FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Styret i Sparebank 1 SMN
Postboks 4796 Torgarden
7467 TRONDHEIM

Vår referanse
25/10707
Deres referanse

05.06.2026

Tilsynsrapport

1 Innledning

Finanstilsynet har gjennomført IKT-tilsyn med SpareBank 1 SMN (foretaket). Formålet med tilsynet var å gjøre en vurdering av hvordan foretaket administrerer, utvikler, drifter, vedlikeholder og sikrer IKT-systemer og -tjenester. Finanstilsynet så på foretakets styring med og kontroll av IKT-virksomheten med spesiell vekt på hvordan foretaket overholder regulatoriske krav knyttet til bruk av IKT-tjenesteleverandører, samt håndtering av IKT-risiko, IKT-sikkerhet og beredskapsarbeid. Tilsynet var i tillegg et oppfølgingstilsyn etter tilsyn 29. og 30. august 2023. Finanstilsynet gjennomførte møte med foretaket 13. og 14. januar 2026. Denne tilsynsrapporten bygger på Finanstilsynets foreløpige rapport fra 27. mars 2026 og styrets kommentar til denne fra 8. mai 2026.

2 Finanstilsynets oppsummering

Tilsynet avdekket enkelte mangler ved foretakets styring med og kontroll av IKT-virksomheten. Selv om foretaket har gjennomført en rekke aktiviteter for å forbedre sitt arbeid med virksomhetens konsekvensanalyse siden forrige IKT-tilsyn, pekte Finanstilsynet på at det fortsatt var enkelte forbedringsområder. Videre ble det stilt spørsmål ved foretakets arbeid med etterlevelse av gjeldende regelverk. Det ble identifisert svakheter i den uavhengige kontrollen med IKT-tredjepartsrisiko, samt forbedringsbehov knyttet til testing av digital operasjonell motstands-dyktighet.

3 Finanstilsynets vurderinger

3.1 Overordnet styring og kontroll

3.1.1 Virksomhetens konsekvensanalyse

Foretak underlagt DORA skal gjennomføre en konsekvensanalyse av virksomheten for å vurdere forretningsmessige konsekvenser ved IKT-avbrudd. Dette presiseres i DORA art. 11 nr. 5. Som en del av konsekvensanalysen skal foretakene vurdere hvilke virkninger alvorlige driftsforstyrrelser kan ha. Dette skal gjøres ved å bruke både kvantitative og kvalitative kriterier, basert på relevante interne og eksterne data, samt scenarioanalyser. Analysen skal ta hensyn til hvor kritiske de identifiserte forretningsfunksjonene og støtteprosessene er, samt avhengigheten av tredjeparter og informasjonsressurser, inkludert hvordan disse henger sammen. Foretak skal også sørge for at IKT-ressurser og -tjenester er utformet og brukt i tråd med analysen, spesielt med tanke på å sikre tilstrekkelig redundans (reservekapasitet) for alle kritiske komponenter.

Finanstilsynet har notert seg at siden forrige stedlige IKT-tilsyn har foretaket gjennomført en rekke aktiviteter for å forbedre sitt arbeid med virksomhetens konsekvensanalyse. I foreløpig rapport

Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

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

Saksbehandler
Irene Støback Johansen
Dir. tlf. 22 93 96 44

pekte Finanstilsynet på at det forventer at foretaket sikrer at virksomhetens krav til oppetid er operasjonalisert og at dette styrer prioriteringer i foretakets kontrollhandlinger i alle forsvarslinjer. Finanstilsynet mener at virksomhetens konsekvensanalyse er såpass sentral i styringen av virksomheten at resultatet av analysen bør legges fram for styret rutinemessig.

Styret bekrefter i sitt svarbrev at foretakets rutine for virksomhetens konsekvensanalyse er oppdatert med at styret rutinemessig skal orienteres om resultatene fra gjennomført analyse. Videre merker Finanstilsynet seg fra svarbrevet at foretaket kontinuerlig jobber med videreutvikling av rutinen. Foretaket bekrefter også at det vil opprettholde et tydelig fokus på at konsekvens-analysen skal legges til grunn i prioriteringer i både førstelinjens arbeid og kontrollhandlinger i øvrige forsvarslinjer.

Finanstilsynet tar styrets svar til etterretning.

3.1.2 Etterlevelse av IKT-regelverk

Da DORA trådte i kraft 1. juli 2025, var ikke hele nivå 2-regelverket ferdigstilt. Det har senere blitt vedtatt ytterligere utfyllende forordninger i januar 2026, ref. DORA-forskriften, noe som innebærer at etterlevelsen av regelverket må videreutvikles og følges opp over tid.

Foretakets DORA-prosjekt ble avsluttet i januar 2025, og da hadde foretaket ferdigstilt de fleste av de identifiserte aktivitetene. Aktiviteter som ikke var ferdigstilt ble da overlevert til ressurser eller avdelinger i foretaket som fikk ansvar for operasjonalisering av det området som aktiviteten gjaldt. Finanstilsynet pekte i foreløpig rapport på at tilsynsmøtet etterlot et inntrykk av at foretaket i for liten grad har prioritert etterlevelsen av nivå 2-regelverket.

Fra styrets svarbrev merker Finanstilsynet seg at foretaket har samhandlingsfora, både internt i foretaket og i SpareBank 1-alliansen, hvor regulatoriske endringer regelmessig er tema. Regulatoriske endringer i nivå 2-regelverket under DORA vurderes og behandles i disse foraene før de innarbeides i rammeverk, styrende dokumenter og operative prosesser. Videre har foretaket etablert en programplan for informasjonssikkerhet og digital motstandsdyktighet for 2026. Planen omfatter blant annet en egen aktivitet knyttet til implementering av DORA nivå 2-krav, inkludert videreutvikling av rammeverket for IKT-risikostyring der slike krav ennå ikke er implementert.

Finanstilsynet noterer at det er foretakets vurdering at det i dag gjøres et grundig arbeid med å overvåke og implementere nivå-2-regelverkene, og at dette arbeidet vil bli videreført.

Finanstilsynet tar styrets svar til etterretning.

3.2 IKT-tjenesteavtaler og IKT-tredjepartsrisiko

Foretaket skal ha en strategi og retningslinjer for bruk av IKT-tjenester som støtter kritiske eller viktige funksjoner, inkludert bruk av leverandører der det er relevant, i henhold til DORA art. 28 nr. 2. Retningslinjene skal sikre at foretaket etterlever kravene i DORA kapittel 5 og kommisjons-forordning (EU) 2024/1773 om krav til retningslinjer for kontraktsforhold ved bruk av tredjeparts-leverandører av IKT-tjenester som støtter kritiske eller viktige funksjoner. Det skal etableres et system for leverandørstyring med klare roller og løpende risikovurdering. Retningslinjene skal sørge for at det stilles tydelig definerte krav som kan følges opp gjennom hele leverandørforholdet.

I den foreløpige rapporten skrev Finanstilsynet at det mener at foretakets andre forsvarslinje bør gjennomføre egen oppfølging av leverandører og underleverandører for å etablere et helhetlig bilde av styring og kontroll med IKT-tjenester levert av tredjepartsleverandører.

Av styrets svarbrev framgår det at foretaket ikke er enig med Finanstilsynet i at det foreligger regulatoriske krav om at andre forsvarslinje skal utføre direkte kontroller hos IKT-tjeneste-leverandører. Foretakets forståelse er at første forsvarslinje har ansvar for løpende operativ

leverandøroppfølging, mens andre forsvarslinje utøver uavhengig overvåking og kontroll av førstelinjens praksis.

Kravene i DORA til hensiktsmessige styrings- og kontrollordninger, inkludert retningslinjer, for styring av IKT-tredjepartsrisiko innebærer at IKT-tredjepartsrisiko skal være underlagt uavhengig kontroll. Av art. 9 i kommisjonsforordning (EU) 2024/1773, som gjelder bruk av IKT-tjenester som støtter kritiske eller viktige funksjoner, framgår det at vurderinger av IKT-tjenesteleverandørers ytelse, kvalitetsstandarder og etterlevelse skal bygge på relevant rapportering, kontroller og uavhengige gjennomganger, samt inngå i revisjonsplanen. Resultatene skal dokumenteres og benyttes til å oppdatere foretakets risikovurderinger. Disse vurderingene inngår som en del av foretakets uavhengige kontroll- og oppfølgingsaktiviteter, og det skal foretas egne, dokumenterte vurderinger av om etablerte indikatorer, rapportering og kontroller gir et tilstrekkelig grunnlag for styring av IKT-tredjepartsrisiko og rapportering til styret. Der tjenestens kritikalitet, risiko eller kompleksitet, eller svakheter i kontrollgrunnlaget tilsier det, forventes det at uavhengige kontroll-funksjoner gjennomfører særskilte kontrollhandlinger rettet mot leverandørforholdet. Det kan være gjennomgang av leverandørdokumentasjon, møter med leverandør, vurdering av revisjons-rapporter eller andre kontrollhandlinger, eventuelt direkte dialog med leverandør.

Finanstilsynet viser til at bruk av oppdragstaker ikke fritar foretaket for dets plikter og ansvar, jf. finansforetaksloven § 13-4 nr. 3. Finanstilsynet legger til grunn at foretakets uavhengige kontroll-funksjoner må ha et tilstrekkelig selvstendig og dokumentert grunnlag for å vurdere risiko, kontrollnivå og etterlevelse også der IKT-tjenester leveres av tredjepart. Kontrollaktivitetene må tilpasses tjenestens kritikalitet, risiko og kompleksitet, men kan ikke begrenses til å bare være en rent formell kontroll av førstelinjens prosess dersom dette ikke gir et tilstrekkelig grunnlag for uavhengig vurdering og rapportering til styret. Finanstilsynet opprettholder på denne bakgrunn vurderingen fra foreløpig rapport og forventer at foretaket styrker den uavhengige kontrollen med IKT-tredjepartsrisiko.

Finanstilsynet forventer at styret påser at foretaket har etablert, dokumentert og etterlever hensiktsmessige styrings- og kontrollordninger som sikrer en uavhengig og effektiv oppfølging og kontroll av IKT-tredjepartsrisiko der kritikalitet, risiko eller kompleksitet, eller svakheter i kontrollgrunnlaget, tilsier det.

Av styrets svarbrev framgår det videre at foretaket er kjent med at Finanstilsynet arbeider med å utvikle moduler som presiserer tilsynets forventninger, og det opplyses at foretaket vil foreta en fornyet vurdering av ovennevnte etter at disse foreligger. Finanstilsynet gjør imidlertid oppmerksom på at interne tilsynsmoduler ikke vil bli publisert på nåværende tidspunkt, og derfor ikke kan legges til grunn for foretakets videre vurderinger.

3.3 Testing av digital operasjonell motstandsdyktighet

Foretak underlagt DORA skal minst én gang i året sikre at det gjennomføres hensiktsmessige tester av alle IKT-systemer og -applikasjoner som støtter kritiske eller viktige funksjoner. Det presiseres i DORA art. 24 nr. 6. IKT-beredskapsplaner og IKT-respons- og gjenopprettingsplaner skal testes minst én gang i året, jf. art. 11 nr. 6 bokstav a). Kravene til kontinuitet og testing av kontinuitetsplaner er utdypet i kommisjonsforordning (EU) 2024/1774. Her heter det blant annet i art. 25 nr. 5 at foretak skal dokumentere resultatene av testingen og at identifiserte mangler som følge av denne, skal analyseres, håndteres og rapporteres til ledelsen. Foretak skal i sine planer identifisere relevante scenarioer og ta høyde for, samt hensynta, scenarioer beskrevet i art. 26 nr. 2.

Finanstilsynet pekte i foreløpig rapport på at ved testing av beredskapsplaner, både for foretakets egne og for IKT-tjenester levert av leverandører, må relevante scenarioer inngå, inkludert verstefallsscenarioer. Videre må foretakets dokumenterte krav i virksomhetens konsekvensanalyse

testes og trenes på. Det er først når testingen av scenarioer og hele forretningsprosesser er utført at foretaket har dokumentasjon på at virksomhetens tilgjengelighetskrav er ivaretatt.

Finanstilsynet merker seg fra styrets svarbrev at foretaket mener at virksomhetens konsekvens-analyse i dag benyttes for valg av scenarioer til testing og øvelser. Foretaket erkjenner dog at dette er et arbeid som skal videreutvikles og at testing og øvelser skal bli enda tydeligere styrt av og koblet opp mot konsekvensanalysen og risikobildet. Foretaket vil også videreutvikle bruken av scenarioer, inkludert verstefallsscenarioer, både i testing og i øvelser.

Finanstilsynet tar styrets svar til etterretning.

4 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 revisor.

For Finanstilsynet

Wenche Fagereng
seksjonsleder

Irene Støback Johansen
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk.