

**FINANSTILSYNET**THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAYStyret i DNB Livsforsikring AS
Postboks 7500
5020 BERGENVår referanse
23/9964
Deres referanse

30.04.2025

Tilsynsrapport

1 Innledning

Finanstilsynet gjennomførte stedlig IKT-tilsyn i DNB Livsforsikring AS (DNB Liv eller foretaket) 5. og 6. desember 2023. I tillegg ble det avholdt møte med foretakets internrevisjonsfunksjon 19. desember 2023.

2 Finanstilsynets oppsummering

Formålet med tilsynet var å gjøre en vurdering av hvordan foretaket administrerer, utvikler, drifter, vedlikeholder og sikrer IKT-systemer og -tjenester. Finanstilsynet har vurdert hvordan foretaket ivaretar styring og kontroll med IKT-virksomheten, hvordan DNB Liv følger opp IKT-tjenesteleverandører, arbeidet med IKT-sikkerhet, beredskap og kontinuitet, samt etterlevelsen av interne og eksterne krav på områdene.

Tilsynet avdekket til dels vesentlige mangler ved foretakets styring med og kontroll av IKT-virksomheten, blant annet knyttet til mangelfull rapportering og oppfølging både av intern og utkontraktert IKT-virksomhet. Finanstilsynet mener DNB Liv i større grad bør innhente uavhengige bekreftelser på at foretakets styring og kontroll med IKT-virksomheten er betryggende. Virksomhetens analyser for avbrudd i kritiske og viktige prosesser dekker for få områder, og øvelse og testing av, og opplæring i, foretakets beredskaps- og kriseløsninger bør omfatte realistiske scenarioer for utvalgte kritiske og viktige prosesser. Finanstilsynet har merket seg at foretaket har og vil iverksette en rekke tiltak.

3 Finanstilsynets merknader

3.1 Forsvarlig organisering av IKT-virksomheten

3.1.1 Ressurssituasjonen på IKT-området

Det framgår av finansforetaksloven § 8-6 første ledd at styret skal sørge for forsvarlig organisering av virksomheten. Finansforetakslovens bestemmelser om forsvarlig organisering omfatter også daglig leders ansvar for å sikre at foretaket har ansatte med nødvendige kvalifikasjoner, erfaring og tilstrekkelig kapasitet for å kunne styre og kontrollere IKT-virksomheten, samt at IKT-forskriften § 2 første ledd stiller kravene om at IKT-virksomheten skal utføres på en betryggende måte.

Basert på observasjonene i IKT-tilsynet, med særlig vekt på mangelfull helhetlig rapportering, svak oppfølging av utkontraktert virksomhet og konsekvensene av at "IKT ansvarlig" går av med pensjon, stilte Finanstilsynet i foreløpig rapport spørsmål ved om foretaket hadde avsatt tilstrekkelige ressurser for å ivareta betryggende styring med og kontroll av IKT-virksomheten.

Av styrets svar framgår det at DNB Liv i januar 2024 opprettet en ny seksjon med ansvar for IKT-virksomheten. En ny seksjonsleder, som også er utpekt som Chief Digital Officer (CDO), ble rekruttert til å lede denne seksjonen. Videre framgår det av styrets svar at styret er av den oppfatning at den nye seksjonen besitter tilstrekkelig teknisk kompetanse til å ivareta DNB Livs oppfølging av IKT-ansvaret.

Finanstilsynet tar styrets svar til etterretning.

3.1.2 Nøkkelpersonrisiko

Kompetanse, kunnskap og ansvar for ulike deler av IKT-virksomheten bør deles på flere for å redusere risikoen ved bortfall av nøkkelperson. For å ha kontroll med nøkkelpersonrisiko på IKT-området, bør styret se til at det finnes dokumenterte rutiner for IKT-virksomheten, jf. finansforetaksloven § 8-6 og § 8-11, og IKT-forskriftens § 2 første ledd.

I foreløpig rapport pekte Finanstilsynet på at "IKT ansvarlig" var i ferd med å pensjoneres og at foretaket i en periode ville ha en forhøyet nøkkelpersonrisiko gitt den erfaring, det brede ansvaret og den nøkkelposisjon som "IKT ansvarlig" hadde. Av styrets svar framgår det at styret mener at den nye seksjonen nevnt over har bidratt til at DNB Liv har fått etablert en vesentlig bedre styring med og kontroll av IKT-virksomheten. Nøkkelpersonrisikoen vurderes betydelig redusert etter den nye organiseringen da det nå er flere ansatte i DNB Liv, inkludert Chief Digital Officer (CDO), som følger opp DNB Livs IKT-virksomhet.

Finanstilsynet tar styrets svar til etterretning.

3.2 Risikostyringsfunksjonen

I finansforetaksloven § 13-5 framgår det at finansforetak skal drives på en forsvarlig måte og ha uavhengige kontrollfunksjoner med ansvar for risikostyring, etterlevelse, aktuarfaglige oppgaver og internrevisjon. Finanstilsynet forventer at de uavhengige kontrollfunksjonene i DNB Liv har tilstrekkelig kompetanse og ressurser for å ivareta sitt ansvar, jf. også kravene til system for risikostyring og internkontroll i forsikringsforetak som framgår av delegert kommisjonsforordning (EU) 2015/35¹ (Solvens II) og EIOPAs retningslinjer om "Guidelines on system of governance".²

God styring med og kontroll av IKT-virksomheten, også den som er utkontraktert, forutsetter at foretaket gjennomfører egne kontroller både for risiko og etterlevelse på IKT-området. Kontrollfunksjonene må sikre at alle vesentlige IKT-risikoer i foretaket er identifisert, målt og rapportert av de relevante organisatoriske enhetene.

Finanstilsynet mener at tilgang på IKT-kompetanse for den uavhengige kontrollfunksjonen for risiko (risikostyringsfunksjonen) er en forutsetning for å kunne identifisere relevante IKT-risikoer, vurdere mulige konsekvenser og fastsette hvilke kontroller som er hensiktsmessige utfra foretakets til enhver tid gjeldende IKT-risikobilde, jf. krav til kompetanse i finansforetaksloven § 8-11 tredje ledd.

¹ Delegert kommisjonsforordning Solvens II (EU) 2015/35: <https://lovdata.no/static/NLX3/32015r0035.pdf>

² EIOPA Guidelines on System of Governance - https://www.eiopa.europa.eu/publications/guidelines-system-governance_en

3.2.1 Ansvar for IKT-risiko

Basert på Finanstilsynets observasjon av uklare ansvarsforhold mellom konsernet (DNB Bank ASA ved Technology and Services (DNB T&S)) og DNB Liv når det gjelder ansvaret for IKT-risiko, påpekte Finanstilsynet i sin foreløpige rapport at det er fare for at vesentlige risikoer ikke blir identifisert, vurdert og mitigert. Finanstilsynet stilte derfor spørsmål ved hvorvidt DNB Liv etterlever bestemmelsene i finansforetaksloven om forsvarlig virksomhet på IKT-området, herunder utkontraktert IKT-virksomhet, jf. § 13-5.

Fra styrets svar framgår det at styret erkjenner ansvaret for å sikre forsvarlige styrings- og kontrollsystemer for IKT-virksomheten, inkludert regelmessige risikoanalyser og rapportering, og at det er dette som er grunnlaget for å vurdere om IKT-risiko identifiseres og styres innenfor foretakets rammer for akseptabel risiko. Finanstilsynet har notert seg at styret mener at gjennomførte organisatoriske endringer og presisering av ansvaret mellom konsernet og DNB Liv har skapt nødvendig klarhet for styring med og kontroll av IKT-risiko i foretaket.

Finanstilsynet tar styrets svar til etterretning og ber om å få tilsendt oversikt over hvilke rapporter som inngår i den periodiske rapporteringen etter at ny organisering er etablert, samt informasjon om hvem som utarbeider rapportene og hvem som er mottaker og behandler av rapportene.

3.2.2 Begrenset IKT-kompetanse og oppmerksomhet på IKT-risiko i risikostyringsfunksjonen

I foreløpig rapport stilte Finanstilsynet spørsmål ved om foretaket i tilstrekkelig grad ivaretar finansforetakslovens krav til kompetanse i risikostyringsfunksjonen i andre forsvarslinje, når denne skal identifisere risiko, vurdere konsekvenser og fastsette kontroller for å styre og kontrollere IKT-risiko.

Fra styrets svar har Finanstilsynet notert seg at styret erkjenner at IKT-området er komplekst og at det krever god kompetanse og gode kontrollrutiner. Videre at DNB Liv med bakgrunn i dette vil iverksette tiltak for å bedre IKT-kompetansen i andrelinjen. Styret vil revidere kontrollrutinene som skal sikre overvåking og rapportering av det samlede IKT-risikoområdet, og styret opplyser at IKT-området vil få en større plass i den regelmessige rapporteringen fra første- og andrelinjen. Finanstilsynet har videre merket seg at styret vurderer at de planlagte tiltakene vil imøtekomme påpekningene fra Finanstilsynet.

Finanstilsynet tar styrets svar til etterretning.

3.3 Rapportering på IKT-området

For å sikre en betryggende styring av og kontroll med foretakets IKT-virksomhet er det Finanstilsynets forventning at styret har fastsatt krav til daglig leder om rapportering for IKT-virksomheten, jf. Finansforetaksloven § 8-6, fjerde ledd.

For at daglig leder skal kunne rapportere til styret i henhold til styrets fastsatte krav er det Finanstilsynets forventning at daglig leder stiller krav om og mottar periodiske rapporter fra den/de IKT-ansvarlige om IKT-virksomheten, jf. finansforetaksloven § 8-11 tredje ledd. For å sikre et helhetlig bilde av status og risiko knyttet til IKT-virksomheten bør daglig leder også stille krav om at øvrige avdelinger/enheter inkluderer status og risiko for relevante IKT-temaer i sin periodiske rapportering.

Finanstilsynet forventer at den periodiske rapporteringen fra andrelinjens kontrollfunksjoner til daglig leder inkluderer vurderinger av relevante IKT-temaer.

3.3.1 Manglende kravstilling til rapporteringen fra daglig leder til styret

Med bakgrunn i mottatt dokumentasjon og informasjon i tilsynsmøtet pekte Finanstilsynet i foreløpig rapport på at det ikke framkom om styret har stilt krav til daglig leder om rapportering av forhold knyttet til IKT-virksomheten. Fra styrets svar har Finanstilsynet merket seg at styret har tydeliggjort sine krav til administrasjonen om årlig og periodisk rapportering av relevant informasjon om risiko, status og utvikling knyttet til IKT-virksomheten. Videre har Finanstilsynet notert seg at det vil bli utarbeidet en egen instruks for å fastsette disse kravene, og at de forbedrede rapporteringsrutinene iverksettes fra 2025.

Finanstilsynet tar styrets svar til etterretning.

3.3.2 Manglende kravstilling til rapporteringen på IKT-området fra virksomheten til daglig leder

Finanstilsynet pekte i foreløpig rapport på at det ikke framkom om daglig leder har stilt krav til virksomheten om periodisk rapportering av forhold knyttet til IKT-virksomheten. Videre oppfattet Finanstilsynet at DNB Liv i liten grad vurderte statusrapportene som ble mottatt fra DNB T&S som IKT-tjenesteleverandør. Finanstilsynet pekte også på at IKT-risikorapportene hovedsakelig ble utarbeidet av DNB T&S, og at DNB Liv i liten grad vurderte og behandlet den mottatte informasjonen.

Fra styrets svar framgår det at statusrapporteringen for IKT-virksomheten fra førstelinjen, som også inkluderer IKT-risiko, nå utarbeides i samarbeid mellom DNB Liv og DNB T&S og inkluderer DNB Livs uavhengige vurdering. Finanstilsynet har merket seg at DNB Liv har endret praksis til å selv delta i risikovurderingen som gjennomføres av førstelinjen, og at DNB Liv nå selv stiller krav til hvilke risikovurderinger som skal utføres. Basert på disse vurderingene vil DNB Liv selv foreta årlige, selvstendige og uavhengige risikovurderinger som behandles av ledelsen i DNB Liv.

Styret vurderer nå at den månedlige rapporteringen til daglig leder om IKT-virksomheten, som inkluderer informasjon fra statusmøter mellom DNB Liv og DNB T&S, og at daglig leder deltar på disse møtene kvartalsvis, gir daglig leder tilstrekkelig grunnlag for oppfølging og mulighet for videre rapportering til styret.

Finanstilsynet tar styrets svar til etterretning.

3.4 Konsekvensanalyse ved avbrudd i tjenesteleveransene (BIA)

I henhold til IKT-forskriften § 13 skal det foreligge oppdatert dokumentasjon av hvert IKT-system som er viktig for foretakets virksomhet. Hensiktsmessige planer for håndtering av driftsavbrudd og tiltak for etablering av kriseberedskap for IKT-virksomheten, jf. IKT-forskriften § 11, bør utarbeides basert på en konsekvensanalyse (BIA) av de kritiske prosessene i foretaket. Konsekvensanalysen skal bidra til å sikre at foretakets beredskapsplaner baseres på forretningskritikalitet. Planene skal prioritere gjenoppretting av de mest forretningskritiske tjenester og prosesser basert på analysens resultater, inkludert akseptabel nedetid for det enkelte IKT-system. Beredskapsplanene, som viser foretakets prioriteringer for gjenoppretting, bør også formidles til relevante leverandører. For å verifisere at fungerende planer og løsninger er etablert, må det minst årlig gjennomføres opplæring, øvelse og testing, jf. IKT-forskriften § 11.

I foreløpig rapport pekte Finanstilsynet på at DNB Liv ikke har tilstrekkelig grunnlag for å fastsette krav til planer og løsninger som sikrer nødvendig kontinuitet og beredskap for foretakets tjenesteleveranser siden de ikke har gjennomført BIA basert på konsernets nye mal, og inkludert analyser av konsekvenser for verst tenkelige avbruddsscenarioer. Finanstilsynet ba derfor styret om å vurdere hvilke konsekvenser den manglende gjennomgangen av resterende prosesser i henhold til det nye rammeverket for BIA påvirker foretakets evne til å håndtere avbrudd i tjenesteleveransene.

Finanstilsynet ba også om DNB Livs tidsplan for ferdigstilling av BIA i henhold til det nye rammeverket.

Fra styrets svar har Finanstilsynet notert seg at DNB Liv tar til etterretning Finanstilsynets kommentar om mangelfull gjennomføring av BIA og at foretaket framover vil ta hensyn til dette ved å gjennomføre BIA på flere områder. Gjennomgangen skal i henhold til plan være ferdig innen utgangen av mai måned hvert år.

Finanstilsynet tar styrets svar til etterretning.

3.5 Internrevisjonens arbeid

I finansforetakslovens § 8-16 annet ledd stilles det krav om at styret skal organisere og fastsette retningslinjer for internrevisjonen. Internrevisjonens hovedoppgave er å gi styret trygghet for at foretakets system for intern virksomhetsstyring, herunder internkontroll og risikostyring, er av tilfredsstillende kvalitet og at det etterleves effektivt i foretaket.

Internrevisjonen i DNB Liv er utkontraktert til Konsernrevisjonen i DNB Bank ASA. Finanstilsynet stilte i foreløpig rapport spørsmål om styret i tilstrekkelig grad inkluderer IKT-temaer i internrevisjonens kontrollarbeid, gitt den risiko og viktighet som IKT-virksomheten har for foretakets tjenesteleveranser. Finanstilsynet stilte videre spørsmål om i hvilken grad Konsernrevisjonen har vurdert og foreslått undersøkelser for å bekrefte en betryggende styring og kontroll av IKT-virksomheten i foretaket, med særlig fokus på kontroll med implementeringen av konsernets ulike rammeverk for styring og kontroll på IKT-området.

Av styrets svar framgår det at styret etter IKT-tilsynet har besluttet å søke bekreftelse på betryggende styring med og kontroll av IKT-området, noe som var i tråd med Konsernrevisjonens plandokument og styrepresentasjonen for 2024. Videre har Finanstilsynet notert seg at styret vurderer at Konsernrevisjonen gjennom sine utførte revisjoner, tiltak og planer har tilstrekkelig fokus på IKT-området i DNB Liv.

Finanstilsynet har notert seg at styret viser til at Konsernrevisjonen tidligere har fulgt opp implementering av rammeverk på konsernnivå, og at det i løpet av året gjennomføres relasjonsmøter med konsernheter for blant annet sikkerhet/cyber og tredjepartsrisikostyring, der innsikt fra disse møtene inngår i Konsernrevisjonens risikovurdering og periodiske revisjoner og rapportering. Fra styrets svar har Finanstilsynet videre notert seg at Konsernrevisjonen i 2024 har etablert en rutine som skal identifisere konsernrevisjoner som omfatter datterselskaper slik at styret i DNB Liv på denne måten vil motta hele eller deler av rapporter som omfatter prosesser som er relevant for foretaket.

Finanstilsynet tar styrets svar til etterretning.

3.6 IKT-sikkerhet

IKT-forskriften § 5 stiller krav til 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. Forskriften § 5 stiller videre krav til å etablere retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene. Ytterligere utdypinger finnes i EIOPAs retningslinjer for IKT-sikkerhet og virksomhetsstyring.

IKT-forskriften § 13 stiller krav til at det er etablert en oppdatert oversikt over organisasjon, utstyr, IKT-systemer og vesentlige forhold i IKT-virksomheten. Ovennevnte retningslinjer fra EIOPA har lignende bestemmelser.

3.6.1 Etterlevelse av sikkerhetskravene i konsernet

I foreløpig rapport pekte Finanstilsynet på at for at DNB Liv skal ha styring og kontroll med IKT-sikkerheten iht. kravene i konsernets instruks var det Finanstilsynets forventning at DNB Liv sørger for å ferdigstille implementeringen av konsernets IT-sikkerhetsrammeverk. Rammeverket skal bidra til at DNB Liv etablerer et helhetlig bilde av IKT-sikkerhetsrisiko. Finanstilsynet poengterte at den manglende oppfølgingen av påpekte avvik kan resultere i ikke-tilsiktede hendelser med store konsekvenser.

Fra styrets svar har Finanstilsynet notert seg at sikkerhetsrammeverket på tidspunktet for IKT-tilsynet ikke var tilpasset DNB Livs behov og at det derfor ikke var fullt ut operasjonalisert. Det framgår videre av styrets svar at rammeverket nå er tilpasset DNB Liv, og at DNB Liv har operasjonalisert dette. Videre at DNB Liv gjennom året vil utvikle og tilpasse operasjonaliseringen.

Finanstilsynet tar styrets svar til etterretning.

3.6.2 Tilgangsstyring

Finanstilsynet pekte i foreløpig rapport på at det var manglende kontroll med brukertilganger for brukere med utvidede tilganger til IKT-utstyr, systemer og data både for egne ansatte og for ansatte hos IKT-tjenesteleverandører. Finanstilsynet stilte spørsmål ved om DNB Liv dokumenterer at kontrollene av brukertilganger er gjennomført, og om avvik identifisert i gjennomganger er håndtert og lukket i tråd konsernets retningslinjer for tilgangsstyring.

Fra styrets svar har Finanstilsynet notert seg at sluttrapporten for resertifisering av brukere for 2022 og 2023 ble distribuert til IKT-ansvarlig i DNB Liv, men at disse ikke ble forelagt daglig leder. Lignende sluttrapport for 2024 foreligger ikke ennå, og styret har i forbindelse med påpekningen fra Finanstilsynet bedt om at daglig leder sikrer at rapporten blir mottatt og behandlet. Av styrets svar framgår det videre at tilgangskontroll er et av områdene som ettergås i forbindelse med den årlige finansielle revisjonen av DNB Liv utført av eksterntrevisor. Rapporten for 2023 viste ikke behov for "vesentlige tiltak". DNB Liv vil motta rapporten for 2024 i løpet av februar. Finanstilsynet har notert seg at styret vurderer at tilgangsstyring med de iverksatte tiltak er tilfredsstillende ivaretatt.

Finanstilsynet tar styrets svar til etterretning.

3.6.3 Mangelfull sikkerhetstesting

Finanstilsynet pekte i foreløpig rapport på at tilsynet ikke kunne se at DNB Liv følger en fastsatt prosedyre for å vurdere behovet og frekvensen for sikkerhetstesting i egne løsninger.

Fra styrets svar har Finanstilsynet notert seg at DNB Liv vurderer at de prosesser og prosedyrer som er innført etter det stedlige tilsynet er tilstrekkelig for god oppfølging av sikkerhetstesting. Av styrets svar framgår det også at DNB Liv har planlagt sikkerhets- og penetrasjonstesting for sine viktigste systemer, som skal utføres av et eksternt firma i første kvartal 2025.

Finanstilsynet tar styrets svar til etterretning.

3.7 IKT-Utkontraktering

DNB Liv har i all hovedsak utkontraktert sine IKT-tjenester til DNB T&S. Dette inkluderer IKT-leveranser avtalt med underleverandører. I henhold til IKT-forskriften § 2 annet ledd, skal foretaket ha retningslinjer som sikrer at utkontraktert IKT-virksomhet oppfyller kravene i § 12. Kravene i § 2 og § 12 gjelder uavhengig av om oppdragstaker for den utkontrakterte IKT-virksomheten er et foretak innen samme konsern, jf. rundskriv nr. 7/2021 "Veiledning om utkontraktering" kapittel 3 første avsnitt.

I foreløpig rapport var det Finanstilsynet oppfatning at oppfølgingen av de utkontrakterte IKT-tjenestene i stor grad er overlatt til DNB T&S. Det var derfor Finanstilsynets vurdering at DNB Liv ikke følger opp IKT-utkontraktingen i tilstrekkelig grad. Finanstilsynet pekte på at DNB Liv ikke har satt tydelige krav til IKT-leverandørene, og at DNB Liv sitt ansvar for risikostyring og internkontroll, når hele eller deler av IKT-virksomheten er utkontraktert, ikke synes å være tilstrekkelig ivaretatt. Kfr. også Finanstilsynets merknader til det uklare ansvarsforholdet til andrelinje risikostyring i konsernet og i DNB Liv i punkt "3.2.1 Ansvar for IKT-risiko".

Fra styrets svar framgår det at DNB Liv følger opp utkontraktingen i månedlige møter med DNB T&S basert på faste agendapunkter, og at kravstillingen til IKT-leverandører blir ivaretatt gjennom disse møtene. Fra styrets svar har Finanstilsynet notert seg at styret er enig i viktigheten av å formalisere og dokumentere dialogen rundt IKT-underleverandører. Styret vurderer at oppfølgingen av IKT-underleverandører er tilstrekkelig ivaretatt gjennom oppfølgingsmøtene med DNB T&S.

Finanstilsynet tar styrets svar til etterretning.

I tilsynet ble tre fellestjenester for forsikringsbransjen vurdert som utkontrakterte tjenester av Finanstilsynet. Finanstilsynet påpekte at disse tjenestene må følges opp som utkontrakting iht. IKT-forskriften.

Fra styrets svar har Finanstilsynet merket seg at DNB Liv er enig i at de tre løsningene skal følges opp som utkontraktert IKT virksomhet, og at DNB Liv vil tydeliggjøre dette gjennom overvåking, oppgraderinger, rapportering og faste møter med de tre leverandørene.

Finanstilsynet tar styrets svar til etterretning.

3.8 Endrings og avvikshåndtering

I tilsynsmøtet ble DNB Liv sin hendelsesrapportering vurdert. Basert på den tilsendte hendelsesoversikten påpekte Finanstilsynet i tilsynsmøtet at DNB Liv synes å ha flere rapporteringspliktige hendelser enn det som er rapportert til Finanstilsynet. Finanstilsynet understreket at DNB Liv selv plikter å rapportere hendelser til Finanstilsynet, og at dersom DNB Liv mener at de er omfattet av innrapporterte hendelser fra DNB Bank ASA så må dette klart framgå av hendelsesrapporteringen som sendes fra DNB Bank ASA.

Av styrets svar framgår det at DNB Liv vil etablere rutiner slik at relevante hendelser blir rapportert til Finanstilsynet fortløpende.

Finanstilsynet tar styrets svar til etterretning.

3.9 Datakvalitet

Basert på mottatt dokumentasjon og informasjonen i tilsynsmøtet, oppfattet Finanstilsynet at DNB Liv er i ferd med å iverksette konsernets rammeverk for "Data governance" (styring med og kontroll av data). I foreløpig rapport var det Finanstilsynets vurdering at arbeidet med å implementere konsernets rammeverk for styring med og kontroll av data er i en tidlig fase, og at DNB Liv med utgangspunkt i de mulige konsekvensene som dårlig datakvalitet kan medføre bør intensivere arbeidet med å iverksette et helhetlig rammeverk for styring av og kontroll med data.

Fra styrets svar har Finanstilsynet notert seg at styret er enig i viktigheten av god styring og kontroll for å opprettholde god datakvalitet, og at de vil sikre at arbeidet med datakvalitet blir ivaretatt i dagens løsning og ved overgang til ny dataplattform. Videre framgår det av styrets svar at DNB Liv i 2023 og 2024 har arbeidet med å avstemme data mellom fagsystemer, datakilder og DNB Liv sitt eget datavarehus. Oppgaver som inngår i det nye rammeverket, slik som å dokumentere oversikt over hvilke data som produseres, hvor de behandles og tilgjengeliggjøres,

og hvem som er juridisk eier, er allerede på plass gjennom arbeidet som er utført i forhold til DNB Liv sitt eget datavarehus. I forbindelse med DNB Liv sin etablering av ny dataplattform vil det bli etablert prosesser for å kvalitetssikre dataoverføringene til det nye datavarehuset. Chief Digital Officer (CDO) vil sørge for at dataeiere og brukere følger konsernet sitt rammeverk.

Finanstilsynet tar styrets svar til etterretning.

3.10 Beredskap og krisehåndtering

Foretaket har ansvar for at nødvendig kontinuitet og beredskap er sikret, jf. IKT-forskriften § 11. EIOPAs retningslinjer for IKT-sikkerhet og virksomhetsstyring utdyper IKT-forskriftens bestemmelser med retningslinjer knyttet til utarbeidelse av kontinuitets-, respons-, kommunikasjons- og gjenopprettingsplaner ved kriser, samt hvordan testing skal foregå.

Foretakets kriseplaner må inkludere kriterier for når kriseplaner skal iverksettes, jf. IKT-forskriften § 11 annet ledd. For å ha trygghet for at de viktigste leverandørene er forberedt på å bistå foretaket, er det Finanstilsynets forventning at kravene til kriseberedskap hos IKT-leverandørene er sikret i form av avtaler. Foretaket bør videre sikre at IKT-tjenesteleverandører som har leveranser knyttet til de virksomhetskritiske prosessene er omfattet av foretakets øvelse og testing, jf. IKT-forskriften § 11 siste ledd.

3.10.1 Mangelfull plan for IKT-kontinuitet og -beredskap, samt uklar sammenheng mellom virksomhetens kontinuitets- og beredskapsplan, og plan for IKT-kontinuitet og -beredskap

DNB Liv har utarbeidet en generell plan for kontinuitet og beredskap og en spesifikk plan for IKT-kontinuitet og -beredskap. Finanstilsynet observerer at den generelle planen inkluderer angivelse av roller med navn på ansatte som har sluttet og at den spesifikke planen er oppført med titler/angivelser som tyder på manglende oppdatering. Finanstilsynet stilte derfor spørsmål ved om DNB Liv har etablert prosedyrer som sikrer et helhetlig og oppdatert planverk for kontinuitet og beredskap.

I svaret fra styret framgår det at styret tar Finanstilsynets kommentar til etterretning og at styret vil sikre at planene oppdateres minimum årlig. DNB Liv vil iverksette tiltak for å oppdatere og sikre versjonshåndtering av dokumentasjon og planer for IKT-kontinuitet og -beredskap. Det samme gjelder for dokumentasjon og planer for forretningskontinuitet for DNB Liv.

Finanstilsynet tar styrets svar til etterretning.

3.10.2 Krav til virksomhetens kontinuitet og beredskap i tekniske løsninger

I et helhetlig rammeverk for kontinuitet og beredskap forventer Finanstilsynet at foretaket vurderer og kontrollerer at virksomhetens krav til kontinuitet og beredskap, slik disse er framsatt ved BIA (Konsekvensanalyse ved avbrudd i tjenesteleveransene (BIA)), er ivaretatt i de tekniske løsningene som er etablert i foretaket og hos IKT-tjenesteleverandører. Med bakgrunn i Finanstilsynets observasjon om mangelfulle prosedyrer for oppdatering av planverket for beredskap og krisehåndtering stilte Finanstilsynet i foreløpig rapport spørsmål ved om det er etablert prosedyrer for å sikre at kravene fra BIA er ivaretatt i foretakets beredskaps- og kriseplaner. Finanstilsynet bad derfor om en redegjørelse for hvordan DNB Liv kontrollerer at kravene blir ivaretatt av IKT-tjenesteleverandører.

Fra styrets svar framgår det at DNB Liv har oversikt over aller forretningskritiske applikasjoner med angivelse av RTO (mål for gjenopprettingstid) og RPO (mål for gjenopprettingspunkt) pr. applikasjon. I testrapporter for kontinuitetstesting for de forretningskritiske applikasjonene framgår det at kravene til RTO/RPO for DNB Liv sine systemer er oppfylt, noe som etter styrets vurdering dokumenterer at kravene fra BIA er ivaretatt for IKT-løsningene i DNB Liv.

Finanstilsynet tar styrets svar til etterretning.

3.10.3 Mangelfull opplæring, øvelse og testing ifm. foretakets beredskaps- og kriseløsninger

For å verifisere at foretakets planer og løsninger for beredskap og kontinuitet virker som forutsatt skal foretaket minst årlig gjennomføre opplæring, øvelse og testing, jf. IKT-forskriften § 11, tredje ledd.

Fra mottatt dokumentasjon og informasjon i tilsynsmøtet oppfatter Finanstilsynet at den utførte testingen i DNB Liv i stor grad er systemmessig kontinuitetstesting, samt i noen grad skrivebordsøvelser. Finanstilsynet vurderte i foreløpig rapport at skrivebordsøvelser og systemmessig kontinuitetsstesting ikke er tilstrekkelig til å oppfylle IKT-forskriftens krav om at foretaket skal øve på, og teste at foretakets planer og løsninger for beredskap og kontinuitet virker som forutsatt. Finanstilsynet forventer at DNB Liv med utgangspunkt i en risikobasert tilnærming, gjennomfører praktiske øvelser og tester basert på realistiske scenarier for utvalgte kritiske og viktige prosesser, der også foretakets ledelse og relevante IKT-leverandører blir involvert. Videre forventes det at dokumentasjon fra utført opplæring, øvelse og testing av beredskap og kontinuitet inngår som grunnlag i vurderingen av foretakets evne til å håndtere avbrudd i foretakets tjenesteleveranser. Finanstilsynet bad om styrets vurdering av egen opplæring, øvelse og testing.

Fra styrets svar framgår det at styret vurderer at utførte skrivebordstester, sammen med systemmessige tester bekrefter at DNB Liv har tilfredsstillende kontroll med at foretakets planer og løsninger for beredskap og krisehåndtering fungerer, og at dette også er bekreftet i håndteringen av faktiske hendelser. Styret anerkjenner Finanstilsynets tilbakemelding om at skrivebordstester kombinert med systemmessige tester ikke er tilstrekkelig for å oppfylle IKT-forskriftens krav, og at det er nødvendig med mer omfattende øvelser og tester for å verifisere at de fastsatte kontinuitets- og beredskapstiltakene fungerer effektivt, spesielt for prosesser hvor det er avhengighet mellom flere systemer, tjenester og leverandører. DNB Liv vil derfor gjennomføre minst én årlig øvelse basert på realistiske scenarier for utvalgte kritiske og viktige prosesser i tillegg til skrivebordstester og systemmessige tester. Disse øvelsene vil også involvere foretakets ledelse og relevante IKT-leverandører.

Finanstilsynet tar styrets svar til etterretning.

3.10.4 Arbeidet med beredskap og kontinuitet inngår i liten grad i foretakets ordinære drift

Basert på observasjoner nevnt i punkt 3.4 over og i dette punktet om beredskap og kontinuitet (3.10), var Finanstilsynets vurdering i foreløpig rapport at DNB Liv ikke har etablert rutiner og prosedyrer som sikrer at arbeidet med beredskap og kontinuitet inngår i foretakets ordinære drift, der resultatene fra BIA og helhetlige øvelser og tester danner grunnlaget for tiltaksplaner internt i DNB Liv, og hos berørte IKT-tjenesteleverandører.

Fra styrets svar oppfatter Finanstilsynet at DNB Liv allerede har fokus på de mest kritiske prosessene, og at det er etablert forbedringsprosesser som kontinuerlig sikrer forbedring av kontinuitets- og beredskapsplaner gjennom å identifisere korrigerings- og forbedringstiltak når hendelser oppstår, med mål om å forhindre at samme hendelse skjer igjen. Fra styrets svar har Finanstilsynet også merket seg at det er gjennomført kontinuitetstesting av IKT-systemer hos eksterne IKT-tjenesteleverandører, og at det ikke er identifisert kritiske svakheter i de systemene som er testet. Videre har Finanstilsynet merket seg at DNB Liv har arbeidet kontinuerlig med å sikre beredskap og kontinuitet innenfor de områder som ansees som spesielt kritiske for virksomheten i etterkant av tilsynet, og at dette arbeidet fortsatt vil ha et høyt fokus.

Finanstilsynet tar styrets svar til etterretning.

4 Videre oppfølging

Finanstilsynet ber foretaket sende kopi av dette brevet til revisor.

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

For Finanstilsynet

Olav Johannessen
seksjonsleder

Jarleif Løddøen
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk.