FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

SECTOR FUND SERVICES AS
Postboks 462 Sentrum
0105 OSLO

VÅR REFERANSE	DERES REFERANSE		DATO
23/2616			12.02.2024

Tilsynsrapport

Finanstilsynet gjennomførte stedlig IKT-tilsyn i Sector Fund Services AS (SFS) 25. april 2023.

SFS har konsesjon til å forvalte alternative investeringsfond og verdipapirfond.

Hensikten med tilsynet var å gjøre en vurdering av hvordan foretaket administrerer, utvikler, drifter, vedlikeholder og sikrer IKT-systemer og -tjenester. For dette området ble tilsynet 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 at regulatoriske krav på dette området overholdes.

Til grunn for merknadene ligger Finanstilsynets foreløpige rapport datert 30. oktober 2023 og styrets kommentarer til denne i brev av 29. november 2023.

Finanstilsynet har følgende merknader etter det stedlige tilsynet:

1. Organisering

Krav til forvalters risikostyringsfunksjon følger av AIF-loven § 3-7 og verdipapirfondloven § 2-12 med forskrifter. Det stilles videre krav til risikostyring i forskrift om risikostyring og internkontroll. 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, 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 etterlevelses- og risikostyringsfunksjonen er andrelinje-funksjonene som vurderer og følger opp foretakets IKT-virksomhet på et overordnet nivå, men at det ikke ble stilt krav til eller gjort vurderinger av teknisk/IKT-faglig karakter. Videre pekte Finanstilsynet på at styret må sikre at foretaket har tilstrekkelig IKT-kompetanse i andrelinje-funksjonene til å vurdere IKT-risikoen i risikostyringen og til å kontrollere etterlevelsen på dette området.

Styret skriver i sitt svar at de anser organiseringen av første-, andre- og tredjelinje som tilstrekkelig gitt foretakets størrelse og virksomhetsområde. Det er styrets oppfatning at etterlevelses- og risikokontrollfunksjonene har tilstrekkelig ressurser og IKT-kompetanse til å kunne kontrollere og

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

stille relevante krav til førstelinjen. Videre peker styret i sitt svar på at det fra foretakets revisor ikke har kommet fram kommentarer på mangelfull organisering eller oppfølging av IKT-risiko, eller om foretaket har tilstrekkelig ressurser og IKT-kompetanse.

Finanstilsynet tar styrets svar til etterretning, men vil likevel peke på viktigheten av at foretakets etterlevelse og risikofunksjon følger opp foretakets IKT-virksomhet, og har tilstrekkelig kompetanse til dette.

2. Overordnet styring av IKT-risiko

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 annet 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. Forskrift om risikostyring og internkontroll § 6, første ledd stiller krav om at foretaket "løpende skal vurdere hvilke vesentlige risikoer som er knyttet til virksomheten".

Det var Finanstilsynets foreløpige vurdering at foretaket ikke adresserte IKT-risiko i kvartalsvis risikorapportering til styret. Finanstilsynet pekte på at det forventes at IKT-risiko løpende identifiseres, styres, overvåkes og kontrolleres av foretaket. Videre forventer Finanstilsynet at vurderingen av IKT-risikoen opp mot styrevedtatte måltall, rammer og/eller krav inkluderes i foretakets faste rapporter som går til styret.

I styrets svar pekes det på at foretaket har rammeverk og retningslinjer som vurderes som hensiktsmessige, tydelige og avklarende. Videre er det styrets vurdering at foretaket opererer i tråd med fastsatte kriterier for akseptabel risiko forbundet med IKT-systemene, samt at IKT-risiko løpende identifiseres, styres, overvåkes og kontrolleres av foretaket.

I styrets svar pekes det også på at det er styrets vurdering at den faste rapporteringen fra de ulike funksjonene i foretaket i tilstrekkelig grad dekker IKT-risiko, herunder måltall, rammer, krav og IKT-sikkerhet.

Finanstilsynet tar styrets svar til etterretning, men vil likevel peke på viktigheten av foretakets håndtering av IKT-risiko og at rapportering av IKT-risiko inngår som en del av den faste rapporteringen til styret.
.

3. Nøkkelpersonrisiko

Forvalteren skal etter AIF-loven § 3-1 innrette sin virksomhet slik at foretaket til enhver tid har tilstrekkelige og egnede ressurser for forsvarlig forvaltning. Tilsvarende krav til organisering av virksomheten følger av verdipapirfondloven § 2-11.

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

I styrets svar er det som vedlegg oversendt detaljert skriftlig dokumentasjon på IKT-systemer, IKT-infrastruktur og IKT-sikkerhetssystemer. Styret skriver videre at deres vurdering er at i en liten organisasjon vil alltid nøkkelpersonrisiko være et tema, men det vurderes at nøkkelpersonrisiko i tilstrekkelig grad er håndtert både gjennom foretakets organisering. Gjennom etablerte grupper, skriftlig dokumentasjon og informasjonsdeling sikres også erfaringsoverføring. Styret skriver i sitt svar videre at nøkkelpersonrisikoen er tilpasset virksomhetens omfang og kompleksitet.

Finanstilsynet tar styrets svar til etterretning.

4. Virksomhetens 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 virksomhetsprosesser. Virksomhetens konsekvensanalyse skal bidra til å sikre at foretakets beredskapsplaner utarbeides med basis i det som er kritisk for virksomheten. Planene skal basere seg på foretakets prioriteringer for gjenoppretting av virksomhetskritiske 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 foretas regelmessig opplæring, øvelse og testing, jf. IKT-forskriften § 11.

Finanstilsynet pekte i foreløpig rapport på at foretaket ikke har gjennomført en tilstrekkelig forretningsmessig konsekvensanalyse. Uten virksomhetens konsekvensanalyse vil foretakets kriseplan, jf. IKT-forskriften § 11, være utarbeidet uten prioriteringer for gjenoppretting av virksomhetskritiske tjenester og prosesser. Finanstilsynet forventer at foretaket utarbeider virksomhetens konsekvensanalyser ledet av forretningssiden, der resultatet av konsekvensanalysen blant annet vil gi oversikt over foretakets systemportefølje der kritikaliteten systemene har for foretakets virksomhet er angitt. Videre pekte Finanstilsynet på at det bør framgå av analysen hva som er akseptabel nedetid for det enkelte IKT-system. Resultatet av analysen bør også formidles til relevante leverandører.

I styrets svar pekes det på at kravene til funksjon og ytelse for foretakets IKT-systemer er fundamentert i virksomheten og ikke initiert av IKT-tjenesteleverandøren, og at dette gjenspeiles i foretakets forretningsmessige konsekvensanalyse som nå er utarbeidet. Videre skriver styret at det i stor grad er forretningssiden i foretaket og i Sector Asset Management-gruppen som har definert systembehov og krav til oppetid, hvor akseptabel nedetid vurderes for hvert enkelt system.

Finanstilsynet tar styrets svar til etterretning.

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, med dokumentasjon av testresultater, som viser at kriseløsningen virker som forutsatt.

Finanstilsynet pekte i foreløpig rapport på at foretaket kan ha utfordringer med å håndtere for eksempel et cyberangrep, hvor angriper har etablert digitalt fotfeste på innsiden av foretakets nettverk, som følge av omfanget av beredskapstesting av viktige og kritiske system. Finanstilsynet pekte videre på at foretaket selv er ansvarlig for at opplæring, øvelse og testing av foretakets kriseløsning gjennomføres årlig.

Styret skriver i sitt svar at de anser beredskapen til å være tilstrekkelig ivaretatt gjennom kontinuitets- og katastrofeplanen, samt den regelmessige testingen av IKT-løsningene, inkludert penetrasjonstesting. Videre skriver styret at opplæringen og testingen av foretakets ansatte utføres på tilfredsstillende måte, blant annet gjennom obligatoriske opplæringssesjoner, Sector-skolen og phishing tester.

Finanstilsynet tar styrets svar til etterretning, men vil samtidig peke på at det i testingen av beredskapen i IKT-systemene er viktig at gjenoppretting av data og system også omfattes.

6. Tilgangsstyring

Etter IKT-forskriften § 5 om sikkerhet skal foretaket 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". Prosedyrene skal inneholde "retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IT-systemene".

Finanstilsynet pekte i foreløpig rapport på at etablert form for tilgangsstyring ikke var tilstrekkelig, da det for IKT-tjenesteleverandør var mulighet for å misbruke tilgangen til ikke-tjenstlige oppslag som vanskelig lot seg avdekke. Finanstilsynets pekte videre på at foretaket må sikre at IKT-leverandør etablerer løsninger for tilgangsstyring og kontrollrutiner som i størst mulig grad sørger for at tilganger tildeles og kontrolleres for det enkelte oppdrag.

Styret skriver i sitt svar at foretaket har etablert rutiner og tekniske løsninger som vil styrke overvåkningen og sporbarheten ytterligere, samt sikre foretaket mot IKT-leverandørens mulighet til å manipulere tilgangssystemet. Videre er det innført begrensninger for hvem som har mulighet til å gjøre endringer knyttet til tilgangsstyring. Styret skriver videre at det anses at tilgangskontroll er tilstrekkelig ivaretatt gjennom skriftlig dokumentasjon, rutiner og testing. Videre har foretaket styrket sin kontroll ved å gi tidsbegrensede tilganger knyttet til IKT-leverandør, samt implementering av ekstrasystem for overvåkning og sporbarhet.

Finanstilsynet tar styrets svar til etterretning.

7. Oppfølging av utkontrakterte tjenester

Adgangen til å utkontraktere virksomhet fremgår av henholdsvis AIF-loven § 3-5 og verdipapirfondloven § 2-9. For utkontraktering av IKT-virksomhet gjelder IKT-forskriften §§ 2 og 12.

I henhold til IKT-forskriften § 2 annet ledd 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 § 2 fjerde ledd 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".

Foretaket har ansvar for at alle krav som stilles i IKT-forskriften oppfylles, også der hele eller deler av virksomheten er utkontraktert, jf. IKT-forskriften § 12. Det framgår av § 12 tredje ledd at foretaket må sikre at organisasjonen, i egen regi eller gjennom formalisert samarbeid med andre foretak enn IKT-leverandøren, har tilstrekkelig kompetanse til å forvalte utkontrakteringsavtalene.

Finanstilsynet pekte i foreløpig rapport på viktigheten av at foretaket gjennom sine rutiner for oppfølging av leverandørene gjennomfører kontroll av utkontraktert virksomhet, og at IKT-tjenesteleverandørene leverer i henhold til de krav avtalen stiller. Finanstilsynet pekte videre på at foretaket må ha tilstrekkelig kunnskap og ressurser til å følge opp alle IKT-tjenester som inngår i avtalen med IKT-tjenesteleverandører.

Finanstilsynet pekte også på at foretaket burde vurdere noen av avtalene om kjøp av IKT-tjenester for å se om de faller inn under IKT-forskriftens § 12 Utkontraktering og at de aktuelle avtalene eventuelt endres for å sikre at avtalene håndteres etter de krav som stilles til utkontraktering av IKT-virksomhet, og er i henhold til IKT-forskriften § 12.

Styret skriver i sitt svar at det er etablert rutiner for årlig innhenting og kontroll av oppdaterte dokumenter knyttet til IKT-leverandørens internkontroll og interne rutiner i forbindelse med foretakets internkontrollgjennomgang. Videre skriver styret at deres vurdering er at oppfølging av utkontraktert virksomhet i tilstrekkelig grad er ivaretatt gjennom instruksverket, den formelle rapporteringen, avtalehåndtering og gjennom rutiner. Det er styrets oppfatning at den løpende dialogen med foretakets IKT-leverandør er godt ivaretatt, både gjennom regelmessig tilstedeværelse på foretakets kontor, samt i møter i IT Security-gruppen og IKT-gruppen.

Styret viser til at det er gjennomført vurderinger av de aktuelle avtalene opp mot IKT-forskriften, og at avtalene vil bli håndtert etter de krav som stilles til utkontraktering av IKT-virksomhet, og i henhold til IKT-forskriften § 12.

Finanstilsynet tar styrets svar til etterretning.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Stig Ulstein
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.