FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

SPAREBANKEN MØRE
Ved styret
Postboks 121
6001 ÅLESUND

VÅR REFERANSE	DERES REFERANSE		DATO
24/2319			03.09.2024

Tilsynsrapport

Finanstilsynet gjennomførte stedlig IKT-tilsyn i Sparebanken Møre (banken) 11. og 12. april 2024. Hensikten med tilsynet var 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 for utkontrakterte IKT-tjenester, samt overholdelse av regulatoriske krav på IKT-området.

Til grunn for tilsynsrapporten ligger Finanstilsynets foreløpige rapport datert 15. mai 2024 og styrets kommentarer til rapporten i brev av 19. juni 2024.

Finanstilsynet har følgende merknader etter det stedlige tilsynet:

1. Organisering

Finansforetaksloven § 13-5 stiller krav til forsvarlig virksomhet og god forretningsskikk. Banken skal ha klare og hensiktsmessige styrings- og kontrollsystemer samt hensiktsmessige retningslinjer og rutiner for å styre, overvåke, og rapportere risiko foretaket er eller kan bli eksponert for, jf. finansforetaksloven § 13-5 første ledd.

Det er bankens første forsvarslinje som står som eier av styregodkjente styrende dokumenter på IKT-området som strategier og policyer. Finanstilsynet pekte i foreløpig rapport på at det forventer at overordnede styringsdokumenter følges opp for å sikre at bankens drift og planer utføres i henhold til disse, og at bankens andre og tredje forsvarslinje følger opp etterlevelsen av og kontrollerer at de styrende dokumentene er operasjonalisert i samsvar med styrets beslutninger.

Styret bekrefter i sitt svarbrev at slike kontroller fra andre- og tredjelinjen er operasjonalisert i henhold til vedtatte strategier og retningslinjer.

Finanstilsynet tar styrets svar til orientering.

2. Overordnet risikostyring

CRR/CRD-forskriften § 35 stiller krav om at styret skal godkjenne og regelmessig vurdere retningslinjer for å påta foretaket risikoer og for å identifisere, styre, overvåke og kontrollere

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

risikoene. IKT-forskriften § 2 første ledd stiller krav til at foretaket skal fastsette overordnede mål, strategier, og sikkerhetskrav for IKT-virksomheten. Av IKT-forskriften § 3 første ledd skal det fastsettes grenser for akseptabel risiko forbundet med bruk av IKT-systemene og etter § 3 annet ledd skal det minst en gang årlig, eller ved endringer som har betydning for IKT-sikkerheten, gjennomføres risikoanalyser. Resultatet av risikoanalysen skal dokumenteres.

I foreløpige rapport var det Finanstilsynets vurdering at det ikke i tilstrekkelig grad gjennomføres egne kontroller eller revisjonsgjennomganger av bankens utkontrakterte IKT-virksomhet for å kunne vurdere etterlevelse av foretakets overordnede målsetting om å ha effektiv styring og overvåkning av operasjonell risiko.

Styret ga i sitt svarbrev en gjennomgang av førstelinjens rutine for oppfølging av leverandører. Videre opplyser styret om at de skal påse at andrelinjens kontroller utvides til å dekke selvstendig vurderinger av IKT-tjenesteleverandører.

Finanstilsynet tar styrets svar til orientering.

Finanstilsynet ble under tilsynet informert om at banken har etablert en styringsgruppe for operasjonell risiko og at denne er bemannet med medlemmer fra både første og andre forsvarslinje. Siden styringsgruppen er sammensatt av både første og andre forsvarslinje stilte Finanstilsynet spørsmål om det er utarbeidet et mandat for styringsgruppen som blant annet sikrer uavhengigheten til kontrollfunksjonene i bankens andre forsvarslinje.

Styret viser i sitt svarbrev til rutiner hvor mandatet til styringsgruppen er beskrevet og skriver videre at nødvendig presiseringer i mandatet skal oppdateres.

Finanstilsynet tar styrets svar til orientering.

3. Rapportering av IKT-risiko

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.

Banken hadde på tidspunktet for tilsynet enkelte risikoer som lå utenfor bankens aksepterte risikotoleranse innen operasjonell risiko. Finanstilsynet pekte i foreløpig rapport på viktigheten av at risikoer utenfor bankens definerte risikotoleranse følges opp særskilt.

Styret skriver i sitt svarbrev at de tar Finanstilsynets bemerkning til etterretning.

Finanstilsynet tar styrets svar til orientering.

I foreløpig rapport vurderte Finanstilsynet videre det som viktig at banken ved mottak av uavhengige revisjonserklæringer, som ISAE-rapporter, gjennomfører egne kontroller som skal sikre at innholdet i rapportene er relevant og gjeldende for banken.

Styret gir i sitt svarbrev en gjennomgang av hvordan ISAE-rapporter behandles og følges opp. Styret skriver videre at ISAE 3402 og/eller ISAE 3000 er nyttig supplement og bidrag til de øvrige kontroller og oppfølgingen som gjøres.

Finanstilsynet tar styrets svar til orientering og legger til grunn at ISAE-rapportene gjennomgås for å sikre at innholdet i rapporten er relevant og gjeldende for banken.

4. Virksomhetsmessig konsekvensanalyse

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. Planene skal basere seg på foretakets prioriteringer for gjenoppretting av forretningskritiske tjenester og prosesser. Prioriteringene for gjenoppretning 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.

Finanstilsynet pekte i foreløpig rapport på at det forventes at banken utarbeider virksomhetsmessige konsekvensanalyser ledet av forretningssiden, der resultatet av analysen gir oversikt over bankens systemportefølje og der kritikaliteten systemene har for bankens virksomhet er angitt. Det legges til grunn at rutine for utarbeidelse av virksomhetsmessig konsekvensanalyse etableres og inngår i foretakets ordinære drift.

Styret skriver i sitt svarbrev at bankens prosjekt for virksomhetsmessig konsekvensanalyse er gjennomført i henhold til fastsatt plan. Videre opplyser styret at rutine for vedlikehold av virksomhetsmessig konsekvensanalyse vil bli etablert og inngå i ordinær drift, og at resultatet av analysen vil bli formidlet til IKT-tjenesteleverandører der det er relevant.

Finanstilsynet tar styrets svar til orientering.

5. Kriseberedskap

I IKT-forskriftens § 11 framgår kravene til 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, med dokumentasjon av testresultater, som viser at kriseløsningen virker som forutsatt.

I foreløpig rapport vurderte Finanstilsynets at bankens etterlevelse av IKT-forskriftens § 11 ikke var tilstrekkelig ivaretatt da bankens testing av krisescenarioer er mangelfull, siden tester ikke har bakgrunn i en dokumentert konsekvensanalyse.

I sitt svarbrev skriver styret at de etter deres oppfatning etterlever IKT-forskriften §11. Styret viser i den sammenheng til bankens interne retningslinjer og rutiner både for kontinuitet og sikkerhet. Videre viser styret til særskilte krav til leverandørers kontinuitets- og katastrofeløsninger i utkontrakteringsavtaler.

Finanstilsynet opprettholder sin vurdering om at bankens testing er mangelfull og ber banken om at beredskapstester gjennomføres med utgangspunkt i dokumentert konsekvensanalyse og inneholder relevante scenarier som for eksempel løsepengevirus.

6. Utkontraktering

I henhold til IKT-forskriften § 2 skal banken ha retningslinjer for å sikre at utkontraktert IKT-virksomhet oppfyller kravene i § 12. Dette gjelder blant annet krav til skriftlig avtale, der avtalen skal sikre foretakets rett til å kontrollere/revidere leverandørens aktiviteter, samt Finanstilsynets tilgang til opplysninger og mulighet for å føre tilsyn hos IKT-leverandøren. Videre framgår det av samme paragraf at "*avtaler om utkontraktering av IKT-virksomhet og endring av slike avtaler skal behandles av styret. Styret skal presenteres en plan for utkontrakteringen, en risikovurdering av utkontrakteringsforholdet og en beskrivelse av hvordan foretaket skal sikre leveransene"*.

I foreløpig rapport kommenterte Finanstilsynet på at bankens sikkerhetspolicy ikke benyttes som utgangspunkt for krav som stilles til leverandører og underleverandører, og pekte på viktigheten av at banken sikrer at krav, blant annet fra sikkerhetspolicyen for den interne organisasjonen, også gjøres gjeldende for disse. Videre presiserte Finanstilsynet viktigheten av at banken må være trygg på at alle leverandører og underleverandører presenterer nødvendig informasjon for å gjennomføre oppfølging av utkontrakterte tjenester.

Styrets opplyser i sitt svarbrev at banken er av den oppfatning at de får nødvendig informasjon for å kunne følge opp og kontrollere den utkontrakterte IKT-virksomheten på en forsvarlig måte for viktige og kritiske IKT-leverandører. Videre opplyser styret at banken vil fortsette med å stille krav til leverandører på dette området og sikre nødvendige kontroller for å sikre etterlevelse av bankens krav til informasjonssikkerhet.

Finanstilsynet tar styrets svar til orientering og legger til grunn at bankens krav til informasjonssikkerhet skal være tema i faste oppfølgingsmøter med IKT-leverandører i henhold til bankens rutine for leverandøroppfølging.

7. IKT-sikkerhet

IKT-forskriften § 5 stiller krav om at foretaket skal ha prosedyrer for å sikre beskyttelse av utstyr, systemer og informasjon av betydning for foretakets virksomhet, mot skader, misbruk, uautorisert adgang og endring, samt hærverk. Foretaket har ansvar for risikostyring og internkontroll også der hele eller deler av virksomheten er utkontraktert, jf. IKT-forskriften § 12. Det framgår av bestemmelsen at foretaket må sikre at leverandørens aktiviteter kontrolleres. Videre skal det finnes retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene.

IKT-forskriften § 13 stiller krav til at det er etablert en "oppdatert oversikt over organisasjon, utstyr, IKT-systemer og vesentlige forhold i IKT-virksomheten". Finanstilsynets vurdering er at dette omfatter oppdaterte oversikter over IT-systemer, nettverksenheter, databaser etc. og at utstyrsoversikten bør inneholde tilstrekkelige konfigurasjonsdata og angi avhengigheter mellom utstyr/komponenter.

I foreløpig rapport pekte Finanstilsynet på at banken bør ha en detaljert oversikt over alle komponenter som inngår i infrastrukturen, herunder maskinvare og programvare, da dette vurderes som vesentlig for sikkerhetsstyringen. Videre understrekte Finanstilsynet at det er bankens ansvar å sikre at alle IKT-tjenesteleverandører som banken har utkontrakterte IKT-tjenester til, har etablert gode rutiner og kontroller for konfigurasjonsstyring av de tjenester som inngår i leveransene til banken.

Styret opplyser i sitt svarbrev at styret er av den oppfatning at kravene i IKT-forskriften § 13 er ivaretatt. Videre opplyser styret at det er avtalefestet med IKT-tjenesteleverandørene at deres CMDB (konfigurasjonsdatabase) til enhver tid skal være oppdatert.

Finanstilsynet tar styrets svar til orientering og legger til grunn at de avtalefestede kravene til CMDB blir fulgt opp og kontrollert.

I foreløpig rapport ba Finanstilsynet banken om å vurdere risikoen ved å bruke "single sign-on"-løsning uten to-faktor autentisering opp mot bankens produksjonssystemer.

Styrets opplyser i sitt svarbrev at banken har en pågående dialog med leverandøren av fagsystemene om å finne alternative løsninger og sikkerhetsmekanismer som reduserer risiko ved bruk av "single sign-on".

Finanstilsynet tar styrets svar til orientering.

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.