Risikostyring & internkontroll med fokus på verdiskaping for selskapet

VFF Complianceseminar

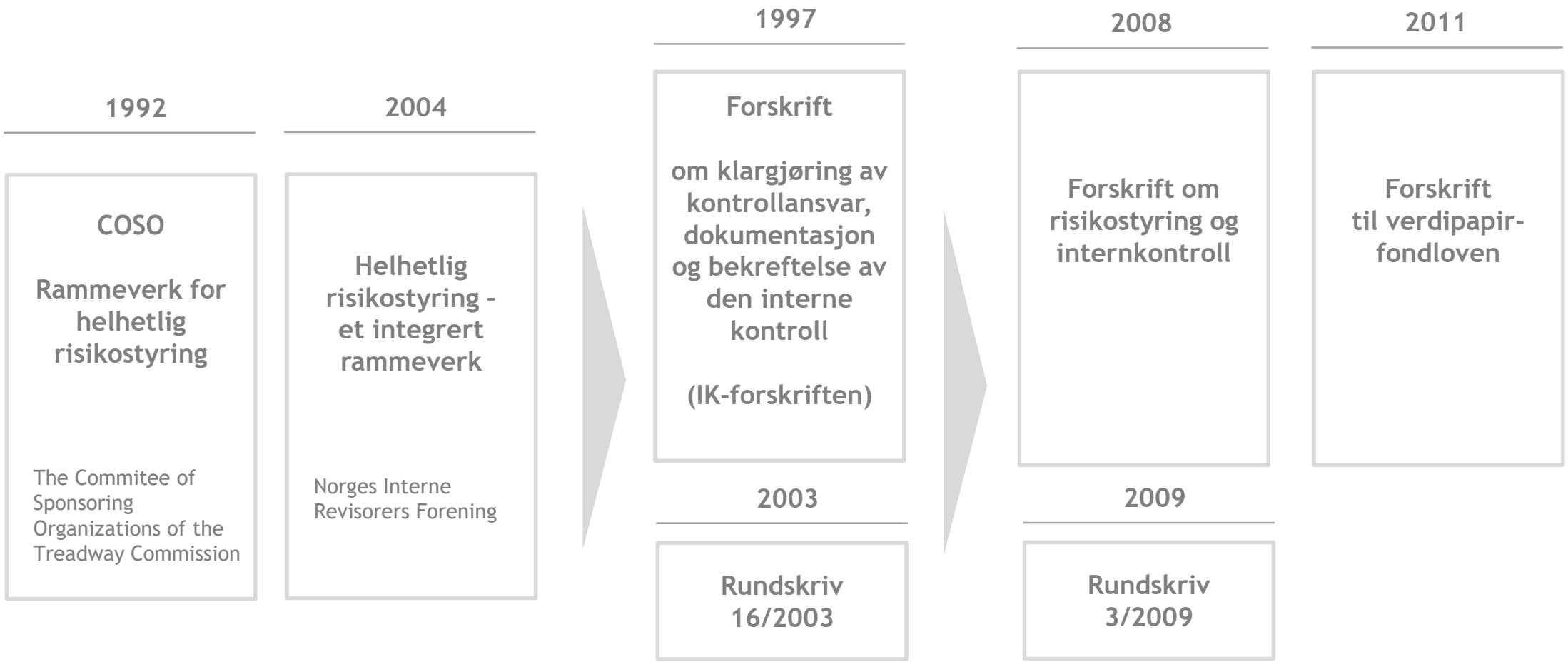
24. november 2016

AGENDA

1. Rammeverk for helhetlig risikostyring
2. Risikostyring og internkontroll
3. Verdipapirfond- og risikostyringsforskriften
4. Styrets og ledelsens ansvar
5. Løpende vurdering
6. Dokumentasjonskrav og rapportering

Rammeverk for helhetlig risikostyring

Prinsippene i COSO sentralt for bestemmelsene i dagens lover og forskrifter knyttet til risikostyring og internkontroll



Utgangspunkt for utarbeidelse av prinsippene i COSO

Forutsetninger

1. Enhver virksomhet eksisterer for å skape verdier for sine interessenter
2. Alle virksomheter står overfor usikkerhet
3. Utfordringen for virksomhetene er å avgjøre hvor mye usikkerhet den skal akseptere i sin streben for å skape verdier for sine interessenter

Verdiskaping

Maksimal verdiskaping oppnås når virksomhetene

- fastsetter strategi og målsettinger
- slik at det er optimal balanse mellom vekst- og lønnsomhetsmål
- og relaterte risikoer,
- og utnytter ressursene målrettet og kostnadseffektivt

for å nå virksomhetens mål.

Rammeverk for helhetlig risikostyring (COSO)

Helhetlig risikostyring innebærer:

- Å samordne risikoappetitt og strategi
- Å forbedre beslutninger angående risikohåndtering
- Å redusere driftsrelaterte overraskelser og tap
- Å identifisere og håndtere sammensatte risikoer og risikoer som gjelder på tvers av virksomheten
- Å utnytte muligheter
- Å forbedre utnyttelse av kapital

Risikostyring og internkontroll som en del av virksomhetsstyringen

Helhetlig virksomhetsstyring

Strategi og målsettinger

Risikostyring og internkontroll

Organisering, roller og ansvar

Samfunnsansvar

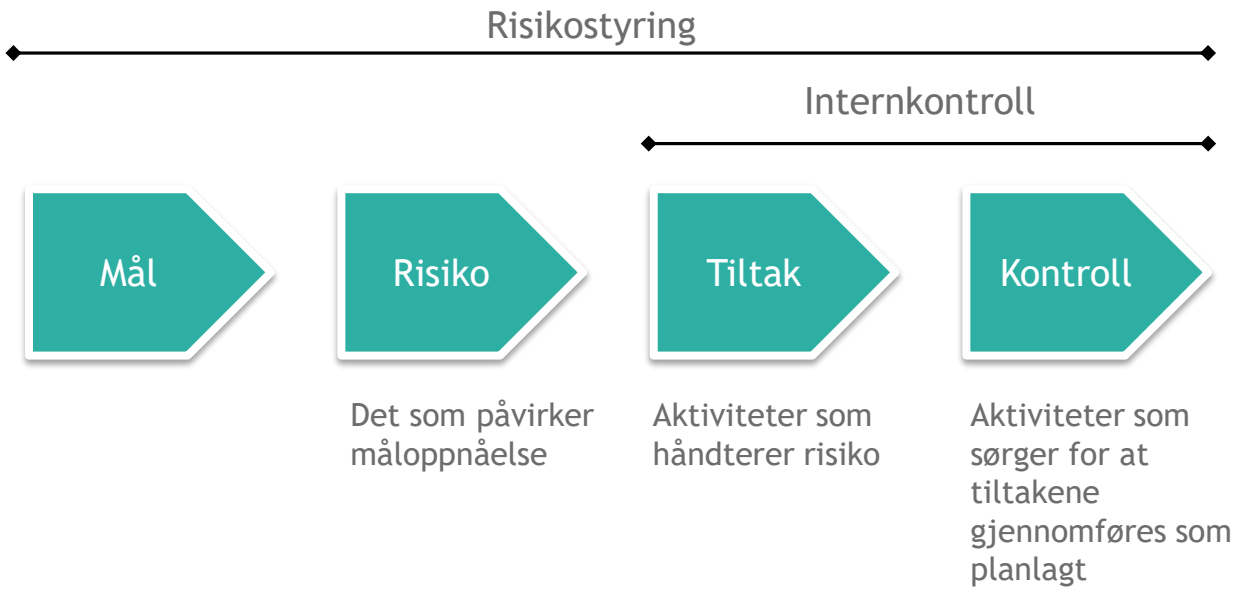
Kvalitet og kontinuerlig forbedring

Personalutvikling og insentiver

Måling og rapportering

Risikostyring og internkontroll

Risikostyring og internkontroll



Finanstilsynet om risikostyring

“ Foretakets risikostyring er hva foretaket gjennom strategi, organisasjon, rutiner og forsvarlig drift gjør for å nå fastsatte mål og sikre sine og kundenes verdier, samt pålitelig rapportering og etterlevelse av lover og regler. Dette innebærer mer enn det som tradisjonelt har vært oppfattet som internkontroll. ”

Kilde: Kredittilsynets veiledning til forskrift om risikostyring og internkontroll (Rundskriv 3/2009)

Verdipapirfondsforskriften og risikostyringsforskriften

Hvilke krav stilles i lovgivningen?

Forskrift om risikostyring og internkontroll

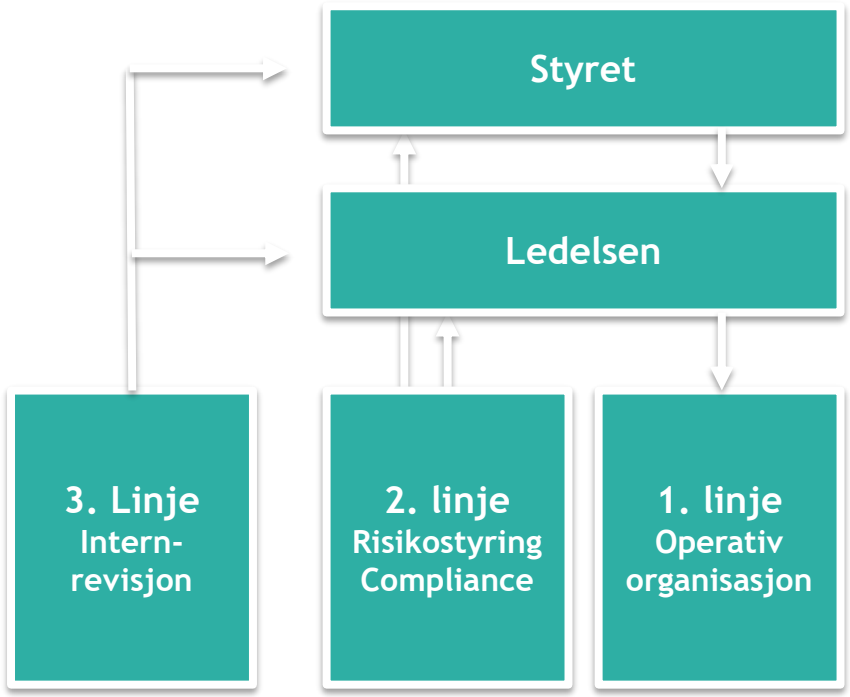
- Stiller krav til styret og ledelsen
- Ingen klare krav til organisering av foretaket
- Krav til årlig oppsummering fra daglig leder til styret
  - Skal oppsummere det løpende internkontrollarbeidet og evt. avdelingslederes vurderinger
- Fremmer forholdsmessighet
- Er foreslått opphevet for flere virksomheter ved innføring av Finansforetaksloven, men er foreslått videreført for verdipapirforetak

Forskrift til verdipapirfondloven

- Organisering: krav om risikostyrings- og compliancefunksjon samt internrevisjon (kan ligge i linjen)
- Detaljerte krav til foretakets styring og kontroll
- En detaljering av risikostyringsforskriften
- Fremmer forholdsmessighet

Styrets og ledelsens ansvar

Ansvar for risikostyringsprosessen



- 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
- Loven åpner for at ansvaret legges til linjen «dersom foretaket kan godtgjøre at kravet ikke står i rimelig forhold til virksomhetens art, omfang og kompleksitet og kontrollfunksjonen allikevel forblir effektiv»

Hvorfor styret skal involvere seg i risikostyringen?

Krav om at styret påser:

- At risikostyring og internkontroll gjennomføres i tilstrekkelig omfang og på en systematisk og effektiv måte
  - Tilpasset driften
  - Praktisk og oversiktlig form
- Etablering og gjennomføring av tiltak for å korrigere eller redusere avvik avdekket i interne kontroller
- Etterlevelse av rammebetingelser
- Tilrettelegger for tilsyn fra Finanstilsynet
- Vurdere og regelmessig gjennomgå de retningslinjer, tiltak og rutiner
- At ansvarlige for kontrollfunksjoner har nødvendig autoritet, ekspertise, ressurser og tilgang til relevant informasjon

Verdien ligger i:

- ✓ Bevisstgjøring rundt hvilke risikoer som ligger i selskapet
- ✓ Bedre beslutningsgrunnlag ved fokus på måloppnåelse
- ✓ Bedre forståelse av verdidrivere
- ✓ Redusere negative overraskelser
- ✓ Utnytte muligheter
- ✓ Samordne risikoappetitt og strategi

Hva bør et styre forvente av daglig leder?

RISIKOSTYRINGSPROSESSEN

- Løpende engasjere seg i den overordnede risikovurderingen og bruke informasjonen aktivt
- Aktivt vurdere om styrings- og kontrollapparatet er forsvarlig
- Følge opp at eventuelle linjeledere deltar aktivt
- Systematisk identifisering, vurdering og oppfølging av tiltak, herunder allokering av ressurser
- Gjennomfører vurderinger etc. innenfor sitt ansvarsområde (det er ikke tilstrekkelig kun å bygge på eksempelvis complianceavdelinger eller internrevisjonens konklusjoner)

RAPPORTERING

- I tråd med styrets prinsipper og legge til rette for at styret kan utføre påse-ansvaret
- Utgangspunkt: mål og strategier fastsatt av styret
- Restrisiko skal være i tråd med styrets risikoapetitt
- Tiltak som skal iverksettes bør følges opp med en handlingsplan med tydelig ansvar og frister
- Jevnlig rapportere status tiltak/handlingsplaner til styret

Løpende vurdering

RISIKOSTYRINGSFUNKSJONEN SKAL:

- Vurdere markeds-, likviditets- og motpartsrisiko samt all annen vesentlig risiko, herunder operasjonell risikorisiko, i fondene
- Gi styret råd om identifisering av risikoprofil for hvert verdipapirfond som forvaltes
- Rapportere regelmessig til styret om samsvaret mellom aktuelt risikonivå for hvert verdipapirfond og fastsatt risikoprofil, overholdelse av risikogrenser og om risikostyringen er tilstrekkelig og effektiv
- Rapportere regelmessig til foretakets ledelse om gjeldende risikonivå for hvert verdipapirfond og eventuelle avvik fra risikogrenser slik at det raskt kan foretas nødvendige tiltak, og gjennomgå og eventuelt bistå i etableringen av system og rutiner for verdsettelse av unoterte derivater
- Plikter og ansvar knyttet til verdsettelsen

COMPLIANCEFUNKSJONEN SKAL:

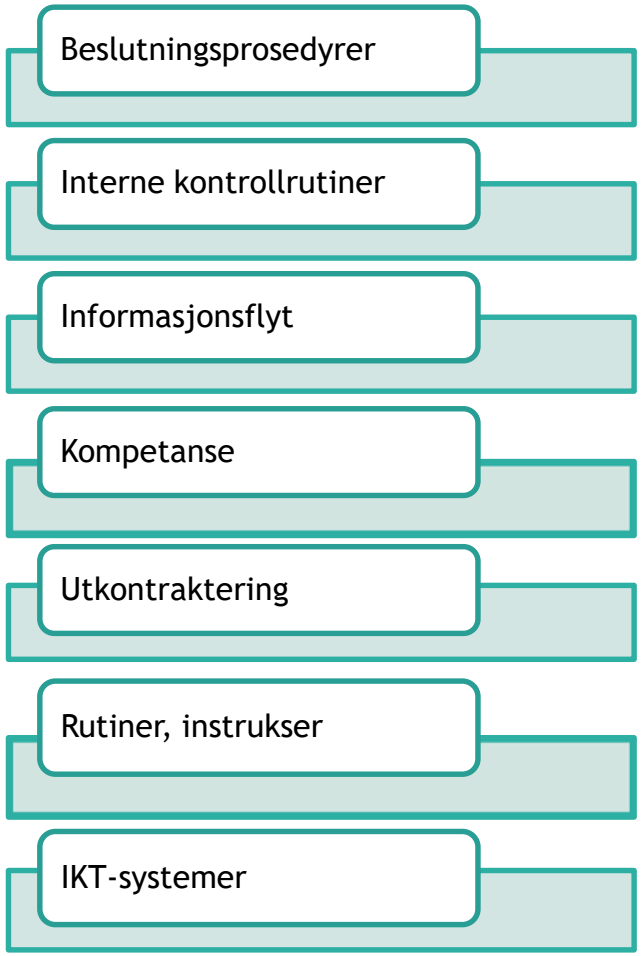
- Bidra til å redusere etterlevelsesrisiko ved å kontrollerer etterlevelse og tilrettelegger for eventuelle tilsyn
- Vurdere om tiltak, retningslinjer og rutiner for å sikre etterlevelse er tilstrekkelig effektive
- Gi råd og veiledning etter verdipapirfondloven til foretakets ledelse, ansatte og andre som utøver virksomhet på vegne av foretaket

INTERNREVISJONEN SKAL:

- Vurdere om foretakets systemer, internkontroll og ordninger er tilstrekkelige og effektive
- Gi råd og innsikt på bakgrunn av vurderingene
- Følge opp at anbefalinger og tiltak implementeres i henhold til planer
- Rapportere til styret

Rapportering og dokumentasjonskrav

VERDIPAPIRFONDFORSKRIFTEN §2-6 DOKUMENTASJONSKRAV



- Krav til skriftlighet i strategi, styreinstruks, policies, rutiner (med ansvarliggjøring ved brudd) organisasjonskart (med rapporteringslinjer) og stillingsinstrukser. Prinsipper for styring og kontroll bør foreligge.
- Rutiner bør inneholde beskrivelse av nøkkelkontroller. Dokumentasjon av internkontroll, eksempelvis fullmaktsmatriser, må foreligge.
- Opp- og nedstrømsinformasjon er avgjørende for internkontrollmiljøet, og dokumenteres ved rapportering.
- Retningslinjer for ansettelser, konkurransedyktige betingelser, opplæringsprogram etc.
- SLAer med rapporteringsfrekvens og -art tilpasset oppfølgingen (for eksempel jevnlig drifts- og avviks-/ hendelses-rapportering fra leverandør), innhenting av uttalelse internkontroll, egnethetsvurdering, krav til leverandører etc.
- Rutiner for regnskapsføring, instrukser for ansattes styreverv,
- Rutiner for informasjonshåndtering, herunder beredskapsplaner for kontinuitet i IT-systemer

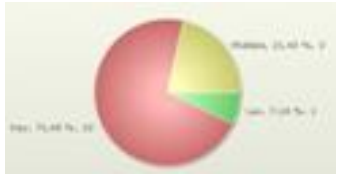
HVA BETYR DOKUMENTASJONSKRAVENE I PRAKSIS?

- Internkontroll krever ryddighet og et gjennomtenkt system
  - Synliggjøres for tilsynsmyndighetene ved (skriftlig) dokumentasjon
  - Ajourhold er en vanlig utfordring, bør gjøres årlig
  - Retningslinjer kan samles i ett styringsdokument

- Intern konsistens
  - Strategier og policies bør være utgangspunkt for vurdering og rapportering
  - Utgangspunkt i mål
  - Vesentlige risikoer identifisert bør som hovedregel være gjenstand for regelmessig vurdering
  - Tilbakeblikk på tidligere perioder
    - NB: Bør tilgjengeliggjøres i rapporteringen til styret

- Risikoanalyse og handlingsplaner
  - Bør ajourholdes og følges opp gjennom året
    - Beslutningsgrunnlag

HVORDAN DOKUMENTERE RISIKOVURDERINGEN?



- Ansvarlig/berørt enhet/avdeling
- Målsetning
- Hendelse/usikkerhet
  - Kan medføre at målsetningen ikke nås dersom hendelsen inntreffer
- Sannsynlighet for at hendelsen inntreffer og konsekvensen dersom den gjør det
  - Kan defineres kvantitativt
  - Representerer iboende risiko
- Eksisterende tiltak
  - Rutiner og tiltak for å minke sannsynligheten for at hendelsen inntreffer og eventuelt også konsekvensen av hendelsen
- Gjenværende risiko
  - Basert på vurdering av sannsynlighet og konsekvens
- Eventuelle tiltak for å håndtere risikoen
  - Frist for oppfølging
  - Ansvar internt

TAKK FOR OPPMERKSOMHETEN

john.christian.lovaas@bdo.no
mob + 47 982 06 999