

**FINANSTILSYNET**THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAYStyret i NORSE SECURITIES AS
Postboks 2027 Vika
0125 OSLOVår referanse
25/10139
Deres referanse

28.09.2026

Tilsynsrapport

1 Innledning

Finanstilsynet har gjennomført stedlig IKT-tilsyn i Norse Securities AS (heretter "foretaket"). Finanstilsynet gjennomførte møte med foretaket 17. september 2025. I gjennomgangen fokuserte Finanstilsynet på styring med og kontroll av IKT-virksomheten inkludert risikostyring, drift, sikkerhet, bruk av tjenesteleverandører og beredskap. Denne tilsynsrapporten bygger på Finanstilsynets foreløpige rapport fra 2. juni 2026 og styrets kommentar til denne fra 31. august 2026.

2 Finanstilsynets oppsummering

Tilsynet avdekket vesentlige mangler ved foretakets styring med og kontroll av IKT-virksomheten. Dette gjaldt særlig foretakets styrings- og kontrollrammeverk, inkludert strategi, risikostyring og interne kontrollaktiviteter. Videre pekte Finanstilsynet på mangler i foretakets gjennomføring av konsekvensanalyse av virksomheten, endringsledelse, oppfølging av IKT-tjenesteleverandører og testing av beredskaps- og kontinuitetsløsninger. Finanstilsynet ba i foreløpig rapport foretaket snarest rette opp i manglene og vedlegge en handlingsplan for etterlevelse av DORA-forordningen (heretter DORA).

Foretaket har i etterkant av tilsynet gjennomført omfattende tiltak for å rette opp de påpekte forholdene, blant annet gjennom oppdaterte styringsdokumenter, etablering av kontrollrammeverk, gjennomføring av konsekvensanalyse og styrket oppfølging av IKT-risiko og tjenesteleverandører. Finanstilsynet legger til grunn at de gjennomførte tiltakene i stor grad følger opp de avdekkede manglene.

3 Finanstilsynets vurderinger

3.1 Strategi og organisering

Styret skal fastsette prinsipper for risikostyring for foretaket som helhet og innenfor hvert enkelt virksomhetsområde. Det følger av forskrift om risikostyring og internkontroll § 3. Daglig leder skal påse en forsvarlig risikostyring og internkontroll på basis av en vurdering av aktuelle risikoer i henhold til policyer fastsatt av styret, jf. § 4. Videre skal daglig leder sikre at risikostyring og internkontroll gjennomføres og overvåkes på en forsvarlig måte.

Foretaket skal ha et internt styrings- og kontrollrammeverk som sikrer en effektiv og forsvarlig håndtering av IKT-risiko, for å oppnå høy digital operasjonell motstandsdyktighet, jf. DORA art. 5 nr. 1. Styret har det endelige ansvaret for å fastsette og godkjenne strategien for digital operasjonell motstandsdyktighet, herunder fastsette et passende risikotoleransenivå for foretakets

IKT-risiko, jf. art. 5 nr. 2. Strategien skal være integrert i foretakets styringssystem og omfatte klare roller og ansvar. I art. 6 nr. 8 stilles det innholdsmessige krav til foretakets strategi for digital operasjonell motstandsdyktighet. Videre skal foretaket tildele ansvaret for å styre og å føre kontroll med IKT-risiko til en kontrollfunksjon og sikre et passende nivå av uavhengighet for en slik kontrollfunksjon for å unngå interessekonflikter, jf. art. 6 nr. 4.

3.1.1 Styrings- og kontrollrammeverk

Finanstilsynet pekte i foreløpig rapport på at foretakets IKT-strategi manglet flere sentrale elementer for digital operasjonell motstandsdyktighet og som det stilles krav til i DORA art. 5 nr. 2 jf. DORA art. 6 nr. 8. Strategien beskrev ikke hvordan rammeverket for IKT-risikostyring understøtter foretakets forretningsstrategi og mål, og det var ikke fastsatt en risikotoleranse for IKT-risiko. Videre manglet foretaket informasjonssikkerhetsmål med tilhørende nøkkelindikatorer og rapporteringskrav. Foretaket hadde i underliggende styrende dokumenter etablert krav til prosesser som må være på plass i tråd med kravene i DORA, men disse var ikke knyttet til overordnede mål eller strategier, og manglet tilhørende nøkkelindikatorer og rapporteringskrav.

I den foreløpige rapporten vurderte Finanstilsynets at foretaket ikke hadde en styringsmodell som la til rette for en forsvarlig håndtering av IKT-risiko. Finanstilsynet mente derfor at foretakets interne styrings- og kontrollrammeverk var mangelfullt og ikke oppfylte kravene etter DORA art. 5 og 6. De samme forholdene medførte etter Finanstilsynets vurdering også mangler i foretakets styring med og kontroll av IKT-virksomheten etter risikostyringsforskriften § 3 og 4. Manglende mål, risikotoleranse og styringsparametere for IKT-risiko reduserte etter Finanstilsynets vurdering styrets og ledelsens mulighet til å styre og følge opp IKT-risiko.

Styret skriver i sitt svar at de er enig i Finanstilsynets vurdering av manglene i IKT-strategien. Foretaket opplyser at strategien er oppdatert og vedtatt av styret. Foretaket har videre etablert et rammeverk som skal sikre sammenheng mellom strategien og underliggende styrende dokumenter, inkludert dokumentansvar og årsplan.

Finanstilsynet merker seg av ettersendt dokumentasjon at foretaket har gjennomført tiltak for å håndtere forholdene som ble påpekt under tilsynet, og tar styrets svar til etterretning.

3.1.2 Operasjonalisering av styrende dokumenter

Finanstilsynet pekte i foreløpig rapport på at foretaket i begrenset grad gjennomførte kontroller av egen IKT-virksomhet og tjenester levert gjennom IKT-tjenesteavtaler. Finanstilsynet merket seg at oppfølgingen i hovedsak var basert på rapportering av avvik, og det ble ikke gjennomført systematiske kontroller av om krav i foretakets styrende dokumenter etterleves. Etter Finanstilsynets vurdering medfører dette at styregodkjente styringsdokumenter på IKT-området i liten grad var operasjonalisert gjennom et etablert kontrollregime, slik DORA art. 5 nr. 1 forutsetter. Finanstilsynet la videre til grunn at foretaket ikke hadde etablert tilstrekkelig uavhengig kontroll av etterlevelsen av krav på IKT-området, jf. DORA art. 6 nr. 4

Styret skriver i sitt svar at de er enig i at foretaket ikke har gjennomført tilstrekkelig planmessige kontroller av egen IKT-virksomhet. Styret opplyser at oppfølgingen tidligere har vært basert på avviksrapportering, styreorienteringer og årlige risikovurderinger, men at det nå er etablert en kontrollrutine som beskriver kontrollhandlinger, ansvarlig forsvarslinje, frekvens og krav til dokumentasjon. Styret opplyser videre at første kontrollrunde er gjennomført og dokumentert, og at status for gjennomførte kontroller og oppfølging av avvik skal rapporteres periodisk til ledelsen og styret.

Finanstilsynet tar styrets svar til etterretning.

3.2 Virksomhetens konsekvensanalyse

Foretaket skal gjennomføre en konsekvensanalyse av virksomheten (business impact analysis, BIA) for å vurdere virksomhetsmessige konsekvenser ved IKT-avbrudd. Det følger av DORA art. 11 nr. 5. Som en del av konsekvensanalysen skal foretaket 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. 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.

Finanstilsynet forventer at det er forretningssiden i foretaket som har ansvaret for resultatet av en slik konsekvensanalyse. Resultatet av konsekvensanalysen vil blant annet gi oversikt over foretakets systemportefølje, der systemenes kritikalitet for virksomheten er angitt. Videre bør det framgå av analysen hva som er akseptabel nedetid for det enkelte IKT-system. Resultatet av analysen bør også formidles til relevante leverandører. Det legges til grunn at foretaket har rutiner for utarbeidelse og vedlikehold av konsekvensanalysen.

Finanstilsynets vurdering i foreløpig rapport var at foretaket ikke hadde gjennomført en konsekvensanalyse av virksomheten i samsvar med kravene i DORA art. 11 nr. 5. Selv om foretakets kontinuitets- og katastrofeplan viste til at det skulle gjennomføres en driftskonsekvensanalyse, kunne Finanstilsynet ikke se at listen over vesentlige IKT-enheter var basert på en systematisk analyse av virksomhetsmessige konsekvenser ved IKT-avbrudd. Det forelå heller ikke rutiner for gjennomføring og vedlikehold av en slik analyse. Etter Finanstilsynets vurdering medførte dette at foretakets kontinuitets- og kriseplanverk ikke var utformet på grunnlag av dokumenterte forretningsmessige prioriteringer og avhengigheter.

Styret skriver i sitt svar at de er enig i at foretaket ikke hadde gjennomført en tilstrekkelig konsekvensanalyse av virksomheten, og opplyser at tidligere vurderinger av vesentlige IKT-enheter i hovedsak var basert på erfaring. Foretaket har nå gjennomført en konsekvensanalyse ledet av forretningssiden, som er behandlet av styret. Styret opplyser videre at det er etablert rutiner for årlig oppdatering av analysen, at resultatene er formidlet til driftsleverandøren, og at analysen er lagt til grunn for et revidert kontinuitets- og katastrofeplanverk.

Finanstilsynet tar styrets svar til etterretning, og merker seg fra mottatt dokumentasjon at foretaket nå har gjennomført en konsekvensanalyse av virksomheten. Finanstilsynet legger til grunn at foretaket fortsetter å holde konsekvensanalysen oppdatert og benytter den som grunnlag i foretakets IKT-risikostyring.

3.3 Endringsledelse

Foretaket skal ha dokumenterte policyer, framgangsmåter og kontroller for håndtering av IKT-endringer. Det følger av DORA art. 9 nr. 4 (e). 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 endringsledelse. Formålet er å sikre at alle endringer av IKT-systemer registreres, testes, vurderes, godkjennes, gjennomføres og verifiseres på en kontrollert måte. Kravene til policy for endringshåndtering er videre utdypet i kommisjonsforordning (EU) 2024/1174 (RTS for Rammeverk for IKT-risikostyring) art. 17. Foretaket er ansvarlig for etterlevelse av kravene selv om IKT-virksomheten er helt eller delvis tjenesteutsatt, se DORA art. 28 nr. 1 (a).

Finanstilsynet pekte i foreløpig rapport på at foretaket ikke hadde etablert dokumenterte retningslinjer for endringsledelse i samsvar med kravene i DORA art. 9 nr. 4 (e). Foretaket viste til rutiner for håndtering av endringer i egen IKT-infrastruktur, men opplyste samtidig at endringer initiert av IKT-tjenesteleverandører ble håndtert gjennom leverandørenes egne prosesser. Etter Finanstilsynets vurdering innebar dette at foretaket ikke hadde etablert et helhetlig og dokumentert

rammeverk som sikret styring og kontroll med alle endringer som påvirker foretakets IKT-virksomhet, herunder endringer gjennomført av tjenesteleverandører.

Styret opplyser i sitt svar at foretaket allerede før tilsynet hadde krav om at planlagte endringer og vedlikehold, herunder endringer hos driftsleverandøren, skulle klareres med administrerende direktør og/eller IKT-ansvarlig. Videre viser styret til at inngåtte avtaler stiller krav om varsling og samtykke ved endringer. Styret er imidlertid enig i at foretaket manglet en særskilt og dokumentert rutine for endringsledelse. Foretaket har derfor vedtatt en egen rutine for endringsledelse. Rutinen omfatter både egne og leverandørinitierte endringer og inneholder blant annet krav til endringslogg, funksjonsskille, testing, tilbakerulling og håndtering av nødendringer. Foretaket opplyser videre at det skal etableres en fast varslingsrutine med driftsleverandøren.

Finanstilsynet merker seg foretakets presisering om at det også før tilsynet var etablert krav til varsling og godkjenning av endringer hos driftsleverandøren. Finanstilsynet noterer seg fra mottatt dokumentasjon at det i foretakets nye retningslinje for endringsledelse er definert endringsprosedyrer for definerte endringstyper. Finanstilsynet legger til grunn at foretaket i henhold til den nye rutinen er ansvarlig for alle endringer som innføres i foretakets driftsmiljø, og at disse er underlagt risikobasert oppfølging.

3.4 IKT-tredjepartsrisiko

Foretaket skal kontinuerlig identifisere alle kilder til IKT-risiko, og vurdere cybertrusler og IKT-sårbarheter som er relevante for deres IKT-støttede forretningsfunksjoner, informasjonsverdier og IKT-ressurser. Det følger av DORA art. 8 nr. 2. Foretaket skal regelmessig, og minst årlig, gjennomgå risikoscenarioer som påvirker dem.

Foretaket skal ha en strategi og policyer for bruk av IKT-tjenester som støtter kritiske eller viktige funksjoner, inkludert bruk av leverandører der det er relevant, jf. DORA art. 28 nr. 2. 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 pekte i foreløpig rapport på at foretakets risikovurderinger av IKT-risiko og risiko knyttet til bruk av IKT-tjenesteleverandører var mangelfull. I den årlige risikoanalysen framgikk vurderinger av sannsynlighet og konsekvens, men det var ikke beskrevet hvilket grunnlag vurderingene bygget på. Under tilsynet opplyste foretaket at det ikke hadde tilstrekkelig informasjon om leveransene fra IKT-tjenesteleverandørene til å kunne foreta nærmere vurderinger. Etter Finanstilsynets vurdering hadde foretaket dermed ikke et tilstrekkelig grunnlag for å identifisere og vurdere IKT-risiko knyttet til tjenester levert av tredjeparter.

Styret skriver i sitt svar at de er enig i at tidligere risikovurderinger har manglet dokumenterte begrunnelser og tilstrekkelig informasjonsgrunnlag. Foretaket opplyser at det har etablert en egen rutine for risikoanalyse av IKT-tjenesteleverandører med krav til dokumenterte vurderinger, register over IKT-tjenesteavtaler og exit-strategier. Det er videre gjennomført nye risikovurderinger av driftsleverandør og øvrige relevante leverandører basert på innhentet dokumentasjon. Styret opplyser at vurderingene er dokumentert og inngår i foretakets kontroll- og oppfølgingsprosesser.

Finanstilsynet tar styrets svar til etterretning.

3.5 IKT-sikkerhet

Foretaket skal ha robuste sikkerhetsmekanismer for å beskytte IKT-systemer og data. Det følger av DORA art. 9. 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. Etter art. 9 nr. 4 (c) skal foretaket etablere 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 foretaket ikke gjennomførte kontroller av om IKT-tjenesteleverandører etterlevde foretakets krav til IKT-sikkerhet inkludert tilgangsstyring. Finanstilsynet stilte også spørsmål ved foretakets oversikt over IKT-tjenesteleverandørers tilgang til foretakets driftsmiljø. Finanstilsynets vurdering var at foretaket ikke hadde etablert tilstrekkelige kontrollrutiner for å verifisere at konfidensialitet, integritet og tilgjengelighet i kritiske systemer og data var ivarettatt.

Styret skriver i sitt svar at de erkjenner at leverandørers etterlevelse av foretakets sikkerhetskrav ikke ble kontrollert ved tidspunktet for det stedlige tilsynet. Styret presiserer samtidig at foretaket selv administrerer brukerrettigheter til systemer som inneholder kundesensitive opplysninger, og at tilgang til slike data ikke gis til leverandøren uten foretakets godkjenning. Styret opplyser at foretaket nå har etablert faste kontroller av tilganger, attestasjoner og tjenesterapportering som del av sitt kontrollrammeverk.

Finanstilsynet tar styrets svar til etterretning.

3.6 Beredskap og kontinuitet

Foretaket skal ha robuste og dokumenterte beredskaps- og kontinuitetsplaner for å sikre virksomhetens kontinuitet ved alvorlige IKT-hendelser. Det følger av DORA art. 11 nr. 1. Etter art. 11 nr. 6 skal planene testes minst én gang i året. Kravene til kontinuitet og testing av kontinuitetsplaner er utdypet i kommisjonsforordning (EU) 2024/1774 om krav til rammeverk for risikostyring (RTS for IKT-risikostyringsrammeverk). I art. 25 nr. 1 presiseres det at planene skal ta hensyn til virksomhetens konsekvensanalyse. I henhold til art. 25 nr. 2 skal testingen baseres på plausible, alvorlige scenarioer som simulerer potensielle forstyrrelser og inkludere testing av IKT-tjenesteleveranser der det er relevant. Foretaket skal ifølge art. 25 nr. 5 dokumentere resultatene av testingen, og identifiserte mangler som følge av denne skal analyseres, håndteres og rapporteres til ledelsen.

Finanstilsynet konstaterte i foreløpig rapport at foretaket ikke hadde gjennomført testing av beredskaps- og kontinuitetsløsningene i samsvar med kravene i DORA artikkel 11 nr. 6. Foretaket kunne framlegge dokumentasjon på årlige vurderinger av driftsløsningen, men disse var ikke basert på hendelsesscenarioer som kunne medføre alvorlige driftsforstyrrelser. Det forelå heller ikke dokumentasjon som viste at testene tok utgangspunkt i virksomhetens konsekvensanalyse. Etter Finanstilsynets vurdering tilfredsstilte den gjennomførte aktiviteten derfor ikke kravene til testing av beredskaps- og kontinuitetsplaner.

Styret skriver i sitt svar at de er enig i at foretakets tidligere testmetodikk ikke oppfylte kravene til scenariobasert testing. Styret opplyser at foretaket nå har gjennomført en scenariobasert test som er dokumentert, og identifiserte observasjoner og tiltak ble rapportert til styret. Styret opplyser videre at kontinuitets- og katastrofeplanen er revidert med utgangspunkt i den gjennomførte konsekvensanalysen, og at planen nå stiller krav til årlig testing.

Finanstilsynet tar styrets svar til etterretning.

4 Videre oppfølging

Finanstilsynet ber om å motta kopi av protokollen fra styremøtet hvor Finanstilsynets tilsynsrapport blir behandlet.

Vi ber foretaket sende kopi av dette brevet til revisor.

For Finanstilsynet

Wenche Fagereng
seksjonsleder

Hanne Teigland
seniorrådgiver

Dokumentet er godkjent elektronisk.