FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Gjensidige Forsikring ASA
V/Styret
Postboks 700 Sentrum
0106 OSLO

Vår referanse
24/3856
Deres referanse
b09889759f19

17.12.2024

Tilsynsrapport - IT-tilsyn i Gjensidige Forsikring ASA

1 Innledning

Finanstilsynet gjennomførte stedlig IKT-tilsyn i Gjensidige Forsikring ASA 12. og 13. juni 2024. Hensikten med tilsynet var å gjøre en vurdering av hvordan foretaket 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 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 25. september 2024 og styrets kommentarer til rapporten i brev av 25. oktober 2024.

2 Finanstilsynets merknader

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. I IKT-forskriften § 2 første ledd stilles det videre krav til at foretaket skal fastsette overordnede mål, strategier, og sikkerhetskrav for IKT-virksomheten.

Finanstilsynet pekte i foreløpig rapport på at det vurderes som viktig at styregodkjente styringsdokumenter som strategier og policyer følges opp for å sikre at foretakets drift og planer utføres i henhold til disse, og at disse også følges opp av de kontrollfunksjonene som ikke står som eier av de styregodkjente styringsdokumentene.

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

Styret skriver i sitt svar at de er kjent med at det gjøres omfattende risikobaserte kontroller i både andre- og tredjelinje for å sikre at kravene i de styrende dokumenter ivaretas og er operasjonalisert.

Finanstilsynet tar styrets svar til orientering og legger til grunn at kontrollene som gjennomføres resulterer i rapportering som gir foretaket tilstrekkelig informasjon til å vurdere oppfyllelse av de styrende dokumentene.

Virksomhetens konsekvensanalyse

Det skal foreligge oppdatert dokumentasjon av det enkelte IKT-system som er av betydning for foretakets virksomhet, jf. IKT-forskriften § 13. Hensiktsmessige planer og tiltak for tilgjengelighet og kontinuitet bør etableres med utgangspunkt i konsekvensanalyser for foretakets kritiske forretningsprosesser. Virksomhetens 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 foretas regelmessig opplæring, øvelse og testing, jf. IKT-forskriften § 11.

Finanstilsynet pekte i foreløpig rapport på at foretaket ved tilsynstidspunktet ikke har en enhetlig virksomhetsmessig konsekvensanalyse. Uten en slik konsekvensanalyse vil foretakets kriseplan være utarbeidet uten forretningsmessige prioriteringer.

Styret skriver i sitt svar at det i 2023 ble etablert et prosjekt for å modernisere metodikk for virksomhetsmessig konsekvensanalyse. Videre bekrefter styret at dette skal gjennomføres for alle virksomhetsområder og at resultatet fra virksomhetsmessig konsekvensanalyser inngår i foretakets ordinære prosesser og beredskapsplaner. Resultatet av dette arbeidet rapporteres til styret.

Finanstilsynet tar styrets svar til orientering.

Kontrollfunksjoner og rapportering

I finansforetaksloven § 13-5 andre ledd stilles det krav om at et finansforetak skal ha uavhengige kontrollfunksjoner med ansvar for risikostyring, etterlevelse og internrevisjon.

Finanstilsynet pekte i foreløpig rapport på viktigheten av at første og andre forsvarslinje utfører egne kontroller av eller hos IKT-tjenesteleverandører og/eller deres underleverandører.

Styret gir i sitt svar en redegjørelse for foretakets oppfølging og kontrollfunksjonenes kontroller av IKT-tjenesteleverandører og/eller deres underleverandører. Styret skriver om viktigheten av oppfølging av tredjeparter, og vil se til at foretaket trapper opp stedlig kontroll og systematisk sikkerhetsoppfølging av kritiske og viktige IKT-tjenesteleverandører. Styret bekrefter videre at foretakets kontrollfunksjon i andrelinje er styrket.

Finanstilsynet tart styrets svar til orientering.

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 ble under tilsynsmøtet informert om at endringer som gjennomføres gjennom DevOps-prosessen i foretaket ikke er underlagt den etablerte endringshåndteringsprosessen, og er derfor heller ikke dokumentert i foretakets endringshåndteringsverktøy. Videre ble Finanstilsynet informert om at maskinlæringsmodeller som settes i produksjon heller ikke er underlagt endrings-håndteringsprosessen. Finanstilsynets vurdering er at foretakets etterlevelse av IKT-forskriften § 9 er mangelfull. For å sikre sporbarhet og ansvarliggjøring ved endringer som kan påvirke driften eller foretakets kunder mener Finanstilsynet at alle endringer skal gjennomføres i henhold til den enhver tid gjeldende endringshåndteringsprosess.

Styrets skriver i sitt svar at styret vil sørge for at administrasjonen innlemmer DevOps og endringsprosessen for maskinlæringsmodeller i den overordnede endringshåndteringsprosessen.

Finanstilsynet tar styrets svar til orientering.

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.

I foreløpig rapport pekte Finanstilsynet på utfordringer ved bruk og oppfølging av brukertilganger med utvidede rettigheter og hvordan bruken av disse kan gi muligheter for å misbruke tilgangen til ikke-tjenstlige oppslag som vanskelig lar seg avdekke. Finanstilsynet stilte videre spørsmål om foretakets styring og kontroll med tilganger ved utkontraktert virksomhet er tilstrekkelig.

Styrets skriver i sitt svar at alle tilganger for medarbeidere eller ansatte hos IKT tjeneste-leverandører er underlagt foretakets krav til tilgangsstyring. Videre viser styret til dokumentasjon som omhandler tilgangsstyring av tilganger med utvidede rettigheter. Styret skriver videre i sitt svar om hvordan foretakets kontrollfunksjoner følger opp og kontrollerer tilgangsstyring for foretaket og IKT-tjenesteleverandørers etterlevelse av foretakets krav.

Finanstilsynet tar styrets svar til orientering, men understreker viktigheten av løsninger for tilgangsstyring og kontrollrutiner som i størst mulig grad sørger for at tilganger tildeles og kontrolleres for det enkelte oppdrag. Det gjelder særlig for ansatte hos IKT-tjenesteleverandører.

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.

I foreløpig rapport pekte Finanstilsynet på at ved testing av beredskapsplaner, for foretakets egne og for utkontrakterte IKT-tjenester, må relevante informasjonssikkerhetsscenarioer inngå, herunder verstefallsscenarioer. Videre mente Finanstilsynet at det er først når testingen av relevante scenarioer er utført at foretaket har dokumentasjon på at IKT-tjenestenes tilgjengelighetskrav er ivaretatt.

Styret skriver i sitt svar at foretaket vil øke omfang i testene, samtidig som hensynet til kompleksitet, investerings-behov og forretningsrisiko ivaretas.

Finanstilsynet tar styrets svar til orientering.

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

For Finanstilsynet

Olav Johannessen
Seksjonsleder

Stig Ulstein
Senior tilsynsrådgiver

Dokumentet er godkjent elektronisk.