



Styret i Gjensidige Forsikring ASA
Postboks 700 Sentrum
0106 OSLO

VÅR REFERANSE
19/2846

DERES REFERANSE

DATO
27.02.2020

Tilsynsrapport

Finanstilsynet gjennomførte stedlig tilsyn i Gjensidige Forsikring ASA 28. og 29. mai 2019. Tema var overordnet styring og kontroll med Gjensidige-gruppas forsikringsvirksomhet, herunder med internmodellen. Til grunn for tilsynsrapporten ligger Finanstilsynets foreløpige tilsynsrapport av 9. september 2019 og styrets tilsvaret av 28. november 2019. Finanstilsynet har følgende merknader etter det stedlige tilsynet:

DEL 1. FORHOLD KNYTTET TIL RISIKONIVÅ OG KAPITALISERING

1 Risikoer

Som det framgår av tabell 1, bidrar forsikringsrisiko knyttet til skadeforsikring og finansiell risiko (markedsrisiko) mest til solvenskapitalkravet i kapitalkravsberegningen. Foretaket benytter en partiell internmodell til å beregne kapitalkravet for det vesentligste av forsikringsrisikoen og markedsrisikoen. Internmodellen er omtalt i punkt 2.

Tabell 1: Ansvarlig kapital, solvenskapitalkrav og solvenskapitaldekning per 31. desember 2019, i mrd. kroner.

	Gjensidige Forsikring gruppe
Tellende kapital	21,9
Skade- og helseforsikringsrisiko	7,6
Livsforsikringsrisiko	1,9
Markedsrisiko	7,9
Motpartsrisiko	0,5
Diversifisering	(5,0)
Basiskrav til solvenskapital	12,8
Operasjonell risiko	0,8
Justering for utsatt skatt	(3,0)
Solvenskapitalkrav	10,6
Solvenskapitaldekning prosent	206 %

Konsernpolicy for risikostyring og internkontroll, sist revidert i november 2019, angir de vesentlige risikotypene: forsikringsrisiko, finansiell risiko, operasjonell risiko (herunder compliancerisiko) og forretningsmessig- og strategisk risiko. Operasjonell risiko er i konsernpolicyen definert som "Risikoen for at potensielle hendelser eller forhold kan oppstå og gi en økonomisk konsekvens og/eller tap av omdømme. Operasjonell risiko skyldes menneskelige feil, svakheter i systemer, feil i prosesser eller eksterne hendelser.". Forretningsmessig- og strategisk risiko er definert som "Forhold som manglende evne til å etablere og implementere forretningsplaner og strategier, fatte

beslutninger, allokere ressurser eller respondere på endringer i omgivelsene." Finanstilsynet forstår det slik at forretningsmessig og strategisk risiko i kapitalkravssammenheng inngår i operasjonell risiko, se punkt 4 nedenfor.

2 Internmodellen

Foretaket fikk 31. januar 2018 tillatelse til å bruke en partiell internmodell til å beregne solvenskapitalkravet. Internmodellen omfatter det vesentligste av foretakets skadeforsikringsrisiko og markedsrisiko. Livsforsikringsrisiko, motpartsrisiko og operasjonell risiko, samt enkeltelementer og -porteføljer innen skadeforsikrings- og markedsrisiko beregnes etter standardmetoden. Tillatelsen ble gitt med vilkår og begrensninger. Foretaket må anvende standardmetoden for stormrisiko og for samvariasjon (korrelasjon) mellom forsikrings- og markedsrisiko. Inntil videre er modellendringer som reduserer solvenskapitalkravet søknadspårligte.

2.1 To modellversjoner

Finanstilsynet viste i foreløpig tilsynsrapport til at foretaket for enkelte formål fraviker modellen for regulatoriske formål, og ba styret redegjøre for beslutningsprosesser for bruk av "egen" internmodell og for hvordan denne blir validert. I sitt tilsvaer redegjør styret for bakgrunn og beslutningsprosesser. Det framgår av styrets svar at valideringen i det vesentligste omhandler modellen som brukes regulatorisk. Styret påpeker at alle endringer blir validert i forkant av søknad til Finanstilsynet om modellendringer. Finanstilsynet mener at dersom resultater fra den "egne" internmodellen skal brukes i egenvurderingen av risiko og solvens (ORSA) og kommuniseres utad, slik foretaket gjør i delårs- og årsrapportene, bør denne modellversjonen valideres. Finanstilsynet mener det bør framgå av ekstern rapportering om modellen er validert.

2.2 Vilkaer knyttet til kalibrering av modellen

Finanstilsynet påpekte i foreløpig tilsynsrapport at solvenskapitalkravet for premierisiko for enkelte produkter, herunder "øvrig" motorvognforsikring (ekskl. ansvar) for privatpersoner i Norge, var lavt sammenlignet med empirien. Det framgår av styrets svar at et parametersett fra en tidligere modellversjon feilaktig var lastet inn i modellen, noe som førte til en underrapportering av solvenskapitalkravet på drøyt 20 prosent for nevnte produkt. Feilen har også påvirket andre produkter, og samlet effekt av underrapporteringen av solvenskapitalkravet er på om lag 100 mill. kroner (1 prosent). Det framgår av styrets svar at foretaket har iverksatt tiltak for å unngå at dette gjentar seg. Finanstilsynet legger til grunn at foretaket korrigerer feilen slik at sammenligningstall fra tidligere perioder i framtidig års- og delårsrapportering er korrekte. *Foretaket bes redegjøre for iverksatte tiltak og status, samt eventuelle risikovurderinger av hendelsen, innen 31. mars 2020.*

Finanstilsynet registrerer at det i etterkant av tilsynet ble avdekket feil i diversifiseringseffektene innen markedsrisiko i parallellrapporteringen av solvenskapitalkravet før tillatelsen, og legger til grunn at feilen ikke har påvirket rapporteringen av solvenskapitalkravet til myndighetene og offentligheten.

Finanstilsynet påpekte i foreløpig tilsynsrapport at reduserte erstatningsavsetninger for yrkesskade- og trafikksforsikringer og enkelte andre produkter har ført til redusert estimert reserverisiko. I sitt tilsvaer viser styret til at de reduserte avsetningene representerer et beste estimat for erstatningene. Styret viser videre til at de største avviklingstapene i foretakets historikk gjennomgående inntreffer hyppigere ifølge modellen enn i historikken. Finanstilsynet vil påpeke at foretakets historikk ikke nødvendigvis er representativ for framtidige tap, særlig dersom den er basert på for høye

avsetninger. Finanstilsynet legger til grunn at foretaket kritisk vurderer begrensninger i egen datahistorikk i vurderingen av modellestimatene, særlig i tilfeller der foretaket gjør vesentlige endringer i grunnlaget for avsetningene.

I vilkårene for tillatelsen ba Finanstilsynet foretaket i større grad hensynta mulig underrapportering av skadebeløp for inntrufne, men ikke rapporterte skader (IBNR-skader) i kalibreringen av frekvensskadebeløp. Finanstilsynet påpekte i foreløpig tilsynsrapport at foretaket hadde utelatt nyere datapunkter i kalibreringen av frekvensskadebeløp for "øvrige" motorvognforsikring (ekskl. ansvar) for privatpersoner i Norge, selv om disse indikerte høyere skadebeløp. Det framgår av styrets svar at inkludering av de nye datapunktene ville hatt liten effekt på solvenskapitalkravet. Finanstilsynet fastholder at foretaket bør ha en konservativ tilnærming til å ekskludere datapunkter.

Finanstilsynet påpekte i foreløpig tilsynsrapport at foretaket hadde oppkalibrert den "egne" modellen for sjøforsikring på bakgrunn av nye data, men ikke endret modellen som brukes regulatorisk. Finanstilsynet presiserte at den utvidede søknadsplikten bare gjelder for endringer som reduserer solvenskapitalkravet, og at modellen bør oppkalibreres umiddelbart dersom valideringsresultater eller dataoppdateringer tilsier at enkelte risikoer er undervurdert. Styret svarer at kapitalkravet kan bli urimelig høyt dersom bare endringer som øker solvenskapitalkravet gjennomføres. Finanstilsynet fastholder at en forsiktig tilnærming tilsier at en mulig underestimert av risiko bør korrigeres raskere enn en mulig overestimert.

3 Klimarisiko

Finanstilsynet viste i foreløpig tilsynsrapport til at klimarisiko har vært omtalt i foretakets "emerging risk"-rapporter siden 2009 og til utførlig omtale av tiltak for å håndtere og begrense klimarisiko i årsrapporten for 2018. Finanstilsynet påpekte at klimarisiko ikke var omtalt i foretakets rapport om solvens og finansiell stilling for 2018 og at ingen av stress- og scenariotestene som er referert i egenvurderingen av risiko og solvens for 2018 omfatter klimarisiko. Finanstilsynet påpekte videre at analyser og modeller basert på historiske data kan undervurdere risikoen framover og at scenarioanalyser kan brukes til å vurdere hvordan virksomheten påvirkes av utviklingen i fysiske forhold, markeder og rammevilkår. Finanstilsynet ba i foreløpig tilsynsrapport om styrets kommentar, herunder styrets vurdering av behovet for økt vektlegging av klimarisiko i interne risikovurderinger og ekstern rapportering.

Det framgår av styrets svar at foretaket gjennom sin bærekraftstrategi har satt mål for hvordan foretaket skal bidra til reduksjon i klimautslipp gjennom skadeforebygging, skadeerstatningsprosesser og egne utslipp. Styret viser til at foretaket med skadeforebyggende tiltak hos kunder, og ved å bidra med kompetanse og skadedata til det offentlige, styrker evnen til å stå imot og tilpasse seg klimarelaterte skader. Styret opplyser at foretaket fortløpende vurderer underliggende trender som en integrert del av arbeidet med forsikringsrisiko og vurderer å ha god kontroll på gradvise endringer i risikobildet som klimaendringer er en del av. Styret opplyser at selv om det på enkelte områder observeres noe økende skadeomfang, som overvannsskader, forventes det at for fysisk risiko vil effektene mest sannsynlig skje gradvis og over en lengre tidsperiode. Styret ser likevel behov for å øke vektleggingen av klimarisiko i interne risikovurderinger og ekstern rapportering.

Det framgår av tilsvaret at stadig fler av foretakets investeringsbeslutninger er basert på vurderinger av klimarisiko og øvrige ESG-faktorer. Foretaket anser at det har kommet lengst innenfor eiendom når det gjelder strategi, måling og oppfølging. Foretaket investerer i eiendom gjennom direkte

investeringer og har kontroll på hele verdikjeden. For andre investeringer har foretaket ikke kommet like langt. Det skyldes blant annet begrenset tilgang til data og standardisering av informasjon om klimaavtrykk. Foretaket tar sikte på å gi anslag for investeringsporteføljens karbonavtrykk i årsrapporten for 2019.

Gjensidige vil i årsrapportene så langt som mulig etterleve rammeverket fra Financial Stability Boards "Task Force for Climate-related Financial Disclosures" (TCFD). Finanstilsynet legger til grunn at foretaket også vil inkludere klimarisiko i Rapport om solvens og finansiell stilling.

Finanstilsynet tar styrets svar til orientering. Finanstilsynet legger til grunn at styret vurderer hvordan stress- og scenariotester kan avdekke risiko knyttet til enkelte porteføljer eller risikofaktorer og at klimarisiko vies oppmerksomhet i ORSA.

4 Egenvurdering av risiko og solvens 2018

Finanstilsynet påpekte i foreløpig tilsynsrapport at foretaket bruker ulike scenarier i framskrivninger av kapitalposisjoner og stress- og sensitivitetstester av kapitalbehovet, og at valg av scenario ikke alltid er godt begrunnet. Videre påpekte Finanstilsynet at enkelte antagelser om prisfall på aksjer og eiendom og svekkede forsikringsresultater framsto som milde antagelser i en stresstest. Styret redegjør i svaret for valg av scenariene og opplyser om endringer i stresstester og scenarioanalyser. Det framgår av styrets svar at enkelte antagelser er mer konservative i egenvurderingen for 2019, som Finanstilsynet mottok 4. desember 2019. Finanstilsynet vurderer ikke endringene eller egenvurderingen for 2019 i denne endelige rapporten, men vil eventuelt gi en separat tilbakemelding.

Foretaket har testet tilstrekkeligheten av kapitalkravet for operasjonell risiko ved sju scenarier. Finanstilsynet påpekte at ingen scenarier ligger utenfor risikoområdene som er identifisert i internkontrollprosessen. Det gjelder blant annet tap knyttet til operasjonell risiko på investeringsområdet og operasjonell risiko i konsernriskoene. Det er dermed usikkert om scenariene er tilstrekkelige til å teste kapitalbehovet.

Styret opplyser i tilsvaret at foretaket har identifisert og kvantifisert de tapshendelseskategoriene som er beskrevet i Finanstilsynets modul for operasjonell risiko. Styret opplyser at scenariene er identifisert gjennom årlige risikovurderinger, hendelsesregistrering og eksterne kilder og dekker i enkelte tilfeller konsernriskoene der disse kan føre til operasjonelle tap som påvirker kapitalkravet. Det framgår av styrets svar at i den årlige risikoanalysen vurderes hvert år behovet for å inkludere et scenario på investeringsområdet, men sannsynligheten for en stor hendelse vurderes som så liten at det ikke har en vesentlig innvirkning på kapitalkravet.

Finanstilsynet legger til grunn at foretaket, som del av vurderingen av kapitalbehovet for operasjonell risiko også vurderer operasjonell risiko i forretningsmessig og strategisk risiko og behovet for å inkludere scenarier for slik risiko. Finanstilsynet anbefaler at vurderinger om hvorfor scenarier på vesentlige virksomhetsområder er utelatt framkommer klarere av egenvurderingen. Finanstilsynet vil for øvrig bemerke at modulen for operasjonell risiko som det refereres til er utarbeidet for bankområdet, og at vurderingene derfor bør tilpasses virksomheten i forsikringsforetak.

DEL 2. FORHOLD KNYTTET TIL STYRING OG KONTROLL

5 Styring og kontroll av internmodellen

5.1 Validering

Den årlige valideringen av internmodellen skal undersøke om det beregnede kapitalkravet er tilstrekkelig til å dekke risikoen i virksomheten, og etterprøve forutsetningene som ligger til grunn for modellen og parameterne som benyttes. I forbindelse med tilsynet fikk Finanstilsynet tilsendt styrebehandlet valideringsrapport for 2018, samt en utfyllende valideringsrapport til leder for risikostyring.

Finanstilsynet påpekte i foreløpig tilsynsrapport at manglende omtale av tester og resultater gjør det vanskelig å vurdere om valideringen etterprøver modellforutsetningene, parameterne og resultatene i henhold til kravene. Det framgår av styrets svar at valideringsrapporten for 2019 er omstrukturert med delrapporter som forklarer tester og resultater i mer detalj.

Valideringen omfatter scenarioanalyser hvor utslag av enkelthendelser eller negativ utvikling i porteføljer og markeder sammenlignes med solvenskapitalkravet, både separat for forsikringsrisiko og markedsrisiko og samlet. Finanstilsynet reiste i foreløpig tilsynsrapport spørsmål om scenariene er alvorlige nok til å teste kapitalbehovet i et ett av 200-årsscenario. Finanstilsynet registrerer at valideringsrapporten for 2019 skal inneholde flere og mer alvorlige scenarier for markedsrisiko. Finanstilsynet fastholder at sammenligninger av tap i enkeltscenarier med solvenskapitalkravet må ta høyde for at scenariene ikke nødvendigvis representerer et ett av 200-årsscenario.

Finanstilsynet påpekte i foreløpig tilsynsrapport at enkelte anbefalinger fra valideringen for 2017 ikke er fulgt opp. Det framgår av styrets svar at administrasjonen vil gjennomgå oppfølging av valideringsfunn og utestående anbefalinger.

Finanstilsynet ber om å få tilsendt styrebehandlet valideringsrapport for 2019, referat fra styrebehandlingen og foretakets planer for oppfølging av funn i valideringen.

5.2 IT-risiko

I vilkårene for tillatelsen til bruk av internmodell la Finanstilsynet til grunn at foretaket gjennomfører planlagte tiltak for å sikre modellen mot uautoriserte endringer, sikre kvalitet og integritet i modell og regneark og følge opp leverandører og leveranser fra disse. Modellutviklingsenheten presenterte under tilsynet sitt arbeid med risikoreduserende tiltak, herunder implementering av en standard for utvikling og bruk av regneark. I foreløpig tilsynsrapport la Finanstilsynet til grunn at styret påser at det er nødvendig og tilstrekkelig styring og kontroll av IT-risikoen i modellen.

Finanstilsynet merker seg fra tilsvaret at styret vil påse at det fortsatt er fokus på styring og kontroll av IT-risikoen i modellen. Feilrapporteringen av solvenskapitalkravet omtalt i punkt 2.2 viser hvor viktig det er å styre IT-risiko knyttet til modellen.

5.3 Internrevisjon

I foreløpig tilsynsrapport kommenterte Finanstilsynet at internrevisjon av internmodellen var begrenset til gjennomgang av valideringen og at det ikke framgår av revisjonsrapporten hvilke

tester som er gjennomført og hvordan disse er valgt ut. Finanstilsynet ba styret kommentere om gjennomgangen var tilstrekkelig.

Finanstilsynet bemerket videre at en separat revisjon av IT-risikoen i internmodellen ikke står på revisjonsplanen, men at det var planlagt revisjoner av flere IT-områder, som er relevante for IT-risikoen i modellen. Finanstilsynet la til grunn at internrevisjonen oppsummerer og tydeliggjør forhold fra revisjonene som berører internmodellen.

I sitt tilsvaret viser styret til "validation instruction" og revisjonsmetodikken. Styret opplyser at antall og type tester er utførlig omtalt i revisjonsbekreftelsen for internmodellvalidering i 2019, og at bekreftelsen gjengir relevante observasjoner og funn fra andre revisjoner.

Finanstilsynet forutsetter at styret i behandlingen av revisjonsbekreftelsen vurderer om en gjennomgang av valideringen er tilstrekkelig som revisjon av internmodellen, og tar særskilt stilling til om IT-revisjon av internmodellen bør settes på revisjonsplanen.

Finanstilsynet ber om å få tilsendt revisjonsbekreftelsen for internmodellvalideringen i 2019 og referat fra styrebehandlingen.

6 Overordnet styring og kontroll

6.1 Strategi

Det kan oppstå målkonflikter mellom foretakets bærekraftsmål og mer kortsiktige lønnsomhetsmål ved spørsmål om forsikring av ny virksomhet eller teknologi i overgangen til et lavutslippssamfunn. Finanstilsynet ba om styrets vurdering av behovet for å gi administrasjonen strategiske føringer for håndtering av målkonflikter mellom bærekraftsmål og andre virksomhetsmål.

Det framgår av styrets svar at detaljerte vurderinger av risikoappetitt for spesifikke bransjer bør gjøres med hensyn til kompetanse og evne til å håndtere og vurdere forsikringsrisiko. Styret vil innenfor denne rammen påse at bærekraftsmål er et moment i diskusjoner om og prioriteringer av virksomhetsmål framover.

6.2 Overordnede retningslinjer

6.2.1 Konsernpolicy for risikostyring og internkontroll

Finanstilsynet kommenterte i foreløpig tilsynsrapport enkelte forhold i konsernpolicy for risikostyring og internkontroll. Etter Finanstilsynets vurdering bør foretaket angi førstelinjelederens styrings- og kontrollansvar i konsernpolicyen slik det angis for andre- og tredjelinjefunksjoner. Finanstilsynet stilte videre spørsmål ved om policyen bør sette krav til risikogjennomgang før større endringer i virksomheten og ved alvorlige hendelser.

Finanstilsynet registrerer at revidert konsernpolicy angir førstelinjelederens styrings- og kontrollansvar og presiserer at førstelinjen skal gjennomføre en risikovurdering som del av beslutningsgrunnlaget for større endringer. Finanstilsynet legger til grunn at styret vurderer om policyen bør stille krav om risikogjennomgang ved alvorlige hendelser.

6.2.2 Beredskap og kontinuitet

Finanstilsynet stilte i foreløpig tilsynsrapport spørsmål ved om strategien for krise og beredskap og arbeidet med forretningsmessig kontinuitet har tilstrekkelig forankring i foretaket.

Styret svarer at beredskapsarbeidet har bred forankring i ledelse og styre, og viser til at gruppens styrevedtatte sikkerhetspolicy stiller krav til kontinuitets- og beredskapsledelse og at det årlig gjennomføres opplæring og øvelser. Finanstilsynet merker seg at styret i forbindelse med omorganisering og styrking av det operative sikkerhetsarbeidet, vil påse at styrende dokumenter, organisering og planer knyttet til krise og beredskap tydeliggjøres og forankres ytterligere.

6.3 Organisering og ansvarsforhold

6.3.1 Andrelinjefunksjoner

Aktuar-, compliance- og risikostyringsfunksjonene er organisert under finansdirektør. Foretaket opplyste at ved beslutning om administrativ tilhørighet, ble hensynet til at andrelinjefunksjonene skal tilhøre et større fagmiljø tillagt stor vekt. Andrelinjefunksjonene har faglige rapporteringslinjer direkte til daglig leder og styret.

Finanstilsynet forutsatte i foreløpig tilsynsrapport at styret og daglig leder påser at de valgte administrative løsningene ikke begrenser andrelinjefunksjonenes autoritet, faglige integritet og selvstendige vurderinger.

Det framgår av styrets svar at andrelinjefunksjonenes uavhengighet sikres ved at daglig leder ansetter og fastsetter lønn og andre betingelser, som er uavhengig av foretakets resultat, og at de ikke kan avsettes uten samtykke fra styret. Etter styrets vurdering begrenser de valgte administrative løsningene ikke andrelinjefunksjonenes autoritet, faglige integritet og selvstendige vurdering.

Etter Finanstilsynets oppfatning bør kontrollfunksjoner (andrelinjefunksjoner) rendyrkes for å sikre tilstrekkelig uavhengighet fra utøvende funksjoner (førstelinjefunksjoner). Finanstilsynet mener at leder av den enkelte kontrollfunksjon organisatorisk bør være direkte underlagt daglig leder.

6.4 Risikorapportering

Foretaket har en rekke risikorapporter. Styret får årlig en samlet vurdering av risikosituasjonen med forslag til konsernrisikoer for kommende år og kvartalsvis rapportering om utviklingen i disse. I tillegg har foretaket blant annet risikorapporter fra kontrollfunksjoner og konsernroller. Flere av disse rapportene peker på andre risikoer enn konsernrisikoene.

Finanstilsynet stilte i foreløpig tilsynsrapport spørsmål ved om risikorapportene til styret, gir styret tilstrekkelig oversikt over Gjensidiges risikobilde. Finanstilsynet viste til at det ikke kommer klart fram av rapportene hva som kan gå galt og påvirke foretakets evne til å nå mål og strategier, og hvilke risikoreducerende tiltak som er iverksatt eller skal iverksettes. Finanstilsynet viste til eksempler på risikorapporter som har mer preg av å være statusrapporter om pågående arbeid enn en oppdatering av risikobilde og konkretisering av risikoer.

Styret redegjør i tilsvaret for prosesser og arbeid med blant annet konsernrisikoer, operasjonelle risikoer og forretningsmessige og strategiske risikoer, herunder om risikorapportering til ulike

nivåer i organisasjonen. Når det gjelder forretningsmessig og strategisk risiko framgår det av styrets svar at foretaket vil igangsette et arbeid for å forbedre oppfølging og rapportering.

Etter det Finanstilsynet kan se, kommenterer eller besvarer styret ikke Finanstilsynets spørsmål og kommentarer til innholdet i risikorapporteringen, men begrenser svaret til en omtale av prosessene. Finanstilsynet er derfor fortsatt i tvil om risikorapportene gir styret nødvendig, fullstendig og samlet oversikt over risikobildet. Finanstilsynet merker seg imidlertid at foretaket vil igangsette et arbeid for å forbedre oppfølging og rapportering av forretningsmessig og strategisk risiko.

7 Styring av operasjonell risiko

7.1 Operasjonell risiko

I foreløpig tilsynsrapport påpekte Finanstilsynet at foretakets styring av operasjonell risiko framstår som mangelfull og bør forbedres. Innsendte risikorapporter kan tyde på at foretaket har begrenset operasjonell risiko til faktiske hendelser, compliance og informasjonssikkerhet. Videre påpekte Finanstilsynet at det generelt er lite omtale av risikoreduserende tiltak i rapportene, og at flere av rapportene har preg av å være oppsummerende årsrapporter framfor konkretisering av risikoer. Rapporteringen framsto for Finanstilsynet som lite helhetlig. Finanstilsynet stilte spørsmål ved om rapporteringen er egnet til å gi styret og ledelsen en samlet oversikt over operasjonell risiko og styringen av denne.

Finanstilsynet viste til at konsernrevisjonen i sin rapport fra revisjon av operasjonell risikostyring fra oktober 2018, peker på vesentlige svakheter. Revisjonen påpekte et behov for løpende oppfølging av risikoer og risikoreduserende tiltak, ikke bare årlig. Revidert enhet, konsernansvarlig for operasjonell risiko, var ikke enig og viste til at hyppigere oppfølging av risikoer og tiltak vil kreve mer støtte til linjeledelsen fra risiko- og compliance-koordinatorene i førstelinjen og fra andrelinjen. Finanstilsynet påpekte i foreløpig tilsynsrapport at ansvaret for risikostyring og internkontroll i egen enhet ligger hos den enkelte linjeleder.

Finanstilsynet ba styret påse at foretaket forbedrer sitt arbeid med operasjonell risiko og styring av denne. Tilsynet presiserte at dette innbefatter helhetlig rapportering, at styret bør forvise seg om at risikoreduserende tiltak med ansvarlige og tidsfrister for gjennomføring er dokumentert og blir fulgt opp, og at det bør være mulig å følge utviklingen av risikoene over tid. Finanstilsynet ba om styrets kommentar, herunder til bemerkningene angående revidert enhets tilsvaret til revisjonsrapporten om operasjonell risikostyring.

Finanstilsynet kan ikke se at styret i sitt tilsvaret har kommentert Finanstilsynets synspunkter og bemerkninger vedrørende oppfølging av operasjonell risiko, eller påpekt feil eller misforståelser i foreløpig tilsynsrapport. Tilsvaret gir dermed ikke noen avklaring eller innblikk i hvordan styret vurderer konsernets operasjonelle risikoer eller arbeidet med og styringen av operasjonell risiko. Det framgår imidlertid av styrets svar at styret vil be administrasjonen igangsette arbeid for å forbedre rapportering og oppfølging av operasjonell risiko. Finanstilsynet legger til grunn at styret med dette anerkjenner Finanstilsynets vurderinger, og Finanstilsynet opprettholder på denne bakgrunn sine foreløpige vurderinger om at styringen av operasjonell risiko framstår som mangelfull. Finanstilsynet forutsetter at forbedringsarbeidet prioriteres og følges opp av styret.

7.2 IT-risiko

I foreløpig tilsynsrapport viste Finanstilsynet til IT-virksomhetens vesentlige betydning for foretaket. Flere av konsernriskoene er IT-relaterte og det pågår omfattende IT-satsinger og endringer, blant annet et infrastruktur-prosjekt, nytt kjernesystem, omfattende utkontraktering, nye avtaler, økt bruk av skytjenester og bruk av flere nye leverandører.

Finanstilsynet påpekte at det ikke framkom av tilsynsdokumentasjonen at det har vært utarbeidet en helhetlig risikovurdering av konsernets IT-virksomhet. Etter Finanstilsynets vurdering var risikovurderingen av IT, som for annen operasjonell risiko, fragmentert og ga ikke et helhetlig bilde av IT-risikoen. Finanstilsynet ba styret sørge for en helhetlig rapportering av IT-risiko.

Finanstilsynet viste til IKT-forskriftens krav til risikoanalyser, hendelsesrapportering og at mangelfull etterlevelse har vært påpekt tidligere. Finanstilsynet ba styret påse at IKT-forskriften etterleves.

Det framgår av styrets svar at prosesser for håndtering av IT-hendelser er gjennomgått og at foretaket vil rapportere til Finanstilsynet om hendelser i utenlandske filialer og orientere om hendelser i utenlandske datterforetak. Finanstilsynet tar styrets svar til etterretning.

Styret gir ingen kommentarer til Finanstilsynets påpekning om mangelfulle risikovurderinger, men beskriver hvordan det arbeides med risikovurderinger på IT-området. Styret kommenterer ikke tilsynets påpekning av mangelfull etterlevelse av IKT-forskriften, men refererer til foretakets prosess for vurdering av etterlevelse av forskriften. Etter det Finanstilsynet kan se, påpeker heller ikke styret feil eller misforståelser i foreløpig tilsynsrapport, og Finanstilsynet fastholder at risikovurderingene framstår som lite helhetlige. Etter Finanstilsynets vurdering medfører foretakets omfattende IT-satsninger og endringer en betydelig risiko. Finanstilsynet forutsetter at styret påser at styringen av operasjonell risiko i IT-virksomheten styrkes. *Finanstilsynet ber om en statusrapport for arbeidet innen utgangen av 2020.*

Finanstilsynet antar at etableringen av datterforetaket Gjensidige Business Services AB, som skal være gruppens hovedleverandør av IT-tjenester og IT-leveranser, medfører økt operasjonell risiko en periode inntil den nye leverandøren fungerer som forutsatt. Organisering, roller, ansvar, prosesser og rutiner, samt økt behov for koordinering og oppfølging er stikkord i denne sammenheng. Finanstilsynet legger til grunn at styret påser at risikoen i tilknytning til det nye datterforetaket vurderes, rapporteres og styres i tråd med gruppas rammer, og sees i sammenheng med gruppas øvrige risikoer.

*

Finanstilsynet ber om å motta kopi av protokollen fra styremøtet hvor Finanstilsynets tilsynsrapport blir behandlet. Kopi av dette brevet bes sendt til ekstern og intern revisor.

For Finanstilsynet

Hege Bunkholt Elstrand
seksjonssjef

Ellen Jakobsen
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.