FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

KREDINOR AS
Postboks 782 Sentrum
0106 OSLO

| VÅR REFERANSE | DERES REFERANSE | | DATO |
|---|---|---|---|
| 23/15918 | | | 03.06.2024 |

## Tilsynsrapport - IT-tilsyn i Kredinor AS

Finanstilsynet gjennomførte stedlig IKT-tilsyn i Kredinor AS 3. og 4. april 2024. Hensikten med tilsynet var å gjøre en vurdering av hvordan foretaket administrerer, utvikler, drifter, vedlikeholder og sikrer IKT-systemer og -tjenester. Tilsynet ble 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 for utkontrakterte IKT-tjenester, samt overholdelse av regulatoriske krav på IKT-området.

Til grunn for tilsynsrapporten ligger Finanstilsynets foreløpige rapport datert 16. april 2024 og styrets kommentarer til rapporten i brev av 24. mai 2024.

Finanstilsynet har følgende merknader etter det stedlige tilsynet:

### Organisering

Det stilles krav til risikostyring i forskrift om risikostyring og internkontroll. I forskriftens § 3 stilles det 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.

Det er Finanstilsynets vurdering at for å ha god styring og kontroll på egen IKT-virksomhet, også den som er utkontraktert, bør foretaket gjennomføre egne kontroller både når det gjelder risiko og etterlevelse. Finanstilsynet mener videre det er viktig med tilstrekkelig IKT-kompetanse og nok ressurser i de tre forsvarslinjene for å kunne utarbeide et kontrollrammeverk som følger opp egen og utkontraktert virksomhet. Kontrollfunksjonene skal sikre at alle vesentlige risikoer i foretaket er identifisert, målt og rapportert av de relevante organisatoriske enhetene.

I foreløpig rapport pekte Finanstilsynet i sin vurdering på at foretakets oppfølging av IKT-risiko er mangelfull og ikke i samsvar med regelverket, jf. forskrift om risikostyring og kontroll § 4.

Styret skriver i sitt svar at det for førstelinjen er etablert arbeidsprosesser for å sikre oppfølging, videre er det også for andre- og tredjelinje, inkludert for utkontraktert IKT-virksomhet, igangsatt jevnlige kontroller som skal sikre tilstrekkelig oppfølging av IKT-risiko.

**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

Finanstilsynet tar styrets svar til orientering.

Finanstilsynet ble under tilsynet informert om at Kredinor har funnet det hensiktsmessig å organisere informasjonssikkerhetsansvarlig sammen med funksjonene under Chief Digital and Technology Officer for mest og best mulig faglig erfaringsutveksling og informasjonsdeling.

Finanstilsynet pekte i foreløpig rapport på at dersom informasjonssikkerhetsansvarliges plassering i organisasjonen medfører at denne ikke har en uavhengig rolle i forhold til Kredinors førstelinje, må Kredinor sikre at andrelinjen bemannes med ressurser og kompetanse som kan kontrollere og se til at foretakets IT-sikkerhetspolicy er operasjonalisert i foretaket, og at de samme kravene også gjelder for IKT-tjenesteleverandører og underleverandører.

I styrets svar vises det til hvor Kredinor har organisert informasjonssikkerhetsansvarlig i sin organisasjon og videre hvordan uavhengige kontrolloppgaver skal ivaretas.

Finanstilsynet tar styrets svar til orientering.

**Overordnet risikostyring**
IKT-forskriften § 2 første ledd stiller krav til at foretaket skal fastsette overordnede mål, strategier, og sikkerhetskrav for IKT-virksomheten. Etter 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".

Finanstilsynet forventet i foreløpig rapport at styregodkjente styringsdokumenter som strategier og policyer implementeres og følges opp for å sikre at foretakets drift og planer utføres i henhold til Kredinors overordnede strategi. Videre pekte Finanstilsynet på at det kan være formålstjenlig at andrelinjen har kontrolloppgaven med å følge opp de overordnede strategier og policyer for IKT-området.

Styret skriver i sitt svar at de deler Finanstilsynets syn på oppfølgingsansvaret og vil sikre at oppfølging og vedlikehold henholdsvis ivaretas.

Finanstilsynet tar styrets svar til orientering.

**Rapportering av IKT-risiko**
Etter forskrift om risikostyring og internkontroll § 8 skal Kredinors styre ut ifra vurderingene gjort etter § 6 annet ledd og 7 annet ledd i samme forskrift, føre tilsyn med den daglige ledelse og foretakets virksomhet for øvrig, og sørge for at daglig leder regelmessig gir styret informasjon om foretakets virksomhet.

Finanstilsynet pekte i foreløpig rapport på at det meste av foretakets IKT-virksomhet er utkontraktert. Det er Finanstilsynets vurdering at for å kunne ivareta målsetningene som stilles i

interne retningslinjer, er det viktig at det gjennomføres egne kontroller på IKT-tjenester levert av IKT-tjenesteleverandør. Videre ble det pekt på at eksempel på slike kontroller er kontroll med etterlevelse av styrende dokumenter, samt kontroller på områder som tilgangsstyring, endringshåndtering, utvikling, prosjektstyring, beredskap, kompetanse og tilgang på ressurser.
I Finanstilsynets foreløpige rapport var det Finanstilsynets vurdering at det ikke i tilstrekkelig grad gjennomføres egne andrelinjekontroller av IKT-virksomhet for å kunne vurdere etterlevelse av foretakets styrende dokument.

Styret viser i sitt svar til omfattende endringer for internkontrollrapportering, også for IKT-området, og at det i tillegg er etablert egne kontroller for sentrale områder.

Finanstilsynet tar styrets svar til orientering.

**Forretningsmessig 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 forretningsprosesser. Forretningsmessig konsekvensanalyse 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 foretas regelmessig opplæring, øvelse og testing, jf. IKT-forskriften § 11.

Finanstilsynet pekte i foreløpig rapport på at det forventes at foretaket utarbeider forretningsmessige konsekvensanalyser ledet av forretningssiden, der resultatet av konsekvensanalysen blant annet vil gi oversikt over foretakets systemportefølje og der kritikaliteten systemene har for foretakets virksomhet er angitt. Videre bør det av analysen fremgå hva som er akseptabel nedetid for det enkelte IKT-system. Resultatet av analysen bør også formidles til relevante leverandører. Det legges til grunn at rutine for utarbeidelse av forretningsmessig konsekvensanalyse etableres og inngår i foretakets ordinære drift.

Styret skriver i sitt svar at det vil iverksette et arbeid for å utarbeide en forretningsmessig konsekvensanalyse hvor avhengigheter og hvilken kritikalitet systemene har for foretakets virksomhet inkluderes.

Finanstilsynet tar styrets svar til orientering.

**Kriseberedskap**
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 det er foretaket selv som er ansvarlig for at opplæring, øvelse og testing av foretakets kriseløsning gjennomføres årlig. Videre pekte Finanstilsynet på at tester som gjennomføres, både internt i foretaket og hos leverandører, ikke er satt opp med bakgrunn i en dokumentert forretningsmessig konsekvensanalyse. Videre skriver Finanstilsynet at foretaket, med utgangspunkt i sikkerhetspolicy eller andre retningslinjer, må stille krav til testscenarier av kriseløsning hos leverandører eller underleverandører. Dette for å vurdere egnetheten til kriseløsningen og robustheten til organisasjonen inkludert utkontraktert IKT-virksomhet.

Styret viser i sitt svar til at det ved utarbeidelse av forretningsmessig konsekvensanalyse vil sikres at den kobles mot kriseberedskapsplanen, samt til gjennomførte og planlagte beredskapstester.

Finanstilsynet tar styrets svar til orientering.

**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 samme paragraf 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 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.

Finanstilsynets pekte i foreløpig rapport på at det etter Finanstilsynet vurdering er viktig at Kredinor sikrer at egne krav også gjelder for leverandører. Finanstilsynet presiserte viktigheten av at Kredinor må være trygg på at alle leverandører og underleverandører presenterer all informasjon som er nødvendig for å gjennomføre oppfølging av utkontrakterte tjenester. Dette inkluderer at avtaler inneholder tilstrekkelige bestemmelser med innsynsrett for å kunne utøve den nødvendige oppfølgingen av leverandører og underleverandører.

I sitt svar redegjør styret om prosessen for inngåelse av utkontrakteringsavtaler samt oppfølging av disse, og om avtalenes innhold om Kredinors innsynsrett og rett til å kontrollere.

Finanstilsynet tar styrets svar til orientering.

**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. 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 leverandørens aktiviteter kontrolleres. Videre skal det finnes

retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene.

IKT-forskriften § 13 stiller krav til at det er etablert en "oppdatert oversikt over organisasjon, utstyr, IKT-systemer og vesentlige forhold i IKT-virksomheten". Finanstilsynets vurdering er at dette omfatter oppdaterte oversikter over IT-systemer, nettverksenheter, databaser etc. og at utstyrsoversikten bør inneholde tilstrekkelige konfigurasjonsdata og angi avhengigheter mellom utstyr/komponenter.

Finanstilsynet pekte i foreløpig rapport på viktigheten av å ha en fullstendig utstyrsoversikt (Configuration Management Database - CMDB) som inneholder registrering av utstyr, dokumentasjon av sammenhenger mellom utstyr/tjenester og at alt utstyr er oppført med eier.

I styrets svar er det vist til hvordan IKT-tjenesteleverandører ivaretar sine utstyrsoversikter og hvordan Kredinor følger opp og viderefører arbeidet med å komplettere informasjon knyttet til Kredinors applikasjonsportefølje.

Finanstilsynet tar styrets svar til orientering.

**Tilgangsstyring**
IKT-forskriften § 5 Sikkerhet 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 IT-systemene".

Finanstilsynet pekte i foreløpig rapport på viktigheten av å ha god styring og kontroll med tilganger, særlig av utkontraktert IKT-virksomhet. Videre pekte Finanstilsynet på risikoen ved stående tilganger og muligheten for ikke-tjenstlig oppslag.

Styret viser i sitt svar til jevnlige gjennomganger av alle tilganger, også av tilganger hos IKT-tjenesteleverandør, samt at det gjennomføres egne andrelinjekontroller med påfølgende tiltak.

Finanstilsynet tar styrets svar til orientering, men understreker viktigheten av løsninger for tilgangsstyring og kontrollrutiner som i størst mulig grad sørger for at tilganger tildeles og kontrolleres for det enkelte oppdrag.

**Endringsledelse**
Operasjonelle hendelser som medfører vesentlig reduksjon i funksjonalitet som følge av brudd på konfidensialitet, integritet eller tilgjengelighet til IKT-systemer og/eller data skal uten ugrunnet opphold rapporteres til Finanstilsynet, jf. IKT-forskriften § 9 tredje ledd. Foretaket skal rapportere hendelser som foretaket selv kategoriserer som alvorlig eller kritisk, jf. § 9 tredje ledd annet punkt. Foretaket bør videre rapportere andre avvik dersom disse avdekker spesielle sårbarheter i applikasjon, arkitektur, infrastruktur eller forsvarsverk.

Finanstilsynet ba i foreløpig rapport foretaket etablere og dokumentere en egen prosess med rutiner for håndtering av endringer og at prosess med rutiner sikrer at det er Kredinor som står som eier og ansvarlig for alle endringer som innføres i foretakets IKT-virksomhet.

Styret skriver i sitt svar at det er fastsatt tidspunkt for oppstart av arbeidet med å strømlinjeforme endringsprosessen for Kredinor, og at arbeidet vil følges opp til det er gjennomført.

Finanstilsynet tar styrets svar til orientering.

Kopi av dette brevet bes sendt til valgt revisor.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Stig Ulstein
senior tilsynsrådgiver

*Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.*