FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

OSLO BØRS ASA
Postboks 460 Sentrum
0105 OSLO

VÅR REFERANSE	DERES REFERANSE		DATO
22/7660			26.01.2024

Tilsynsrapport

Finanstilsynet gjennomførte stedlig IKT-tilsyn i Oslo Børs ASA 27. oktober 2022. Formålet med tilsynet var å gjøre en vurdering av foretakets arbeid med kontinuitets- og kriseledelse og oppfølging av tilgangsrettigheter til foretakets IKT-systemer.

Til grunn for tilsynsrapporten ligger Finanstilsynets foreløpige rapport datert 25. mai 2023 og styrets kommentarer til rapporten i brev av 8. september 2023.

Finanstilsynet har følgende merknader etter det stedlige tilsynet:

Innledende kommentar

Oslo Børs har tillatelse fra Finanstilsynet til å drive som markedsoperatør. Som markedsoperatør har Oslo Børs også tillatelse til å drive flere typer handelsplasser. Verdipapirhandelloven setter en rekke krav til den virksomheten børsen har tillatelse til å drive. Kravene er i seg selv uavhengig av virksomhetens størrelse, selv om oppfyllelse av deler av virksomhetskravene kan avhenge av virksomhetens størrelse. Oslo Børs, som er en del av Euronext-konsernet, har utkontraktert en betydelig andel av børsens IKT-virksomhet til andre foretak i Euronext-konsernet. Finanstilsynet minner om at Oslo Børs er innehaver av tillatelsene til å drive handelsplasser i Norge og børsen har dermed ansvar for å ha kontroll med den utkontrakterte tjenesten, uavhengig av om tjenesten utføres konserninternt.

Organisering

Det framgår av verdipapirhandelloven § 11-8 første ledd punkt 1 og 2 at styret i Oslo Børs skal sørge for forsvarlig organisering av virksomheten. Forskrift om risikostyring og internkontroll stiller i § 3 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, iht. retningslinjer fastsatt av styret. Videre skal daglig leder sikre at risikostyring og internkontroll gjennomføres og overvåkes på en forsvarlig måte. Delegert kommisjonsforordning 2017/584 (RTS 7) artikkel 3 (1) bokstav d presiserer at organiseringen og styringsordningen i foretaket skal sikre adskillelse av oppgaver og ansvarsområder for å sikre effektivt tilsyn med etterlevelse av regelverket.

Finanstilsynet ba i foreløpig rapport styret vurdere om foretaket har tilstrekkelig IKT-kompetanse i andrelinjefunksjonen til å etterleve kravene som stilles til foretakets etterlevelsesfunksjon.

Styret skriver i sitt svar at det er børsens syn at organiseringen av andrelinjefunksjonen på Oslo Børs er tilstrekkelig organisert og oppfyller gjeldende lov- og forskriftskrav. Videre skriver Oslo

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00

post@finanstilsynet.no
www.finanstilsynet.no

Saksbehandler
Stig Ulstein
Dir. tlf. 22 93 99 66

Børs at det likevel er besluttet ytterligere tiltak for å styrke etterlevelsesfunksjonens oppfølging av Oslo Børs-spesifikke IKT-systemer, for slik å sikre enda bedre etterlevelse.

Finanstilsynet tar styrets svar til etterretning.

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 framgår det at Oslo Børs "minst en gang årlig, eller ved endringer som har betydning for IKT-sikkerheten, skal gjennomføre risikoanalyser for å påse at risiko styres innenfor akseptable grenser i forhold til foretakets virksomhet. Resultatet av risikoanalyser skal dokumenteres". I forskrift om risikostyring og internkontroll § 6 første ledd framgår det videre krav om at foretaket "løpende skal vurdere hvilke vesentlige risikoer som er knyttet til virksomheten".

I Finanstilsynets foreløpige rapport ble det pekt på viktigheten av at nåværende risiko- og sårbarhetsanalyse gjennomgås og tilpasses virksomheten i Oslo Børs, og at analysen skal definere omfang, grenser, ansvar og kompetansekrav for IKT-virksomheten til foretaket. Videre ble det pekt på at det bør utarbeides rutiner som sikrer at hele IKT-virksomheten i børsen blir gjennomgått i denne forbindelse.

Styret skriver i sitt svar at det er Oslo Børs' syn at foretaket har et adekvat rammeverk for risikostyring og fastsettelse av risikotoleranse for IKT-risiko. Styret skriver at rammeverket er lokalt tilpasset Oslo Børs, slik at det hensyntar den virksomhet børsen driver. Videre har Oslo Børs fastsatt egne risikoer for IKT som løpende rapporteres til ledelsen og styret, som del av Oslo Børs Risk Profile. Styret er av den oppfatning at Oslo Børs har dokumentasjon og rutiner som innfrir kravene i IKT-forskriften § 3 og forskrift om risikostyring og internkontroll § 6.

Finanstilsynet tar styrets svar til etterretning.

Rapportering av IKT-risiko

Etter verdipapirhandelloven § 11-8 første ledd skal styret føre tilsyn med foretakets virksomhet. Ifølge bestemmelsens tredje ledd skal styremedlemmene ha tilstrekkelig tilgang til opplysninger og dokumenter som de trenger for å føre tilsyn med beslutninger som treffes av markedsoperatørens daglige ledelse. Styrets rolle knyttet til foretakets system for risikostyring og internkontroll framgår av forskrift om risikostyring og internkontroll § 3. Av forskriftens § 8 følger det at styret skal forelegges en vurdering av risikosituasjonen utarbeidet av daglig leder.

Finanstilsynet ble under tilsynet informert om at risiko for IKT-området ikke inngikk i foretakets faste risikorapporter til styret. Finanstilsynet er av den oppfatning at styret, for å kunne føre tilsyn med foretakets virksomhet, også må sikre seg løpende og oppdatert informasjon om risikoen knyttet til foretakets IKT-virksomhet, en risiko Finanstilsynet anser å være en av foretakets større risikoer.

Finanstilsynet pekte i foreløpig rapport på at foretaket må sikre å innhente relevant informasjon om risikoen med foretakets IKT-virksomhet, slik at styret kan ta de nødvendige beslutninger om foretakets risikoprofil og ha kontroll med foretakets IKT-risiko.

I styrets svar pekes det på hvordan foretaket rapporterer risk og etterlevelse kvartalsvis, inklusive IKT-risikoer, for Oslo Børs ledelse og styre. Styret skriver videre at rapporteringen skjer i tråd med det som er blitt definert i Oslo Børs Risk Appetite Framework og Oslo Børs Risk Management Policy, og inkluderer de tre mest sentrale IT-relaterte risikoene for Oslo Børs. Ettersom styret

kvartalsvis får en oppdatering rundt risikosituasjonen på Oslo Børs, er Oslo Børs av den oppfatning at styret alt er klar over og har et bevisst forhold til de sentrale risikoene tilknyttet IT i foretaket.

Styrets vurdering er at styret får tilstrekkelig informasjon om sentrale risikoer forbundet med Oslo Børs' IKT-virksomhet.

Finanstilsynet tar styrets svar til etterretning.

Nøkkelpersonsrisiko

I RTS 7 artikkel 5 (1) stilles det krav til foretaket om å sikre at ansatte har tilstrekkelig ressurser og kompetanse.

Finanstilsynet ble under tilsynet gjort kjent med at det for tre av rollene i foretakets IKT-organisasjon ikke er sikret beredskap dersom en eller flere av de som utfører rollene ikke er tilgjengelig for foretaket. Rollene det pekes på er leder for IKT, ansvarlig for IKT-sikkerhet og ansvarlig for endringsledelse.

Finanstilsynet pekte i foreløpig rapport på at tilsynet vurderte at foretaket må sikre at tap av nøkkelpersoner ikke utgjør en risiko for foretakets IKT-virksomhet. Foretaket bør sørge for at viktig kunnskap er dokumentert og erfaring overført til andre medarbeidere.

Styret skrev i sitt svar at Oslo Børs er del av et større konsern med flere ansatte med dyp kompetanse innen IKT. Ved tap av nøkkelpersonell på IT-avdelingen lokalt, vil Oslo Børs derfor kunne dra på ressurser fra øvrige lokasjoner i gruppen, for å sikre forsvarlig IT-drift.

Finanstilsynet presiserer i denne sammenheng at Oslo Børs har utkontraktert størstedelen av børsens IKT-virksomhet til foretak internt i Euronext-konsernet. Oslo Børs har dermed en særskilt oppgave med å ha kontroll med IKT-tjenestene som leveres til børsen. Det vil kunne oppstå rollekonflikter dersom kontroll av IKT-tjenestene dekkes opp av ressurser i Euronext-gruppen som også er leverandør av IKT-tjenestene. Styret bør sørge for at tilstrekkelig personell lokalt har kompetanse til å kontrollere de utkontrakterte IKT-tjenestene og også sørge for å unngå rollekonflikter som kan oppstå dersom nøkkelpersonell erstattes av ressurser internt i Euronext-gruppen. Styret bør også vurdere om konsernintern overføring av oppgaver knyttet til nøkkelpersoner kan anses å være utkontraktering av virksomhet, og som dermed skal meldes til Finanstilsynet etter Finanstilsynsloven § 4 c, jf. RTS 7 artikkel 6 punkt 5 og 6.

Finanstilsynet vil understreke styrets ansvar til å sikre at tilstrekkelig personell lokalt har kompetanse til å kontrollere foretakets utkontrakterte IKT-tjenester.

Forretningsmessig konsekvensanalyse

IKT-forskriften § 11 stiller krav til at foretak skal ha en dokumentert kriseplan, slik at forretningsmessig kontinuitet kan opprettholdes. Kriseplanen skal iverksettes dersom IKT-driften ikke kan opprettholdes som følge av en krise. Minimumskravene til en slik kriseplan framgår av IKT-forskriften § 11 annet ledd. Av RTS 7 artikkel 15 (2) framgår det at foretakets kriseplan skal sikre at handelsplassen kan gjenoppta handel innen to timer, samt at datatap ved en hendelse skal være minimalt. RTS 7 artikkel 16 (4) stiller krav til at handelsplasser skal ha gjennomført en konsekvensanalyse som identifiserer risiko og konsekvensene ved bortfall. En slik analyse skal gjennomføres og gjennomgås periodisk. Kravene gjelder også ved utkontraktering av IKT-virksomhet jf. kravene i IKT-forskriften § 12.

Finanstilsynet pekte i foreløpig rapport på at Oslo Børs har et selvstendig ansvar for å sikre at forretningsmessige konsekvensanalyser (BIA) gir tilstrekkelig grunnlag for å utarbeide og etablere

planer for beredskap og kontinuitet ut ifra et kritikalitetsperspektiv. Dette gjelder også der virksomheten er utkontraktert.

Styret skrev i sitt svar at foretakets BIA definerer hvilke aktiviteter/prosesser, med tilhørende applikasjoner, som er kritiske og identifiserer minimumsressursene som kreves for å opprettholde disse kritiske aktivitetene. Videre at det er ytterligere BIAer i Euronext-gruppen som inneholder vurderinger av kritikaliteten av andre komponenter (applikasjoner) med tilknytning til handelssystemet.

Finanstilsynet tar styrets svar til etterretning.

Tilgangsstyring i Norge

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", og det skal være etablert "retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene". RTS 7 artikkel 23 (2) bokstav a-d, viser videre til at foretaket skal etablere tiltak for fysisk og digital tilgangskontroll for å identifisere, forhindre eller minimere risiko for uautorisert tilgang til system og/eller data.

På bakgrunn av informasjon gitt av foretaket på tilsynsmøtet, og i ettersendt dokumentasjon, var det Finanstilsynets vurdering i foreløpig rapport at Euronext-konsernets retningslinjer for tilgangsstyring ikke følges for lokale systemer. Det ble videre påpekt at det var brukere med administrasjonsrettigheter lokalt. Finanstilsynets vurdering var at foretaket bør etablere tiltak for å redusere risikoen for at egne ansatte, konsulenter og personell hos leverandører har tilganger som ikke samsvarer med de til enhver tid tjenstlige behov. Det bør også etableres kontrollrutiner for å verifisere at brukertilganger er slettet i systemer, der ansatte for eksempel har sluttet eller skiftet stilling.

I styrets svar vises det til det pågående arbeid i Oslo Børs med å implementere gruppens standard for tilgangsstyring (IAM, Identity Access Management), som vil komme på plass når migreringsprosjektet er ferdig i løpet av 2023. Videre i svaret ble det pekt på arbeidet som ytterligere skal forbedre fysisk og digital tilgangskontroll for gjenværende lokale systemer. Dette vil iverksettes i løpet av 2023.

Finanstilsynet tar styrets svar til etterretning.

Oppfølging av utkontrakterte tjenester

Foretaket plikter å ha retningslinjer som sikrer at utkontraktert virksomhet oppfyller kravene i IKT-forskriften § 12, jf. IKT-forskriften § 2 annet ledd. Foretaket har ansvaret for at IKT-virksomheten oppfyller kravene i IKT-forskriften. Dette gjelder også der hele eller deler av IKT-virksomheten er utkontraktert, jf. IKT-forskriften § 12 første ledd. Videre framgår det ytterligere krav som foretaket må etterleve i RTS 7 artikkel 6 (3) bokstav a-n.

Foretaket har utkontraktert flere vesentlige deler av sin virksomhet til selskaper i konsernet de inngår i. Dette inkluderer også vesentlig deler av IKT-virksomheten.

I foreløpig rapport pekte Finanstilsynet på at det var uklart for tilsynet hvordan oppfølging av konsernintern utkontraktert IKT-virksomhet rapporteres til styre og ledelse i foretaket. Videre om det var etablert møteplasser med leverandørene for oppfølging av de utkontrakterte IKT-tjenestene og eventuelt hvordan det sikres oppfølging på ulike nivå. Finanstilsynet understrekte styrets ansvar

for å sikre at det gjennomføres tilstrekkelig oppfølging og tilsyn med konserninterne leverandører til foretaket.

I styrets svar beskrives det hvordan Oslo Børs har organisert oppfølgningen av tjenester som mottas fra andre konsernselskaper, dette dels gjennom det etablerte systemet for oppfølgning som konsernet benytter og dels gjennom etablering av ytterligere ordninger på Oslo Børs. Videre skriver styret at for Oslo Børs er det viktig at organiseringen av oppfølgingen er tilstrekkelig fleksibel slik at den raskt kan tilpasses endringer i spekteret av tjenester som tilbys, endringer i de enkelte tjenestene og endringer i organisasjonen til Oslo Børs.

Styret skriver videre at det er etablert et omfattende regime for oppfølging av utkontrakterte tjenester, inkludert konserninterne utkontrakteringer. I svaret fra styret beskrives de ulike roller, ansvarsområder og møteplasser. Det er styrets vurdering at oppfølging av de utkontrakterte IKT-tjenestene er godt i varetatt.

Finanstilsynet tar styrets svar til etterretning.

Kopi av rapporten bes sendt valgt revisor.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Stig Ulstein
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.