FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Styret i Kommunalbanken AS
Postboks 1210 Vika
0110 OSLO

VÅR REFERANSE	DERES REFERANSE		DATO
24/2526			16.09.2024

Tilsynsrapport

Finanstilsynet gjennomførte stedlig IKT-tilsyn i Kommunalbanken (foretaket) 3. mai 2024.

Hensikten med tilsynet var å gjøre en vurdering av hvordan foretaket administrerer, utvikler, drifter, vedlikeholder og sikrer IKT-systemer og -tjenester. Finanstilsynet vurderte styring med og kontroll av IKT-virksomheten med spesiell vekt på IKT-risiko, endrings- og avvikshåndtering, datastyring og forvaltning, IKT-sikkerhet, utkontraktering og beredskap.

Til grunn for tilsynsrapporten ligger Finanstilsynets foreløpige rapport datert 14. juni 2024 og styrets kommentarer til rapporten i brev av 16. august 2024.

Finanstilsynet har følgende merknader etter tilsynet:

Overordnet styring og kontroll

Organisering

Det framgår av finansforetaksloven § 8-6 første ledd at styret skal sørge for forsvarlig organisering av virksomheten. Videre i lovens § 13-5 andre ledd stilles det krav om at et finansforetak skal ha uavhengige kontrollfunksjoner med ansvar for risikostyring, etterlevelse og internrevisjon. CRR/CRD-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 at foretaket skal ha en uavhengig kontrollfunksjon for kontroll av etterlevelse, og 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.

Finanstilsynet pekte i foreløpig rapport på at gitt behovene Kommunalbanken har, ikke minst som følge av det pågående konverteringsprosjektet, er foretaket etter Finanstilsynets vurdering helt avhengig av personell med både riktig og tilstrekkelig kompetanse innen IKT i alle de tre forsvarslinjene for å nå foretakets strategiske mål og sikre forsvarlig drift av virksomheten. Finanstilsynet kommenterte på at enkelte IKT-relaterte nøkkelstillinger i foretaket på tidspunktet for tilsynsmøtet sto ubesatt.

Finanstilsynet har merket seg fra styrets svar at antall internt ansatte i IKT-funksjonen i første forsvarslinje vil økes i inneværende år og ytterligere økes gjennom strategiperioden 2024-2027,

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00

post@finanstilsynet.no
www.finanstilsynet.no

Saksbehandler
Åshild Johnsen
Dir. tlf. 22 93 97 02

samt at de nyopprettede mellomlederstillingene i Teknologi og operasjoner nå er besatt. Videre har Finanstilsynet merket seg at rekruttering til stillingen i andrelinjen i avdeling Risikostyring forventes å bli besatt i løpet av 2024, og at styret regelmessig mottar status på rekruttering til de ubesatte stillingene.

Finanstilsynet tar styrets svar til etterretning.

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 risikoene. IKT-forskriften § 2 første ledd stiller videre krav til at foretaket skal fastsette overordnede mål, strategier, og sikkerhetskrav for IKT-virksomheten. Etter IKT-forskriften § 3 første ledd skal det fastsettes grenser for akseptabel risiko forbundet med bruk av IKT-systemene.

I foreløpig rapport kommenterte Finanstilsynet at versjonslogg ikke framgår av foretakets overordnede strategi og IKT-strategi for 2024-2026, dvs. at de manglet informasjon om hvem som har utarbeidet og godkjent dokumentene, versjonsnummer, hva som er nytt/endret, samt når dette er gjort. Finanstilsynet anbefalte at overordnet styringsdokumentasjon påføres versjonslogg.

Finanstilsynet har merket seg fra styrets svarbrev at styret vurderer å ha tilstrekkelig oversikt over endringene i styrende dokumenter, men at det for ordens skyld vil innføre versjonslogg i samtlige styrende dokumenter fra og med neste oppdatering.

Videre pekte Finanstilsynet i foreløpig rapport på at det ikke kunne se at foretakets overordnede retningslinjer tydelig operasjonaliserer og konkretiserer styrets risikoappetitt for operasjonell risiko, inkl. IKT-risiko, jf. IKT-forskriften § 3.

Fra styrets svarbrev har Finanstilsynet notert at styrets samlede risikostyring gjøres gjennom et fastsatt rammeverk som årlig vurderer og fastsetter risikoappetitt for restrisiko for ulike identifiserte risikokategorier. For alle risikokategoriene er det fastsatt kvalitative terskler, som er konkretisert gjennom risikoappetittutsagn. Risikoappetitt for operasjonell risiko, herunder for IKT og cyber, er operasjonalisert gjennom administrerende direktørs retningslinjer og gjennom klassifisering av IKT-systemer etter forretningsverdi og akseptabel nedetid. Styret erkjenner at styrets risikoappetitt på IKT-området fremstår som noe fragmentert. Styret finner det derfor hensiktsmessig at operasjonaliseringen av risikoappetitten på IKT-området, inkl. cyberrisiko, videreutvikles og tydeliggjøres, herunder mer spesifikke konsekvenskriterier for IKT-risiko.

Finanstilsynet tar styrets svar til etterretning.

Rapportering av IKT-risiko og cyberrisiko

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.

I foreløpig rapport vurderte Finanstilsynet at foretakets styrerapportering av operasjonell risiko, herunder IKT-risiko og IKT-sikkerhetsrisiko, var fragmentert og mangelfull, noe som gjør at det blir utfordrende for styret å ha oversikt over risikoen. For Finanstilsynet framsto det videre som en mangel at risikoen knyttet til det pågående prosjektet for å erstatte foretakets utlånssystem ikke er omtalt i og omfattet av den løpende risikorapporteringen. For at styret skal kunne ha en samlet oversikt over foretakets operasjonelle risiko, inkludert IKT-risiko og IKT-sikkerhetsrisiko, er det Finanstilsynets oppfatning at styret regelmessig bør bli presentert for en helhetlig og fullstendig vurdering og analyse av foretakets risiko og sårbarhet, jf. kravene i finansforetaksloven og IKT-forskriften nevnt over.

Styret skriver i sitt svarbrev at det vurderer at det mottar adekvat informasjon om operasjonell risiko, der den samlede rapporteringen fra administrasjonen er dekkende mht. omfang, format og frekvens for styrets styring av operasjonell risiko. Rapporteringen vurderes til å være i tråd med gjeldende regelverk. Imidlertid vurderer styret det som hensiktsmessig å videreutvikle rammeverket for operasjonell risikostyring, inkl. rapporteringsstruktur. Styret deler Finanstilsynets vurdering om å utvide dagens ROS-analyse til å omfatte all IKT-relatert risiko (IT og cyber) og heretter også inkludere vurderingene av cybertruslene og deres relevans for foretaket slik at etterfølgende rapportering til styret fremstår som mindre fragmentert enn dagens rapporteringsstruktur.

Finanstilsynet tar styrets svar til etterretning.

Risikovurdering av IKT-risiko og cyberrisiko

Et finansforetak skal til enhver tid ha oversikt over, og med jevne mellomrom vurdere, hvilke enkelte risikoer og samlet risiko som er knyttet til virksomheten, jf. finansforetaksloven § 13-6 første ledd. Etter IKT-forskriften § 3 annet ledd skal det minst en gang årlig, eller ved endringer som har betydning for IKT-sikkerheten, gjennomføres risikoanalyser for å påse at IKT-risikoen styres innenfor akseptable grenser i forhold til foretakets virksomhet. Resultatet av risikoanalysen skal dokumenteres.

Kommunalbanken vurderer risiko og sårbarhet minimum årlig i en ROS-analyse som behandles av styret. I foreløpig rapport var Finanstilsynets vurdering at ROS-analysen primært har fokus på informasjonssikkerhet og cyberrisiko, og i begrenset grad på mer operasjonelle risikoer og IKT-driftsrelaterte sårbarheter. Prosjekt- og konverteringsrisikoen knyttet til utvikling av, og tilpasning og konvertering til nytt utlånssystem, er ikke nevnt i foretakets ROS-analyse, selv om dette etter planen skal skje i løpet av inneværende år, og etter Finanstilsynets vurdering er det knyttet stor risiko til prosjektet. Finanstilsynet pekte i foreløpig rapport på at når ROS-analysen til Kommunalbanken ikke omtaler utviklingen og implementeringen av nytt utlånssystem, reflekterer ikke analysen den reelle operasjonelle risikoen i foretaket.

Finanstilsynet har merket seg fra styrets svarbrev at kravet om gjennomføring av risikoanalyser på IKT-området vurderes å være oppfylt, men kan fremstå som fragmentert. Styret deler Finanstilsynets vurdering om å utvide dagens ROS-analyse til å omfatte all IKT-relatert risiko (IT og cyber) og heretter også inkludere vurderingene av cybertruslene og deres relevans for foretaket. Styret skriver videre at det har behandlet rapporter om status i implementeringsprosjektet flere ganger siden anskaffelsen i desember 2021, og at slik IKT-relatert risiko av hensyn til helheten også vil inntas i ROS-analysen framover.

Finanstilsynet tar styrets svar til etterretning.

Virksomhetsmessig konsekvensanalyse
Ifølge IKT-forskriften § 13 skal det foreligge oppdatert dokumentasjon av det enkelte IKT-system som er av betydning for foretakets virksomhet. Virksomhetsmessig konsekvensanalyse skal bidra til å sikre at foretakets beredskapsplaner utarbeides med basis i virksomhetsmessig kritikalitet. Planene skal basere seg på foretakets prioriteringer for gjenoppretting av virksomhetskritiske 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. For å verifisere at det er etablert fungerende planer og løsninger må det minst årlig foretas opplæring, øvelse og testing, jf. IKT-forskriften § 11.

Finanstilsynet viste i foreløpig rapport til at foretaket ikke har gjennomført en virksomhetsmessig konsekvensanalyse. Foretaket hadde utarbeidet en systemoversikt, men Finanstilsynet oppfattet at det primært var foretakets IT-avdeling som hadde utarbeidet denne med begrenset involvering fra forretningssiden. Finanstilsynets vurdering var at uten en virksomhetsmessig konsekvensanalyse vil foretakets kriseplan, være utarbeidet uten virksomhetsmessige prioriteringer.

Finanstilsynet har fra styrets svar merket seg at styret vurderer at beredskapsplanen, kontinuitetsplanen og sikringstiltakene er innrettet etter systemenes forretningsverdi, slik denne er vurdert av forretningsenhetene. Prioriteringsrekkefølgen for gjenoppretting som er avtalt med driftsleverandøren, reflekterer systemenes forretningsverdi. Styret skriver videre at de ser det som formålstjenlig at vurderingene og analysen som ligger til grunn for klassifiseringen av de ulike systemene og IKT-tjenestene etter forretningsverdi, formaliseres i en virksomhetsmessig konsekvensanalyse.

Finanstilsynet tar styrets svar til etterretning.

Styring med og kontroll av IKT-risiko

Endrings- og avvikshåndtering
I henhold til IKT-forskriften § 9 skal foretaket sikre at prosedyrer for avviks- og endringshåndtering foreligger og følges. Prosedyrene for endringshåndtering skal omfatte alle endringer som kan påvirke IKT-systemene og skal sikre forsvarlig, formell behandling og dokumentering av endringene.

Finanstilsynet pekte i foreløpig rapport på at når et av foretakets hovedsystemer går fra egen-utviklet programvare til lisensiert programvare, kan endringshåndteringen bli mindre effektiv fordi foretaket må stille i kø for prioriteringer hos leverandøren. Finanstilsynet viste til at applikasjonsleverandørens rolle ikke framkom i rutinene for endringshåndtering.

Finanstilsynet ba i foreløpig rapport foretaket sikre at rutinene for endringshåndtering beskriver hvordan endringer i lisensiert programvare, skal gjennomføres. Finanstilsynet ba videre foretaket sikre at ROS-analysen vurderer risiko knyttet til endringshåndtering av lisensiert programvare.

Styret viser i sitt svar til at foretaket gjennomfører installasjon, testing og produksjonssetting av nye versjoner av lisensiert programvare. Foretaksspesifikk funksjonalitet løses i hovedsak med konfigurasjon av den lisensierte programvaren og er ikke avhengig av programvareleverandøren for

de fleste funksjonelle tilpasningene. Endrings- og avvikshåndtering for lisensiert, konfigurerbar programvare følger samme prosess uavhengig av leverandør. Styret viser videre til at det vurderer det som hensiktsmessig at ROS-analysen fremover skal omfatte en vurdering av all IKT-relatert risiko, herunder vurderinger av sårbarhet knyttet til lisensiert programvare.

Finanstilsynet tar styrets svar til etterretning.

IKT-sikkerhet

Ifølge IKT-forskriften § 5 skal 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. I tillegg skal det foreligge retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene.

Finanstilsynet viste i foreløpig rapport til leverandørens månedsrapport hvor det er listet brukere både i foretaket og hos leverandøren som har tilgang til foretakets servere og systemer. Typer tilganger/roller er imidlertid ikke spesifisert, og det framkommer ikke hva slags tilgang den enkelte bruker har. Finanstilsynet antar at ansatte hos leverandøren har ulike tilganger inkludert at noen av dem har privilegerte tilganger til kritiske driftsoperasjoner. Finanstilsynets vurdering i foreløpig rapport var at foretaket bør sikre at det framgår hvilken type tilgang den enkelte har, inkludert den enkelte ansatte/konsulent hos leverandøren. Finanstilsynet anbefalte også at foretaket gjør en risikovurdering av om tilgangene til leverandøren er innenfor foretakets risikoappetitt.

Fra styrets svar framgår det at foretaket har innsyn i leverandørens retningslinjer og prosedyrer for tilgangsstyring, samt resultatet av årlige eksterne revisjoner av leverandøren som blant annet omfatter tilgangsstyring. Samlet vurderer styret at foretaket har tilstrekkelig innsikt i hvem som har tilgang til relevant infrastruktur, men vil søke å få utvidet rapportering fra leverandøren om type tilganger per bruker i månedsrapporteringen, herunder for å vurdere hvorvidt tilgangene er basert på tjenstlig behov.

Finanstilsynet pekte videre på at foretaket manglet en rutine der foretakets krav til logging og oppfølging av loggene framgår. Oppfølging av logger kan omfatte både logging av ekstern aktivitet mot foretakets internettportal, og logging av intern aktivitet i foretakets systemer. Kravene til logging og loggoppfølging må også gjøres kjent for driftsleverandøren, og leverandøren må forplikte seg til å etterleve dem.

Det framgår av styrets svar at styret finner det hensiktsmessig at prosess og rutine for loggoppfølging dokumenteres på samme måte som endrings- og avvikshåndtering, dvs. én rutine uavhengig av hvilken loggoppfølging det gjelder.

Finanstilsynet tar styrets svar til etterretning.

Beredskap

IKT-forskriften § 11 stiller krav til at foretaket skal ha en dokumentert kriseplan, slik at forretningsmessig kontinuitet kan opprettholdes. Kriseplanen skal iverksettes dersom IKT-driften ikke kan opprettholdes som følge av en krise. Minimumskravene til en slik kriseplan fremgår av IKT-forskriften § 11 annet ledd. IKT-forskriften § 11 tredje ledd stiller krav til at det skal

gjennomføres opplæring, øvelse og testing av at kriseløsningen fungerer som forutsatt og at resultatet av testen skal dokumenteres.

Finanstilsynet la i foreløpig rapport til grunn at beredskapsplanen vil oppdateres som følge av gjennomføringen av den virksomhetsmessige konsekvensanalysen, ref. punkt over. Styret viser i sitt svar til at beredskapsplanen oppdateres årlig eller ved vesentlige endringer i virksomheten, og at dersom den forestående formaliseringen av analysen av systemenes forretningsverdi resulterer i endringer, vil dette reflekteres i beredskapsplanen, kontinuitetsplanen og prioriteringsrekkefølgen for gjenoppretting av systemer.

Finanstilsynet anbefalte videre at foretaket gjennomfører beredskapsøvelse der også driftsleverandøren deltar og slik øker utbytte av øvelsen. Styret viser i sitt svar til at øvelsen i 2021 var med deltakelse fra driftsleverandøren, mens scenarioene i 2022 og 2023 hadde andre testformål. Styret viser videre til at de finner det formålstjenlig at øvelser også framover regelmessig inkluderer deltakelse fra driftsleverandøren.

Finanstilsynet tar styrets svar til etterretning.

Kopi av dette brevet bes sendt til valgt revisor.

For Finanstilsynet

Olav Johannessen
seksjonsleder

Åshild Johnsen
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.