FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

SPAREBANK 68 GRADER NORD
Postboks 63
8376 LEKNES

VÅR REFERANSE	DERES REFERANSE		DATO
22/6489			29.08.2023

Tilsynsrapport

Finanstilsynet gjennomførte stedlig tilsyn i Sparebanken 68º Nord (Banken) 2. september 2022. Tilsynet hadde som formål å gjøre en vurdering av hvordan Banken administrerer, utvikler, drifter, vedlikeholder og sikrer IKT-systemer og -tjenester. Tilsynet ble avgrenset til elektronisk forsvar og tilhørende emner innen IKT-sikkerhet og styring og kontroll med IKT-virksomheten. Videre ønsket Finanstilsynet å gjøre en vurdering av Bankens beredskapsarbeid relevant for IKT-området, herunder vurdere beredskapen i Banken og for utkontrakterte IKT-tjenester, samt at regulatoriske krav på dette området overholdes.

Til grunn for disse merknadene ligger Finanstilsynets foreløpige rapport datert 10. februar 2023 og styrets kommentarer til rapporten i brev av 28. februar 2023.

Finanstilsynet har følgende merknader etter det stedlige tilsynet:

Overgang fra Eika Alliansen - til Lokalbank-samarbeidet

Banken gikk 24. oktober 2021 ut av Eika Alliansen etter en oppsigelsestid på tre år. Finanstilsynet ble under tilsynet informert om at det ifm. uttredelsen ble utarbeidet en Gap-analyse som viste hvilke tjenester bankene i Lokalbank-samarbeidet mottok fra Eika Alliansen og hvilke tiltak som måtte etableres for å dekke opp de enkelte påviste gapene.

Av styrets svar blir det bekreftet at alle gap i analysen var lukket innen migreringen 25. november 2021.

Finanstilsynet tar styrets svar til etterretning.

Organisering

Det framgår av finansforetaksloven § 8-6 første ledd at styret skal sørge for forsvarlig organisering av virksomheten. Videre stilles det i lovens § 13-5 andre ledd krav om at Banken skal ha uavhengige kontrollfunksjoner med ansvar for risikostyring, etterlevelse og internrevisjon. CRR/CRD IV-forskriften stiller i § 38 krav om at Banken skal ha en uavhengig risikokontroll-funksjon med tilstrekkelig kompetanse og ressurser, og at risikokontrollfunksjonen skal sikre at alle

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00

post@finanstilsynet.no
www.finanstilsynet.no

Saksbehandler
Stig Ulstein
Dir. tlf. 22 93 99 66

vesentlige risikoer i Banken er identifisert, målt og rapportert av de relevante organisatoriske enhetene.

Finanstilsynet ble i tilsynet informert om at ansvaret for IKT-sikkerhet, oppfølging av IKT-utkontraktering og førstelinje risikorapportering for hele IKT-området ligger i IT-gruppen. Finanstilsynet pekte i foreløpig rapport på at det er viktig for Banken å opprettholde høy kompetanse på IKT-området. Videre påpekte Finanstilsynet at Banken med bakgrunn i sin størrelse i Lokalbank-samarbeidet har et særlig ansvar for å bidra med bank- og IKT-kompetanse inn i samarbeidet. Finanstilsynet påpekte derfor viktigheten av at Banken har gjennomført og dokumentert sine vurderinger for forsvarlig virksomhetsstyring innenfor IKT-området.

Finanstilsynet ba også Banken vurdere om den har tilstrekkelig kompetanse i andrelinje-funksjonen for IKT-området og om funksjonen har en tilstrekkelig uavhengig rolle.

I svaret fra styret framgår det at Banken vurderes å ha en forsvarlig organisering og god kompetanse innenfor IKT-området, og at Bankens kontrollfunksjoner i tilstrekkelig grad informerer styret om risikofaktorer som avdekkes. Det framgår også at styret mener Banken har tilstrekkelig kompetanse til å etterleve kravene som stilles til andrelinje-funksjonen på IKT-området selv om andrelinje-funksjonen ikke har spesialkompetanse innenfor IKT.

Finanstilsynet understreker styrets ansvar for å sikre at Bankens kontrollfunksjoner har tilstrekkelig kompetanse på IKT-området til å utføre kontroller på bankens IKT-virksomhet.

Finanstilsynet pekte i foreløpig rapport også på viktigheten av at revisjonsplanene for bankens internrevisjon inneholder planer for revisjoner av IKT-virksomheten.

Finanstilsynet har fra styrets svar merket seg at intern revisor skal foreta en årlig gjennomgang av IKT-området. Finanstilsynet vil understreke styrets ansvar for at revisjonsaktiviteter av IKT-virksomheten inkluderes i Bankens årlige internrevisjonsplan.

Overordnet risikostyring

CRR/CRD IV-forskriften stiller krav om at styret skal godkjenne og regelmessig vurdere retningslinjer for å påta Banken risikoer og for å identifisere, styre, overvåke og kontrollere risikoene. IKT-forskriften § 2 første ledd stiller videre krav til at Banken skal fastsette overordnede mål, strategier og sikkerhetskrav for IKT-virksomheten.

I foreløpig rapport viste Finanstilsynet også til bestemmelsen i IKT-forskriften § 3 hvor det framgår at Banken skal "minst en gang årlig, eller ved endringer som har betydning for IKT-sikkerheten, gjennomføre risikoanalyser for å påse at risiko styres innenfor akseptable grenser i forhold til Bankens virksomhet. Resultatet av risikoanalysen skal dokumenteres". Finanstilsynets vurdering i foreløpig rapport var at Bankens etterlevelse av IKT-forskriften § 3 ikke er tilstrekkelig ivaretatt.

Av styrets svar framgår det at Banken har gjennomført en oppdatering av risiko og sårbarhetsvurdering i 2022 og at denne vil behandles i Bankens styre. Videre skriver styret at Banken ikke har fastsatt kriterier for akseptabel risiko forbundet med bruk av IKT-systemer, men at det er iverksatt et arbeid i Lokalbank-samarbeidet for å finne kriterier å styre etter som passer for

Banken. Finanstilsynet har videre fra styrets svar notert seg at Banken vil tilpasse malen for risiko- og sårbarhetsanalysen utarbeidet av Lokalbank-alliansen til Banken, ut fra Bankens eget perspektiv.

Finanstilsynet fastholder at Bankens etterlevelsen av IKT-forskriften § 3 ikke er tilstrekkelig ivaretatt. Finanstilsynet understreker viktigheten av at arbeidet med å utarbeide mal for risiko- og sårbarhetsanalyse for bruk av IKT-system i Lokalbank-samarbeidet samt fastsette kriterier for akseptabel risiko blir ferdigstilt og at styret påser at arbeidet med å tilpasse denne til Banken blir gjennomført.

Rapportering av IKT-risiko

Etter finansforetaksloven § 8-6 fjerde ledd skal styret føre tilsyn med den daglige ledelse og Bankens virksomhet ellers, og sørge for at daglig leder regelmessig gir styret informasjon om Bankens virksomhet. Krav til styrets rolle knyttet til Bankens system for risikostyring og internkontroll følger av CRR/CRD IV-forskriften § 35. Der presiseres det blant annet at styret skal sikre seg tilgang til risikoinformasjon og fastsette omfang, format og frekvens på rapporteringen.

I foreløpig rapport ble det pekt på at rapportering av risiko for IKT-området ikke inngikk i Bankens faste risikorapporter til styret.

Det framgår av styrets svar at det er gjennomført tiltak som sikrer at Banken vil rapportere IKT-risiko regelmessig til Bankens ledelse, revisjons- og risikoutvalg og styre.

Finanstilsynet tar styrets svar til etterretning.

Driftsavbrudd og beredskap

Banken har ansvar for at nødvendig forretningsmessig kontinuitet og beredskap er sikret, jf. IKT-forskriften § 11 Driftsavbrudd og kriseberedskap. EBAs retningslinjer for IKT og sikkerhet gir en utdyping av IKT-forskriftens bestemmelse for hvordan foretak skal sikre forretningsmessig kontinuitet basert på forretningsmessig konsekvensanalyser (BIA[1]). Videre gir den råd om utarbeidelse av kontinuitetsplaner, respons- og gjenopprettingslaner, testing og kommunikasjons-planer ved kriser.

I foreløpig rapport pekte Finanstilsynet på at hensiktsmessige planer og tiltak for tilgjengelighet og kontinuitet bør etableres med utgangspunkt i forretningsmessige konsekvensanalyser (BIA) for Bankens kritiske forretningsprosesser. Videre skal de forretningsmessige konsekvensanalysene bidra til å sikre at Bankens beredskapsplaner utarbeides med basis i forretningsmessig kritikalitet, og at planene fastsetter Bankens prioritering for gjenoppretting av systemer/løsninger.

Det framgår av styrets svar at styret er enig i Finanstilsynets vurderinger og at Banken vil utarbeide og iverksette rutiner for området.

Finanstilsynet tar styrets svar til etterretning.

I foreløpig rapport pekte Finanstilsynet også på at Banken 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.

[1] BIA – Business Impact Analysis

I styrets svar vises det til Bankens Kriseplan IKT og at denne inneholder definisjoner og scenarier med eksempler på hendelser som vurderes som krise, samt at innholdet i kriseplanen vurderes som tilstrekkelig for formålet.

Finanstilsynet tar styrets svar til etterretning.

Leverandørstyring

Det ble i foreløpig rapport pekt på at Banken i henhold til forskrift om meldeplikt ved utkontraktering av virksomhet mv. § 1 skal foretaket ha en samlet oversikt over utkontrakteringsavtaler.

I styrets svar fremkommer det at Bankens oversikt over utkontrakteringer er oppdatert og komplettert og at innholdet i oversikten videreutvikles for å sikre god intern oppfølging.

Finanstilsynet tar styrets svar til etterretning.

I foreløpig rapport pekte Finanstilsynet også på viktigheten av at Banken kjenner til Exit-mulighetene i avtaler og den operasjonelle risikoen denne innebærer for Banken for å unngå Lock-in risiko. Det ble også pekt på at Banken burde sikre gode Exit-bestemmelser i utkontrakteringsavtalene, slik at det blant annet er tydelig hva som skal til for å komme ut av avtalen, hvor lang tid dette tar og hvilken bistand leverandøren forplikter seg til. I tillegg bør banken også vurdere mulige alternativer.

Det framgår av styrets svar at Banken har gjennomført vurderinger som viser risikoen ved eksisterende avtaler og leverandører og vurdering av Lock-In risiko, og at denne er håndterbar.

Finanstilsynet tar styrets svar til etterretning.

Systemsikkerhet

IKT-forskriften § 5 Sikkerhet stiller krav om at Banken skal ha "prosedyrer som skal 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". Ytterligere utdypinger finnes i EBAs retningslinjer for IKT og sikkerhet.

Det ble i foreløpig rapport pekt på at Banken har etablert en egen sikkerhetspolicy og at denne også gjelder for utkontraktert IKT-virksomhet. Videre ble det pekt på at det bør være etablert rutiner for styring og kontroll av systemsikkerhet for utkontraktert IKT-virksomhet. Banken må også sikre at tjenesteleverandørene innfrir sikkerhetskravene som Banken har besluttet i egen sikkerhetspolicy. Dette inkluderer sårbarhetsstyring med krav til oppdateringer, håndtering av maskin- og programvare som ikke lenger er støttet av leverandør, livssyklushåndtering med krav til anskaffelser/avhending av utstyr m.fl.

Finanstilsynet merker seg fra styrets svar at styret mener Banken har kontroll på at leverandørene innfrir kravene til sikkerhet besluttet i Bankens sikkerhetspolicy gjennom kontroll av ISAE 3402 rapporten og Lokalbank-samarbeidets jevnlige møter med leverandørene.

Finanstilsynet fastholder at Banken må sikre at tjenesteleverandørene innfrir sikkerhetskravene i Bankens besluttede sikkerhetspolicy og bør etablere egne rutiner for styring og kontroll av systemsikkerhet for utkontraktert IKT-virksomhet. Finanstilsynet mener at Bankens kontrollaktiviteter ikke i tilstrekkelig grad verifiserer leverandørers etterlevelse av Bankens besluttede sikkerhetspolicy. Blant annet viser ISAE 3402-rapporter etterlevelse av leverandørers egen sikkerpolicy og ikke til etterlevelse av den enkelte tjenestekjøpers sikkerhetspolicy.

Tilgangsstyring – utkontraktert IKT-virksomhet

IKT-forskriften § 5 Sikkerhet stiller krav om at Banken skal ha "prosedyrer som skal 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". Ytterligere utdyping finnes i EBAs retningslinjer.

I foreløpig rapport ble det pekt på at dersom en ansatt hos "IKT-tjenesteleverandør" innehar en rolle hvor det er nødvendig å ha tilganger til Bankens IKT-driftsmiljø anser "IKT-tjenesteleverandør" dette som et tjenstlig behov for å kunne utføre arbeidet. Ved et slikt definert tjenstlig behov vil den ansatte bli satt opp med permanente tilganger til Bankens IKT-driftsmiljø uten tidsbegrensning eller andre typer begrensninger for når tilgangene kan benyttes.

Det framgår av styrets svar at ansatte hos "IKT-tjenesteleverandør" ikke har permanente tilganger, men gis tidsbegrenset tilgang til Bankens IKT-driftsmiljø.

Finanstilsynet tar styrets svar til etterretning. Finanstilsynet legger til grunn at svaret gjelder for alle driftsoppgaver, uavhengig av plattform, leverandør eller underleverandør, hvor det skal utføres driftsoppgaver på løsninger som inneholder Bankens kundedata.

Kopi av dette brevet bes sendt til valgt revisor.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Stig Ulstein
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.