FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Styret i Sparebanken Sør
Postboks 200
4662 KRISTIANSAND S

VÅR REFERANSE	DERES REFERANSE		DATO
22/5154			05.01.2023

Tilsynsrapport etter stedlig IKT-tilsyn

Finanstilsynet gjennomførte stedlig IKT-tilsyn i Sparebanken Sør 21. juni 2022. Tilsynet hadde som formål 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 vurdere foretakets beredskap og beredskapsarbeid innen IKT-området opp mot regulatoriske krav, herunder for utkontrakterte IKT-tjenester.

Til grunn for disse merknadene ligger Finanstilsynets foreløpige rapport datert 22. august 2022 og styrets kommentarer til rapporten i brev av 28. oktober 2022.

Finanstilsynet registrerer fra styrets svar at styret oppfattet at varselet om IKT-tilsyn i utgangspunktet ikke omfattet andre- og tredjelinjes oppfølging av IKT-risiko. Finanstilsynet bemerker at bankens uavhengige kontrollfunksjoner, jf. finansforetaksloven § 13-5 (2), er vesentlige for bankens styring og kontroll av risiko knyttet til IKT-virksomheten. For at Finanstilsynet skal kunne gjøre en vurdering av bankens risiko må vurderingen dermed også inkludere andre og tredje forsvarslinje.

Finanstilsynet tar styrets ettersendte kontroll- og risikorapporter fra andre og tredje forsvarslinje til etterretning.

Finanstilsynet har følgende merknader etter det stedlige tilsynet:

Overordnet styring og kontroll av IKT-risiko

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 § 38 stiller krav om at banken 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.

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

Interessekonflikter
I foreløpig rapport stilte Finanstilsynet spørsmål ved bankens håndtering av mulige interessekonflikter som følge av at Leder Sikkerhet og Compliance fremsto å ha mer enn én rolle, og uten å ha en stillingsinstruks.

Finanstilsynet merker seg fra styrets svar at banken deler oppfatningen om at det kan være uheldig å bruke en stillingsbetegnelse som "Compliance" på en del av denne funksjonen. Hovedfunksjonen skal være knyttet til "sikkerhet" i første forsvarslinje, og stillingsbetegnelse er endret til "Leder IT-sikkerhet". Finanstilsynet tar videre til etterretning at banken vil utarbeide stillingsinstruks for denne funksjonen.

Oppfølging av IKT-risiko i andre og tredje forsvarslinje
Finanstilsynet vurderte i foreløpig rapport at bankens oppfølging av IKT-risiko i andre og tredje forsvarslinje var mangelfull. Det blant annet som følge av at etterlevelsesfunksjonen vurderer og følger opp bankens IKT-virksomhet på et overordnet nivå, men uten å stille krav til eller gjør vurderinger av mer teknisk/IKT-faglig karakter. Tilsynet etterlot et inntrykk av at risikostyringsfunksjonen ikke var involvert i vurderinger av IKT-risiko. Videre var IKT-risiko i liten grad inkludert i andrelinjens løpende risikorapportering til styret, se merknad under. Når det gjelder internrevisjonens oppfølging av IKT-risiko bemerket Finanstilsynet i foreløpig rapport at internrevisors revisjon var begrenset til en oppfølgingsrevisjon. Finanstilsynet stilte også spørsmål ved hvordan banken sikrer at etterlevelses- og risikokontroll-funksjonene har tilstrekkelig ressurser og IKT-kompetanse til å kunne kontrollere og stille krav til førstelinjen på området.

Det framgår av styrets svar at styret ikke deler Finanstilsynets vurdering. Selv om styret erkjenner at det alltid vil foreligge et forbedringspotensial på alle områder, vurderer styret at totaliteten i styring og kontroll fra andre- og tredjelinje er tilfredsstillende og hensiktsmessig, og at banken har tilstrekkelige ressurser og IKT-kompetanse til å kunne kontrollere og stille krav til førstelinjen. Styret peker blant annet på at en oppfølging av IKT-risiko fra andre- og tredjelinjefunksjonene bør bygge på hva som samlet gjøres i disse funksjonene, og at det i de siste årene er det gjort et betydelig antall kontroller og undersøkelser på området. Når det gjelder tredje forsvarslinje henviser styret spesielt til revisjonen av informasjonssikkerhet og utkontraktering som ble gjennomført i 2020, og oppfølgingen av alle anbefalingene som ble gitt der.

Finanstilsynet merker seg styrets svar og ettersendt dokumentasjon, spesielt ettersendte rapporter fra Compliance vedrørende kontroll av ikke-tjenstlig oppslag/taushetsplikt datert august 2022 og utkontraktering datert september 2022. Finanstilsynet understreker viktigheten av at styret og ledelsen i banken sørger for at bankens uavhengige kontrollfunksjoner til enhver tid har tilstrekkelig IKT-kompetanse og -ressurser i alle forsvarslinjer. Finanstilsynet understreker videre viktigheten av at kontrollfunksjonene i sitt arbeid har en risikobasert tilnærming. Det slik at bankens arbeid med IKT-risiko og IKT-sikkerhetsrisiko, inkludert informasjonssikkerhet, kontinuitet og beredskap, prioriteres i tråd med utviklingen i risikobildet. Finanstilsynet har også merket seg revisors anbefalinger i ovennevnte internrevisjonsrapport fra revisjon av informasjonssikkerhet og utkontraktering i 2020. Finanstilsynet forventer at bankens styre og ledelse prioriterer arbeidet med oppfølgingen av anbefalingene, spesielt sett i lys av dagens risikobilde. Det vises videre til merknad i punkt om Konsekvensanalyse (Business Impact Analysis, BIA) nedenfor.

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.

Styrets risikotoleranse for informasjonssikkerhet er ikke nærmere omtalt eller operasjonalisert i bankens overordnede styringsdokumenter. Finanstilsynet understrekte i foreløpig rapport viktigheten av at bankens rammeverk og retningslinjer er tydelige og avklarende for å sikre at banken opererer i tråd med styrets risikotoleranse.

Finanstilsynet har fra styrets svar merket seg at styret ser det kan være behov for å videreutvikle rammeverk og tydeliggjøre risikotoleranse for operasjonell risiko, slik at styret i større grad kan ha oversikt over både total operasjonell risiko og "undertyper" av operasjonell risiko, som for eksempel IKT-risiko og sikkerhetsrisiko. Finanstilsynet tar til etterretning at styret vil påse at det innarbeides en tydeligere definisjon av hvordan lav, middels og høy risiko defineres innenfor operasjonell risiko/IKT-risiko ved kommende revisjon av relevante styringsdokumenter, samt at det også er et siktemål å innarbeide tydeligere kvantitative målsettinger og risikotoleransegrenser for disse risikoområdene.

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 er av den oppfatning at styret, for å kunne føre tilsyn med daglig ledelse og banken for øvrig, må sikre seg løpende og oppdatert informasjon om IKT-risikoen i banken. Finanstilsynet presiserte i foreløpig rapport at tilsynet forventer at IKT-risiko, herunder IKT-sikkerhetsrisiko, vurderes og inkluderes i bankens faste risikorapporter til styret.

Det framgår av styrets svar at styret deler Finanstilsynets oppfatning om at det er viktig med løpende og oppdatert informasjon om IKT-risikoen i banken for å kunne føre tilsyn med daglig ledelse og banken for øvrig. Styret presiserer at det gis omtale av IKT-risiko og IKT-sikkerhetsrisiko til risikoutvalget og styret både i konkrete compliance- og revisjonsrapporter, samt i årsrapport og halvårsrapport for IT-sikkerhet. Videre opplyser styret at når det gjelder rapportering av operasjonell risiko, har dette fått en stadig større plass i den kvartalsvise risikorapporten til styret, og under denne delen belyses det også temaer i tilknytning til IKT-risiko og IKT-sikkerhetsrisiko. Finanstilsynet tar til etterretning styrets svar om at det arbeides det med å videreutvikle og forbedre helhetlig rapportering for operasjonell risiko som også inkluderer IKT-risiko, og legger til grunn at styret sikrer at IKT-risiko og IKT-sikkerhetsrisiko også vurderes og rapporteres i bankens kvartalsvise risikorapport.

Styring og kontroll av IKT-risiko

Konsekvensanalyse (Business Impact Analysis, BIA)

Banken har ansvar for at nødvendig forretningsmessig kontinuitet og beredskap er sikret, jf. IKT-forskriften § 11. Hensiktsmessige planer og tiltak for tilgjengelighet og kontinuitet bør etableres med utgangspunkt i forretningsmessige konsekvensanalyser (BIA) for foretakets kritiske forretningsprosesser.

Finanstilsynet ga i foreløpig rapport uttrykk for at banken hadde mangler i sin etterlevelse av kravene i IKT-forskriften § 11 vedrørende driftsavbrudd og kriseberedskap. Banken har ikke utarbeidet konsekvensanalyser basert på forretningssidens behov. Finanstilsynet forventer at banken etablerer rutine for å gjennomføre forretningsmessige konsekvensanalyser og kommuniserer resultatet med relevante tjenesteleverandører.

Det framgår av styrets svar at styret er av den oppfatning at banken har en veletablert "Beredskapsplan for IT-Drift". Videre opplyses det at Business Impact Analysis (BIA) er definert i bankens retningslinje (ISMS), men at den ikke er ferdig operasjonalisert. Banken vil derfor iverksette en prosess for operasjonalisering, og det presiseres at det er naturlig at dette utføres i samarbeid med kundeområdene i førstelinje.

Finanstilsynet tar styrets svar til etterretning. Finanstilsynet forventer at banken snarlig operasjonaliserer bankens forretningsmessige konsekvensanalyse, slik at den blir i tråd med kravene i IKT-forskriften § 11 og EBAs "Guidelines on ICT and security risk management" (EBA/GL/2019/04).

Leverandørstyring

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 at avtaler om utkontraktering av IKT-virksomhet og endring av slike avtaler skal behandles av styret, som skal presenteres en plan og en risikovurdering av utkontrakteringsforholdet, samt en beskrivelse av hvordan foretaket skal sikre leveransene.

I henhold til forskrift om meldeplikt ved utkontraktering av virksomhet mv. § 1 skal banken ha en oppdatert oversikt over alle utkontrakteringsavtaler.

Finanstilsynet pekte i foreløpig rapport på at bankens oppfølging av utkontraktert IKT-tjenester var mangelfull. Finanstilsynet mente banken blant annet ikke etterlever kravene i IKT-forskriften hva gjelder retningslinjer og rutiner som skal sikre at utkontraktert IKT-virksomhet oppfyller IKT-forskriftens krav. Finanstilsynet mente videre at banken ikke etterlever kravet til samlet oversikt over utkontrakteringsavtaler i meldepliktforskriften § 1.

Finanstilsynet har merket seg fra styrets svar at styret mener banken har tilstrekkelige rutiner og retningslinjer for leverandøroppfølging og utkontraktering, men er enig i at det er et forbedrings-potensial knyttet til operasjonaliseringen. Styret opplyser at det legger til grunn at administrasjonen har påbegynt iverksettelse av nødvendige tiltak for å dekke gap påpekt av etterlevelsesfunksjonen i september 2022. Videre opplyses det at banken allerede har etablert en rolle med ansvar for leverandørstyring som innebærer at det blir en tydeligere systematisering av arbeidet med

leverandørstyring. Finanstilsynet tar styrets opplysning til etterretning og legger til grunn at styret påser at bankens rammeverk for leverandørstyring og utkontraktering, samt oversikt over utkontrakteringsavtaler, er i samsvar med regelverket.

Systemsikkerhet

IKT-forskriften § 5 stiller krav om at banken skal ha prosedyrer for å sikre beskyttelse av utstyr, systemer og informasjon av betydning for bankens 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.

IKT-forskriften § 13 stiller krav til at det er etablert en oppdatert oversikt over organisasjon, utstyr, IKT-systemer og vesentlige forhold i IKT-virksomheten.

Finanstilsynet presiserte i foreløpig rapport at banken må sikre at styrets besluttede sikkerhetskrav i sikkerhets-policyens innfris, også for utkontraktert virksomhet. I foreløpig rapport pekte Finanstilsynet på at bankens utstyrsoversikt var mangelfull, med mangelfull registrering av utstyr, manglende dokumentasjon av sammenhenger mellom utstyr/tjenester og at ikke alt utstyr er oppført med eier.

Det framgår av styrets svar at styret legger til grunn at banken til enhver tid har en oppdatert oversikt over organisasjon, utstyr, IKT-systemer og vesentlige forhold i IKT-virksomheten, og at banken gjennom sine tekniske styringssystemer har en komplett oversikt over alle enheter som inneholder bankens data og hvem som bruker disse. Bankens IKT-systemer er dokumentert i tidligere oversendt systemkatalog.

Finanstilsynet registrerer fra styrets svar at banken tilstreber å etterleve IKT-forskriftens og styrets besluttede sikkerhetskrav. Finanstilsynet har videre merket seg fra styrets svar at banken til enhver tid har en oppdatert oversikt over organisasjon, utstyr, IKT-systemer og vesentlige forhold i IKT-virksomheten, men opprettholder vurderingen fra foreløpig rapport om at bankens utstyrsoversikt for de utkontrakterte IKT-tjenestene er mangelfull. Finanstilsynet forutsetter at styret iverksetter tiltak som sikrer at den blir i samsvar med det som forventes av en slik oversikt, jf. IKT-forskriften § 13 og EBAs "Guidelines on ICT and security risk management" (EBA/GL/2019/04).

Sikkerhetshendelse

I 2021 ble det avdekket et sikkerhetsbrudd hos en av bankens IKT-tjenesteleverandører. Hendelsen var omfattende og vurderes av Finanstilsynet som et alvorlig brudd på avtalen mellom banken og IKT-tjenesteleverandøren.

Finanstilsynet merker seg at styret kommenterer generelt at det legger til grunn at administrasjonen fremover vil ha en tettere oppfølging av sentrale leverandører. Finanstilsynet tar videre til etterretning at styret beklager at hendelsen ikke ble vurdert som en kritisk eller alvorlig sikkerhets-hendelse som skulle rapporteres til Finanstilsynet, og at dersom styret hadde vært kjent med omfanget av hendelsen ville nok banken ha vurdert det annerledes.

Service Desk-prosess

Finanstilsynet pekte i foreløpig rapport på at det ikke var etablert en hensiktsmessig Service Desk-prosess hos bankens IKT-tjenesteleverandør som sikrer en komplett oversikt over bankens henvendelser angående driftsoppdrag. Tjenstlige behov de ansatte hos IKT-tjenesteleverandør har

for å utføre driftsoppgaver for banken på bakgrunn av henvendelsene ble ikke tilstrekkelig dokumentert. Det gjorde det ikke mulig å sammenstille antall henvendelser mottatt fra banken opp mot antall oppslag utført mot bankens IKT-driftsmiljø. Det var derfor Finanstilsynets vurdering at det ikke var mulig for hverken banken eller IKT-tjenesteleverandør å finne ut om leverandørens ansatte bruker sine tilganger til uautoriserte oppslag i bankens kundedata.

Finanstilsynet merker seg fra styrets svar at banken har løpende dialog med IKT-tjenesteleverandør for å følge opp ansattes tilganger til bankens kundedata. IKT-tjenesteleverandøren har iverksatt et omfattende forbedringsprogram for å identifisere og implementere tiltak for å redusere risiko for lignende hendelser, men også for å gjøre både IKT-tjenesteleverandøren og bankene bedre i stand til å oppdage uautoriserte oppslag.

Finanstilsynet fastholder at det med dagens løsning og praksis ikke er mulig for hverken banken eller IKT-tjenesteleverandør å ha kontroll med om ansatte hos leverandør bruker sine tilganger til uautoriserte oppslag i bankens kundedata. Finanstilsynet anser manglene knyttet til Service Desk-prosessen hos IKT-tjenesteleverandør som alvorlige. Finanstilsynet merker seg at IKT-tjenesteleverandøren har iverksatt et forbedringsprogram, men minner om at bruk av oppdragstaker er uten innvirkning på bankens plikter og ansvar. Finanstilsynet forventer at banken iverksetter de tiltakene den kan for å sikre at IKT-tjenesteleverandøren, og også banken, har komplett oversikt over alle henvendelser angående driftsoppdrag, og at formålet med oppslagene leverandøren gjør mot bankens kunder dokumenteres på en slik måte at uautoriserte oppslag i bankens kundedata kan avdekkes. Finanstilsynet ber om å få en skriftlig redegjørelse på status fra styret innen 28. februar 2023.

Tilgangsstyring – utkontraktert virksomhet
Finanstilsynet pekte i foreløpig rapport på at sikkerhetshendelsen viser at etablert rutine for tilgangsstyring og oppfølging hos IKT-tjenesteleverandør ikke var tilstrekkelig, da det gir muligheter for å misbruke tilgangen til ikke-tjenstlige oppslag som vanskelig lar seg avdekke. Finanstilsynet stilte også spørsmål ved bankens styring og kontroll med tilgangsrettigheter ved utkontraktert virksomhet og om denne har vært tilstrekkelig.

Det framgår av styrets svar at styret deler Finanstilsynets vurdering av at etablert rutine for tilgangsstyring og oppfølging hos IKT-tjenesteleverandør ikke var tilstrekkelig, og det henvises til forbedringsprogrammet. Styret erkjenner at Sparebanken Sør har begrensede verktøy og muligheter for kontroll med ansattes bruk av systemene.

Finanstilsynet fastholder at etablert rutine for tilgangsstyring og oppfølging hos IKT-tjenesteleverandør, samt banken oppfølging av denne, ikke er tilstrekkelig. Finanstilsynet anser manglene knyttet til bankens styring og kontroll med tilgangsrettigheter ved utkontraktert virksomhet som alvorlige. Finanstilsynet forventer at banken er bevisst sitt ansvar og inntil IKT-tjenesteleverandøren har på plass en tilfredsstillende løsning iverksetter nødvendige tiltak som sikrer at ansatte har tilganger som i størst mulig grad samsvarer med tjenstlig behov. Finanstilsynet ber om å få en skriftlig redegjørelse fra styret innen 28. februar 2023.

Logging av brukeraktivitet
Finanstilsynet pekte i foreløpig rapport på at informasjonen som banken mottar fra IKT-tjenesteleverandør i form av logger over brukeraktivitet hos leverandøren ikke var tilstrekkelig for å avdekke ikke-tjenstlige oppslag i kundedata. Finanstilsynet mente også at banken ikke i tilstrekkelig

grad har stilt krav til informasjon som gjør det mulig å sammenstilles data på en måte som vil kunne avdekke ikke-tjenstlige oppslag på kundedata.

Finanstilsynet registrerer fra styrets svar at styrets vurdering er at dette er en viktig problemstilling som banken må følge opp med IKT-tjenesteleverandør for å sikre løsninger slik at man begrenser mulighetene for ikke-tjenstlige oppslag på kundedata fremover. Styret henviser til forbedrings-programmet og at leverandøren har orientert banken om at man forventer å være ferdig med de viktigste aktivitetene før utgangen av 2022

Finanstilsynet fastholder at informasjonen som banken mottar fra IKT-tjenesteleverandør i form av logger ikke synes å være tilstrekkelig for å avdekke ikke-tjenstlig oppslag i bankens kundedata. Finanstilsynet anser bankens mangler i kontrollarbeidet med å avdekke om det foretas ikke-tjenstlige oppslag i bankens kundedata som alvorlig. Finanstilsynet har fra styrets svar merket seg at de viktigste aktivitetene fra IKT-tjenesteleverandørens side skal være gjennomført innen utgangen av 2022. Finanstilsynet ber om styrets bekreftelse på at banken mottar logger over brukeraktivitet hos IKT-tjenesteleverandøren, som er tilstrekkelig for å avdekke ikke-tjenstlige oppslag, innen 28. februar 2023.

Finanstilsynet ber om å få oversendt kopi av protokollen fra styremøtet hvor tilsynsrapporten blir behandlet.

Kopi av dette brevet bes sendt til bankens valgte revisor.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Stig Ulstein
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.