FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Styret i SPAREBANKEN VEST
Postboks 7999
5020 BERGEN

Vår referanse
24/3852
Deres referanse

18.02.2025

Tilsynsrapport

1 Innledning

Finanstilsynet gjennomførte IKT-tilsyn 10. og 11. juni 2024 med Sparebanken Vest (heretter omtalt "foretaket"). Formålet med tilsynet var å gjøre en vurdering av hvordan foretaket administrerer, utvikler, drifter, vedlikeholder og sikrer IKT-systemer og -tjenester. For dette området så tilsynet på styring med og kontroll av IKT-virksomheten. Tilsynet vektla systemløsninger som støtter foretakets kjernevirksomhet og prioriterte IKT-systemer som foretaket har utkontraktert.

Til grunn for disse merknadene ligger Finanstilsynets foreløpige rapport datert 16. september 2024 og styrets kommentarer til rapporten i brev av 12. desember 2024, signert av Konserndirektør Risk Management på vegne av styret.

2 Finanstilsynets merknader

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 om at foretaket skal ha en uavhengig kontroll-funksjon 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.

IKT-forskriften § 2 første ledd presiserer at IKT-virksomheten skal utføres på en betryggende måte, mens tredje ledd har bestemmelser om at det skal oppnevnes ansvarlige i foretaket for de ulike delene av IKT-virksomheten.

Finanstilsynet understreket i foreløpig rapport at styret må vurdere, og håndtere, mulige interesse-konflikter mellom ulike roller som innehas av samme person. Når flere roller tillegges én person

Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

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

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

kreves særlig bevissthet og aktsomhet for å unngå mulige interessekonflikter og sikre at andrelinjens uavhengighet ivaretas. Styret skriver i sitt svarbrev at det er en problemstilling som foretaket har oppmerksomhet på, og etter styrets vurdering legger foretakets policy for informasjonssikkerhet til rette for en adekvat håndtering av interessekonflikter. Finanstilsynet har videre merket seg styret kommentar at det i forbindelse med sammenslåingen med Sparebanken Sør er en klar målsetning å etablere en funksjon med ansvar for informasjonssikkerhet med større uavhengighet i andrelinjefunksjonen.

Finanstilsynet stilte i foreløpig rapport spørsmål ved hvordan foretaket sikrer at risikokontrollfunksjonen i andre forsvarslinje har tilstrekkelig ressurser til å kunne kontrollere og stille krav til førstelinjen på IKT-området. Finanstilsynet merker seg at det er styrets vurdering at kontrollfunksjonene p.t. har tilstrekkelig ressurser inn mot dette området, men at dette er noe som løpende vurderes i foretaket. Finanstilsynet har videre notert seg at ressursallokering er et sentralt tema som nå underlegges en vurdering i forbindelse med sammenslåingen med Sparebanken Sør.

Finanstilsynet stilte videre spørsmål om ressursbruken til intern revisor står i forhold til foretakets størrelse og risikoprofil, herunder den digitale satsningen og kompleksiteten på IKT-området, og om avsatte internrevisjonsressurser er tilstrekkelig for å kontrollere at foretaket er organisert og drives på en forsvarlig måte og i samsvar med gjeldende krav til virksomheten. Finanstilsynet stilte også spørsmål om hvor stor del av det totale timebruket for 2024 som var reservert oppfølging av IKT-risiko. Finanstilsynet har notert seg at styret vurderte ressursuttaket som inngikk i årsplanen for 2024 som adekvat, og at det i forbindelse med årsplanen for 2025 vil ta med seg kommentarene fra Finanstilsynet. Videre kommenterer styret at ressursuttaket vil bli underlagt en grundig vurdering i forbindelse med sammenslåingen med Sparebanken Sør.

Finanstilsynet merker seg styrets kommentarer til foretakets organisering av virksomheten. Finanstilsynet forutsetter at styret, uavhengig av fusjonsprosessen, er bevisst sitt ansvar for forsvarlig organisering av virksomheten.

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.

Finanstilsynet kommenterte i foreløpig rapport at en finner det kritikkverdig at foretaket før april 2024 ikke hadde en strategi for styring av en så vesentlig risiko som IKT-risiko. Styret tar Finanstilsynets kommentar til etterretning, men understreker i svarbrevet at styring av IKT-risiko var tilfredsstillende forankret i et sett av risikostrategier og øvrige styringsdokumenter også før april 2024. Finanstilsynet har merket seg at det er viktig for foretaket å videreutvikle foretakets rammeverk på området, ikke minst i lys av den kommende fusjonen, og tar styrets kommentarer til etterretning.

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-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 stilte Finanstilsynet spørsmål ved om styret mottar adekvat informasjon om foretakets IKT-virksomhet. Finanstilsynet noterer fra styrets svarbrev at det fra og med tredje kvartal 2024 rapporteres til styret i henhold til styrevedtatte KPI'er for henholdsvis risikoappetitt og -toleranse, og at rapporten er utvidet med førstelinjerapportering. Styret kommenterer videre at det nå vurderer at foretaket har en tilfredsstillende rapportering inn mot konsernledelse og styret, men at det er naturlig at det vil bli ytterligere forbedringer og justeringer fremover. Det både som følge av at foretaket høster erfaring, tilpasning til DORA samt sammenslåingen med Sparebanken Sør.

Finanstilsynet tar styrets svar til etterretning.

IKT-drift

Ifølge IKT-forskriften § 8 første ledd skal driften av IKT-virksomhet være basert på dokumenterte prosedyrer. Prosedyrene skal sikre fullstendig, rettidig og korrekt behandling og oppbevaring av data. Foretaket skal ha dokumenterte driftsløsninger for IKT-virksomheten, jf. § 8 annet ledd. Driftsløsningene skal sikre tilgjengelighet i tråd med foretakets dokumenterte krav. For å motvirke avvik i IKT-systemene, som vil påvirke oppnåelsen av foretakets dokumenterte krav, skal foretaket gjennomføre regelmessige analyser og tiltak, jf. § 8 annet ledd annet punktum. Foretaket skal videre teste og dokumentere at driften fungerer i henhold til foretakets dokumenterte krav, jf. § 8 tredje ledd.

Finanstilsynet pekte i foreløpig rapport på at foretakets driftsprosesser for intern drift i liten grad var dokumenterte, og at foretaket eksempelvis ikke synes å ha dokumenterte prosedyrer som sikrer fullstendig, rettidig og korrekt håndtering av data. Finanstilsynet ba foretaket dokumentere drifts-prosedyrene i samsvar med IKT-forskriftens § 8. Styret skriver i sitt svarbrev at foretaket nå skal revidere, ettergå og samle all dokumentasjon på en egnet plass og sikre at dette tilgjengeliggjøres for relevant personell på en enkel måte. Aktivitetene vil samkjøres med aktivitetene i integrasjons-programmet.

Finanstilsynet legger til grunn at foretakets IKT-virksomhet skal basere seg på dokumenterte prosedyrer i samsvar med IKT-forskriftens § 8.

Virksomhetsmessig konsekvensanalyse

Ifølge IKT-forskriften § 13 skal det foreligge oppdatert dokumentasjon av det enkelte IKT-system som er av betydning for foretakets virksomhet. Hensiktsmessige planer og tiltak for tilgjengelighet og kontinuitet bør etableres med utgangspunkt i konsekvensanalyser for foretakets kritiske forretningsprosesser. Virksomhetsmessig konsekvensanalyse skal bidra til å sikre at foretakets beredskapsplaner utarbeides med basis i forretningsmessig kritikalitet. Planene skal basere seg på foretakets prioriteringer for gjenoppretting av forretningskritiske 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.

I foreløpig rapport pekte Finanstilsynet på at foretaket hadde mangler i sin etterlevelse av kravene i IKT-forskriften § 11 vedrørende driftsavbrudd og kriseberedskap da foretaket ikke hadde gjennomført en virksomhetsmessig konsekvensanalyse. Finanstilsynet tar styrets svar om at foretaket nå har gjennomført en ny konsekvensanalyse av hele virksomhetens kritiske funksjoner og prosesser 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.

Finanstilsynet pekte i foreløpig rapport på at gjennomførte beredskapstester i stor grad var basert på enkeltscenarioet der ett datasenter blir utilgjengelig, og at alternativt datasenter tar over driften, en såkalt 'fail-over' test. Verstefallscenarioer var ikke inkludert i beredskapstestingen, verken for foretakets egne eller for utkontrakterte IKT-tjenester, og tilsynet pekte på at det først er når testingen av relevante scenarioer er utført at foretaket har dokumentasjon på at tilgjengelighets-krav er ivaretatt. Styret opplyser i sitt svarbrev at foretaket er i dialog med hovedleverandør for å øke antall testscenarioer, inkludert verstefallsscenarioer, og det er enig i at fremtidige øvelser og tester må omfatte leverandører og teste verstefallsscenarioer. Styret opplyser videre at planen er å etablere en tydelig sammenheng mellom virksomhetsmessig konsekvensanalyse og beredskaps-scenarioene som skal underlegges øving, og at dette vil med på øvingsplanen for 2025.

Finanstilsynet har merket seg styrets svar. Finanstilsynet forutsetter at foretaket gjennomfører de tiltakene foretaket er i dialog med hovedleverandør om inkludert testing, samt etablerer en tydelig sammenheng mellom virksomhetens konsekvensanalyse og beredskapsscenarioene.

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/revidere leverandørens aktiviteter, samt Finanstilsynets tilgang til opplysninger og mulighet for å føre tilsyn hos IKT-leverandøren. Videre framgår det av § 12 at foretaket har ansvar for at IKT-virksomheten oppfyller alle krav som stilles i forskriften og at dette gjelder også der hele eller deler av IKT-virksomheten er utkontraktert. Av bestemmelsene i § 13 framgår det at foretaket skal sikre at det har en samlet oppdatert dokumentasjon over organisasjon, utstyr, IKT-systemer og vesentlige forhold i IKT-virksomheten.

Det var Finanstilsynets vurdering i foreløpig rapport at foretakets oppfølging av utkontraktert virksomhet var mangelfull da foretaket manglet en detaljert oversikt over alle komponenter som inngår i infrastrukturen, herunder maskinvare og programvare, som inkluderte komponentenes sikkerhetsstatus. Styret skriver i sitt svarbrev at foretaket har tilfredsstillende oversikt over egne og leverandørers sikkerhetskomponenter, herunder status, men ser at denne oversikten er noe fragmentert. Foretaket er derfor i prosess med å utvikle et sett med interne registre som vil gi bedre oversikt og grunnlag for mer detaljert oppfølging og dialog med underleverandører.

Det var videre Finanstilsynets vurdering at foretaket ikke fulgte opp at IKT-tjenesteleverandører hadde etablert gode rutiner og kontroller for konfigurasjonsstyring av de tjenester som inngår i leveransene til foretaket. Av styrets svarbrev framgår det at foretaket har startet en dialog med hovedleverandører for å styrke og videreutvikle de regelmessige kontrollene over komponentene i infrastrukturen, og at kontrollaktivitetene vil bli strukturert i en årsplan som trer i kraft fra januar 2025. Styret skriver videre at mer presise registre og mer systematisk kontrollarbeid, samlet i en kontrollplan, vil etter foretakets vurdering styrke foretakets risikostyring innenfor de områdene som Finanstilsynet adresserer.

Finanstilsynet har merket seg styrets svar. Finanstilsynet legger til grunn at omtalte tiltak blir iverksatt.

Endring- 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. Foretaket skal videre sikre at prosedyrene for endringshåndtering gir en stabil, planlagt og forutsigbar drift. Prosedyrene for avvikshåndtering skal omfatte alle avvik som oppstår i driften av IKT-systemene. Videre skal avviksbehandlingen identifisere årsaken til avvik, hindre gjentagelse og sikre forsvarlig og formell behandling av avviket. Avvikene skal dokumenteres og prosedyrene skal inneholde retningslinjer for eskalering.

Finanstilsynet ba i foreløpig rapport foretaket etablere og dokumentere en egen prosess med rutiner for håndtering av endringer da foretaket manglet en egen dokumentert endringsprosess. Den bør inkludere standardendringer som Finanstilsynet har erfart kan feile og føre til alvorlige hendelser, endringer som gjennomføres i DevOps-prosessen og endringer i maskinlærings- og kunstig intelligensalgoritmer. Styret bekrefter i sitt svarbrev at foretaket vil revidere utviklingsrutinen i lys av innspillene fra Finanstilsynet.

Videre ba Finanstilsynet i foreløpig rapport foretaket sørge for at prosedyre for avvikshåndtering sikrer at oppfølging inkluderer rapportering av tiltak som etableres som følge av avviket. Det gjelder også for utkontraktert IKT-virksomhet. Foretaket vil ifølge styrets svarbrev gjennomgå rutineverk for hendelsesrapportering i forbindelse med DORA og vil da oppdatere rutineverket for hendelsesrapportering. Det vil sikre at foretaket også inkluderer rapportering av tiltak som etableres som følge av avviket, både for egen og utkontraktert virksomhet. Foretaket vil framover inkludere tiltaksbeskrivelser, inklusiv sekundering, i førstelinjerapporteringen som også legges fram for konsernledelse og styret.

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. 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 pekte i foreløpig rapport at foretakets sikkerhetspolicy ikke benyttes som utgangspunkt for krav som stilles til leverandører og underleverandører. Foretaket presenterte som en del av tilsynet lister med krav som skal følges internt i foretaket, men disse kravene benyttes ikke ut mot leverandører med en tilhørende forventning om at samme standard opprettholdes av leverandører. Finanstilsynets vurdering var at det er viktig at foretaket sikrer at krav, blant annet fra sikkerhets-policyen for den interne organisasjonen, også gjøres gjeldende for leverandører. Finanstilsynet merker seg at foretaket sier seg enig i Finanstilsynets vurdering, og vil sørge for at kravene gjøres gjeldende for leverandører. Foretaket har utviklet et kontraktvedlegg med informasjonssikkerhetskrav som vil bli knyttet til leverandørenes kontrakter i forbindelse med revisjonen av kontrakter som følger innføring av DORA.

Finanstilsynet tar styrets svar til etterretning.

Som det framgår av angjeldende rapport avdekket tilsynet til dels vesentlige mangler ved foretakets styring med og kontroll av IKT-virksomheten. Finanstilsynet har merket seg fra styrets svarbrev at foretaket har og vil iverksette en rekke tiltak i løpet av første og andre kvartal 2025 for å bedre foretakets styring med og kontroll av sin IKT-virksomhet. *Finanstilsynet ber styret bekrefte innen **31. august 2025** at alle tiltak omtalt i styrets svarbrev er gjennomført og med forventet resultat.*

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

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

For Finanstilsynet

Olav Johannessen
seksjonsleder

Irene Støback Johansen
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk.