IIA Norge

Operasjonell risikostyring - en innføring

1. utgave 2022

Hva er governance?

Et ansvarlig samspill mellom eiere, styret og ledelse sett i et langsiktig, bærekraftig perspektiv. Formålet er å sikre at virksomheten skaper verdier, når sine mål og følger lover og regler. Utgjør de strukturer, prosesser og verktøy som brukes for å styre aktiviteter, ressurser og risiko i en virksomhet.

Internrevisjon

Styrets verktøy for å fremme og beskytte virksomhetens verdier og påse god styring og kontroll. Opererer med risikobasert tilnærming til prioritering av revisjonsoppdrag. Gir objektive bekreftelser, råd og skaper økt innsikt for styret og ledelse.

Compliance

Compliance knyttes til etterlevelse av relevant lovverk, reguleringer både nasjonalt og internasjonalt, så vel som virksomhetens interne retningslinjer. Fokus på compliance risiko og bidrar til å styrke etterlevelse og øke bevissthet i virksomheten. Lovpålagt funksjon i bank og finans.

Risikostyring

Sentralt i god governance er helhetlig, proaktiv risikostyring. Denne prosessen bidrar til å sikre best mulig beslutningsgrunnlag på strategisk nivå i virksomheten. Dekker negative konsekvenser og muligheter.

Innholdsfortegnelse

1 Definisjon og innledning

1.1 Hva er operasjonell risiko?

De fleste virksomheter søker eller tilstreber gjerne en effektiv driftsmodell som maksimerer muligheten for å nå målene. Virksomheten kan ha ulike målsetninger slik som samfunnsansvar og bærekraft som ikke nødvendigvis er begrenset til finansielle og forretningsmessige målsettinger. Operasjonell risikostyring handler om å være bevisst hvilke *operasjonelle valg og tilhørende operasjonelle risikoer* som kan oppstå på vei mot å nå disse målene.

Det er mange definisjoner på hva operasjonell risiko er. I denne veilederen er de fire dimensjonene beskyttelse av fysiske eiendeler, mennesker, organisasjon og teknologi lagt til grunn for definisjonen av operasjonell risiko, fordi det viser seg at rotårsaken for operasjonelle risikohendelser ofte er knyttet til disse.

Disse forholdene kan enten ha en opp- eller nedsideeffekt, og er med på å øke eller redusere sannsynligheten for at organisasjonen når dens overordnende mål.

Vi legger derfor til grunn følgende definisjoner av begrepet operasjonell risiko og tilhørende begreper:

Operasjonell risiko knyttes til fysiske eiendeler, mennesker, prosesser og bruk av teknologi i virksomhetens utøvelse av daglige aktiviteter og tjenester og kan gi opphav til både positive og negative effekter. Dette inkluderer håndtering av usikkerheter, muligheter og risikoer i den løpende driften samt konsekvenser av uønskede hendelser.

Effektene kan også oppstå på grunn av eksterne hendelser (teknologi, trender, lovkrav, politiske forventninger) og har også sammenheng med de beslutninger som tas under rådende forhold og med utgangspunkt i et begrenset informasjonsgrunnlag. Effekter kan være ulemper (nedside), gevinster og/eller opplevd nytte (oppside).

Usikkerheter er ikke-kjente størrelser eller at det foreligger utilstrekkelig informasjon.

Risikoer er kjente størrelser innenfor visse forventninger, mens muligheter er en uutnyttet oppside til de aktivt benyttes.

I en kompleks verden med stadige endringer har operasjonell risiko fått større betydning enn før, og får økt oppmerksomhet hos styre og toppledelse. Typiske faktorer som gjerne inkluderes ved i operasjonell risikostyring er:

a) Bruk av teknologi både i form av tradisjonell databehandling og på de nye områdene kunstig intelligens, IoT, metaverse, blokkjeder mv.) samt sammenkoblede digitale tjenester.
b) Regelverksutvikling (f.eks. åpenhetsloven, sikkerhetsloven, GDPR og outsourcing til land utenfor EU - Schrems II).
c) Stadig mer komplekse datastrukturer og automatiserte prosesser.
d) Konkurranse som driver frem oppkjøp og fusjoner.
e) Eksterne trusler slik som krig, pandemi, cyberkriminalitet og psykisk helse.
f) Interne omorganiseringer er den nye normalen for å møte krav og forventninger.
g) Utkontraktering, tredjepartsleverandører og forsyningskjeder, samt tilhørende plikter relatert til menneskerettigheter (åpenhetsloven).

I tillegg til interne behov som:

h) Å øke kvaliteten på driften
i) Å bedre styring og kontroll på grensesnitt og overganger internt og eksternt
j) Å redusere sannsynlighet og konsekvenser av uønskede hendelser
k) Å møte regulatoriske krav og forventinger på en effektiv måte
l) Fysisk sikkerhet av bygninger, herunder mot innbrudd, tyveri og brann.

1.2 Hvorfor skal vi drive med operasjonell risikostyring?

Formålet med risikostyring er å understøtte beslutninger og finne de beste alternativene og mulige løsningene for virksomheten gitt rammebetingelser, organisasjonsevnen og finansiell kapasitet. Operasjonell risikostyring er derfor en viktig del av virksomhetsstyringen.

Risiko handler om usikkerhet knyttet til hva som kan skje i fremtiden. Utfallet kan bli bedre eller dårligere enn det vi har planlagt eller forutsatt. Det er her operasjonell risiko har en uutnyttet oppside ved at styringen kan bli bedre gjennom en riktigere og en mer effektiv styring og kontroll. Virksomhetene kan oppnå dette gjennom økt bevissthet om hva som sørger for måloppnåelse, hva som kan gå galt og hvordan ha kontroll på disse områdene, samt hvilke områder i virksomheten som kan ha fordeler av økt automatisering eller andre organisatoriske behov.

Operasjonell risikostyring hjelper oss med å definere og forstå risiko (trusler og muligheter), slik at vi kan ta bedre beslutninger på alle nivåer i en virksomhet for å nå målsettingene som virksomheten selv har satt.

1.3 Funksjon for operasjonell risikostyring – sikre et felles rammeverk

I veileder om risikostyring utarbeidet av IIA Norge, ble det valgt å omtale og definere en funksjon for risikostyring som ivaretar en «systematisk og objektiv tilnærming til å identifisere, analysere og vurdere risiko, samt utforme og gjennomføre tiltak som skal sørge for at risikoen håndteres innenfor definerte risikorammer». Egen funksjon er ofte knyttet til regulatoriske krav. For andre virksomheter (private så vel som offentlige virksomheter) er det viktig at det er ledelsen som håndterer den operasjonelle risikostyringen, men som gjerne støttes av en risikofunksjon. Det er viktig at ledelsen og prosesseiere eier risikostyringen for egne områder/prosesser.

Et felles rammeverk for operasjonell risikostyring bør bestå av følgende:

- En overordnet policy inkl. mål for operasjonell risikostyring (f.eks. redusere kostnader, øke kvalitet over tid, bedre beslutninger), som fastslår roller og mandat, og sikrer myndighet (uavhengighet).
- En omforent og vedtatt prosess som legges til grunn når de involverte skal koordinere internt og legge sine planer, og som legger føringer i forhold til:
  - Kompetanse
  - Kapasitet
  - Systemverktøy
- Nødvendige instruksjoner, enten inkludert i prosessbeskrivelsen eller gjennom korte og konkrete styrende dokumenter som er gjennomarbeidet og omforent vedtatt, som sikrer:
  - Hensiktsmessig ansvarsdeling mellom sentral funksjon og linjeansvar for gjennomføring av risikostyring.
  - Bistand til og opplæring for linjen som støtter opp under en sunn kultur og holdningsforbedringer.
  - Regelmessig rapportering til leder på status i forhold til plan og endringer i den.

Den konkrete utformingen av funksjonen avhenger av virksomhetens størrelse, behov og styringsmodell. For eksempel er det ofte slik at en stor og kompleks organisasjon har en avdeling ledet av en Chief Risk Officer (CRO), mens en mindre organisasjon kan plassere dette ansvaret på en annen funksjon slik som f.eks. Controller eller Chief Financial Officer (CFO). Hovedpoenget er at noen i virksomheten må være utpekt og ha et dedikert ansvar for operasjonell risiko med et definert mandat. Tilsvarende må ansvaret for operasjonell risiko være tydelig plassert og det må være en forankring opp mot ledelsen og eventuelt styret slik at styringen av operasjonell risiko inngår i virksomhetens overordnende styringsprosesser som en del av øvrig virksomhetsstyring.

Større organisasjoner finner det ofte hensiktsmessig å ha en egen organisatorisk enhet for operasjonell risikostyring, med leder og stab som rapporterer til CRO eller kvalitetssjef, mens mindre virksomheter ivaretar operasjonell risikostyring under en annen funksjon med hovedansvar for helhetlig risikostyring, økonomistyring, drift og/eller kvalitetsstyring. I modne virksomheter utvikles det ofte også en operasjonell risikoappetitt med tilhørende toleransegrenser for ulike deler av det operasjonelle risikouniverset.

Gjennom å plassere ansvaret for et felles rammeverk for operasjonell risikostyring og en funksjon/rolle med ansvar for å vedlikeholde dette, eventuelt med støtte gjennom en teknisk systemløsning, økes sjansen for å oppnå en god og kostnadseffektiv operasjonell risikostyring. Dette gjelder uansett størrelse og organisering.

Figur 1: sammenhengen mellom virksomhetsstyring og operasjonell risikostyring

I dette dokumentet konstaterer vi at det er en sammenheng mellom operasjonell risikostyring og den overordnende virksomhetsstyringen.

Risikostyring og internkontroll bør virksomheten etablere innenfor alle relevante risikoområder, herunder innenfor operasjonell risiko. Hovedpoenget er at det operasjonelle risikobildet må sees i sammenheng med de øvrige veivalg og prioriteringer i virksomheten som en helhetlig portefølje av risikoer.

2 Foreslått modell for arbeidet med operasjonell risikostyring

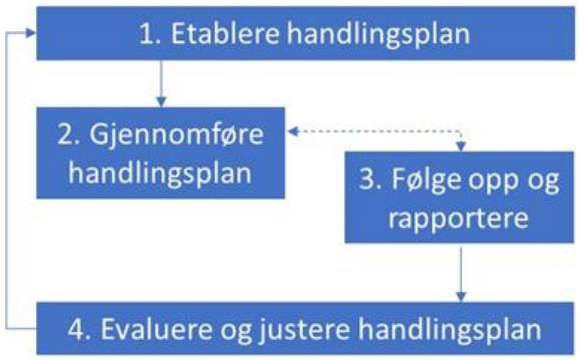
Kjernen i all risikostyring er det som gjerne kalles handlingsplan. Enkelte bruker også begrepet risikohåndteringsplan.

Handlingsplanen er en oversikt over hvilke aktiviteter som skal bidra til å håndtere risiko, og dermed øke sannsynligheten for måloppnåelse og de positive effektene.

Operasjonell risikostyring handler i praksis om å

1) etablere en risikobasert handlingsplan som hensyntar virksomhetens målbilde,
2) gjennomføre handlingsplanen,
3) følge opp og rapportere samt
4) evaluere og justere handlingsplanen

I sum er dette illustrert i følgende firetrinns modell:

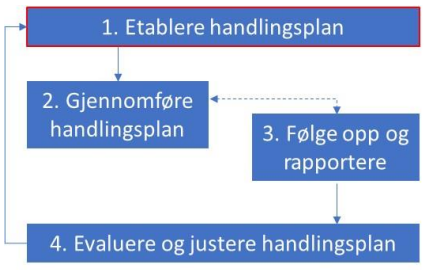


Figur 2: Firetrinns modell for arbeidet med operasjonell risikostyring

I det etterfølgende blir hvert steg omtalt hver for seg.

2.1 Etablere handlingsplan

De fleste virksomheter lager prosjektplaner for å styre prosjekter, en forretningsplan for å styre strategiske tiltak, en markedsplan for å styre kunderettede tiltak eller en finansiell plan for å styre investeringer, kapital og likviditet, men hvor mange virksomheter lager egne handlingsplaner for å styre operasjonell risiko?



Etablering av handlingsplan handler om å definere de aktiviteter som virksomheten anser som viktigst å prioritere i håndteringen av operasjonell risiko.

For å klare dette må man kunne identifisere, beskrive og vurdere de viktigste operasjonelle risikoene – altså mulige hendelser eller forhold knyttet til mennesker, prosesser eller systemer som vil kunne gi positiv eller negativ innvirkning på veien mot målene. I denne sammenheng er det viktig at man bestreber å kvantifisere risiko i kroner og øre, dette kan også inkludere vurderinger av kvalitetskostnader, slik at man både kan prioritere der man skal legge inn innsatsen samt vurdere kost/nytten av foreslåtte tiltak. Dette inkluderer også å ta stilling til hvilke deler av virksomhetens operasjoner som bør utkontrakteres elle forsikres fordi vi enten ikke har kapasitet eller evne til å bære risikoene selv.

Videre må virksomheten være i stand til å gjennomføre og dokumentere risikostyringen. Dokumentasjon skal være et synlig bevis for en strukturert angrepsvinkel, selv om dokumentasjon selvfølgelig ikke er et mål i seg selv – det er de virkelige handlinger som teller. Unntaket kan være etterlevelse der det kan være lovpålagte krav om dokumentasjon, som gjør det mulig å følge opp vurderinger og de forutsetningene som ble lagt til grunn på en systematisk og strukturert måte.

Handlingsplanen blir ikke bedre enn kvaliteten på selve risikovurderingen, der verdier, sårbarheter og trusselscenarioer sammenstilles til konkrete risikobeskrivelser.

Det viktigste suksesskriteriet for dette steget er kompetanse (ref. kapittel 1 om krav til et felles rammeverk for operasjonell risikostyring) om egen virksomhet og gjeldende trusselbilde. Kunnskap om din egen virksomhet, verdiskapningen som skjer gjennom kjerne- og støtteprosesser, samt forpliktelser knyttet til etterlevelse, er en nødvendig forutsetning for at virksomheten skal kunne:

1. Si noe konkret om hva slags innvirkning de identifiserte potensielle hendelsene eller forholdene vil kunne ha for virksomheten.
2. Prioritere disse potensielle hendelsene eller forholdene opp mot hverandre.
3. Vurdere hvordan virksomheten realistisk kan håndtere de prioriterte potensielle hendelsene eller forholdene dersom de skulle inntreffe – helt konkret hvilke kapasitetsmessige forutsetninger som må være på plass for at risikoen realistisk skal kunne håndteres.
4. Vurdere om prosessene og kontrollene kan forbedres gjennom f.eks forenkling eller automatisering.

Uten god kompetanse om egen virksomhet og gjeldende trusselbilde og mulighetsområde, er det fare for at handlingsplanen blir bestående av irrelevante aktiviteter som ikke lar seg gjennomføre i praksis.

For å lage gode og relevante risikobeskrivelser må virksomheten ta utgangspunkt i hvordan man rent operasjonelt har tenkt å komme frem til de forretningsmessige målene – rettere sagt hvordan man tenker å organisere fysiske eiendeler, mennesker, prosesser og teknologi for å nå sine mål. Når dette er klart, kan man ta for deg de typiske trekkene i listen a) – l) under kapittel 1, og vurdere i hvilken grad hver enkelt faktor vil kunne ha en innvirkning på veien mot måloppnåelse. Der ett eller flere av disse trekkene vil kunne ha høy grad av innvirkning på operasjon(er) på vei til måloppnåelse bør mulige tiltak identifiseres og defineres.

Deretter må tiltak vurderes og besluttes. Det er nærliggende å tenke at man gjerne vil velge den veien til mål som umiddelbart virker tryggest. Det er her oppside-/mulighetsaspektet kommer inn, og viktigheten av å gjøre en god evaluering av tiltakene med hensyn til kost/nytte. I denne sammenheng er det viktig at man bestreber å kvantifisere foreslåtte tiltak og vurderer dem opp mot vurderingen av risiko uttrykt i kroner og øre. Det kan nemlig finnes en annen måte å organisere fysiske eiendeler, mennesker, prosesser og teknologi på, som kanskje er «mindre trygg», men som samtidig innebærer muligheter ift. lavere kostnader, kortere «time-to-market», høyere kvalitet mv. Helt konkret må virksomheten etter beste evne estimere hva som må til for å iverksette, gjennomføre og følge opp hvert enkelt tiltak. Dette estimatet vurderes så opp mot den mulige nytten, eller effekten, som man forventer at tiltaket vil ha på din evne til å nå målet. En måte å

vurdere effekten på tiltakene er å etablere og følge opp relevante KPIer, inkludert avvik/hendelser av betydning.

«Leveransen» fra dette første steget skal være gjennomtenkte, prioriterte og målrettede tiltak som organisasjonen mener vil ha god effekt gjennom en akseptabel innsats.

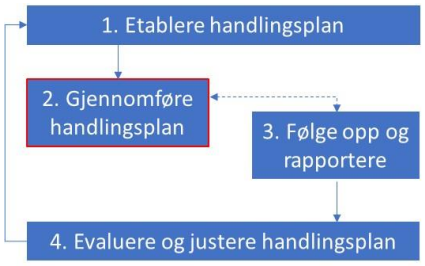
En typisk fallgruve ved gjennomføring av en risikovurdering er at man er for rask og lite presis i risikobeskrivelsene. Gode risikobeskrivelser er en forutsetning for at vurderingen og handlingsplanen kan gjøres spiss nok, slik at organisasjonen kan ta innover seg faktiske scenarioer eller plausible scenarioer som virksomheten må ha kontroll med.

Det vil alltid være noen eksterne risikoer som er helt ukjente eller nye, eller områder som mangler et tilstrekkelig data og/eller vurderingsgrunnlag, og de må behandles særskilt for å skille disse fra mer forventede risikoer i interne prosesser, systemer og organisasjon.

Noen av disse risikoområdene vil også kunne inngå i ulike forsikringsordninger fordi nedetid og ulike typer av driftsstans kan skape store økonomiske ringvirkninger i hele virksomheten.

2.2 Gjennomføre handlingsplan

I siste fase under etablering av handlingsplanen skal det lages estimater på hva som må til for å iverksette og følge opp hvert enkelt tiltak. Gjennomføring av handlingsplanens definerte og valgte tiltak kan defineres som den aktive risikostyringen.



De viktigste suksesskriteriene for dette steget er at:

- Tiltakene har konkrete, navngitte eiere som kan sikre god fremdrift i aktivitetene de har fått ansvaret for.
- Eier av et tiltak har den kompetanse, myndighet og kapasitet som er trengs for å sikre nødvendig fremdrift.

Muligheten til å skaffe seg tilstrekkelig med kompetanse, myndighet og kapasitet bør være sikret i virksomhetens overordnede policy, som blant annet fastslår roller og mandat (ref. kapittel 1 om krav til et felles rammeverk for operasjonell risikostyring).

Et klart og tydelig mandat reduserer sjansen for tvilstilfeller, uklare ansvarsområder og unødvendige konflikter i arbeidet med å gjennomføre og følge opp tiltakene i handlingsplanen.

Med utgangspunkt i tilstrekkelig kompetanse, kapasitet, mandat og myndighet skal eier av ett eller flere tiltak i handlingsplanen kunne lede og følge opp sine tiltak, herunder samle og styre nødvendige ressurser for å gjennomføre tiltakene. Det kan godt hende at flere tiltak kan settes sammen i et konkret prosjekt, med tilhørende organisering, måling og rapportering i henhold til virksomhetens egen prosjektmodell. I alle tilfeller bør tiltaksansvarlige sørge for at følgende punkter

er utført som utgangspunkt for en effektiv gjennomføring av egne tiltak i handlingsplanen:

1. Definere og kvalitetssikre forutsetninger for å levere på tiltaket, herunder sikre tilstrekkelig ramme både med hensyn til personell, kompetanse og økonomi.
2. Konkretisere hva som kjennetegner at tiltaket er gjennomført.
3. Avklare og vedta planen/tidslinjen for tiltaket, herunder organisering og eventuelle avhengigheter.
4. Sette en tidsfrist for når tiltaket skal være gjennomført.
5. Konkretisere hvem som bekrefter, eller godkjenner, at tiltaket er levert.

«Leveransen» fra dette andre steget skal være at alle avtalte tiltak enten er gjennomført som planlagt, eventuelt utsatt eller terminert som følge av at de underveis i gjennomføringen ikke lengre er vurdert som relevante eller regningssvarende.

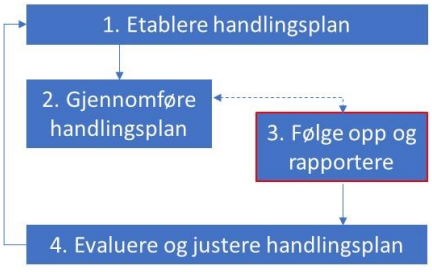
En typisk fallgruve innen risikostyring er at man ikke erkjenner eller prioriterer godt nok viktigheten av å plassere et tydelig eierskap og fordele ansvar internt. Eierskap til risikoer og de tilhørende tiltakene i handlingsplanen skal sikre realisme i egne planer vurderes og at den planlagte gjennomføringen kan følges opp. I andre omgang bidrar dette til at man ikke blir fristet til å lage en lang tiltaksliste uten å prioritere, følge opp eller validere effekt og forventet nytte.

En annen typisk fallgruve er at man undervurderer viktigheten av å diskutere, vedta og dokumentere hva som må til for faktisk å kunne levere på tiltaket. I slik tilfeller legges tiltaket inn som en ordinær linjeoppgave uten at den ansvarlige tildeles tilstrekkelige rammer for å levere, til tross for at gjennomføring av tiltaket krever særskilte ressurser for at det skal kunne gjennomføres. Dette fører gjerne til at tiltaket havner i en «kamp» med øvrige linjeoppgaver hos den som har fått ansvaret, og dermed ikke får den prioriteten det var forutsatt at det skulle ha med utgangspunkt i de identifiserte operasjonelle risikoene.

Viktigheten av å diskutere, vedta og dokumentere hva som må til for faktisk å kunne levere på vedtatte tiltak må ikke undervurderes.

2.3 Følge opp og rapportere

Dette steget handler om å følge opp i to dimensjoner/ulike nivåer:
I den ene dimensjonen handler det om å følge opp status på de avtalte tiltakene og sikre god koordinering og kommunikasjon av hvorvidt de involverte risikoeiere og tiltaksansvarlige er i rute når det gjelder gjennomføring av tiltakene i handlingsplanen.



På en måte kan dette steget sees på som en støtte til gjennomføringen av handlingsplanen, som henviser spesielt til punkt 3. i tiltaksansvarliges 5 punkter for effektiv gjennomføring av egne tiltak i kapittel 2.2 (dvs. avklare og vedta planen/tidslinjen for tiltaket, herunder organisering og eventuelle avhengigheter).

I den andre dimensjonen handler dette steget om å følge opp og rapportere på faktorer som gjør det mulig for virksomheten å evaluere og eventuelt justere grunnlaget for handlingsplanen – altså

det operasjonelle risikobildet. Dermed kan dette steget også sees på som grunnlaget for selskapets evne til å tilpasse og skreddersy den operasjonelle risikostyringen, slik at den kan gjøres så kostnadsvennlig og effektfull som mulig.

2.3.1 Følge opp og rapportere på tiltak

De viktigste suksesskriterier for dette steget er at:

- det foreligger definerte rutiner og forpliktelser for hvordan oppfølging og rapportering skal gjøres, herunder både til hvem og hvor ofte, og med hvilket innhold samt hvordan eskalering skal foregå
- det finnes en enkel samhandlingsarena/-plattform for kommunikasjon og koordinering på tvers av de som er involvert i den operasjonelle risikostyringen.

Rutiner og forpliktelser utarbeides ofte best i sammenheng med eller basert på arbeidet med prosessbeskrivelse og eventuelt konkrete og målrettede instrukser.

En tilfredsstillende samhandlingsarena/-plattform oppnås gjennom å definere faste møteplasser for gjennomgang og rapportering, gjerne støttet med et systemverktøy som er kjent for, og kan brukes, av alle involverte. Ref. kapittel 1 om krav til et felles rammeverk for operasjonell risikostyring.

Det faktum at oppfølging og rapportering er beskrevet som et eget steg indikerer at tiltak av ulike årsaker vil kunne bli forsinket eller vanskeligere å gjennomføre enn forventet eller planlagt. Det er gjerne i disse situasjonene man ser hvorvidt man har lykkes med planleggingen og tilretteleggingen av kompetanse, kapasitet, mandat og myndighet hos de tiltaksansvarlige.

En typisk fallgruve er at man ikke har sørget for å innarbeide en praksis som faktisk gjenspeiler god etterlevelse av de styrende dokumentene som ligger vedtatt. Da har man altså et teoretisk underlag i det dokumenterte rammeverket, som beskriver «slik ønsker vi å gjøre det hos oss» - mens faktisk praksis er en annen.

Ofte vises dette gjennom at tiltaksansvarlige ikke har den gjennomføringsevnen som de ifølge rammeverket skulle hatt, og/eller at man i oppfølging og rapportering ikke har med seg de rette interessentene. Dette resulterer i at tiltaksansvarlige står litt i stampe, og det er ingen enkelt tilgang på beslutningstakere som kan gripe inn for å justere tilgang på ressurser og sikre fremgang der hvor tiltaksansvarlige, til tross for innledende steg, ikke har tilstrekkelig gjennomføringsevne. For å unngå å havne i en slik situasjon er det svært viktig at det er lagt til rette for eskalering og effektiv håndtering av utfordringene med å gjennomføre tiltaket.

Det å utvikle en god avviksrapporteringkultur fra mottak til behandling er viktig for vellykket styring av operasjonell risiko, og hvis nødvendig at man endrer praksis.

2.3.2 Følge opp og rapportere på grunnlaget for handlingsplanen

Dette steget handler om å samle inn informasjon om og rapportere på forhold som gjør det mulig å evaluere og justere handlingsplanen i takt med utviklingen av virksomhetens prosesser, kontekst og trusselbilde.

Kvaliteten i handlingsplanen og dermed den operasjonelle risikostyringen blir ikke bedre enn evnen til å fange opp og utnytte informasjon om den løpende driften og den aktuelle forretningsmessige konteksten.

Et viktig suksesskriterium for dette steget er kompetanse om egen virksomhet og gjeldende trusselbilde, på samme måte som når handlingsplanen skulle etableres. Ved etablering av handlingsplanen er det viktig med kompetanse om nåsituasjonen. Under oppfølging og rapportering dreier det seg i større grad om oversikt og kompetanse knyttet til endringer i eksisterende forhold eller introduksjon av nye forhold som kan ha innvirkning på den operasjonelle risikoen. Med andre ord handler dette suksesskriteriet seg om evnen til å måle og fange opp forhold knyttet til de fire dimensjonene fysiske eiendeler, mennesker, organisasjon og teknologi.

Nedenfor er listet opp noen av de viktigste forholdene som bør vurderes inkludert i målingene:

- Oppfølging av gjennomføring av handlingsplaner og (forbedrings-)prosjekter (tiltak for å redusere risiko, ref. kapittel 2.3.1 ovenfor)
- Analyse av driftsrelaterte KPIer, kvalitets- og avviksrapporter som belyser mulige rotårsaker, herunder oppfølging av tiltak i etterkant av hendelser, gjennomgang av avviks- og kvalitetsrapporter, behandlingstid, backlogger, feilprosent, svik, svinn og andre former for misligheter, kundeklager, sykefravær, medarbeidertilfredshet mm.
- Endringer i kontekstuelle forhold f.eks. tilgang på råvarer, teknologiendringer, eksterne hendelser som naturkatastrofer, tilfeller av cyberkrim mm. Grunnlag for denne rapporteringen skal være innsikten som operasjonell risikostyringsfunksjonen bygger opp gjennom å følge med relevant media, faglige fora, uønskede hendelser internt og eksternt mv.

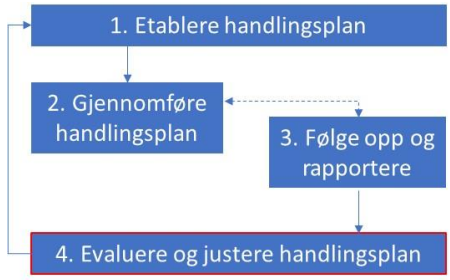
Disse kan videre konkretiseres/kategoriseres i fysiske eiendeler, mennesker, organisasjon og teknologi. En konkretisering av hva som faktisk skal måles bør være angitt i det overordnede rammeverket for operasjonell risikostyring. All informasjon fra målingene samles i en rapporteringsstruktur, som gjerne er definert av risikostyringsfunksjonen. Det viktigste med rapporteringen er at det kommer frem klart og tydelig hvilke målinger som er gjort og hva målingene betyr med hensyn til forretningens mål og tiltakene i handlingsplanen.

«Leveransen» fra dette tredje steget i denne modellen for operasjonell risikostyring skal være en dokumentert innsamling av målinger og forhold som gir grunnlag for både gjennomføringen og evalueringen av handlingsplanen.

2.4 Evaluere og justere handlingsplan

Dette steget handler om å sikre god koordinering og kommunikasjon av hvorvidt selskapet gjennom den vedtatte handlingsplanen er på rett vei når det gjelder å håndtere operasjonell risiko.

Det viktigste suksesskriteriet for dette steget er at virksomheten sikrer et godt grunnlag gjennom oppfølging og rapportering i forrige steg.



Enkelt oppsummert kan man si at dette siste steget dreier seg om å «kvalitetssikre» eller «re-etablere» handlingsplanen. Med utgangspunkt i de målinger og rapporteringer som er gjort skal man på nytt definere nåsituasjonen. Når nåsituasjonen er definert skal man vurdere hvorvidt hvert enkelt tiltak i handlingsplanen fortsatt er relevant og effektivt.

Ved å gjennomgå følgende spørsmål skal det være enklere å gjøre en målrettet vurdering av tiltakene:

- Er grunnlaget for etableringen av handlingsplanen endret? I så fall, hva er endret, og hvordan virker det inn på vår beskrivelse av våre operasjonelle risikoer?
- Er de identifiserte potensielle hendelsene i risikovurderingen fortsatt relevante, eller bør noen fjernes eller erstattes med andre mer relevante scenarioer?
- Er prioriteringen av potensielle hendelsene eller forholdene fortsatt riktig, eller bør noe endres?
- Er de kapasitetsmessige forutsetningene for å kunne håndtere de prioriterte potensielle hendelsene eller forholdene fortsatt dekket?

Fra dette steget er det en glidende overgang til første steg igjen, fordi man nå sitter med et nytt situasjons- og risikobilde - grunnlaget for handlingsplanen, samt en oppdatert handlingsplan.

Om denne publikasjonen

Dette dokumentet er utarbeidet av en arbeidsgruppe bestående av engasjerte og dyktige medlemmer. IIA Norge retter en stor takk til:

Mazhar Ahmad, Head of operational risk, Statkraft
Alf Olav Uldal, Fagleder kvalitet, Lede AS
Martin Stevens, Internrevisor, Gjensidige Forsikring
Roger Ølstad, Partner/leder cyber- og informasjonssikkerhet, Agenda Risk AS

Om IIA Norge

IIA Norge er interesseorganisasjonen for alle som arbeider med eller har interesse av god governance - med fokus på internrevisjon, risikostyring og compliance.

Formålet til IIA Norge er å gi medlemmer et solid faglig fundament og styrke kunnskapen i virksomheter om styring, kontroll og internrevisjon.

Vi har etablert faglige og aktive nettverk der erfaringsutveksling og kunnskapsdeling praktiseres. Vi har egne nettverk for finans, ledere, statlig sektor, compliance og forretningsetikk, risikostyring og IT-revisjon. Hvert nettverk består av engasjerte medlemmer fra ulike virksomheter innen spesifikke bransjer eller på tvers av bransjer. Som medlem av IIA Norge kan du delta i alle nettverk og får tilgang til verktøy og nettverksdokumentasjon. Les mer på www.iia.no.

Andre aktuelle veiledere fra IIA Norge:

- Veileder for risikostyringsfunksjonen
- Veileder for compliancefunksjonen (norsk og engelsk)
- Veileder for virksomhetsstyring (norsk og engelsk)
- Modenhetsmodell virksomhetsstyring
- Modenhetsmodell risikostyring
- Good Practice Guidelines for the Enterprise Risk Management Function
- Spørsmål et styre bør stille for å forstå hvordan en virksomhet styrer sine risikoer (norsk og engelsk)

IIA Norge administrerer også videreutdanning, sertifisering og diplomeringene:

- Diplomert internrevisor
- Certified Internal Auditor (CIA)
- Certification in Risk Management Assurance (CRMA)