FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

SPAREBANK 1 NORD-NORGE
Postboks 6800 Stakkevollan
9298 TROMSØ

VÅR REFERANSE	DERES REFERANSE		DATO
22/12410			26.05.2023

Tilsynsrapport

Finanstilsynet gjennomførte stedlig tilsyn i Sparebank 1 Nord-Norge (Banken) 13. januar 2023. Tilsynet hadde som formål 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 Banken og for utkontrakterte IKT-tjenester, samt at regulatoriske krav på dette området overholdes.

Samtaler ble gjennomført i tilsynsmøtet med representanter fra Banken, samt i eget møte med internrevisor.

Til grunn for disse merknadene ligger Finanstilsynets foreløpige rapport datert 20. februar 2023 og styrets kommentarer til rapporten i brev av 1. april 2023.

Finanstilsynet har følgende merknader etter det stedlige tilsynet:

Organisering – IKT-strategi

Det framgår av IKT-forskriften § 2 første ledd at foretaket skal fastsette overordnede mål, strategier og sikkerhetskrav for IKT-virksomheten.

Finanstilsynet gjennomgikk som en del av tilsynet Bankens forretningsstrategi og IKT-strategi.

Finanstilsynets pekte i foreløpig rapport på at Bankens IKT-strategi i stor grad er rettet mot Bankens arbeid med teknologi, og da særlig hvordan Banken skal forholde seg til arbeid med teknologi i SpareBank 1-alliansen, og i liten grad underbygger kundefokuset det pekes på i forretningsstrategien.

Av styrets svar framgår det at Banken de siste årene har lagt ned store ressurser i å oppdatere sitt strategiske rammeverk. Videre framgår det at strukturen på det strategiske rammeverket tilsier at de ulike strategiene må sees i sammenheng med hverandre, og at et viktig fokusområde i arbeidet med strategien har vært å påse at sammenhenger mellom de ulike strategiene, samt øvrige styrende dokumenter, er ivaretatt på en fullgod måte. På den bakgrunn er det styrets vurdering at kundefokus samlet sett er ivaretatt på en tilstrekkelig måte i det samlede strategiske rammeverket.

Finanstilsynet tar styrets svar til etterretning.

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

Organisering – systemeier

Det framgår av IKT-forskriften § 2 tredje ledd at det skal oppnevnes ansvarlige i foretaket for de ulike delene av IKT-virksomheten.

Finanstilsynet gjennomgikk i tilsynet Bankens beskrivelse av systemeier-rollen og hvilke oppgaver som er tildelt til systemeier.

Finanstilsynet pekte i foreløpig rapport på at systemeierne av Bankens IKT-systemer er organisert i Bankens IKT-organisasjon. Det ble også pekt på at Finanstilsynet finner det vanskelig å se at en systemeier organisert i IKT-organisasjonen kan utføre systemeieroppgaver på vegne av den som er forretningsmessig ansvarlig for produktet IKT-tjenesten understøtter.

Finanstilsynet pekte i foreløpig rapport også på at systemeierskap bør ligge i forretningsenheten med systembehovet og være forankret på ledernivå med bakgrunn i at systemeier er bestiller og funksjonell premissgiver innen systemets funksjonsområde og ansvarlig for finansiering og kontrakter.

Finanstilsynet har merket seg fra styrets svar at Banken har systemeiere som også er plassert utenfor IKT-organisasjon, men at en stor del av systemeierskapet ligger i IKT-organisasjonen. Finanstilsynet har videre merket seg at styrets vurdering er at forretningssidens behov på systemsiden blir ivaretatt på en adekvat måte, også i de tilfeller der systemeierskap er tillagt andre enheter.

Finanstilsynets opprettholder sin vurdering om at systemeiere for systemer som understøtter Bankens forretningsområder bør være organisert i den enhet som er ansvarlig for forretningsområdet IKT-systemet understøtter.

Rapportering av IKT-risiko

Etter finansforetaksloven § 8-6 fjerde ledd skal styret føre tilsyn med den daglige ledelse og foretakets virksomhet ellers, og sørge for at daglig leder regelmessig gir styret informasjon om foretakets virksomhet. Styrets rolle knyttet til foretakets system for risikostyring og internkontroll framkommer av bestemmelsene i CRR/CRD IV-forskriften § 35, der det blant annet presiseres at styret skal sikre seg tilgang til risikoinformasjon og fastsette omfang, format og frekvens på rapporteringen.

Banken mottar årlig ISAE 3402-rapport fra IKT-tjenesteleverandør. Revisjonen er utført av tjenesteleverandørs eksterne revisor og er en uavhengig revisorbekreftelse av internkontrollen for prosessering av finansiell informasjon i IKT-systemene, samt andre generelle kontroller knyttet til leveransen av IKT-tjenester. Formålet med erklæringen er i hovedsak å redusere behovet for at Bankens eksternrevisor selv må utføre revisjonshandliger for å vurdere dataintegriteten i systemer som behandler finansielle data.

Finanstilsynet understreker at Bankens kritiske systemer og nettverk ikke nødvendigvis omfattes av revisjonsrapporten eller inngår i testutvalget som legges til grunn for de tester som gjennomføres i revisjonen. Resultatet av testene, slik de er beskrevet i ISAE 3402-rapporten, gir indikasjoner på leverandørens styring og kontroll av egen IKT-virksomhet. Finanstilsynets vurdering er at erklæringen ikke kan anses som en fullverdig bekreftelse fra leverandøren på etterlevelse av Bankens egne krav satt i strategier, policyer og kvalitetsmål. Det forventes at Banken gjennomfører egne vurderinger av i hvilken grad erklæringen og bekreftelsen omfatter Bankens utkontrakterte tjenester, og de prosesser som leverandøren benytter for å understøtte IKT-leveransene til Banken.

Av styrets svar framgår det at Banken på generelt grunnlag deler Finstilsynets vurdering om at revisjonsrapporten ISEA 3402 ikke nødvendigvis dekker alle kritiske systemer og nettverk i Banken eller er å anse som en fullstendig bekreftelse fra leverandøren på etterlevelse av bankens egne krav.

Finanstilsynet understreker viktigheten av tiltakene, både taktiske og operasjonelle, Banken har iverksatt gjennom prosjekt og andre aktiviteter for å kunne bruke rapporter fra leverandør inn i egen styring og kontroll med IKT-virksomheten.

Tilgangsstyring – utkontraktert IKT-virksomhet

IKT-forskriften § 5 Sikkerhet 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. Ytterligere utdyping finnes i den europeiske banktilsynsmyndighetens Guidelines on ICT and security risk management (EBA/GL/2019/04).

Finanstilsynet pekte i foreløpig rapport på at tilgangslogger som følge av oppslag på databasenivå ikke i tilstrekkelig grad følges opp og rapporteres på av IKT-tjenesteleverandør. Videre ble det pekt på at det er viktig at Banken har kontroll med leverandørens tilganger og gjennomfører en effektiv overvåking av data som blir aksessert i systemet. Videre må Banken ha kontroll med hvilke av leverandørens brukere som har tilgang til sensitive data, og kunne dokumentere dette.

Det framgår av styrets svar at de er enig i at det er behov for tiltak knyttet til oppfølging av tilganger hos leverandører og at Banken har iverksatt tiltak for å bedre oppfølgingen.

Finanstilsynet tar styrets svar til etterretning.

Kopi av dette brevet bes sendt til ekstern og intern revisor.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Stig Ulstein
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.