FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

STREX PAYMENT AS
Postboks 1044
0277 OSLO

Vår referanse
23/9234
Deres referanse

05.12.2024

Tilsynsrapport

Finanstilsynet gjennomførte stedlig IKT-tilsyn i Strex Payment AS (foretaket) 23. og 24. september 2023. Tilsynet hadde som formål å vurdere det samlede foretakets styring av IKT-virksomheten med særlig vekt på internkontroll og styring av vesentlige risikoer, arbeidet med hvitvasking og terrorfinansiering og avstemming av klientmidler. Kun merknader knyttet til IKT-virksomheten går fram av rapporten, mens merknader knyttet til arbeidet med hvitvasking og terrorfinansiering og avstemming av klientmidler vil følge i egen tilsynsrapport.

Til grunn for tilsynsrapporten ligger Finanstilsynets foreløpige rapport datert 27. september 2024 og styrets kommentarer til rapporten i brev av 12. november 2024.

Finanstilsynet har følgende merknader som gjelder IKT-virksomheten i foretaket etter det stedlige tilsynet:

Forhold knyttet til organisering

Styret skal påse at foretaket har en klar organisasjonsstruktur. Det følger av forskrift om risikostyring og internkontroll (risikostyringsforskriften) § 3 punkt 2.

I et lite foretak kan kritisk kompetanse sitter hos én person. Da er det vanskelig å gjennomføre god arbeidsdeling. I denne situasjonen er det særs viktig å analysere sårbarheter, etablere arbeidsdeling der det er mulig, og innføre kompenserende tiltak der dette ikke er mulig. En analyse vil kunne avdekke behov for å dublere kompetanse tilstrekkelig til at en uavhengig kontroll er effektiv.

Finanstilsynet pekte i foreløpig rapport på at foretaket ikke i tilstrekkelig grad har dokumentert at en analyse, for å avdekke behov for å dublere kompetanse tilstrekkelig slik at den uavhengige kontrollen er effektiv, har funnet sted.

Styret erkjenner i sitt svar at foretaket ikke i tilstrekkelig grad har dokumentert at en slik analyse og kartlegging har funnet sted. Styret skriver videre i sitt svarbrev at foretaket vil revidere og ytterligere presisere/utdype selskapets dokumentasjon og rutine for periodisk analysering av sårbarheter, slik at dette tydeligere etablerer arbeidsdeling der det er praktisk mulig og beskriver kompenserende tiltak der dette ikke er mulig.

Finanstilsynet tar styrets svar til orientering og legger til grunn at foretaket reviderer og ytterligere presiserer/utdyper foretakets dokumentasjon for området.

Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

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

Saksbehandler
Gisle Solemsjø Haugseth
Dir. tlf. 22 93 97 33

Daglig leder skal sørge for å etablere en forsvarlig risikostyring og internkontroll på basis av en vurdering av aktuelle risikoer etter retningslinjer fastsatt av styret. Det følger av risikostyringsforskriften § 4.

Finanstilsynet påpekte i foreløpig rapport at det ikke framgår av mottatt dokumentasjon, informasjon om hvordan foretakets forsvarslinjer er organisert, og hvordan nødvendig uavhengighet mellom forsvarslinjene er etablert. Foretakets organisering gir etter Finanstilsynets vurdering ikke tilstrekkelig uavhengighet i risikostyringen og internkontrollen av IKT-virksomheten.

Styret skriver i sitt svarbrev at styret ikke er enig i Finanstilsynets foreløpige vurdering. Styret opplyser imidlertid at styret vil sørge for å tydeliggjøre ansvarslinjer og organisering i framtidig dokumentasjon i lys av den reviderte/oppdaterte analysen og kartlegging nevnt over som vil bli foretatt i selskapet.

Finanstilsynet bemerker at så lenge IT-organisasjonen rapporterer direkte til Chief Operating Officer (COO), og COO ivaretar kontrolloppgavene som andrelinje kontrollfunksjon for etterlevelse, vil denne organiseringen vanskeliggjøre en forsvarlig gjennomføring av foretakets risikostyring og internkontroll. Finanstilsynet ber foretaket sørge for en forsvarlig risikostyring og internkontroll i tråd med kravene i § 4 i risikostyringsforskriften.

Forhold knyttet til kriseberedskap

Det framgår av IKT-forskriften § 11 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 kriseløsningen virker som forutsatt, og hvor resultatet av testen skal dokumenteres.

I foreløpig rapport pekte Finanstilsynet på at tester blir gjennomført både internt i foretaket og hos leverandører, men foretaket viste ikke til noen krav eller scenarioer, som f.eks. et omfattende løsepengevirus på sentral IKT-infrastruktur, som stilles til testing av kriseløsning hos leverandører eller underleverandører.

Styret skriver i sitt svarbrev at styret noterer seg tilsynets tilbakemelding om tydeligere krav til leverandører og underleverandører om krav til testing av kriseløsninger, og vil sørge for forbedringer på dette punkt.

Finanstilsynet tar styrets svar til orientering.

Forhold knyttet til 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.

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 organisasjonen, i egen regi eller gjennom formalisert samarbeid med andre foretak enn IKT-leverandøren, har tilstrekkelig kompetanse til å forvalte utkontrakteringsavtalene.

Foretaket har utkontraktert store deler av IKT-virksomheten. Finanstilsynets vurdering i foreløpig rapport var at foretakets hovedleverandør er den leverandøren som får størst oppmerksomhet når det

gjelder oppfølging av IKT-tjenesteleveranser. Finanstilsynet forventer imidlertid at foretaket har rutiner, tilstrekkelig kunnskap og ressurser for oppfølging av alle sine leverandører med utgangspunkt i de krav foretaket har i sine styringsdokumenter og risikovurderinger.

Styret opplyser i sitt svarbrev at selskapet følger opp og styrebehandler alle sine leverandøravtaler hvor det blir vurdert at en utkontraktering finner sted. Det opplyses videre at styret tar Finanstilsynets forventning til etterretning, og bekrefter at selskapet har tilstrekkelig kunnskap og ressurser for slik oppfølging og styring som kreves overfor eksterne leverandører.

Finanstilsynet tar styrets svar til orientering.

Forhold knyttet til tilgangsstyring

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.

Finanstilsynet ble under tilsynet informert om at dersom en ansatt hos IKT-tjenesteleverandør innehar en rolle hvor det er nødvendig å ha tilganger til IKT-driftsmiljø til foretaket, anser leverandøren dette som et tjenstlig behov for å kunne utføre sitt arbeid. Ved et slikt definert tjenstlig behov vil den ansatte bli satt opp med permanente tilganger til foretakets IKT-driftsmiljø uten tidsbegrensning eller andre typer begrensninger for når tilgangene kan benyttes.

Finanstilsynets vurdering i foreløpig rapport var at denne form for tilgangsstyring ikke er forsvarlig, da det gir muligheter for å misbruke tilgangen til ikke-tjenstlige oppslag som vanskelig lar seg avdekke. Finanstilsynet mener at foretaket må sikre at IKT-tjenesteleverandør etablerer løsninger for tilgangsstyring og kontrollrutiner som i størst mulig grad sørger for at tilganger tildeles og kontrolleres for det enkelte oppdrag.

Styret tar Finanstilsynets vurdering til etterretning, og bekrefter at foretaket vil revidere sine rutiner og prosedyrer for tilgangskontroll gjennom hyppigere gjennomgang/vurdering av nødvendige tilganger.

Finanstilsynet tar styrets svar til orientering.

Kopi av dette brevet bes sendt til valgt revisor.

For Finanstilsynet

Olav Johannessen
seksjonsleder

Gisle Solemsjø Haugseth
seniorrådgiver

Dokumentet er godkjent elektronisk.