FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

STOREBRAND ASSET MANAGEMENT AS
Postboks 500
1327 LYSAKER

Vår referanse
25/10098
Deres referanse

05.03.2026

Tilsynsrapport

1. Innledning

Finanstilsynet gjennomførte IKT-tilsyn 17. og 18. november 2025 i Storebrand Asset Management AS (SAM). Formålet med tilsynet var å gjøre en vurdering av hvordan foretaket administrerer, utvikler, drifter, vedlikeholder og sikrer IKT-systemer og -tjenester. For dette området så tilsynet på styring med og kontroll av IKT-virksomheten. Tilsynet hadde fokus på systemløsninger som støtter foretakets kjernevirksomhet, spesielt IKT-systemer levert av IKT-tjenesteleverandører.

Til grunn for disse merknadene ligger Finanstilsynets foreløpige rapport datert 23. desember 2025 og styrets kommentarer til rapporten i brev av 12. februar 2026.

2. Finanstilsynets oppsummering

Tilsynet avdekket ingen vesentlige mangler ved foretakets styring med og kontroll av IKT-virksomheten. Det er noen mindre påpekninger knyttet til foretakets risikostyring, blant annet uklarheter i overordnet oppfølging av styringsdokumentasjon, utkontraktert IKT-virksomhet og testing av beredskapsplaner.

3. Finanstilsynets vurderinger

Finanstilsynet har følgende merknader etter det stedlige tilsynet:

3.1. Overordnet styring og kontroll

DORA-forordningen art. 5 nr. 1 stiller krav til at foretak underlagt DORA skal ha et forsvarlig, helhetlig og veldokumentert rammeverk for IKT-risikostyring som en del av sitt overordnede risikostyringssystem, slik at de kan håndtere IKT-risiko på en rask, effektiv og grundig måte og oppnå en høy grad av digital operasjonell motstandsdyktighet. Videre følger det av nr. 2 at rammeverket for IKT-risikostyring som et minimum skal omfatte strategier, retningslinjer, framgangsmåter, IKT-protokoller og -verktøyer som er nødvendige for på forsvarlig vis og i tilstrekkelig grad å beskytte alle informasjonsressurser og IKT-ressurser.

Finanstilsynet pekte i foreløpig rapport på at styregodkjente styringsdokumenter som strategier og policyer bør følges opp for å sikre at foretakets planer og drift utføres i henhold til disse. Videre pekte Finanstilsynet på at foretakets andre- og tredjelinje bør følge opp etterlevelsen av strategier og kontrollerer at de styrende dokumentene er operasjonalisert i henhold til disse.

Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

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

Saksbehandler
Stig Ulstein
Dir. tlf. 22 93 99 66

Styret skriver i sitt svar at styret fastsetter styrende dokumenter og strategier relevant for IKT-området, herunder IKT-strategi og at styrende dokumenter og vedtatt strategi operasjonaliseres gjennom henholdsvis rutiner og årlige operasjonelle målsettinger av førstelinje. Videre skriver styret at revidert IKT-strategi vedtas på årlig basis og det mottar regelmessig rapportering på oppnåelse av strategiske målsettinger.

Finanstilsynet tar styrets svar til etterretning og legger til grunn styrets oppfølging av etterlevelse av styregodkjente styringsdokumenter, og at kontrollporteføljene dekker alle relevante områder innenfor IKT.

Finanstilsynet pekte videre i foreløpig rapport på at foretaket må sikre at det har tilstrekkelig IKT-ressurser og -kompetanse på IKT-området i andre forsvarslinje for å utføre nødvendig oppfølging av IKT-tjenesteleverandører.

Styret skriver i sitt svar at styret vurderer årlig ressurssituasjonen for de uavhengige kontrollfunksjonene, og da særlig sett opp mot foretakets utvikling, både når det gjelder omfang og kompleksitet samt det etablerte samarbeidet med konsernfunksjoner. Videre skriver styret at det i de siste årene har vært en økning, både i kapasitet og i kompetanse, innenfor ulike fagområder blant de uavhengige kontrollfunksjonene. Dette gjelder også IKT-området.

Finanstilsynet tar styrets svar til etterretning og legger til grunn at ressurssituasjon og kompetanse for IKT-området per nå er på et tilfredsstillende nivå.

3.2. Virksomhetens konsekvensanalyse

DORA-forordningen presiserer i art. 11 nr. 5 at foretak underlagt DORA skal gjennomføre en konsekvensanalyse av virksomheten for å vurdere forretningsmessige konsekvenser ved IKT-avbrudd. Som en del av konsekvensanalysen skal foretak vurdere hvilke virkninger alvorlige driftsforstyrrelser kan ha. Dette skal gjøres ved å bruke både kvantitative og kvalitative kriterier, basert på relevante interne og eksterne data, samt scenarioanalyser. Analysen skal ta hensyn til hvor kritiske de identifiserte forretningsfunksjonene og støtteprosessene er, samt avhengigheten av tredjeparter og informasjonsressurser – inkludert hvordan disse henger sammen. Foretak skal også sørge for at IKT-ressurser og -tjenester er utformet og brukt i tråd med analysen, spesielt med tanke på å sikre tilstrekkelig redundans (reservekapasitet) for alle kritiske komponenter.

Som del av rammeverket for IKT-risikostyring skal foretak ifølge DORA-forordningen art. 8 nr. 1 identifisere, klassifisere og dokumentere alle forretningsfunksjoner som støttes av IKT. Dette inkluderer roller og ansvarsområder, samt de IKT-ressursene som støtter disse funksjonene. Dokumentasjonen skal også vise hvordan disse elementene henger sammen og hvilke avhengigheter som finnes, med tanke på IKT-risiko.

Finanstilsynet pekte i foreløpig rapport på at foretaket bør utføre kontroller for å sikre at operasjonalisering av krav i konsekvensanalysen er dokumentert og rapporteres på, og at foretakets andrelinje har en sentral rolle i dette arbeidet.

Styret skriver i sitt svar at foretaket har etablert et register hvor avhengigheter mellom forretningsfunksjoner, underliggende IKT-tjenester og tredjeparter er dokumentert og at det her fastsettes og dokumenteres virksomhetens krav til den enkelte IKT-tjeneste basert på kritikalitet på den enkelte forretningsfunksjon og forretningsfunksjonens avhengighet til underliggende IKT-tjenester.

Finanstilsynet tar styret svar til etterretning og legger til grunne at foretaket vil påse at andre forsvarslinje gjennomfører uavhengige kontroller av at de krav som følger av virksomhetens konsekvensanalyse er operasjonalisert av IKT-området.

3.3. IKT-tredjepartsrisiko

I henhold til DORA-forordningen art. 28 nr. 2 skal foretak underlagt DORA ha en strategi og retningslinjer for bruk av IKT-tjenester som understøtter kritiske eller viktige funksjoner når det benyttes IKT-tjenesteleverandører. Retningslinjene skal sikre etterlevelse av kravene i kapittel 5 om styring og kontroll med IKT-tjenestekjøp, samt de detaljerte kravene som framgår av tilhørende delegert kommisjonsforordning (EU) 2024/1773.

Finanstilsynet pekte i foreløpig rapport på at foretaket bør sørge for tilstrekkelig kompetanse og ressurser hos kontraktseier for å sikre oppfølging av leverandører. Andre linje bør utføre kontroller på at IKT-tjenester fra leverandører følges opp i henhold til interne retningslinjer. Videre ble det vist til at den risikobaserte tilnærmingen til oppfølging må tilpasses foretakets konsekvensanalyse av virksomheten.

Styret skriver i sitt svar at de arbeider kontinuerlig med å forbedre styrings -og kontrolloppsettet for IKT-tjenester levert av tredjeparter. Styret skriver videre at foretaket har igangsatt et program for kompetanseheving knyttet til styring og kontroll med IKT, som inkluderer et eget opplæringsprogram for kontraktseiere for å sikre tilstrekkelig kompetanse.

Finanstilsynets tar styrets svar til etterretning.

3.4. Beredskap og kontinuitet

DORA-forordningen presiserer i art. 24 nr. 6 at foretak underlagt DORA minst én gang i året skal sikre at det gjennomføres hensiktsmessige tester av alle IKT-systemer og -applikasjoner som støtter kritiske eller viktige funksjoner. Videre stiller art. 11 nr. 6 (a) krav til at selve planverket skal testes minst én gang i året. Kravene til kontinuitet og testing av kontinuitetsplaner er utdypet i delegert kommisjonsforordning (EU) 2024/1774 art. 24 og 25. Her heter det i art. 25 nr. 5 at finansielle enheter skal dokumentere resultatene av testingen, og at identifiserte mangler som følge av denne skal analyseres, håndteres og rapporteres til ledelsen.

Finanstilsynets pekte i foreløpig rapport på at testing av beredskapsplaner, både for foretakets egne og for IKT-tjenester levert av tredjepartsleverandører, må inkludere relevante informasjonssikkerhetsscenarioer, herunder også verstefalls scenarioer.

Styret skriver i sitt svar at de i sitt arbeid med beredskap vil inkludere komplekse scenarier i sine tester av kriseløsninger, inkludert involvering av tredjeparter og aktiviteter for gjenoppretting og alternativ drift.

Finanstilsynets tar styrets svar til etterretning.

Kopi av dette brevet bes sendt til ekstern og intern revisor.

For Finanstilsynet

Olav Johannessen
seksjonsleder

Stig Ulstein
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk.