FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Sparebank 1 Lom og Skjåk
Sognefjellsvegen 4
2686 LOM

Vår referanse
24/5529
Deres referanse

01.04.2025

Tilsynsrapport

1 Innledning

Finanstilsynet gjennomførte stedlig tilsyn 16. og 17. september 2024 hos Sparebank 1 Lom og Skjåk (heretter omtalt "foretaket"). Formålet med tilsynet var å gjøre en vurdering av hvordan foretaket administrerer, utvikler, drifter, vedlikeholder og sikrer IKT-systemer og -tjenester.

Til grunn for disse merknadene ligger Finanstilsynets foreløpige rapport datert 06. desember 2024 og styrets kommentarer til rapporten i brev av 28. februar 2025.

2 Finanstilsynets merknader

Organisering

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 i § krav 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.

Videre stiller forskriften 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 presiserer forskriften kravene til internrevisjon.

Finanstilsynet pekte i foreløpig rapport på at bankens oppfølging av IKT-risiko var mangelfull, og pekte spesielt på at foretaket bør se på rollefordelingen i første- og andrelinje slik at behovet for risikostyring og kontroll knyttet til hele IKT-virksomheten blir tilstrekkelig ivaretatt. Videre pekte Finanstilsynet på at siden foretakets IKT-virksomhet i svært stor grad er utkontraktert stiller det særlig krav til foretakets forsvarslinjer som må utføre egne kontroller av IKT-tjenesteleveransene.

Styret oppgir i sitt svar at foretakets tre forsvarslinjer gjennomfører faste kontroller av IKT-tjenesteleverandører og underleverandører og at de har etablert et system for oppfølging og kontroll av kritiske og viktige IKT-tjenesteleverandører og underleverandører, som de vurderer som tilfredsstillende. Styret informerte om at de har tatt Finanstilsynets merknader i foreløpig rapport til etterretning, og har med bakgrunn i dette tilpasset periodiske rapporteringer fra foretakets første- og andrelinje til foretakets styre. Andrelinje vil i sin kontrollplan i større grad legge vekt på selvstendig vurdering av kvaliteten på de kontroller og den oppfølging som gjennomføres i førstelinje.

Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00
post@finanstilsynet.no
finanstilsynet.no

Saksbehandler
Hanne Teigland
Dir. tlf. 22 93 97 62

Finanstilsynet tar styrets svar til etterretning, men understreker at selv om IKT-virksomheten er helt eller delvis utkontraktert, er det foretaket som har ansvaret. Det er derfor viktig at foretaket gjennomfører kontroller av rapporteringen de mottar fra leverandør. Finanstilsynet forventer at foretaket, i tillegg til den operasjonelle oppfølgingen av leverandør, sørger for at kontroller gjennomføres og dokumenteres i de tre forsvarslinjene.

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 krav til at foretaket skal fastsette overordnede mål, strategier, og sikkerhetskrav for IKT-virksomheten.

Finanstilsynet pekte i foreløpig rapport på at styregodkjente styringsdokumenter på IKT-området, som strategier og policyer, må utarbeides i samsvar med forretningsstrategier og operasjonaliseres. Finanstilsynet pekte videre på at foretakets første forsvarslinje må etablere kriterier for å kunne vurdere operasjonaliseringen av de styrende dokumentene, og at bankens andrelinje har kontrolloppgaven med å følge opp de overordnede strategier og policyer for IKT-området.

Styret har i sitt svar opplyst at foretakets styrende dokumenter stiller krav til IKT-virksomheten, og at det gjennomføres periodiske lederbekreftelser, internkontrollrapportering og øvrig rapportering, som foretaket ikke fikk tydeliggjort under tilsynet. Styret oppgir at foretaket i tråd med Finanstilsynets forventning har etablert kriterier for å kontrollere operasjonaliseringen av kravene fastsatt i styrende dokumenter, og vil arbeide videre med aktiviteter og kontrollplaner for ytterligere å styrke kontroll med operasjonaliseringen.

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. Beredskapsplanene, som viser foretakets prioriteringer for gjenoppretting, bør formidles til relevante IKT-tjenesteleverandører. For å verifisere at det er etablert fungerende planer og løsninger må det foretas regelmessig opplæring, øvelse og testing, jf. IKT-forskriften § 11.

Finanstilsynet pekte i foreløpig rapport på at foretakets kriseplan, jf. IKT-forskriften § 11, ikke er basert på forretningsmessige prioriteringer. Finanstilsynet understreket at foretaket bør utarbeide virksomhetsmessig konsekvensanalyser som skal inneholde foretakets forretningsmessige prioriteringer, slik at resultatet benyttes til å stille krav til foretakets IKT-virksomhet om de ulike forretningsprosessers tilgjengelighetskrav. Dette for at kritikaliteten for systemene som inngår i de ulike forretningsprosessene identifiseres.

Styret skriver i sitt svarbrev at de er klar over risikoene som medfølger mangel på en virksomhetsmessig konsekvensanalyse og at foretaket er i prosess med utarbeidelse av en konsekvensanalyse for virksomheten. Styret mener at foretakets plan for gjennomføring av konsekvensanalysen og implementering av resultatene fra den vil ivareta gjeldende og framtidige krav til en virksomhetsmessig konsekvensanalyse, og at foretaket gjennom dette vil imøtekomme Finanstilsynets merknad.

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 av at kriseløsningen virker som forutsatt. Resultatet av øvelsen og testingen skal dokumenteres.

Finanstilsynet pekte i foreløpig rapport på at foretaket selv er ansvarlig for at opplæring, øvelse og testing av foretakets kriseløsning gjennomføres årlig. Når den virksomhetsmessige konsekvensanalysen foreligger, må beredskapsplaner oppdateres slik at de samsvarer med resultatene fra 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.

I sitt svar viser styret til foretakets arbeid med krav til hvordan test av kriseløsninger hos IKT-tjenesteleverandører og underleverandører skal gjennomføres. Som nevnt over har foretaket startet arbeidet med en konsekvensanalyse for virksomheten og har planlagt å oppdatere planverket for beredskap i tråd med resultatene fra konsekvensanalysen.

Finanstilsynet tar styrets svar til etterretning.

Videre kommenterte Finanstilsynet i foreløpig rapport at ved testing av beredskapsplaner, både for foretakets egne og for utkontrakterte IKT-tjenester, må relevante informasjonssikkerhetsscenarioer inngå. Informasjonssikkerhetsscenariene bør inkludere verstefallscenarioer. Beredskapstestingen bør omfatte scenarioer med langvarig utilgjengelighet av tjenester slik at planverk for gjenoppretting og alternativ drift inngår i testingen. Det er først når testingen av relevante scenarioer er utført, foretaket har dokumentasjon på at tilgjengelighetskrav er ivaretatt.

Styret skriver i sitt svar at de vurderer foretakets valgte scenarioer som svært relevant sett i lys av erfaringer fra tidligere hendelser samt systemets kritikalitet og kompleksitet. Videre viser styret til at foretaket har evaluert gjennomføring og resultatet av øvelsen som vil bli brukt i utforming av framtidige løsninger.

Finanstilsynet tar styrets svar til etterretning, men presiserer at det er viktig at foretaket vurderer scenarioer der planverk for gjenoppretting og alternativ drift blir testet ved langvarig nedetid og hendelser som avviker fra det foretaket erfaringsmessig opplever.

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 IKT-tjenesteleverandørens aktiviteter, samt Finanstilsynets tilgang til opplysninger og mulighet for å føre tilsyn hos IKT-tjenesteleverandøren. Videre framgår det av samme paragraf 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 utkontrakteringsforholdet og en beskrivelse av hvordan foretaket skal sikre leveransene.

Foretaket har ansvar for styring og kontroll også der hele eller deler av virksomheten er utkontraktert, jf. IKT-forskriften § 12 første ledd. Det framgår av bestemmelsen at foretaket må sikre at organisasjonen, i egen regi eller gjennom formalisert samarbeid med andre foretak enn IKT-tjenesteleverandøren, har tilstrekkelig kompetanse til å forvalte utkontrakteringsavtalene.

Foretaket har utkontraktert store deler av IKT-virksomheten, hvor hovedleverandørene får størst oppmerksomhet i foretakets oppfølging av IKT-tjenesteleveranser. I foreløpig rapport pekte Finanstilsynet på at foretakets HR-system er en utkontraktert tjeneste som er avgjørende for kontroll på tilgangsstyring i foretaket og at leverandøren av denne tjenesten ikke blir fulgt opp i henhold til foretakets etablerte prosedyrer for oppfølging og styring av IKT-leveranser fra eksterne IKT-tjenesteleverandører.

Styret skriver i sitt svar at foretaket tar til etterretning at kritikalitetsnivået fastsatt for tilgangs-systemet vurderes å smitte over på HR-systemet, og foretaket har derfor påbegynt prosess med å gjøre en ny vurdering av kritikalitetsnivået. Deretter vil foretaket oppdatere prosess for oppfølging av IKT-tjenesteleverandøren.

Finanstilsynet tar styrets svar til etterretning.

Foretaket, sammen med de andre foretakene i norsk betalingsinfrastruktur, har utkontraktert felles tjenester som inngår i rammeavtalen for felles operasjonell infrastruktur.

I foreløpig rapport pekte Finanstilsynet på at oppfølging av disse utkontrakterte IKT-tjenestene er av stor viktighet for foretaket og at det bør etableres egne prosedyrer for dette. Prosedyrene skal sikre at partenes forpliktelser, for eksempel nødvendig kapasitet, sikkerhet, overvåkning, kompetanse og krav til kontinuitet er etablert. Alle tekniske og organisatoriske grenseflater mot avtalepartene bør også dokumenteres. Finanstilsynet pekte videre på at selv om de utkontrakterte IKT-tjenestene er fellestjenester eller tjenester levert av underleverandører, har foretaket oppfølgingsansvar for kjøp og bruk av tjenestene.

Styret skriver i sitt svar at også utkontrakterte tjenester for felles betalingsinfrastruktur følges opp på strategisk, taktisk og operasjonelt nivå. Styret ser at det er behov for å formalisere og dokumentere foretakets oppfølging av utkontrakterte tjenester. Foretaket har igangsatt et DORA-prosjekt hvor leverandørstyring vil være sentralt.

Finanstilsynet tar styrets svar til etterretning.

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. Foretaket har ansvar for risikostyring og internkontroll også der hele eller deler av virksomheten er utkontraktert, jf. IKT-forskriften § 12. Det framgår av bestemmelsen at foretaket må sikre at IKT-tjenesteleverandørers aktiviteter kontrolleres. 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. Finanstilsynets vurdering er at dette omfatter oppdaterte oversikter over IT-systemer, nettverksenheter, databaser, etc. og at utstyrsoversikten bør inneholde tilstrekkelige konfigurasjonsdata og angi avhengigheter mellom utstyr/komponenter.

I foreløpig rapport ba Finanstilsynet foretaket sikre at IKT-tjenesteleverandørene etterlever sikkerhetskravene som foretaket har besluttet i egen sikkerhetspolicy. Dette inkluderer sårbarhetsstyring med krav til oppdateringer, håndtering av ikke-supportert maskin- og programvare, livssyklushåndtering med krav til anskaffelser/avhending av utstyr, med mer.

Styret viser i sitt svar til at foretaket har tilgang til detaljerte utstyrsoversikter for sine største leverandører, men erkjenner at det er et forbedringspotensial knyttet til utforming og oppfølging av sikkerhetskravene som foretaket har besluttet i egen sikkerhetspolicy. Styret oppgir at foretaket framover vil sørge for at styringsdokumentet blir oppdatert for å sikre etterlevelse av gjeldende og framtidige krav.

Finanstilsynet tar styrets svar til etterretning.

Tilgangsstyring

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 IT-systemene.

Finanstilsynet pekte i foreløpig rapport på at foretakets styring og kontroll med tilganger, også ved bruk av IKT-tjenesteleverandører og ved utkontraktert IKT-virksomhet, ikke er tilstrekkelig, da det gir muligheter for å misbruke tilgangen til ikke-tjenstlige oppslag som vanskelig lar seg avdekke. Finanstilsynet pekte på at foretaket må sikre at IKT-tjenesteleverandør etablerer løsninger for tilgangsstyring og kontrollrutiner som i størst mulig grad sørger for at tilganger tildeles og kontrolleres for det enkelte oppdrag.

Styret skriver i sitt svar at foretaket de siste årene har hatt særlig stor oppmerksomhet på oppfølging av tilganger til ansatte i foretaket, og mener at tildeling og kontroll av tilganger til ansatte blir håndtert på en tilfredsstillende måte. Styret erkjenner at det er et forbedringspotensial i oppfølging av tildeling og kontroll av tilganger hos leverandører, men viser til at foretaket utfører kontroller av tildeling av tilganger hos leverandører som foretaket har utkontraktert tjenester til.

Finanstilsynet tar styrets svar til etterretning og forventer at foretaket gjennomfører tiltak for å redusere risikoen med permanente tilganger hos leverandør.

Hendelsesrapportering

Operasjonelle hendelser som medfører vesentlig reduksjon i funksjonalitet som følge av brudd på konfidensialitet, integritet eller tilgjengelighet til IKT-systemer og/eller data skal uten ugrunnet opphold rapporteres til Finanstilsynet, jf. IKT-forskriften § 9 tredje ledd. Foretaket skal rapportere hendelser som foretaket selv kategoriserer som alvorlig eller kritisk. Videre forventer Finanstilsynet at foretaket rapportere andre avvik dersom disse avdekker spesielle sårbarheter i applikasjon, arkitektur, infrastruktur eller forsvarsverk. EBAs retningslinjer for IKT og sikkerhet beskriver nærmere hvilke krav som stilles til deteksjonsløsninger og hendelseshåndtering.

Finanstilsynet pekte i foreløpig rapport på at foretaket må sikre at policyer og rutiner for hendelses-håndtering inneholder oppfølging av tiltak som IKT-tjenesteleverandør etablerer i forbindelse med IKT-hendelser.

Styret skriver i sitt svar at foretaket deltar aktivt i håndtering av hendelser hos IKT-tjenesteleverandører gjennom etablert struktur for beredskap i alliansen, men ser det er forbedringspotensial knyttet til foretakets oppfølging og kontroll av tiltak i leverandørkjeden i etterkant av hendelser. Styret ser behov for å tydeliggjøre de styrende dokumentene knyttet til hendelseshåndtering slik at etablert prosess formaliseres og forberedes ytterligere.

Finanstilsynet tar styrets svar til etterretning og legger til grunn at foretakets styrende dokumenter framover legger føringer for oppfølging og kontroll av tiltak i etterkant av hendelser.

Endringsledelse

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. Foretaket skal videre sikre at prosedyrene for endringshåndtering gir en stabil, planlagt og forutsigbar drift.

Finanstilsynet pekte i foreløpig rapport på at foretaket bør etablere en egen prosess med rutiner for håndtering av endringer for å sikre at det er foretaket som står som eier og ansvarlig for alle endringer som innføres i foretakets IKT-virksomhet.

Styret viser i sitt svar til at foretaket har en etablert prosess for godkjenning av nye produkter og prosesser. Styret viser til at Finanstilsynets merknad omhandler håndtering av endringer i foretakets IKT-infrastruktur, som ikke er omfattet av denne rutinen. Styret informerer i sitt svar om at foretaket er i gang med etablering av rammeverk for endringsprosessen, som vil ha en

risikobasert tilnærming av endringshåndtering og har som mål å sikre at foretaket i tilstrekkelig grad kvalitetssikrer planlagte endringer før iverksettelse. Styret viser til at foretaket, gjennom den formaliserte prosessen, vil påse at foretaket står som eier og ansvarlig for endringer som innføres i foretakets IKT-virksomhet.

Finanstilsynet tar styrets svar til etterretning og legger til grunn at en formell endringsprosess som omfatter alle endringer som omfatter foretaket etableres, herunder endringer som utføres av tjenesteleverandør.

Vi ber foretaket sende kopi av dette brevet til valgt revisor.

For Finanstilsynet

Olav Johannessen
seksjonsleder

Hanne Teigland
rådgiver

Dokumentet er godkjent elektronisk.