FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

STOREBRAND LIVSFORSIKRING AS
Postboks 500
1327 LYSAKER

Vår referanse
24/18271
Deres referanse

09.05.2025

Tilsynsrapport

1 Innledning

Finanstilsynet gjennomførte tilsyn 25. og 26. november 2024 med Storebrand Livsforsikring AS (heretter omtalt "foretaket").

Formålet med tilsynet var å gjøre en vurdering av hvordan foretaket administrerer, utvikler, drifter, vedlikeholder og sikrer IKT-systemer og -tjenester. Tilsynet var avgrenset til elektronisk forsvar og tilhørende emner innen IKT-sikkerhet, og styring og kontroll med IKT-virksomheten. Videre ønsket Finanstilsynet å gjøre en vurdering av foretakets beredskapsarbeid relevant for IKT-området, herunder vurdere beredskapen i foretaket og for utkontrakterte IKT-tjenester, samt overholdelse av regulatoriske krav på IKT-området.

Til grunn for tilsynsrapporten ligger Finanstilsynets foreløpige rapport datert 26. februar 2025 og styrets kommentarer til rapporten i brev av 1. april 2025.

2 Finanstilsynets oppsummering

Tilsynet avdekket noen forhold der foretaket bør gjøre endringer og tilpasninger, blant annet knyttet til oppfølging av styregodkjente styringsdokumenter for å sikre at foretakets drift og planer utføres i henhold til disse, gjennomføre egne kontroller hos relevante IKT-tjenesteleverandører og at relevante informasjonssikkerhetsscenarioer må inngå ved testing av beredskapsplaner, der også verstefallsscenarioer inkluderes.

3 Finanstilsynets merknader

3.1 Strategi og organisering

Foretaket skal ha klare og hensiktsmessige styrings- og kontrollsystemer samt hensiktsmessige retningslinjer og rutiner for å styre, overvåke og rapportere risiko foretaket er eller kan bli eksponert for, jf. finansforetaksloven § 13-5 første ledd. IKT-forskriften § 2 første ledd stiller videre krav til at foretaket skal fastsette overordnede mål, strategier og sikkerhetskrav for IKT-virksomheten.

Finanstilsynet pekte i foreløpig rapport på at det forventes at styregodkjente styringsdokumenter som strategier og policyer følges opp for å sikre at foretakets drift og planer utføres i henhold til disse. Siden det er foretakets første forsvarslinje som er eier av strategier for IKT-området,

Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

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

Saksbehandler
Stig Ulstein
Dir. tlf. 22 93 99 66

forventer Finanstilsynet at foretakets andre og tredje forsvarslinje følger opp etterlevelsen av strategier og kontrollerer at de styrende dokumentene er operasjonalisert i henhold til disse.

Styret skriver i sitt svar at styret tar Finanstilsynets merknad knyttet til oppfølging av etterlevelse av styregodkjente styringsdokumenter til etterretning, og vil påse at kontrollvirksomheten i andre og tredje forsvarslinje omfatter alle relevante områder innenfor IKT.

Finanstilsynet tar styrets svar til etterretning.

3.2 Virksomhetens 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.

Finanstilsynet viste i foreløpig rapport til at foretaket har utført en virksomhetsmessig konsekvensanalyse og bruker denne som styringsinformasjon og i instrukser og retningslinjer, blant annet til å styre hvor tett leverandører skal følges opp i henhold til kritikalitet. Finanstilsynet pekte på at andre forsvarslinje bør utføre kontroller på om kritikalitet stemmer over ens med virksomhetens konsekvensanalyse. Videre bør det kontrolleres om dette stemmer med hva som er operasjonalisert.

Styret skriver i sitt svarbrev at styret vil påse at andre forsvarslinje gjennomfører uavhengige, risikobaserte kontroller av at leverandørens kritikaliteter i samsvar med virksomhetens konsekvensanalyse.

Finanstilsynet tar styrets svar til etterretning.

3.3 Kontrollfunksjoner

I finansforetaksloven § 13-5 andre ledd stilles det krav om at et finansforetak skal ha uavhengige kontrollfunksjoner med ansvar for risikostyring, etterlevelse, internrevisjon og aktuarfaglige oppgaver. Foretakets uavhengige kontrollfunksjoner skal ha tilstrekkelig kompetanse tilpasset risikoen ved og omfanget av virksomheten i foretaket.

Det er Finanstilsynets vurdering at for å ha god styring og kontroll på IKT-virksomheten, også den som er utkontraktert, bør foretaket gjennomføre egne kontroller både når det gjelder risiko og etterlevelse.

Finanstilsynet pekte i foreløpig rapport på at for å sikre at foretakets første- og andrelinjefunksjoner gjennomfører egne kontroller på utkontraktert IKT-virksomhet, må foretaket sikre tilstrekkelig ressurser og kompetanse på IKT-området for å utføre den nødvendige oppfølgingen.

Styret skriver i sitt svar at de deler Finanstilsynets syn på viktigheten av egne kontroller av IKT-tjenesteleverandører.

Finanstilsynet tar styrets svar til etterretning.

3.4 IKT-drift

IKT-forskriften § 9 stiller krav til at prosedyrene for endringshåndtering skal omfatte alle endringer som kan påvirke IKT-systemene og skal sikre forsvarlig, formell behandling og dokumentering av endringene. Foretaket skal sikre at prosedyrene for endringshåndtering gir en stabil, planlagt og forutsigbar drift.

Finanstilsynet pekte i foreløpig rapport på at alle med ansvar for IKT-drift må sørge for å få tilstrekkelig informasjon for alle områder ansvaret omfatter, slik at foretaket sikrer en forsvarlig, formell behandling, og dokumentasjon av IKT-relaterte endringer.

Styret viser i sitt svar til foretakets fastsatte endringsprosedyrer. Det er styrets vurdering at prosedyrene sikrer en forsvarlig, formell og dokumentert behandling av alle endringer, noe som er utgangspunkt for stabil og forutsigbar IKT-drift i foretaket. Styret erkjenner imidlertid at etterlevelse av endringsrutinen kan styrkes for enkelte områder.

Finanstilsynet påpekte videre i foreløpig rapport at foretaket må sørge for at prosedyren for avvikshåndtering sikrer at oppfølging inkluderer rapportering av tiltak som blir etablertsom følge av avviket. Dette gjelder også for utkontraktert IKT-virksomhet.

Styret skriver i sitt svar at status på tiltak etter IKT-hendelser knyttet til kritiske og viktige funksjoner inkluderes i hendelsesrapporteringen til foretakets ledelse.

I foreløpig rapport kommenterte Finanstilsynet på at for å sikre forsvarlighet, sporbarhet og ansvarliggjøring ved endringer skal endringer som kan påvirke driften eller foretakets kunder inngå i den til enhver tid etablerte endringshåndteringsprosessen. Videre pekte Finanstilsynet på at dette også må gjelde for produksjonssetting og endringer av maskinlæringsmodeller.

Styret skriver i sitt svar at foretaket vil følge opp at endringshåndteringsprosessen følges også på dette området.

Finanstilsynet tar styrets svar til etterretning.

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.

Finanstilsynet pekte i foreløpig rapport på at en desentral oppfølging kan medføre ulik grad og kvalitet på oppfølgingen av den utkontrakterte IKT-virksomheten og at foretaket derfor bør sørge for tilstrekkelig kompetanse og ressurser hos kontrakteier for å sikre god kvalitet på oppfølgingen av leverandører.

Styret skriver i sitt svar at de vil påse at foretaket har tilstrekkelig kompetanse og kapasitet hos kontraktseier.

Finanstilsynet tar styrets svar til etterretning.

3.6 Beredskap

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. Det skal minst årlig gjennomføres opplæring, øvelse og testing av at kriseløsningen virker som forutsatt. Resultatet av testen skal dokumenteres.

Foretaket er selv 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 kravene som stilles i analysen. Det er viktig at test av kriseløsningen gjennomføres på foretaksnivå og at foretaket gjør testene til sine egne, også for de IKT-tjenester som er utkontrakterte, for å vurdere egnetheten til kriseløsningen og robustheten til egen organisasjon og relevante IKT-tjenesteleverandører.

Finanstilsynet pekte i foreløpig rapport på at det ved testing av beredskapsplaner, for foretakets egne og for utkontrakterte IKT-tjenester, må relevante informasjonssikkerhetsscenarioer inngå, der også verstefallsscenarioer er inkludert i beredskapstestingen. Videre legges det til grunn at planverk for gjenoppretting og alternativ drift testes, for eksempel i scenarioer ved langvarig utilgjengelighet av tjenester, og utføres i henhold til interne instrukser.

Styret skriver i sitt svar at i fremtidig risikobasert beredskapstesting vil leverandører involveres i større grad, og at samspill mellom intern IKT-organisasjon og leverandører vil inngå som en del av testen. Videre kommenterer styret at foretaket vil risikobasert velge ut relevante informasjonssikkerhetsscenarioer som skal inngå i testingen, inkludert verstefallsscenarioer.

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

Stig Ulstein
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk.