FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Styret i LANDKREDITT BANK AS
Postboks 1824 Vika
0123 OSLO

Vår referanse
25/8700
Deres referanse

17.03.2026

# Tilsynsrapport

## 1. Innledning

Finanstilsynet har gjennomført stedlig IKT-tilsyn i Landkreditt Bank AS (heretter omtalt foretaket). Hensikten 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. Finanstilsynet gjennomførte møter med foretaket 5. og 6. november 2025. Til grunn for tilsynsrapporten ligger Finanstilsynets foreløpige rapport datert 13. januar 2026 og styrets kommentarer til rapporten i brev av 18. februar 2026.

## 2. Finanstilsynets oppsummering

Tilsynet avdekket flere mangler ved foretakets styring med og kontroll av IKT-virksomheten. Dette omfatter svakheter i organisering og rolleavklaringer, mangelfulle og utdatert styrings-dokumentasjon samt overordnet metodikk for konsekvensanalyse. Videre var det uklarheter i risikorapportering og manglende etterlevelse av gjeldende regelverk, samt begrenset oppfølging av internrevisjonens anbefalinger. Det ble også identifisert forbedringsbehov knyttet til oppfølging av IKT-tjenesteleverandører, tilgangsstyring og testing av beredskaps- og kontinuitetsplaner.

## 3. Finanstilsynets vurderinger

### 3.1. Organisering

Styret skal sikre en forsvarlig organisering av virksomheten, herunder at foretaket har uavhengige kontrollfunksjoner for risikostyring, etterlevelse og internrevisjon, jf. finansforetaksloven § 8-6 første ledd og § 13-5 andre ledd. Videre stiller CRR/CRD-forskriften §§ 38–40 krav om at foretaket etablerer uavhengige funksjoner for risikokontroll, etterlevelse og internrevisjon, med tilstrekkelig kompetanse og ressurser, og at vesentlige risikoer identifiseres, måles og rapporteres.

Foretak underlagt DORA-forordningen (DORA) skal etablere et internt rammeverk for styring og kontroll av IKT-risiko som sikrer høy digital operasjonell motstandsdyktighet, jf. DORA art. 5 nr. 1. Etter art. 5 nr. 2 bokstav c skal ledelsen fastsette klare roller og ansvarsområder for IKT-funksjonene og sørge for hensiktsmessige styrings- og kontrollordninger. I henhold til art. 5 nr. 3 skal foretaket enten etablere en særskilt funksjon som overvåker kontrakter med IKT-tredjeparter, eller utpeke et medlem av den øverste ledelsen med ansvar for slik oppfølging.

Finanstilsynet pekte i foreløpig rapport på at stillingsinstruks på IKT-området må oppdateres slik at den samsvarer med gjeldende regelverk og korrekt hjemmelsgrunnlag. Videre påpekte Finanstilsynet at foretakets ressurser og kompetanse innen IKT i andre forsvarslinje fremstår som

Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

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

Saksbehandler
Gisle Solemsjø Haugseth
Dir. tlf. 22 93 97 33

begrensede, særlig sett i lys av utfordringene knyttet til etterlevelse av det nye regelverket som trådte i kraft 1. juli (DORA).

Styret skriver i sitt svar at styret tar tilsynets merknad til etterretning, og opplyser at påpekt stillingsinstruks nå er oppdatert i tråd med nytt regelverk. Styret skriver videre at det vil følge opp at andrelinjen har tilstrekkelige ressurser, kompetanse og hensiktsmessig organisering, spesielt sett i lys av DORA.

Finanstilsynet tar styrets svar til etterretning.

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

Finanstilsynet pekte i foreløpig rapport på at tydeliggjøring av risikotoleranse, styringsprinsipper, strategiske prioriteringer og kvalitetsmål framgår delvis av Digitalt veikart og delvis av konsernets IKT-håndbok. Håndboken ble sist oppdatert 30. september 2025 og bygget på tilsynstidspunktet på IKT-forskriften, uten omtale av DORA.

Finanstilsynet pekte videre på at dokumentasjonen reflekterer konserntilhørigheten, men at den bør tilpasses slik at den tydelig viser hva som gjelder for foretaket. Finanstilsynet presiserte at det forventer at styret godkjenner og jevnlig vurderer alle styringsdokumenter av vesentlig betydning for foretakets IKT-virksomhet, i tråd med gjeldende regelverk.

Styret opplyser i sitt svarbrev at oppdatert Digitalt veikart, gjeldende for perioden 2026-2028, ble behandlet i foretakets styre 21. januar 2026, samt at foretakets IKT-håndbok er under revisjon. Styret bekrefter videre at styret vil påse at det er tydelig hvilke styringsdokumenter som gjelder for foretaket og hvilke som gjelder konsernet. Det opplyses videre at styrets regelmessige behandling og godkjenning av styringsdokumenter følger fastsatt årshjul for foretaket.

Finanstilsynet tar styrets svar til etterretning.

## 3.3. Virksomhetens konsekvensanalyse

DORA presiserer i art. 11 nr. 5 at foretak underlagt DORA skal gjennomføre en konsekvensanalyse av virksomheten for å vurdere forretningsmessige konsekvenser ved IKT-avbrudd. Som en del av konsekvensanalysen skal foretak 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.

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. Etter

Finanstilsynets vurdering bør det framgå av rutinen at både rutinen og resultatet av konsekvens-analysen skal legges fram for styret.

Finanstilsynet pekte i foreløpig rapport på at Landkreditt-konsernet har en rutine for gjennomføring av forretningsmessig konsekvensanalyse som gjelder for alle foretak i konsernet. Rutinen er kort og overordnet, og det framgår ikke hvordan den er integrert i foretakets eget rutineverk.

Finanstilsynet viste i foreløpig rapport til at foretaket i sin konsekvensanalyse har identifisert flere kjerneprosesser som kritiske, men at rapporten er på et relativt overordnet nivå. Det ble bekreftet under tilsynet at foretakets metodikk for gjennomføring av konsekvensanalyser skal videreutvikles.

Styret opplyser i sitt svarbrev at det tar Finanstilsynets merknader til etterretning og at rutinen for gjennomføring av virksomhetens konsekvensanalyse er oppdatert med kriterier for vurdering av kritiske prosesser, ansvarsplassering og krav til godkjenning. Styret bekrefter at det vil videre-utvikle konsekvensanalysen i tråd med Finanstilsynets kommentarer. Styret opplyser videre at det deler Finanstilsynets vurdering av at konsekvensanalysen er sentral for å identifisere de mest kritiske prosessene, funksjonene og ressursene for å sikre forsvarlig drift.

Finanstilsynet tar styrets svar til etterretning.

## 3.4. Risikovurdering, rapportering og kontroll

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

Finanstilsynet pekte i foreløpig rapport på at ledere for alle vesentlige virksomhetsområder skal foreta løpende vurderinger av internkontrollen, at vurderingene skal dokumenteres, og at daglig leder minst én gang årlig skal utarbeide en samlet vurdering av internkontrollen som skal forelegges styret, jf. forskriften § 37.

I henhold til DORA skal roller og ansvarsområder for IKT-funksjoner tydeliggjøres, samt at det skal etableres styrings- og kontrollordninger som sikrer effektiv kommunikasjon og koordinering. DORA stiller også krav om at kunnskap og ferdigheter til å forstå og vurdere foretakets IKT-risiko og konsekvensene for virksomheten skal være tilstrekkelig, jf. art. 5 nr. 4.

Finanstilsynet pekte i foreløpig rapport på uklare sammenhenger mellom styrets fastsatte risikoappetitt og vurdert risikonivå, og om det er behov for ytterligere tiltak for å bringe risikonivået i samsvar med den fastsatte appetitten. Videre pekte Finanstilsynet på at compliance-rapporteringen mangler en vurdering av foretakets etterlevelse av DORA.

Styret opplyser i sitt svarbrev at tiltakene for å redusere restrisiko er gjennomført. Styret opplyser videre at det tar Finanstilsynets merknader om rapportering av IKT-risiko til etterretning og vil påse at risikorapporteringen til styret vil styrkes.

Finanstilsynet tar styrets svar om risikorapportering til etterretning. Finanstilsynet legger til grunn styret vil påse at foretakets andre forsvarslinje framover også vil vurdere og rapportere om foretakets etterlevelse av DORA.

## 3.5. Oppfølging av funn fra tredje forsvarslinje – internrevisjon

Finanstilsynet pekte i foreløpig rapport på at internrevisjonen har gitt en rekke anbefalinger innen IKT-området, men flere av disse har svært lange frister. Under tilsynsmøtet fremsto ansvars-

fordelingen ved manglende fristoppnåelse som uklar, og foretaket har ikke etablert krav om styre- eller ledelsesgodkjenning for å endre fristene.

Finanstilsynet anbefalte foretaket å etablere en strukturert prosess for oppfølging av internrevisjonens anbefalinger, der myndighet til å endre frister tydeliggjøres. Kritiske anbefalinger bør prioriteres, og foretaket bør dokumentere gjennomførte tiltak.

Styret opplyser i sitt svarbrev at foretaket har revidert rutinen og prosessen for oppfølging av internrevisjonens anbefalinger etter det stedlige tilsynet. Status for anbefalingene vil heretter gjennomgås kvartalsvis i bankens ledermøte, og eventuelle fristendringer skal godkjennes av administrerende direktør. Styret vil videre motta kvartalsvis rapportering om administrasjonens oppfølging av internrevisjonens rapporter, inkludert informasjon om endringer i frister.

Finanstilsynet tar styrets svar til etterretning.

## 3.6. IKT-tjenesteavtaler

I henhold til DORA 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 kapittel 5 og tilhørende nivå 2-regelverk under DORA, herunder 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.

Finanstilsynet pekte i foreløpig rapport på at foretaket kjøper store deler av sine IKT-tjenester. Foretakets oppfølging av hovedleverandøren synes imidlertid i hovedsak å være begrenset til mottak av ISAE 3402-rapporter, samt rapportering om tilgjengelighet og lignende i henhold til hovedavtalen. Finanstilsynet mente foretaket i større grad bør følge opp hovedleverandøren gjennom egne kontroller, både i første og andre forsvarslinje.

Finanstilsynet minnet foretaket på at de har ansvaret for at IKT-virksomheten oppfyller kravene i DORA, også der hele eller deler av virksomheten er levert gjennom IKT-tjenesteavtaler. Basert på observasjonene under tilsynet stilte Finanstilsynet spørsmål ved om foretaket har iverksatt tilstrekkelige tiltak på dette området.

Styret har i sitt svarbrev presisert at det er enig i betydningen av en forsvarlig oppfølging av hovedleverandøren. Styret fremhever at foretaket benytter betydelige interne ressurser på leverandøroppfølging, og at dette utgjør en sentral del av den løpende driften. Videre opplyser styret at styret vil påse at det blir etablert mer omfattende egne kontroller av tredjeparts-leverandører og at foretaket vil gjennomføre jevnlige andrelinjekontroller av hovedleverandøren, i tråd med compliance-planen for 2026.

Finanstilsynet tar styrets svar til etterretning.

## 3.7. IKT-sikkerhet – Tilgangsstyring

I samsvar med DORA art. 9 skal foretak underlagt DORA ha robuste sikkerhetsmekanismer for å beskytte IKT-systemer og data. Art. 9 nr. 2 viser til at foretaket skal etablere prosedyrer som sikrer konfidensialitet, integritet og tilgjengelighet for systemer, nettverk og informasjon som er kritisk for virksomheten. I henhold til artikkelens nr. 4 bokstav c) skal foretaket iverksette retningslinjer og kontroller som begrenser fysisk eller logisk tilgang til IKT-systemer til det som er nødvendig for legitime og godkjente funksjoner og aktiviteter, og som regulerer tilgangsrettigheter og sikrer en forsvarlig administrasjon av disse.

Finanstilsynet anbefalte i foreløpig rapport at foretaket etablerer rutiner for regelmessig gjennomgang av tilgangsrettigheter hos IKT-tjenesteleverandører, og kontrollere at tilganger er i samsvar med tjenstlig behov.

Styret tar Finanstilsynets anbefaling om mer detaljerte rutinebeskrivelser for oppfølging av tilgangsrettigheter hos tjenesteleverandører til etterretning, og bekrefter at foretaket vil utarbeide dette. I tillegg vil compliance gjennomføre jevnlige andrelinjekontroller av hovedleverandøren.

Finanstilsynet tar styrets svar til etterretning.

## 3.8. Beredskap og kontinuitet

DORA presiserer i art. 24 nr. 6 at foretak underlagt DORA 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 kommisjonsforordning (EU) 2024/1774 (RTS for IKT-risikostyringsrammeverk) art. 24 og 25. Her heter det 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.

Finanstilsynet pekte i foreløpig rapport på at foretaket ikke har ferdigstilt sine beredskaps- og kontinuitetsplaner. Finanstilsynet presiserte videre at det forventer at foretaket gjør beredskaps-testene til sine egne og ikke kun baserer seg på konserntester. Foretaket bør vurdere omfanget av tester som involverer foretakets hovedleverandør, for å sikre at områder som foretaket selv har definert som kritiske, blir tilstrekkelig ivaretatt. For å verifisere at etablerte planer og løsninger fungerer etter hensikten, må foretaket sørge for regelmessig opplæring, øvelser og testing.

Styret har i sitt svarbrev opplyst at beredskaps- og kontinuitetsplanen er ferdigstilt og formelt godkjent av styret etter det stedlige tilsynet. Planen bygger på funn og prioriteringer fra virksomhetens konsekvensanalyse. Styret bekrefter at det deler Finanstilsynets vurdering av behovet for regelmessig opplæring, øvelser og testing, og vil påse at alle kritiske prosesser og funksjoner identifisert i konsekvensanalysen testes med relevante scenarioer i 2026.

Opplæring i nye planer og prosesser vil inngå i foretakets opplæringsplan for ledelse og berørte ansatte i 2026.

Finanstilsynet tar styrets svar til etterretning.

# 4. Videre oppfølging

Vi ber foretaket sende kopi av dette brevet til revisor.

For Finanstilsynet

Olav Johannessen
senior tilsynsrådgiver

Gisle Solemsjø Haugseth
seniorrådgiver

*Dokumentet er godkjent elektronisk.*