

Redegørelse om funktionsinspektion i Forsikringselskabet Privatsikring A/S

Finanstilsynet var i februar 2024 på funktionsinspektion i Forsikringselskabet Privatsikring A/S (selskabet eller Privatsikring).

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

Sammenfatning og risikovurdering

Privatsikring er et gruppe 1-forsikringselskab, som tegner skadesforsikringsprodukter i Danmark gennem bankassurance-partnerskaber. Privatsikring har historisk tilbudt forsikringer til privatkunder. I august 2022 blev brandet Erhvervsikring etableret, så Privatsikring nu også tilbyder forsikringer til erhvervs kunder gennem det nyetablerede brand. Selskabet er en del af Alm. Brand koncernen.

Selskabets forretningsmodel indebærer omfattende anvendelse af IT, hvilket medfører, at selskabet er udsat for IT-risici. Derudover er selskabets operationelle risikoniveau forhøjet som følge af processen med selskabets integration i Alm. Brand A/S.

Selskabets IT-ansvarlige er IT-direktøren, som befinder sig i 1. forsvarslinje, hvor også afdelingen for IT-governance er placeret. Selskabet har herudover etableret en risikostyringsfunktion, som er forankret i risikostyringsafdelingen og dermed placeret i 2. forsvarslinje.

Bestyrelsens arbejde

Finanstilsynet konstaterede, at bestyrelsen i sin vurdering af egen risiko og solvens ikke tager stilling til, om det aktuelt forhøjede risikoniveau for operationelle risici, herunder IT-risici, betyder, at der er forskel på niveauet af operationelle risici, der ligger til grund for opgørelsen af kapitalkravet efter standardmodellens modul for operationelle risici, og selskabets aktuelle risikoniveau.

Med henblik på at vurdere, om solvenskapitalkravet afspejler selskabets aktuelle operationelle risikoniveau, har selskabet fået påbud om at sikre et tilstrækkeligt fokus på forskellene mellem selskabets operationelle risikoniveau og de operationelle risici bag standardmodellens solvenskapitalkrav i vurderingen af egen risiko og solvens¹.

Risikostyringsfunktionen

Risikostyringsfunktionen skal sætte rammerne for operationel risikostyring i hele selskabet. Finanstilsynet konstaterede imidlertid, at IT-governance afdelingens rammeværk for IT-risikostyring i 1. forsvarslinje ikke følger risikostyringsfunktionens overordnede rammeværk for risikostyring, men bl.a. anvender andre sandsynlighedsklasser og konsekvensklasser.

Finanstilsynet vurderede, at de IT-risici, som IT-governance afdelingen har identificeret, dermed ikke var vurderet med udgangspunkt i samme tilgang som risikostyringsfunktionens, hvorfor den ansvarlige for risikostyringsfunktionen ikke har sikret, at alle væsentlige IT-risici i virksomheden måles og overvåges korrekt.

¹ Jf. § 4, stk. 2, i bekendtgørelse om ledelse og styring af forsikringselskaber m.v. (ledelsesbekendtgørelsen).

Selskabet styrer IT-risici igennem risikoreducerende foranstaltninger. Finanstilsynet konstaterede, at der i selskabets risikorapportering ikke er nogen kobling mellem de risikoreducerende foranstaltninger og de risici, som skal mitigeres. Derfor er det ikke tydeligt, hvordan selskabets risikoreducerende foranstaltninger har en effekt på de enkelte risici. Den manglende kobling giver dårlige forudsætninger for styringen såvel som rapporteringen af selskabets risici.

Finanstilsynet vurderede desuden, at risikostyringsfunktionens involvering i alle relevante dele af IT-risikostyringsprocessen, herunder identifikation, vurdering, håndtering og rapportering af IT-risici, ikke var tilstrækkeligt dokumenteret.

Selskabet har derfor fået påbud om, at den ansvarlige for risikostyringsfunktionen skal sikre, at alle væsentlige risici i virksomheden identificeres, måles, overvåges, styres og rapporteres korrekt².

² Jf. bilag 6, nr. 12, i ledelsesbekendtgørelsen