FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

OBOS-BANKEN AS
Postboks 6666 st olavs plass
0129 OSLO

VÅR REFERANSE	DERES REFERANSE		DATO
22/5351			09.12.2022

Tilsynsrapport

Finanstilsynet gjennomførte stedlig tilsyn i OBOS-banken AS (banken) 14. og 15. juni 2022. Tilsynet hadde som formål å gjøre en vurdering av bankens arbeid med kontinuitets- og kriseledelse, oppfølging av tilgangsrettigheter til bankens IT-systemer og arbeid med datakvalitet.

Til grunn for disse merknadene ligger Finanstilsynets foreløpige tilsynsrapport datert 2. september 2022 og styrets kommentarer til foreløpig tilsynsrapport i brev av 12. oktober 2022.

Finanstilsynet har følgende merknader etter det stedlige tilsynet:

1. Styrende dokumenter

IKT-forskriften § 2 Planlegging og organisering stiller krav til at banken skal fastsette overordnede mål, strategier og sikkerhetskrav for IT-virksomheten.

Finanstilsynet viste i foreløpig rapport til at banken er i prosess med å implementere OBOS-konsernets styrende dokumenter. Finanstilsynet understreket derfor viktigheten av at styrende dokumenter i banken må hensynta regelverket som banken er underlagt.

Finanstilsynet har merket seg fra styrets svar at banken ved tilslutning til konsernets styrende dokumenter innenfor informasjonssikkerhet og beredskap vil påse at disse sikrer etterlevelse av regulatoriske krav som banken er underlagt.

Finanstilsynet tar styrets svar til etterretning.

2. Kontroll med tilganger gitt tjenesteleverandører

IKT-forskriften § 5 Sikkerhet stiller krav til at prosedyrer inneholder retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene. Av IKT-forskriften § 12 Utkontraktering framgår det at foretaket ved utkontraktering av hele eller deler av IKT-virksomheten har ansvar for at IKT-virksomheten oppfyller alle krav som stilles etter denne forskrift.

Finanstilsynets pekte i foreløpig rapport på at etablert rutine for tilgangsstyring og oppfølging hos leverandør ikke er tilstrekkelig, da det gir muligheter for å misbruke tilganger til ikke-tjenstlige oppslag som vanskelig lar seg avdekke. Finanstilsynet stilte også spørsmål ved banken sin styring og kontroll med tilgangsrettinger ved utkontraktert virksomhet og om denne har vært tilstrekkelig.

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

Finanstilsynet har merket seg fra styrets svar at det er iverksatt tiltak for å sikre bedre kontroll med sine leverandørers tilgangsrettigheter, samt til å innta bestemmelser i hovedavtaler når disse skal fornyes.

Finanstilsynet legger til grunn at banken, bl.a. gjennom krav i avtaler og kontrollaktiviteter, iverksetter tiltak for sikre bedre kontroll med leverandørers tilganger til IKT-systemene, og tar styrets svar til etterretning.

Finanstilsynet understreker bankens ansvar for styring og kontroll med tilgangsrettigheter, også ved utkontraktering. Ved utkontraktering må banken stille nødvendige krav til oppdragstaker for å sikre at banken ivaretar styring og kontroll med tilgangsrettigheter på en forsvarlig måte, herunder sikre at oppdragstaker har etablert nødvendige rutiner og prosesser for slik styring og kontroll.

3. Rammeverk for datakvalitet

IKT-forskriften § 4 Kvalitet stiller krav til at det fastsettes kvalitetsmål for de enkelte deler av IKT-virksomheten knyttet opp mot bankens øvrige mål. Banken skal videre ha dokumenterte prosedyrer for oppfølging av fastsatte kvalitetsmål.

Finanstilsynet ble under tilsynet informert om at banken ikke har et overordnet rammeverk for arbeid med datakvalitet, men at dette inngår som initiativ med utgangspunkt i generelt arbeid med IKT. I foreløpig rapport pekte Finanstilsynet på at risikoen for feil som følge av dårlig datakvalitet potensielt kan ha store konsekvenser, og at bankens strategiske satsning med mål om økt bruk av automatisering forutsetter god datakvalitet. Finanstilsynet vurderte derfor i foreløpig rapport at banken burde etablere et overgripende rammeverk for styring og kontroll med data.

Finanstilsynet har fra styrets svar merket seg at etablering av et overgripende rammeverk og rutiner for styring og kontroll med data vil skje i takt med bankens utvikling av tjenester og prosesser som innebærer økt automatisering og digitalisering.

Finanstilsynet vurderer at god styring og kontroll med data er en forutsetning for automatisering og effektivisering av forretningsprosesser. Finanstilsynet understreker styrets ansvar for å sikre at bankens data er pålitelige, konsistente og at de ikke blir misbrukt.

4. Forretningsmessig konsekvensanalyse

IKT-forskriften § 11 stiller krav til at banken har etablert en kriseplan som skal kunne iverksettes dersom IKT-driften ikke kan opprettholdes med tilgjengelige ressurser. Av den europeiske banktilsynsmyndighetens (EBA) "Guidelines on ICT and Security Risk Management" punkt 3.7.1. framgår det at banken i sitt kontinuitetsarbeid bør gjennomføre en forretningsmessig konsekvensanalyse.

Finanstilsynet pekte i foreløpig rapport på at banken ikke hadde gjennomført analyser tilsvarende en forretningsmessig konsekvensanalyse, men at det var gjort en vurdering og kartlegging av sentrale IT-systemer, komponenter og funksjoner. Det var videre Finanstilsynets forståelse at arbeidet ble ledet av bankens IT-avdeling. Finanstilsynet pekte på at banken burde gjennomføre en forretningsmessig konsekvensanalyse med utgangspunkt i forretningsområdene behov og at analysen bør vise hvordan bortfall av forretningstjenester kan innvirke på bankens forretningsdrift.

Finanstilsynet merker seg fra styrets svar at banken vil intensivere sitt arbeid med å kartlegge og dokumentere kritiske forretningsprosesser, inkludert underliggende systemer. Av styrets svar

framgår det videre at den forretningsmessige konsekvensanalysen vil gjennomgås jevnlig av ledelsen, og oppdateres minst årlig. Banken vil benytte dette som grunnlag i sitt arbeid med kravsetting til beredskaps- og kontinuitetsplaner både internt og ved utkontraktering.

Finanstilsynet understreker styrets ansvar for å sikre at forretningsmessige konsekvensanalyser utarbeides med utgangspunkt i forretningsområdenes behov. Finanstilsynet legger til grunn at forretningsområdene gjøres ansvarlige for forretningsmessige konsekvensanalyser.

5. Testaktiviteter

IKT-forskriften § 11 stiller krav til at banken gjennomfører opplæring, øvelse og testing av kriseløsninger. EBAs "Guidelines on ICT and Security Risk Management" kapittel 3.7 utdyper nærmere krav til testing av kriseplanen.

Finanstilsynet pekte i foreløpig rapport på at banken i liten grad er involvert i planlegging av tester av kriseløsninger gjennomført av bankens leverandør. Det ble videre pekt på at banken burde være aktiv å stille krav i utvelgelsen av hva som skal testes, og at testen skal ta utgangspunkt i IT-systemer, komponenter og funksjoner som understøtter bankens forretningskritiske tjenester, identifisert i bankens forretningsmessige konsekvensanalyse. Finanstilsynet understreket i foreløpig rapport at det ikke er noen garanti for at tester initiert av bankens leverandører omfatter de IT-systemer, komponenter og funksjoner som understøtter kritiske forretningstjenester for banken.

Av styrets svar framgår det at banken gjennomfører årlige testaktiviteter og at resultatet av øvelsen meddeles leverandører hvor det vurderes relevant. Finanstilsynet merker seg videre av styrets svar at styret er enig i Finanstilsynets påpekning og at banken vil følge opp sine leverandører tettere og stille krav til testaktiviteter. Det framgår videre at banken vil påse at krav til involvering ved planlegging av tester og beredskapsarbeid skal inntas i bankens avtaler med sine leverandører. Banken vil i samband med dette også oppdatere sine rutiner.

Finanstilsynet tar styrets svar til etterretning.

Finanstilsynet ber om at kopi av dette brevet sendes til bankens valgte revisor.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Andreas Schei Andersen
førstekonsulent

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.