FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Haugesund Sparebank
Postboks 203
5501 HAUGESUND

Vår referanse
25/11323
Deres referanse

12.03.2026

Tilsynsrapport

1 Innledning

Finanstilsynet gjennomførte stedlig IKT-tilsyn med Haugesund Sparebank (heretter omtalt 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 styring med og kontroll av IKT-virksomheten med spesiell vekt på IKT-risiko, IKT-drift, IKT-sikkerhet, bruk av IKT-tjenesteleverandører og beredskap. Finanstilsynet gjennomførte møter med foretaket 10. og 11. november 2025. Denne tilsynsrapporten bygger på Finanstilsynets foreløpige rapport fra 8. januar 2026 og styrets kommentar til denne fra 13. februar 2026.

Foretaket er sammen med de andre bankene i Eika-alliansen eier av Eika Gruppen som leverer felles IKT-tjenester til bankene.

2 Finanstilsynets oppsummering

Tilsynet avdekket enkelte mangler ved foretakets styring med og kontroll av IKT-virksomheten Innen flere områder av foretakets IKT-virksomhet manglet det operasjonalisering av styregodkjente styringsdokumenter, og foretaket må i større grad stille krav til rapportering fra IKT-tjenesteleverandører i første og andre forsvarslinje. Foretaket er ansvarlig for å sikre tilstrekkelig oppfølging av eksterne leverandører, selv om foretaket i stor grad baserer seg på leverandøroppfølgingen som utføres av alliansen foretaket er en del av.

3 Finanstilsynets vurderinger

3.1 Strategi og organisering

DORA art. 6 nr. 1 stiller krav til at foretak underlagt DORA skal ha et forsvarlig, omfattende 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 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. 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.

I den foreløpige rapporten pekte Finanstilsynet på at flere områder innen IKT-virksomheten manglet operasjonalisering av styrende dokumenter, og at foretaket må utarbeide en

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

konkret og tidfestet plan for å sikre at styregodkjente styringsdokumenter operasjonaliseres gjennom fastsatte rutiner, opplæring, kontroller og rapportering.

Styret skriver i sitt svar at foretaket har igangsatt arbeidet med å operasjonalisere IKT-rammeverket, og vil sikre sporbar etterlevelse av DORA-kravene. Videre svarer styret at de vil følge opp det videre arbeidet med operasjonalisering gjennom en tidfestet handlingsplan.

Finanstilsynet tar styrets svar til etterretning.

3.2 Kontrollfunksjoner og rapportering

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 av de relevante organisatoriske enhetene. 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.

I henhold til DORA art. 5 nr. 1 skal foretak underlagt DORA 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 motstandsdyktighet. Videre følger det av art. 5 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 art. 5 nr. 6 skal det enten opprettes en funksjon for å følge opp kontraktsforhold inngått med tredjepartsleverandører av IKT-tjenester om bruk av IKT-tjenester, eller utpekes et medlem av den øverste ledelsen som er ansvarlig for å føre tilsyn med tilhørende risikoeksponering og relevant dokumentasjon.

3.2.1 Rapportering fra IKT-tjenesteleverandør

Finanstilsynet viste i foreløpig rapport til at faste rapporter foretaket mottar fra IKT-tjenesteleverandørens andrelinje i liten grad var knyttet til foretakets egne styregodkjente styringsdokumenter. Finanstilsynet understreket at manglende tilpasning til interne styrings-dokumenter kan medføre at vesentlige risikoer relatert til IKT-tjenester ikke blir tilstrekkelig identifisert, vurdert og fulgt opp i tråd med foretakets egne risikostyringsprosesser. Finanstilsynet pekte på at foretakets førstelinje bør stille tydelige krav til rapportering fra tjenesteleverandører i henhold til foretakets styregodkjente styringsdokumenter, og at foretakets andrelinje bør kontrollere at rapporteringen er hensiktsmessig og gjennomført.

Finanstilsynet har merket seg styrets svar om at det gjennomføres jevnlige kontroller for å sikre at foretakets kontroller i både første- og andrelinje er hensiktsmessige. Styret oppgir at det er naturlig for andrelinjen å etablere kontroll av at foretaket mottar hensiktsmessige rapporter, både i henhold til det førstelinjen i foretaket krever av leverandører og i henhold til det andrelinjen ser som behov for å dekke foretakets risiko på IKT-området.

Finanstilsynet tar styrets svar til etterretning.

3.2.2 IKT-kompetanse i andre forsvarslinje

I foreløpig rapport understreket Finanstilsynet viktigheten av å ha tilstrekkelig IKT-kompetanse i andrelinjen, særlig når foretakets informasjonssikkerhetsfunksjon er organisert i førstelinjen. Finanstilsynet merket seg fra tilsynet at andrelinjen i varierende grad stiller krav på IKT-området,

og stilte spørsmål ved hvordan foretaket sikrer at andrelinjen har tilstrekkelig ressurser og kompetanse til å kunne kontrollere og stille krav til førstelinjen på IKT-området.

Styret skriver i sitt svar at andrelinjen er styrket med én stilling i forbindelse med fusjonen, og at samlede ressurser for andrelinjen anses som tilfredsstillende. Styret viser til at foretakets andrelinje deltar i ordinær opplæring innen IKT-sikkerhet, både i regi av Eika Gruppen og IT-sjef, samt eksterne konferanser. Foretaket vil følge utviklingen i Eika-samarbeidet også hva angår eventuelt særskilt opplæring for andrelinje etter innføring av DORA-regelverket.

Finanstilsynet tar styrets svar til etterretning, og legger til grunn at styret sikrer at andelinje-funksjonen har nødvendig kompetanse og tilstrekkelige ressurser til å stille krav til og kontrollere førstelinjen på IKT-området, i samsvar med de forhold som er påpekt i tilsynsrapporten.

3.3 Virksomhetens konsekvensanalyse

Etter DORA art. 11 nr. 5 skal foretak underlagt DORA 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.

Finanstilsynet viste i foreløpig rapport til at foretaket i begrenset grad har sikret at prioriteringene og kravene som fremgår av virksomhetens konsekvensanalyse er kommunisert videre til relevante IKT-leverandører. Finanstilsynet pekte på at foretaket må sikre at informasjonen fra konsekvens-analysen inngår som en del av grunnlaget for styring av IKT-tjenester levert av tredjeparter, og at leverandørene har kjennskap til hvilke forretningsfunksjoner som er kritiske, hvilke tilgjengelighets- og gjenopprettingskrav som gjelder, samt hvilke avhengigheter som må ivaretas ved alvorlige driftsforstyrrelser.

Styret skriver i sitt svar at Eika Gruppen har utarbeidet malen foretaket benytter og en tilhørende metodikk som sikrer operasjonalisering gjennom at leverandører, tjenester og systemer tar utgangspunkt i kritikalitetsvurderingen. Videre stilles det krav til leverandører, tjenester og systemer i henhold til konsekvensanalysen og disse følges opp i tråd med Eika Gruppens modell for IKT-risikostyring.

Finanstilsynet merker seg styrets svar, men understreker at foretaket må gjøre en selvstendig vurdering av IKT-tjenesteleveransene opp mot kravene stilt i konsekvensanalysen.

3.4 IKT-drift

DORA stiller i art. 9 nr. 4 bokstav e) krav til at foretak underlagt DORA skal ha dokumenterte retningslinjer, framgangsmåter og kontroller for håndtering av IKT-endringer. Dette omfatter endringer av programvare, maskinvare, maskinvarekomponenter, systemer eller sikkerhets-parametere. Retningslinjene skal bygge på en risikovurderingsmetode og inngå som en integrert del av foretakets 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 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 at foretaket ikke har etablert en tydelig klassifisering av endringstyper utover nødendringer. Finanstilsynet merket seg videre at forhåndsgodkjente

endringer ikke følges opp særskilt. Finanstilsynet ba i foreløpig rapport foretaket sikre at alle endringstyper er identifisert, med tilhørende kriterier for klassifisering. Videre pekte Finanstilsynet på at foretaket bør etablere rutiner for rapportering av utviklingen i antall forhåndsgodkjente endringer, samt analysere sammenhengen mellom slike endringer og driftsstabilitet. Kontroll-funksjonene bør gjennomføre kontroller for å verifisere at kriteriene for forhåndsgodkjenning er oppfylt.

Styret skriver i sitt svar at de har registrert Finanstilsynets påpekninger, og vil sikre at foretakets endringsprosess revideres til å omfatte alle endringstyper med tilhørende kriterier for klassifisering. Styret peker på at endringer forvaltes gjennom avtale med sin leverandør. Styret vil følge opp at det etableres en rutine som sikrer at foretaket benytter blant annet endringsinformasjon fra leverandør som del av egen styring og kontroll, herunder analyse av endringstyper og utvikling over tid.

Finanstilsynet tar styrets svar til etterretning.

3.5 IKT-tredjepartsrisiko

I henhold til DORA art. 28 nr. 2 skal foretak underlagt DORA ha en strategi og retningslinjer for bruk av IKT-tjenester som støtter kritiske eller viktige funksjoner, inkludert bruk av leverandører der det er relevant. 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.

Finanstilsynet viste i foreløpig rapport til at foretaket årlig mottar revisjonsrapporter og risiko-vurderinger av underleverandører fra Eika Gruppen, men fant det ikke dokumentert hvordan foretaket stiller egne krav til rapporteringen, eller hvordan mottatt informasjon behandles i foretaket. Finanstilsynet pekte på at foretaket må gjøre en selvstendig vurdering av risikoen ved bruk av IKT-tjenesteleverandører og sikre at Eika Gruppen rapporterer på dette, slik at risiko-vurderinger og revisjonsrapporter blir analysert og innarbeides i foretakets arbeid med risikostyring og kontrollrammeverk i første og andre forsvarslinje.

Styret skriver i sitt svar at foretaket gjennomfører en rekke aktiviteter mot leverandører og underleverandører for å sikre at foretakets selvstendige vurderte risiko tas til følge og rapporteres på. Styret noterer seg likevel Finanstilsynets forventning, og vil gjennomgå rutinene, både for hvordan dette best blir innarbeidet som en konkret del av det løpende IKT-arbeidet, og hvordan de best dokumenterer utførelsen av dette.

Finanstilsynet tar styrets svar til etterretning.

3.6 IKT-sikkerhet

I samsvar med DORA art. 9 skal foretak underlagt DORA ha robuste sikkerhetsmekanismer for å beskytte IKT-systemer og data. DORA art. 9 nr. 2 viser til at foretak 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 viste i foreløpig rapport til at foretakets egne kontroller av tilgangsstyring ikke inkluderte leverandørers tilgang til foretakets driftsmiljø. For å være tilstrekkelig betrygget om at tilganger er begrenset til legitime og godkjente funksjoner, understreket Finanstilsynet at foretakets førstelinje må etablere og gjennomføre periodiske kontroller av leverandørtilganger. Disse kontrollene bør inkludere verifisering av at tilgangene er nødvendige, tidsbegrensede og i tråd med

foretakets retningslinjer for tilgangsstyring. Videre pekte Finanstilsynet på at foretakets andrelinje har oppgaven med å se til at dette gjennomføres på en tilfredsstillende måte.

Styret skriver i sitt svar at for å sikre at leverandørtilganger blir jevnlig og periodisk kontrollert, har foretaket etablert felles løsning med leverandør for oversikt og periodisk kontroll. Dette inkluderer ansatte hos leverandører og underleverandører. Videre oppgir styret at det er innført rutiner som tydeliggjør hvilke tilganger som er nødvendige og i hvilken varighet, med tilhørende rapportering som benyttes som grunnlag for foretakets egne kontroller. Styret informerer om at foretakets andrelinje vil følge opp gjennomføring av dette gjennom andrelinjens kontrollregime.

Finanstilsynet tar styrets svar til etterretning.

3.7 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 nivå 2-regelverket under DORA, herunder i 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 de ikke kunne se at foretakets IKT-tjenesteleverandører utførte relevant testing av beredskapsplan hvor scenarioer ved angrep eller innbrudd i tjenesteleverandørenes IKT-infrastruktur, eksempelvis angrep med løsepengevirus med påfølgende gjenoppretting av data, er inkludert. Finanstilsynet understreket at ved testing av beredskapsplaner, både for foretakets egne IKT-tjenester og for IKT-tjenester levert av tjenesteleverandører, må relevante informasjonssikkerhetsscenarioer inngå, inkludert test av verstefallsscenarioer. 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 og virksomhetens konsekvensanalyse.

Styret skriver i sitt svar at foretaket, i samarbeid med leverandør, vil utarbeide planverk for utvidet beredskapstesting, inkludert gjenoppretting og alternativ drift i et verstefallsscenario. Foretaket gjennomfører også jevnlig test av lokal beredskapsplan.

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

Hanne Teigland
rådgiver

Dokumentet er godkjent elektronisk.