Veileder for risikostyringsfunksjonen

2018 utgaven

7. november 2018

Finansnettverket IIA Norge

Hvorfor ble veilederne utarbeidet av IIA Norge?

- Bidra til profesjonalisering av 2. forsvarslinje og bl.a.:
  - Unngå dobbeltarbeid
  - Unngå "hull" i forsvarsverket
  - Bidra til en effektiv og hensiktsmessig virksomhetsstyring

- Bidra til oppnåelsen av ett av IIA Norges overordnet mål:
  - IIA Norge er interesseorganisasjonen for alle som arbeider med eller har interesse av fagområdene internrevisjon, governance (virksomhetsstyring), risikostyring, compliance og kontroll.
- Og gi internrevisorer en «benchmark» for å kunne vurdere 2. linjen opp mot

Målet med veilederen

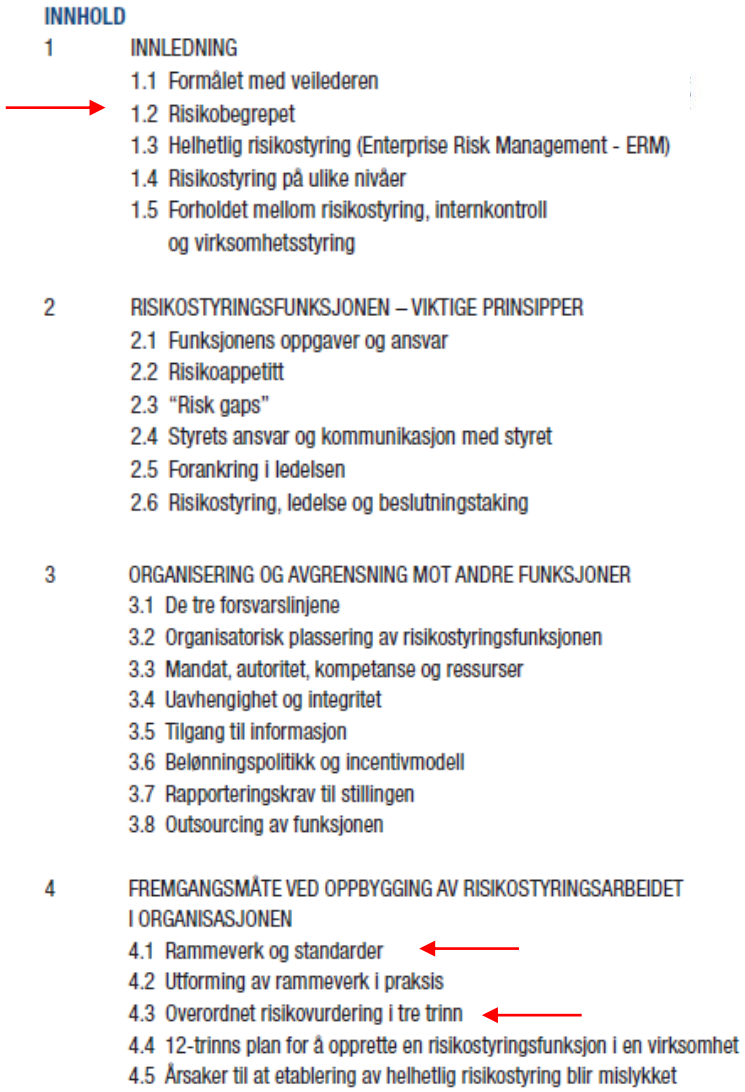
Veilederen skal beskrive gjeldende god praksis for risikostyringsfunksjoner uavhengig av bransje, regelverk og størrelse på virksomheten

Fokus på helhetlig risikostyring (ERM) i praksis og prinsipper som er gjeldende på tvers av bransjespesifikke veiledere og regulatoriske krav

- *Viktige prinsipper for risikostyring*
- *Organisering og avgrensning mot andre funksjoner*
- *Fremgangsmåte ved oppbygging av risikostyringsarbeidet i organisasjonen*

2018 oppgradering

- Ytterligere styrke koblingen mellom risikostyringsarbeidet og øvrige aktiviteter knyttet til strategiutvikling og -implementering, løpende drift og arbeid med kontinuerlig forbedring
- Tydeliggjøre at veilederen er allmenngyldig; like relevant for virksomhet med et offentlig mandat som for en rent finansielt motivert virksomhet
- Oppdatert med referanser til endelige versjoner av nye rammeverk fra COSO og ISO
- Korreksjoner i tekst og inkludering av tilbakemeldinger siden første versjon

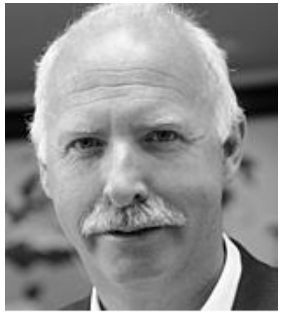


INNHOLD

Arbeidsutvalget

Martin Stevens
Gjensidige

Ayse B. Nordal
Undervisningsbygg

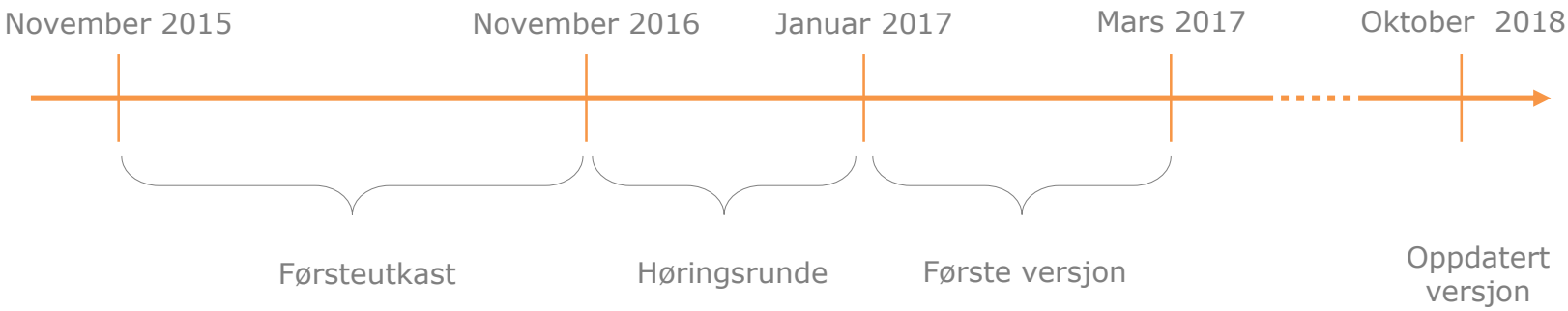


Petter Kapstad
Statoil

Ole Martin Kjørstad
Norges Bank

Prosessen

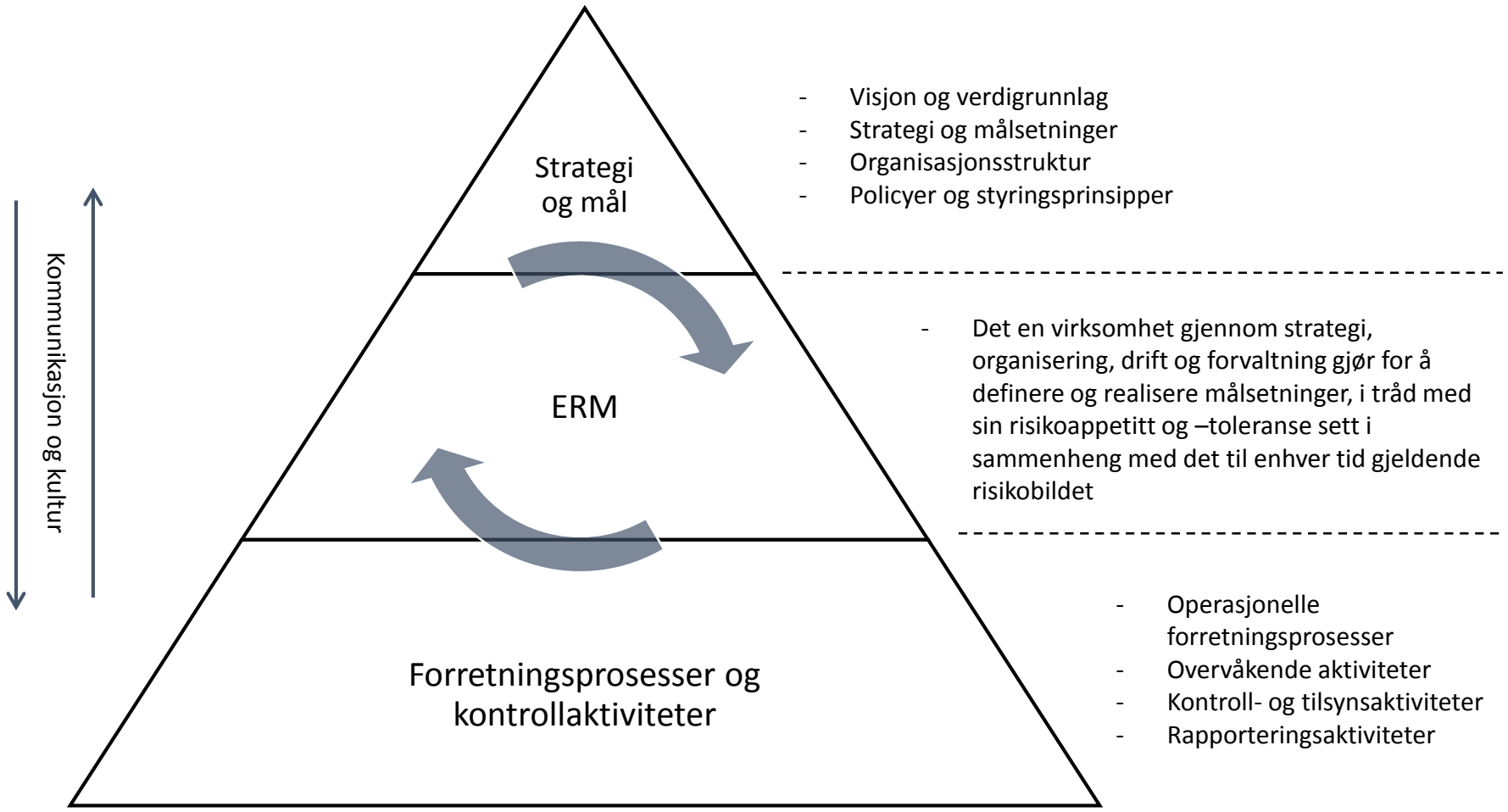
Arbeidsutvalget jobbet med veilederen gjennom 2016, og en oppdatert versjon første halvår 2018.



Innledning

Hva er helhetlig risikostyring?

Hva er helhetlig risikostyring?



- Visjon og verdigrunnlag
- Strategi og målsetninger
- Organisasjonsstruktur
- Policyer og styringsprinsipper

- Det en virksomhet gjennom strategi, organisering, drift og forvaltning gjør for å definere og realisere målsetninger, i tråd med sin risikoappetitt og –toleranse sett i sammenheng med det til enhver tid gjeldende risikobildet

- Operasjonelle forretningsprosesser
- Overvåkende aktiviteter
- Kontroll- og tilsynsaktiviteter
- Rapporteringsaktiviteter

Risikostyringsfunksjonen

Viktige prinsipper

Funksjonens oppgaver og ansvar

Veilederen fokuserer på
«risikostyringsfunksjonen»

Styret eller virksomhetens øverste organ skal «påse at» virksomheten har etablert forsvarlig risikostyring og internkontroll

Daglig leder har overordnet operativt ansvar for risikostyringen. Øvrige ledere skal sørge for forsvarlig risikostyring og internkontroll innenfor sine ansvarsområder.

Funksjonens oppgaver og ansvar

Bistå organisasjonen med å iverksette og implementere en effektiv prosess for å identifisere, vurdere og håndtere risiko.

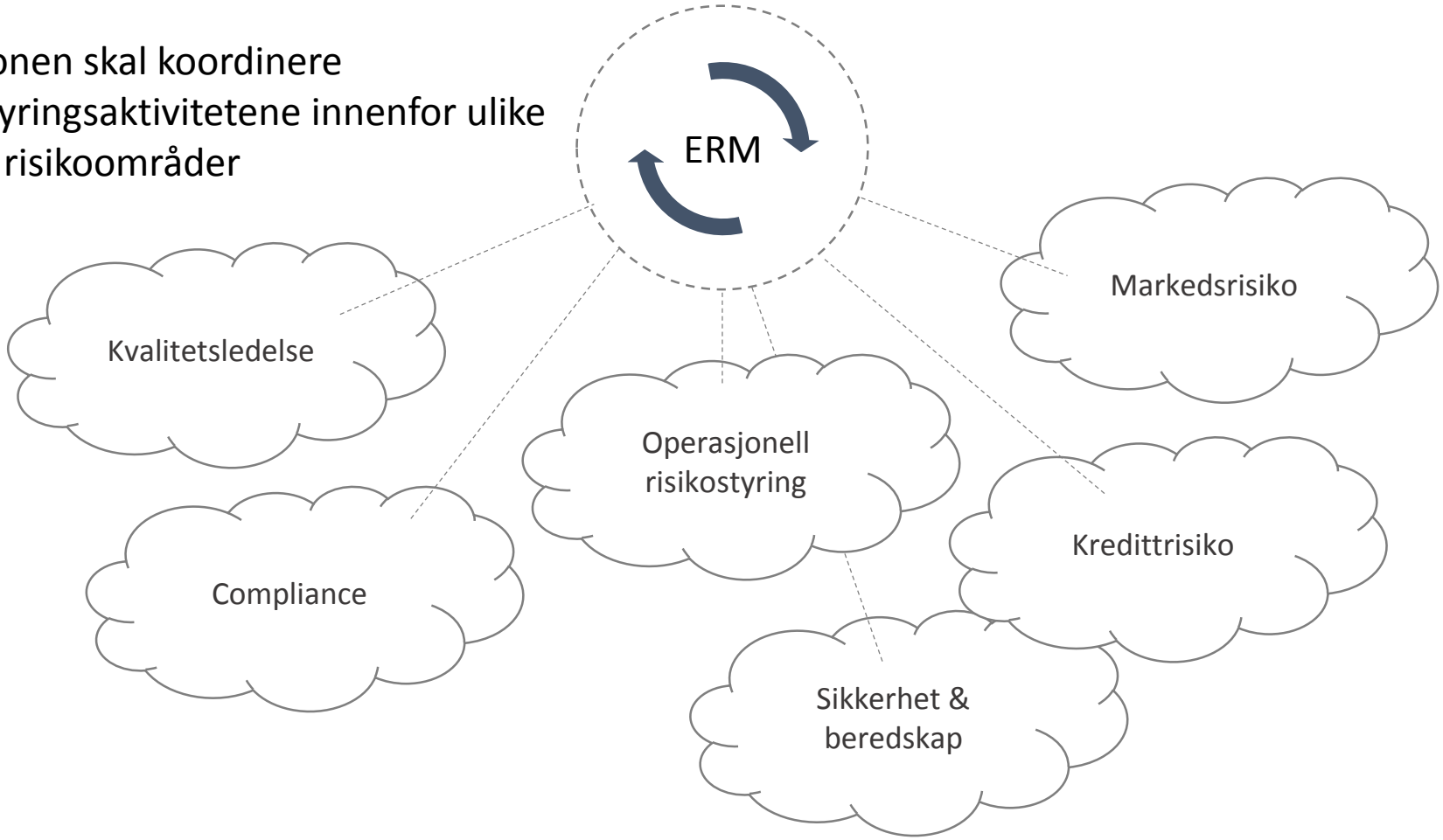
Selvstendig overvåke risikobildet

Flagge utviklingstrender for eksisterende risikoer og potensielt utfall av nye trusler/muligheter

Risikostyringsfunksjonen bør ha ansvar for å følge opp fremdriften i det samlede risikostyringsarbeidet

Funksjonens oppgaver og ansvar

Funksjonen skal koordinere risikostyringsaktivitetene innenfor ulike fag- og risikoområder



Risikoappetitt

Det nivå av usikkerhet en organisasjon er villig- og har evne til å påta seg for å kunne gjennomføre sine aktiviteter og realisere sine mål.

Risikoappetitt må kunne operasjonaliseres

Risikoappetitt handler om både *vilje* og *evne*

«Risk gaps» – misforhold mellom risiko og forventet avkastning

Ansvar og forankring

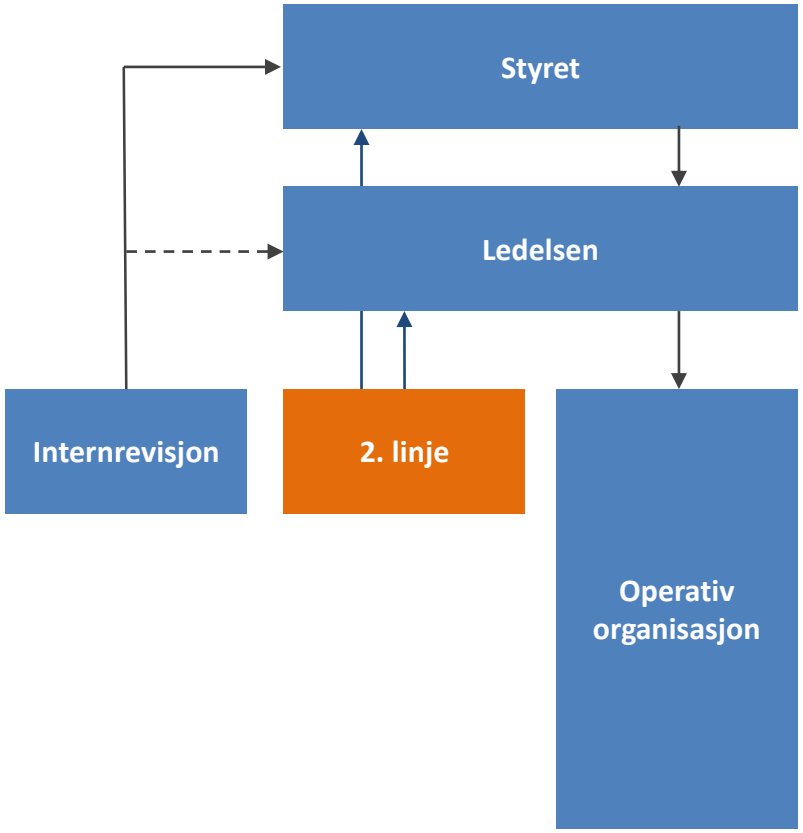
Ansvaret for virksomhetens risikostyring og internkontroll kan ikke delegeres bort fra styret og ledelsen

Det operative ansvaret for å legge til rette for, fasilitere og drive risikostyringsarbeidet er et typisk 2. linjeansvar

Risikostyring må integreres med øvrig arbeid med strategi- og handlingsplaner

Styret og ledelsen må delegere nødvendig myndighet og ansvar til ansvarlig for risikostyringsprosessen

Ansvarlig for risikostyring bør ha en direkte kanal til styret



Risikostyring og beslutningstaking

Det er usikkerhet assosiert med alle beslutninger.

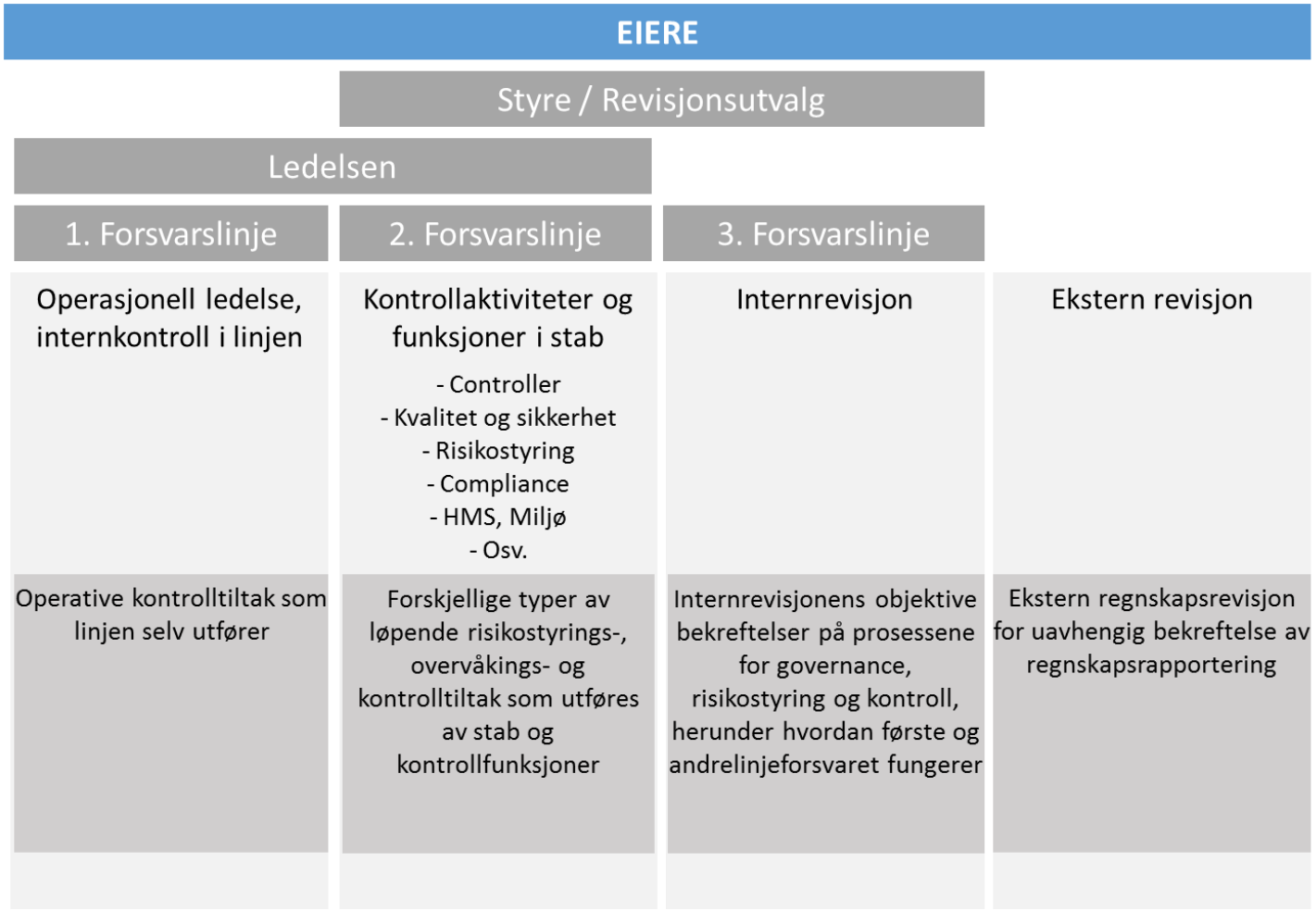
God risikostyring handler om å legge til rette for at beslutninger fattes på best mulig grunnlag.

Bedre beslutningsgrunnlag kan også styrke evnen til å håndtere et utfall som i utgangspunktet ikke var ønsket.

Organisering

Og avgrensning mot andre funksjoner

De tre forsvarslinjene

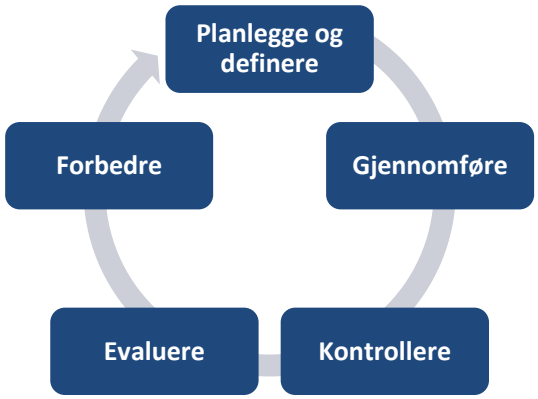


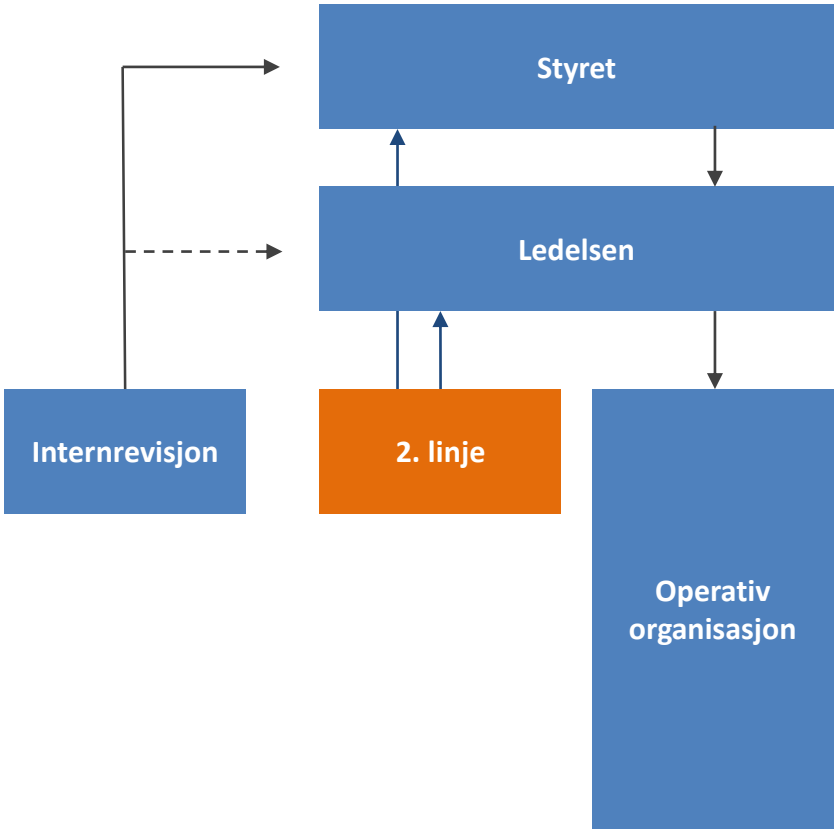
Andrelinjen

Dels *proaktivt* og dels *reaktivt* mandat.

Bidra til utvikling og forvaltning

Rapportere og aktivt identifisere avvik fra ønsket utvikling





Organisatorisk plassering og mandat

Organisatorisk plassering av risikostyringsfunksjonen vil avhenge av virksomheten og modenhetsnivået for helhetlig risikostyring i organisasjonen.

- *Separat stabsenhet med rapportering til toppledelse og styret*
- *Samordnet med andre risiko- og kontrollfunksjoner*
- *Forankret i annen rollebeskrivelse*

Uavhengig av organisering, må funksjonen tilordnes tilstrekkelig ***mandat, autoritet, kompetanse og ressurser***

Autoritet, kompetanse og ressurser

Husk at risikostyring er en profesjon som krever faglig kompetanse samt relevant bakgrunn og erfaring

En faglig karrierestige vil bidra positivt til utvikling av individet og funksjonen

Andre viktige forutsetninger

- Uavhengighet og integritet
- Outsourcing

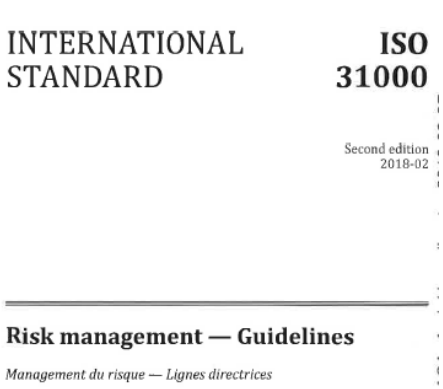
Oppbygging av risikostyringsarbeidet

Fremgangsmåte

Rammeverk og standarder

Veilederen har ikke som mål å beskrive et spesifikt eksempel på benyttet metodikk og hvordan man kan organisere risikostyringsarbeidet.

To standarder / rammeverk har oppnådd internasjonal aksept og er oversatt til norsk.



Utforming av rammeverk i praksis

En fellesnevner for eksisterende standarder og rammeverk er at det omfatter metoder og prosesser som brukes av organisasjonen til å styre risiko og utnytte muligheter.

Typiske elementer i et rammeverk:

- Identifikasjon av interne og eksterne forhold som påvirker virksomhetens målsetninger
- Fastsettelse av risikoappetitt og risikostyringspolitikk
- Utforming av risikostyringsfunksjonen og funksjonens ansvarsområder
- Etablering av interne og eksterne kommunikasjonsmekanismer
- Tildeling av ressurser til funksjonen

12 trinn for implementering

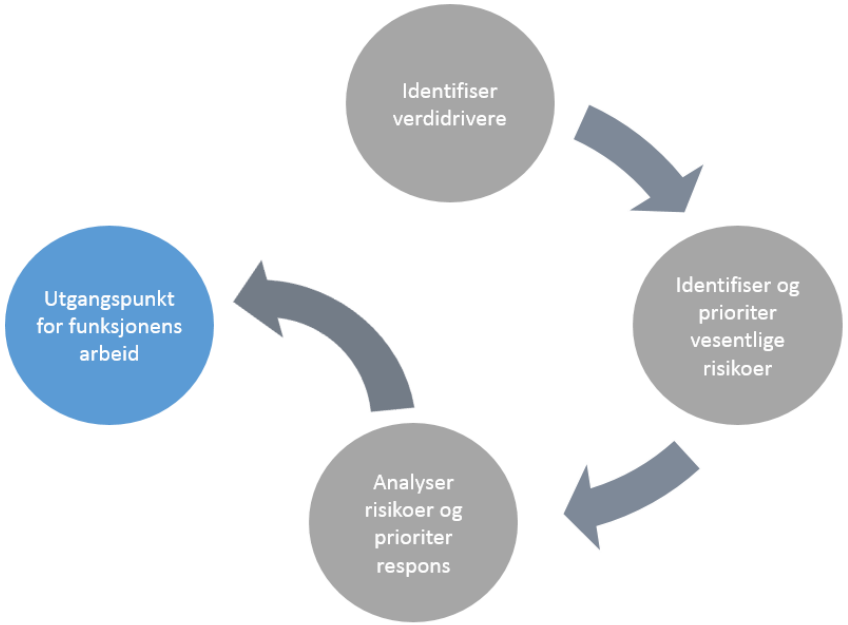
1. Utarbeide mandat og stillingsbeskrivelse, definere roller og rapporteringslinjer
2. Ansette leder for risikostyringsfunksjonen
3. Fastsette policy for implementering av risikostyring
4. Se til at ERM-funksjonen dekker alle typer risiko
5. Styret og ledelsen må definere risikoappetitten
6. Kommunisere implementeringsplan til organisasjonen
7. Definere karrierestige for risikostyring
8. Vurder å etablere Risk Managers i linjen
9. Sørg for regelmessig kommunikasjon og rapportering knyttet til risikoeksponering
10. Kommunikasjon vedrørende risiko må være proaktiv og risikoeierskap må allokeres
11. Arbeidsformen må sikre tett samarbeid med strategi- og linjefunksjoner
12. Årlig / periodisk rapportering til styret

Overordnet risikovurdering

4.3 Overordnet risikovurdering i tre trinn

En virksomhet som aldri tidligere har foretatt en overordnet risikovurdering kan gjøre dette gjennom en enkelt tre-trinns prosess (se illustrasjon figur 7):

1. Identifisere og definere virksomhetens verdidrivere. Det vil si, spørre seg «hvorfor eksisterer denne virksomheten, og hva påvirker måloppnåelsen i positiv og negativ retning?» I denne sammenheng kan verdi være et vidt begrep. Det kan omfatte eksempelvis liv og helse eller oppfyllelse av et offentlig mandat, like fullt som kostnader og verdsettelse i kroner og øre.
2. Identifisere, evaluere og analysere vesentlig usikkerhet som kan påvirke verdidriverne. Dette omfatter både de elementene som kan føre til bedre utfall enn forventet og et dårligere utfall. Det skal vurderes hvilke av disse risikoer som anses som vesentlige og som skal styres aktivt. For alle risikoer bør det vurderes om de skal styres (aktivt håndtere og følge opp), deles (dele risikoeksponering med en annen part eller gjennom forsikring) eller unngås (endre operativ drift eller fullt ut forsikre en risiko). Som del av det å styre en risiko, kan bevisst økt risikoeksponering også være et alternativ.
3. Usikkerheten kan kvantifiseres i form av sannsynlighet og konsekvens, og bør være med på å danne grunnlag for arbeidsoppgavene til Risikostyringsfunksjonen (se 4.4). Ved bruk av en slik skala, må det tydelig defineres hva som menes med de ulike nivåene av sannsynlighet og konsekvens. Herunder må konsekvensskalaen defineres for relevante kategorier, eksempelvis økonomi, måloppnåelse, HMS og omdømme. Sannsynlighet må kunne vurderes også for usikkerhet som ikke historisk kan beregnes, gjennom en kvalitativ vurdering av hvor sannsynlig det er at en situasjon oppstår fremover i tid. Virksomhet som ikke måler sin måloppnåelse i kroner og øre, bør definere intervaller for konsekvens som knyttes opp mot grad av konsekvens for sine mål/mandater.



Årsaker til at etablering mislykkes

- Uklar visjon, manglende verdigrunnlag og dårlig formulerte strategier
- Manglende kobling mellom strategiske mål og risikostyring
- Uklart mandat og manglende forståelse for ansvarsfordeling
- Ansvarlig med manglende generell risikostyringskompetanse og strategisk forståelse
- Manglende helhetlig fokus
- Manglende eierskap til systemverktøy
- Verktøy benyttes uten at begrensninger er tatt hensyn til
- Kultur som ikke legger til rette for åpenhet
- Manglende prioritering av vesentlige risikoer
- Manglende forståelse for samvariasjon mellom risikoer
- Manglende styring og oppfølging av IT-risiko
- Manglende fokus på utvikling og endring i risikobildet
- Manglende forankring og forståelse for nytte av risikostyringsarbeidet i organisasjonen
- Uklar organisering og ansvarsdeling mellom risikostyringsfunksjonen og risikoeiere
- Usunn konkurranse (profesjonskrig) mellom beslektede funksjoner
- Mangelfulle risikoanalyser og analyser basert på svake eller ikke beskrevne forutsetninger
- Manglende kvalitetssikring av analyser
- Manglende helhetlig fokus i rapportering og ulike formater/premisser for risikovurderinger som hindrer aggregering

Kontakt, kurs og fagmateriell

- Vi ønsker engasjement, innspill, artikkelforfattere, bidragsytere mm. Mailadresse: risikostyring@iia.no
- Vi planlegger møteplasser, kurs og konferanser
  - **Risikostyring roundtable** 20.11.18 Risikoappetitt
  - **GRC seminar** 13.02.19
  - **Kurs for videregående** 29.02.19
- Se vår webside https://iia.no/risikostyring/ og ERM modenhetsmodellen https://iia.no/risikostyring/publikasjon/modenhetsmodell-risikostyring/