FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

WEBOPPGJØR AS
Postboks 2454 Drotningsvik
5834 BERGEN

VÅR REFERANSE	DERES REFERANSE		DATO
22/10738			19.06.2023

Tilsynsrapport

Finanstilsynet gjennomførte stedlig IKT-tilsyn i Weboppgjør AS (Foretaket) 9. november 2022. Tilsynet hadde som formål å gjøre en vurdering av Foretakets styring og kontroll med IKT-virksomheten med særskilt vekt på løsninger som støtter oppgjørsfunksjonen.

Finanstilsynet har følgende merknader etter det stedlige tilsynet.

Forhold knyttet til styrende dokumenter

IKT-forskriften § 2 første ledd stiller krav til at foretaket skal fastsette overordnede mål, strategier, og sikkerhetskrav for IKT-virksomheten. Det skal foreligge en beskrivelse av den enkelte prosess og hvordan ansvaret for administrasjon, anskaffelse, utvikling, drift, systemvedlikehold, sikring av informasjon og avvikling utføres på en betryggende måte.

Foretaket opplyser at de er i sluttfasen av etablering/revidering av styrende dokumenter, og at disse skal gjøres tilgjengelig på en hensiktsmessig måte.

Finanstilsynet pekte i foreløpig rapport på viktigheten av at Foretaket sikrer at kravene i det finansregulatoriske regelverket til enhver tid ivaretas og styrets ansvar for å sikre at styrende dokumenter, herunder retningslinjer, rutiner, instrukser o.l., sikrer Foretakets etterlevelse av regelverket.

Det framgår av styrets svar til foreløpig rapport at foretaket vil imøtekomme Finanstilsynets kommentarer.

Finanstilsynet tar styrets svar til etterretning.

Forhold knyttet til nøkkelpersonsrisiko

Det fremgår av IKT-forskriften § 2 tredje ledd at foretaket skal oppnevne ansvarlige for de ulike delene av IKT-virksomheten. Det er videre presisert at med ansvarlig menes en funksjon eller stilling.

Finanstilsynet påpekte i foreløpig rapport at Foretaket ikke har en funksjon eller stilling som har ansvarsområde IKT-risiko. Finanstilsynet oppfattet at ansvaret var delt mellom ett fåtall personer i Foretaket, som i tillegg har andre ansvarsområder.

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00

post@finanstilsynet.no
www.finanstilsynet.no

Saksbehandler
Gisle Haugseth
Dir. tlf. 22 93 97 33

Finanstilsynet stilte i foreløpig rapport spørsmål om Foretakets organisering av IKT-ansvaret på ett fåtall personer, som også har andre ansvarsområder, kan medføre at IKT-virksomheten ikke vies tilstrekkelig oppmerksomhet. Videre var det Finanstilsynets syn at Foretaket bør gjennomføre en vurdering av nøkkelpersonsrisiko mht. ivaretakelse og oppfølging av IKT-virksomheten til Foretaket.

Styret har i sitt svar til foreløpig rapport sagt seg enig i Finanstilsynets observasjoner, og har i etterkant av det stedlige tilsynet gjennomført en risikovurdering av nøkkelpersonsrisiko knyttet til ivaretakelse og oppfølging av IKT-virksomheten i foretaket.

Finanstilsynet tar styrets svar til etterretning.

Forhold knyttet til risikostyring

Det fremgår av IKT-forskriften § 3 første ledd at foretaket skal fastsette kriterier for akseptabel risiko. Videre skal foretaket ha en dokumentert prosess for gjennomføring av risikoanalyser for IKT-virksomheten, jf. annet ledd. I annet ledd er det videre presisert at prosessen skal definere klare ansvarsforhold og omfatte oppfølging av tiltak som skal iverksettes på bakgrunn av resultatene i risikoanalysen.

Risikoanalyser skal gjennomføres minst en gang i året, eller ved endringer som har betydning for IKT-sikkerheten, jf. IKT-forskriften § 3 tredje ledd. Analysene skal gjennomføres for å påse at risiko styres innenfor akseptable grenser i forhold til foretakets virksomhet. Analysene skal dokumenteres.

Foretaket har gjennomført en risikoanalyse av operasjonell og IKT-risiko forbundet med sin virksomhet. Under tilsynsmøtet stilte Finanstilsynet spørsmål ved metodikken Foretaket anvendte ved gjennomføring av risikoanalysen.

Finanstilsynet påpekte i foreløpig rapport viktigheten av at Foretakets rammeverk for risiko brukes skjematisk i gjennomføring av risikovurderinger, at terskelverdier for de ulike risikoområdene er tydelig definert og at ansvarlige for tiltak blir pekt ut.

I sitt svar til foreløpig rapport skriver styret at foretaket har påbegynt et arbeid med å revidere "Styrets risikotoleranse" som styrende dokument. Risikovurderingene er oppdatert med ansvarlige for gjennomføring og implementering av tiltak, samt med status for gjennomføring av tiltak.

Finanstilsynet tar styrets svar til etterretning.

Forhold knyttet til utkontraktering og oppfølging av leverandører

Foretaket plikter å ha retningslinjer som sikrer at utkontraktert virksomhet oppfyller kravene i IKT-forskriften § 12, jf. IKT-forskriften § 2 annet ledd. IKT-forskriften § 12 første ledd stiller krav til skriftlig avtale, der avtalen skal sikre foretakets rett til å kontrollere, herunder revidere leverandørens aktiviteter. I tillegg må avtalen sikre at Finanstilsynet gis tilgang til opplysninger og tilsyn hos IT-leverandøren, jf. § 12 annet ledd.

Videre skal utkontrakteringsavtaler som gjelder IT-virksomhet, og endring av slike avtaler, behandles av styret, jf. IKT-forskriften § 2 fjerde ledd. Videre skal styret presenteres en plan for utkontrakteringen, en risikovurdering av utkontrakteringsforholdet og en beskrivelse av hvordan foretaket skal sikre leveransene.

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.

Finanstilsynet påpekte i foreløpig rapport at leverandørkjeden til Foretaket har blitt lengre og mer kompleks, og at Foretaket bør kontraktsfeste, formalisere og sikre møteplasser på strategisk, operativt og taktisk nivå. Dagens praksis med uformelle møteplasser, med manglende eller mangelfull dokumentasjon anses ikke å være tilstrekkelig for oppfølging av utkontraktert virksomhet.

Finanstilsynet ba derfor Foretaket sikre at det etableres tilstrekkelige møteplasser med alle leverandører for å sikre at utkontraktert IKT-virksomhet leveres iht. det finansregulatoriske regelverket og i tråd med Foretakets behov.

Styret har i sitt svar til foreløpig rapport sagt seg enige i Finanstilsynets observasjoner, og har igangsatt et arbeid med å formalisere samarbeidet med leverandørene.

Finanstilsynet tar styrets svar til etterretning.

Forhold knyttet til kontroll med tilganger gitt tjenesteleverandører

Ifølge IKT-forskriften § 5 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. I tillegg skal det foreligge retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene. Foretaket plikter å ha retningslinjer som sikrer at utkontraktert virksomhet oppfyller kravene i IKT-forskriften § 12, jf. IKT-forskriften § 2 annet ledd.

Finanstilsynet påpekte i foreløpig rapport at det var Finanstilsynet sin oppfatning at Foretakets hovedleverandør har tilgang til Foretakets kjernesystemer i produksjon. Videre oppfattet Finanstilsynet at Foretaket ikke i tilstrekkelig grad har oversikt over tildelte tilganger til ansatte hos Foretakets leverandører.

Finanstilsynets pekte videre på at Foretaket ikke har tilstrekkelig styring og kontroll med tilganger som er gitt til leverandører.

Finanstilsynet understrekte styrets ansvar for hensiktsmessig tilgangsstyring, også mot leverandører. Dette innebærer at alle tilganger vurderes ut ifra tjenstlig behov, at tilgangene gjennomgås og kontrolleres jevnlig og at leverandørers tilganger er tema i Foretakets oppfølging av utkontrakterte IKT-virksomhet.

Styret har i sitt svar til foreløpig rapport sagt seg enig i Finanstilsynets kommentarer. Videre mener styret at foretaket sine oppdaterte tilleggsavtaler til utkontraktert IKT-virksomhet vil være med å styrke foretaket sin kontroll med tilganger, herunder spesielt tilgang til kjernesystemet.

Finanstilsynet tar styrets svar til etterretning.

Forhold knyttet til forretningsmessig konsekvensanalyse

Ifølge IKT-forskriften § 11 skal foretaket ha etablert en kriseplan som skal kunne iverksettes dersom IKT-driften ikke kan opprettholdes med tilgjengelige ressurser.

Finanstilsynet påpekte i foreløpig rapport at Foretaket bør gjennomføre en forretningsmessig konsekvensanalyse. Analysen bør vise hvordan bortfall av forretningstjenestene kan innvirke på Foretakets forretningsdrift. Gjennomføring av en forretningsmessig konsekvensanalyse vil kartlegge hvor lenge Foretaket kan operere uten sentrale forretningstjenester, og hvilke eventuelle alternative løsninger som kan anvendes for å opprettholde driften av forretningen. Resultatet av Foretakets analyse bør formidles til leverandører dersom analysen viser avhengighet til leverandører for leveranse av forretningskritiske tjenester.

Styret har i sitt svar til foreløpig rapportsagt seg enige med Finanstilsynetsvurdering om at en konsekvensanalyse er et nyttig verktøy til å forbedre selskapets oversikt og fremtidige arbeid med beredskap, krisehåndtering og planlegging, og at foretaket vil ta dette med seg i sitt videre arbeid.

Finanstilsynet tar styrets svar til etterretning.

Forhold knyttet til testaktiviteter

IKT-forskriften §11 tredje ledd stiller krav til at det minst årlig skal gjennomføres opplæring, øvelse og testing av at kriseløsningen fungerer som forutsatt. Resultatet av testen skal dokumenteres.

Finanstilsynet påpekte i foreløpig rapport at Foretaket i større grad enn i dag bør stille krav om at Foretaket involveres i leverandørers testplanlegging. Dette for å sikre at de systemer som inngår i Foretakets forretningskritiske tjenester blir tilstrekkelig ivaretatt i testen.

Styret opplyser i sitt svar til foreløpig rapport at krav om at foretaket involveres i testaktiviteter hos leverandør vil bli innarbeidet i utkontrakteringsavtalene.

Finanstilsynet tar styrets svar til etterretning.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Gisle Solemsjø Haugseth
seniorrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.