FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Styret i ASKIM & SPYDEBERG SPAREBANK
Postboks 143
1801 ASKIM

Vår referanse
25/2822
Deres referanse

16.10.2025

Tilsynsrapport

1 Innledning

Finanstilsynet gjennomførte stedlig IKT-tilsyn i Askim & Spydeberg Sparebank (heretter omtalt foretaket) den 28. april 2025.

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

Til grunn for tilsynsrapporten ligger Finanstilsynets foreløpige rapport datert 1. juli 2025 og styrets kommentarer til rapporten i brev av 12. september 2025. Tilsynsrapporten er utarbeidet med utgangspunkt i IKT-forskriften, som var gjeldende regelverk for foretaket på tilsynstidspunktet. Fra 1. juli 2025 skal foretaket etterleve DORA-forordningen med tilhørende delegerte kommisjonsforordninger, jf. DORA-loven § 1.

2 Finanstilsynets oppsummering

Tilsynet avdekket ingen vesentlige mangler ved foretakets styring med og kontroll av IKT-virksomheten. Det ble likevel påpekt mangelfull oppfølging av styregodkjente styringsdokumenter, samt at rutiner for enkelte områder, som sikkerhetspatching og oppfølging av logger, ikke var tilstrekkelig etablert. Videre ble det avdekket mangler i vurdering og dokumentasjon av leverandørers beredskapstester, mangler i rutinene for leverandøroppfølging og forbedringsområder i endringshåndteringen.

3 Finanstilsynets vurderinger

3.1 Strategi og organisering

Styret skal godkjenne og regelmessig vurdere retningslinjer for å påta foretaket risikoer og for å identifisere, styre, overvåke og kontrollere risikoene, jf. CRR/CRD-forskriften § 35. IKT-forskriften § 2 første ledd stiller videre krav til at foretaket skal fastsette overordnede mål, strategier, og sikkerhetskrav for IKT-virksomheten, og i § 3 første ledd stilles det krav om at foretaket skal fastsette kriterier for akseptabel risiko forbundet med bruk av IKT-systemene.

Finanstilsynet pekte i foreløpig tilsynsrapport på sine forventninger om at styregodkjente styringsdokumenter følges opp for å sikre at foretakets planer og drift utføres i henhold til disse. I tillegg forventes det at foretakets andre- og tredjelinje følger opp etterlevelse av strategier, og kontrollerer at de styrende dokumentene er operasjonalisert i henhold til disse.

Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

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

Saksbehandler
Snorre Vik Sanfelt
Dir. tlf. 22 93 97 08

Styret skriver i sitt svar at foretaket gjennomfører en årlig gjennomgang av status opp mot strategien i foretakets overordnede ROS-analyse, som inkluderer IKT-området. Videre svarer styret at foretakets policydokument er operasjonalisert gjennom underliggende retningslinjer på IKT-området, som løpende kontrolleres av foretakets første- og andrelinje i henhold til foretakets internkontrollplan.

Finanstilsynet tar styrets svar til etterretning, men peker på at det er viktig at det rapporteres på operasjonalisering av målene i strategiske dokumenter. Dette gjelder både foretakets egne og styrevedtatte alliansedokumenter.

3.2 Kontrollfunksjoner og rapportering

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.

Finanstilsynet forventer at IKT-risiko løpende identifiseres, styres, overvåkes og kontrolleres. Videre forventer Finanstilsynet at vurderingen av IKT-risikoen opp mot styrevedtatte måltall, rammer og/eller krav inkluderes i foretakets faste rapporter som går til styret.

3.2.1 Behandling av "gule risikoer"

I foreløpig rapport stilte Finanstilsynet spørsmål ved at en rekke gule risikoer fortsatt sto som gule, selv etter at risikoreduserende tiltak var gjennomført. Videre spurte Finanstilsynet styret om hvordan antallet gule risikoer samsvarte med den styrevedtatte risikotoleransen på IKT-området.

Styret erkjenner at definisjonen av lav risikotoleranse kan være noe snever, slik at den potensielt ikke fanger opp det totale risikobildet på IKT-området. Styret skriver at foretaket vil utvide definisjonen for å sikre bedre gjenspeiling av faktisk risikonivå.

Finanstilsynet tar styrets svar til etterretning.

3.2.2 Andre forsvarslinjes IKT-rapportering

I foreløpig rapport pekte Finanstilsynet på at rapportene fra andrelinjen i hovedsak gjengir informasjon fra førstelinjen, og stilte spørsmål ved andrelinjens rapportering av IKT-risiko og etterlevelse av IKT-regelverket. Finanstilsynet stilte også spørsmål ved om styret mottar tilstrekkelig informasjon på området.

Styret skriver i sitt svar at styret er usikker på grunnlaget for Finanstilsynets bemerkning om at andrelinjerapporteringen i hovedsak gjengir informasjon fra førstelinjen. Styret redegjør i sitt svar for rapporteringen fra andrelinjen, herunder datagrunnlaget for rapportene. Foretaket viser til at det krysshenvises mellom rapportene til første- og andrelinje med den hensikt å unngå dobbelt-rapportering. Rapporteringene har ulike datapunkter og formålet med henvisningene er å gi styret et bredt bilde av status på IKT-området, uten at det i for stor grad forårsaker gjentakelser og dobbeltrapportering.

Finanstilsynet kan av styrets svar ikke se om styret vurderer informasjonen fra andrelinjen som tilstrekkelig, men legger dette til grunn basert på styrets redegjørelse.

3.3 IKT-drift

Ifølge IKT-forskriften § 8 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. 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. Foretaket skal videre teste og dokumentere at driften fungerer i henhold til foretakets dokumenterte krav.

3.3.1 Dokumentasjon av IKT-virksomheten

Finanstilsynet viste i foreløpig rapport til delvis overlappende informasjon i ulik dokumentasjon av IKT-virksomheten, og anbefalte å rendyrke dokumentasjonen i retningslinjer/rutiner på de enkelte IKT-områdene.

Finanstilsynet har fra styrets svar merket seg at foretaket i forbindelse med implementeringen av DORA-forordningen har etablert et nytt rammeverk på IKT-området, der dokumentasjonen av IKT-virksomheten er rendyrket i retningslinjer og policydokumenter på IKT-området.

3.4 Endringshåndtering

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.

3.4.1 Rutine for vurdering av forhåndsgodkjente endringer

I foreløpig rapport viste Finanstilsynet til foretakets rutine for endringshåndtering og definisjonen av forhåndsgodkjente endringer i denne. Videre etterspurte Finanstilsynet krav, blant annet basert på erfaringer fra hendelser som har oppstått, til at det gjøres regelmessige, eksempelvis årlige, vurderinger av hva som kan kvalifiseres som forhåndsgodkjente endringer.

Styret forklarer i sitt svar at de ikke har hatt praksis for årlig å revidere forhåndsgodkjente endringer. Etter tilsynet har foretaket imidlertid inkludert et punkt i skjemaet for leverandør-oppfølging, hvor revidering av forhåndsgodkjente endringer vurderes.

Finanstilsynet tar styrets svar til etterretning.

3.4.2 Hendelser etter endringer

Finanstilsynet stilte i foreløpig rapport spørsmål knyttet til å forstå sammenhengen mellom endringer og hendelser, basert på mottatte lister over endringer og over hendelser.

Styret informerer i sitt svar at det registreres på hendelsen og ikke på endringen om en endring har medført avvik/hendelser. Endringsoversikten vil derfor ikke vise om endringen medførte avvik. Styret viser videre til at gjennomgang av hendelser de siste 12 månedene er et fast punkt i foretakets leverandøroppfølging. Dette innebærer at endringer som har medført feil vurderes løpende i oppfølgingen av foretakets leverandører.

Finanstilsynet mener at en kvalitetsindikator for endringshåndteringen er graden av hendelser som oppstår som følge av endringer. Finanstilsynet anbefaler foretaket å tydeliggjøre om endringer har medført avvik/hendelser.

3.5 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 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. Foretaket skal videre ha en samlet og oppdatert oversikt over alle avtaler om utkontraktering av virksomhet. Det følger av meldepliktforskriften § 1.

3.5.1 Mangelfulle rutiner for oppfølging av leverandører

Finanstilsynet viste i foreløpig rapport til at foretakets kvartalsvise rapport fra førstelinjen til ledelsen har utfyllende referanser til rapporteringen fra leverandørene, og til at foretaket har utarbeidet et skjema som understøtter en prosess for leverandøroppfølging som sikrer en strukturert oppfølging av leverandørene. Til tross for dette kunne ikke Finanstilsynet se at foretaket hadde rutiner som i detalj beskrev kravene til rapportering fra leverandørene, inkludert hvordan foretaket skal følge opp informasjonen i rapportene.

Styret viser i sitt svar til at foretakets retningslinjer for utkontraktering beskriver de generelle kravene til leverandørene, at frekvens på oppfølgingen skal avhenge av leverandørens kritikalitet, og at dette er operasjonalisert i nevnte skjema for leverandøroppfølging.

Finanstilsynet har merket seg at krav til leverandøroppfølgingen er nærmere beskrevet i et eget kapittel i de nye retningslinjene foretaket har utarbeidet etter innføringen av DORA-forordningen i norsk rett. Retningslinjene var vedlagt styrets svar, og Finanstilsynet tar dette til etterretning.

3.6 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.[1]

3.6.1 Retningslinjer og rutiner for patching

Finanstilsynet stilte i foreløpig rapport spørsmål om status på sikkerhetspatching er innenfor foretakets risikotoleranse og videre om foretakets gjeldende retningslinjer og rutiner for sikkerhetspatching.

Finanstilsynet har merket seg styrets svar som redegjør for status på sikkerhetspatching, og at foretakets vurdering er at statusen er innenfor foretakets risikotoleranse. Finanstilsynet kan av styrets svar ikke se at foretaket har bekreftet at foretaket har retningslinjer og rutiner for sikkerhetspatching. Finanstilsynet forventer at foretaket etablerer dette.

I DORA-forskriften som omfatter utfyllende regelverk etter DORA-forordningen, er det i teknisk reguleringsstandard (RTS) 2024/1774 art.10 spesifiserte krav til håndtering av sårbarheter.

[1] EBA Guidelines on ICT and security risk management, EBA/GL/2019/04

3.6.2 Manglende rutine for oppfølging av logger

Finanstilsynet pekte i foreløpig rapport på at foretaket bør ha en rutine der foretakets krav til logging og oppfølging av loggene framgår, særlig knyttet til brukere med tilgang til sensitive systemer og data. Kravene må også gjøres kjent for leverandørene, og leverandørene må forplikte seg til å etterleve dem.

Styret viser i sitt svar til at foretaket har utkontraktert oppgavene knyttet til logging og oppfølging. Videre opplyses det at foretaket gjennomgår kriteriene for loggføring som et ledd i avtaleinngåelse, og at leverandørens gjennomføring testes gjennom foretakets testprogram.

Etter Finanstilsynets vurdering skal foretaket ha egne retningslinjer som beskriver foretakets krav til logging, uavhengig av leverandører, og som man kan måle leverandørenes etterlevelse mot. Finanstilsynet forventer at foretaket etablerer dette.

I DORA-forskriften som omfatter utfyllende regelverk etter DORA-forordningen, er det i teknisk reguleringsstandard (RTS) 2024/1774 art.12 spesifiserte krav til loggføring.

3.7 Beredskap

I IKT-forskriften § 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 testen skal dokumenteres, jf. IKT-forskriften § 11 tredje ledd.

Finanstilsynet presiserer at foretaket selv er ansvarlig for at opplæring, øvelse og testing av foretakets kriseløsning gjennomføres årlig, samt oppfølging av IKT-tjenesteleverandører for å sikre at de overholder kravene i IKT-forskriften § 11. Det er viktig at test av kriseløsningen gjennomføres på foretaksnivå og at foretaket gjør testene relevante for foretaket, både med omfang og relevante scenarioer for å vurdere egnetheten til kriseløsningen og robustheten til egen organisasjon og relevante IKT-tjenesteleverandører.

3.7.1 Virksomhetens konsekvensanalyse som utgangspunkt ved kravstilling

I foreløpig rapport vurderte Finanstilsynet at ved testing av beredskapsplaner, for foretakets egne og for utkontrakterte IKT-tjenester, må foretakets dokumenterte krav i virksomhetens konsekvensanalyse testes og trenes på. Det er på denne måten foretaket kan få bekreftet at forretningens behov er ivaretatt. Finanstilsynet anmodet foretaket i større grad om å harmonisere beredskapsarbeidet med virksomhetens konsekvensanalyse og anvende dette i kravstilling mot relevante leverandører.

Styret skriver i sitt svar at i forbindelse med implementering av DORA-forordningen har det blitt etablert en ny plan for krisehåndtering. Denne krisehåndteringsplanen tar utgangspunkt i virksomhetens konsekvensanalyse ved fastsettelse av kriterier for krise, minimumsdrift, prioritering ved gjenoppretting og vilkår for vellykket gjenoppretting.

Finanstilsynet tar styrets svar til etterretning.

3.7.2 Foretakets vurdering av beredskapstester

Finanstilsynet pekte videre på at i oppfølgingen av leverandørens beredskapstesting, må foretaket selv behandle og vurdere hvorvidt testene er tilfredsstillende sett opp mot kravene i virksomhetens konsekvensanalyse.

Styret skriver i sitt svar at foretaket, i etterkant av det stedlige tilsynet, har inkludert et nytt punkt i foretakets skjema for leverandøroppfølging. Formålet med dette er å sikre dokumentasjon av kontroller som gjennomføres i forbindelse med krisetester hos foretakets leverandører.

Finanstilsynet tar styrets svar til etterretning.

4 Videre oppfølging

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

Vi ber foretaket sende kopi av dette brevet til revisor.

For Finanstilsynet

Olav Johannessen
seksjonsleder

Snorre Vik Sanfelt
rådgiver

Dokumentet er godkjent elektronisk.