FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Fana Sparebank
Postboks 10 Nesttun
5852 BERGEN

VÅR REFERANSE	DERES REFERANSE		DATO
23/9322			26.04.2024

Tilsynsrapport

Finanstilsynet gjennomførte stedlig IKT-tilsyn i Fana Sparebank (Fana) 25. og 26. oktober 2023. Hensikten med tilsynet var å gjøre en vurdering av hvordan foretaket 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 foretakets beredskapsarbeid relevant for IKT-området, herunder vurdere beredskapen i foretaket og for utkontrakterte IKT-tjenester, samt overholdelse av regulatoriske krav på IKT-området.

Til grunn for tilsynsrapporten ligger Finanstilsynets foreløpige rapport datert 12. februar 2024 og styrets kommentarer til rapporten i brev av 12. april 2024.

Finanstilsynet har følgende merknader etter det stedlige tilsynet:

1. Overordnet styring og kontroll

1.1. Organisering

Det framgår av finansforetaksloven § 8-6 første ledd at styret skal sørge for forsvarlig organisering av virksomheten. Videre stilles det krav til at finansforetak skal ha uavhengige kontrollfunksjoner med ansvar for risikostyring, etterlevelse og internrevisjon, jf. § 13-5 andre ledd. CRR/CRD IV-forskriften stiller krav i § 38 om at foretaket skal ha en uavhengig risikokontrollfunksjon med tilstrekkelig kompetanse og ressurser, og at risikokontrollfunksjonen skal sikre at alle vesentlige risikoer i foretaket er identifisert, målt og rapportert av de relevante organisatoriske enhetene. Forskriften stiller videre krav i § 39 til at foretaket skal ha en uavhengig kontrollfunksjon for kontroll av etterlevelse, samt ha retningslinjer og prosedyrer for å avdekke risiko for at foretaket ikke oppfyller sine forpliktelser etter lov og forskrift. I § 40 stiller forskriften krav om internrevisjon.

Det er Finanstilsynets vurdering at for å ha god styring og kontroll på IKT-virksomheten, også den som er utkontraktert, bør foretaket gjennomføre egne kontroller både når det gjelder risiko og etterlevelse. Finanstilsynet mener videre at det er viktig med tilstrekkelig IKT-kompetanse og nok ressurser i de tre forsvarslinjene for å følge opp egen og utkontraktert IKT-virksomhet.

Finanstilsynet pekte i foreløpig rapport på at foretakets oppfølging av IKT-risiko i de tre forsvarslinjene er mangelfull og ikke i samsvar med regelverket, jf. finansforetaksloven § 13-5 annet ledd og CRR/CRD IV-forskriften § 39. Finanstilsynet pekte videre på hvordan foretaket sikrer

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

at foretaket har tilstrekkelig ressurser og kompetanse på IKT-området for å utføre den nødvendige oppfølgingen, både i første og andre linje, og minnet om styrets ansvar for å sørge for en forsvarlig organisering av virksomheten, jf. finansforetaksloven § 8-6.

Det kom fram i styrets svar at sett på bakgrunn av igangsatte tiltak, gjennomførte aktiviteter og en nå fulltallig organisasjon, er styret av den oppfatning at banken er rigget til å kunne sikre oppfyllelse av regelverket mht. de tre forsvarslinjer, jf. finansforetaksloven § 13-5 annet ledd og CRR/CRD IV-forskriften § 39. Videre skriver styret at deres vurdering er at bankens organisasjon har riktig kompetanse på IKT-området til å utføre nødvendig oppfølging i tråd med IKT-forskriften.

Finanstilsynet tar styrets svar til etterretning og legger til grunn de planlagte tiltak, gjennomførte aktiviteter samt styrets oppfølging av disse.

Finanstilsynets pekte i den foreløpige rapporten på at det ut ifra det som sto om ansvar og eierskap i policy for informasjonssikkerhet kunne være uklart hvem som hadde det formelle ansvaret for informasjonssikkerhetsområdet.

Styret skrev i sitt svar at policy for informasjonssikkerhet vil oppdateres og at ansvaret tydeliggjøres.

Finanstilsynet tar styrets svar til orientering.

Finanstilsynet pekte i foreløpig rapport på at dersom informasjonssikkerhetsansvarlig er organisert i foretakets førstelinje, vil det medføre at informasjonssikkerhetsansvarlig ikke har en uavhengig rolle i forhold til foretakets førstelinje. Dette medfører at foretaket må sikre at andrelinjen bemannes med ressurser og kompetanse som kan kontrollere og se til at foretakets IKT-sikkerhetspolicy er operasjonalisert i foretaket, og at de samme kravene også gjelder for IKT-tjenesteleverandører og underleverandører.

Styret skriver i sitt svar at de vil påse at bankens andrelinje bemannes med ressurser og kompetanse som kan kontrollere og se til at banken policy for informasjonssikkerhet er operasjonalisert i foretaket, og at de samme kravene også gjelder for IKT- tjenesteleverandører og underleverandører.

Finanstilsynet tar styrets svar til orientering.

I foreløpig rapport pekte Finanstilsynet på at foretakets tre forsvarslinjer må ha tilgang til relevant informasjon, og at kontrollfunksjonenes uavhengighet må ivaretas, også for utkontraktert virksomhet. Det vises til kravene til andrelinjen i CRR/CRD IV-forskriften § 38 annet ledd.

Styret skriver i sitt svar at utveksling av kontrollinformasjon mellom banken og tjenesteleverandør er ivaretatt og at operasjonalisering av sikkerhetskrav og oppfølging av disse er noe som vil bli prioritert og fulgt opp i alle forsvarslinjer.

Finanstilsynet tar styrets svar til orientering.

1.2. Overordnet risikostyring

CRR/CRD IV-forskriften § 35 stiller krav om at styret skal godkjenne og regelmessig vurdere retningslinjer for risikoer foretaket påtar seg og for å identifisere, styre, overvåke og kontrollere risikoene. IKT-forskriften § 2 første ledd stiller videre krav til at foretaket skal fastsette overordnede mål, strategier og sikkerhetskrav for IKT-virksomheten.

Finansforetaksloven § 13-5 stiller krav til forsvarlig virksomhet og god forretningsskikk. Foretaket 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.

Finanstilsynet pekte i foreløpig rapport på at det forventes at styregodkjente styringsdokumenter som strategier og policyer følges opp for å sikre at foretakets drift og planer utføres i henhold til disse. Videre skrev Finanstilsynet at det også forventes at foretakets andrelinje og tredjelinje, som følger opp etterlevelsen av strategien, kontrollerer at de styrende dokumentene er operasjonalisert i henhold til strategien.

Styret skriver i sitt svar at det for styregodkjente styringsdokumenter som strategier og policyer i tydeligere grad vil tillegges kontrolloppgaver for 1. og 2. linje, samt at det i dialog med internrevisor skal sikres at kontroller for operasjonalisering av strategier blir hensyntatt i revisjonsplanene.

Finanstilsynet tar styrets svar til orientering.

1.3. Forretningsmessig konsekvensanalyse

Foretaket har ansvar for at nødvendig forretningsmessig kontinuitet og beredskap er sikret, jf. IKT-forskriften § 11. EBAs retningslinjer for IKT og sikkerhet[1] gir en utdyping av IKT-forskriftens bestemmelse for hvordan foretaket skal sikre forretningsmessig kontinuitet basert på forretnings-messig konsekvensanalyser (BIA[2]).

Hensiktsmessige planer og tiltak for tilgjengelighet og kontinuitet bør etableres med utgangspunkt i forretningsmessige konsekvensanalyser for foretakets kritiske forretningsprosesser. Konsekvensanalysen 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 gjenoppretting 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. For å verifisere at det er etablert fungerende planer og løsninger må foretaket gjennomføre regelmessig opplæring, øvelse og testing, jf. IKT-forskriften § 11.

Finanstilsynet pekte i foreløpig rapport på at det er Finanstilsynet vurdering at foretaket har mangler i sin etterlevelse av kravene i IKT-forskriften § 11 samt EBAs retningslinjer for IKT og sikkerhet kapittel 3.7.1 vedrørende driftsavbrudd og kriseberedskap, da foretaket ikke har gjennomført en helhetlig forretningsmessig konsekvensanalyse. Finanstilsynet forventer at foretaket utarbeider forretningsmessige konsekvensanalyser ledet av forretningssiden, der resultatet av konsekvens-analysen blant annet vil gi oversikt over foretakets systemportefølje og angi kritikaliteten systemene

[1] EBA/GL/2019/04: EBA Guidelines on ICT and security risk management.
[2] BIA – Business Impact Analysis

har for foretakets virksomhet. Det legges til grunn at en rutine for utarbeidelse av forretningsmessige konsekvensanalyser etableres og inngår i foretakets ordinære drift.

Styret skriver i sitt svar at aktiviteter med å etablere en forretningsmessig konsekvensanalyse var planlagt på tilsynstidspunktet og at arbeidet med å sluttføre denne og sikre etterlevelse av IKT-forskriftens § 11 samt EBAs retningslinje for IKT-sikkerhet og risiko vil følges opp.

Finanstilsynet tar styrets svar til orientering.

2. Styring med og kontroll av IKT

2.1. Kriseberedskap

I IKT-forskriftens § 11 framgår krav 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 at kriseløsningen virker som forutsatt. EBAs retningslinjer for IKT og sikkerhet gir også anbefalinger om utarbeidelse av kontinuitetsplaner, respons- og gjenopprettingsplaner, testing og kommunikasjonsplaner ved kriser.

Finanstilsynet pekte i foreløpig rapport på at det er foretaket selv som er ansvarlig for at opplæring, øvelse og testing av foretakets kriseløsning gjennomføres årlig. Når den forretningsmessige 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.

Styret skriver i sitt svar at banken har, som nevnt tidligere, iverksatt tiltak for å gjennomføre en forretningsmessig konsekvensanalyse. Videre vil foretakets beredskap og kriseplaner oppdateres og kommuniseres til relevante leverandører, og beredskapstester vil gjennomføres basert på resultatene fra den forretningsmessige konsekvensanalyse.

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.