FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Styret i SANTANDER CONSUMER BANK AS
Postboks 177
1325 LYSAKER

Vår referanse
25/15170
Deres referanse

28.05.2026

Tilsynsrapport

1 Innledning

Finanstilsynet har gjennomført IKT-tilsyn med Santander Consumer Bank AS (foretaket). Formålet med tilsynet var å gjøre en vurdering av hvordan foretaket administrerer, utvikler, drifter, vedlikeholder og sikrer IKT-systemer og -tjenester. Finanstilsynet så på foretakets styring med og kontroll av IKT-virksomheten med spesiell vekt på hvordan foretaket overholder regulatoriske krav knyttet til bruk av IKT-tjenesteleverandører, samt håndtering av IKT-risiko, IKT-sikkerhet og beredskapsarbeid. Tilsynet var i tillegg et oppfølgingstilsyn etter tilsyn 19. og 20. september 2023. Finanstilsynet gjennomførte møte med foretaket 3. og 4. februar 2026. Denne tilsynsrapporten bygger på Finanstilsynets foreløpige rapport fra 26. mars 2026 og styrets kommentarer til denne 28. april 2026.

2 Finanstilsynets oppsummering

Tilsynet avdekket enkelte mangler ved foretakets styring med og kontroll av IKT-virksomheten. Dette gjelder særlig avklaringen av roller og ansvar i andre forsvarslinje for oppfølging av etterlevelse av DORA-regelverket, dokumentasjon av styrets vurderinger og beslutninger i styreprotokollene, videreutvikling av datastyring og dataforvaltning, uavhengige kontroller og revisjoner av tjenester satt ut til IKT-tjenesteleverandører, samt sårbarhets- og patchhåndtering.

3 Finanstilsynets vurderinger

Finanstilsynet har følgende merknader etter det stedlige tilsynet:

3.1 Overordnet styring og kontroll

3.1.1 Organisering av ansvar for kontroll med etterlevelsen av DORA i andrelinjen

Styret skal sørge for forsvarlig organisering av virksomheten, og det stilles krav om at et finansforetak skal ha uavhengige kontrollfunksjoner med ansvar for risikostyring, etterlevelse og internrevisjon. Det framgår av finansforetaksloven § 8-6 første ledd og § 13-5 andre ledd. CRR/CRD-forskriften stiller krav i § 38 om at foretaket skal ha en uavhengig risikokontrollfunksjon 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 om 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. Forskriften presiserer kravene til internrevisjon i § 40.

Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00
post@finanstilsynet.no
finanstilsynet.no

Saksbehandler
Jarleif Lødøen
Dir. tlf. 22 93 98 00

I henhold til DORA art. 5 nr. 1 skal foretak underlagt DORA ha et internt rammeverk for styring og kontroll som sikrer en effektiv og forsvarlig styring av IKT-risiko for å oppnå et høyt nivå av digital operasjonell motstandsdyktighet. Videre følger det av art. 5 nr. 2 bokstav c) at ledelsen skal fastsette klare roller og ansvarsområder for alle IKT-relaterte funksjoner og etablere hensiktsmessige styringsordninger for å sikre effektiv og rettidig kommunikasjon, samarbeid og koordinering mellom disse funksjonene.

Finanstilsynet pekte i foreløpig rapport på at foretaket har plassert ansvaret for oppfølging av etterlevelse og implementering av DORA i risikokontrollfunksjonen. Oppfølgingen av regelverk på IKT-området skiller seg dermed fra oppfølgingen av annet regelverk, som det andre betalingstjenestedirektivet (PSD2), personvernforordningen (GDPR) og hvitvaskingsregelverket (AML), der etterlevelsesfunksjonen har ansvar for å følge opp etterlevelsen. Finanstilsynet stilte spørsmål ved om den valgte arbeidsdelingen i andrelinjen mellom etterlevelse og risikokontrollfunksjonen for oppfølging av etterlevelsen av DORA-loven og -forskriften er i tråd med foretakets egne stillingsinstrukser og policy.

Styret skriver i sitt svar at foretakets internkontrollprogram bygger på en modell med tre forsvarslinjer, og at andrelinjeoppfølgingen er organisert gjennom aktiviteter i både risikofunksjonen og etterlevelsesfunksjonen. Styret viser til at risikofunksjonen har et dedikert ansvar for andrelinjeoppfølging av IKT- og DORA-relaterte risikoer. Styret skriver samtidig at etterlevelsesfunksjonen utøver uavhengig andrelinjeoppfølging gjennom et program for etterlevelse, deltakelse i komiteer, årlig risikovurdering og testing. Styret opplyser videre at det tar Finanstilsynets vurdering til etterretning og at det vil vurdere behovet for å justere roller og ansvar for risikofunksjonen og etterlevelsesfunksjonen. For å styrke andrelinjens overvåking av etterlevelsesrisiko innenfor IKT-området vil etterlevelsesfunksjonen inkludere risikobaserte aktiviteter i årsplanen for 2026 og rapportere regelmessig til styret om foretakets etterlevelse av DORA.

Finanstilsynet tar styrets svar til etterretning.

3.1.2 Manglende dokumentasjon av styrets vurderinger i styreprotokollene

Det framgår av § 35 i CRR/CRD-forskriften at foretakets styre skal godkjenne og regelmessig vurdere retningslinjer for å påta foretaket risikoer og for å identifisere, styre, overvåke og kontrollere risikoer som foretaket er eller kan bli eksponert for. Styret skal sikre seg tilgang til risikoinformasjon og fastsette omfang, format og frekvens på rapporteringen.

Finanstilsynet pekte i foreløpig rapport på at kun et fåtall av styreprotokollene som omhandlet IKT-relaterte emner for 2024 og 2025 dokumenterte at det hadde funnet sted diskusjoner i styret, og hvilke vurderinger styret hadde gjort. Flere sentrale saker var protokollført uten kommentarer eller spørsmål fra styret. Finanstilsynet ba derfor styret utvide omtalen i styreprotokollene slik at styrets vurderinger og beslutninger knyttet til IKT-risiko dokumenteres tilstrekkelig til at de kan etterprøves i ettertid.

Styret opplyser i sitt svar at det er innstilt på å sikre forsvarlig behandling av vesentlige risikoområder, herunder IKT- og cyberrisiko, i samsvar med CRR/CRD-forskriften § 35. Styret bekrefter at det vil styrke protokolleringen slik at vurderinger og beslutninger om IKT-risiko kan etterprøves i ettertid. Styret presiserer samtidig at de aktuelle sakene har vært gjenstand for substansiell behandling og diskusjon både i styrets risikoutvalg og i styret.

Finanstilsynet tar styrets svar til etterretning.

3.2 IKT-drift – datakvalitet

Foretak som er underlagt DORA, skal etablere tiltak som forebygger manglende tilgjengelighet, svekkelse av autentisitet og integritet, brudd på fortrolighet samt tap av data. Dette følger av DORA art. 9 nr. 3 bokstav b) og c). Foretakene skal også sikre at opplysningene er beskyttet mot risikoer

som oppstår i forbindelse med databehandling, herunder dårlig forvaltning, prosessrelaterte risikoer og menneskelige feil.

Finanstilsynet pekte i foreløpig rapport på at mangelfull datakvalitet og manglende kontroller til å avdekke dette har vært en gjentagende årsak til hendelser. Finanstilsynet viste videre til at foretakets egenevalueringer av datakvalitet svekket seg over flere år, før den har bedret seg de siste to årene. Egenevalueringen viser imidlertid at den fortsatt ligger under tidligere nivå. Internrevisjonen har dessuten påpekt manglende eller forsinket gjennomføring av tiltak, og at enkelte utbedringstiltak har vært åpne over lengre tid. I den foreløpige rapporten opprettholdt Finanstilsynet vurderingen fra IKT-tilsynet i 2023 om at foretakets datakvalitetskontroller synes hensiktsmessige. Samtidig understreket Finanstilsynet behovet for å videreføre arbeidet med løpende justering og forbedring med uforminsket styrke, ettersom datastyring og -forvaltning fortsatt har forbedringspotensial.

Styret skriver i sitt svar at det anerkjenner Finanstilsynets vurdering og merker seg forventningen om videre forbedring av foretakets datastyring og -forvaltning. Styret bekrefter at foretaket vil fortsette å ha høy oppmerksomhet på datakvalitet, med mål om å videreutvikle bankens styring og forvaltning av data i tråd med regulatoriske forventninger og beste praksis i bransjen.

Finanstilsynet tar styrets svar til etterretning.

3.3 IKT-tjenesteavtaler og IKT-tredjepartsrisiko

Foretaket har ansvar for risikostyring og internkontroll også der deler av virksomheten leveres av IKT-tjenesteleverandører, jf. DORA art. 28. Det skal etableres et system for leverandørstyring med klare roller og løpende risikovurdering. Foretaket skal ha retningslinjer som sørger for at det stilles tydelig definerte krav som kan følges opp gjennom hele leverandørforholdet. I kommisjonsforordning (EU) 2024/1773, regulatorisk teknisk standard for krav til retningslinjer for kontraktsvilkår ved bruk av IKT-tjenester som støtter kritiske eller viktige funksjoner, art. 9 nr. 2 beskrives hvordan et foretak skal vurdere om IKT-tjenesteleverandører møter ytelses- og kvalitetsstandarder i henhold til avtale og interne retningslinjer. I artikkelens bokstav (e) framgår det at det skal gjennomføres uavhengige gjennomganger og revisjoner for å vurdere etterlevelse av regulatoriske krav og interne retningslinjer.

Finanstilsynet pekte i tilsynet i 2023 på at foretakets andrelinje må gjennomføre uavhengige leverandørkontroller. Foretaket har ettersendt risikofunksjonens kontrollplan for 2026. Der framgår det at andrelinjen blant annet skal gjennomføre uavhengige risikovurderinger av IKT-tjenesteleverandører, og utfordre førstelinjen på deres kontrollhandlinger av IKT-tjenesteleverandører. Finanstilsynet pekte i foreløpig rapport på at risikofunksjonens kontrollplan for 2026 ikke konkretiserte omfang, metode eller hvilke leverandører som skal omfattes av uavhengige kontroller. Finanstilsynet stilte spørsmål ved hvordan foretaket sikrer at det gjennomføres uavhengige gjennomganger og revisjoner av tjenester satt ut til IKT-tjenesteleverandører.

Styret skriver i sitt svar at selv om styret forstår denne merknaden som rettet mot andrelinjen, ønsker styret å framheve at internrevisjonen har dekket sentrale IKT-risikoer i 2024–2025. Styret opplyser at internrevisjonen har et dedikert team og metodikk for IKT-revisjoner, og at alle IKT-risikoer skal gjennomgås minst én gang i en fireårig revisjonsplansyklus, avhengig av revisjonsresultatene.

Når det gjelder andre forsvarslinje, skriver styret at risikofunksjonens kontrollplan skal styrkes, og at en revidert versjon av den årlige kontrollplanen skal legges fram for styret for behandling og godkjenning i andre kvartal 2026. Den reviderte kontrollplanen skal inneholde ytterligere detaljer om omfang, metode og leverandører. Styret opplyser også at relevante funn fra uavhengige kontroller og tester rapporteres og eskaleres i en ny, dedikert risikorapport, og at andrelinjen gjennomfører tematiske gjennomganger, stikkprøver, verifikasjonshandlinger og andre uavhengige gjennomganger.

Finanstilsynet tar styrets svar til etterretning.

3.4 IKT-sikkerhet – sårbarhets- og patchhåndtering

3.4.1 [redacted] sårbarhetsoppdateringer

Foretak underlagt DORA skal etablere og opprettholde effektive sikkerhetsmekanismer for å beskytte IKT-systemer og data. Dette følger av DORA art. 9. Dette omfatter krav til kontinuerlig overvåking og kontroll av IKT-systemers sikkerhet og virkemåte, samt etablering av retningslinjer, prosedyrer og tekniske tiltak som sikrer håndtering av tekniske sårbarheter og gjennomføring av nødvendige oppdateringer. Kravene utdypes i kommisjonsforordning (EU) 2024/1774, som stiller krav til risikobasert sårbarhetshåndtering, dokumentert patchstyring og kontroll med IKT-tjenester levert av tredjepartsleverandører.

Finanstilsynet viste i foreløpig rapport til funn fra internrevisjonen i 2025, [redacted] Finanstilsynet pekte videre på at antallet sårbarhetsoppdateringer som var gjennomført innen SLA-kravet økte betydelig i 2025, [redacted] Finanstilsynet forventet at foretaket fortsatte arbeidet med å sikre at sårbarhetsoppdateringer utføres innen tidsfristen.

Styret skriver i sitt svar at den omtalte revisjonen ble lukket med en oppfølgingsrevisjon, [redacted]

Finanstilsynet tar styrets svar til etterretning.

3.4.2 Mangelfull rutine for sårbarhetsoppdatering

Både for program- og maskinvare som omfattes av automatiske oppdateringsmekanismer og de som krever manuelle rutiner, skal foretaket ha dokumenterte og risikobaserte prosesser for sårbarhetshåndtering og oppdatering. Disse prosessene skal inngå som en integrert del av foretakets helhetlige IKT-risikostyring, jf. DORA art. 8 og art. 9 nr. 1, 2 og 4.

Finanstilsynet pekte i foreløpig rapport på at foretakets rutine for patching ikke ga tilstrekkelig oversikt over hvilken program- og maskinvare som omfattes av automatiske oppdateringsløsninger og hvilken som ikke lar seg kontrollere og oppdatere gjennom slike mekanismer. Rutinen stilte heller ikke krav til verifisering av at oppdateringer gjennomføres som forutsatt for alle relevante systemer, herunder at de prioriteres i tråd med systemenes kritikalitet og tilhørende risiko. Finanstilsynet forventer at foretaket etablerer og dokumenterer tydelige og etterprøvbare kontrollmekanismer for automatiske og manuelle oppdateringer.

Styret erkjenner i sitt svar at dagens rutine ikke tilstrekkelig angir hvilke eiendeler eller hvilken maskinvare som inngår i automatiserte prosesser. Foretaket vil derfor oppdatere rutinen med mer detaljerte beskrivelser og avgrensning av automatisert patching og hvilke eiendeler som håndteres manuelt. Styret opplyser at all planlagt patching inngår i en automatisert prosess, og at resultatene reflekteres og oppdateres i CMDB basert på patchgruppe og registrert endring. Styret viser videre til at foretaket følger Santander-konsernets prioriteringsmodell for sårbarheter og patching, og at avvik i patchprosessen rapporteres og håndteres gjennom endringshåndtering fram til løsning.

Finanstilsynet tar styrets svar til etterretning.

4 Videre oppfølging

Vi ber foretaket sende kopi av dette brevet til valgt revisor.

For Finanstilsynet

Wenche Eline Fagereng
seksjonsleder

Jarleif Lødøen
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk.