FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Styret i Eika Boligkreditt AS
Postboks 2349 Solli
0201 OSLO

Vår referanse
25/10706
Deres referanse

17.04.2026

Tilsynsrapport

1 Innledning

Finanstilsynet har gjennomført IKT-tilsyn med Eika Boligkreditt AS (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. Finanstilsynet gjennomførte møte med foretaket 2. og 3. desember 2025. Denne tilsynsrapporten bygger på Finanstilsynets foreløpige rapport fra 18. februar 2026 og styrets kommentar til denne fra 20. mars 2026.

2 Finanstilsynets oppsummering

Tilsynet avdekket enkelte mangler ved foretakets styring med og kontroll av IKT-virksomheten. Dette omfatter svakheter i organisering, i operasjonaliseringen av styringsdokumentasjon samt i oppfølgingen av tredjepartsrisikoen. Videre ble det påpekt svakheter i foretakets arbeid med etterlevelse av gjeldende regelverk, og det ble identifisert forbedringsbehov knyttet til tilgangsstyring og testing av både sikkerhet, beredskap og kontinuitet.

3 Finanstilsynets vurderinger

3.1 Overordnet styring og kontroll

3.1.1 Organisering

Styret skal sørge for forsvarlig organisering av virksomheten, og det stilles krav om at et finansforetak skal ha uavhengige kontrollfunksjoner med ansvar for risikostyring, etterlevelse og internrevisjon. Det framgår av finansforetaksloven § 8-6 første ledd og § 13-5 andre ledd. CRR/CRD-forskriften stiller krav i § 38 om at foretaket skal ha en uavhengig risikokontrollfunksjon med tilstrekkelig kompetanse og ressurser, og at risikokontrollfunksjonen skal sikre at alle vesentlige risikoer i foretaket er identifisert, målt og rapportert. Forskriften stiller videre krav i § 39 om at foretaket skal ha en uavhengig kontrollfunksjon for kontroll av etterlevelse, og retningslinjer og prosedyrer for å avdekke risiko for at foretaket ikke oppfyller sine forpliktelser etter lov og forskrift. Forskriften presiserer kravene til internrevisjon i § 40.

Foretak underlagt forordning (EU) 2022/2554 om digital operasjonell motstandsdyktighet i finanssektoren (DORA) skal ha innført et internt rammeverk for styring og kontroll som sikrer en effektiv og forsvarlig styring av IKT-risiko for å oppnå et høyt nivå av digital operasjonell

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

motstandsdyktighet. Det følger av DORA art. 5 nr. 1. Videre følger det av nr. 2 bokstav c) at ledelsen skal fastsette klare roller og ansvarsområder for alle IKT-relaterte funksjoner og etablere hensiktsmessige styringsordninger for å sikre effektiv og rettidig kommunikasjon, samarbeid og koordinering mellom disse funksjonene. Ifølge samme artikkel nr. 6 skal det enten opprettes en funksjon for å følge opp kontraktsforhold inngått med tredjepartsleverandører av IKT-tjenester, eller utpekes et medlem av den øverste ledelsen som er ansvarlig for å føre tilsyn med tilhørende risikoeksponering og relevant dokumentasjon.

På tidspunktet for det stedlige tilsynet hadde ikke foretaket en egen ressurs for oppfølging og kontroll av IKT-virksomheten. Tilsynet etterlot videre et inntrykk av at den konkrete kompetansen på IKT og IKT-risiko i foretakets andre forsvarslinje var begrenset. Finanstilsynet stilte videre spørsmål ved om styret anser det samlede omfanget av revisjonsaktiviteter innen IKT-virksomheten som tilstrekkelig for perioden 2025–2026.

Finanstilsynet minnet i foreløpig rapport om viktigheten og nødvendigheten av å ha tilstrekkelig med ressurser og kompetanse på IKT-området, både i første-, andre- og tredje forsvarslinje. Finanstilsynet mener foretaket har manglet ressurser på IKT-området i alle de tre forsvarslinjene, samt IKT-kompetanse i første- og andre forsvarslinje.

Finanstilsynet har merket seg at styret deler Finanstilsynets vurdering av viktigheten av tilstrekkelige ressurser og kompetanse i alle forsvarslinjer. Styret redegjør i sitt svarbrev for tiltak foretaket har iverksatt og vil iverksette som forventes å styrke både ressursene og kompetansen i første og andre forsvarslinje. Videre redegjør styret for de vurderingene som ligger til grunn for fastsettelsen av omfanget av revisjonsaktivitetene, og for hvorfor dette vurderes som tilstrekkelig for perioden 2025–2026, samt videre i tråd med langtidsplanen. Styret opplyser samtidig at internrevisjonsprosjektets omfang vil bli justert ved behov, i samråd med foretakets internrevisor. Finanstilsynet merker seg at styret samlet sett vurderer at tiltakene styrker både kapasitet og kompetanse innen IKT-risiko på tvers av forsvarslinjene.

Finanstilsynet tar styrets svar til etterretning.

3.1.2 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.

Foretak underlagt DORA skal ha et forsvarlig, omfattende 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. Det følger av DORA art. 6 nr. 1. 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 beskytte alle informasjonsressurser og IKT-ressurser.

I henhold til DORA 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.

Foretaket har utarbeidet et omfattende sett av styringsdokumenter relevante for styring av operasjonell risiko, inkludert IKT-risiko. Styringsdokumentene er basert på Eika-maler og er enten nyopprettede eller oppdaterte, samt styregodkjente. Styringsdokumentene er imidlertid i begrenset grad operasjonaliserte i foretaket. Finanstilsynet forutsatte i foreløpig rapport at styret følger opp administrasjonens operasjonalisering av de styregodkjente styringsdokumentene.

Styret skriver i sitt svarbrev at det slutter seg til betydningen av å sikre at styringsdokumentene blir fullt ut operasjonalisert i virksomheten, og at styret vil følge dette arbeidet løpende ved fast rapportering av status i styremøtene.

Finanstilsynet tar styrets svar til etterretning.

3.1.3 Etterlevelse av IKT-regelverk

Administrasjonen iverksatte i 2025 et prosjekt for å sikre etterlevelse av DORA-regelverket – "DORA-prosjektet", og iverksatte en rekke tiltak med frister i 2025 og 2026. Finanstilsynet pekte i foreløpig rapport på at verken prioritet eller kritikalitet framgår av oversikten over tiltak, heller ikke status på tiltakene. Finanstilsynet la til grunn at styret følger opp administrasjonen for å sikre at etterlevelse av gjeldende regelverk gis nødvendig prioritet, ressurser og kompetanse, og ba styret kommentere på status på DORA-prosjektet.

Styret skriver blant annet i sitt svarbrev at styret vurderer at administrasjonens løpende arbeid med DORA-prosjektet og gjennomføring av tiltak har forsvarlig framdrift. Styrket oppfølging av hovedleverandøren av IKT-tjenester har resultert i en forbedret samhandling, og administrasjonen har gjennomført flere sentrale aktiviteter som forbedrer etterlevelsen av regelverket. Styret skriver videre at administrasjonen vil fortsette arbeidet med å operasjonalisere rammeverket i den løpende driften i foretaket.

Finanstilsynet tar styrets svar til etterretning og forventer at styret viderefører prioriteringen av dette arbeidet.

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. Videre følger det av art. 30 nr. 1 at krav til tjenesteavtale (Service Level Agreement, SLA) skal nedfelles i foretakets IKT-tjenesteavtaler.

Foretaket har nylig oppdatert sin SLA med hovedleverandøren av IKT-tjenester for å få bedre kontroll på IKT-tjenesteleveransene. Finanstilsynet pekte i foreløpig rapport på at foretaket ikke gjør kontroller i andre og tredje forsvarslinje på om bestemmelsene i styrende dokumenter eller SLA er oppfylt. Finanstilsynet mente at foretakets oppfølging av IKT-tredjepartsrisiko var mangelfull, jf. DORA art. 28.

Styret bekrefter i sitt svarbrev at det har merket seg Finanstilsynets vurdering av oppfølgingen av IKT-tredjepartsrisikoen. Det redegjør videre for tiltak foretaket har iverksatt og vil iverksette som forventes å styrke oppfølgingen av foretakets IKT-tredjepartsrisiko. Blant annet vil andre forsvarslinje gjennomføre etterlevelseskontroller av oppfyllelse av bestemmelser i styrende dokumenter, og internrevisjonen vil gjennomgå IKT-leveranser og leverandøroppfølging i 2026 i tråd med langtidsplanen.

Finanstilsynet tar styrets svar til etterretning.

3.3 IKT-sikkerhet - tilgangsstyring

Foretak skal ha robuste sikkerhetsmekanismer for å beskytte IKT-systemer og data. Det følger av DORA art. 9. Artikkelen 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 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 pekte i foreløpig rapport på at det under tilsynet ble informert om at foretaket ikke har kjennskap til hvem eller hvor mange ansatte hos IKT-tjenesteleverandøren som har tilgang til foretakets IKT-driftsmiljø. Videre framkom det at foretaket ikke gjennomfører kontroller av IKT-tjenesteleverandørens tilganger. Finanstilsynet mente foretakets styring og kontroll med tilganger hos IKT-tjenesteleverandører er utilstrekkelig og ikke i samsvar med DORA art. 9 nr. 4 bokstav c).

I sitt svarbrev presiserer styret at styring og kontroll knyttet til tilganger hos IKT-tjeneste-leverandøren er etablert og operasjonalisert, og at Finanstilsynets inntrykk her skyldes mangelfull framstilling under selve tilsynsmøtet. Foretaket har etablert retningslinjer og kontroller for tilgangs-styring i tråd med DORA art. 9, der leverandørens tilgang til driftsmiljøet følges opp gjennom løpende leverandøroppfølging og inngår i dokumentasjon oversendt ekstern revisor. Finanstilsynet merker seg at foretaket likevel vil vurdere om ytterligere presiseringer kan gjøres i rutiner og dokumentasjon for å sikre at denne praksisen framkommer tydeligere.

Finanstilsynet tar styrets svar til etterretning.

3.4 Testing av sikkerhet og beredskap

3.4.1 Sikkerhetstesting

Foretak underlagt DORA skal utarbeide, opprettholde og gjennomgå et forsvarlig og omfattende program for testing av den digitale operasjonelle motstandsdyktigheten som en integrert del av rammeverket for IKT-risikostyring. Det følger av DORA art. 24 nr. 1. Hensiktsmessige tester skal minst én gang i året gjennomføres av alle IKT-systemer og applikasjoner som støtter kritiske eller viktige funksjoner, jf. art. 24 nr. 6. Art. 24 nr. 5 stiller videre krav om at foretaket har retningslinjer for å følge opp og avhjelpe forhold som avdekkes gjennom testing.

Finanstilsynet uttalte i foreløpig rapport at foretakets etterlevelse av DORA art. 24 nr. 6 framstår som mangelfull, ettersom det under tilsynet ble opplyst at sikkerhetstesting utført av IKT-tjenesteleverandøren ikke har vært gjennomført årlig, og at foretaket mottar begrenset informasjon om gjennomførte sikkerhetstester.

Styret bekrefter i svarbrevet at det deler Finanstilsynets vurdering av at etterlevelsen av kravene i DORA art. 24 må styrkes, særlig når det gjelder hyppighet, omfang og innsyn i gjennomførte sikkerhetstester for kritiske og viktige systemer. Finanstilsynet har merket seg at tilsynets presisering har styrket foretakets dialog med IKT-tjenesteleverandøren, og at foretaket i kommende revisjon av SLA vil tydeliggjøre sine forventninger for å styrke sikkerhetstesting samt sikre tilstrekkelig innsikt og kontroll.

Finanstilsynet tar styrets svar til etterretning.

3.4.2 Testing av beredskap og kontinuitet

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 følger av DORA art. 24 nr. 6. Videre stiller art. 11 nr. 6 bokstav a) krav til at selve planverket skal testes minst én gang i året. Kravene til kontinuitet og testing av kontinuitetsplaner er utdypet i delegert kommisjonsforordning (EU) 2024/1774 art. 25. Her heter det i art. 25 nr. 2 at testingen skal baseres på plausible, men alvorlige scenarioer som simulerer potensielle forstyrrelser, og inkludere testing av IKT-tjenesteleveranser der det er relevant. I henhold til artikkelens nr. 5 skal resultatene av testingen dokumenteres, og identifiserte mangler som følge av denne skal analyseres, håndteres og rapporteres til ledelsen.

Finanstilsynet presiserte i foreløpig rapport at foretaket har ansvar for å gjennomføre årlig opplæring, øvelser og testing av kriseløsningen på foretaksnivå, også for IKT-tjenester levert av tredjepartsleverandører, basert på virksomhetens konsekvensanalyse. Gjennomgangen av tester i

2024 og 2025 viser at det ikke er gjennomført relevant beredskapstesting som omfatter alvorlige informasjonssikkerhetshendelser hos leverandørene. Finanstilsynet legger til grunn at testing av beredskapsplaner skal omfatte relevante, herunder verstefallsscenarioer, og gi dokumentasjon for at tilgjengelighetskravene er ivaretatt.

Styret bekrefter i sitt svarbrev at styret er enig i og deler Finanstilsynets vurdering av at kravene i DORA om årlig opplæring, øvelser og testing av kriseløsningen, også for IKT-tjenester levert av eksterne leverandører, må styrkes og gjennomføres på foretaksnivå. Foretaket har etablert beredskapsplanverk basert på egen konsekvensanalyse, men erkjenner behov for å videreutvikle testingen for å styrke egnethet, robusthet og samhandling, særlig ved scenarioer som omfatter angrep på leverandørens IKT-infrastruktur. Dette inngår som et prioritert tiltak i den videre operasjonaliseringen av DORA-kravene.

Finanstilsynet tar styrets svar til etterretning.

4 Videre oppfølging

Vi ber foretaket sende kopi av dette brevet til revisor.

For Finanstilsynet

Wenche Fagereng
seksjonsleder

Irene Støback Johansen
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk.