FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Høland og Setskog Sparebank
Styret
Postboks 54
1941 BJØRKELANGEN

| VÅR REFERANSE | DERES REFERANSE | | DATO |
|---|---|---|---|
| 21/3377 | | | 03.12.2021 |

## Tilsynsrapport

Finanstilsynet gjennomførte stedlig tilsyn i Høland og Setskog Sparebank (Banken) 21. mai 2021. Tilsynet hadde som formål å vurdere Bankens arbeid innen kontinuitetsledelse, herunder hvordan bankens prosesser for å sikre at forretningskritiske tjenester og prosesser kan operere ved hendelse, som definert i IKT-forskriften.

Til grunn for disse merknadene ligger Finanstilsynets foreløpige tilsynsrapport datert 17. august 2021 og styrets kommentarer til foreløpig tilsynsrapport i brev av 27. september 2021.

Finanstilsynet har følgende merknader etter det stedlige tilsynet:

### Forretningsmessig konsekvensanalyse

Rettslig utgangspunkt:

***IKT-forskriftens § 8. Drift og § 11. Driftsavbrudd og kriseberedskap.***

Finanstilsynet pekte i foreløpig rapport på at Banken hadde vesentlige mangler knyttet til gjennomføring av forretningsmessige konsekvensanalyser, som vurderes som sentralt for å kunne utarbeide en kriseplan.

Finanstilsynet ba Banken iverksette en prosess for gjennomføring av en forretningsmessig konsekvensanalyse for å sikre at banken identifiserer forretningskritiske prosesser og tjenester, samt de systemer som underbygger disse. Både Bankens forretningsområder og IT-organisasjonen ble bedt om å ta del i dette arbeidet.

Finanstilsynet har fra styrets svar merket seg at det er påbegynt en prosess for forretningsmessig konsekvensanalyse. Det bemerkes at Banken etter gjennomført analyse, vil samarbeide med Eika Gruppen for å sikre samsvar mellom Bankens kontinuitetsplan og tilsvarende plan i Eika Gruppen.

Finanstilsynet understreker styrets ansvar for å sikre at Bankens kontinuitetsplan underbygges av en forretningsmessig konsekvensanalyse, prosesser og rutiner som sikrer kontinuerlig vurdering og forbedring av både forretningsmessig konsekvensanalyse og kontinuitets- og kriseplan.

**FINANSTILSYNET**
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00

post@finanstilsynet.no
www.finanstilsynet.no

**Saksbehandler**
Andreas Schei Andersen
Dir. tlf 22 93 98 00

## Utkontraktering og oppfølging av utkontrakterte tjenester

Rettslig utgangspunkt:

***IKT-forskriftens § 12. Utkontraktering.***

Banken opplyste i tilsynsmøtet om at Bankens utkontrakteringer og oppfølging av sentrale underleverandører i all hovedsak skjer gjennom Eika Gruppen av Eika IT.

I foreløpig rapport understrekte Finanstilsynet at Banken er ansvarlig for all IKT-virksomhet, inkludert den virksomhet som er utkontraktert jf. IKT-forskriften § 12. Finanstilsynets vurderinger i foreløpig rapport omfattet to områder relatert til utkontraktering:

1. Styring og kontroll med utkontrakterte tjenester
2. Organisering og håndtering ved hendelser hos leverandør

Finanstilsynet merker seg styrets svar om at de er bevisste på at ansvaret for utkontraktert virksomhet påhviler Banken.

### *1. Styring og kontroll med utkontrakterte tjenester*

I foreløpig tilsynsrapport påpekte Finanstilsynet at Banken ikke i tilstrekkelig grad følger opp sine underleverandører, men at dette ivaretas av Eika Gruppen, på vegne av Banken. Finanstilsynet vurderer styring og kontroll med utkontrakterte tjenester sentralt for at Banken kan sikre ivaretakelse av kontinuitet i systemer som underbygger forretningskritiske prosesser og funksjoner.

Finanstilsynet har merket seg fra styrets svar at styret vil påse at det etableres en prosess som sikrer at Banken har tilstrekkelige kontrollmekanismer for styring og kontroll med utkontrakterte tjenester, samt at denne vil harmoniseres og tilpasses kontrollmekanismer og kompetanse hos Eika Gruppen. Av svaret fremgår det videre at Eika Gruppen vil samle ytterligere informasjon for styring og kontroll med utkontrakterte tjenester på bankgrupperingens ekstranett, samt vurderinger om det skal fremlegges en erklæring på leverandøroppfølging til bankene.

### *2. Organisering og håndtering ved hendelser hos leverandør*

I foreløpig tilsynsrapport vurderte Finanstilsynet at Bankens organisering og rutiner, herunder planverk, for håndtering av hendelser kun var dekkende for hendelser som ville være lokale. IKT-hendelser inngikk ikke i Bankens kriseplan og Banken var her avhengig av Eika Gruppen mht. organisering, håndtering og oppfølging av hendelser som rammet bankens IKT-systemer. Iverksettelse av bankens kriseplan ble således gjort på bakgrunn av vurderinger gjort av Eika Gruppen, basert på kriterier som Banken selv ikke var kjent med.

Finanstilsynet understrekte i foreløpig tilsynsrapport at Banken bør sikre at relevante kriterier og vurderinger ligger til grunn for iverksettelse av kriseplan og at dette bør bero på Bankens vurderinger vedrørende forretningskritiske funksjoner/prosesser. Det ble videre pekt på at dette arbeidet bør formidles til Eika Gruppen, slik at dette hensyntas ved eskalering av hendelser og etablering av kriseledelse.

I styrets svar fremgår det at Eika Gruppen har lagt sin forretningsmessige kontinuitetsplan til grunn for rutiner knyttet til organisering og håndtering av hendelser hos leverandør. Videre fremgår det at planen er delt med Banken for å sikre at Banken er kjent med kriteriene som ligger til grunn for iverksettelse av kriseplanen. Banken vil i det videre arbeidet med utarbeidelse av

forretningskontinuitetsplan inkludere kriterier for eskalering og etablering av kriseledelse og iverksettelse av kriseplan.

Finanstilsynet understreker viktigheten av at Bankens vurderinger deles med Eika Gruppen, for å sikre at Bankens forretningsmessige behov ivaretas.

## Testing av kriseløsning

Rettslig utgangspunkt:

***IKT-forskriftens § 11. Driftsavbrudd og kriseberedskap.***

Finanstilsynet pekte i foreløpig rapport på at Banken i liten grad aktivt var involvert i test av kriseløsninger hos Bankens leverandører, men at dette arbeidet ble gjort av Eika Gruppen. Finanstilsynet påpekte i foreløpig rapport viktigheten av at banken selv har innsikt i og bidrar inn i prosessen vedrørende testing av kriseløsninger. Banken ble bedt om å ta en mer aktiv rolle knyttet til testing av kriseløsningene for systemer som inngår i bankens forretningskritiske prosesser og funksjoner.

Det fremgår av styrets svar at Banken i sin forretningsmessige kontinuitetsplan vil presisere behovet for kompetanse og innsikt for å kunne planlegge og gjennomføre krisetester i samarbeid med sine underleverandører.

Finanstilsynet bemerker seg også at Eika Gruppen påpeker at bankene i større grad enn tidligere aktivt vil involveres i krisetester relatert til forretningskritiske tjenester felles for bankgrupperingen, hvor dette er formålstjenlig.

Kopi av dette brevet bes sendt til Bankens valgte revisor.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Andreas Schei Andersen
førstekonsulent

*Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.*