FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Amesto Accounthouse AS
Styret
Postboks 6395 Etterstad
0604 OSLO

VÅR REFERANSE	DERES REFERANSE		DATO
18/5533			16.11.2018

Kommentarer til håndteringen av IKT-risikoen i regnskapsførervirksomheten i Amestogruppen

1. Innledning

Finanstilsynet viser til stedlig tilsyn hos Amesto AccountHouse AS (AAH) den 18. og 19. juni 2018. Det stedlige tilsynet inkluderte også en gjennomgang av regnskapsførerselskapets IKT-virksomhet. Finanstilsynets merknader etter det stedlige tilsynet datert 16. oktober 2018 gjelder andre forhold enn selskapets IKT-virksomhet.

I likhet med andre regnskapsførerselskaper i Amesto-gruppen, benytter AAH Amesto-gruppens IKT-løsninger i sin virksomhet. AAH og de andre regnskapsførerselskapene har dermed utkontraktert de vesentligste delene av sin IKT-virksomhet til selskaper i Amesto-gruppen. Dette innebærer at systemene i de selskapene i Amesto-gruppen som utfører IKT-tjenester for AAH og andre regnskapsførerselskaper er av vesentlig betydning for AAH og de øvrige regnskapsførerselskapene i Amesto-gruppen. At det foreligger nødvendige avtaler er viktig for å sikre en forsvarlig håndtering av IKT-risikoen.

Som følge av måten IKT-virksomheten var organisert på i Amesto-gruppen valgte Finanstilsynet å kommentere IKT-virksomheten og AAHs håndtering av IKT-risikoen i et eget brev, jf. Finanstilsynets foreløpige merknader til dette i brev av 28. august 2018. Selskapets tilsvar er mottatt i e-post 25. september 2018.

2. Utkontraktering

Regnskapsførerselskaper har fullt ut ansvar for utkontraktert virksomhet. Dette prinsippet har kommet til uttrykk i forskrift om risikostyring og internkontroll som gjelder for regnskapsførerselskaper. Forskriften § 5 har følgende ordlyd:

"Foretaket har ansvar for risikostyring og internkontroll også der deler av virksomheten er utkontraktert. Det skal foreligge en skriftlig avtale som sikrer dette. Avtalen må sikre at foretaket gis rett til innsyn i og kontroll med utkontraktert virksomhet.

Avtalen skal sikre at Finanstilsynet gis tilgang til opplysninger fra og tilsyn med virksomheten der Finanstilsynet finner det nødvendig.

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00
Telefaks 22 63 02 26

post@finanstilsynet.no
www.finanstilsynet.no

Saksbehandler
Tommy Bolsøy
Dir. tlf 22 93 98 80

Foretaket skal sørge for at organisasjonen besitter tilstrekkelig kompetanse til å håndtere utkontrakteringsavtalen".

At utkontraktering skjer til andre selskaper i et konsern er uten betydning for regnskapsførerselskapets ansvar for virksomheten. Forskjellen er at det kan være enklere å få gjennomført de tiltakene som er nødvendig for å oppfylle lovkrav eller å få iverksatt tiltak som fremstår som nødvendig på grunnlag av en forsvarlig vurdering av hvordan de ulike risikoene skal håndteres.

AAH benytter systemer og tjenester som leveres til annet selskap i Amesto-gruppen, herunder tjenester som Amesto-gruppen kjøper inn fra eksterne.

Det forelå ikke formelle avtaler som gjør at AAH oppfyller kravene i risikostyringsforskriften § 5.

AAH har bekreftet at de nødvendige avtaler vil bli inngått innen utløpet av 2018. Finanstilsynet ber om å få tilsendt disse når de foreligger.

3. Risikovurdering

IKT-risikoen er en sentral risiko i regnskapsførerselskaper fordi svikt i slike systemer vil kunne få alvorlige konsekvenser for selskapets oppdragsgivere[1]. Regnskapsførerselskapet må gjøre en selvstendig vurdering av IKT-risikoen, herunder av utkontraktert virksomhet og den må håndteres i samsvar med risikostyringsforskriften.

Etter det stedlige tilsynet reiste Finanstilsynet spørsmål knyttet til AAHs vurdering av selskapets IKT-risiko, herunder for utkontraktert IKT-virksomhet. Spørsmålene gjaldt særlig:

Oppfølgning av drift

Finanstilsynet mener egen kontroll med sentrale IKT-prosesser er en forutsetning for gjennomføring av tilfredsstillende styring og kontroll på IKT-området. Dette gjelder også ved konsernintern utkontraktering.

Basert på opplysninger gitt under tilsynet la Finanstilsynet til grunn at AAH ikke selv utfører oppfølging vedrørende infrastrukturleveranser på områder som problemhåndtering, patching, endringskontroll og hendelser fordi dette ble utført av selskapets IKT-leverandører. I tilsvaret er det fremhevet at AAH i praksis opptrer som avtalepart mot alle sentrale leverandører og at AAH gjør egne vurderinger og handlinger med tanke på tjenestene som benyttes av AAH.

Finanstilsynet finner å kunne legge til grunn at det skjer en oppfølgning av driften fra AAHs side.

[1] Fellesrapport etter Finanstilsynets tematilsyn om IKT-risikoen i regnskapsførerselskaper i 2015, datert 15. april 2016 er publisert på Finanstilsynets nettsted. Denne kan være til hjelp i håndteringen av IKT-risikoen. Også forskrift av 21. mai 2003 nr. 630 om bruk av informasjons- og kommunikasjonsteknologi (IKT-forskriften) vil kunne gi veiledning om hvordan IKT-risikoen kan håndteres på en forsvarlig måte.

Prosjektmetode
Finanstilsynet ble under tilsynet informert om at det ikke er utarbeidet dokumentert prosjektmetode som skal sikre at prosjekt for å implementere nye regnskapskunder blir dokumentert og kvalitetssikret.

I tilsvaret er det vist til at det foreligger sjekklister som skal benyttes ved implementering av nye kunder som både dekker system og formalia, men at sjekklistene ikke alltid benyttes. Videre er det opplyst at det i løpet av kort tid vil bli innført et nytt system og klare rutiner som begge vil sikre både det formelle rundt oppstart og systemoppsett.

Tilgangsstyring
Under tilsynet ble det opplyst at IKT-tjenesteleverandører av utkontrakterte tjenester for AHH har brukeridentiteter med utvidede rettigheter. Når det tildeles brukeridentiteter med utvidede rettigheter (administratortilgang) er gode rutiner for tildeling, bruk av rettighetene, dokumentasjon og kontroll et viktig risikoreduserende tiltak. AHHs rutiner inneholder ikke krav til dokumentasjon for når en brukeridentitet med utvidede rettigheter brukes, eller hva den brukes til.

Det fremgår av tilsvaret at AAH holder på med en gjennomgang av alle interne rutiner og at Finanstilsynets synspunkt vil bli ivaretatt i den forbindelse. Arbeidet med rutinene og dokumentasjon av disse vil være avsluttet i løpet av året. Finanstilsynet tar dette til etterretning.

Penetrasjonstesting
Utviklingen i cyber-kriminalitet innebærer økt risiko. Penetrasjonstesting av den samlede IKT-virksomheten er et viktig tiltak i håndteringen av denne risikoen.

Under tilsynet ble det opplyst at penetrasjonstesting av AAHs systemer ikke har en fast syklus for gjennomføring, og at det var usikkert når siste penetrasjonstest ble gjennomført. I e-post 3. juli 2018 er det oversendt dokumentasjon som gir et litt bredere bilde.

Finanstilsynet mener at AAHs risikovurdering må inkludere behovet for å etablere en fast syklus for gjennomføring av penetrasjonstesting, både fra innsiden og utsiden av selskapets brannmurer for alle de sentrale IKT-leverandørene. I tilsvaret bekrefter AAH at det vil bli vurdert hvordan dette kan gjøres og at det vil bli tatt hensyn til i arbeidet med en ny "Security Policy" for konsernet som tar utgangspunkt i de krav som ligger i ISO 27001. Finanstilsynet tar dette til etterretning.

Kapasitet i IKT-organisasjonen
Under tilsynet ble Finanstilsynet informert om at det i Amesto-gruppens strategidokument er lagt opp til en vesentlig omsetningsvekst, blant annet som følge av salg av et produkt som selskapet er med på å utvikle sammen med to andre aktører. Fordi kapasitet og kompetanse på IKT-området er av sentral betydning for IKT-risikoen i Amesto-gruppen, og også i AAH og de andre regnskapsførerselskapene i gruppen, reiste Finanstilsynet spørsmål ved om den etablerte IKT-organisasjonen var i stand til å håndtere en vesentlig økning i omsetningen på en forsvarlig måte.

I tilsvaret gis det uttrykk for enighet i at det er behov for en styrking på IKT-området som følge av den strategiske satsingen. Blant annet opplyses det at det arbeides med etablering av en utviklingsfunksjon som forventes å bli operativ i løpet av 2018. Finanstilsynet tar redegjørelsen til

etterretning, og legger til grunn at IKT-organisasjonen løpende blir tilpasset behovet slik at både kapasiteten og kompetansen er forsvarlig til enhver tid.

4. Finanstilsynets konklusjon

Det stedlige tilsynet avdekket enkelte svakheter knyttet til IKT virksomheten for regnskapsførerselskapene i Amesto-gruppen. Finanstilsynet tar til etterretning at AAH har påbegynt og vil iverksette ytterligere tiltak for å utbedre svakhetene.

For Finanstilsynet

Kjersti Elvestad
seksjonssjef

Tommy Bolsøy
seniorrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.