

Redegørelse om funktionsinspektion af IT-risikostyring i Pensam Pension forsikringsaktieselskab

Indledning

Finanstilsynet var i juni 2024 på funktionsinspektion i Pensam Pension forsikringsaktieselskab (Pensam Pension). Inspektionen omhandlede virksomhedens IT-risikostyring. Undersøgelsen tog udgangspunkt i virksomhedens indsendte materiale og rapporteringer til Finanstilsynet.

Sammenfatning og risikovurdering

Pensam Pension administrerer ca. 500.000 arbejdsmarkedspensionsordninger til FOAs faggrupper. Virksomhedens forretningsmodel indebærer omfattende anvendelse af IT, hvilket medfører en række iboende IT-risici.

IT-risikostyring

Generelt vurderer Finanstilsynet, at IT-risici er et væsentligt risikoområde for Pensam Pension. Bestyrelsen skal derfor fastsætte, hvilke og hvor store IT-risici Pensam Pension må påtage sig, samt aktivt tage stilling til strategiske mål for håndtering af IT-risici.

Finanstilsynet konstaterede, at Pensam Pension har arbejdet med IT-risici og også foretager risikovurderinger på området samt overordnet set har fastsat en metode for blandt andet IT-risikostyring.

Finanstilsynet vurderede dog, at Pensam Pension skal styrke metoden til IT-risikostyring yderligere, for at kunne måle og opgøre sine IT-risici tilstrækkeligt. Finanstilsynet konstaterede, at politikker eller retningslinjer ikke i tilstrækkelig grad angiver principperne for opgørelse eller måling af IT-risici, og at principperne derfor ikke er tilstrækkeligt forankret i bestyrelsen. Der er dermed risiko for, at virksomheden ikke styrer og måler sine IT-risici i tilstrækkelig grad i overensstemmelse med bestyrelsens ønsker. Finanstilsynet har derfor

påbudt bestyrelsen at fastsætte klare principper for opgørelse og måling af IT-risici¹.

¹ § 95, stk. 2, nr. 2, i lov om forsikringsvirksomhed samt § 7, stk. 3, nr. 5, § 8, stk. 1, nr. 2, og bilag 6, nr. 2, litra a, i bekendtgørelse om ledelse og styring af forsikringselskaber m.v.