FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Sparebank 1 Østlandet
Postboks 203
2302 HAMAR

VÅR REFERANSE	DERES REFERANSE		DATO
21/8667			13.05.2022

Tilsynsrapport

Finanstilsynet gjennomførte stedlig tilsyn i SpareBank 1 Østlandet (banken) 13.-14. oktober 2021. Tilsynet hadde som formål å vurdere bankens styring og kontroll med IT-området, herunder de tre forsvarslinjer (3 lines of defence).

Til grunn for disse merknadene ligger Finanstilsynets foreløpige tilsynsrapport datert 9. februar 2022 og styrets kommentarer til foreløpig tilsynsrapport i brev av 3. mars 2022.

Finanstilsynet har følgende bemerkninger etter det stedlige tilsynet.

IT-risiko i bankens styrende dokumenter

Finanstilsynet pekte i foreløpig rapport på viktigheten av å ha IT-risiko klart definert og innlemmet i styrende dokumenter.

Det fremgår av styrets svar at bankens definisjon av operasjonell risiko vurderes å dekke IT-risiko. Styret påpeker videre i sitt svar at det foreligger standarder og retningslinjer for å vurdere risiko relatert til informasjonssikkerhet.

Finanstilsynet understreker viktigheten av at bankens vurdering av, og kriterier for, akseptabel risiko på IT-området hensyntar relevant regelverk, rundskriv og retningslinjer.

Risikotoleranse knyttet til bankens bruk av IT

Finanstilsynet pekte i foreløpig tilsynsrapport på at foretakets indikatorsett for risikovilje og -evne var uegnet til vurderinger av operasjonell risiko, herunder IT-risiko. Det framgår av IKT-forskriften § 3 Risikoanalyse at foretak skal fastsette kriterier for akseptabel risiko forbundet med bruk av IT. Finanstilsynet anser det som ikke tilfredsstillende at banken baserer oppfølging og rapportering av operasjonell risiko på gjeldende indikatorsett.

Det framgår av styrets svar at bruk av pilar 2-kravene som referanse ved styrets vurdering av risikotoleranse er for å knytte det opp mot soliditet og signalisere at dette er en "*risikokategori styret ikke ønsker å anvende pilar 2-kapital på*". Styret viser videre til at "*implisitt innebærer dette at styret ønsker at banken skal ha så god styring og kontroll at banken skal karakteriseres ved få og små operasjonelle tap, som ikke skal kunne skade konsernets soliditet, resultat eller omdømme i*

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00

post@finanstilsynet.no
www.finanstilsynet.no

Saksbehandler
Aksel Palm
Dir. tlf 22 93 98 00

vesentlig grad". Videre skriver styret at de oppfatter at banken tar høyde for reell operasjonell risiko knyttet til mulige hendelser, her med henvisning til øvrig styrende dokumentasjon som foreligger. Styret skriver også at banken, basert på internrevisjonens anbefalinger og bemerkninger fra Finanstilsynet, vil vurdere indikatorsettet som anvendes ved neste ordinære revidering av styringsdokumentasjonen.

Finanstilsynet fastholder sin vurdering om at bankens bruk av nevnte indikatorsett ikke er tilstrekkelig egnet til styring og kontroll med operasjonell risiko, siden det fastsettes annethvert år og tar utgangspunkt i vurderinger gjort av andre enn banken selv. Videre anser Finanstilsynet det hensiktsmessig for banken å bruke et indikatorsett for risikovilje og -evne som utledes av og kan sees i direkte sammenheng med bankens uttalte risikotoleranse.

Finanstilsynet legger til grunn at styret påser at indikatorsettet revideres for å holde oversikt, kontrollere og styre operasjonell risiko.

IT-ressurser i andrelinjen

Finanstilsynet pekte i foreløpig rapport på at bankens andrelinje ikke hadde dedikerte IT-ressurser for oppfølging og kontroll av IT-relaterte aktiviteter i førstelinjen. Videre pekte Finanstilsynet på at andrelinjen i enkelte tilfeller ved IT-relaterte spørsmål må konsultere med IT-ressursene i førstelinjen.

Det framgår av styrets svar at "*Styret er enig med Finanstilsynet i viktigheten av at andrelinjefunksjonene har tilstrekkelig kompetanse og kapasitet*". Videre framgår det av styrets svar at en ny vurdering av kompetanse og ressursbehov knyttet til andrelinjefunksjonene vil gjøres.

Finanstilsynet forventer at styrets vurderinger om ressurser og kompetanse tar utgangspunkt i andrelinjefunksjonenes nåværende kompetanse- og ressurssituasjon.

Kontrollarbeid i risikostyringsfunksjonen

Finanstilsynet bemerket i foreløpig tilsynsrapport at kontrollaktiviteter som utføres av bankens risikostyringsfunksjon opp mot bankens IT-virksomhet skjer i et begrenset omfang og med manglende dokumentering. Finanstilsynet viste videre til internrevisjonens anbefalinger om at banken bør vurdere behovet for å etablere flere kontroller.

Av styrets svar framgår det at risikostyringsfunksjonens årsplan for 2022 er gjennomgått av styrets risikoutvalg. Finanstilsynet registrerer fra styrets svar at det i 2021 ble gjennomført et arbeid for å supplere og dokumentere kontrollaktiviteter i risikostyringsfunksjonen, og at disse er samlet i en egen kontrollplan – som også er behandlet av styrets risikoutvalg.

Finanstilsynet tar styrets svar til orientering, og merket seg at risikostyringsfunksjonens årsplan ble behandlet av styrets risikoutvalg. Finanstilsynet ber banken om å oversende risikostyringsfunksjonens kontrollplan for 2022.

Nøkkelpersonsrisiko i andrelinjen

Finanstilsynet bemerket i foreløpig rapport at bemanningen av bankens etterlevelsesfunksjon i andrelinjen utgjør en nøkkelpersonsrisiko, da det er ett årsverk som bemanner denne funksjonen. Finanstilsynet reiste også spørsmål om bankens avtale om bruk av eksterne ressurser ved utilgjengelighet av bankens ene årsverk i funksjonen er tilstrekkelig for å håndtere nøkkelpersonsrisikoen.

Av styrets svar framgår det at styret er kjent med at det foreligger en "*potensiell nøkkelpersonrisiko"* i bankens etterlevelsesfunksjon. Videre framgår det at risikoen har vært diskutert ved flere anledninger, og at det på den bakgrunn ble inngått avtale om bruk av en dedikert ekstern ressurs ved behov. Styret viser til at den dedikerte ressursen på konsulentoppdrag har større involvering i etterlevelsesarbeid i banken, enn hva Finanstilsynet bemerket i foreløpig tilsynsrapport. Videre skriver styret at de vil ha fokus på nøkkelpersonrisiko, kompetanse og kapasitet i andrelinjefunksjonene i banken.

Finanstilsynet forventer at styret sørger for at nøkkelpersonrisikoen er på et forsvarlig nivå og at vurderinger knyttet til nøkkelpersonrisiko tar utgangspunkt i bemanningssituasjonen i etterlevelsesfunksjonen.

Internkontrollverktøy

Finanstilsynet pekte i foreløpig rapport på at arbeidet med risiko opp mot sikkerhet og tilhørende kontroller hadde forbedringsmuligheter om det ble organisert i verktøy hvor koblinger mellom risikovurderinger og kontroller kommer tydeligere fram. Finanstilsynet viser videre til internrevisjonens rapporter, der det framgår at det er behov for tydeligere veiledning knyttet til hendelsesregisteringen. Banken har også et pågående arbeid med å implementere et nytt GRC-system (Governance, Risk and Compliance).

Av styrets svar fremgår det at det løpende arbeides med å bedre rapporteringskulturen for registrering av uønskede hendelser. Styret viser videre til at konfigurering og implementering av nytt GRC-system skjer gjennom samarbeid i SpareBank 1-alliansen, hvor første fase er levert og implementert i banken i løpet av første kvartal 2022.

Finanstilsynet tar styrets svar til etterretning og ber om få oversendt status for implementering av første fase på prosjektet.

Kopi av dette brevet bes sendt til bankens valgte revisor.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Aksel Palm
seniorrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.