FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Styret i TRØGSTAD SPAREBANK
Postboks 114
1861 TRØGSTAD

Vår referanse
24/6872
Deres referanse

10.01.2025

Tilsynsrapport

1 Innledning

Finanstilsynet gjennomførte stedlig IKT-tilsyn i Trøgstad Sparebank (foretaket eller banken) tirsdag 3. september 2024.

Hensikten med tilsynet var å gjøre en vurdering av hvordan foretaket administrerer, utvikler, drifter, vedlikeholder og sikrer IKT-systemer og -tjenester. Finanstilsynet ville se på styring med og kontroll av IKT-virksomheten med spesiell vekt på IKT-risiko, endrings- og avvikshåndtering, datastyring og forvaltning, IKT-sikkerhet, utkontraktering og beredskap.

Til grunn for tilsynsrapporten ligger Finanstilsynets foreløpige rapport datert 23. oktober 2024 og styrets kommentarer til rapporten i brev av 25. november 2024.

2 Finanstilsynets merknader

Overordnet styring og kontroll

Organisering og kontrollfunksjoner

Det framgår av finansforetaksloven § 8-6 første ledd at styret skal sørge for forsvarlig organisering av virksomheten. Videre i lovens § 13-5 andre ledd stilles det krav om at et finansforetak skal ha uavhengige kontrollfunksjoner med ansvar for risikostyring, etterlevelse og internrevisjon. I finansforetaksforskriften § 8-3 er det gitt unntak fra krav om internrevisjon for finansforetak som har en samlet forvaltningskapital lavere enn 10 milliarder kroner.

IKT-forskriften § 2 første ledd presiserer at IKT-virksomheten skal utføres på en betryggende måte. Det skal oppnevnes ansvarlige i foretaket for de ulike delene av IKT-virksomheten, og at det med ansvarlig menes en funksjon eller stilling. Foretakets førstelinje skal sørge for at IKT-sikkerheten er etablert og ivaretas i tråd med foretakets policyer og retningslinjer, herunder gjennomføre nødvendige kontroller. Foretakets andrelinje skal være en uavhengig funksjon som fører kontroll med førstelinjens risikostyring og etterlevelse.

Finanstilsynet viste i foreløpig rapport til at foretaket hadde en person som jobbet full tid med IKT (IT-ansvarlig) og som hadde hatt denne rollen i mange år. Banken var på tilsynstidspunktet i prosess med å ansette ytterligere en person på IKT-området for å redusere nøkkelpersonsrisikoen. Finanstilsynet har merket seg fra styrets svar at ytterligere en person nå er ansatt.

Finanstilsynet pekte videre i foreløpig rapport på at andrelinjefunksjonen i banken opptrådde i flere roller, også som stedfortreder for IT-ansvarlig i førstelinjen. Finanstilsynet viste til at banken burde

Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00
post@finanstilsynet.no
finanstilsynet.no

Saksbehandler
Åshild Johnsen
Dir. tlf. 22 93 97 02

vurdere å finne en stedfortreder til IT-ansvarlig i førstelinjen. Styret opplyser i sitt svar at banken nå har endret stedfortreder for IT-ansvarlig til økonomisjef, for å sikre etterlevelsesfunksjonens uavhengighet frem til den nye ressursen på IKT-området er på plass.

Finanstilsynet har fra styrets svar også merket seg at banken har oppdatert IT-ansvarliges stillingsinstruks for å definere arbeidsoppgavene, rollene og ansvaret til IT-ansvarlig.

Finanstilsynet tar styrets svar til etterretning.

Rapportering

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. 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

Rapportering fra førstelinjen

Banken er en bank i Eika Alliansen, og Eika Gruppen (Eika) er hovedleverandør av IKT-tjenester til banken.

Finanstilsynet viste i foreløpig rapport til at det på tilsynsmøtet framsto som at det først og fremst var andrelinjen som vurderte informasjonen/dokumentasjonen fra Eika inkludert at andrelinjen rapporterte kvartalsvis operasjonell risiko til styret. Finanstilsynet stilte spørsmål ved om styret mottar adekvat informasjon om foretakets IKT-virksomhet basert på førstelinjens rapportering til ledelsen og styret.

Styret viser i sitt svar til at det er IT-ansvarlig som årlig utarbeider ROS-analysen på IT-området som sendes bankens styre og ledelse, og at IT-ansvarlig er tett involvert i den årlige internkontrollbekreftelsen som utarbeides av banksjef. Bankens styre vil påse at bankens IT-ansvarlig jevnlig rapporterer til ledelsen.

Rapportering fra andrelinjen

Finanstilsynet kommenterte i foreløpig rapport at de kvartalsvise compliance- og risikorapportene fra andrelinjen er omfangsrike, men i liten grad omtaler vurderinger av IKT-risikoen eller bankens etterlevelse av IKT-forskriften. Etter Finanstilsynets vurdering burde banken videreutvikle rapporteringen til styret slik at vurderinger av risikonivå og etterlevelse innen IKT-området tydeligere framkommer.

Styret viser i sitt svar til at banken har utvidet risikorapporten med en egen side for vurdering av risikonivå og trender på IT-området. Videre har banken i etterkant av tilsynsmøtet videreutviklet compliance-rapporten til å inkludere etterlevelse av IKT-forskriften, samt til å gi et mer oppsummerende bilde av etterlevelsesrisiko og trender.

Finanstilsynet tar styrets svar til etterretning.

Manglende dokumentasjon av styrets vurderinger i styreprotokollene

Det framgår av § 35 i CRR/CRD-forskriften at foretakets styre skal godkjenne og regelmessig vurdere retningslinjer for å påta foretaket risikoer og for å identifisere, styre, overvåke og kontrollere risikoer som foretaket er eller kan bli eksponert for. Styret skal sikre seg tilgang til risikoinformasjon og fastsette omfang, format og frekvens på rapporteringen.

Med henvisning til bankens felles risiko- og revisjonsutvalg utgått av styret samt oversendte protokoller behandlet i henholdsvis risiko- og revisjonsutvalget og styret i perioden, viste

Finanstilsynet til at det i liten grad framgår av styreprotokollene hvilke vurderinger styret har gjort ved behandling av rapportene som først har vært behandlet i risiko- og revisjonsutvalget.

Finanstilsynet pekte i foreløpig rapport på at styret skal sikre seg tilgang til sentral risikoinformasjon slik at risiko, inkludert IKT-risiko, som banken er eller kan bli eksponert for, i tilstrekkelig grad behandles av styret. Finanstilsynet ba styret utvide omtalen i styreprotokollene slik at styrets vurderinger og beslutninger av IKT-risiko dokumenteres tilstrekkelig omfattende til at de kan etterprøves i ettertid.

Styret viser i sitt svar til at alle referatene fra risiko- og revisjonsutvalget blir referert i styremøtet, og dette blir dokumentert i styreprotokollene. Styret viser videre til at de tar kommentaren til etterretning og vil utbedre dette i fremtidige styreprotokoller.

Finanstilsynet tar styrets svar til etterretning.

Risikovurderinger for IKT-området

Foretaket skal fastsette kriterier for akseptabel risiko, jf. IKT-forskriften § 3 første ledd. Videre skal foretaket ha en dokumentert prosess for gjennomføring av risikoanalyser for IKT-virksomheten, jf. annet ledd. I annet ledd er det videre presisert at prosessen skal definere klare ansvarsforhold og omfatte oppfølging av tiltak som skal iverksettes på bakgrunn av resultatene i risikoanalysen. Risikoanalyser skal gjennomføres minst en gang i året, eller ved endringer som har betydning for IKT-sikkerheten, jf. IKT-forskriften § 3 tredje ledd. Analysene skal gjennomføres for å påse at risiko styres innenfor akseptable grenser i forhold til foretakets virksomhet. Analysene skal dokumenteres.

Finanstilsynet pekte i foreløpig rapport på at risikoene knyttet til leverandørene først og fremst beskriver bortfall av tjenestene og i liten grad omtaler risiko for feil eller tap av data. Finanstilsynet anbefalte at banken tydeligere adresserer risikoene for brudd på integritet (feil i systemer) og konfidensialitet (tap av data) samt risikoen for sikkerhetshendelser, i IKT-risikoanalysen.

Fra styrets svar framgår det at styret tar Finanstilsynets anbefaling til etterretning.

Virksomhetsmessig konsekvensanalyse (BIA[1])

Ifølge IKT-forskriften § 13 skal det foreligge oppdatert dokumentasjon av det enkelte IKT-system som er av betydning for foretakets virksomhet. Hensiktsmessige planer og tiltak for tilgjengelighet og kontinuitet bør etableres med utgangspunkt i konsekvensanalyser for foretakets kritiske forretningsprosesser. Virksomhetsmessig konsekvensanalyse skal bidra til å sikre at foretakets beredskapsplaner utarbeides med basis i forretningsmessig kritikalitet.

Finanstilsynet ble under tilsynsmøtet informert om at foretaket ikke har gjennomført en virksomhetsmessig konsekvensanalyse, men at det er igangsatt et prosjekt for å etablere et rammeverk for dette og at det vil bli gjennomført en virksomhetsmessig konsekvensanalyse innen utgangen av 2024.

Finanstilsynet viste i foreløpig rapport til at uten en virksomhetsmessig konsekvensanalyse, vil foretakets kriseplan, jf. IKT-forskriften § 11, være utarbeidet uten forretningsmessige prioriteringer. Finanstilsynet forventer at foretaket utarbeider virksomhetsmessig konsekvensanalyse ledet av forretningssiden, der resultatet av konsekvensanalysen blant annet vil gi oversikt over foretakets systemportefølje der kritikaliteten systemene har for foretakets virksomhet er angitt. Videre bør det framgå av analysen hva som er akseptabel nedetid for det enkelte IKT-system. Resultatet av

[11] Business Impact Analysis

analysen bør også formidles til relevante leverandører. Det legges til grunn at rutine for utarbeidelse av virksomhetsmessig konsekvensanalyse etableres og inngår i foretakets ordinære drift.

Finanstilsynet har merket seg styrets svar der det framgår at styret vil påse at banken etablerer rutine for utarbeidelse av virksomhetsmessig konsekvensanalyse, at denne vil inngå i foretakets ordinære drift, samt at dette arbeidet vil ledes av forretningssiden.

Finanstilsynet tar styrets svar til etterretning.

Styring med og kontroll av IKT-virksomheten

Endrings- og avvikshåndtering

Foretaket skal ha prosedyrer for endringshåndtering og påse at disse følges, jf. IKT-forskriften § 9 første ledd. Prosedyrene skal omfatte alle endringer som kan påvirke IKT-systemene, jf. § 9 fjerde ledd. Videre skal prosedyrene sikre forsvarlig, formell behandling og dokumentering av endringene. Foretaket skal sikre at prosedyrene for endringshåndtering gir stabil, planlagt og forutsigbar drift.

Finanstilsynet stilte i foreløpig rapport spørsmål til hvorfor enkelte endringer, som førte til alvorlige avvik og som Eika rapporterte som IKT-hendelser til Finanstilsynet, manglet i bankens oversikt over IKT-endringer hvor det oppsto problemer etter endringen forrige og inneværende år. Finanstilsynet forstår fra styrets svar at banken ikke var tilstrekkelig varslet av leverandøren om endringene. Finanstilsynet har videre merket seg at inntil nå har Finanstilsynet mottatt mer informasjon fra Eika om hendelser enn det banken har. Banken har ikke mottatt de utfyllende rapportene om hendelser som Finanstilsynet mottar etter ca. 30 dager. For enkelte hendelser framkommer det først i den utfyllende rapporten om hendelsen var forårsaket av en endring eller ikke. Banken har derfor manglet denne informasjonen. Finanstilsynet har fra styrets svar merket seg at Eika vil endre sine rutiner, slik at sluttrapportene om hendelsene også deles med bankene.

Finanstilsynet understreker at selv om IKT-virksomheten er helt eller delvis utkontraktert, er det foretaket som har ansvaret og det er derfor viktig at banken er kjent med årsakene til IKT-hendelsene som rammer den.

Utkontraktering

Foretaket plikter å ha retningslinjer som sikrer at utkontraktert virksomhet oppfyller kravene i IKT-forskriften § 12, jf. IKT-forskriften § 2 annet ledd. IKT-forskriften § 12 første ledd stiller krav til skriftlig avtale og at avtalen skal sikre foretakets rett til å kontrollere, herunder revidere leverandørens aktiviteter. I tillegg må avtalen sikre at Finanstilsynet gis tilgang til opplysninger fra og tilsyn hos IT-leverandøren, jf. § 12 annet ledd. Utkontrakteringsavtaler vedrørende IKT-virksomhet og endring av slike avtaler skal behandles av styret, jf. IKT-forskriften § 2 fjerde ledd. Videre skal styret presenteres en plan for utkontrakteringen, en risikovurdering av utkontrakteringsforholdet og en beskrivelse av hvordan foretaket skal sikre leveransene.

Foretaket har ansvaret for at IKT-virksomheten oppfyller kravene i IKT-forskriften. Dette gjelder også der hele eller deler av IKT-virksomheten er utkontraktert, jf. IKT-forskriften § 12 første ledd.

Bankens IKT-tjenester er i all hovedsak utkontraktert. Eika inngår på vegne av bankene i alliansen avtalene om utkontraktering til underleverandører. Enkelte oppgaver er utkontraktert til Eika, eksempelvis førstelinje-support fra Eika Service Senter (ESS).

<u>Manglende møteplasser mellom førstelinjen og Eika</u>

Finanstilsynet ble på tilsynsmøtet informert om at Eika deler en rekke typer IKT-relatert informasjon og dokumentasjon med bankene via det såkalte Eiketreet. Eika avholder også webinarer om ulike temaer der bankene kan stille spørsmål. På tilsynsmøtet framkom det at IT-ansvarlig har mye kontakt med ESS knyttet til den daglige oppfølgingen av IKT-operasjonene. Sett bort fra kontakten med ESS,

var Finanstilsynets inntrykk at kommunikasjonen mellom Eika og banken fortrinnsvis var enveis, dvs. fra Eika til banken. Finanstilsynet stilte i foreløpig rapport spørsmål om banken manglet formelle møteplasser med Eika for direkte dialog om oppfølgingen av den utkontrakterte IKT-virksomheten.

Styret viser i sitt svar til at i tillegg til at Eika avholder månedlige IT-webinarer, har bankene i alliansen en egen teams-kanal for IT-ansvarlige. Dette er en arena som ligger til rette for og som benyttes til toveis kommunikasjon for oppfølging av endringer, revisorbekreftelse for leverandører, hendelser, leverandørers kriseplaner m.m. Bankens styre anser den eksisterende teams-kanalen som tilfredsstillende ift. en aktiv, digital, møteplass for toveiskommunikasjon med Eika (og andre IT-ansvarlige) på IKT-området.

Finanstilsynet tar styrets svar til etterretning og understreker viktigheten av at banken vurderer den IKT-relaterte dokumentasjonen fra leverandøren og følger opp denne gjennom aktiv toveis kommunikasjon med leverandøren.

Manglende rutine for oppfølging av leverandører

Finanstilsynet kommenterte i foreløpig rapport at oppfølging av utkontraktert IKT-virksomhet er beskrevet i et kapittel i bankens 'Retningslinjer for utkontraktering', men at banken mangler en egen mere detaljert rutine for dette. Sett i lys av bankens absolutte leverandøravhengighet på IKT-området, var Finanstilsynets vurdering at banken burde ha en egen rutine for oppfølging av utkontraktert IKT-virksomhet som i større detalj beskriver rapporteringene fra leverandøren (frekvens, innhold, med mer) og videre hvordan banken skal vurdere den mottatte informasjonen.

Styret viser til at de mener 'Retningslinjer for utkontraktering' langt på vei dekker flere punkter for oppfølging av utkontraktert virksomhet, men er enige i at det bør utarbeides en praktisk arbeidsrutine for oppfølging av utkontraktert virksomhet med frekvens, innhold, med mer.

Finanstilsynet tar styrets svar til etterretning og forutsetter at rutinen utarbeides.

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 med dokumentasjon av testresultater, som viser om kriseløsningen virker som forutsatt. Finanstilsynet presiserer at foretaket selv er ansvarlig for at opplæring, øvelse og testing av foretakets kriseløsning gjennomføres årlig.

Når den virksomhetsmessige konsekvensanalysen foreligger, må beredskapsplaner oppdateres slik at de samsvarer med risikoene avdekket i analysen. Det er viktig at test av kriseløsningen gjennomføres på foretaksnivå og at foretaket gjør testene til sine egne for å vurdere egnetheten til kriseløsningen og robustheten til organisasjonen. Resultatet av testen skal dokumenteres jf. IKT-forskriften § 11.

Finanstilsynet pekte i foreløpig rapport på at ikke bare IT-ansvarlig, men hele bankens beredskapsutvalg må engasjeres i årlige skrivebordstester og øvelser av kriseplanen. Finanstilsynet pekte videre på at ved testing av beredskapsplaner, for foretakets egne og for utkontrakterte IKT-tjenester, må relevante informasjonssikkerhetsscenarioer inngå, der også verstefallsscenarioer er inkludert i beredskapstestingen.

Fra styrets svar framgår det at ved utarbeidelse av «Kriseplan IT» for 2024 har banken involvert hele beredskapsutvalget, for å sikre opplæring i planen, samt involvering av forretningssiden. Bankens styre sier seg enig i at beredskapstesten kan ha forbedringspotensial.

Finanstilsynet tar styrets svar til etterretning og understreker at informasjonssikkerhetsscenarioer må inngå i beredskapstestingen.

Kopi av dette brevet bes sendt til valgt revisor.

For Finanstilsynet

Olav Johannessen
seksjonsleder

Åshild Johnsen
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk.