FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

SPAREBANKEN ØST
Postboks 67
3301 HOKKSUND

Vår referanse
24/2857
Deres referanse

29.04.2025

Tilsynsrapport

1 Innledning

Finanstilsynet gjennomførte stedlig IKT-tilsyn i Sparebanken Øst (heretter "banken" eller "foretaket") den 16. april 2024. Til grunn for tilsynsrapporten ligger Finanstilsynets foreløpige rapport datert 17. desember 2024 og styrets kommentarer til rapporten i brev av 12. februar 2025.

2 Finanstilsynets oppsummering

Hensikten med tilsynet var å gjøre en vurdering av hvordan banken 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, endrings- og avvikshåndtering, datastyring og forvaltning, IKT-sikkerhet, utkontraktering og kontinuitet.

Tilsynet avdekket til dels vesentlige mangler ved foretakets styring med og kontroll av IKT-virksomheten, blant annet knyttet til mangelfull rapportering av både intern og utkontraktert IKT-virksomhet, en forhøyet nøkkelpersonrisiko på IKT-området og mangelfull hendelsesrapportering. Finanstilsynet mener Sparebanken Øst i større grad bør innhente uavhengige bekreftelser på at foretakets styring og kontroll med IKT-virksomheten er betryggende. Virksomhetens analyser for avbrudd i kritiske og viktige prosesser dekker for få områder, og øvelse og testing av, og opplæring i, foretakets beredskaps- og kriseløsninger bør omfatte realistiske scenarioer for utvalgte kritiske og viktige prosesser. Finanstilsynet har merket seg at foretaket har og vil iverksette en rekke tiltak.

3 Finanstilsynets merknader

3.1 Organisering av IKT-virksomheten

2.1.1 Nøkkelpersonrisiko

For å håndtere risikoen ved eventuelt tap av nøkkelpersonell, kan foretaket sikre at kompetanse, kunnskap og ansvar på IKT-området fordeles på flere personer, samt sørge for at viktige rutiner og prosedyrer knyttet til IKT-virksomheten dokumenteres, jf. kravene i finansforetaksloven § 8-6 og § 8-11, samt IKT-forskriftens § 2 første ledd.

I foreløpig rapport vurderte Finanstilsynet at banken, på tilsynstidspunktet hadde en forhøyet nøkkelpersonrisiko på IKT-området, gitt den erfaring, det brede ansvaret og den nøkkelposisjon som IKT-direktøren har.

Styret skriver i sitt svar, at etter det stedlige tilsynet har det blitt gjort en rekke tiltak for å redusere nøkkepersonrisikoen. Foretaket har rekruttert en ressurs til utkontraktering og beredskap, samt at

anti-svindelarbeidet overføres til en annen leder og avdeling. Styret vurderer nøkkelpersonrisikoen innenfor IKT-området som forsvarlig.

Finanstilsynet tar styrets svar til etterretning og noterer seg tiltakene som er iverksatt. Finanstilsynet legger til grunn at styret sikrer en forsvarlig lederorganisering på IKT-området gitt den viktighet IKT-virksomheten har for banken.

3.2 De uavhengige kontrollfunksjonene for risiko og etterlevelse

2.2.2 Manglende IKT-kompetanse i andrelinjen (de uavhengige kontrollfunksjonene for risiko og etterlevelse)

CRR/CRD-forskriften § 38 tredje ledd og § 39 andre ledd har krav om at bankens uavhengige kontrollfunksjoner for risiko og etterlevelse skal ha tilstrekkelig kompetanse og ressurser. Finanstilsynets vurderer at tilgang på kompetanse innen IKT, spesielt for den uavhengige kontrollfunksjonen for risiko, er en forutsetning for at denne selvstendig skal kunne identifisere IKT-risikomomenter og vurdere hvilke kontroller som er hensiktsmessige gitt bankens til enhver tid gjeldende IKT-risikobilde.

I foreløpig rapport stilte Finanstilsynet spørsmål ved om banken i tilstrekkelig grad ivaretar CRR/CRD-forskriftens krav til IKT-kompetanse i de uavhengige kontrollfunksjonenes ved utførelsen av kontrollarbeidet knyttet til IKT-risiko.

Styret skriver i sitt svar at leder etterlevelse og leder risikostyring har lang erfaring i banken som sikrer forståelse av banksystemer, infrastruktur i det finansielle systemet, produkter og datavarehus. Videre skriver styret blant annet at IKT-kompetanse i andrelinjen ikke utelukkende handler om teknisk IKT-kompetanse, men også i stor grad evnen til å gjøre selvstendige vurderinger av risikoen som foreligger innenfor IKT. Styret er av den oppfatningen at andrelinje i Sparebanken Øst tilfredsstiller krav til IKT-kompetanse i henhold til CRR/CRD-forskriften.

Finanstilsynet tar styrets svar til etterretning og legger til grunn at lederne for etterlevelse og risikostyring løpende vil sikre at avdelingene innehar tilstrekkelig IKT-kompetanse.

3.3 Internrevisjonens arbeid

Finansforetaksloven § 8-16 annet ledd krever at styret organiserer og fastsetter retningslinjer for internrevisjonen. Kravene til internrevisjonen står i første ledd, hvor det presiseres at internrevisjonen skal kontrollere at foretaket er organisert og drives på en forsvarlig måte og i samsvar med gjeldende krav til virksomheten. Internrevisjonen skal gi styret trygghet for at foretakets system for intern virksomhetsstyring, inkludert internkontroll og risikostyring, er av tilfredsstillende kvalitet og etterleves effektivt i foretaket.

I foreløpig rapport pekte Finanstilsynet på at banken i større grad bør søke uavhengige bekreftelser fra internrevisor på at det er tilfredsstillende styring av og kontroll med de ulike deler av IKT-virksomheten.

Styret skriver i sitt svar at det er blitt utført jevnlig internrevisjonsprosjekter innenfor ulike deler av IKT-området de siste årene. Styret skriver at i 2025 er det planlagt et større internrevisjonsprosjekt i forbindelse med implementering av DORA-loven[1]. Videre har Finanstilsynet merket seg fra styrets

[1] Lov om digital operasjonell motstandsdyktighet i finanssektoren.

svarbrev at styret vil vurdere å gjennomføre IKT-relatert internrevisjonsprosjekt som fast del av kontrollarbeidet for internrevisor de kommende årene.

Finanstilsynet tar styrets svar til etterretning.

3.4 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 (BIA) 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 gjenoppretting 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 pekte Finanstilsynet på at foretaket ikke hadde gjennomført en BIA. Finanstilsynet pekte videre på at foretaket bør etablere en rutine for å gjennomføre BIA, og at representanter for de kritiske og viktige funksjonene i foretaket deltar i analysen. Videre forventer Finanstilsynet at rutinen for BIA blir en del av foretakets ordinære drift.

Styret skriver i sitt svarbrev at det er styrets vurdering at beredskapen i banken har vært håndtert på en forsvarlig måte og vil påse at dette arbeidet dokumenteres ytterligere gjennom en oppdatert BIA inkludert en tydeliggjøring av verst tenkelige avbruddsscenarioer.

Finanstilsynet har merket seg at styret vil påse at bankens arbeid med beredskap dokumenteres ytterligere gjennom en BIA.

Når det gjelder Finanstilsynets påpekning i foreløpig rapport om at foretaket bør etablere en rutine for å gjennomføre BIA og forventningen om at en slik rutine blir en del av foretakets ordinære drift kan ikke Finanstilsynet se at styret har kommentert dette. Finanstilsynet legger til grunn at styret påser at en slik rutine blir etablert.

3.5 IKT-sikkerhet – kontroll av leverandørens tilganger

IKT-forskriften § 5 krever at banken har prosedyrer for å beskytte utstyr, systemer og informasjon av betydning for foretakets virksomhet, mot skader, misbruk, uautorisert adgang og endring, samt hærverk. Videre skal banken ha retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene. EBAs retningslinjer for IKT-sikkerhet og -risiko gir nærmere utdypinger.

I foreløpig rapport pekte Finanstilsynet på at banken ikke har etablert rutiner for å styre og kontrollere tilgangene for ansatte hos IKT-tjenesteleverandør som har tilgang til bankens systemer og/eller data.

Styret skriver i sitt svar at styret ikke deler Finanstilsynets oppfatning om at Sparebanken Øst ikke har rutiner for kontroll av tilgangene til ansatte hos driftsleverandøren som har tilgang til bankens systemer og data. Styret skriver at styret vil følge opp dialogen med systemleverandøren framover og sikre at det etableres en fast rapportering av systemtilganger fra systemleverandørens side. En intern vurdering av behovet for kontroll av tilgangsstyringen vil være en del av denne oppfølgingen.

Finanstilsynet tar styrets svar til etterretning.

3.6 IKT-utkontraktering

I henhold til IKT-forskriften § 2 skal foretaket ha retningslinjer som sikrer at utkontraktert IKT-virksomhet oppfyller kravene i § 12. Dette inkluderer krav til skriftlig avtale, som skal sikre bankens rett til å kontrollere, herunder revidere leverandørens aktiviteter, samt Finanstilsynets tilgang til opplysninger og mulighet for tilsyn hos IKT-leverandøren. Videre skal avtaler om utkontraktering av IKT-virksomhet og endringer av slike avtaler behandles av styret, som også skal presenteres en plan for utkontrakteringen, en risikovurdering av utkontrakteringsforholdet og en beskrivelse av hvordan banken skal sikre leveransene.

I tillegg fastslår IKT-forskriften § 12 at banken har ansvar for risikostyring og internkontroll, selv når hele eller deler av virksomheten er utkontraktert.

Finanstilsynet påpekte i foreløpig rapport at banken ikke synes å ha rutiner for oppfølging av leverandører, inkludert krav til rapportering fra disse.

Styret skriver i sitt svar at de ikke deler Finanstilsynets synspunkt om at banken har manglende rutiner for oppfølging av IKT-leverandører hva gjelder utkontraktert virksomhet. Videre beskriver styret arbeidet som gjøres før inngåelse av avtale om utkontraktering, samt at banken har en policy for utkontraktering basert Finanstilsynets veiledning om utkontraktering. Styret vurderer at banken har tilfredsstillende kontroll tilknyttet oppfølgingen av den utkontrakterte virksomheten og ser samtidig behovet for å forbedre dokumentasjonen tilknyttet dette.

Finanstilsynet kan av styrets svar ikke se at Finanstilsynets forventning om at banken har fastsatt rutine for oppfølging IKT-leverandører er adressert. Finanstilsynet observerer at banken utfører kontrollaktiviteter, men mener at banken bør ha en dokumentert rutine for oppfølging av IKT-leverandørene som i større detalj beskriver rapporteringene fra leverandøren (frekvens, innhold, med mer) og hvordan banken skal vurdere og behandle den mottatte informasjonen. Finanstilsynet legger til grunn at styret påser at en slik rutine blir etablert.

3.7 Endrings- og avvikshåndtering

IKT-forskriftens § 2, § 6 og § 9 har bestemmelser for endringsstyring. For operasjonelle hendelser som medfører vesentlig reduksjon i funksjonalitet som følge av brudd på konfidensialitet, integritet eller tilgjengelighet til IKT-systemer og/eller data, krever § 9 tredje ledd at banken uten ugrunnet opphold skal rapportere hendelsen til Finanstilsynet. EBAs retningslinjer for IKT-sikkerhet og -risiko beskriver nærmere hvilke krav som stilles til deteksjonsløsninger og hendelseshåndtering.

I foreløpig rapport vurderte Finanstilsynet at bankens manglende rapportering av hendelser til Finanstilsynet er brudd på kravet til hendelsesrapportering i IKT-forskriften § 9. Dette forholdet ble vurdert som kritikkverdig.

Styret erkjenner i sitt svar at banken ikke har overholdt sin rapporteringsplikt ved alvorlige eller kritiske hendelser. Videre skriver styret at i etterkant av det stedlige tilsynet har bankens rutiner på området blitt skjerpet.

Finanstilsynet tar styrets svar til etterretning og merker seg at tiltak har blitt innført for sikre etterlevelse av regelverket.

3.8 Beredskap og krisehåndtering

IKT-forskriftens § 11 krever at banken har en dokumentert kriseplan som kan iverksettes hvis IKT-driften svikter på grunn av en krise. Det framgår videre av IKT-forskriften at banken minst årlig skal gjennomføre opplæring, øvelse og testing for å dokumentere at kriseløsningen fungerer som forventet. EBAs retningslinjer for IKT-sikkerhet og -risiko gir anbefalinger om utarbeidelse av kontinuitetsplaner, respons- og gjenopprettingsplaner, testing og kommunikasjonsplaner ved kriser.

I foreløpig rapport vurderte Finanstilsynet at for å kunne vurdere egnetheten til kriseløsningene og robustheten til organisasjonen bør det etableres en rutine for årlig gjennomføring av opplæring, øvelse og test, der denne rutinen inngår i foretakets ordinære drift. Finanstilsynet ga også uttrykk for at testaktiviteten i 2023 og framgangsmåten ikke er tilstrekkelig for å oppfylle IKT-forskriftens krav om å øve på og teste at kriseløsningene fungerer som forutsatt. Videre pekte Finanstilsynet på at disse testene ikke var satt opp med bakgrunn i en dokumentert BIA, sikkerhetspolicy eller andre retningslinjer som stiller krav ved test av kriseløsning hos leverandører eller underleverandører.

Styret skriver i sitt svar om bankens strategiske valg av løsninger som reduserer kompleksitet og risiko sammenliknet med andre banker som utvikler og drifter egne tjenester. Styret skriver at IKT-tjenesteleverandør gjennomførte flere øvelser i 2023 og første kvartal 2024 og at styret vurderer disse til å støtte kritiske prosesser og være tilfredsstillende.

Finanstilsynet tar styrets svar til etterretning og bemerker at testaktiviteter bør planlegges basert på realistiske scenarioer slik at banken på denne måten sikrer at kritiske og viktige tjenester og prosesser omfattes.

4 Videre oppfølging

Finanstilsynet ber foretaket sende kopi av dette brevet til revisor.

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

For Finanstilsynet

Olav Johannessen
seksjonsleder

Snorre Vik Sanfelt
førstekonsulent

Dokumentet er godkjent elektronisk.