

Redegørelse om IT-inspektion hos A/S Arbejdernes Landsbank

1. Indledning

Finanstilsynet gennemførte en IT-inspektion i A/S Arbejdernes Landsbank (herefter AL/banken) i november-december 2022. Formålet med inspektionen var at undersøge, om banken havde betryggende håndtering af følgende IT-områder:

- IT-sikkerhedsstyring og IT-risikostyring
- IT-beredskab, herunder IT-sikkerhedshændelses- og problemstyring
- IT-revision.

2. Sammenfatning

Finanstilsynet har vurderet, at AL har grundlæggende mangler i sin IT-sikkerhedsstyring og IT-risikostyring samt i sin styring af IT-beredskabet. Disse forhold har medført en forøget operationel risiko for banken. Finanstilsynet har givet AL påbud for at udbedre manglerne.

Bankens metode til IT-risikostyring er ikke baseret på en systematisk gennemgang af bankens forretningsprocesser eller IT-systemer, og metoden er ikke understøttet af tilstrækkelig dokumentation. Desuden har AL ikke sikret, at væsentlige IT-risici, der identificeres af bankens leverandører, systematisk inkluderes i bankens IT-risikostyring. Yderligere mangler AL at skabe en tydelig sammenhæng mellem risici i bankens IT-risikoregister og de tilhørende planer for risikobehandling. Finanstilsynet har derfor påbudt AL at sikre, at IT-risici på tværs af banken og bankens leverandører bliver identificeret, vurderet, behandlet, overvåget og rapporteret.

AL har identificeret, at banken på en række områder ikke efterlever ledelsesbekendtgørelsens bilag 5 om IT-strategi, IT-risikostyringspolitik og IT-sikkerhedspolitik. AL har imidlertid ikke konsekvent udarbejdet handlingsplaner for at sikre efterlevelsen. Finanstilsynet har derfor påbudt AL at sikre, at

handlingsplaner for alle områder udarbejdes samt at statusrapporteringen på fremdriften forbedres.

Banken gennemfører regelmæssige test af IT-sikkerheden, men banken mangler en tydelig sammenhæng til IT-risikovurderingsprocessen, når den planlægger sine IT-sikkerhedstest. Finanstilsynet har påbudt AL at sikre sammenhæng mellem test af IT-sikkerheden samt identificerede trusler og sårbarheder fra risikovurderingsprocessen.

AL's processer og metode til at styre sit IT-beredskab har mangler. For det første har AL ikke sikret, at bankens IT-beredskab lever op til kravene i dens IT-beredskabspolitik, herunder at bankens IT-beredskab skal planlægges, så det kan håndtere en række udvalgte scenarier. For det andet har AL ikke udarbejdet individuelle forretningskonsekvensanalyser for bankens forretningsprocesser, og banken har derfor ikke et tilstrækkeligt grundlag til at fastlægge sine beredskabsmålsætninger. For det tredje mangler banken at sikre, at dens forretningskontinuitetsplaner er af tilstrækkelig kvalitet, er dækkende ift. alle bankens forretningsprocesser, er opdaterede samt afprøves tilstrækkeligt. Finanstilsynet har derfor påbudt AL at sikre, at bankens metode til styring af sit IT-beredskab forbedres.

AL har ikke et tilstrækkeligt overblik over, om afprøvninger af IT-beredskabet hos bankens væsentlige leverandører dækker alle bankens relevante forretningsprocesser og understøttende IT-tjenester. Desuden mangler banken overblik over status på leverandørernes læringspunkter fra deres beredskabsafprøvninger. Finanstilsynet har derfor påbudt AL at styrke bankens opfølgning på afprøvninger af IT-beredskabet hos bankens væsentlige leverandører.

Bankens solvensbehov var den 30. juni 2022 opgjort til 10,0 pct. Banken havde i sin seneste solvensopgørelse ikke taget tilstrækkelig højde for ovenstående mangler. Inspektionen førte derfor til en forøgelse af solvensbehovet til afdækning af operationelle risici relateret til mangler i IT-sikkerhedsstyring, IT-risikostyring samt IT-beredskab svarende til i alt 0,2 procentpoint.