FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Styret i SPAREBANK 1 ØSTLANDET
Postboks 203
2302 HAMAR

Vår referanse
25/7179
Deres referanse

23.12.2025

Tilsynsrapport

1 Innledning

Finanstilsynet gjennomførte stedlig IKT-tilsyn i Sparebank1 Østlandet (foretaket eller banken) 20. – 21. august 2025. Hensikten med tilsynet var å gjøre en vurdering av hvordan foretaket administrerer, utvikler, drifter, vedlikeholder og sikrer IKT-systemer og -tjenester. Finanstilsynet så på styring med og kontroll av IKT-virksomheten med spesiell vekt på IKT-risiko, IKT-drift, IKT-sikkerhet, bruk av IKT-tjenesteleverandører og beredskap.

IKT-forskriften ble med virkning fra 1. juli 2025 erstattet av DORA-loven[1] med tilhørende forskrift[2]. Regelverket gjennomfører DORA-forordningen[3] med utfyllende nivå 2-rettsakter direkte i norsk rett. Tilsynsvarselet ble sendt før DORA-regelverket trådte i kraft i Norge. Siden selve tilsynet ble gjennomført etter ikrafttredelsen, er DORA-regelverket det rettslige grunnlaget for Finanstilsynets vurderinger knyttet til tilsynet.

Til grunn for tilsynsrapporten ligger Finanstilsynets foreløpige rapport datert 29. oktober 2025 og styrets kommentarer til rapporten i brev av 27. november 2025.

2 Finanstilsynets oppsummering

Tilsynet avdekket enkelte mangler ved foretakets styring med og kontroll av IKT-virksomheten. Foretakets styringsdokumenter manglet på enkelte områder av IKT-virksomheten operasjonalisering i form av standarder og/eller rutiner, og på andre områder var det mangler i rutinene. Finanstilsynet pekte videre på behov for å styrke internkontrollen gjennom strukturert og dokumentert oppfølging av funn fra revisjonsrapporter og beredskapstester.

2.1 Overordnet styring og kontroll

Overordnede styringsdokumenter

Styret skal godkjenne og regelmessig vurdere retningslinjer for å påta foretaket risikoer og for å identifisere, styre, overvåke og kontrollere risikoene, jf. CRR/CRD-forskriften § 35.

DORA-forordningen art. 6 nr. 1 stiller krav til at finansielle enheter skal ha et forsvarlig, helhetlig og veldokumentert rammeverk for IKT-risikostyring som en del av sitt overordnede risikostyrings-system, slik at de kan håndtere IKT-risiko på en rask, effektiv og grundig måte og oppnå en høy

[1] Lov 27. mai 2025 nr. 18 om digital operasjonell motstandsdyktighet i finanssektoren (DORA-loven).

[2] Forskrift 24. juni 2025 nr. 1296 om digital operasjonell motstandsdyktighet i finanssektoren (DORA-forskriften).

[3] Forordning (EU) 2022/2554 om digital operasjonell motstandsdyktighet i finanssektoren (DORA-forordningen).

Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

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

Saksbehandler
Åshild Johnsen
Dir. tlf. 22 93 97 02

grad av digital operasjonell motstandsdyktighet. Videre følger det av nr. 2 at rammeverket for IKT-risikostyring som et minimum skal omfatte strategier, retningslinjer, framgangsmåter, IKT-protokoller og -verktøyer som er nødvendige for på forsvarlig vis og i tilstrekkelig grad å beskytte alle informasjonsressurser og IKT-ressurser.

Foretaket hadde etablert et dokumenthierarki for den styrende dokumentasjonen bestående av IKT-strategien, policyer, standarder og rutiner, parallelt med tilpasningen til DORA-forordningen. På tilsynstidspunktet var foretaket ikke ferdig med dette, og Finanstilsynet pekte i foreløpig rapport på at på enkelte områder av IKT-virksomheten manglet det operasjonalisering i form av standarder og/eller rutiner.

Foretaket beskriver strukturen på den styrende dokumentasjonen som en styrende del, en gjennomførende del og en kontrollerende del. Finanstilsynet stilte i foreløpig rapport spørsmål til hvordan dette stemmer med standarder og rutiner, da innholdet i mottatte standarder og rutiner heller kan beskrives som kravstillende og gjennomførende deler.

Finanstilsynet har merket seg styrets svar om at standarder og rutiner innenfor IKT-området kan beskrives som kravstillende og gjennomførende, mens foretakets «Ledelsessystem for informasjonssikkerhet» inneholder en styrende, en gjennomførende og en kontrollerende del.

Virksomhetens konsekvensanalyse

DORA-forordningen presiserer i art. 11 nr. 5 at finansielle enheter skal gjennomføre en konsekvensanalyse av virksomheten for å vurdere forretningsmessige konsekvenser ved IKT-avbrudd. Som en del av konsekvensanalysen skal de finansielle enhetene 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. Finansielle enheter 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.

Som del av rammeverket for IKT-risikostyring skal finansielle enheter ifølge art. 8 nr. 1 identifisere, klassifisere og dokumentere alle forretningsfunksjoner som støttes av IKT. Dette inkluderer roller og ansvarsområder, samt de informasjons- og IKT-ressursene som støtter disse funksjonene. Dokumentasjonen skal også vise hvordan disse elementene henger sammen og hvilke avhengigheter som finnes, med tanke på IKT-risiko.

Konsekvensanalysen er vesentlig for foretaket for å forstå hvilke prosesser, funksjoner og ressurser som er mest kritiske for driften og den virksomheten styret er ansvarlig for. Videre er konsekvensanalysen viktig underlagsdokumentasjon for utarbeidelsen av overordnede styringsdokumenter som styret skal godkjenne og regelmessig vurdere, jf. CRR/CRD-forskriften § 35.

Foretaket gjennomførte en konsekvensanalyse av virksomheten høsten 2024 som skulle revideres og oppdateres høsten 2025. Finanstilsynet pekte i foreløpig rapport på at metodikk og framgangsmåte for analysen som var beskrevet i resultatrapporten, også burde inngå i foretakets rutine for gjennomføring av virksomhetens konsekvensanalyse.

Finanstilsynet pekte videre på at det ikke framkommer av rutinen at styret skal gjøres kjent med konsekvensanalysen. Finanstilsynet understreket at rutinen for gjennomføring av virksomhetens konsekvensanalyse bør presisere at både denne (rutinen) og resultatet av konsekvensanalysen skal framlegges for styret.

Finanstilsynet har merket seg fra styrets svarbrev at styret er enig i Finanstilsynets kommentarer. Finanstilsynet har videre merket seg at i etterkant av tilsynet er foretakets rutine for gjennomføring av virksomhetens konsekvensanalyse oppdatert i tråd med tilsynets merknader. Metodikk og fremgangsmåte som framgår av resultatrapporten er presisert i rutinen, og det framgår at styret

skal gjøres kjent med både rutinen for gjennomføringen av konsekvensanalysen og resultatet av konsekvensanalysen.

Finanstilsynet tar styrets svar til etterretning.

Rapportering og internkontroll

Etter finansforetaksloven § 8-6 fjerde ledd skal styret føre tilsyn med den daglige ledelse og foretakets virksomhet for øvrig, og sørge for at daglig leder regelmessig gir styret informasjon om foretakets virksomhet. Styrets rolle knyttet til foretakets system for risikostyring og internkontroll er utdypet i CRR/CRD-forskriften § 35. Der presiseres det blant annet at styret skal sikre seg tilgang til risikoinformasjon og fastsette omfang, format og frekvens på rapporteringen.

Ledere på alle vesentlige virksomhetsområder skal løpende vurdere gjennomføringen av internkontrollen, vurderingene skal dokumenteres, og daglig leder skal minimum årlig utarbeide en samlet vurdering av internkontrollen som skal forelegges styret for behandling, jf. forskriftens § 37.

DORA-forordningen presiserer i art. 5 nr. 2 bokstav c) at ledelsen i den finansielle enheten skal fastsette klare roller og ansvarsområder for alle IKT-relaterte funksjoner. Det skal samtidig etableres hensiktsmessige styrings- og kontrollordninger for å sikre effektiv og rettidig kommunikasjon, samarbeid og koordinering mellom disse funksjonene. Art. 5 nr. 4 stiller krav til at ledelsen til enhver tid skal ha tilstrekkelig kunnskap og ferdigheter til å forstå og vurdere IKT-risikoen, og hvordan den påvirker virksomheten.

Finanstilsynet viste i foreløpig rapport til et åpent funn fra 2024 i foretakets oversikt over anbefalinger/pålegg fra internrevisjonen og andre eksterne gjennomganger. På forespørsel under tilsynet var det usikkerhet knyttet til status på funnet. Finanstilsynet stilte spørsmål til om foretakets internkontroll og oppfølging av funn etter eksterne revisjoner/gjennomganger er tilstrekkelig strukturert og dokumentert.

Styret skriver i sitt svar at banken kontinuerlig jobber med å ivareta sikkerhet og driftskontinuitet i bankens IKT-systemer og tjenester inkludert sikkerhetstesting, oppfølging av funn og avvik og re-testing for å vurdere om det er gjennomført relevante tiltak. Finanstilsynet kan imidlertid ikke se at styret har besvart Finanstilsynets spørsmål om foretakets internkontroll og oppfølging av funn etter eksterne revisjoner/ gjennomganger er tilstrekkelig strukturert og dokumentert. Finanstilsynet forventer at foretaket styrker internkontrollen gjennom å dokumentere en strukturert prosess for oppfølging av funn fra eksterne revisjoner.

2.2 IKT-drift

Endringshåndtering

DORA-forordningen stiller i art. 9 nr. 4 bokstav e) krav til at finansielle enheter skal ha dokumenterte retningslinjer, framgangsmåter og kontroller for håndtering av IKT-endringer. Dette omfatter endringer av programvare, maskinvare, maskinvarekomponenter, systemer eller sikkerhetsparametere. Retningslinjene skal bygge på en risikovurderingsmetode og inngå som en integrert del av den finansielle enhetens overordnede prosess for endringsstyring. Formålet er å sikre at alle endringer av IKT-systemer registreres, testes, vurderes, godkjennes, gjennomføres og verifiseres på en kontrollert måte.

Kravene i DORA-forordningens artikkel er nærmere utdypet i nivå 2-regelverket under DORA, herunder i art. 17 i delegert kommisjonsforordning (EU) 2024/1774 om krav til rammeverk for risikostyring (RTS for IKT-risikostyringsrammeverk).

Finanstilsynet pekte i foreløpig rapport på mangler i foretakets endringshåndteringsrutiner. Finanstilsynet mener rutinene bør spesifisere hvordan testing av endringer skal gjennomføres,

sikre rutinemessig vurdering av hva som skal kvalifisere som standard endring og sikre oversikt over om endringer har medført hendelser.

Fra styrets kommentarer har Finanstilsynet merket seg at styret er enig med Finanstilsynet i at de operasjonelle rutinene knyttet til endringshåndtering kan styrkes, og foretaket vil oppdatere standard og rutiner slik at forholdene Finanstilsynet pekte på ivaretas. Finanstilsynet har videre merket seg at det nå er obligatorisk å oppgi endringsnummer når en hendelse kan knyttes til en endring.

Finanstilsynet tar styrets svar til etterretning.

Avvikshåndtering

DORA-forordningen art. 18 og 19 stiller krav om klassifisering og rapportering av hendelser og cybertrusler til myndighetene. Kravene er nærmere utdypet i nivå 2-regelverket under DORA-forordningen, herunder i de delegerte kommisjonsforordningene (EU) 2024/1772 om klassifisering av hendelser og cybertrusler, (EU) 2025/301 om innhold og frister for rapportering og (EU) 2025/302 om maler og prosedyrer for rapportering.

Finanstilsynet pekte i foreløpig rapport på at foretakets rutine for hendelsesrapportering etter DORA ikke omtaler at deler av hendelsesrapporteringen leveres som en IKT-tjeneste av SpareBank 1 Utvikling, og heller ikke at foretaket har bedt om å kunne rapportere aggregert sammen med øvrige banker i alliansen. Ettersom dette utgjør vesentlige elementer i foretakets praktiske håndtering av hendelsesrapporteringen, forventer Finanstilsynet at slike forhold framgår tydelig av foretakets rutine.

Styret viser i sitt svar til at de vil påse at rutinen revideres, inkludert at SpareBank 1 Utviklings rolle knyttet til rapporteringen til Finanstilsynet tydeliggjøres.

Finanstilsynet tar styrets svar til etterretning.

2.3 IKT-tjenesteavtaler

I henhold til DORA-forordningen art. 28 nr. 2 skal foretaket ha en strategi og retningslinjer for bruk av IKT-tjenester som støtter kritiske eller viktige funksjoner, inkludert bruk av ulike leverandører der det er relevant. Retningslinjene skal sikre at foretaket etterlever kravene i DORA-forordningen kapittel 5 og tilhørende nivå 2-regelverk under DORA, herunder delegert kommisjonsforordning (EU) 2024/1773 om krav til retningslinjer for kontraktsforhold ved bruk av tredjepartsleverandører 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. Videre følger det av art. 30 nr. 1 at krav til Service Level Agreement (SLA) skal nedfelles i foretakets IKT-tjenesteavtaler.

I henhold til DORA-forordningen art. 6 nr. 3 skal foretakets rammeverk for IKT-risikostyring minimere virkningen av IKT-risiko gjennom å innføre egnede strategier, retningslinjer, framgangsmåter og IKT-protokoller og -verktøyer.

Finanstilsynet pekte i foreløpig rapport på at det ikke kunne se at krav til leverandøroppfølgingen var nedfelt i standarder og rutiner. I alliansesammenheng er banken stor, og DORA-forordningen stiller skjerpede krav til større banker enn mindre (jf. proporsjonalitetsprinsippet). Finanstilsynet forventer detaljerte standarder og rutiner for leverandøroppfølging. For leverandører av kritiske eller viktige IKT-tjenester bør det etableres egne rutiner som beskriver frekvens og innhold i rapporteringen fra leverandøren, inkludert oppfyllelse av sikkerhetskrav, beredskapstesting, krav i virksomhetens konsekvensanalyse, hendelser, mm. Finanstilsynet mener videre at rutinene, som en del av foretakets IKT-risikostyringsrammeverk, skal beskrive hvordan foretaket skal følge opp det leverandøren rapporterer.

Finanstilsynet konstaterer at styret i sitt svarbrev har tatt tilsynets kommentarer til etterretning. Finanstilsynet har fra styrets svar merket seg at gjeldende styringsdokument av juni 2025 beskriver kravene til leverandøroppfølging på overordnet nivå, og at styret vil påse at mer detaljerte krav vil framgå tydelig av standarder og rutiner. Arbeidet med å ferdigstille disse er igangsatt, og rutinene vil bli oppdatert slik at krav om individuell oppfølging knyttet til leverandørene av kritiske eller viktige IKT-tjenester ivaretas.

Finanstilsynet har videre merket seg at styret er kjent med proporsjonalitetsprinsippet der DORA stiller skjerpede krav til større banker. Banken har derfor valgt å sentralisere oppfølgingen av strategiske leverandører og har etablert en egen avdeling for utkontraktering. Dette skal bidra til å sikre en enhetlig tilnærming og tilstrekkelig kompetanse hos kontrakteiere.

Finanstilsynet tar styrets svar til etterretning.

2.4 Beredskap og kontinuitet

DORA-forordningen presiserer i art. 24 nr. 6 at finansielle foretak minst én gang i året skal sikre at det gjennomføres hensiktsmessige tester av alle IKT-systemer og -applikasjoner som støtter kritiske eller viktige funksjoner. Art. 11 nr. 6 viser til at selve planverket skal testes minst én gang i året. Kravene til kontinuitet og testing av kontinuitetsplaner er utdypet i RTS for IKT-risikostyringsrammeverk art. 24 og 25. Her heter det i art. 25 nr. 5 at finansielle enheter skal dokumentere resultatene av testingen og at identifiserte mangler som følge av denne, skal analyseres, håndteres og rapporteres til ledelsen.

Finanstilsynet viste i foreløpig rapport til at foretaket hadde vedlagt dokumentasjon av et stort antall beredskapstester og øvelser. Noen tester var i egen regi, andre sammen med andre banker i alliansen, og mange var utført hos leverandører. En del av testene hadde avdekket feil eller forbedringsområder, men foretaket kunne ikke redegjøre for status på disse. Finanstilsynet kunne ikke se at foretaket hadde rutiner som sikret systematisk oppfølging av funn fra kontinuitets- og beredskapstester. Der beredskapstester utføres hos leverandør, er slike funn en del av det foretaket skal følge opp leverandøren på. Finanstilsynet stilte i foreløpig rapport spørsmål om internkontrollen, inkludert leverandøroppfølgingen, var tilstrekkelig.

Styret viser i sitt svar til at banken arbeider med å implementere et program for sikkerhetstesting av kritiske IKT-systemer og tjenester hvor tester gjennomført hos underleverandører inngår. Sentralt i dette er å styrke bankens evne til å sette krav, samt følge opp og dokumentere funn. Styret viser videre til bankens kommende omorganisering og til at banken har økt bemanningen for leverandøroppfølging. Dette vil ifølge styret sikre en mer helhetlig og koordinert oppfølging av leverandørene, herunder oppfølgingen av funn fra gjennomførte tester, og bedre internkontrollen på området.

Finanstilsynet har merket seg styrets svar, men understreker at oppfølgingen av funn fra kontinuitets- og beredskapstester skal sikres systematisk oppfølging.

For Finanstilsynet

Olav Johannessen
seksjonsleder

Åshild Johnsen
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk.