FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

AXACTOR NORWAY AS
Postboks 673 Strømsø
3003 DRAMMEN

Vår referanse
25/6331
Deres referanse

07.08.2026

Tilsynsrapport

1 Innledning

Finanstilsynet gjennomførte inkassotilsyn og IKT-tilsyn i perioden 16. til 18. juni 2025 med Axactor Norway AS (heretter omtalt "foretaket"). Formålet med tilsynet av foretakets inkassovirksomhet var å kontrollere foretakets risikovurderinger, internkontroll, rutiner for inndrivelsesprosessen og avstemming av klientmidler. Hensikten med IKT-tilsyn var å gjøre en vurdering av hvordan foretaket administrerer, utvikler, drifter, vedlikeholder og sikrer IKT-systemer og -tjenester. Tilsynet var avgrenset til elektronisk forsvar og tilhørende emner innen IKT-sikkerhet, og styring og kontroll med IKT-virksomheten. Videre ønsket Finanstilsynet å gjøre en vurdering av foretakets beredskapsarbeid relevant for IKT-området, herunder vurdere beredskapen i foretaket og for utkontrakterte IKT-tjenester, samt overholdelse av regulatoriske krav på IKT-området.

Til grunn for tilsynsrapporten ligger Finanstilsynets foreløpige rapport datert 6. januar 2026 og styrets kommentarerX til rapporten i brev av 4. februar 2026.

Finanstilsynet sendte foretaket en tilsynsrapport 26. mai 2026. Den tidligere tilsynsrapporten inneholdt i punkt 3.3 vurderinger som bygget på en uriktig forståelse av inkassoforskriften § 2-2 første ledd siste punktum. Det er ikke grunnlag for å konstatere at foretaket har brutt god inkassoskikk i de sakene som er omtalt der. Denne tilsynsrapporten erstatter den tidligere tilsynsrapporten. Punkt 3.3 er fjernet, mens resten av rapporten er uendret.

2 Finanstilsynets oppsummering

Finanstilsynet ba foretaket om en redegjørelse for foretakets organisering, overordnet risikostyring, rapportering av IKT-risiko, konsekvens analyse, kriseberedskap og foretakets kontroll med utkontrakterte avtaler.

3 Finanstilsynets merknader

3.1 Omkostningsgebyr og motregningserklæring

Ved betalinger fra skyldner i utenlandsk valuta påløper det et omkostningsgebyr hos foretakets bankforbindelse på grunn av omregning av utenlandsk valuta til norske kroner. Omkostningsgebyret motregnes innbetalingen og bokført beløp på klientkonto blir tilsvarende lavere. Foretaket har redegjort for sine rutiner knyttet til dette.

Finanstilsynet tar styrets svar til etterretning.

Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

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

Saksbehandler
Arne Solberg
Dir. tlf. 22 93 98 05

3.2 Inkassoforetakets mottak og behandling av rettsgebyr

Inkassoforetak som mottar inkassoportefølje fra tidligere inkassoforetak/prosessfullmektig sender brev til forliksråd, namsmann eller tingrett for å orientere om ny prosessfullmektig.

Når foretaket overfører inkassoportefølje til nytt inkassoforetak/ny prosessfullmektig, vil det kunne være mottatt rettsgebyr knyttet til rettslige inndrivingstiltak. Foretaket kan derfor fortsatt ha innestående på klientkonto fordi det på tidspunktet for overføringen av saker ikke er mottatt saksinformasjon fra namsmannen som stadfester/tilkjenner saksøker/kreditor rettsgebyr innbetalt av skyldner.

Foretaket har redegjort for sine rutiner knyttet til mottak og behandling av rettsgebyr og Finanstilsynet tar styrets svar til etterretning.

4 IKT

4.1 Organisering

Det stilles krav til risikostyring i forskrift om risikostyring og internkontroll. I forskriften § 3, punkt 4 stilles det krav om at styret skal fastsette prinsipper for risikostyring for foretaket som en helhet og innenfor hvert enkelt virksomhetsområde. Av § 4 framgår det at daglig leder skal påse en forsvarlig risikostyring og internkontroll på basis av en vurdering av aktuelle risikoer, i henhold til retningslinjer fastsatt av styret. Videre skal daglig leder sikre at risikostyring og internkontroll gjennomføres og overvåkes på en forsvarlig måte

Finanstilsynet pekte i foreløpig rapport på at styregodkjente strategier og policyer følges opp for å sikre at drift og planer gjennomføres i tråd med disse, og vurderer at når strategiene for IKT-området ligger i første forsvarslinje, bør etterlevelse, operasjonalisering og kontroll av styrende dokumenter følges opp av foretakets andre- og tredjelinje.

Finanstilsynet tar styrets svar til etterretning og legger til grunn styrets vurdering av dokumentasjon og operasjonaliseringen av denne.

4.2 Overordnet risikostyring

IKT-forskriften § 2 første ledd stiller krav til at foretaket skal fastsette overordnede mål, strategier, og sikkerhetskrav for IKT-virksomheten. Av IKT-forskriften § 3 første ledd skal det fastsettes grenser for akseptabel risiko forbundet med bruk av IKT-systemene og etter § 3 tredje ledd skal det minst en gang årlig, eller ved endringer som har betydning for IKT-sikkerheten, gjennomføres risikoanalyser for å påse at IKT-risikoen styres innenfor akseptable grenser i forhold til foretakets virksomhet. Resultatet av risikoanalysen skal dokumenteres.

Finanstilsynet pekte i foreløpig rapport på at foretakets forsvarslinjer ikke gjennomfører egne kontroller av de utkontrakterte IKT-tjenestene, til tross for at store deler av foretakets IKT-virksomhet er satt ut til eksterne leverandører.

Styret skriver i sitt svarbrev at det er styrets vurdering at foretaket gjennom mottatt materiale viser en moden og strukturert risikostyringsmodell med formelle prosesser, tydelige roller og dokumenterte kontrollmekanismer som oppfyller kravene i IKT-forskriften §§ 2, 3 og 12 samt forskrift om risikostyring og internkontroll §§ 3 og 4.

Finanstilsynet tar styrets svar til etterretning og legger til grunn at foretaket har operasjonalisert de prosesser, rutiner og retningslinjer som er mottatt.

4.3 Rapportering av IKT-risiko

Finanstilsynet pekte i den foreløpige rapporten på at foretaket mottar årlige ISAE 3402-erklæringer fra sine IKT-tjenesteleverandører, men at disse primært er utarbeidet for eksternt revisjonsformål og ikke gir noen garanti for at foretakets kritiske systemer inngår i revisjonens testutvalg.

Erklæringene gir en indikasjon på leverandørenes styring og kontroll og kan etter Finanstilsynets vurdering ikke anses som en fullgod bekreftelse på etterlevelse av foretakets krav. Finanstilsynet vurderer det derfor som viktig at foretaket gjennomfører egne vurderinger av relevans og dekning ved mottak av ISAE-rapporter.

Styret skriver i sitt svar at informasjon om IKT-risiko i dag formidles gjennom ledelseslinjen og inngår løpende i daglig leders rapportering til styret. Etter styrets vurdering gir dette et reelt og tilstrekkelig beslutningsgrunnlag. Styret vil imidlertid vurdere å styrke den formelle distribusjonen av sentrale IKT-rapporter for å øke sporbarhet og transparens.

Finanstilsynet tar styrets svar til orientering.

4.4 Forretningsmessig konsekvensanalyse

Ifølge IKT-forskriften § 13 skal det foreligge oppdatert dokumentasjon av det enkelte IKT-system som er av betydning for foretakets virksomhet. Hensiktsmessige planer og tiltak for tilgjengelighet og kontinuitet bør etableres med utgangspunkt i konsekvensanalyser for foretakets kritiske forretningsprosesser. Forretningsmessig konsekvensanalyse skal bidra til å sikre at foretakets beredskapsplaner utarbeides med basis i forretningsmessig kritikalitet. Planene skal basere seg på foretakets prioriteringer for gjenoppretting av forretningskritiske tjenester og prosesser. Prioriteringene for gjenoppretning skal basere seg på resultatene fra analysen hvor det også skal framgå hva som er akseptabel nedetid for det enkelte IKT-system. Beredskapsplanene, som viser foretakets prioriteringer for gjenoppretting, bør formidles til relevante leverandører. For å verifisere at det er etablert fungerende planer og løsninger må det minst årlig foretas opplæring, øvelse og testing, jf. IKT-forskriften § 11.

Finanstilsynet pekte i den foreløpige rapporten på at foretaket ikke har gjennomført en forretningsmessig konsekvensanalyse, og at kriseplanen dermed er utarbeidet uten virksomhetsmessige prioriteringer. Finanstilsynet forventer at foretaket utarbeider slike analyser, inkludert vurdering av systemkritikalitet og akseptabel nedetid per system, og at resultatene formidles til relevante leverandører og inngår i ordinær drift.

Styret skrev i sitt svarbrev at styret tar Finanstilsynets merknad til etterretning og vil etablere en formell BIA i tråd med forskriftens krav.

Finanstilsynet tar styrets svar til orientering.

4.5 Kriseberedskap

I IKT-forskriftens § 11 framgår kravene til at foretaket skal ha en dokumentert kriseplan som skal kunne iverksettes dersom IKT-driften ikke kan opprettholdes som følge av en krise, og at det minst årlig skal gjennomføres opplæring, øvelse og testing, med dokumentasjon av testresultater, som viser at kriseløsningen virker som forutsatt.

Finanstilsynet pekte i den foreløpige rapporten på at foretaket sin testing av kriseløsningen ikke er tilstrekkelig, da tester gjennomføres uten grunnlag i en dokumentert forretningsmessig

konsekvensanalyse og uten klare krav til leverandører. Styret har i sin tilbakemelding redegjort om behovet for en mer formelt forankret og BIA-basert beredskapstesting.

Finanstilsynet tar styrets svar til orientering.

4.6 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. Videre framgår det av samme paragraf at *"avtaler om utkontraktering av IKT-virksomhet og endring av slike avtaler skal behandles av styret. Styret skal presenteres en plan for utkontrakteringen, en risikovurdering av utkontrakteringsforholdet og en beskrivelse av hvordan foretaket skal sikre leveransene".*

Finanstilsynet pekte i den foreløpige rapporten på at det er Finanstilsynets vurdering at foretaket ikke stiller tilstrekkelige krav til leverandører og underleverandører basert på foretakets egen sikkerhetspolicy, og at krav som gjelder internt ikke videreføres i utkontrakteringen. Tilsynet merket seg også utfordringer med å få fullstendig informasjon fra leverandører ved kontroller eller revisjoner.

Styrets skriver i sitt svar at utkontraktering av IKT-virksomhet innebærer særskilt ansvar etter IKT-forskriften §§ 2 og 12. Foretaket mener at Finanstilsynets vurdering ikke gjenspeiler den faktiske kontrollen selskapet utøver over sine leverandører. Etter styrets vurdering foreligger det en forsvarlig og dokumentert styringsmodell for utkontraktert IKT-virksomhet i tråd med forskriftens krav.

Finanstilsynet tar styrets svar til etterretning og legger til grunn at foretaket stiller tilstrekkelige krav til leverandører og underleverandører basert på foretakets egen sikkerhetspolicy. Videre legges det til grunn at foretaket mottar fullstendig informasjon fra leverandører ved kontroller eller revisjoner.

4.7 IKT-sikkerhet

IKT-forskriften § 5 stiller krav om at foretaket skal ha prosedyrer for å sikre beskyttelse av utstyr, systemer og informasjon av betydning for foretakets virksomhet, mot skader, misbruk, uautorisert adgang og endring, samt hærverk. Foretaket har ansvar for risikostyring og internkontroll også der hele eller deler av virksomheten er utkontraktert, jf. IKT-forskriften § 12. Det framgår av bestemmelsen at foretaket må sikre at leverandørens aktiviteter kontrolleres. Videre skal det finnes retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene.

IKT-forskriften § 13 stiller krav til at det er etablert en *"oppdatert oversikt over organisasjon, utstyr, IKT-systemer og vesentlige forhold i IKT-virksomheten"*. Finanstilsynets vurdering er at dette omfatter oppdaterte oversikter over IT-systemer, nettverksenheter, databaser etc. og at utstyrsoversikten bør inneholde tilstrekkelige konfigurasjonsdata og angi avhengigheter mellom utstyr/komponenter.

I foreløpig rapport pekte Finanstilsynet på at foretaket ikke kan dokumentere at krav til konfigurasjonsstyring er ivaretatt hos egne IKT-tjenesteleverandører. Tilsynet vurderte at foretaket mangler en oppdatert og verifiserbar oversikt over infrastrukturkomponenter og deres sikkerhetsstatus, og at det ikke er etablert tilstrekkelige kontroller for å sikre at leverandører følger kravene i IKT-forskriften § 12.

Styret skriver i sitt svar at de ikke kan slutte seg til Finanstilsynets vurdering av manglende oversikt, kontroll eller modenhet.

Finanstilsynet tar styrets svar til etterretning og legger til grunn at det for IKT-tjenesteleverandører stilles krav til at det er etablert en *"oppdatert oversikt over organisasjon, utstyr, IKT-systemer og vesentlige forhold i IKT-virksomheten"* foreligger og at dette omfatter oppdaterte oversikter over IT-systemer, nettverksenheter, databaser etc. og at utstyrsoversikten inneholder tilstrekkelige konfigurasjonsdata og angi avhengigheter mellom utstyr/komponenter

Vi ber foretaket sende kopi av dette brevet til revisor.

For Finanstilsynet

Arne Solberg
seksjonsleder

Marianne Kalleberg
seniorrådgiver

Dokumentet er godkjent elektronisk.