FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Styret i Nidaros Sparebank
Postboks 300
7541 KLÆBU

VÅR REFERANSE	DERES REFERANSE		DATO
23/3394			08.12.2023

Tilsynsrapport etter stedlig IKT-tilsyn

Finanstilsynet gjennomførte stedlig tilsyn i Nidaros Sparebank 4. og 5. mai 2023. Tilsynet hadde som formål å gjøre en vurdering av hvordan foretaket administrerer, utvikler, drifter, vedlikeholder og sikrer IKT-systemer og -tjenester. For dette området ble tilsynet 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 at regulatoriske krav på dette området overholdes.

Til grunn for disse merknadene ligger Finanstilsynets foreløpige rapport datert 4. september 2023 og styrets kommentarer til rapporten i brev av 20. oktober 2023.

Finanstilsynet har følgende merknader etter det stedlige tilsynet:

Overordnet styring og kontroll

Organisering og ansvarsforhold

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 et finansforetak skal ha uavhengige kontrollfunksjoner med ansvar for risikostyring, etterlevelse og internrevisjon. CRR/CRD IV-forskriften stiller krav i § 38 om at foretaket skal ha en uavhengig risikokontroll-funksjon 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 i § 39 krav om at banken skal ha retningslinjer og prosedyrer for å avdekke risiko for at foretaket ikke oppfyller sine forpliktelser etter lov og forskrift. Foretaket skal ha en uavhengig kontrollfunksjon for etterlevelse med tilstrekkelig kompetanse og ressurser, som blant annet skal kontrollere at foretaket oppfyller sine forpliktelser etter paragrafens første ledd.

I foreløpig rapport pekte Finanstilsynet på at det stedlige tilsynet etterlot et inntrykk av at risikokontrollfunksjonen ikke er involvert i vurderinger av IKT-risiko, noe som Finanstilsynet vurderer å ikke være i samsvar med CRR/CRD IV-forskriften § 38. Videre pekte Finanstilsynet på at foretaket på tidspunktet for tilsynsbesøket og i nesten trekvart år ikke hadde hatt en uavhengig funksjon for kontroll av etterlevelse, og følgelig ingen kontroll av foretakets etterlevelse av IKT-regelverket i perioden. Foretakets manglende kontroll av etterlevelse, både generelt og av IKT-regelverket, er i strid med CRR/CRD IV-forskriften § 39. Etter Finanstilsynets vurdering var

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00

post@finanstilsynet.no
www.finanstilsynet.no

Saksbehandler
Irene Støback Johansen
Dir. tlf. 22 93 96 44

foretakets oppfølging av IKT-risiko i andre forsvarslinje mangelfull og ikke i samsvar med regelverket.

Finanstilsynet stilte videre spørsmål ved hvordan foretaket sikret at foretaket har tilstrekkelig ressurser og kompetanse på IKT-området i første linje, blant annet som følge av at foretakets IKT-ressurs var begrenset til IT-ansvarlige som var 50 prosent utleid til allianseselskapet LB Selskapet AS.

Styret skriver i sitt svarbrev at styret har besluttet å ansette en ny medarbeider med ansvar for kontroll av etterlevelse (compliance) som vil tiltre 1. januar 2024. Fram til dette tidspunktet har foretaket leid inn ekstra eksterne ressurser innen etterlevelse samt utvidet ansvarsområdet til risikokontrollfunksjon til også å omfatte kontroll av etterlevelse. Det ble presisert at foretakets risikokontrollfunksjon nå følger opp operasjonell risiko inkludert IKT-risiko månedlig, blant annet med kvartalsvis rapportering til styret i henhold til nye "KPI-er" innen IKT-området.

Det framgår videre av styrets svarbrev at foretaket har utvidet IKT-området med en IKT-rådgiver fra 1. juli 2023. Styret er av den oppfatning at IKT-området i foretaket etter iverksatte tiltak har tilstrekkelig med ressurser og vil oppfylle kravene til organisering og overholdelse av regelverket.

Finanstilsynet anser regelverksbrudd som alvorlig. Finanstilsynet merker seg styrets kommentarer. Finanstilsynet forutsetter at styret framover er bevisst sitt ansvar for forsvarlig organisering av virksomheten, både i første og andre forsvarslinje.

Overordnet risikostyring

CRR/CRD IV-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 risikoene. IKT-forskriften § 2 første ledd stiller videre krav til at foretaket skal fastsette overordnede mål, strategier, og sikkerhetskrav for IKT-virksomheten.

Foretakets overordnede styringsdokumentasjon på IKT-området er basert på maler fra allianseselskapet LB Selskapet AS. Foretaket har i varierende grad tilpasset styringsdokumentasjonen til foretaket. Styringsdokumentet for IKT-virksomheten i foretaket er etter Finanstilsynets vurdering overordnet og gir i begrenset grad konkrete mål, strategier og sikkerhetskrav for IKT-virksomheten. I foreløpig rapport presiserte Finanstilsynet at det forventer at styret godkjenner og regelmessig vurdere alle styringsdokumenter som er av vesentlig betydning for IKT-virksomheten i foretaket i samsvar med regelverket.

Av styrets svarbrev merker Finanstilsynet seg at tilsynets kommentarer vil tas til etterretning i kommende revideringer av foretakets styringsdokumentasjon på IKT-området.

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 IV-forskriften § 35. Der presiseres det blant annet at styret skal sikre seg tilgang til risikoinformasjon og fastsette omfang, format og frekvens på rapporteringen.

Finanstilsynet pekte i foreløpig rapport på at foretakets IKT-risiko i begrenset grad omtales i den kvartalsvise IKT-rapporten som sendes styret i foretaket. Etter Finanstilsynets vurdering var foretakets rapportering av IKT-risiko, inkludert IKT-sikkerhetsrisiko, mangelfull.

Det framgår av styrets svarbrev at styret nå har vedtatt måltall og rammer for de ulike områdene innenfor operasjonell risiko, inkludert IKT-risiko, og at risikokontrollfunksjonen som nevnt over nå rapporterer til styret kvartalsvis på måltallene med tilhørende rammer. Styret kommenterer videre at de tiltak det har iverksatt vil sikre at styret til enhver tid har det nødvendige grunnlag for å oppfylle sitt ansvar for å påse at banken oppfyller de krav som stilles til virksomheten på området.

Finanstilsynet tar styrets svar til etterretning.

Styring med og kontroll av IKT-risiko

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.

Foretaket har ikke gjennomført en forretningsmessig konsekvensanalyse. Foretaket har utarbeidet en systemoversikt, men som kommentert i foreløpig rapport oppfatter Finanstilsynet at det er foretakets IKT-avdeling som har utarbeidet denne oversikten, uten å involvere forretningssiden i foretaket. Med bakgrunn i at det ikke er gjennomført en forretningsmessig konsekvensanalyse var det Finanstilsynet vurdering i foreløpig rapport at foretaket har mangler i sin etterlevelse av kravene i IKT-forskriften § 11 vedrørende driftsavbrudd og kriseberedskap.

Finanstilsynet merker seg fra styrets svar at styret vil påse at foretaket kartlegger og dokumentere de kritiske forretningsprosesser med underliggende systemer, og at forretningsområdene blir inkludert i dette arbeidet. Konsekvensanalysen vil bli revidert årlig, og ivaretakelse av rutiner og oppfølging på dette området vil bli fulgt opp fra styrets side, herunder å påse at konsekvensanalysen blir formidlet til relevante leverandører.

Finanstilsynet tar styrets svar til etterretning.

Kriseberedskap

I IKT-forskriftens § 11 framgår kravene 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. Også EBAs retningslinjer for IKT og sikkerhet gir anbefalinger om utarbeidelse av kontinuitetsplaner, respons- og gjenopprettingsplaner, testing og kommunikasjonsplaner ved kriser.

Finanstilsynets vurdering i foreløpig rapport var at foretaket, som følge av mangelfull opplæring, øvelse og testing, kan ha utfordringer med å håndtere for eksempel et cyberangrep, hvor angriper

[1] EBA/GL/2019/04: EBA Guidelines on ICT and security risk management

har etablert digitalt fotfeste på innsiden av foretakets nettverk. Finanstilsynet presiserer at foretaket selv er ansvarlig for at opplæring, øvelse og testing av foretakets kriseløsning gjennomføres årlig. 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

Finanstilsynet tar til etterretning styrets svar om at styret vil vurdere om det skal gjennomføres en test hvor det simuleres et alvorlig cyberangrep, og at det vil legges til rette for videreføring av trening og øvelser i organisasjonen for øvrig for å vurdere egnetheten til kriseløsningen og robustheten til organisasjonen.

Utkontraktering

I henhold til IKT-forskriften § 2 skal foretaket 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, herunder revidere, leverandørens aktiviteter, samt Finanstilsynets tilgang til opplysninger og mulighet for å føre tilsyn hos IKT-leverandøren. Videre framgår det av § 2 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 utkontrakterings-forholdet og en beskrivelse av hvordan foretaket skal sikre leveransene. Det følger videre av forskriftens § 12 at foretaket har ansvar for risikostyring og internkontroll også der hele eller deler av virksomheten er utkontraktert.

Foretaket har utkontraktert store deler av IKT-virksomheten. Finanstilsynets vurdering i foreløpig rapport var at foretakets oppfølging av tjenesteleverandørene var mangelfull. Det blant annet som følge av at oppfølgingen av leverandørene gjøres via allianseselskapet LB Selskapet AS. Det stedlige tilsynet etterlot videre et inntrykk av at foretaket i liten grad følger opp leverandørene av fellestjenestene eller andre leverandører utover hovedleverandøren.

Styret skriver i sitt svar at styret nå etter iverksatte tiltak er av den oppfatning at foretaket har tilstrekkelig kompetanse til å forvalte utkontrakteringsavtalene. Videre omtaler styret enkelte tiltak som er iverksatt i alliansen. Finanstilsynet har videre merket seg fra styrets svarbrev at det vil be om at det fremlegges en bekreftelse for at foretaket og allianseselskapet har den nødvendige kunnskap og ressurs som er nødvendig for å følge opp de viktigste IKT-tjenestene.

Finanstilsynet minner om at bruk av oppdragstakere er uten innvirkning på foretakets plikter og ansvar, og forutsetter at styret iverksetter ytterligere tiltak dersom det vurderer at foretaket ikke har tilgang på nødvendig kunnskap og ressurser.

Nøkkelpersonrisiko

IKT-forskriftens § 2 stiller krav om at det skal oppnevnes ansvarlige, det vil si funksjon eller stilling, i foretaket for de ulike deler av IKT-virksomheten.

I foreløpig rapport kommenterte Finanstilsynet at det var Finanstilsynets vurdering at nøkkelperson-risikoen innen IKT i foretaket er høy, noe som innebærer en betydelig sårbarhet. Det som følge av at foretakets IKT-ressurs var begrenset til IT-ansvarlig. Finanstilsynets mente at foretaket må sikre at tap av nøkkelpersoner ikke utgjør en risiko for foretakets IKT-virksomhet. Foretaket bør sørge for at viktig kunnskap er dokumentert og erfaring overført til andre medarbeidere.

Styret skriver i sitt svar at det tar til etterretning Finanstilsynets oppfatning av at nøkkelperson-risikoen innen IKT-området synes å være høy og sårbar. Som en konsekvens av ansettelse av IKT-rådgiver i 100 prosent stilling, sammenholdt med en forsterkning av organisasjonen, er det styrets oppfatning at nøkkelpersonrisikoen innenfor IKT-området er vesentlig redusert.

Finanstilsynet tar styrets svar til etterretning og legger til grunn at styret følger opp nøkkelperson-risikoen i foretaket. Finanstilsynet understreker styrets ansvar for å sikre at foretaket har tilstrekkelig kunnskap og ressurser på IKT-området.

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. Videre skal det finnes retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene. Nærmere utdypinger finnes i EBAs retningslinjer for IKT og sikkerhet.

Finanstilsynet kommenterte i foreløpig rapport at etterlevelse av styrende dokument som IKT-sikkerhetspolicy må følges spesielt opp og særlig for tjenester som er utkontraktert. Finanstilsynet ba foretaket sikre at retningslinjer og rutiner som gjelder for banken implementeres og følges opp også for utkontrakterte IKT-tjenester.

Finanstilsynet tar til etterretning at styret i sitt svarbrev er enig med Finanstilsynet i at bankens retningslinjer og rutiner også må fange opp kontroller for alle utkontrakterte tjenester. Styret skriver videre at administrasjonen innen utgangen av inneværende år vil fremlegger en rapport til styret som kan bekrefte at IKT-forskriftens § 5 overholdes også for utkontrakterte tjenester.

Finanstilsynet ber styret bekrefte, så snart det har behandlet administrasjonens rapport, at foretakets retningslinjer og rutiner også overholdes for utkontrakterte tjenester, jf. IKT-forskriften § 5.

Finanstilsynet ber om å motta kopi av protokollen fra styremøtet hvor Finanstilsynets tilsynsrapport blir behandlet.

Kopi av dette brevet bes sendt til valgt revisor.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Irene Støback Johansen
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.