FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Styret i
FREMTIND FORSIKRING AS
Postboks 778 Sentrum
0106 OSLO

Vår referanse
25/7275
Deres referanse

23.03.2026

Tilsynsrapport

1. Innledning

Finanstilsynet gjennomførte IKT-tilsyn 27. og 28. august 2025 i Fremtind Forsikring AS (foretaket). Formålet med tilsynet var å gjøre en vurdering av hvordan foretaket administrerer, utvikler, drifter, vedlikeholder og sikrer IKT-systemer og -tjenester. For dette området så tilsynet på styring med og kontroll av IKT-virksomheten. Tilsynet hadde fokus på systemløsninger som støtter foretakets kjernevirksomhet, spesielt IKT-systemer levert av IKT-tjenesteleverandører.

Til grunn for disse merknadene ligger Finanstilsynets foreløpige rapport datert 16. desember 2025 og styrets kommentarer til rapporten i brev av 5. februar 2026.

2. Finanstilsynets oppsummering

Tilsynet avdekket ingen vesentlige mangler ved foretakets styring med og kontroll av IKT-virksomheten. Det er gitt noen merknader knyttet til foretakets risikostyring, blant annet uklarheter i overordnet oppfølging av styringsdokumentasjon, oppfølging av tjenester levert av tredjepartsleverandører og testing av beredskapsplaner.

3. Finanstilsynets vurderinger

3.1. Overordnet styring og kontroll

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. Forsikringsforetak skal i tillegg ha uavhengige kontrollfunksjoner med ansvar for aktuarfaglige oppgaver. Det framgår av finansforetaksloven § 8-6 første ledd og § 13-5 andre ledd.

DORA-forordningen (DORA) art. 5 nr. 1 stiller krav til at foretak underlagt DORA skal ha 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 Finanstilsynet forventer at styregodkjente styringsdokumenter som strategier og policyer følges opp for å sikre at foretakets planer og drift utføres i henhold til disse. Videre pekte Finanstilsynet på at det forventes at foretakets andre- og tredje forsvarslinje følger opp etterlevelsen av strategier og kontrollerer at de styrende dokumentene er operasjonalisert i henhold til disse.

Styret skriver i sitt svar at det tar Finanstilsynets merknad til etterretning og at det aktivt vil følge opp at operasjonalisering, opplæring, oppfølging og kontroller skjer.

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

Finanstilsynet tar styrets svar til etterretning.

Finanstilsynet pekte i foreløpig rapport på at dersom ansvaret for informasjonssikkerhet legges til førstelinjen må foretaket sikre at andrelinjen har tilstrekkelige ressurser og kompetanse om informasjonssikkerhet. Foretaket må også sørge for at andrelinjen følger opp at foretakets IKT-sikkerhetspolicy er operasjonalisert både internt og hos IKT-tjenesteleverandører og deres underleverandører.

Styret skriver i sitt svarbrev at foretaket vil følge opp at ny organisering og styrking av kapasitet og kompetanse i andrelinjen effektivt bidrar til å sikre etterlevelse av styrende dokumenter og policyer på IKT-sikkerhetsområdet.

Finanstilsynet tar styrets svar til etterretning.

3.2. 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.

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 viktigheten av å gjennomføre egne kontroller eller revisjonsgjennomganger av IKT-tjenester levert av tredjepartsleverandører for å kunne vurdere etterlevelse av foretakets overordnede målsetting om å ha effektiv styring og overvåkning av operasjonell risiko. Det er Finanstilsynets vurdering at det ikke i tilstrekkelig grad gjennomføres egne kontroller eller revisjonsgjennomganger av foretakets IKT-tjenester levert av tredjepartsleverandører.

Styret skriver i sitt svarbrev at foretaket aktivt vil følge opp at kontrollaktiviteter og rapportering gjennomføres i tråd med gjeldende regelverk og DORAs krav til styring, kontroll og rapportering på IKT-området.

Finanstilsynet tar styrets svar til etterretning.

3.3. Foretakets tredje forsvarslinje – internrevisjon

DORA presiserer i art. 6 nr. 6 og 7 at rammeverket for IKT-risikostyring regelmessig skal være gjenstand for internrevisjon i tråd med den foretakets revisjonsplan. Revisorene skal ha tilstrekkelig kunnskap, ferdigheter og ekspertise med hensyn til IKT-risiko samt være tilstrekkelig uavhengige. Hyppigheten av IKT-revisjoner og deres fokus skal stå i et rimelig forhold til foretakets IKT-risiko. Foretaket skal på grunnlag av konklusjonene fra internrevisjonen opprette en formell oppfølgingsprosess, herunder regler om rettidig verifisering og utbedring av kritiske resultater fra IKT-revisjonen.

Finanstilsynet skrev i foreløpig rapport at ressursbruken til uavhengige internrevisjonsaktiviteter på IKT-området ikke står i forhold til foretakets størrelse og risikoprofil, herunder den digitale satsingen og kompleksiteten på IKT-området.

Styret skriver i sitt svarbrev at foretaket vil prioritere å sikre fokus og adekvat ressursbruk i internrevisjon av IKT framover. Det blir vist til at internrevisjonen allerede har gjennomført revisjon av foretakets tilpasning til nytt DORA-regelverk.

Finanstilsynet tar styrets svar til etterretning

3.4. Virksomhetens konsekvensanalyse

DORA presiserer i art. 11 nr. 5 at foretaket skal gjennomføre en konsekvensanalyse av virksomheten for å vurdere forretningsmessige konsekvenser ved IKT-avbrudd. Som en del av konsekvensanalysen skal foretaket vurdere hvilke virkninger alvorlige IKT-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. Foretaket 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 foretaket ifølge forordningens art. 8 nr. 1 identifisere, klassifisere og dokumentere alle forretningsfunksjoner som støttes av IKT. Dette inkluderer roller og ansvarsområder, samt de 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.

Finanstilsynet pekte i foreløpig rapport på viktigheten av at styret gjøres kjent med virksomhetens konsekvensanalyse.

Styret skriver i sitt svarbrev at foretaket har utarbeidet en konsekvensanalyse for virksomheten for foretakets forretningsprosesser, og at resultatene fra den gjennomførte analysen danner grunnlaget for styresak om en oppdatert konsekvensanalyse. Styret skriver videre at det tar Finanstilsynets merknad til etterretning, og at saken allerede er berammet for behandling i styret.

Finanstilsynet tar styrets svar til etterretning.

3.5. IKT-drift

DORA stiller i art. 9 nr. 4 bokstav e) krav til at foretaket 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 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 i DORA art. 9 nr. 4 bokstav e) om håndtering av IKT-endringer er nærmere utdypet i kommisjonsforordning (EU) 2024/1774 (RTS for IKT-risikostyringsrammeverk) art. 17.

Finanstilsynet pekte i foreløpig rapport på at foretaket bør sørge for at prosedyrer for avvikshåndtering sikrer at oppfølgingen inkluderer rapportering av tiltak som etableres som følge av avviket. Dette gjelder også for IKT-tjenester levert av leverandører.

Styret skriver i sitt svarbrev at foretaket vil følge opp at tiltakene for å forbedre prosedyrene for avvikshåndtering gjennomføres. Videre skriver styret at dette omfatter forbedret oppfølging av tiltak som etableres som følge av avvik, samt etablering av mekanismer for rapportering av oppfølgingen.

Finanstilsynet tar styrets svar til etterretning.

Prosedyrene for endringshåndtering skal omfatte alle endringer som kan påvirke IKT-systemene og sikre en forsvarlig, formell behandling og dokumentasjon av disse. Foretaket skal sikre at prosedyrene for endringshåndtering gir en stabil, planlagt og forutsigbar drift.

Finanstilsynet pekte i foreløpig rapport på at det bør rapporteres særskilt på utviklingen i antall forhåndsgodkjente endringer og deres sammenheng med driftsstabilitet. Videre pekte

Finanstilsynet på at kontrollfunksjonene bør gjennomføre kontroller for å sikre at kriteriene for forhåndsgodkjenning er oppfylt.

Styret skriver i sitt svarbrev at foretakets forhåndsgodkjente endringer er mindre og reverserbare endringer, som utgjør lav risiko. Styret skriver videre at foretaket er i prosess med å etablere forbedret prosesstyring for endringshåndtering, for å øke sporbarhet, rapportering og revisjonsspor. Dette for å gi bedre oversikt over endringer og tydeligere kobling til hendelser, slik at kontrollfunksjoner kan bekrefte etterlevelse og følge opp avvik.

Finanstilsynet tar styrets svar til etterretning.

Finanstilsynet pekte i foreløpig rapport på at endringsprosessen ikke inkluderer kontroll av om endringen kan medføre behov for justering av beredskapsplanene. Finanstilsynet skriver i rapporten at foretakets endringshåndteringsprosess bør inneholde en vurdering av om endringen krever en oppdatering av gjeldende beredskapsplaner.

Styret skriver i sitt svar at som del av DORA-tilpasningen etableres det et nytt kontrollpunkt i risikovurderingen for å sikre oppdaterte beredskaps- og gjenopprettingsplaner.

Finanstilsynet tar styrets svar til etterretning.

3.6. IKT-sikkerhet

I henhold til DORA art. 9 nr. 4 bokstav c) skal foretaket gjennomføre retningslinjer som begrenser fysisk og logisk tilgang til IKT-ressurser til det som kreves for legitime og godkjente funksjoner og aktiviteter. Det skal innføres retningslinjer, framgangsmåter og kontroller som regulerer tilgangsrettigheter og sikre en forsvarlig forvaltning av disse.

Finanstilsynet pekte i foreløpig rapport på viktigheten av at foretaket må sikre at IKT-tjenesteleverandører etablerer løsninger for tilgangsstyring og kontrollrutiner som i størst mulig grad sørger for at tilganger tildeles og kontrolleres per oppdrag.

Styret redegjør i sitt svar om viktigheten av å utføre kontroll med tredjepartstilganger og vil følge aktivt opp planlagte tiltak for dette området gjennom den ordinære styrerapporteringen.

Finanstilsynet tar styrets svar til etterretning.

3.7. IKT-tjenesteavtaler

I henhold til DORA art. 28 nr. 2 skal foretaket ha en strategi og retningslinjer for bruk av IKT-tjenester som understøtter kritiske eller viktige funksjoner når det benyttes IKT-tjenesteleverandører. Retningslinjene skal sikre etterlevelse av kravene i kapittel 5 om styring og kontroll med IKT-tjenestekjøp, samt de detaljerte kravene som framgår av tilhørende kommisjonsforordning (EU) 2024/1773.

Det skal etableres retningslinjer for leverandørstyring med klart definerte roller og løpende risikovurdering. Retningslinjene skal sørge for tydelige og oppfølgingsbare krav gjennom hele leverandørforholdet, inkludert krav til Service Level Agreements (SLA) i IKT-tjenesteavtaler, jf. DORAs art. 30 nr. 1. I henhold til DORA art. 30 nr. 3 bokstav e) nr. i) skal IKT-tjenesteavtalene som støtter kritiske eller viktige funksjoner sikre at foretaket gis rett til innsyn i og kontroll med kjøp av IKT-tjenester.

Finanstilsynet ba i foreløpig rapport foretaket gå gjennom kritiske og viktige IKT-tjenesteavtaler for å sikre at de er i henhold til gjeldende regelverk.

Styret skriver i sitt svar at de kritiske og viktige IKT-tjenesteavtalene er gjennomgått og at det er forhandlet med leverandørene. Der det har vært nødvendig for å oppfylle DORA-kravene er det inngått endringsbilag. Det framgår videre av svaret at nødvendige tillegg eller justeringer er innarbeidet i avtalene.

Finanstilsynet tar styrets svar til etterretning.

Finanstilsynet pekte i foreløpig rapport på at desentralisert oppfølging av IKT-tjenester levert av leverandører kan gi ulik kvalitet og grad av kontroll. Finanstilsynet pekte videre på at foretaket bør sikre at kontrakteiere har tilstrekkelig kompetanse og ressurser til å ivareta en god og ensartet oppfølging av leverandører av IKT-tjenester.

Styret skriver i sitt svar at det som en del av DORA-prosjektet er etablert en forbedret rutine for leverandøroppfølging og at det gis løpende og obligatorisk opplæring i god avtaleoppfølging for avtaleansvarlige og mellomledere. Styret skriver videre at foretaket også etablerer noe mer sentral støtte for og kontroll av avtaleoppfølgingen. For å forbedre oppfølgingen av enkelte avtaler er endret plassering av avtaleansvar under vurdering.

Finanstilsynet tar styrets svar til etterretning.

Finanstilsynet skrev i foreløpig rapport at ved å benytte styrende dokumenter i gjennomgang av IKT-tjenesteleveranser kan foretaket bedre sikre at foretakets krav til levering av viktige og kritiske IKT-tjenester blir etterlevd.

Styret skriver i sitt svarbrev at det tar Finanstilsynets kommentarer til etterretning. Styret bekrefter at foretakets kontrollfunksjoner vil styrke egen oppfølging av leverandører og underleverandører for å etablere et helhetlig bilde av styring og kontroll med deres leveranser av IKT-tjenester.

Finanstilsynet tar styrets svar til etterretning.

3.8. Beredskap og kontinuitet

DORA presiserer i art. 24 nr. 6 at foretaket minst én gang i året skal sikre at det gjennomføres hensiktsmessige tester av alle IKT-systemer og -applikasjoner som støtter kritiske eller viktige funksjoner. Videre stiller art. 11 nr. 6 krav 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. I art. 25 nr. 5 står det at foretaket skal dokumentere resultatene av testingen og at 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, øvelse og testing av kriseløsningen. Når virksomhetens konsekvensanalyse foreligger, skal beredskapsplaner oppdateres slik at de samsvarer med kravene som framgår av analysen. Det er avgjørende at testingen av kriseløsningen skjer på foretaksnivå, og at foretaket gjør testene til sine egne – også for IKT-tjenester levert av tredjepartsleverandører – for å vurdere kriseløsningens egnethet og organisasjonens robusthet.

Finanstilsynet pekte i foreløpig rapport på at ved testing av beredskapsplaner, både for foretakets egne og for IKT-tjenester levert av tredjepartsleverandører, må relevante informasjonssikkerhets-scenarioer inkluderes, herunder også verstefallsscenarioer. Finanstilsynet skrev videre om viktigheten av at planverk for gjenoppretting og alternativ drift testes, for eksempel i scenarioer ved langvarig utilgjengelighet av tjenester, og at testene gjennomføres i samsvar med interne instrukser.

Styret skriver i sitt svarbrev at andrelinjen vil følge opp at både førstelinjen og leverandører gjennomfører hensiktsmessig testing av henholdsvis egne beredskapsplaner og IKT-systemer, slik at foretaket har et helhetlig bilde av beredskapsevnen og robustheten i verdikjeden. Videre skriver styret at det vil følge opp at testingen av beredskapsplaner og kriseløsninger gjennomføres i samsvar med gjeldende regelverk og interne instrukser.

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

Stig Ulstein
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk.