FINANSTILSYNET

Finanstilsynet

5. juli 2024

J.nr. 23-012769

Redegørelse om IT-inspektion hos SDC A/S

1. Indledning

Finanstilsynet har gennemført en IT-inspektion hos SDC A/S i efteråret 2023.

Inspektionen omfattede følgende områder:

- IT-sikkerhedsstyring
- IT-risikostyring
- IT-beredskabsstyring

2. Sammenfatning

Finanstilsynet vurderer, at SDC har mangler i sin IT-sikkerheds- og IT-risikostyring samt IT-beredskabsstyring. Disse mangler indebærer en forhøjet IT-risiko. På den baggrund har Finanstilsynet givet SDC 2 påbud for at sikre en tilstrækkelig styring af områderne.

SDC har ikke sikret en tilstrækkelig IT-sikkerhed- og IT-risikostyring. Det skyldes blandt andet, at SDC ikke har en tilstrækkelig klar udmøntning af sin målsætning for det ønskede IT-sikkerhedsniveau[1]. Derudover har SDC ikke i tilstrækkelig grad sikret, at kravene i IT-sikkerhedspolitikken modsvarer de IT-risici, som SDC har identificeret i den årlige risikovurdering[2].

SDC har valgt en risikovurderingstilgang, som er centreret omkring risikovurdering af systemer. Som konsekvens af den valgte risikovurderingstilgang, foretages der ikke en tilstrækkelig dokumenteret risikovurdering af forretningsprocesser, som understøtter SDC's serviceleverancer og de tilsluttede pengeinstitutter[3].

---

[1] Bekendtgørelse nr. 1103 af 30. juni 2022 om ledelse og styring af pengeinstitutter m.fl., § 1. stk. 3, jf. bilag 5, nr. 4, litra b og nr. 13.

[2] Bekendtgørelse nr. 1103 af 30. juni 2022 om ledelse og styring af pengeinstitutter m.fl., § 1. stk. 3, jf. bilag 5, nr. 8-9 og nr. 107-108.

[3] Bekendtgørelse nr. 1103 af 30. juni 2022 om ledelse og styring af pengeinstitutter m.fl., § 1. stk. 3, jf. bilag 5, nr. 22-26.

Inspektionen har også vist, at SDC mangler en tilstrækkelig styring af sin proces for IT-risikovurdering som grundlag for datacentralens scenariebaserede tilgang til vurdering af IT-risici. SDC's årlige IT-risikovurderingsproces tager udgangspunkt i risikoscenarier, hvor formålet er at beregne det gennemsnitlige årlige tab ved scenarierne gennem en Monte Carlo-simulering af hændelser. Finanstilsynet har identificeret en række mangler i IT-risikostyringsprocessen i forhold til eksempelvis kvalitetssikring af datagrundlaget, parametre, forudsætninger samt tabsberegninger[4].

Manglerne medfører en risiko for, at SDC's ledelse ikke har et tilstrækkeligt og retvisende beslutningsgrundlag til at risikostyre og prioritere sikkerhedsindsatsen og løbende evaluerer sikkerhedsniveauet. SDC har derfor fået påbud om at sikre tilstrækkelige metoder og processer for IT-sikkerheds- og IT-risikostyring, som grundlag for rapportering om IT-risici. Herunder sikre en klar udmøntning af målsætningen for IT-sikkerhedsniveauet, sikre sammenhæng mellem rammeværker for henholdsvist IT-sikkerheds- og IT-risikostyring, risikovurdere forretningsprocesser samt sikre, at styringen af IT-risici bygger på et tilstrækkelig grundlag.

SDC har ikke fastsat IT-beredskabsmålsætninger baseret på konsekvensanalyser af forretningsprocesser (BIA), som understøtter SDC's serviceleverancer og de tilsluttede pengeinstitutter. Dette medfører, at SDC har en mangelfuld fastsættelse af beredskabsmålsætninger. SDC arbejder desuden på at styrke sine processer for operationel robusthed både i forhold til planlægning og test af beredskab[5].

Manglerne medfører en risiko for, at de kritiske forretningsprocesser ikke kan genetableres i overensstemmelse med forventninger hertil. SDC har derfor fået påbud om at sikre, at IT-beredskabsmålsætninger fastsættes på grundlag af konsekvensanalyser af forretningsprocesser.

[4] Bekendtgørelse nr. 1103 af 30. juni 2022 om ledelse og styring af pengeinstitutter m.fl., § 1. stk. 3, jf. bilag 5, nr. 6 og nr. 106.

[5] Bekendtgørelse nr. 1103 af 30. juni 2022 om ledelse og styring af pengeinstitutter m.fl., § 1. stk. 3, jf. bilag 5, nr. 9, litra k, nr. 91-92 og nr. 99.