rettigheter.	Alle våre saksbehandlere har gjennomført opplæring i den nye loven og forskriften. Vi har arrangert web-eksamen hvor alle har bestått. Vi har litt problemer med raskt å gi nyansatte innføring i regelverket, før de settes til saksbehandling.
2. Risiko for at informasjonen til brukerne ikke er god nok når det gjelder innholdet i rettigheten og praktisk framgangsmåte for å oppnå rettigheten.	Vi har laget en kort og konsis beskrivelse av rettigheten, hvilke kriterier som skal være oppfylt for å kunne oppnå den, samt praktiske anvisninger om hvordan bruker skal gå fram for å fremme krav om rettigheten.
3. Risiko for at våre søknadsskjemaer er for kompliserte og vanskelig tilgjengelig for brukeren.	Søknadsskjemaene kan lastes ned fra vår internettside eller fås tilsendt ved telefonhenvendelse. Vi mottar en del spørsmål knyttet til utfylling av skjemaene. Dette gjelder særlig punkt C og E i skjemaet. Vi vil vurdere å gjøre noe med dette.
4. Risiko for at det gjøres feil i saksbehandlingen slik at brukeren oppnår mindre eller større rettighet enn han/hun har krav på.	Vi opplever at om lag halvparten av klagen på vår saksbehandling tas til følge. Dette er en for stor andel, og viser at vi må analysere hva som er årsaken til dette.
5. Risiko for at vi har ineffektive prosedyrer for saksbehandling som forsinker saksbehandlingen unødig.	Vi har i perioder en betydelig andel ikke ferdigbehandlede saker. Dette gjelder både ikke påbegynte saker, og påbegynte ikke ferdigbehandlede saker. Vi mener at dette først og fremst skyldes: <ul style="list-style-type: none">• Vi skiller ikke på saker som er «tunge» eller «lette».• Vi har skjev arbeidsbelastning blant saksbehandlerne.• Vi bruker mye tid på å kontakte brukere som har gitt mangelfull informasjon i søknadene.• Vi har et høyt sykefravær blant saksbehandlerne som igjen forsinker saksbehandlingen.
6. Risiko for at vi ikke iverksetter vedtakene tilstrekkelig raskt etter at de er fastsatt.	Det går gjennomsnittlig to arbeidsdager mellom vedtak og iverksettelse av vedtak. Vi har gode prosedyrer på dette og har holdt dette måltallet over lang tid.
7. Risiko for at vi har ineffektive prosedyrer for behandling av klager på vår saksbehandling.	I perioder blir klagen liggende relativt lenge før de er ferdigbehandlet. Dette skyldes at vi har ressursproblemer i perioder grunnet blant annet høyt sykefravær. Vi vil vurdere nærmere hva som skal gjøres med dette.

Gjennomgangseksempel forts.

På bakgrunnen av informasjonen overfor har ledelsen vurdert risikoene og plassert disse i et risikokart (numrene henviser til risikoene slik de er beskrevet på forrige side):



3.5 Prosess for utarbeidelse av risikokart på lavere organisasjonsnivåer

I tillegg til et risikokart for det samlede virksomhetsområdet, bør det på samme måte utarbeides risikoanalyser og risikokart for alle vesentlige deler av virksomhetsområdet.

Lederne av de enkelte virksomhetsområdene bør benytte den samme framgangsmåten som er beskrevet for overordnet nivå. Det betyr at risikovurderingen tar utgangspunkt i målsettingene for området, de forholdene det er viktigst å lykkes med (kritiske suksessfaktorer), ledelsens oppfatning av en konsekvensskala og de viktigste risikofaktorene som knytter seg til måloppnåelsen.



Lederen av virksomhetsområdet bør involvere sine ledere i å utarbeide risikokartet. Kartet bør utarbeides i forbindelse med utarbeidelsen av virksomhetsplaner og brukes som et aktivt verktøy i en slik prosess. Risikokartet slik det vurderes på bakgrunn av vedtatt virksomhetsplan, bør inngå som en del av denne planen.

Risikokart for virksomhetsområder bør utarbeides første gang i forbindelse med planleggingsaktiviteter for området. Dersom slike prosesser ikke er planlagt innenfor en tidsramme som er nødvendig for å ha forventet framdrift i implementeringen av risikostyringen, bør ledelsen av virksomhetsområdet prioritere dette arbeidet og ikke vente til neste planleggingsprosess.

Risikovurderingene på lavere organisasjonsnivåer vil også knyttes mot mål som inngår i de tidligere nevnte hovedgruppene for målsettinger:

- Mål og resultatkrav.
- Pålitelig regnskapsrapportering og økonomiforvaltning.
- Overholdelse av lover og regler.

3.6 Risikoanalyse av operative prosesser

De enkelte virksomhetsområdene vil også inkludere en rekke operative prosesser. Med operative prosesser menes løpende aktiviteter som er knyttet til kjernevirksomheten i forvaltningsorganet. Operative prosesser kan for eksempel være mottak av henvendelser til virksomheten, beregning og utbetaling av lønn, beregning og utbetaling av ytelser til brukere, drift av IT-systemer osv. Slike prosesser kan en litt enkelt beskrive som «skulle bare mangle at de fungerer». Med dette menes at en virksomhetsledelse og omverdenen ofte vil forvente at det er etablert tilstrekkelig kontroll med slike prosesser.



Imidlertid vil også en operativ prosess være utsatt for risikoer i forhold til å nå målsettingen ved prosessen. Risikoene kan påvirkes av beslutninger som tas på et overordnet nivå, for eksempel kutt i ressursene eller nye/utvidede oppgaver. I tillegg vil de operative prosessene inneholde risikoer som knytter seg til de ulike aktivitetene som inngår i den enkelte prosess. Dette kan blant annet vedrøre risikoen for at det gjøres operasjonelle feil eller at IT-systemene ikke støtter prosessen slik som forutsatt. Slike risikoer kan føre til at det oppstår svikt og feil i de daglige prosessene i virksomheten, som igjen kan ha små eller store konsekvenser. En god risikostyring tilsier at virksomheten har tilfredsstillende kontroll også med slike risikoer.

Det bør derfor gjennomføres risikovurderinger av alle vesentlige operative prosesser som virksomheten utfører. Virksomhetens ledelse bør beslutte hvilke operative prosesser som er å betrakte som vesentlige. Dersom det ikke allerede er gjennomført og dokumentert slike risikovurderinger, bør det utarbeides en plan for dette arbeidet som en del av implementeringen av strukturert risikostyring i virksomheten. Den som er ansvarlig for prosessen, har også ansvaret for å gjennomføre vurderingene.

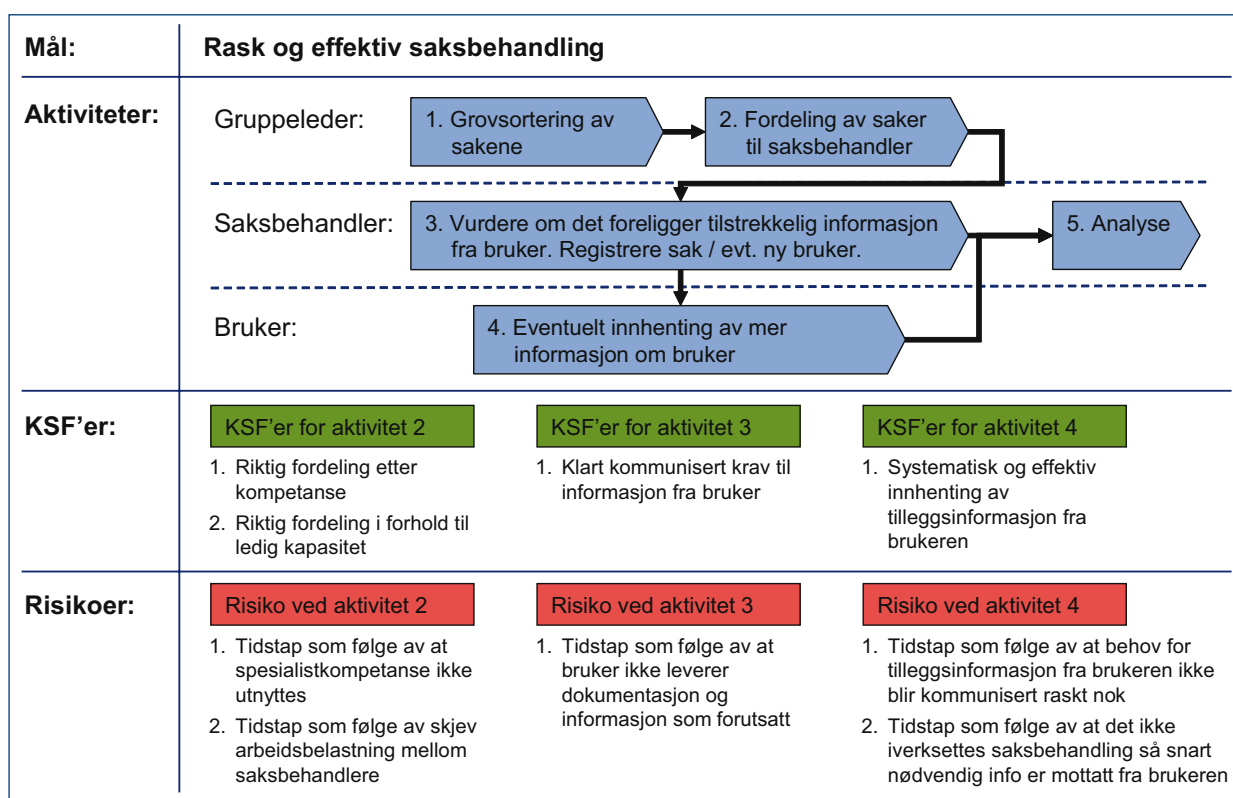
Det er en viktig forutsetning for å kunne gjøre gode risikoanalyser at det foreligger en god oversikt over de aktuelle prosessene. I det inngår oversikt over og forståelse for:

- Hvilke mål som er satt for prosessen.
- Hvilke aktiviteter som inngår i prosessen og hvem som er involvert i den.

- Hvilke kritiske suksessfaktorer det er i prosessen (i forhold til målene med den).
- Hvilke risikoer som påvirker mulighetene for å lykkes.

Kunnskap om slike forhold vil være avgjørende for å sikre en god risikovurdering av prosesser. Figuren nedenfor illustrerer et utsnitt av hvordan en prosess kan kartlegges og risikoer identifiseres før det gjøres en vurdering av hvilke risikoer som må reduseres. Det er mange måter å kartlegge prosesser på, og figuren er således kun et eksempel. Figuren viser i tillegg hvordan også prosesskartleggingen knyttes opp mot mål, kritiske suksessfaktorer (KSF'er) og risikoer.

Figur 5: Eksempel på prosesskartlegging



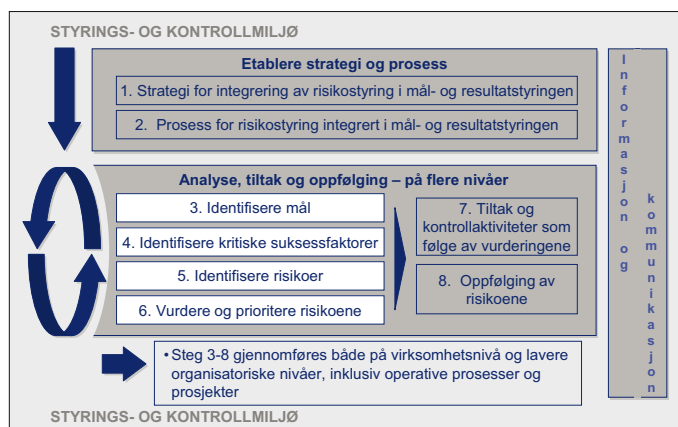
Videre må de ansvarlige for prosessen også i samråd med sine ledere fastsette konsekvenskala eller kvalitetsmål for prosessen. Dette kan for eksempel være saksbehandlingstid, hvor lenge en IT-applikasjon kan være ute av funksjon, eller verbale formuleringer der tallmål ikke er praktisk anvendelige. Slike konsekvensskalaer må ikke gå utover den konsekvenskalaen som virksomhetens ledelse har vedtatt for risikovurderinger på et overordnet nivå, men representere den samme holdning til hvor alvorlig ulike grader av avvik fra målene er.

Analysene bør oppdateres når det oppstår hendelser som kan antas å endre den tidligere risikovurderingen. Slike hendelser kan være endringer i bemanning, tap av nøkkelkompetanse, mindre ressurser tilgjengelig, endringer i IT-systemer osv. Risikovurderingen bør også oppdateres når det er implementert tiltak som forventes å skulle redusere risikoen i en eller flere prosesser til et akseptabelt nivå. Oppdateringen bør finne sted på det tidspunkt disse tiltakene forventes å ha hatt effekt. For spesielt kritiske eller risikoutsatte prosesser bør det vurderes å gjennomføre periodiske oppdateringer uten at det foreligger spesielle hendelser. For områder hvor det er lovpålagt med risikovurderinger, må det sikres at risikovurderingene på disse områdene gjennomføres i samsvar med lovens krav.

3.7 Risikoanalyse av prosjekter

De fleste virksomheter benytter prosjekter som en del av sin styring. De kan variere mellom store, langvarige og komplekse prosjekter til små, kortvarige og mindre komplekse. Behovet for styring og kontroll kan derfor variere fra prosjekt til prosjekt. Prinsippene for risikostyring må innarbeides i de prosjektene som virksomheten gjennomfører. Normalt vil målene for et prosjekt være en leveranse med følgende mål:

- Riktig kvalitet.
- Til riktig tid.
- Med riktig prosjektkostnad.

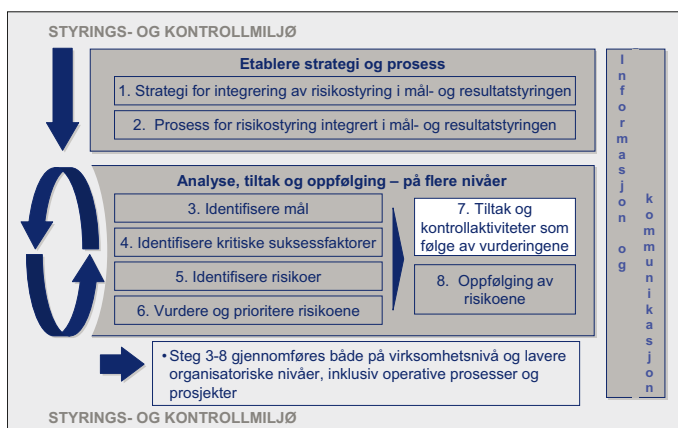


I tillegg vil også overføring av resultatet av prosjektet til linjeorganisasjonen ofte representere et kritisk punkt for å lykkes med et prosjekt.

På samme måte som beskrevet tidligere i dokumentet vil det også knytte seg kritiske suksessfaktorer og risikoer til disse prosjektmålene. I prosjekter vil det vanligvis være behov for hyppigere kartlegging, vurdering og prioritering av risikoer enn hva som er tilfelle for en løpende operativ aktivitet. Virksomhetene bør derfor innarbeide prosedyrer for hvordan risikostyring skal inngå i den prosjektstyringsmetodikken som benyttes.

3.8 Tiltak og kontrollaktiviteter som følge av vurderingene

Prioriteringen av risikoene øker bevisstheten om hvilke tiltak som fungerer for dårlig og hvilke nye tiltak som eventuelt er nødvendige for å redusere risikoen til et akseptabelt nivå. Det er viktig å være klar over at tiltak i denne sammenheng inkluderer alle forhold som bidrar til å redusere risikoer. Dette kan være alt fra utvikling av en sunn og god organisasjons- og ledelseskultur til implementering av helt konkrete kontrollaktiviteter.



Risikovurderinger vil, uavhengig av hvilket nivå de er gjennomført på eller om de er knyttet til et prosjekt eller en operativ prosess, lede til ulike typer beslutninger om hvordan risikoen bør håndteres. Skillet mellom sannsynlighet og konsekvens i risikovurderingene vil være til hjelp når ledelsen skal vurdere hvilken håndtering som vil ha størst effekt.

Beslutninger omkring håndtering av risiko kan generelt deles inn i følgende kategorier:

- *Å unngå* – Å gå ut av de aktivitetene som er en kilde til risiko. Å unngå risiko kan for eksempel innebære å avvikle en tjeneste som det er stor misnøye med på grunn av kvaliteten.
- *Å redusere* – Tiltak blir iverksatt for å redusere sannsynligheten for eller konsekvensen av risikoen, eller begge deler. Å redusere risiko kan for eksempel innebære å iverksette tiltak for å endre en arbeidsprosess slik at kvaliteten på tjenesten forbedres.
- *Å dele* – Å redusere risikoen sannsynlighet eller konsekvens ved å overføre, eller på annen måte dele en bit av risikoen med andre. Å dele risiko kan for eksempel være å inngå samarbeid med andre aktuelle virksomheter i regionen for å forbedre kvaliteten på tjenesten.
- *Å akseptere* – Ingen tiltak blir iverksatt for å påvirke risikoen sannsynlighet eller konsekvens.

Ikke alle alternativene vil være aktuelle i alle beslutningssituasjoner.

Å unngå er en form for håndtering som indikerer at det ikke er identifisert noen alternativer som kan redusere konsekvens og sannsynlighet til et akseptabelt nivå og samtidig er gjennomførbart ut fra en vurdering av kostnad i forhold til nytte. Å redusere og dele er former for håndtering som reduserer gjenværende risiko til et nivå som er innenfor ønskede risikotoleranser, mens å akseptere er en form for håndtering som tilsier at risikoen allerede er innenfor akseptabelt nivå.

Etter å ha valgt form for risikohåndtering, må ledelsen identifisere nødvendige kontrollaktiviteter som skal bidra til å sikre at de tiltakene ledelsen har besluttet, blir gjennomført på en hensiktsmessig måte og til rett tid. Tiltakene må innarbeides i handlingsplaner eller lignende for å bringe risikoen i samsvar med akseptert nivå. En viktig del av denne planen er å etablere kontrollaktiviteter for å sikre at risikohåndteringen blir utført på en effektiv måte.

Identifisere nødvendige kontrollaktiviteter

Kontrollaktiviteter består vanligvis av to hovedelementer. Det første elementet består av en beskrivelse av kontrollaktiviteten og hvordan den skal gjennomføres. Dette kan være i form av policyer, retningslinjer, rutine- eller arbeidsbeskrivelser som gjerne også tydeliggjør ansvar og frekvens for slike aktiviteter. Beskrivelsen må kommuniseres til de medarbeidere som har ansvar for etterlevelse på en måte som sikrer forståelse. Det andre hovedelementet er den faktiske gjennomføringen av kontrollaktiviteten slik den er beskrevet skriftlig eller muntlig. Kontrollaktivitetene gjennomføres av mennesker direkte med eller uten anvendelse av teknologi. Det må følges opp at kontrollaktivitetene gjennomføres som forutsatt, og korrigerende tiltak må iverksettes hvis nødvendig.

Kontrollaktiviteter utføres i hele organisasjonen, på alle nivåer og i alle funksjoner. De omfatter en rekke ulike aktiviteter. Siden hver virksomhet har sitt eget sett av målsettinger og tilnærminger, vil det være forskjeller i former for risikohåndtering og tilhørende kontrollaktiviteter. Selv om to virksomheter har identiske målsettinger og tar like beslutninger om hvordan de skal oppnås, vil kontrollaktivitetene sannsynligvis være forskjellige. Hver eneste virksomhet er ledet av ulike mennesker som bruker sitt individuelle skjønn i gjennomføringen av kontroll. Videre gjenspeiler kontrollaktivitetene de omgivelsene virksomheten opererer i, i tillegg til størrelsen og kompleksiteten på organisasjonen, aktivitetenes natur og omfang og virksomhetens historie og kultur.

Bredden og variasjonen i mulige kontrollaktiviteter er meget stor, og det ligger utenfor rammen for dette metodokumentet å søke å beskrive alle typer kontrollaktiviteter. En inndeling kan for eksempel være i *preventive, oppdagende, manuelle, maskinelle og ledelseskontroller*.

På bakgrunn av den omfattende avhengigheten av informasjonssystemer for å drive en virksomhet, understrekes behovet for at hensiktsmessige generelle IKT-kontroller og applikasjonskontroller er implementert for alle vesentlige systemer. Dette gjelder spesielt i forhold til å oppnå målsettinger innenfor de to kategoriene pålitelig regnskapsrapportering og økonomiforvaltning samt overholdelse av gjeldende lover og regler.

Vurdering av effekten av tiltaket og kostnad sammenholdt med nytten

Ved en beslutning om å iverksette ytterligere tiltak og kontrollaktiviteter, må ledelsen vurdere hvilken effekt tiltaket forventes å ha på risikoens sannsynlighet og konsekvens, kostnaden sammenholdt med nytten, og når tiltaket kan forventes å ha effekt. Ledelsen må også vurdere relativ kostnad og nytte ved de alternative tiltak.

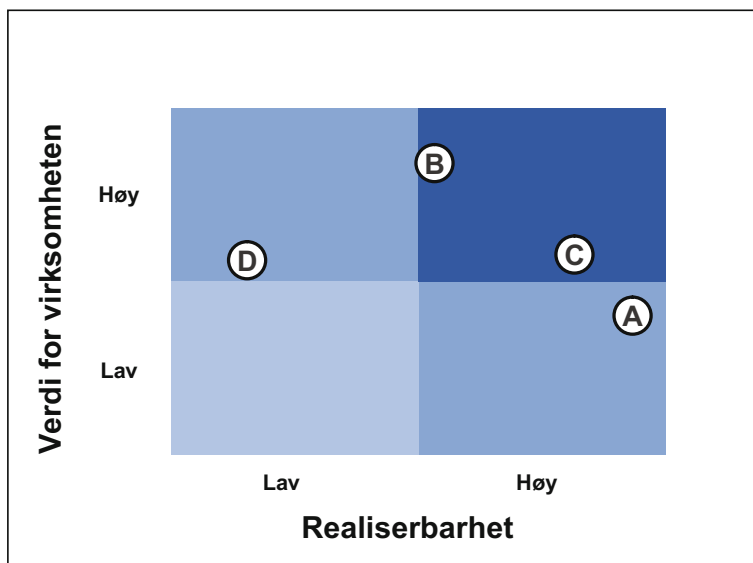
Vurderingene vil i praksis være situasjonsbetinget. For eksempel vil en stor offentlig oppmerksomhet på et område kunne føre til at ledelsen vurderer det som viktigere at tiltaket virker raskt enn at det er det rimeligste tiltaket. Det vil derfor være opp til den enkelte virksomhet, eventuelt i samråd med overordnet myndighet, å vektlegge de ulike momentene i de enkelte tilfellene.

Virksomheten bør innarbeide prosessen for vurdering av eventuelle nye tiltak i sine ordinære vurderings- og beslutningsprosedyrer. Dette er viktig slik at det ikke etableres alternative beslutningsløyper som følge av implementeringen av risikostyring. I det følgende omtales prinsippene for vurdering av eventuelle nye tiltak basert på risikovurderinger. Dette er ikke ment å skulle være fullt ut dekkende for den saksbehandling som virksomhetene vil gjennomføre før beslutning om implementering av nye tiltak iverksettes.

Ledelsen må ha en oppfatning av hvilken effekt nye tiltak forventes å ha. Ytterligere tiltak kan påvirke enten sannsynlighet eller konsekvens, eller de kan påvirke begge disse forholdene. Et tiltak vil kunne påvirke flere risikoer, og det er derfor nødvendig å analysere forventede effekter av et nytt tiltak. I mange tilfeller finnes det ikke tilstrekkelig objektiv informasjon til å kunne vurdere hvilken effekt et tiltak vil ha. Ledelsen vil da i tillegg måtte bygge sine beslutninger på skjønn. Å fatte beslutninger under usikkerhet er en normal del av det å ha lederansvar. Risikovurdering som metode endrer ikke på dette, men den bidrar til en systematisk analyse av hva som kan forventes å være effekten av et tiltak.

Figuren på neste side er en illustrasjon av vurderingene omkring nye tiltak med tilhørende kontrollaktiviteter (A, B, C, D). Vurderingene gjøres med hensyn til om tiltakene vil ha effekt på den aktuelle risikoen (verdi for virksomheten) og om de vil være gjennomførbare ut fra kostnader, ressursbruk, kompleksitet osv.

Figur 6: Tiltaksprioritering



Hensikten med å bruke en slik tilnærming, er å knytte vurdering og prioritering av nye tiltak opp mot de risikoene de er ment å skulle redusere. På den måten kan en bedre sikre at det er de beste tiltakene som blir gjennomført, og at bevisstheten omkring hva som ønskes oppnådd økes. Resultatet av dette vil være mer effektiv ressursbruk ved at man kan redusere antall tiltak som iverksettes, og større risikoreducerende effekt for den aktuelle risikoen ved at de beste tiltakene gis prioritet. Det kan også være at prosessen har bidratt til økt forståelse for at enkelte eksisterende tiltak ikke har den ønskede effekt og at de derfor skal avvikles.

Den aktuelle risikoanalysen bør oppdateres, slik at den viser hva gjenværende risiko forventes å være etter implementering av aktuelle nye tiltak. Denne oppdaterte versjonen vil gi ledelsen et godt grunnlag for å ta stilling til om de nye tiltakene vil være tilstrekkelige. På grunn av usikkerhet omkring framtiden, begrensede ressurser og begrensninger forbundet med enhver aktivitet vil det alltid eksistere et visst nivå av gjenværende risiko.

Gjennomgangseksempel – risikohåndtering

Virksomheten har vurdert i hvilken grad den skal akseptere eller redusere risikoene som påvirker mulighetene for å nå målet om høy brukertilfredshet. Utgangspunktet er de risikovurderingene som er foretatt og avspeilet i risikokartet, ledelsens risikotoleranse samt de begrensninger som ligger i ressursene ledelsen har til disposisjon til å utføre virksomhetens samlede oppgaver.

Ledelsen har følgende vurdering av videre håndtering av de aktuelle risikoene:

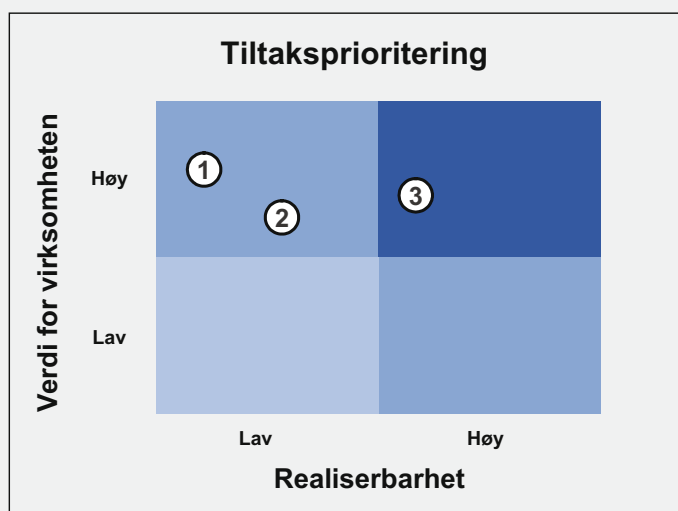
Risiko	Mulige tiltak
1. Risiko for at våre saksbehandlere ikke har tilstrekkelig kunnskap om brukernes lovfestede rettigheter.	Vi aksepterer risikoen slik den er og prioriterer ikke nye tiltak på dette området.
2. Risiko for at informasjonen til brukerne ikke er god nok når det gjelder innholdet i rettigheten og praktisk framgangsmåte for å oppnå rettigheten.	Vi aksepterer risikoen slik den er og prioriterer ikke nye tiltak på dette området.
3. Risiko for at våre søknadsskjemaer er for kompliserte og vanskelig tilgjengelig for brukeren.	Risikoen er noe for høy på grunn av uklarheter omkring punkt C og E i søknadsskjemaet. Vi vil derfor vurdere å endre veiledningen på disse punktene.
4. Risiko for at det gjøres feil i saksbehandlingen slik at brukeren oppnår mindre eller større rettighet enn han/hun har krav på.	Risikoen er vurdert til å være for høy. Andelen av klager som får medhold, er for høy, og vi vil derfor vurdere å iverksette ett eller flere av tiltakene nedenfor: <ul style="list-style-type: none"> • Alle vedtakene kvalitetssikres av en annen saksbehandler • Etablere ukentlige erfaringsmøter hvor saksbehandlerne utveksler informasjon om prinsipielle eller vanskelige saker som er under behandling • Etablere et elektronisk vedtaksarkiv som gjøres tilgjengelig på vårt intranett og som viser korte versjoner av saker og avgjørelser. Det skal være et søkbart arkiv.
5. Risiko for at vi har ineffektive prosedyrer for saksbehandling som forsinker saksbehandlingen unødige.	Risikoen vurderes som for høy. Vi vil vurdere å gjennomføre ett eller flere av følgende tiltak: <ul style="list-style-type: none"> • Innføring av grovsortering av innkomne søknader i «tunge» og «lette» saker. • Opprettelse av team for håndtering av «tunge» saker. • Ukentlig fordeling/omfordeling av saker mellom saksbehandlerne for å unngå skjev arbeidsbelastning. • Se på om informasjonen kan gjøres bedre slik at vi får ned omfanget av mangelfull informasjon fra brukerne. • Opprettelse av eget team som kontakter brukerne for å få inn manglende opplysninger. Det trenger ikke å være saksbehandlerressurser. • Gjennomføre arbeidsmiljøundersøkelse for å få bedre forståelse for hva som forårsaker sykefraværet. • Opprette felles prosjektgruppe med IKT-avdelingen og softwareleverandøren for å kartlegge årsakene til ustabiliteten i saksbehandlersystemet som igjen forsinker saksbehandlingen.

Gjennomgangseksempel forts.

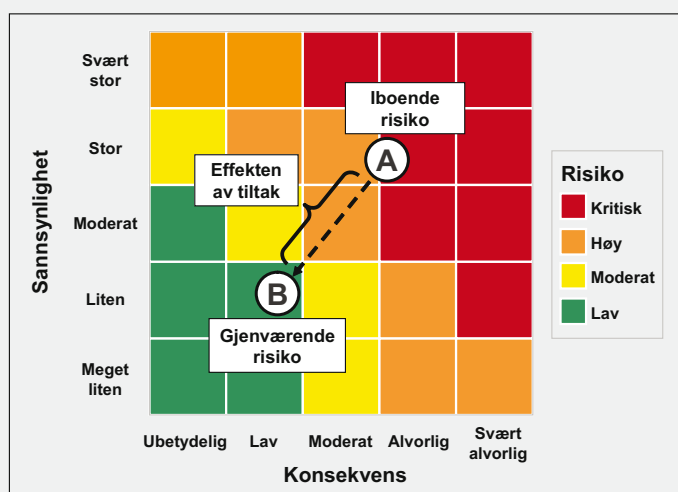
Risiko	Mulige tiltak
6. Risiko for at vi ikke iverksetter vedtakene tilstrekkelig raskt etter at de er fastsatt.	Risikoen er vurdert som akseptabel. Ingen ytterligere tiltak vil iverksettes.
7. Risiko for at vi har ineffektive prosedyrer for behandling av klager på vår saksbehandling.	Risikoen er vurdert som for høy. Vi vil derfor vurdere å gjennomføre ett eller flere av følgende tiltak: <ul style="list-style-type: none">• Gjennomføre arbeidsmiljøundersøkelse for å få bedre forståelse for hva som forårsaker sykefraværet.• Etablere løpende måling og rapportering av hvor mange klagesaker som ikke er ferdigbehandlet fordelt på hvor lang tid det er siden klagen ble mottatt. Informasjonen skal brukes til å kunne prioritere ressurser i perioder hvor ubehandlede saker blir for høy eller tiden fra mottatt klage til klagevedtak blir for lang.

Gjennomgangseksempel forts.

På bakgrunn av disse vurderingene, har ledelsen for alle risikoene gjennomført en prioritering av hvilke tiltak som vil ha størst betydning for å redusere de aktuelle risikoene, og i hvilken grad de er gjennomførbare. Figuren nedenfor illustrerer hvordan de mulige tiltakene knyttet til å oppnå riktigere saksbehandling (risiko 4) er prioritert. Prioriteringen er gjort med bakgrunn i forventet effekt av det enkelte tiltak og en vurdering av kostnad i forhold til nytte. Dette er nærmere begrunnet i sakspapirene og gjengis ikke her. På bakgrunn av dette er det besluttet å gjennomføre tiltak nr. 3 med tilhørende kontrollaktiviteter for å sikre at tiltaket blir gjennomført.



Ledelsen har på bakgrunn av vedtaket om å gjennomføre tiltak nr. 3, også oppdatert sin vurdering av hvordan risikoen for uriktig saksbehandling vil være etter at tiltak nr. 3 er gjennomført. Den oppdaterte risikovurderingen framkommer i figuren nedenfor. Den viser hvordan risikoen var vurdert før tiltaket (A), og hvordan risikoen forventes å bli redusert etter gjennomføring av tiltak nr. 3 (B).



3.9 Oppfølging av risikoene

3.9.1 Hensikten med oppfølging av risikoene

Risikostyringen må følges opp, og det må vurderes om den fungerer over tid. Dette oppnås gjennom løpende oppfølgingsaktiviteter, evalueringer eller en kombinasjon av de to. Omfanget og hyppigheten av evalueringene avhenger primært av risikovurderingen og av hvor effektive de løpende oppfølgingsrutinene er. Ledelsen må selv vurdere hvor ofte det er behov for evalueringer for å ha rimelig grad av sikkerhet for at risikostyringen fungerer effektivt.

En løpende oppfølging av hvordan risikoene håndteres, vil være en viktig del av ledelsens samlede styringsinformasjon og en del av den samlede risikostyringen. Dersom oppfølgingen viser at risikoen er som forventet og forutsatt

av ledelsen, indikerer det at de iverksatte tiltakene fungerer som forventet. Dersom det viser seg at risikoen er høyere enn forutsatt, vil det kunne indikere behov for ytterligere tiltak eller undersøkelser om hvorfor de tiltakene som er implementert ikke har den forventede effekten.

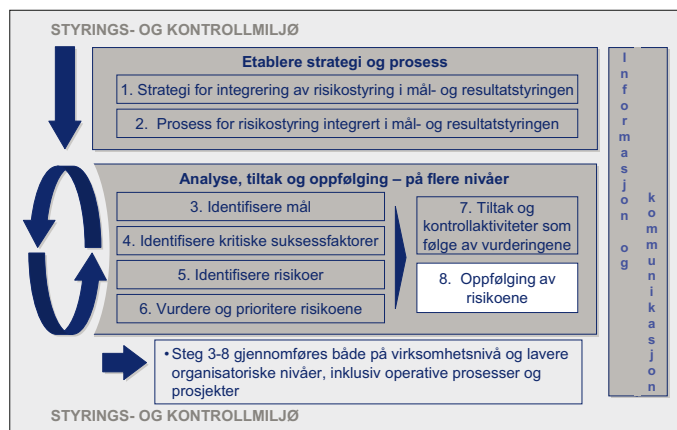
Oppfølgingen kan også vise at risikoen er lavere enn forventet og lavere enn det som er ønskelig. Det kan indikere behov for økt ambisjonsnivå, eller indikere en mulighet for å flytte ressurser (tiltak) fra ett område over til et annet område hvor risikoen vurderes som for høy.

En god oppfølging av risikoer vil derfor gi ledelsen god styringsinformasjon og muligheten til å iverksette nødvendige tiltak på et tidlig tidspunkt. Ledelsens oppfølging har også en betydelig preventiv verdi. For det første er den med på å sikre at de som daglig gjennomfører tiltakene og utøver kontrollaktivitetene, gjør dette som forutsatt. For det andre gir engasjement fra lederen i en medarbeiders oppgaver motivasjon til å utføre oppgavene best mulig.

3.9.2 Praktiske måter å følge opp risikoer på

Det skal være fastsatt styringsparametere som dekker alle vesentlige forhold i virksomhetens planer. Oppfølging basert på hensiktsmessige styringsparametere er en effektiv måte for ledelsen til å skaffe seg informasjon om hvordan måloppnåelsen er, og dermed også om risikosituasjonen. Risikoene vil som tidligere nevnt være avledet av analyser av mål og kritiske suksessfaktorer, f.eks. kort saksbehandlingstid og høy medarbeidertilfredshet. Det er i mange tilfeller mulig å etablere styringsparametere som sier noe om situasjonen for slike og lignende typer av kritiske suksessfaktorer. Slike styringsparametere vil i mange virksomheter allerede være etablert og innarbeidet i den ordinære rapporteringen. Dersom de mangler helt eller delvis, bør ledelsen vurdere hvilke styringsparametere som er hensiktsmessige å etablere i forbindelse med implementeringen av risikostyringen. Risikostyringsprosessen kan også bidra til at virksomheten ser behov for andre og mer hensiktsmessige styringsparametere enn de etablerte.

For risikoer som knytter seg til løpende og operative prosesser i virksomheten, kan det være vanskeligere å etablere hensiktsmessige styringsparametere med tilstrekkelig utsagnskraft.



Men også operasjonelle forhold bør måles ved bruk av styringsparametere. For eksempel kan håndteringen av risiko for at feil variabel lønn registreres for ansatte, måles ved antall klager i forbindelse med lønnsutbetalinger. I tillegg kan oppfølgingen skje på ulike andre måter, for eksempel ved systematisk gjennomgang i møter, samtaler rundt driftsproblemer, rapporter, stikkprøver og drøfting av feilsituasjoner som oppstår.

Virksomhetens ledelse skal forsikre seg om at de samlede tiltakene som etableres for å følge opp risikoene, totalt sett er tilstrekkelig for å kunne ha nødvendig kontroll med virksomheten.

Gjennomgangseksempel – oppfølging

Virksomhetens ledelse har besluttet å følge opp risikohåndteringen ved hjelp av styringsparametere inkludert i den øvrige virksomhetsstyringen.

For å følge med i virksomhetens håndtering av risikoer knyttet til målet om høy brukertilfredshet følger ledelsen opp følgende styringsparametere:

Styringsparameter	Måltall	Resultat siste måned
Andel saksbehandlere som har gjennomført opplæring.	100%	95%
Antall spørsmål omkring hvordan en søknad fylles ut.	<10	8
Andel klager som gis medhold.	<5%	8%
Antall saker som ikke er ferdigstilt.	<100	248

For viktige områder hvor det ikke finnes hensiktsmessige styringsparametere, bør det vurderes å innføre egne evalueringer fra ledere. Med dette menes evalueringer foretatt av ledere med ansvar for viktige prosesser hvor de bekrefter om de har tilstrekkelig kontroll med risikoene. En evaluering kan også konkludere med at det ikke er tilstrekkelig kontroll, og at det vil innføres ytterligere tiltak. Evalueringen bør i disse tilfellene også vurdere hvilken effekt nye tiltak antas å ha, og når tiltakene forventes å gi slik effekt. Det bør vurderes å innarbeide systematiske egne evalueringer som en del av den samlede rapporteringen i virksomheten. Egenevalueringene kan være et viktig supplement til rapporteringen av mer objektive styringsparametere.

Evalueringer kan også foretas på et mer objektivt grunnlag av personer som har større avstand til det som skal evalueres. En evaluering kan ha en bred tilnærming og ta for seg risikostyringen i virksomheten som helhet. I andre tilfeller kan det være hensiktsmessig at evalueringen begrenses til en spesifikk driftsenhet, prosess eller avdeling, mens andre områder av virksomheten blir evaluert over tid.

3.9.3 Bruk av kontrollere og internrevisjon

Mange virksomheter benytter kontrollere i sin virksomhetsstyring. Controllernes oppgaver kan variere betydelig både innenfor den enkelte virksomheten og mellom ulike virksomheter. Felles for kontrollernes oppgaver er at de utføres på vegne av en eller flere ledere i virksomheten. De bistår lederen med å følge opp sitt ansvarsområde og inngår som en del av den samlede operative virksomhetsstyringen på det enkelte område. I større organisasjoner er det uvanlig at kontrollere er knyttet ansvarsmessig direkte opp til virksomhetens ledelse. En controller kan ha utførende oppgaver i forbindelse med risikostyringen, og vil dermed ikke være tilstrekkelig objektiv til å evaluere risikostyringen som helhet for virksomhetens ledelse.

Flere større statlige virksomheter har etablert egne internrevisjonsenheter. Internrevisjonen arbeider systematisk etter internasjonalt anerkjente standarder og metoder. Disse standardene krever bl.a. at internrevisjonsfunksjonen skal være uavhengig, og at interne revisorer skal være objektive i utøvelsen av sitt arbeid. Internrevisjonen vil derfor rapportere til styret for de virksomheter som har det, og ellers til virksomhetens ledelse.

Internrevisjonens primære oppgave er ved sine revisjonshandlinger å bistå virksomhetens ledelse i deres oppfølging av om det er etablert en robust risikostyring og intern kontroll i virksomheten, og at den er tilstrekkelig og effektiv. En internrevisjon er et nyttig verktøy for virksomhetens ledelse som en ekstra sikring av at risikostyringen er tilstrekkelig og integrert i virksomhetens mål- og resultatstyring. En godt kvalifisert internrevisjon kan også bidra med nyttige innspill til ledere på alle nivåer om mulige forbedringer i den løpende risikostyring og internkontrollen.

3.10 Risikostyringens begrensninger

Uansett hvor godt risikostyringen planlegges og gjennomføres, kan den bare gi ledelsen og overordnet organ rimelig sikkerhet for at virksomheten vil oppnå sine målsettinger. Det er blant annet begrensninger i tilknytning til:

- Uklare målformuleringer, ulik oppfatning av mål og/eller risikotoleranser som kan medføre at mål/risikoer prioriteres feil.
- Svakheter i menneskelig dømmekraft når metoden anvendes som kan medføre at relevante risikoforhold ikke vurderes, tiltak etableres basert på gale premisser og/eller forventninger til kvaliteten av etablerte tiltak, kontrollaktiviteter og det interne styrings- og kontrollmiljøet, eller at andre vurderinger som ligger til grunn for en avgjørelse, blir feilaktige.
- Beslutninger om etablering av tiltak og kontrollaktiviteter må bygge på en kost/nytte vurdering.

I tillegg representerer det en begrensning at tiltak og kontrollaktiviteter ikke gjennomføres som forutsatt på grunn av ubevisste eller bevisste feil. Ledelsen har også mulighet til å overstyre beslutninger tatt i forbindelse med risikostyringen.

Disse begrensningene vil forhindre virksomhetens ledelse og overordnet organ i å ha absolutt sikkerhet for virksomhetens måloppnåelse.

Stikkordregister

Begrep	Side
Ansvar for risikostyring og intern kontroll	14-15
- departementets administrative ledelse	15
- virksomhetens ledelse	14
- øvrige ledere og ansatte	15
Begrensninger, risikostyringens	49
Beslutninger omkring håndtering av risiko	41
COSO ERM	14
Dokumentasjon	19-20, 22-23
- økonomiregelverkets krav	19-20
- form, frekvens og omfang	20
- formål	22-23
• dokumentasjon av risikostyringsprosessen	23
• dokumentasjon av kontrollaktiviteter og tiltak	23
• dokumentasjon av oppfølging av risiko	23
Gjennomgangseksempel	15
- utgangspunkt overordnet mål	26
- kritiske suksessfaktorer	28
- identifisering av risikoer	30
- konsekvensskala	34
- vurdering og prioritering av risikoene	36-37
- risikohåndtering	44-46
- oppfølging	48
Informasjon og kommunikasjon	22
Intern kontroll; se Risikostyring og intern kontroll	
Internrevisjon	49
Konsekvens	18, 31-34
Konsekvensskala	33-34
Kontrollaktiviteter	
- identifisering av	41
- oppfølging av	41
- se også Tiltak og kontrollaktiviteter	
Kritiske suksessfaktorer	16, 27-28
Mål, identifisering av	26
Mål- og resultatstyring	12
Målsettinger, tre kategorier	17-18
Operative prosesser, risikoanalyse	38-39
Oppfølging av risikoer	47-49
- Egenevalueringer	48
- Evalueringer	48
- Styringsparametere	47-48
Prosess, risikostyring integrert i mål- og resultatstyringen	24
- overordnet nivå	25
- lavere nivåer	37
Prosesskartlegging operative prosesser	38-39

Begrep	Side
Prosjekter, risikoanalyse	40
Risiko	
- definisjon	18
- gjenværende	31-32
- iboende	31-32
- identifisering av	28-31
- vurdering og prioritering	31-37
- som ikke fanges opp i framgangsmåten som er beskrevet	29-30
Risikohierarki	29
Risikokart	32, 35, 37
Risikostyring og intern kontroll	
- definisjon	18
- hovedelementer	19
Risikotoleranse, definisjon	18
Sannsynlighet	18, 31-34
Strategi, integrering av risikostyring i mål- og resultatstyringen	23-24
Styrings- og kontrollmiljø	22
Styringsparametere	19, 27, 30-31, 47-48
Tiltak og kontrollaktiviteter	18, 40-46
- beslutninger omkring håndtering av risiko	41
- definisjoner	18
- identifisere nødvendige kontrollaktiviteter	41
- vurdering og prioritering	42-43
«Top-down» tilnærming	24
Vesentlighet	18

Vedlegg A - Bestemmelser om intern kontroll i økonomiregelverket

Leseren gjøres oppmerksom på at teksten nedenfor ikke er en ren kopi av bestemmelsen slik den er skrevet i økonomiregelverket. Det er av pedagogiske grunner foretatt noen uthevelser og grupperinger, samt tilføyd noen overskrifter i forhold til teksten slik den står i økonomiregelverket.

BESTEMMELSER OM ØKONOMISTYRING I STATEN

2.4 Intern kontroll

Alle virksomheter **skal etablere intern kontroll**. Virksomhetens ledelse har ansvaret for å påse at den interne kontrollen er **tilpasset risiko og vesentlighet**, at den **fungerer på en tilfredsstillende måte** og at den kan **dokumenteres**. Intern kontroll skal primært **være innebygd i virksomhetens interne styring**.

FORMÅL: Den interne kontrollen skal forhindre styringsvikt, feil og mangler slik at:

Mål og resultatkrav

- b) måloppnåelse og resultater står i tilfredsstillende forhold til fastsatte mål og resultatkrav, og at eventuelle vesentlige avvik avdekkes og korrigeres i nødvendig utstrekning
- c) ressursbruken er effektiv

Pålitelig regnskapsrapportering og økonomiforvaltning

- a) beløpsmessige rammer ikke overskrides og at forutsatte inntekter kommer inn
- d) regnskap og informasjon om resultater er pålitelig og nøyaktig
- e) virksomhetens verdier, herunder fast eiendom, materiell, utstyr, verdipapirer og andre økonomiske verdier, forvaltes på en forsvarlig måte

Overholdelse av gjeldende lover og regler

- f) økonomistyringen er organisert på en betryggende måte og utføres i samsvar med gjeldende lover og regler
- g) misligheter og økonomisk kriminalitet forebygges og avdekkes

KOMPONENTER:

For å kunne utøve nødvendig intern kontroll, skal virksomhetens ledelse etablere systemer, rutiner og tiltak med fokus på blant annet følgende faktorer:

Styrings- og kontrollmiljø

- a) ledelsens og tilsattes kompetanse og holdning til resultatoppfølging og kontroll
- Identifisering av mål. Identifisering, vurdering og prioritering av risikoer. Tiltak og kontrollaktiviteter som følge av vurderingene.**

- b) identifisering av risikofaktorer som kan medvirke til at virksomhetens mål ikke nås, og korrigerende tiltak som med rimelighet kan redusere sannsynligheten for manglende måloppnåelse

Oppfølging

- c) sikring av kvaliteten i den interne styringen, herunder forsvarlig arbeidsdeling, og produktivitet i arbeidsprosessene

Informasjon og kommunikasjon

- d) informasjonsrutiner som sikrer at viktig og pålitelig informasjon av betydning for måloppnåelsen kommuniseres på en effektiv måte
- e) rutiner for behandling og lagring av vesentlig informasjon som sikrer konfidensialitet, integritet og tilgjengelighet

Den interne kontrollen skal også ha fokus på å forebygge og avdekke tilsiktede handlinger utført i strid med gjeldende lover og regler, som eksempelvis manipulasjon, forfalskning eller endring av regnskapsdata eller annen resultatinformasjon. Det vises til Statens personalhåndbok for retningslinjer for behandling av saker om underslag, tyveri, bedrageri og utroskap i statstjenesten.

Dersom virksomheten benytter en tjenesteyter, jf. pkt. 4.5, skal virksomhetens interne kontroll være tilpasset arbeidsdelingen mellom virksomheten og tjenesteyteren.

Ved etablering av kontrolltiltak skal virksomhetens ledelse **vurdere hvilke kostnader tiltaket medfører, målt opp mot den nytte og de fordeler som kan oppnås**. Alle tiltak skal forankres på overordnet nivå for å sikre relevans og fullstendighet i risikobildet. For spesielt viktige rutiner skal virksomhetens ledelse vurdere om det er behov for tilleggsrapportering og spesielle analyser for å avdekke eventuelle framtidige avvik.

Senter for statlig økonomistyring har utarbeidet et metodedokument om risikostyring i staten. En god mål- og resultatstyring forutsetter at virksomhetsledelsen kjenner og aktivt håndterer de utfordringer eller usikkerheter som kan påvirke måloppnåelse negativt. Metodedokumentet gir veiledning i hvordan virksomhetene på en strukturert måte kan benytte risikostyring og intern kontroll som et verktøy for å gi rimelig sikkerhet for at virksomheten oppnår sine målsettinger.