FINANSTILSYNET

Redegørelse om funktionsinspektion i GF Forsikring A/S

Finanstilsynet var i februar 2023 på funktionsinspektion i GF Forsikring A/S (herefter selskabet eller GF Forsikring).

Inspektionen omhandlede selskabets IT-risikostyring, og tog udgangspunkt i selskabets indsendte materiale og rapporteringer til Finanstilsynet.

Sammenfatning og risikovurdering

Med flere end 340.000 medlemmer og 46 lokale kontorer spredt over hele landet er GF Forsikring et af Danmarks største medlemsejede forsikringsselskaber. Hovedaktiviteten er skadeforsikring i Danmark. Det største forretningsområde er privatforsikringer. Selskabet er et gruppe 1-forsikringsselskab.

Selskabets forretningsmodel indebærer omfattende anvendelse af IT, hvilket medfører, at selskabet er udsat for IT-risici.

Selskabets IT-ansvarlige i 1. forsvarslinje er selskabets IT-direktør. Herudover har selskabet etableret en risikostyringsfunktion, som er forankret i risikostyringsafdelingen og placeret i 2. forsvarslinje

IT-risikostyring
Generelt vurderer Finanstilsynet, at IT-risici er et væsentligt risikoområde for GF Forsikring A/S. Bestyrelsen skal derfor fastsætte, hvilke og hvor store IT-risici selskabet må påtage sig samt aktivt tage stilling til strategiske mål for IT-risici.

Samlet set vurderer Finanstilsynet, at der er en risiko for, at selskabet påtager sig IT-risici, som ikke er i overensstemmelse med bestyrelsens risikoappetit.

Finanstilsynet konstaterede, at bestyrelsen ikke har fastsat tilstrækkelige risikotolerancegrænser for IT-risici. Finanstilsynet har derfor påbudt selskabet at sikre, at bestyrelsen fastsætter hvilke og hvor store IT-risici, selskabet må påtage sig, og specificerer risikotolerancegrænser for IT-risici, som udgør kontrollerbare grænser for størrelsen af acceptable IT-risici.

Finanstilsynet konstaterede også, at selskabet har en mangelfuld opgørelse af risikoprofilen. Finanstilsynet vurderer, at forsikringsselskaber løbende bør sammenholde deres faktiske risikoprofil med den ønskede risikoprofil, udtrykt ved bestyrelsens risikotolerancegrænser, med henblik på at give bestyrelsen et billede af, hvor selskabet eventuelt ligger udenfor bestyrelsens ønskede niveau for IT-risici. Selskabet er derfor blevet påbudt at fastlægge selskabets risikoprofil for IT-risici.

Selskabet havde ikke fastsat en metode for IT-risikostyring eller formaliseret vurdering af IT-risici, som selskabet er eller kan blive udsat for. Selskabet er derfor blevet påbudt at fastsætte principper for opgørelsen og måling af IT-risici samt at have effektive procedurer til identifikation og vurdering af IT-risici.

Endeligt vurderede Finanstilsynet, at der ikke var tilstrækkelig styring af IT-risici i selskabets risikostyringssystem. Et velfungerende risikostyringssystem indebærer bl.a., at der sker en systematisk vurdering af bl.a. IT-risici, herunder en identifikation, måling, styring og rapportering af IT-risici. Risikostyringsfunktionen har en vigtig opgave i at understøtte risikostyringssystemet ved bl.a. at sikre, at

alle væsentlige risici bliver identificeret, målt, overvåget, styret og rapporteret korrekt. Finanstilsynet har derfor påbudt selskabet at sikre, at risikostyringssystemet omfatter styring af IT-risici.