FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Modul for evaluering av intern virksomhetsstyring

DATO:
15. DESEMBER 2021

FINANSTILSYNET
Postboks 1187 Sentrum
0107 Oslo

Innhold

1 INNLEDNING

1.1 Innhold og formål med modulen

Intern virksomhetsstyring omhandler prinsipper, retningslinjer, verktøy, metoder og prosesser som er forbundet med å vedta et foretaks mål, strategier og styring av risikoer. Det inkluderer hvordan foretakets virksomhet er organisert, hvordan ansvar og fullmakter er definert og fordelt, hvordan rapporteringslinjer er satt opp og hvilken informasjon de formidler samt hvordan systemet for internkontroll er organisert og implementert. Det omfatter også godtgjørelsesordninger, IKT-systemer, utkontraktering og forretningsmessig krise- og beredskapshåndtering. Risiko for hvitvasking og terrorfinansiering samt ESG-risikoer må vurderes i relevante deler av foretakets virksomhet og tas tilstrekkelig hensyn til i foretakets system for styring og kontroll.

Finanstilsynet benytter moduler som arbeidsverktøy ved stedlig tilsyn og ved vurderingen av foretakenes samlede risiko og kapitalbehov, SREP (supervisory review evaluation process). Dette dokumentet utgjør veiledningen for vurdering av foretakets overordnede styring og kontroll. I vurderingene ser Finanstilsynet hen til kompleksiteten og omfanget av virksomheten (proporsjonalitetsprinsippet).

Dokumentet er delt inn i ulike kapitler. Hvert delkapittel inneholder momenter Finanstilsynet legger vekt på ved vurdering av foretakene. Vurderingsmomentene bygger på lov eller forskrift, Finanstilsynets rundskriv og internasjonale anbefalinger. Enkelte vurderinger er basert på Finanstilsynets erfaringer og observasjoner av beste praksis, herunder erfaringer fra tematilsyn.

Med utgangspunkt i momentene som følger av denne modulen, skal faktisk status for foretaket samt Finanstilsynets vurderinger, spørsmål og konklusjoner oppsummeres i et hjelpeskjema. Finanstilsynets interne vurderinger av status for foretakets styring av virksomheten skal oppsummeres i en fire-delt gradering. Finanstilsynet benytter karakterer fra 1 til 4, som representerer beskrivelsen "god", "tilfredsstillende", "mindre tilfredsstillende" og "ikke tilfredsstillende". Klassifiseringen og hjelpeskjemaet benyttes ikke for ekstern kommunikasjon.

1.2 Relevante referanser

Lover og forskrifter

- Lov om finansforetak og finanskonsern (finansforetaksloven)
- Forskrift om finansforetak og finanskonsern (finansforetaksforskriften)
- Forskrift om kapitalkrav og nasjonal tilpasning av CRR/CRD IV (CRR/CRD IV-forskriften)
- Lov om revisjon og revisorer (revisorloven)

Rundskriv

- Rundskriv 1/2020: Vurdering av egnethetskrav
- Rundskriv 2/2020: Godtgjørelsesordninger i finansforetak og verdipapirforetak
- Rundskriv 3/2020: Veiledning om utkontraktering
- Rundskriv 10/2019: Finanstilsynets retningslinjer for gjenopprettingsplaner
- Rundskriv 12/2016: Finanstilsynets praksis for vurdering av risiko og kapitalbehov

Internasjonale retningslinjer og anbefalinger (bl.a. EBA og Baselkomiteen)

- EBA GL on internal governance under CRD (EBA/GL/2021/05)*
- EBA GL on the assessment of suitability of key persons under CRD (EBA/GL/2021/06)*
- EBA GL on sound remuneration policies under CRD (EBA/GL/2021/04)*
- EBA GL on supervisory review and evaluation process (EBA/GL/2018/03)
- EBA GL on outsourcing arrangements (EBA/GL/2019/02)
- EBA GL on communication between CA and statutory auditor (EBA/GL/2016/05)
- EBA Report on management and supervision of ESG risks for credit institutions and investment firms (EBA/REP/2021/18)
- Baselkomiteen: Corporate governance principles for banks – 2015
- Baselkomiteen: Principles for effective risk data aggregation and risk reporting – 2013
- Baselkomiteen: Compliance and the compliance function in banks – 2005
- Baselkomiteen: The internal audit function in banks – 2012
- Financial Stability Board (FSB): Principles for an effective risk appetite framework – 2013

* EBA har vedtatt nye GLs som trer i kraft 31.12.2021.

Annet

- Den norske anbefalingen om eierstyring og selskapsledelse (NUES)

2 FORHOLDSMESSIGHET

Kravene til forsvarlig virksomhetsstyring i relevant regelverk gjelder, med noen unntak, for alle banker, kredittforetak og finansieringsforetak. Styrings- og kontrollordningene samt retningslinjer og rutiner skal etter finansforetaksloven § 13-5 (3) imidlertid være tilpasset risikoen ved og omfanget av virksomheten i foretaket. Foretakenes retningslinjer, rutiner, metoder og verktøy for å styre og overvåke risiko i virksomheten skal være tilpasset foretakets størrelse, forretningsmodell og virksomhetsområder samt risikoprofil.

Forhold som bør hensyntas når omfang og utforming av foretakets vedtatte og implementerte styringsmekanismer skal vurderes er blant annet:

- foretakets samlede forretningskapital,
- geografisk utbredelse, forretningsmodell og type kunder som betjenes,
- foretakets eierstruktur, herunder om det inngår i et finanskonsern,
- foretakets finansieringsstruktur,
- om foretaket anvender godkjente internmodeller for beregning av kapitalkrav,
- type konsesjonsbelagte aktiviteter og tjenester samt kompleksiteten i produkter og kontrakter som tilbys av foretaket,
- i hvilket omfang foretaket har utkontraktert drift av IKT-løsninger og andre deler av virksomheten, herunder bruk av eksterne distribusjonskanaler.

3 STYRETS OG DAGLIG LEDERS ANSVAR FOR STYRING OG OVERVÅKING

Formålet med dette kapittelet er å vurdere styrende dokumenter og styringsprosesser som er etablert for at styret og daglig leder kan etterleve ansvaret og rollen med å styre og overvåke virksomheten i foretaket. Videre vurderes i hvilken grad foretaket har etablert tilstrekkelige retningslinjer og rutiner for å etterleve krav til egnethetsvurderinger av nøkkelpersonell. Se også om særskilte forventninger til styret eller daglig leder i modulene for de enkelte risikotypene.

3.1 Styret

Etter finansforetaksloven § 8-6 (1) hører forvaltningen av foretaket under styret. Styret er ansvarlig for å påse at virksomheten organiseres og drives forsvarlig i tråd med krav i finansforetaksloven kapittel 13 I og II. Kravene til forsvarlig virksomhet og god forretningsskikk innebærer også at styret setter en tydelig tone for hva som er forventet og akseptable adferd for alle ledere og øvrige ansatte i foretaket. Se herunder kapittel 5 om blant annet risikokultur. Styrets rolle knyttet til foretakets system for risikostyring og internkontroll er utdypet i CRR/CRD IV-forskriften § 35. I overvåkingen av virksomheten er det viktig med en åpen dialog der styret konstruktivt utfordrer forslag og beslutninger fra den daglige ledelsen. For å vurdere styrets utøvelse av styring og overvåking av virksomheten følger nedenfor aktuelle momenter:

- Styret må kjenne foretakets juridiske og operasjonelle organisasjonsstruktur, herunder ha oversikt over utkontraktert virksomheten og andre avtaler med tredjeparter som er kritiske for foretakets virksomhet.
- Forretnings- og risikostrategier, risikoappetitt og -rammer samt overordnede planer, retningslinjer og instrukser som er tilpasset virksomheten skal vedtas og jevnlig revideres av styret.
- Styret skal overvåke og styre finansforetakets samlede risiko, og jevnlig vurdere om foretakets styrings- og kontrollordninger er tilpasset risikonivå og omfang av virksomheten.
- Styret skal holde seg oppdatert om foretakets økonomiske stilling og påse at dets virksomhet, regnskap og formuesforvaltning er gjenstand for betryggende kontroll, herunder sikre seg tilgang til risikoinformasjon og fastsette omfang, format og frekvens på rapporteringen.
- Styret skal fastsette instruks for den daglige ledelse og følge opp at daglig ledelse gjennomfører strategien i tråd med styrets vedtak, at retningslinjer etterleves samt at daglig leder regelmessig gir styret informasjon om foretakets virksomhet, stilling og resultatutvikling.
- Styret skal fastsette retningslinjer for internrevisjonen, jf. finansforetaksloven § 8-16 annet ledd og årlig godkjenne funksjonens ressurser og planer, jf. CRR/CRD IV-forskriften § 40.
- Styret skal sørge for at uavhengige kontrollfunksjoner kan ivareta sine arbeidsoppgaver på en effektiv og uavhengig måte.
- Styret må fastsette prinsipper og overordnede retningslinjer for hvordan utkontraktering skal skje, og hvordan utkontraktert virksomhet skal følges opp og overvåkes, jf. rundskriv 3/2020 kapittel 8. Se også om utkontraktering i modul for operasjonell risiko.
- Styret skal fastsette og sørge for at foretaket til enhver tid har og praktiserer retningslinjer og rammer for en godtgjørelsesordning som skal gjelde for hele foretaket og eventuelle datterforetak, jf. finansforetaksforskriften § 15-2.
- Styret skal iverksette de undersøkelser det finner nødvendig for å kunne utføre sine oppgaver.
- Styret skal minimum årlig evaluere sitt arbeid og sin kompetanse knyttet til foretakets risikostyring og internkontroll.
- Styrets samlede ansvar, oppgaver og viktige arbeidsprosedyrer skal dokumenteres i en styreinstruks og oppgavene bør fremgå av en årsplan for styrets arbeid. Styrets vurderinger og beslutninger bør dokumenteres tilstrekkelig omfattende til at de skal kunne etterprøves i ettertid.
- Styret skal foreslå revisor og følge opp arbeidet til valgt revisor.
- Styret bør påse at foretaket har etablert effektive rutiner for å sikre at regnskapet og den finansielle rapporteringen er i tråd med regelverket og relevante standarder. Herunder skal styret vedta delårsregnskap innen 45 dager etter regnskapsperiodens slutt og sørge for at dette uten unødig opphold offentliggjøres på foretakets nettsted, jf. årsregnskapsforskriften § 8-4. Forslag til årsregnskap og årsberetning skal vedtas av institusjonens styre senest tre måneder etter regnskapsårets slutt, jf. årsregnskapsforskriften § 2-1.

For å understøtte styrets behandling og vedtak på ulike saksområder skal det etableres styreutvalg som skal være forberedende og rådgivende organ for styret. I de tilfellene der et samlet styre kan fungere som utvalg, legger Finanstilsynet til grunn at de aktuelle sakene blir gjenstand for grundig behandling i ordinært styremøte. Arbeidet i utvalgene bør dokumenteres tilstrekkelig til at det i ettertid kan etterprøves at arbeidets art og omfang er i samsvar med krav i lov, forskrift og interne instrukser.

Revisjonsutvalg
Etter finansforetaksloven § 8-18 (1) skal finansforetak som er foretak av allmenn interesse etter revisorloven § 1-2 sjette ledd ha et revisjonsutvalg. Unntak fra kravet er gitt i § 8-18 (2) for enkelte finansforetak. Foretak kan etter § 8-20 (3) fastsette i vedtektene at det samlede styret skal fungere som foretakets revisjonsutvalg, men finansforetaksforskriften § 8-4 unntar foretaket som i mer enn 12 måneder har hatt en samlet forvaltningskapital som overstiger 20 milliarder kroner fra denne adgangen. Utvalgets oppgaver går frem av finansforetaksloven § 8-19 (2). Når det gjelder foretakets regnskapsrapportering skal revisjonsutvalget etter paragrafens bokstav c) overvåke systemene for internkontroll, risikostyring og foretakets internrevisjon uten at det bryter med revisjonsutvalgets uavhengige rolle. Internrevisor rapporterer til revisjonsutvalget om sitt arbeid som vedrører systemet for regnskapsrapportering. Videre skal utvalget etter bokstavene e) og f) vurdere og overvåke valgt revisors uavhengighet samt forberede foretakets valg av revisor og gi sin anbefaling om dette.

Krav til sammensetning og kompetanse i revisjonsutvalget kommer frem av finansforetaksloven § 8-20. Etter annet ledd skal utvalget samlet ha den kompetansen som er nødvendig gitt foretakets organisasjon og virksomhet. Minst ett av medlemmene skal ha kvalifikasjoner innen regnskap eller revisjon. For å sette revisjonsutvalget i stand til å utføre oppgavene på en best mulig måte bør arbeidsinstruksen for revisjonsutvalget begrense utvalgets oppgaver og fullmakter til det som er nødvendig for å ivareta de lovpålagte oppgavene.

Risikoutvalg
Finansforetak skal etter finansforetaksloven § 13-6 (4) ha et risikoutvalg oppnevnt av styret. Bare styremedlemmer som ikke inngår i den faktiske ledelsen av virksomheten, kan være medlem av risikoutvalget. Risikoutvalgets oppgaver går frem av finansforetaksforskriften § 13-2. Disse bør inngå i en dokumentert instruks for utvalget. Etter finansforetaksforskriften § 13-1 kan et samlet styre fungere som risikoutvalg i finansforetak med forvaltningskapital som ikke overstiger 20 milliarder kroner. Det vurderes som naturlig at internrevisor rapporterer til risikoutvalget om sitt arbeide som ikke er relatert direkte til overvåking av regnskapsrapporteringen.

Ansvar og oppgaver som tilligger revisjonsutvalget og risikoutvalget skiller seg fra hverandre på en måte som gjør at utvalgene bør være separate, men det er ikke til hinder for at medlemmer er med i begge utvalgene.

Godtgjørelsesutvalg
Foretak med mer enn 50 ansatte og foretak med forvaltningskapital over 5 mrd. kroner skal etter finansforetaksforskriften § 15-3 (2) ha et eget godtgjørelsesutvalg oppnevnt av styret. Utvalget skal forberede all saker om foretakets godtgjørelsesordning som skal avgjøres av styret. Krav til godtgjørelsesordninger er beskrevet i modulens kapittel 6.

3.2 Daglig leder

Daglig leder skal stå for den daglige ledelsen av foretakets virksomhet, og skal følge de retningslinjer og pålegg som styret har gitt. Daglig leders oppgaver samt plikter overfor styret er gitt i finansforetaksloven §§ 8-11 og 8-12. Det pekes også på viktigheten av daglig leders ansvar for å "sette tonen fra toppen" når det gjelder regeletterlevelse generelt og holdninger, adferd og kultur i foretaket spesielt. I kapittel 5 er forventinger til arbeid med risikokultur og adferd utdypet. I sammenheng med vurdering av retningslinjer og rutiner relatert til daglig leders utøvelse av sitt ansvar, følger nedenfor aktuelle momenter:

- Daglig leder skal etter finansforetaksforskriften § 9-2 sette av tilstrekkelige tid til å utføre sine oppgaver i foretaket. Ved vurderingen av hvor mange verv daglig leder kan ha i tillegg til stillingen i foretaket, skal det tas hensyn til individuelle forhold og foretakets virksomhet.
- Det skal være etablert forsvarlige styrings- og kontrollsystemer i tråd med krav i finansforetaksloven § 13-5 og CRR/CRD IV-forskriften del X.
- Det skal være etablert retningslinjer og rutiner for å sikre at foretakets regnskap er i samsvar med lov og forskrifter, og at forvaltning av aktiva og risikostyring er ordnet på en betryggende måte.
- Daglig leder skal gi styret underretning om foretakets virksomhet, stilling og resultatutvikling minst månedlig, i møte eller skriftlig.
- Det skal være fastsatt instrukser som angir ansvarsforhold og de ansattes arbeidsoppgaver og fullmakter, samt rapporterings- og saksbehandlingsregler.
- Daglig leder skal sørge for at foretaket har ansatte som samlet har kvalifikasjoner og erfaringer som trengs for at virksomheten i foretaket drives på en forsvarlig måte.
- Daglig leder oppsummerer årlig de enkelte virksomhetsledernes vurdering av om internkontrollen har vært gjennomført på en tilfredsstillende måte og har forelagt oppsummeringen for behandling i styret i tråd med krav i CRR/CRD IV-forskriften § 37.

3.3 Egnethetsvurdering av nøkkelpersonell

Etter finansforetaksloven § 8-4 (1) skal styret i et finansforetak være allsidig sammensatt. Styremedlemmer skal kunne vurdere, utfordre og føre tilsyn med beslutningene som treffes av foretakets daglige ledelse. Hvert enkelt medlem og det samlede styret må derfor ha relevant kompetanse, tilstrekkelig kapasitet og ellers være egnet til å påta seg styreansvar. Medlemmer av den daglige ledelse og øvrige nøkkelpersoner i foretaket er også underlagt kravene til egnethetsvurdering. Nedenfor følger aktuelle momenter:

- I tråd med kapittel 3.3 i rundskriv 1/2020 må foretaket etablere rutiner for egnethetsvurderinger som bidrar til å sikre at lovkravene oppfylles. Slike rutiner må blant annet klargjøre:
    - hvilke funksjoner i foretaket som er omfattet av egnethetskravene og hvilke som skal meldes til Finanstilsynet,
    - at det skjer en løpende vurdering av de personene som innehar disse funksjonene, og hvilke situasjoner som skal utløse en ny vurdering,
    - hvem som har ansvaret for å foreta vurderingene,
    - hvilken informasjon som skal innhentes, og
    - at vurderingene kan dokumenteres i ettertid.

- Foretaket skal etter finansforetaksloven § 8-9 (1) gi Finanstilsynet melding når styrets sammensetning endres.
- Foretaket skal etter finansforetaksloven § 8-14 (1) gi Finanstilsynet melding ved endringer i daglig ledelse eller faktisk ledelse i foretaket. Slik melding skal om mulig gis på forhånd.
- Foretaket skal etter finansforetaksforskriften § 3-1 annet ledd gi Finanstilsynet melding ved skifte av leder for nøkkelfunksjoner. Slik melding skal om mulig gis på forhånd. Det bemerkes at kretsen av personer som skal egnethetsvurderes av foretaket (dvs. alle innehavere av nøkkelfunksjoner) er større enn personkretsen som må meldes til Finanstilsynet.
- Foretaket må påse at det er innhentet informasjon om eventuelle koblinger til eller verv eller stilling i annet finansforetak, i forretningsforbindelse med finansforetaket eller deltakelse i annen næringsvirksomhet, jf. finansforetaksloven §§ 9-1 til 9-3.
- Foretakets egnethetsvurdering av styrets medlemmer og daglig leder/ledelse skal inkludere om den enkelte kan sette av tilstrekkelig tid til å utføre sine oppgaver i foretaket, herunder etterlevelse av finansforetaksforskriften § 9-2 om begrensninger i antall styreverv, jf. punkt 4.1 i rundskriv 1/2020.
- Ordinær politiattest som er nyere enn tre måneder skal være lagt ved melding til Finanstilsynet, jf. kapittel 3 i rundskriv 1/2020.

På bakgrunn av foretakets melding om gjennomført egnethetsvurdering foretar Finanstilsynet en vurdering og gir tilbakemelding til foretaket dersom Finanstilsynet har spørsmål eller ikke anser personen egnet.

3.4 Valgkomite

Etter finansforetaksloven § 8-4 (2) velger generalforsamlingen styrets leder og de øvrige styremedlemmene så lenge foretaket ikke har en foretaksforsamling, jf. § 8-15. Det anbefales at generalforsamlingen oppnevner en valgkomite (nominasjonsutvalg) som skal forberede valget. I tråd med prinsipp 7 i *Den norske anbefalingen om eierstyring og selskapsledelse* (NUES), bør et flertall i valgkomiteen være uavhengig av styret og øvrige ledende ansatte. Daglig leder eller andre ledende ansatte bør ikke være medlem av komiteen. Foretakets vedtekter skal inneholde regler om valget. Valgkomiteen bør være særlig opptatt av kompetansekravene som gjelder for styret og styreutvalgene ved innstilling av medlemmer til styret.

4 ORGANISERING OG ANSVARSFORHOLD

Formålet med dette kapittelet er å vurdere om foretakets organisering og ansvarsforhold er hensiktsmessig og tydelig, slik at det legges til rette for en effektiv og betryggende ledelse av all virksomhet, både på foretaks- og konsernnivå samt i deler av virksomheten som er utkontraktert.

Et finansforetak skal etter finansforetaksloven § 13-5 (1) organiseres og drives på en forsvarlig måte, og herunder ha en klar organisasjonsstruktur og ansvarsfordeling. Nedenfor følger aktuelle momenter:

- Den juridiske og operative strukturen skal være tilpasset foretakets størrelse og kompleksitet, den skal være forståelig for foretakets ansatte og eksterne interessenter, herunder for tilsynsmyndighetene og den bør være dokumentert.
- Organiseringen av foretakets virksomhet skal sikre tydelig ansvarsfordeling og organiseringen av viktige prosesser skal etter CRR/CRD IV-forskriften § 35 sikre tilstrekkelig arbeidsdeling i disse. Om nødvendig skal informasjonssperrer etableres slik at interessekonflikter så langt som mulig unngås.
- Organiseringen skal også sørge for et tydelig skille mellom de operative forretnings- og støtteenhetene i første linje og de uavhengige kontrollfunksjonene i andre og tredje linje.
- Det skal være etablert tydelige rapporteringsstrukturer og -ansvar som sikrer tilstrekkelig og hensiktsmessig forretnings- og driftsmessig rapportering samt uavhengig rapportering fra kontrollfunksjoner i andre (risiko- og etterlevelsesrapportering) og tredje linje (internrevisjonsrapportering).
- Ansvars- og fullmaktsforhold må være tydelig definert og dokumentert i relevante og hensiktsmessige instrukser for de ansatte, jf. finansforetaksloven § 8-11 (3). For alle vesentlige risikoforhold i foretaket bør omfanget av ansvaret være klart, og det bør være tydelig forankret hos én av lederne i den øverste ledergruppen. Særlig i store foretak med matriseorganisering vil det vanligvis være behov for særskilte innretninger eller verktøy for å oppnå nødvendig tydelighet.
- Det skal etter forskrift om meldeplikt ved utkontraktering mv. §1 foreligge en oppdatert oversikt over alle utkontrakteringsavtaler. Utkontraktering av virksomhet kan etter finansforetaksloven § 13-4 (1) ikke skje i så stort omfang eller på en slik måte at det ikke kan anses forsvarlig eller slik at tilsynet med den utkontrakterte virksomheten eller foretakets samlede virksomhet blir vanskeliggjort. Videre kan kjerneoppgaver ikke utkontrakteres med mindre annet følger av bestemmelser gitt i eller i medhold av lov.
- Finansforetakene skal ha et register over sine finansagenter. Registeret skal gjøres offentlig tilgjengelig på finansforetakets eget nettsted. Avtalene med agentene må minimum inneholde bestemmelser som nevnt i rundskriv 6/2019. Finansforetaket må ha rutiner for oppfølging av at agentene etterlever lover og regler som gjelder for finansforetakets forhold til kundene.
- Organisering av utenlandsvirksomhet må være i samsvar med det som er meldt til Finanstilsynet (datterforetak, grensekryssende eller filialvirksomhet), og det må fremgå hvordan virksomheten er integrert i foretakets system for styring og kontroll, herunder hvilke(n) rapporteringslinjer som gjelder for denne virksomheten og hvordan virksomheten skal følges opp.

5 RISIKOKULTUR, ADFERD OG INTERESSEKONFLIKTER

Formålet med dette kapittelet er å vurdere foretakets retningslinjer og metoder for å fremme en sunn risikokultur og god forretningsskikk i hele foretakets virksomhet. Videre vurderes foretakets retningslinjer og metoder for å sikre at mulige interessekonflikter identifiseres og håndteres ryddig og i åpenhet, slik at krav til likebehandling og armlengdes avstand ivaretas og kundenes interesser kommer i første rekke.

En sunn risikokultur sees gjerne som grunnmuren, og dermed som en vesentlig forutsetning, for god risikostyring i et foretak. Risikokultur er gjerne knyttet til normer, holdninger og adferd relatert til risikostyring og etterlevelse i virksomheten. Arbeidet med risikokultur starter på toppen. Styret og ledelsen har et viktig ansvar i å etablere og å vedlikeholde en risikokultur basert på uttalte kjerneverdier og holdninger som foretaket ønsker skal ligge til grunn for all aktivitet i hele virksomheten. I arbeidet med risikokultur bør det tas utgangspunkt i foretakets vedtatte risikoappetitt, og arbeidet bør hensynta omfang og kompleksitet i foretakets virksomhet. Vektlegging av mangfold blant foretakets styre, ledelse og øvrige ansatte samt at interne prosesser er basert på åpenhet og involvering, der meningsutveksling ønskes velkommen, vil bidra til veloverveide beslutninger og til at risikoen for tap, særlig fra operasjonelle hendelser og fra risikoen knyttet til foretakets renommé, reduseres. Det bør understrekes at risikostyring ikke er forbeholdt risikoeksperter eller kontrollfunksjoner, men at risikostyring og kontroll handler om hvordan hver enkelt medarbeider daglig utfører sitt arbeid. Nedenfor følger aktuelle momenter:

- Styret og ledelsen bør fastsette kjerneverdier og etiske retningslinjer som skal være med å underbygge og tydeliggjøre holdninger og adferd som skal prege risikokulturen i foretaket.
- Ledelsen bør sørge for å kommunisere foretakets kjerneverdier, etiske retningslinjer samt forventninger til alle ansatte om deres ansvar for risikostyring og kontroll.
- Retningslinjer som skal bidra til å fremme mangfold og kjønnsnøytralitet bør være vedtatt og kommunisert i hele organisasjonen.
- Foretaket skal ha en intern varslingskanal etter finansforetaksloven § 13-5 (5) der de ansatte kan varsle internt eller til myndighetene om overtredelser av bestemmelser gitt i eller i medhold av lov, og etter arbeidsmiljøloven kapittel 2A om kritikkverdige forhold. Det bør dermed, i tråd med EBA/GL/2021/05 kapittel 13, være etablert retningslinjer og rutiner for varsling av mulige eller faktiske brudd på eksterne eller interne krav.[1] Varslingsprosedyrene skal gjøres kjent og være tilgjengelig for alle medarbeidere.
- Det arbeides aktivt med å fremme forståelsen for kontrollfunksjonenes rolle som en konstruktiv utfordrer og rådgiver i styringen av risikoer, samt til konstruktiv dialog og en omgangsform preget av respekt og tillit mellom enheter og personer i ulike forsvarslinjer.
- For vurdering av leders måloppnåelse, bør det etableres målekriterier for ikke-finansielle forhold, herunder kriterier som skal bidra til å fremme kultur og adferd i tråd med foretakets normer og kjerneverdier. Se også om godtgjørelsesordninger i kapittel 6.
- Det bør være etablert en tydelig og konsekvent gjennomført praksis for vurdering av sanksjoner ved brudd på eksterne og interne regler samt alvorlige brudd på interne normer og forventninger.
- Foretaket bør ha et system for registrering/rapportering av operasjonelle hendelser og bruke dette aktivt i læring og forbedringsarbeid.
- Foretaket skal ha retningslinjer for behandling av klager fra kunder, jf. rundskriv 4/2019, og et register for å registrere disse. Rutinene skal sikre at alle klager blir undersøkt grundig og at eventuelle interessekonflikter blir identifisert og avgrenset.

[1] Finanstilsynet har også etablert en varslingsportal for varsling av overtredelser av den lovgivningen Finanstilsynet forvalter, ref.: https://www.finanstilsynet.no/om-finanstilsynet/varsling-til-finanstilsynet/

Foretaket skal løpende analysere informasjonen som er mottatt i klagene for å avdekke om klagene skyldes systematiske svakheter i foretaket.

- Foretaket skal ha retningslinjer for håndtering av interessekonflikter både for ansatte og på foretaksnivå, og disse skal være godt kjent i organisasjonen.
- Foretakets retningslinjer og implementerte tiltak skal være tilstrekkelige for å forhindre at foretakets interesser går foran kundenes interesser på en måte som påvirker kundene negativt, jf. finansforetaksloven § 16-1 (4). Retningslinjene og tiltakene skal også forhindre at ansattes private interesser, herunder for medlemmer av ledelsen og styret, på en negativ måte, kan påvirke utførelsen av deres ansvar og oppgaver i foretaket, jf. EBA/GL/2021/05 kapittel 12. Retningslinjene skal også bidra til å forhindre uredelig og uetisk adferd samt beslutninger som er i strid med foretakets interesser. Tiltak som er iverksatt for å unngå eller redusere interessekonflikter, herunder begrunnelsen for hvordan tiltaket vil være effektivt for å sikre objektive beslutninger, skal dokumenteres.
- Foretaket forventes å ha retningslinjer for inngåelse av forretningstransaksjoner med medlemmer av ledelsen, styret, store eiere og nærstående til disse. Retningslinjene bør inneholde krav om at slike forretningstransaksjoner skal dokumenteres tilstrekkelig, herunder at dokumentasjonen til enhver tid er oppdatert.

6 GODTGJØRELSESORDNINGER

Formålet med dette avsnittet er å vurdere foretakets godtgjørelsesordning. Det vises til krav i finansforetaksforskriften kapittel 15 del I om godtgjørelsesordninger i kredittinstitusjoner og verdipapirforetak samt til Finanstilsynets rundskriv 2/2020 for ytterligere informasjon. Nedenfor følger aktuelle vurderingsmomenter:

- Foretaket skal ha etablert en godtgjørelsesordning som omfatter alle medarbeidere i hele foretaket og i datterforetak. Ordningen skal bidra til lik belønning for likt arbeid, uavhengig av kjønn. Ordningen skal videre fremme god styring og kontroll av foretakets risiko, motvirke for høy risikotaking og bidra til å unngå interessekonflikter, jf. finansforetaksforskriften § 15-1 første ledd.
- Ordningen skal være i samsvar med foretakets overordnede mål, risikoappetitt og langsiktige interesser, jf. § 15-2 tredje ledd.
- Godtgjørelsesordningen skal inneholde særskilte regler for ledende ansatte, for andre ansatte og tillitsvalgte med arbeidsoppgaver av vesentlig betydning for foretakets risikoeksponering og for andre ansatte og tillitsvalgte med tilsvarende godtgjørelse, samt for andre ansatte og tillitsvalgte med kontrolloppgaver[2], jf. finansforetaksforskriften § 15-2 første ledd.
- Foretaket skal minst årlig foreta en gjennomgang av praktiseringen av godtgjørelsesordningen og utarbeide en skriftlig rapport om den årlige gjennomgangen. Rapporten skal gjennomgås av uavhengig kontrollfunksjon, jf. § 15-2 fjerde ledd.

[2] Ansatte med kontrollansvar vil normalt omfatte sentrale medarbeidere innenfor internrevisjon samt uavhengige kontrollfunksjoner for etterlevelse og risikokontroll, jf. rundskriv 2/2020 punkt 3.1.3.

- I ordningen skal det fastsettes hvilke grupper av ansatte som skal anses som ledende ansatte, som ansatte med arbeidsoppgaver av vesentlig betydning for foretakets risikoeksponering, samt som ansatte med kontrolloppgaver jf. § 15-3 første ledd.
- Dersom variabel godtgjørelse skal benyttes, skal denne baseres på en kombinasjon av vurderinger av vedkommende person, vedkommende forretningsenhet og foretaket som helhet. Ved måling av resultater skal risiko for foretaket og kostnader knyttet til behov for kapital og likviditet hensyntas. Grunnlag for variabel godtgjørelse knyttet til foretakets resultater skal være en periode på minst to år, jf. § 15-4 femte ledd. Kriterier for måloppnåelse bør være av både kvantitativ og kvalitativ art, og bør inkludere finansielle og ikke-finansielle parametere, jf. EBA/GL/2021/04 punkt 225.
- For ledende ansatte skal variabel godtgjørelse normalt ikke utgjøre mer enn den faste godtgjørelsen, og aldri mer enn det dobbelte av fast godtgjørelse (sistnevnte gjelder dersom den særlige fremgangsmåten for å fastsette en ratio på opptil 200 prosent i § 15-4 andre ledd er fulgt). For daglig leder og medlemmene av ledergruppen skal variabel godtgjørelse ikke utgjøre mer enn halvparten av den faste godtgjørelsen, jf. § 15-4 tredje ledd.
- For ledende ansatte må minst halvparten av årlig variabel godtgjørelse gis i form av aksjer eller andre egenkapitalinstrumenter utstedt av foretaket eller et annet foretak i konsernet, eller i form av betinget kapital som avspeiler foretakets verdivurdering, jf. § 15-4 sjette ledd.
- Variabel godtgjørelse nevnt i punktet over skal ikke kunne disponeres fritt av den ansatte tidligere enn jevnt fordelt på en periode på minst tre år.
- Variabel godtgjørelse skal kun opptjenes eller utbetales dersom det er forsvarlig ut fra foretakets økonomiske stilling.
- Det skal fastsettes kriterier for fradrag og tilbakebetaling av inntil 100 prosent av den samlede variable lønnen, jf. § 15-4 tolvte ledd.
- Godtgjørelse til ansatte med kontrollansvar skal være uavhengig av resultatet i forretningsområdet som de kontrollerer jf. § 15-6.
- Garantert variabel godtgjørelse kan kun benyttes i særlige tilfeller ved nyansettelser, og være begrenset til det første året, jf. § 15-4 fjerde ledd.
- Ledende ansatte skal ikke ha avtaler eller forsikringer som sikrer mot bortfall av variabel godtgjørelse, jf. § 15-4 niende ledd.
- Foretaket bør også ha et rammeverk for godtgjørelse til agenter eller andre som opptrer på vegne av foretaket som sikrer at godtgjørelsen ikke gir insentiver til overdreven risikotaking eller adferd som er i strid med god forretningsskikk og med kundenes behov og interesse.

I Finanstilsynets rundskriv om godtgjørelsesordninger punkt 2.2 legges det til grunn at foretak som yter variabel godtgjørelse som er begrenset til maksimalt halvannen månedslønn per år, og som omfatter alle ansatte, ikke omfattes av godtgjørelsesreglene. Fordelen eller ekstrabetalingene må være del av en generell, ikke skjønnsmessig fastsatt politikk, som omfatter hele foretaket, og som ikke gir insentiv til å ta risiko på vegne av foretaket. Finanstilsynet legger imidlertid til grunn at også foretak som kvalifiserer for det nevnte unntaket i rundskrivet vedtar og dokumenterer retningslinjer for foretakets godtgjørelsesordninger og at disse revideres jevnlig. Videre bemerkes at det nevnte unntaket gjelder under forutsetning av at tildeling og utbetaling av variabel godtgjørelse er forsvarlig tatt i betraktning foretakets kapitalsituasjon.

7 SYSTEMET FOR INTERNKONTROLL OG RISIKOSTYRING

Formål med kapittelet er å vurdere foretakenes samlede system for internkontroll og risikostyring, jf. krav etter finansforetaksloven §§ 13-5 til 13-7 samt CRR/CRD IV-forskriften del X. Etter CRR/CRD IV-forskriften § 35 er styret ansvarlig for at det etableres et tydelig system for styring og oppfølging av alle risikoer som er relevante for foretaket.

7.1 Internkontroll

Internkontroll er en kontinuerlig prosess som skal bidra til å sikre måloppnåelse gjennom:

- effektiv og forsvarlig forretningsdrift,
- hensiktsmessig identifisering, måling og styring av risiko,
- rapportering av pålitelig finansiell og ikke-finansiell informasjon både internt og eksternt,
- hensiktsmessige administrative- og regnskapsprosesser,
- etterlevelse av lover, forskrifter, myndigheters forventinger og foretakets egne interne retningslinjer og vedtak.

Systemet for internkontroll bør dekke hele virksomheten, herunder styrets og ledelsens ansvar og oppgaver, aktiviteter i alle forretningsområder og støttefunksjoner, uavhengige kontrollfunksjoner og all utkontraktert virksomhet. Systemet bør også dekke all aktivitet utenfor hjemlandets grenser. Nedenfor følger aktuelle momenter:

- Overordnede prinsipper for internkontroll skal være tilpasset foretakets omfang og virksomhet og være vedtatt av styret.
- Utfyllende retningslinjer samt systemer, metoder og rutiner for styring og kontroll skal omfatte alle risikoer og tilhørende risikokonsentrasjoner foretaket er, eller kan bli, eksponert for.
- Retningslinjene skal også omhandle foretakets krav, metoder og systemer for identifisering, vurdering og håndtering av risiko relatert til økonomisk kriminalitet og klimaendringer samt andre ESG-risikoer.
- Retningslinjer og annen nødvendig informasjon om metoder og prosesser skal oppdateres jevnlig og distribueres tilstrekkelig i foretaket for å sikre at enheter og medarbeidere er i stand til å utføre oppgavene i tråd med sitt mandat og ansvar.
- Det skal være etablert tydelige og dokumenterte beslutningsprosesser og fullmakter samt en klar fordeling av ansvar for implementering og gjennomføring av de ulike elementer av internkontrollsystemet.
- Ledere på alle virksomhetsområder skal løpende vurdere om iverksatte internkontrolltiltak er tilstrekkelige og om det er behov for nye tiltak.
- Daglig leder skal minimum årlig oppsummere og dokumentere vurderingene av om implementert internkontroll fungerer tilfredsstillende. Oppsummeringen skal forelegges styret for behandling.
- I foretak som ikke har internrevisjon, skal valgt revisor årlig gi styret en bekreftelse om risikostyringen og internkontrollen i foretaket, jf. finansforetaksforskriften § 8-3 (2).

- Det skal være etablert uavhengige kontrollfunksjoner for henholdsvis risikokontroll og etterlevelse. Kontrollfunksjonene skal være effektive, ha tilstrekkelig ressurser og kompetanse samt nødvendig autoritet og status for å kunne oppfylle sitt mandat. De skal videre ha mulighet og plikt til å rapportere direkte til styret ved behov.
- Det skal være vedtatt klare retningslinjer og etablert en prosess (NPAP[3]) for å vurdere og godkjenne risiko knyttet til innføring av nye eller vesentlig endrede produkter, tjenester og andre aktiviteter, herunder for utkontraktering og enkelttransaksjoner som kan påvirke risikobildet vesentlig samt for endringer i forretningsmodellen.
- Uavhengige kontrollfunksjoner for risikostyring og etterlevelse skal involveres i NPAP. For mer om NPAP, se også modul for operasjonell risiko.
- Det skal være etablert en uavhengig kontrollfunksjon med ansvar for internrevisjon, jf. finansforetaksloven §§ 13-5 (2) og 8-16, som har rett til å møte i styremøtene. Unntak fra kravet om internrevisjon etter finansforetaksforskriften § 8-3 gjelder foretak med samlet forvaltningskapital mindre enn 10 milliarder kroner (i mer enn 12 måneder).
- Det skal være etablert virksomhets- og risikorapportering til styret og ledelsen om status og utvikling i foretaket, herunder om risiko og etterlevelse, som er tilstrekkelig dekkende og tidsaktuell.
- Foretaket må sikre at ansvaret for at alvorlige mangler og svakheter som kontrollfunksjonene påpeker i sine rapporter blir forankret tilstrekkelig høyt i organisasjonen og at det følges opp av ledelsen og styret, slik at nødvendige forbedringstiltak kan iverksettes raskt og effektivt.

7.2 Risikostyring

Finansforetak er etter finansforetaksloven § 13-5 pålagt krav om forsvarlig virksomhet. Herunder skal foretakene etablere et risikostyringsrammeverk med klare og hensiktsmessige styrings- og kontrollordninger samt hensiktsmessige retningslinjer og rutiner for å identifisere, styre, overvåke og rapportere alle risikoer foretaket er, eller kan bli, eksponert for. Rammeverket skal være tilpasset risikoen ved og omfanget av virksomheten i foretaket. CRR/CRD IV-forskriften § 36 angir minstekrav til hvilke risikoer foretakets rammeverk skal omfatte.

Etter § 13-6 skal finansforetak til enhver tid ha oversikt over, og med jevne mellomrom vurdere, hvilke enkelte risikoer og samlet risiko, herunder systemrisiko, som er knyttet til virksomheten. Med basis i risikovurderingene skal foretaket vurdere kapitalbehovet på kort og lang sikt og sikre at den ansvarlige kapitalen til enhver tid er på et forsvarlig nivå.

Nedenfor følger aktuelle momenter for vurdering av rammeverket for styring og overvåking av foretakets risiko og kapital:

- Foretaket skal ha vedtatt og dokumentert risikostrategi, risikoappetitt, overordnede retningslinjer og risikorammer som del av systemet for risikostyring.

[3] NPAP – New Product Approval Policy, ref. kapittel 18 I EBA/GL/2021/05

- Foretakets risikoappetitt, overordnede retningslinjer og risikorammer bør være konsistente med foretakets forretningsstrategi og være innenfor foretakets risikokapasitet og finansielle ressurser.
- Foretakets risikoappetitt og tilhørende risikorammer og -mål bør være hensiktsmessig fordelt ned på ulike enheter og forretningsområder i foretaket.
- Foretaket skal ha etablert en uavhengig risikokontrollfunksjon som dekker hele virksomheten og som er aktivt involvert i utformingen av foretakets risikostrategi og i alle diskusjoner om beslutninger som medfører vesentlig endring i foretakets risiko.
- Foretaket bør ha etablert en særskilt prosess for å beslutte om risikoforhold som leder av risikokontroll- eller etterlevelsesfunksjonen har uttrykt seg kritisk til.
- Foretakets ICAAP-/ILAAP-dokumenter skal dekke alle vesentlige risikoer i foretaket og bør være konsistente med forretningsstrategi og praktisk risikostyring.
- Foretaket skal ha etablert et sett med stresstester som gjennomføres jevnlig, herunder i tilknytning til vurderinger i ICAAP/ILAAP, og som er i tråd med EBA-retningslinjene for finansforetaks stresstesting.

7.3 Uavhengige kontrollfunksjoner

Finansforetak skal etter finansforetaksloven § 13-5 (2) ha uavhengige kontrollfunksjoner med ansvar for *internrevisjon*, *risikostyring* og *etterlevelse* av krav fastsatt i eller i medhold av lov eller forskrift. Kontrollfunksjonene for risikostyring (risikokontroll) og etterlevelse (compliance) regnes i modellen med tre forsvarslinjer som foretakets andrelinjeforsvar, mens internrevisjonen utgjør tredjelinje. Nedenfor er det gjengitt krav og forventninger til kontrollfunksjonene basert på bestemmelsene i CRR/CRD IV-forskriften del X, EBA/GL/2017/11 og anbefalinger fra Baselkomiteen som vedrører funksjonenes rolle, ansvar og oppgaver.

Risikokontrollfunksjonen:

- bør som grunnlag for sitt arbeid ha et tydelig formulert mandat fra styret som blant annet uttrykker kontrollfunksjonens formål, ansvar, hovedoppgaver og fullmakter,
- bør være en sentralisert organisert enhet som overvåker risiko i hele virksomheten, herunder risiko knyttet til deler som er utkontraktert samt til virksomhet utenfor hjemlandet,
- bør foreslå foretakets overordnede risikostyringsrammeverk og følge opp at vedtatt rammeverk etterleves og fungerer effektivt,
- skal være aktivt involvert i utarbeidelsen av foretakets risikostrategi, i diskusjoner om alle vesentlige risikoforhold og sørge for at styret og foretaksledelsen mottar risikoinformasjon som er relevant i tid og innhold,
- skal være aktivt involvert i foretakets prosess for risikovurderinger og godkjennelse av nye produkter, tjenester og andre aktiviteter,
- skal ha en leder som har tilstrekkelig kompetanse, erfaring, uavhengighet og integritet, og som har direkte tilgang til styret ved behov,
- skal sikre at alle vesentlige risikoer måles, styres og rapporteres tilstrekkelig av relevante forretningsenheter,

- skal måle, overvåke, rapportere og rådgi om risikosituasjonen uavhengig av enhetene som eier og forvalter risikoene operativt,
- bør på selvstendig grunnlag overvåke risikoeksponeringer løpende mot vedtatt risikoappetitt og -rammer, eskalere brudd på appetitt eller rammer i tråd med etablert rutine og gi anbefalinger om korrigerende tiltak,
- bør jevnlig vurdere og verifisere verdifastsettelsen på vesentlige posisjoner i instrumenter til virkelig verdi,
- skal ivareta ansvaret, spesifisert i kapitalkravsforordningen (CRR), for å følge opp internmodeller som foretak har fått godkjent til bruk for å beregne regulatorisk kapitalkrav, herunder for testing og validering av slike modeller,
- bør også jevnlig teste og overprøve andre interne modeller som anvendes i foretakets risikostyring,
- skal rapportere jevnlig og helhetlig til styret og ledelsen om status og utvikling for risikobildet samt framoverskuende om mulig fremvoksende risikoer,
- bør ha hensiktsmessige IT- og støttesystemer i utførelsen av sitt arbeid.

Se også egne vurderingsmomenter vedrørende uavhengig risikorapportering i punkt 7.3.2.

Etterlevelses-/compliance-funksjonen:

- bør som grunnlag for sitt arbeid ha et tydelig formulert mandat fra styret som blant annet uttrykker kontrollfunksjonens formål, ansvar, hovedoppgaver og fullmakter,
- bør være en sentralisert organisert enhet som dekker hele virksomheten,
- bør foreslå foretakets rammeverk for styring av relevante etterlevelsesrisikoer,
- bør utarbeide en risikobasert plan for overvåking og testing av etterlevelse i foretaket,
- skal identifisere, vurdere og overvåke foretakets vesentlige etterlevelsesrisikoer, og rapportere uavhengig til styret og ledelsen om status og risikonivå,
- bør evaluere forbedringstiltak som enhetene i første linje iverksetter og rapportere vurdert status til styret,
- skal være aktivt involvert i vurdering av etterlevelsesrisiko knyttet til foretakets prosess for risikovurdering og godkjennelse av nye produkter, tjenester og andre aktiviteter,
- bør ved behov gi råd og anbefalinger til ledelsen og styret om aktuelle tiltak for å sikre etterlevelse av gjeldende regulatorisk rammeverk og standarder,
- skal ha en leder som har tilstrekkelig kompetanse, erfaring, uavhengighet og integritet, og som har direkte tilgang til styret ved behov,
- bør gjennomføre nødvendig opplæring av ledelsen og ansatte når det gjelder vesentlige etterlevelsesrisikoer,
- bør ha hensiktsmessige IT- og støttesystemer i utførelsen av sitt arbeid.

Se også egne vurderingsmomenter vedrørende uavhengig risikorapportering i punkt 7.3.2.

Internrevisjonsfunksjonen

Finansforetak skal etter finansforetaksloven § 8-16 ha en uavhengig internrevisjonsfunksjon som skal kontrollere at foretaket er organisert og drives på en forsvarlig måte og i samsvar med gjeldende krav til virksomheten. Funksjonen utgjør i modellen med tre forsvarslinjer foretakets tredje forsvarslinje. Funksjonens hovedoppgave å gi styret trygghet for at foretakets system for intern virksomhetsstyring, herunder internkontroll og risikostyring, er av tilfredsstillende kvalitet og at det etterleves effektivt i foretaket. Unntak fra kravet om

internrevisjonsfunksjon er gitt i finansforetaksforskriften § 8-3 for finansforetak som i mer enn de siste 12 måneder har hatt en samlet forvaltningskapital lavere enn 10 milliarder kroner.

Foretak som ikke har unntak fra kravet om internrevisjon etter finansforetaksforskriften § 8-3, må etablere en uavhengig og effektiv funksjon som:

- er en sentralisert funksjon som dekker hele foretaket og som rapporterer til og er ansvarlig overfor styret,
- har jevnlig kommunikasjon med relevante styreutvalg der slike utvalg er etablert,
- har et tydelig og dokumentert mandat fra styret som blant annet bør uttrykke funksjonens formål, ansvar, hovedoppgaver og fullmakter,
- er sikret organisatorisk uavhengighet og internrevisors objektivitet,
- har tilstrekkelig ressurser, kompetanse og status, og en leder med nødvendig autoritet og erfaring
- er en betrodd rådgiver og sparringpartner for styret og ledelsen,
- bør ha uhindret tilgang til all relevant informasjon og dokumentasjon i hele foretaket, herunder til ledelsesinformasjonssystemer og referat fra alle utvalg og beslutningsorgan, samt har fysisk adgang til alle kontorlokaler og alle enheter i foretaket,
- etterlever relevante nasjonale og internasjonale revisjonsstandarder,
- baserer sitt arbeid på en revisjonsplan som er forelagt styret for godkjenning og som er risikobasert, samtidig som kravene til at visse områder og temaer skal revideres regelmessige er hensyntatt,
- sikrer at alle relevante deler av foretakets virksomhet, herunder kontrollfunksjonene i andre linje, inkluderes i vurderingene av revisjonsbehov,
- vurderer om foretakets rammeverk for styring og kontroll er hensiktsmessig, om det er i tråd med juridiske og regulatoriske krav, med ledelsens vedtak og med foretakets strategi og risikoappetitt,
- vurderer om foretakets vedtatte retningslinjer og rutiner er riktig og effektivt implementert,
- vurderer om kontrolltiltak i virksomheten, herunder iverksatte forbedringstiltak etter påpekte mangler og svakheter, er hensiktsmessige og om de gjennomføres effektivt og med tilstrekkelig kvalitet,
- bør etablere en revisjonsprosess som sikrer at revidert enhet blir hørt og tar eierskap til påpekte svakheter og mangler
- kommuniserer tydelig alvorlighetsgraden og årsaker til de identifiserte mangler og svakheter samt omfang, ansvar og tidsfrist for nødvendige forbedringstiltak,
- rapporterer forhold som vurderes som utilfredsstillende til styret og daglig leder, særlig alvorlige forhold bør eskaleres uten unødig opphold,
- minst årlig rapporterer til styret om risikostyringen og internkontrollen i foretaket, herunder bør status for utvikling i revisjonsanmerkninger som foreløpig ikke er utbedret inkluderes, samt at funksjonen rapporterer om sin virksomhet,
- har hensiktsmessige IT- og støttesystemer i utførelsen av sitt arbeid, herunder for å planlegge og følge opp gjennomføringen av egen revisjonsplan samt for å rapportere status for påpekte mangler og svakheter i de reviderte områdene.

7.3.1 Uavhengighet for interne kontrollfunksjoner

Finansforetak skal etter finansforetaksloven § 13-5 (2) ha uavhengige kontrollfunksjoner. For at kontrollfunksjonene skal kunne anses å være tilstrekkelig uavhengige:

- skal personer i kontrollfunksjonen ikke utføre oppgaver som inngår i virksomheten de er satt til å overvåke og kontrollere,
- skal kontrollfunksjonene være organisatorisk skilt fra de funksjoner og områder som de skal overvåke og kontrollere,
- skal den ansvarlige for en kontrollfunksjon rapportere regelmessig direkte til styret, både skriftlig og muntlig, og være til stede ved styremøter når funksjonens rapport behandles,
- skal kontrollfunksjonene ikke være delaktig i inntektsbringende aktiviteter,
- skal godtgjørelse til ansatte i kontrollfunksjoner ikke utformes slike at det kan stilles spørsmål om deres objektivitet,
- bør kontrollfunksjonene ha direkte tilgang til relevant informasjon og ubehandlede transaksjonsdata fra de aktuelle virksomhetsområdene som funksjonen skal overvåke, for selv å foreta uavhengig måling, kontroll og rapportering.

Kravet om uavhengighet må ikke forstås slik at det legger begrensninger på interaksjon, kommunikasjon eller informasjonsutveksling mellom medarbeidere i første og andre forsvarslinje eller når det gjelder fysisk plassering.

Dersom én person, i foretak som ikke omfattes av CRR/CRD IV-forskriften § 41, har ansvaret for både risikokontroll- og etterlevelsesfunksjonen, eller ansvaret kombineres med annet ansvar i foretaket, må mulige interessekonflikter håndteres på en måte som sikrer åpenhet og ryddighet.

7.3.2 Uavhengig rapportering

Styret skal etter CRR/CRD IV-forskriften § 35 (1) sikre seg tilgang til risikoinformasjon og fastsette omfang, format og frekvens for rapporteringen. Se også kapittel III om praktisk risikorapportering i Baselkomiteens "Principles for effective risk data aggregation and risk reporting – January 2013".

Rapporteringen bør skje jevnlig til styret, ledelsen og andre relevante parter, samtidig som nødvendig konfidensialitet ivaretas. Rapportens innhold må være korrekt og inkludere risiko i hele virksomheten, være tilstrekkelig omfattende og tidsaktuell samt tilpasset behovet i det enkelte foretak. Nedenfor følger aktuelle momenter:

- Risikokontrollfunksjonen bør rapportere minimum hvert kvartal til styret. I store og komplekse foretak bør behovet for månedlig rapportering vurderes.
- Rapporteringen bør inneholde informasjon om faktisk status og utvikling, om kontrollfunksjonenes vurderinger, råd og anbefalinger samt være framoverskuende om mulige fremvoksende risikoer med bl.a. stresstester som grunnlag.
- Risikoapporteringen bør minimum dekke kreditt-, motparts-, markeds-, likviditets- og operasjonell risiko, herunder om IKT, hendelser og kundeklager.
- Etterlevelsesfunksjonen bør som utgangspunkt rapportere kvartalsvis, men for mindre og ikke-komplekse foretak kan det vurderes om halvårlig rapportering er tilstrekkelig.
- Etterlevelsesfunksjonens rapportering bør ta utgangspunkt i funksjonens årsplan og i foretakets vesentlige etterlevelsesrisikoer.

- Etterlevelsesrapporteringen bør minimum omhandle vurdert status for foretaket, funksjonens gjennomførte aktiviteter, herunder kontroller og testing samt ved behov også råd og anbefalinger.
- Etterlevelsesrapporteringen bør minimum dekke status for etterlevelse av hvitvaskingsloven og regelverket om terrorfinansiering, IKT-, data- og informasjonssikkerhet, forbruker- og investorvern, personvern, endringer i relevant regelverk og andre rammevilkår med vurderinger av hva endringene betyr for foretaket. Rapportene bør videre gjengi seneste eventuelle korrespondanse med myndigheter.

7.4 Valgt revisor

Valgt revisor er allmennhetens tillitsperson ved utøvelse av lovfestet revisjon, jf. revisorloven § 9-1 annet ledd. Kapittel 12 i revisorloven omhandler særlige plikter ved revisjon av foretak av allmenn interesse og gjennomfører kravene til revisjon av foretak av allmenn interesse i EUs revisjonsdirektiv.

Informasjon om valgt revisors arbeid, herunder om risikovurderinger, planer og innholdet i revisors kommunikasjon med foretaket er viktig for den helhetlige vurderingen av foretakets styring og kontroll. Særlig relevante kilder til informasjon vil være valgt revisors:

- presentasjoner for revisjonsutvalget om planlegging og resultater fra interimsrevisjonen og resultater fra den avsluttende årsregnskapsrevisjonen,
- tilleggsrapport til revisjonsutvalget, etter revisjonsforordningens (EU nr. 537/2014) artikkel 11, om resultatene av den lovfestede revisjonen,
- revisjonsberetning etter revisjonsforordningens artikkel 10, herunder avsnittet om sentrale forhold ved revisjonen,
- eventuelle nummererte brev til styret om forhold som er fremkommet ved revisjonen og som styret bør gjøres kjent med for å kunne ivareta sitt ansvar og oppgaver, herunder vesentlige mangler i foretakets internkontroll, brudd på bokføringsreglene og andre lovkrav og avdekkede misligheter,
- dokumentasjon av eventuelle attestasjoner og bekreftelser som er gjennomført.

Det avholdes møte med foretakets valgte revisor som del av stedlige tilsyn. For systemviktige foretak møter Finanstilsynet i tillegg foretakenes valgte revisor i egne møter minst én gang per år. Finanstilsynet vurderer fortløpende behovet for egne møter med valgt revisor i andre foretak basert på om særskilte forhold kan tilsi et slikt behov. Slike forhold kan være:

- vesentlige hendelser som er avdekket gjennom tilsynsvirksomheten eller den lovfestede revisjonen,
- utvikling i foretaket som kan medføre en endret risikovurdering og/eller endret behov for tilsynsmessig oppfølging,
- internt bytte av revisor som er ansvarlig for å utføre revisjonsoppdraget,

8 IKT-SYSTEMER, DRIFTS- OG FORRETNINGSMESSIG KONTINUITET OG GJENOPPRETTING

Formålet med dette kapittelet er å vurdere om foretaket har etablert ordninger som synes hensiktsmessige for å styre, overvåke og forbedre effektivitet og pålitelighet i foretakets informasjons- og kommunikasjonssystemer og i beredskaps- og kriseplaner som skal sikre at driften kan videreføres og tap begrenses ved alle typer alvorlige driftsforstyrrelser. Videre vil vurderinger fra gjennomgangen av foretakets plan for å gjenopprette sin finansielle stilling når denne er betydelig svekket, også hensyntas i vurderingen av foretakets interne styring. For mer om vurdering av kravene til foretakenes planer for å forebygge og å håndtere forretnings- og driftsmessige avbrudds- og krisesituasjoner, henvises det til modul for operasjonell risiko. For krav og vurderinger som vedrører foretakenes gjenopprettingsplaner, vises det til Finanstilsynets rundskriv 10/2019 med vedlegg.

Nedenfor følger aktuelle momenter:

- Foretaket må sikre at IKT-systemene er effektive og pålitelige og at foretaket vil være i stand til å fremskaffe presise og fullstendige data fra sine fagsystemer slik at samlet risiko kan beregnes og rapporteres tidsaktuelt for både enkelte forretningsenheter og for hele foretaket, i så vel normale som i situasjoner med stress.
- Foretaket bør være i stand til raskt å kunne tilpasse seg nye behov for risikorapportering, herunder ad hoc forespørsler som følge av endrede interne eller eksterne behov.
- Foretaket skal ha etablert retningslinjer, planer og hensiktsmessige verktøy, metoder og prosesser for å være best mulig forberedt på å håndtere ulike alvorlige forretnings- og driftsforstyrrelser som kan inntreffe, herunder planer for overgang til reserveløsninger på IKT-området, for utkontraktert virksomhet samt for gjenoppretting av kritiske funksjoner.
- Alle medarbeidere i foretaket bør være inkludert i en beredskaps-/kriseplan og alle medarbeidere bør være kjent med aktuelle planer og sitt ansvar i en krisesituasjon.
- Foretaket skal ha utarbeidet en troverdig gjenopprettingsplan med tiltak som vurderes som realistiske.

FINANSTILSYNET
Postboks 1187 Sentrum
0107 Oslo
POST@FINANSTILSYNET.NO
WWW.FINANSTILSYNET.NO