FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Styret i SANTANDER CONSUMER BANK AS
Postboks 177
1325 LYSAKER

VÅR REFERANSE	DERES REFERANSE		DATO
23/7558	Silje Due Bugge		12.03.2024

Tilsynsrapport

Finanstilsynet gjennomførte IKT-tilsyn i Santander Consumer Bank AS 19. og 20. september 2023. Tilsynet ble gjennomført digitalt ved hjelp av Teams. Tilsynet hadde som formål å gjøre en vurdering av hvordan foretaket administrerer, utvikler, drifter, vedlikeholder og sikrer IKT-systemer og -tjenester. Finanstilsynet så på styring med og kontroll av IKT-virksomheten, og vurderte spesielt foretakets styring med og forvaltning av data og datakvalitet, endringshåndtering og utkontraktering relevant for IKT-området. Tilsynet var begrenset til å omfatte virksomheten i Norge.

Til grunn for tilsynsrapporten ligger Finanstilsynets foreløpige rapport datert 29. november 2023 og styrets kommentarer til rapporten i brev av 5. februar 2024.

Finanstilsynet har følgende merknader etter tilsynet:

Overordnet styring og kontroll

Organisering

Det framgår av finansforetaksloven § 8-6 første ledd at styret skal sørge for forsvarlig organisering av virksomheten. Videre i lovens § 13-5 andre ledd stilles det krav om at et finansforetak skal ha uavhengige kontrollfunksjoner med ansvar for risikostyring, etterlevelse og internrevisjon. CRR/CRD IV-forskriften stiller krav i § 38 om at foretaket skal ha en uavhengig risikokontroll-funksjon med tilstrekkelig kompetanse og ressurser, og at risikokontrollfunksjonen skal sikre at alle vesentlige risikoer i foretaket er identifisert, målt og rapportert av de relevante organisatoriske enhetene. Forskriften stiller videre krav i § 39 at foretaket skal ha en uavhengig kontrollfunksjon for kontroll av etterlevelse, og retningslinjer og prosedyrer for å avdekke risiko for at foretaket ikke oppfyller sine forpliktelser etter lov og forskrift. I § 40 stiller forskriften krav om internrevisjon.

I foreløpig rapport pekte Finanstilsynet på at det ikke framgikk av mottatt dokumentasjon hvordan beslutninger som gjelder IKT-virksomheten fattes i foretaket og at det ikke var dokumentert hvordan roller og ansvar på IKT-området fordeles mellom første og andre forsvarslinje. Finanstilsynet stilte spørsmål ved uavhengigheten til foretakets kontrollfunksjoner i andre forsvarslinje på IKT-området og minnet om at uavhengige kontrollfunksjoner ikke er forenelig med utøvende funksjoner i første forsvarslinje.

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00

post@finanstilsynet.no
www.finanstilsynet.no

Saksbehandler
Irene Støback Johansen
Dir. tlf. 22 93 96 44

Det framgår av styrets svar at det er enig i at uavhengige kontrollfunksjoner ikke er kompatibelt med utøvende funksjoner i første forsvarslinje. Etter styrets vurdering oppfyller foretakets organisasjon kravene i regelverket. Styret mener at foretaket har atskilt ansvaret mellom den første og den andre forsvarslinjen for IKT-området, slik at den andre forsvarslinjen er uavhengig.

Finanstilsynet merker seg styrets svar, men understreker viktigheten av at roller og ansvar på IKT-området er tydelig definert og dokumentert i relevante og hensiktsmessige instrukser og retningslinjer.

Rapportering av IKT-risiko

Etter finansforetaksloven § 8-6 fjerde ledd skal styret føre tilsyn med den daglige ledelse og foretakets virksomhet for øvrig, og sørge for at daglig leder regelmessig gir styret informasjon om foretakets virksomhet. Styrets rolle knyttet til foretakets system for risikostyring og internkontroll er utdypet i CRR/CRD IV-forskriften § 35.

Finanstilsynet stilte i foreløpig rapport spørsmål ved om en frekvens på årlig rapportering av IKT-risiko til styret fra risikoeier i første forsvarslinje er tilstrekkelig for at styret skal kunne ha en oversikt over, styring med og kontroll på IKT-risikoen i foretaket. Fra styrets svar tar Finanstilsynet til etterretning at styret vil vurdere behovet for å endre både hyppigheten og nivået av rapportering av IKT-risiko fra den første forsvarslinjen i foretaket.

Finanstilsynet ba videre i foreløpig rapport styret redegjøre for hvordan andre forsvarslinje sikrer at foretaket etterlever sine forpliktelser innen IKT-området. Fra styrets svar framgår det at styret anser andrelinjens nåværende oppfølging som tilfredsstillende. Styret vil imidlertid, som svar på Finanstilsynets anmerkning, og knyttet til implementeringen av DORA-forordningen, vurdere om ansvarsområdene til etterlevelsesfunksjonen og risikofunksjonen bør endres. Finanstilsynet tar styrets svar til etterretning.

I foreløpig rapport stilte Finanstilsynet spørsmål ved om datastyring og -forvaltning vurderes inkludert i revisjonsplanen for 2024, da denne bør ta utgangspunkt i risiko. Finanstilsynet kan ikke se at styret i sitt svarbrev har kommentert dette. Finanstilsynet forventer at revisjonsplanen for inneværende år har revisjonsaktiviteter som inkluderer datastyring og -forvaltning.

Styring med og kontroll av IKT-risiko

Utkontraktering

I henhold til IKT-forskriften § 2 skal foretaket ha retningslinjer for å sikre at utkontraktert IKT-virksomhet oppfyller kravene i § 12. Dette gjelder blant annet krav til skriftlig avtale, der avtalen skal sikre foretakets rett til å kontrollere, herunder revidere, leverandørens aktiviteter, samt Finanstilsynets tilgang til opplysninger og mulighet for å føre tilsyn hos IKT-leverandøren.

Foretaket har ansvar for risikostyring og internkontroll også der hele eller deler av virksomheten er utkontraktert, jf. IKT-forskriften § 12. Det er Finanstilsynets vurdering at for å ha god styring på og kontroll med egen IKT-virksomhet, også den som er utkontraktert, bør foretaket gjennomføre egne kontroller både når det gjelder risiko og etterlevelse.

Finanstilsynet ba i foreløpig rapport foretaket redegjøre for andre forsvarslinjes egne kontroller av risiko og etterlevelse av utkontraktert IKT-virksomhet da det ikke framgikk av mottatt dokumentasjon.

Styret redegjør i svarbrevet for hvordan foretakets risikofunksjon i andre forsvarslinje følger opp og kontrollerer foretakets leverandørstyring inkludert hvordan foretakets komité for utkontraktering og leverandørstyring overvåker, gir anbefalinger og fatter beslutninger om utkontraktering, leverandørstyring og avtaler.

Finanstilsynet kan imidlertid ikke se av styrets svar at foretakets andre forsvarslinje gjennomfører egne vurderinger og kontroller av leverandørene. Finanstilsynet forventer at foretakets andre forsvarslinje gjennomfører egne vurderinger av foretakets utkontrakterte tjenester, og de prosesser som leverandørene benytter for å understøtte IKT-leveransene til foretaket.

Datastyring og -forvaltning

I henhold til IKT-forskriften § 4 skal foretaket fastsette kvalitetsmål for de enkelte deler av IKT-virksomheten. Kvalitetsmålene skal være knyttet opp mot foretakets øvrige mål og foretaket skal ha dokumenterte prosedyrer for oppfølging av de fastsatte kvalitetsmålene. Videre skal driften av IKT-virksomheten i henhold til IKT-forskriften § 8 første ledd være basert på dokumenterte prosedyrer som skal sikre fullstendig, rettidig og korrekt behandling og oppbevaring av data.

I foreløpig rapport vurderte Finanstilsynet foretakets datakvalitetskontroller som hensiktsmessige, men at foretaket må fortsette arbeidet med samme styrke for å sikre kontinuerlig justering og forbedring av datakvaliteten, da foretakets datastyring og -forvaltning fortsatt har et forbedringspotensial.

Finanstilsynet tar til etterretning styrets svar om at selv om foretaket har styrket kontrollmiljøet for datakvalitet betraktelig de siste årene, er styret enig i at foretaket fortsatt skal prioritere dette arbeidet og sørge for kontinuerlige justeringer og forbedringer.

Finanstilsynet stilte videre i foreløpig rapport spørsmål til hvorfor kvaliteten og konsistensen på kundedataene ikke er et tydeligere prioritert mål i foretakets styringsdokumentasjon.

Fra styrets svar framgår det at det å sikre kvalitet og konsistens i kundedataene er et av foretakets prioriterte mål, og styret er enig i at styringsdokumentene bør endres slik at denne prioriteringen framgår tydeligere. Finanstilsynet tar styrets svar til etterretning.

Endringshåndtering

I henhold til IKT-forskriften § 9 første ledd skal foretaket sikre at prosedyrer for avviks- og endringshåndtering foreligger og følges. Det følger videre av forskriftens fjerde ledd at prosedyrene for endringshåndtering skal omfatte alle endringer som kan påvirke IKT-systemene og skal sikre forsvarlig, formell behandling og dokumentering av endringene. Foretaket skal videre sikre at prosedyrene for endringshåndtering gir en stabil, planlagt og forutsigbar drift.

Når det gjelder endringshåndtering er databaser som Configuration Management Database (CMDB) en viktig kilde til informasjon. I foreløpig rapport stilte Finanstilsynet spørsmål ved om foretakets

CMDB trenger å utvides med flere elementer og øke graden av automatisk oppdatering, som ledd i å redusere risikoen ved endringer. Finanstilsynet ba om foretakets vurdering av status på CMDB målt mot foretakets mål for CMDB.

Finanstilsynet tar til etterretning at styret er enig i behovet for å videreutvikle foretakets CMDB og at dette arbeidet allerede er startet.

Finanstilsynet ber om å motta kopi av protokollen fra styremøtet hvor Finanstilsynets tilsynsrapport blir behandlet.

Kopi av dette brevet bes sendt til valgt revisor.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Irene Støback Johansen
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.