FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Styret i SPAREBANK 1 SØR-NORGE ASA
Postboks 250
4068 STAVANGER

Vår referanse
25/3086
Deres referanse

12.09.2025

Tilsynsrapport Sparebank 1 Sør-Norge

1. Innledning

Finanstilsynet gjennomførte IKT-tilsyn 6. og 7. mai 2025 i Sparebank 1 Sør-Norge ASA (heretter omtalt "banken" eller "foretaket"). Formålet med tilsynet var å gjøre en vurdering av hvordan foretaket administrerer, utvikler, drifter, vedlikeholder og sikrer IKT-systemer og -tjenester. For dette området så tilsynet på styring med og kontroll av IKT-virksomheten. Tilsynet vektla systemløsninger som støtter foretakets kjernevirksomhet og prioriterte IKT-systemer som foretaket har utkontraktert.

Til grunn for disse merknadene ligger Finanstilsynets foreløpige rapport datert 5. juni 2025 og styrets kommentarer til rapporten i brev av 7. august 2025.

2. Finanstilsynets oppsummering

Tilsynsrapporten er utarbeidet med utgangspunkt i IKT-forskriften, som var gjeldende regelverk for foretaket på tilsynstidspunktet. Fra 1. juli 2025 skal foretaket etterleve DORA-forordningen med tilhørende delegerte kommisjonsforordninger, jf. DORA-loven § 1.

Tilsynet avdekket ingen vesentlige mangler ved foretakets styring med og kontroll av IKT-virksomheten. Foretakets overordnede risikostyring har noen mindre påpekninger, blant annet knyttet til oppfølging av styringsdokumenter, operasjonalisering av virksomhetens konsekvensanalyse for å styre prioriteringer i foretakets kontrollhandlinger, risikovurdering av IKT-virksomheten, rapportering av IKT-risiko og internkontroll av IKT-området.

3. Finanstilsynets vurderinger

3.1. Strategi og organisering

Foretaket skal ha klare og hensiktsmessige styrings- og kontrollsystemer samt hensiktsmessige retningslinjer og rutiner for å styre, overvåke og rapportere risiko foretaket er eller kan bli eksponert for, jf. finansforetaksloven § 13-5 første ledd. IKT-forskriften § 2 første ledd stiller videre krav til at foretaket skal fastsette overordnede mål, strategier og sikkerhetskrav for IKT-virksomheten.

Finanstilsynet pekte i foreløpig tilsynsrapport på sine forventninger om at styregodkjente styringsdokumenter følges opp for å sikre at bankens planer og drift utføres i henhold til disse, samt at bankens andre- og tredjelinje følger opp etterlevelse av strategier og kontrollerer at de styrende dokumentene er operasjonalisert i henhold til disse.

Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00
post@finanstilsynet.no
finanstilsynet.no

Saksbehandler
Stig Ulstein
Dir. tlf. 22 93 99 66

Styret skriver i sitt svar at banken vil fortsette med å kontinuerlig styrke operasjonalisering, oppfølging og kontroll av etterlevelse av styrende dokumenter i alle forsvarslinjene innen alle relevante IKT-områder.

Finanstilsynet tar styrets svar til etterretning.

3.2. Virksomhetens konsekvensanalyse

Det skal foreligge oppdatert dokumentasjon av det enkelte IKT-system som er av betydning for foretakets virksomhet ifølge IKT-forskriften § 13. Hensiktsmessige planer og tiltak for tilgjengelighet og kontinuitet bør etableres med utgangspunkt i konsekvensanalyser for foretakets kritiske forretningsprosesser. Virksomhetens konsekvensanalyse skal bidra til å sikre at foretakets beredskapsplaner utarbeides med basis i forretningsmessig kritikalitet. Planene skal basere seg på foretakets prioriteringer for gjenoppretting av forretningskritiske tjenester og prosesser. Prioriteringene for gjenoppretning skal basere seg på resultatene fra analysen hvor det også skal framgå hva som er akseptabel nedetid for det enkelte IKT-system. Beredskapsplanene, som viser foretakets prioriteringer for gjenoppretting, bør formidles til relevante leverandører. For å verifisere at det er etablert fungerende planer og løsninger må det foretas regelmessig opplæring, øvelse og testing, jf. IKT-forskriften § 11.

Finanstilsynet bemerket i foreløpig tilsynsrapport at kravene fra virksomhetens konsekvensanalyse i større grad bør operasjonaliseres og styre prioriteringer i foretakets kontrollhandlinger i alle forsvarslinjer.

Styret skriver i sitt svar at det gjennomføres oppfølgingsmøter med strategiske leverandører der virksomhetsmessig konsekvensanalyse blir benyttet som et oppfølgingsverktøy. Styret skriver videre at banken vil øke bruken av virksomhetsmessig konsekvensanalyse i forbindelse med styring og kontroll internt og i oppfølging av leverandører.

Finanstilsynet tar styrets svar til etterretning.

3.3. Kontrollfunksjoner

I finansforetaksloven § 13-5 andre ledd stilles det krav om at et finansforetak skal ha uavhengige kontrollfunksjoner med ansvar for risikostyring, etterlevelse, internrevisjon og aktuarfaglige oppgaver. Foretakets uavhengige kontrollfunksjoner i andre forsvarslinje skal ha tilstrekkelig kompetanse tilpasset risikoen ved og omfanget av virksomheten i foretaket. Det framgår av CRR/CRD-forskriften § 38 og § 39.

Finanstilsynet pekte i foreløpig tilsynsrapport på viktigheten av at andrelinjefunksjoner i sin oppfølging av IKT-risiko gjennomfører egne kontroller av IKT-tjenesteleverandører. Videre forventes det at banken sikrer tilstrekkelig ressurser og kompetanse på IKT-området for å kunne utføre nødvendige kontrolltiltak.

Styret skriver i sitt svar at de tar Finanstilsynets vurdering til etterretning, og vil sikre at andrelinjefunksjonene etablerer tiltak for å videreutvikle oppfølgings- og kontrollregime av IKT-risiko og hos IKT-tjenesteleverandører. Videre deler styret Finanstilsynets vurdering om viktigheten av tilstrekkelig kapasitet og kompetanse i andrelinje for å sikre god oppfølging og kontroll av IKT-virksomheten.

Finanstilsynet tar styrets svar til etterretning.

3.4. IKT-drift

IKT-forskriften § 9 stiller krav om prosedyrer for avviks- og endringshåndtering. Prosedyrene for avvikshåndtering skal omfatte alle avvik som oppstår i driften av IKT-systemene. Videre skal de sikre forsvarlig og formell behandling av avviket, at årsaken til avvik identifiseres og at det iverksettes tiltak for å hindre gjentagelser. Prosedyrene for håndtering av endringer skal omfatte alle endringer som kan påvirke IKT-systemene og skal sikre forsvarlig, formell behandling og dokumentering av disse. Foretaket skal sikre at prosedyrene for endringshåndtering gir en stabil, planlagt og forutsigbar drift.

3.4.1. Endringshåndteringsprosess

Finanstilsynet skrev i foreløpig tilsynsrapport at det bør rapporteres på utvikling i antall forhåndsgodkjente endringer og sammenheng med driftsstabilitet, samt at kontrollfunksjonene bør utføre kontroller for å sikre at kriterier for forhåndsgodkjenning er oppfylt.

Styret skriver i sitt svar at banken vil sikre at sammenhengen mellom antall forhåndsgodkjente endringer og forholdet til driftsstabilitet gjennomgås og følges opp. Videre vil kontrollfunksjonene gjennomføre kontroller av at kriterier for forhåndsgodkjenning er oppfylt.

Finanstilsynet tar styrets svar til etterretning.

3.4.2. Beredskapsplaner

Finanstilsynet pekte i foreløpig tilsynsrapport på at bankens endringsprosess bør inkludere kontroll av om en endring kan medføre behov for justering av beredskapsplanene.

Styret skriver i sitt svar at banken vil sikre at endringsprosessen inneholder kontroll av om endringer fordrer en oppdatering av gjeldende beredskapsplaner for IT-operasjonen.

Finanstilsynet tar styrets svar til etterretning.

3.5. Utkontraktering

I henhold til IKT-forskriften § 2 skal foretaket ha retningslinjer for å sikre at utkontraktert IKT-virksomhet oppfyller kravene i § 12. Dette gjelder blant annet krav til skriftlig avtale, der avtalen skal sikre foretakets rett til å kontrollere, herunder revidere leverandørens aktiviteter, samt Finanstilsynets tilgang til opplysninger og mulighet for å føre tilsyn hos IKT-leverandøren. Videre framgår det av § 12 at foretaket har ansvar for at IKT-virksomheten oppfyller alle krav som stilles i forskriften og at dette også gjelder der hele eller deler av IKT-virksomheten er utkontraktert. Av bestemmelsene i § 13 framgår det at foretaket skal sikre at det har en samlet oppdatert dokumentasjon over organisasjon, utstyr, IKT-systemer og vesentlige forhold i IKT-virksomheten.

Finanstilsynet pekte i foreløpig tilsynsrapport på at desentralisert oppfølging av IKT-tjenester kan medføre ulik grad og kvalitet på oppfølging av den utkontrakterte virksomheten, og at det derfor må sørges for at det er tilstrekkelig kompetanse og ressurser hos kontrakteier for å sikre god kvalitet på oppfølging av leverandør.

Styret skriver i sitt svar at banken har en etablert rolle som fagansvarlig for utkontraktering og at oppfølgingen av bankens strategiske leverandører nå er sentralisert for å sikre en enhetlig tilnærming. Videre vil banken sikre at kontrakteiere har tilstrekkelig kompetanse og ressurser for å sikre god kvalitet på oppfølging av utkontraktert IKT-virksomhet.

Finanstilsynet tar styrets svar til etterretning.

3.6. Beredskap

I IKT-forskriften § 11 framgår kravene til at foretaket skal ha en dokumentert kriseplan som skal kunne iverksettes dersom IKT-driften ikke kan opprettholdes som følge av en krise. Det skal minst årlig gjennomføres opplæring, øvelse og testing av at kriseløsningen virker som forutsatt. Resultatet av testen skal dokumenteres.

Finanstilsynet pekte i foreløpig rapport på at ved testing av beredskapsplaner, både for foretakets egne og for utkontrakterte IKT-tjenester, må relevante informasjonssikkerhetsscenarioer inngå, der også verstefallsscenarioer er inkludert i beredskapstestingen. Videre legges det til grunn at planverk for gjenoppretting og alternativ drift testes, for eksempel i scenarioer ved langvarig utilgjengelighet av tjenester, og utføres i henhold til interne instrukser.

Styret presiserer i sitt svar at det er gjennomført grundige scenarioanalyser og stresstester av operasjonell risiko inkludert cyber på konsernnivå, men tar likevel Finanstilsynets påpekning til etterretning som innspill i det videre arbeidet med scenarioanalyser og beredskapstestingen.

Finanstilsynet pekte videre på at tilsynet forventer at banken gjennomfører egne vurderinger av om testing som gjennomføres av leverandør er tilfredsstillende sett opp mot kravene fra virksomhetens konsekvensanalyse.

Styret tar Finanstilsynet vurdering til etterretning, og vil sikre at det gjennomføres nødvendige dokumenterte vurderinger av om leverandørens beredskapstesting er tilfredsstillende sett opp mot kravene fra virksomhetens konsekvensanalyse.

Finanstilsynet tar styrets svar til etterretning.

4. Videre oppfølging

Videre oppfølging Finanstilsynet ber om å motta kopi av protokollen fra styremøtet hvor Finanstilsynets tilsynsrapport blir behandlet.

Vi ber foretaket sende kopi av dette brevet til valgt revisor.

For Finanstilsynet

Olav Johannessen
seksjonsleder

Stig Ulstein
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk.