FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Styret i SKAGERRAK SPAREBANK
Postboks 24
3995 STATHELLE

Vår referanse
24/19236
Deres referanse

26.05.2025

Tilsynsrapport

1 Innledning

Finanstilsynet gjennomførte stedlig IKT-tilsyn i Skagerrak Sparebank (foretaket) 9. og 10. januar 2025. Hensikten med tilsynet var å gjøre en vurdering av hvordan foretaket administrerer, utvikler, drifter, vedlikeholder og sikrer IKT-systemer og -tjenester. Tilsynet så på styring med og kontroll av IKT-virksomheten generelt og IKT-drift, utkontraktering, IKT-sikkerhet og beredskap spesielt. Tilsynet vektla systemløsninger som støtter foretakets kjernevirksomhet og prioriterte IKT-systemer som foretaket har utkontraktert.

Til grunn for tilsynsrapporten ligger Finanstilsynets foreløpige rapport datert 10. mars 2025 og styrets kommentarer til rapporten i brev av 29. april 2025.

2 Finanstilsynets oppsummering

Tilsynet avdekket til dels vesentlige mangler ved foretakets styring med og kontroll av IKT-virksomheten. Foretakets overordnede risikostyring var mangelfull, blant annet knyttet til manglende styregodkjenning av overordnede styringsdokumenter, prosedyrer for risikovurdering av IKT-virksomheten, rapportering av IKT-risiko og internkontroll av IKT-området. Foretakets oppfølging av leverandører var mangelfull og foretaket oppfyller ikke IKT-forskriftens krav til endringshåndtering, avvikshåndtering, tilgangsstyring samt opplæring, øvelse og testing av foretakets kriseløsning. Finanstilsynet har merket seg at foretaket har og vil iverksette en rekke tiltak i tillegg til tiltak på alle påpekte områder.

3 Finanstilsynets vurderinger

3.1 Overordnet styring og kontroll

3.1.1 Overordnet risikostyring

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. IKT-forskriften § 2 første ledd stiller krav til at foretaket skal fastsette overordnede mål, strategier, og sikkerhets-

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

krav for IKT-virksomheten, og i § 3 første ledd stilles det krav om at foretaket skal fastsette kriterier for akseptabel risiko forbundet med bruk av IKT-systemene.

Foretaket er en bank i Eika Alliansen, og Eika Gruppen (Eika) er hovedleverandør av IKT-tjenester til foretaket. Finanstilsynet pekte i foreløpig rapport på at Eikas IT-strategi, som oppfattes å være en av grunnpilarene i Eika-samarbeidet og som lokal IT-strategi var et tillegg til, ikke var styrebehandlet og godkjent i foretaket. Finanstilsynet forventer at det tydelig framgår av foretakets styringsdokumentasjon hvordan foretaket har gjort alliansens IT-strategi til sin egen, herunder hvilke områder som er relevante og viktige for foretaket og hvilke som eventuelt ikke er det.

Det framgår av styrets svarbrev at Eikas IT-strategi nå er styrebehandlet og godkjent av foretakets styre. Finanstilsynet har merket seg styrets bekreftelser på at det tar Finanstilsynet forventninger til etterretning. I kommende revisjon av styringsdokumenter og foretakets tilpasning til DORA-loven[1] vil det tydelig framgå av styringsdokumentasjonen hvordan foretaket har gjort IT-strategien til sin egen. Videre vil alle styringsdokumenter som er av vesentlig betydning for IKT-virksomheten i foretaket bli godkjent i samsvar med CRR/CRD-forskriften § 35, og revidert minst en gang per år eller ved behov.

I foreløpig rapport kommenterte Finanstilsynet at foretakets overordnede styringsdokumentasjon mangler tydeliggjøring av styrets toleranse for IKT-risiko. Finanstilsynet påpekte at det forventes at styret tydeliggjør hva som er styrets toleranse for IKT-risiko, i samsvar med den styrevedtatte generelle risikotoleransen for operasjonell risiko og IKT-forskriften § 3. Videre kommenterte Finanstilsynet at det forventes at styret definerer overordnede måltall og rammer for IKT-virksomheten som bygger opp under den styrevedtatte risikotoleransen.

Det framgår av styrets svarbrev at styret tar Finanstilsynets merknader til etterretning og at styrets toleranse for IKT-risiko er tydeliggjort. Foretaket vil utarbeide terskler for risikotoleranse knyttet til områdene kritikalitet, integritet, tilgjengelighet, økonomi, omdømme og regulatorisk etterlevelse.

Finanstilsynet tar styrets svar til etterretning.

3.1.2 Konsekvensanalyse ved avbrudd i tjenesteleveranse

Hensiktsmessige planer og tiltak for tilgjengelighet og kontinuitet bør etableres med utgangspunkt i konsekvensanalyser for foretakets kritiske forretningsprosesser. Virksomhetsmessig konsekvensanalyse[2] skal bidra til å sikre at foretakets beredskapsplaner utarbeides med basis i forretningsmessig kritikalitet. Planene skal basere seg på foretakets prioriteringer for gjenoppretting av forretningskritiske tjenester og prosesser. Prioriteringene for gjenoppretning skal basere seg på resultatene fra analysen hvor det også skal framgå hva som er akseptabel nedetid for det enkelte IKT-system. Beredskapsplanene, som viser foretakets prioriteringer for gjenoppretting, bør formidles til relevante leverandører. For å verifisere at det er etablert fungerende planer og løsninger må det minst årlig foretas opplæring, øvelse og testing, jf. IKT-forskriften § 11.

I foreløpig rapport kommenterte Finanstilsynet at foretakets rutine for gjennomføring av konsekvensanalyser er kort og overordnet, og at det ikke framgikk eksempelvis hvem som har godkjent den eller når, hvordan malen for konsekvensanalysen skal brukes, eller hvilke konsekvenser en endret vurdering av kritikalitet får for foretakets krise- og beredskapsplaner. Finanstilsynet forventet at foretaket videreutvikler rutiner og prosessbeskrivelser av virksomhetens konsekvensanalyse. Videre kommenterte Finanstilsynet at både rutinen for gjennomføring av konsekvensanalysen og resultatet av den bør framlegges for styret i foretaket.

[1] Lov om digital operasjonell motstandsdyktighet i finanssektoren som forventes å tre i kraft i Norge i løpet av 2025.

[2] Business Impact Analysis (BIA).

Styret skriver i sitt svarbrev at det tar Finanstilsynets merknader til etterretning og at rutinen for ajourhold og oppdatering av konsekvensanalysen er oppdatert og styregodkjent. Resultatet av den første konsekvensanalysen har blitt framlagt for styret.

Videre pekte Finanstilsynet i foreløpig rapport på at det forventer at foretaket videreutvikler gjennomføringen av konsekvensanalysen. Det bør framgå hvilke typer konsekvenser brudd og nedetid får for de ulike prosessene og systemene. En annen sentral nytteverdi av analysen er å sikre at foretakets krise- og beredskapsplaner utarbeides/oppdateres med basis i forretningsmessig kritikalitet, noe som på tilsynstidspunktet gjensto.

Av styrets svarbrev har Finanstilsynet merket seg at foretaket har oppdatert malen for gjennomføring av konsekvensanalyse med "Detaljert konsekvensbeskrivelse" som vil fylles ut med hvilke konsekvenser brudd og nedetid får for de ulike prosessene og systemene. Når det gjelder om, eventuelt på hvilken måte, foretakets krise- og beredskapsplaner er utarbeidet/oppdatert med basis i forretningsmessig kritikalitet, framgår det av styrets svarbrev at foretakets styringsdokumenter vil oppdateres som følge av oppdatering av konsekvensanalysen.

Finanstilsynet tar styrets svar til etterretning og minner om at en sentral nytteverdi av konsekvensanalysen er å sikre at foretakets krise- og beredskapsplaner utarbeides/oppdateres med basis i forretningsmessig kritikalitet. For å sikre at det blir gjort forventer Finanstilsynet at det tydelig framgår av foretakets rutiner og andre styringsdokumenter.

3.1.3 Risikovurdering av IKT

Et finansforetak skal til enhver tid ha oversikt over, og med jevne mellomrom vurdere, hvilke enkelte risikoer og samlet risiko som er knyttet til virksomheten, jf. finansforetaksloven § 13-6 første ledd. Etter IKT-forskriften § 3 skal foretaket ha en dokumentert prosess for gjennomføring av risikoanalyser av IKT-virksomheten, og prosessen skal blant annet definere klare ansvarsforhold og omfatte oppfølging av tiltak som iverksettes som et resultat av den gjennomførte risikoanalysen. Det skal minst en gang årlig, eller ved endringer som har betydning for IKT-sikkerheten, gjennomføres risikoanalyser for å påse at IKT-risikoen styres innenfor akseptable grenser i forhold til foretakets virksomhet. Resultatet av risikoanalysen skal dokumenteres.

I foreløpig rapport påpekte Finanstilsynet at foretaket mangler en rutine eller dokumentert prosess for gjennomføring av risiko- og sårbarhetsanalyser, noe som er brudd på IKT-forskriften § 3.

Finanstilsynet noterer fra styrets svarbrev at styret tar Finanstilsynets merknader til etterretning og har utarbeidet en rutine for årlig gjennomføring av en risiko- og sårbarhetsanalyse for å identifisere, vurdere og håndtere risikoer knyttet til informasjonssikkerhet, driftssikkerhet og etterlevelse av regelverk.

Finanstilsynet tar styrets svar til etterretning.

3.1.4 Internkontroll og rapportering av IKT-risiko

Styret skal føre tilsyn med den daglige ledelse og foretakets virksomhet for øvrig, og sørge for at daglig leder regelmessig gir styret informasjon om foretakets virksomhet. Det følger av finansforetaksloven § 8-6 fjerde ledd. 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. Ledere på alle vesentlige virksomhetsområder skal løpende vurdere gjennomføringen av internkontrollen, vurderingene skal dokumenteres, og daglig leder skal minimum årlig utarbeide en samlet vurdering av internkontrollen som skal forelegges styret for behandling, jf. forskriftens § 37.

I foreløpig rapport påpekte Finanstilsynet at det ikke kunne se at styret mottar adekvat informasjon om foretakets IKT-virksomhet. Videre var det Finanstilsynets vurdering at foretakets gjennomføring av løpende internkontroll av IKT-området var mangelfull og ikke i samsvar med kravene i

CRR/CRD-forskriften § 37. Finanstilsynet stilte også spørsmål ved foretakets vurdering og rapportering av IKT-risiko og etterlevelse av IKT-regelverket fra foretakets andre forsvarslinje.

Det framgår av styrets svarbrev at ny rutine for gjennomføring og rapportering av internkontroll samt rapportering av IKT-risiko er utarbeidet og styrebehandlet. Status på internkontrollen og IKT-risiko vil framover bli rapportert kvartalsvis til styret etter styregodkjente måltall. Videre bekrefter styret at det vil påse at den løpende risikorapporteringen vil bli utvidet med andrelinjens vurdering av foretakets IKT-risiko samt foretakets etterlevelse av IKT-regelverket.

Finanstilsynet tar styrets svar til etterretning.

3.2 IKT-drift - Endrings- og avvikshåndtering

I henhold til IKT-forskriften § 9 skal foretaket sikre at prosedyrer for avviks- og endringshåndtering foreligger og følges. Prosedyrene for endringshåndtering skal omfatte alle endringer som kan påvirke IKT-systemene og skal sikre forsvarlig, formell behandling og dokumentering av endringene. Foretaket skal videre sikre at prosedyrene for endringshåndtering gir en stabil, planlagt og forutsigbar drift. Prosedyrene for avvikshåndtering skal omfatte alle avvik som oppstår i driften av IKT-systemene. Videre skal avviksbehandlingen identifisere årsaken til avvik, hindre gjentagelse og sikre forsvarlig og formell behandling av avviket. Avvikene skal dokumenteres og prosedyrene skal inneholde retningslinjer for eskalering.

I foreløpig rapport pekte Finanstilsynet på at foretakets dokumenterte prosedyrer eller rutiner for endrings- og avvikshåndtering etter Finanstilsynets vurdering var mangelfulle. Dette var blant annet som følge av manglende henvisning til Eikas rutine som foretakets rutinger bygger på, samt manglende beskrivelse av grensesnittet mellom leverandørens og foretakets aktiviteter i de ulike stegende i endringsprosessene og i avvikshåndteringen. Finanstilsynet ba styret sikre at foretaket dokumenterer klare rutiner for endringshåndtering og avvikshåndtering, samt at disse følges opp.

Styret skriver i sitt svarbrev at det tar Finanstilsynets merknader til etterretning og at det nå er etablert en egen rutine for endringshåndtering. Rutinen tar for seg både endringer initiert av foretaket, av alliansen og av andre leverandører. Videre skriver styret at foretaket har etablert en egen rutine for avvikshåndtering som beskriver både avvik i systemer levert av Eika og systemer levert av andre leverandører. Styret bekrefter videre at det vil påse at avvik blir rapportert.

Finanstilsynet tar styrets svar til etterretning.

3.3 Utkontraktering

I henhold til IKT-forskriften § 2 skal foretaket ha retningslinjer for å sikre at utkontraktert IKT-virksomhet oppfyller kravene i § 12. Dette gjelder blant annet krav til skriftlig avtale, der avtalen skal sikre foretakets rett til å kontrollere, herunder revidere leverandørens aktiviteter, samt Finanstilsynets tilgang til opplysninger og mulighet for å føre tilsyn hos IKT-leverandøren. Videre framgår det av § 12 at foretaket har ansvar for at IKT-virksomheten oppfyller alle krav som stilles i forskriften og at dette gjelder også der hele eller deler av IKT-virksomheten er utkontraktert. Av bestemmelsene i § 13 framgår det at foretaket skal sikre at det har en samlet oppdatert dokumentasjon over organisasjon, utstyr, IKT-systemer og vesentlige forhold i IKT-virksomheten. Foretaket skal videre ha en samlet og oppdatert oversikt over alle avtaler om utkontraktering av virksomhet. Det følger av meldepliktforskriften § 1.

Finanstilsynet minnet i foreløpig rapport om at det er foretaket som har det hele og fulle ansvaret for egen virksomhet, også der hele eller deler av IKT-virksomheten er utkontraktert. Finanstilsynets kommentar var blant annet basert på foretakets manglende operasjonalisering av

leverandøroppfølgingen og dokumenteringen av denne, inkludert oppfølging av foretakets hovedleverandør.

Videre vurderte Finanstilsynet at andrelinjens oppfølging og oppmerksomhet rundt utkontraktert virksomhet ikke var tilstrekkelig. For å avgjøre om utkontraktert virksomhet opererer innen akseptabel risiko og etterlever interne og eksterne krav, må denne delen av virksomheten følges opp, på lik linje som foretakets egen virksomhet, jf. kommentarer over i punkt 3.1.4.

Styret tar i sitt svarbrev Finanstilsynet merknader til etterretning og bekrefter at det har iverksatt en rekke tiltak. Styret bemerker blant annet at det vil sikre at oppfølgingen av utkontraktert virksomhet blir inkludert i førstelinjens kvartalsvise IKT-rapportering, at internkontrollen i de ulike virksomhetsområdene også vil omfatte utkontraktert virksomhet, samt at oppfølgingsplaner for hver avtale blir utarbeidet og operasjonalisert. Styret bekrefter videre at det vil påse at andrelinjens rapportering vil inkludere en vurdering av om risiko i leverandørkjeden er tilstrekkelig identifisert, målt og rapportert av de ulike virksomhetsområdene, at andrelinjen utfører egne risiko- og hendelsesbaserte kontroller av rapporter og analyser fra IKT-tjenesteleverandørene og deres underleverandører samt at andrelinjen iverksetter ytterligere kontrolltiltak om nødvendig.

Finanstilsynet tar styrets svar til etterretning.

3.4 IKT-sikkerhet - tilgangsstyring

IKT-forskriften § 5 stiller krav om at foretaket skal ha prosedyrer for å sikre beskyttelse av utstyr, systemer og informasjon av betydning for foretakets virksomhet, mot skader, misbruk, uautorisert adgang og endring, samt hærverk. Videre skal det finnes retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene.

Finanstilsynet påpekte i foreløpig rapport at foretaket ikke har en dokumentert prosedyre eller rutine for tilgangsstyring inkludert for kontroll av tilganger. Finanstilsynet ba styret sikre at foretaket oppretter en rutine for tilgangsstyring inkludert rutine for kontroll av tilganger på nevnte detaljeringsnivåer.

Av styrets svarbrev framgår det at foretaket har utarbeidet flere ulike rutiner for tilgangsstyring, som etter styrets oppfatning vil være dekkende for foretakets kontroll av tilganger.

Finanstilsynet tar styrets svar til etterretning.

3.5 Beredskap

I IKT-forskriften § 11 framgår kravene til at foretaket skal ha en dokumentert kriseplan som skal kunne iverksettes dersom IKT-driften ikke kan opprettholdes som følge av en krise, og at det minst årlig skal gjennomføres opplæring, øvelse og testing av at kriseløsningen virker som forutsatt. Resultatet av testen skal dokumenteres, jf. IKT-forskriften § 11 tredje ledd. Finanstilsynet presiserer at foretaket selv er ansvarlig for at opplæring, øvelse og testing av foretakets kriseløsning gjennomføres årlig, samt oppfølging av IKT-tjenesteleverandører for å sikre at de overholder kravene i IKT-forskriften § 11. Det er viktig at test av kriseløsningen gjennomføres på foretaksnivå og at foretaket gjør testene relevante for foretaket, både med omfang og relevante scenarioer for å vurdere egnetheten til kriseløsningen og robustheten til egen organisasjon og relevante IKT-tjenesteleverandører.

Det stedlige tilsynet avdekket at foretaket ikke gjennomførte øvelse eller test av sine kriseplaner i 2024. Foretaket etterlever dermed ikke IKT-forskriften § 11.

Av styrets svarbrev har Finanstilsynet merket seg at styret tar tilsynets merknader til etterretning. Styret opplyser at det er utarbeidet en ny rutine for årlig test av beredskap- og kriseplaner, og at rutinen er styregodkjent. Videre framgår det at test av kriseplan med ekstern leverandør er avtalt.

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 valgt revisor.

For Finanstilsynet

Olav Johannessen
seksjonsleder

Irene Støback Johansen
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk.