FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Styret i OBOS-BANKEN AS
Postboks 6666 st olavs plass
0129 OSLO

Vår referanse
25/1324
Deres referanse

01.07.2025

Tilsynsrapport

1 Innledning

Finanstilsynet gjennomførte stedlig IKT-tilsyn OBOS-banken (foretaket) 13. mars 2025.

Hensikten med tilsynet var 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 med spesiell vekt på IKT-risiko, endrings- og avvikshåndtering, datastyring og forvaltning, IKT-sikkerhet, utkontraktering og beredskap.

Til grunn for tilsynsrapporten ligger Finanstilsynets foreløpige rapport datert 9. mai 2025 og styrets kommentarer til rapporten i brev av 6. juni 2025.

2 Finanstilsynets oppsummering

Tilsynet avdekket enkelte forhold der foretaket bør gjøre endringer og tilpasninger i sin styring med og kontroll av IKT-virksomheten. Dette var blant annet knyttet til IKT-strategien som i større grad bør reflektere målene i virksomhetsstrategien, til virksomhetens konsekvensanalyse som manglet forretningens konkrete krav til IKT-systemene, og til mangler i de uavhengige kontrollfunksjonenes rapportering. Videre peker Finanstilsynet på mangelfulle rutiner for enkelte områder, samt til mangler i gjennomføringen av beredskapstester.

3 Finanstilsynets vurderinger

Dette tilsynet ble gjennomført i henhold til IKT-forskriften som gjaldt for IKT-området fram til 1. juli 2025.

3.1 Overordnet styring og kontroll

Overordnede styringsdokumenter

Styret skal godkjenne og regelmessig vurdere retningslinjer for å påta foretaket risikoer og for å identifisere, styre, overvåke og kontrollere risikoene, jf. CRR/CRD-forskriften § 35. IKT-forskriften § 2 første ledd stiller videre krav til at foretaket skal fastsette overordnede mål, strategier og sikkerhetskrav for IKT-virksomheten, og i § 3 første ledd stilles det krav om at foretaket skal fastsette kriterier for akseptabel risiko forbundet med bruk av IKT-systemene.

Finanstilsynet pekte i foreløpig rapport på at foretakets IKT-strategi i hovedsak er rettet mot IKT-sikkerhet. Finanstilsynet anbefalte at IKT-strategien i større grad bør utformes slik at den støtter opp under målene i virksomhetsstrategien. Særlig bør digitale satsinger og prioriteringer reflekteres i IKT-strategien.

Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

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

Saksbehandler
Åshild Johnsen
Dir. tlf. 22 93 97 02

Finanstilsynet har fra styrets svar merket seg at foretaket har identifisert at IKT-strategien var noe mangelfull og ikke tilstrekkelig formalisert. Foretaket er enig i Finanstilsynets observasjoner og vil revidere IKT-strategien.

Finanstilsynet tar styrets svar til etterretning.

Virksomhetens konsekvensanalyse

Det skal foreligge oppdatert dokumentasjon av det enkelte IKT-system som er av betydning for foretakets virksomhet ifølge IKT-forskriften § 13. Hensiktsmessige planer og tiltak for tilgjengelighet og kontinuitet bør etableres med utgangspunkt i konsekvensanalyse for foretakets kritiske forretningsprosesser. Virksomhetens konsekvensanalyse[1] 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 foreløpig rapport på at konsekvensanalysen langt på vei framsto som en risikoanalyse og at forretningens eksplisitte krav til IKT-systemene ikke framkom. Finanstilsynet ba foretaket gjennomføre en konsekvensanalyse hvor forretningen stiller konkrete krav til hva som er akseptabel nedetid og akseptabelt datatap. Når dette er lagt inn i konsekvensanalysen, kan foretaket bruke kravene i beredskapstesting og kravstilling til leverandørene.

Av styrets svar framgår det at foretaket har oppdatert virksomhetens konsekvensanalyse med krav til akseptabel nedetid og datatap knyttet til de kritiske prosessene. Kravene i konsekvensanalysen og andre relevante dokumenter vil formidles og gjennomgås med de kritiske leverandørene for å sikre at leveranser og beredskapsplaner samsvarer. Av styrets svar framgår det videre at foretaket vil, som tidligere, involvere kritiske leverandører i årlige beredskapsøvelser.

Finanstilsynet viste videre i foreløpig rapport til at konsekvensanalysen er vesentlig for foretaket for å forstå hvilke prosesser, funksjoner og ressurser som er mest kritiske for driften og den virksomheten styret er ansvarlig for. Rutinen for gjennomføring av konsekvensanalysen og resultatet av analysen bør derfor framlegges for styret.

Finanstilsynet har fra styrets svar merket seg at revidert konsekvensanalyse og rutinen for gjennomføring av den, blir framlagt for styret den 12. juni 2025.

Finanstilsynet tar styrets svar til etterretning.

Rapportering

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-forskriften § 35. Der presiseres det blant annet at styret skal sikre seg tilgang til risikoinformasjon og fastsette omfang, format og frekvens på rapporteringen.

[1] Virksomhetens konsekvensanalyse = Business Impact Analysis (BIA)

Rapportering fra andrelinjen

Finanstilsynet kommenterte i foreløpig rapport at den kvartalsvise rapporteringen fra etterlevelsesfunksjonen til styret og ledelsen ikke omtalte IKT-området. Selv om andrelinjen vurderer etterlevelse for en del IKT-områder i sin årlige risikovurdering, mente Finanstilsynet at den kvartalsvise rapporteringen fra etterlevelsesfunksjonen til styret bør inneholde en vurdering av etterlevelse på IKT-området.

Styret kommenterer i sitt svar på at etterlevelsesfunksjonen årlig gjennomfører uavhengige kontroller på IKT-området og oppsummerer kontrollene i relevant kvartalsrapport til styret. Videre rapporterer etterlevelsesfunksjonen om IKT-hendelser av vesentlig betydning, om relevant tilsynspraksis og regelverksutvikling på IKT-området kvartalsvis til styret. Etterlevelsesfunksjonen vil fremover sikre at hver kvartalsrapport tydelig omtaler etterlevelsesrisiko på IKT-området.

Finanstilsynet pekte videre på at den kvartalsvis rapporteringen fra risikokontrollfunksjonen til styret og ledelsen manglet en sammenstilt vurdering av IKT-risikoen i foretaket.

Styret viser i sitt svar til at risikokontrollfunksjonen hvert år gjennomfører uavhengige kontroller på IKT-området og redegjør for avvik og anbefalinger i kvartalsrapporten til styret, herunder med nye indikatorer for overvåking av IKT-risiko.

Finanstilsynet har merket seg fra styrets svarbrev at risikokontrollfunksjonen framover vil sikre at risikorapporten tydeligere omtaler IKT-risiko.

Finanstilsynet pekte i foreløpig rapport på at med lov om digital operasjonell motstandsdyktighet (DORA-loven) som trer i kraft i Norge 1. juli 2025, stilles det konkrete krav på IKT-området som understreker behovet for økte ressurser i andrelinjen. Finanstilsynet stilte spørsmål til om andrelinjen har tilstrekkelig ressurser og kompetanse.

Av styrets svar framgår det at styret fortløpende vurderer ressurssituasjonen og nødvendig kompetanse i andrelinjen. Styret opplever at foretaket har kompetentente ressurser på disse områdene. Når det gjelder ressurssituasjonen, har Finanstilsynet merket seg at styret har iverksatt tiltak. Ved særskilte behov vurderer styret behovet for å leie inn eventuelt ytterligere kapasitet eller kompetanse, så vel som eventuell rekruttering.

Finanstilsynet tar styrets svar til etterretning.

Rapportering fra tredjelinjen

Finanstilsynet pekte i foreløpig rapport på at internrevisjonens årlige revisjoner med utgangspunkt i IKT-forskriften mangler omtale av om foretaket etterlever forskriftens krav til endringshåndtering. Finanstilsynet anbefalte at internrevisor utvider sin omtale av avviks- og endringshåndtering i kommende revisjoner.

Finanstilsynet har merket seg styrets kommentar der det framkommer at internrevisjonen minimum årlig gjennomfører en gjennomgang av etterlevelse av IKT-forskriften. I styregodkjent revisjonsplan for 2025 er budsjett og scope for den årlige IKT-revisjonen utvidet for blant annet å hensynta kommende krav i henhold til DORA. Revisjonen vil også dekke og omtale bankens endrings-håndtering.

Finanstilsynet tar styrets svar til etterretning.

3.2 Endrings- og avvikshåndtering

I henhold til IKT-forskriften § 9 skal foretaket sikre at prosedyrer for avviks- og endringshåndtering foreligger og følges. 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. Prosedyrene for avvikshåndtering skal omfatte alle avvik som oppstår i driften av IKT-systemene. Videre skal avviksbehandlingen identifisere årsaken til avvik, hindre gjentagelse og sikre forsvarlig og formell behandling av avviket. Avvikene skal dokumenteres og prosedyrene skal inneholde retningslinjer for eskalering.

Feil i endringshåndteringen er årsaken til mange alvorlige avvik. Test med dekkende testcase kan avdekke slike feil før endringen settes i produksjon. Finanstilsynet viste i foreløpig rapport til at foretakets rutiner for endringshåndtering ikke spesifiserer nærmere hvordan testing av endringer skal gjennomføres. Dette gjelder enten det er prosjektleveranser, nye versjoner av programvare fra leverandør eller andre system-/applikasjons-endringer.

Fra styrets svar framgår det at styret tar Finanstilsynets tilbakemelding til etterretning. Foretaket vil gjennomgå rutinene for endringshåndtering og operasjonalisere disse ytterligere i løpet av tredje kvartal 2025.

Finanstilsynet tar styrets svar til etterretning.

3.3 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. Videre skal det finnes retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene. Nærmere utdypinger finnes i EBAs retningslinjer for IKT og sikkerhet.[2]

Manglende rutine for kontroll av logger

Kontroll og analyse av logger er viktig for å sikre at tilganger benyttes korrekt og for å kunne identifisere uautorisert eller mistenkelig aktivitet. Finanstilsynet pekte i foreløpig rapport på at foretaket mangler en rutine der foretakets krav til logging og oppfølging av loggene framgår, særlig knyttet til brukere med tilgang til sensitive systemer og data. Kravene må også gjøres kjent for driftsleverandøren, og leverandøren må forplikte seg til å etterleve dem.

Styret bemerker i sitt svar at det foreligger noen rutiner innenfor området, men erkjenner at det er forbedringspotensiale. Styret tar derfor tilsynets tilbakemelding til etterretning og vil vurdere tiltak for å følge opp logging og oppfølging av logger for tilgang til sensitive systemer og data.

Finanstilsynet har merket seg styrets svar og forventer at foretaket iverksetter tiltak på området.

Manglende gjennomføring av uavhengige sikkerhetstester

Sikkerhetstester kan avdekke eksponering for tekniske sårbarheter og reduserer risikoen for at svakheter ikke blir oppdaget. Dette kan være sikkerhetstesting både mot applikasjoner, infrastruktur og nettverk. Bruk av tredjeparter til dette kan være en fordel for å sikre større grad av uavhengighet og bedre resultat av testingen.

Finanstilsynet viste i foreløpig rapport til at foretaket mangler retningslinjer for gjennomføring av sikkerhetstester som beskriver krav til hyppighet, omfang, metodikk og sikker gjennomføring

[2] EBA Guidelines on ICT and security risk management, EBA/GL/2019/04

inkludert bruk av eksterne aktører. Finanstilsynet viste videre til foretakets egen omtale av kravene til TLPT[3]-testing i DORA.

Styret kommenterer i sitt svar foretakets planer for penetrasjonstesting, men Finanstilsynet kan ikke se at styret har kommentert foretakets manglende retningslinjer for gjennomføring av sikkerhetstester.

Finanstilsynet forventer at foretaket etablerer retningslinjer for sikkehetstesting.

3.4 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 § 12 at foretaket har ansvar for at IKT-virksomheten oppfyller alle krav som stilles i forskriften og at dette gjelder også der hele eller deler av IKT-virksomheten er utkontraktert. Av bestemmelsene i § 13 framgår det at foretaket skal sikre at det har en samlet oppdatert dokumentasjon over organisasjon, utstyr, IKT-systemer og vesentlige forhold i IKT-virksomheten. Foretaket skal videre ha en samlet og oppdatert oversikt over alle avtaler om utkontraktering av virksomhet. Det følger av meldepliktforskriften § 1.

For foretak med stor leverandøravhengighet på IKT-området, er det viktig å ha egne rutiner for oppfølging av leverandørene som beskriver avtalt rapportering fra leverandøren (frekvens, innhold, med mer) og videre hvordan foretaket skal vurdere den mottatte informasjonen. Videre er det viktig for foretaket å kontrollere at leverandørene etterlever foretakets krav på IKT-området, eksempelvis foretakets krav til endringshåndtering og sikkerhet.

Finanstilsynet kommenterte i foreløpig rapport at foretakets rutine for utkontraktering mangler omtale av avtalt rapportering fra leverandørene og foretakets oppfølging av denne. Den viser heller ikke til hvordan foretaket følger opp at leverandørene etterlever foretakets krav, eksempelvis kravene i konsernrutinene for IT-utvikling og IT-drift.

Styret peker i sitt svar på at foretakets rutine for utkontraktering inkluderer en beskrivelse av krav til innhold i avtaler når det gjelder oppfølging, kontrolltiltak og rapportering fra leverandører. Foretaket vil ved neste revisjon av nevnte rutine, tydeliggjøre kravene til oppfølging og avtalt rapportering av leverandører ytterligere.

Finanstilsynet tar styrets svar til etterretning.

3.5 Beredskap

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 av at kriseløsningene virker som forutsatt. Resultatet av testen skal dokumenteres, jf. IKT-forskriftens § 11 tredje ledd.

Finanstilsynets vurdering i foreløpig rapport var at ved testing av beredskapsplaner, for foretakets egne og for utkontrakterte IKT-tjenester, må foretakets dokumenterte krav i virksomhetens konsekvensanalyse testes og trenes på, for på denne måten få bekreftet at forretningens behov er

[3] TLPT = Threat-Led Penetration Testing

ivaretatt. Finanstilsynet pekte på at testene foretaket har gjennomført ikke har vært satt opp med bakgrunn i konsekvensanalysen. Testene viste heller ikke til noen krav, med utgangspunkt i sikkerhetspolicy eller andre retningslinjer, som stilles ved test av kriseløsning hos leverandører eller underleverandører. Finanstilsynet understreket at ved øvelse og testing må realistiske scenarioer legges til grunn og kritiske og viktige leverandører må involveres. Finanstilsynet vurdering var at etterlevelsen av IKT-forskriftens § 11 ikke var tilstrekkelig ivaretatt.

Styret peker i sitt svar på at beredskapsøvelsen i 2024 for bankens ledelse var rettet mot kontinuitetsplanen for informasjonssikkerhet og krisekommunikasjonsplanen ved et cyberangrep-scenario, der kritiske leverandører for dette scenarioet var involvert i forarbeid, gjennomføring og etterarbeid. Styret erkjenner at beredskapsøvelser i enda større grad bør knyttes til de kritiske prosessene definert i virksomhetens konsekvensanalyse. Foretaket vil hensynta dette i neste øvelse og involvere relevante leverandører i et nytt scenario.

Finanstilsynet tar styrets svar til etterretning.

4 Videre oppfølging

Foretaket bes sende kopi av dette brevet til valgt revisor.

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

For Finanstilsynet

Olav Johannessen
seksjonsleder

Åshild Johnsen
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk.