FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Vedlegg til tematilsyn 2015 – KRT-1175 IKT-Risiko

Skjemaet består av følgende deler:

1. Generelle opplysninger
2. Risikovurdering og styring
3. Regnskapssystemer og oppdragsstyringssystemer
4. Utkontraktering av IKT-virksomhet
5. Sikkerhet
6. Endringer i IKT-systemer
7. Drift og vedlikehold av IKT-systemer
8. Håndtering av alvorlige driftsavbrudd
9. Forholdet til oppdragsgiverne

Noen av spørsmålene gjelder plikter som følger direkte av lovgivningen og den bransjefastsatte standarden GRFS, som trådte i kraft 1. januar 2015. I disse tilfellene er det lenke til den aktuelle lovgivning i skjemaet. Øvrige spørsmål gjelder handlinger eller vurderinger som er ansett som egnet til å ivareta disse pliktene.

Samtlige spørsmål kan besvares på grunnlag av informasjon, vurderinger og kontrakter som er tilgjengelige hos regnskapsførerselskapet. Det er lagt inn hint- og hjelpetekster på de spørsmålene der Finanstilsynet har ment at det er hensiktsmessig.

<u>Spørsmål knyttet til rutiner</u>
Når det svares "ja" på spørsmål om det foreligger rutiner, legger Finanstilsynet til grunn at rutinene er skriftlig. GRFS åpner for at regnskapsførerselskapet kan vurdere behovet for å ha skriftlige rutiner. Finanstilsynet mener imidlertid at de rutinene som søkes kartlagt gjennom spørsmålene må foreligge skriftlig hvis de skal være et egnet virkemiddel for styring og kontroll av IKT-risiko. Dersom det ikke foreligger skriftlige rutiner som dekker forholdet, skal det svares "nei" på spørsmålet.

<u>Spørsmål knyttet til utkontraktering</u>
Mange regnskapsførerselskaper utkontrakterer deler av sin IKT-virksomhet. Selv om dette innebærer at IKT-virksomheten utføres av andre, har regnskapsførerselskapet fortsatt det overordnede ansvaret overfor oppdragsgivere, myndigheter og andre. For å kunne ivareta det overordnede ansvaret, må regnskapsførerselskapets styre og ledelse ha et klart bilde av risikoen på IKT-området og håndtere denne risikoen på en forsvarlig måte. At det internt i regnskapsførerselskapet utpekes personer som har ansvar for enkelte områder eller enkelte oppgaver, fratar ikke regnskapsførerselskapets styre og ledelse det overordnede ansvaret.

Det overordnede ansvaret er et annet enn det kontraktsmessige eller erstatningsrettslige ansvaret som gjelder i forholdet mellom regnskapsførerselskapet og andre parter. Hvordan

regnskapsførerselskapets styre og ledelse håndterer kontraktsmessig risiko, vil imidlertid kunne være av betydning for vurderingen av hvordan det overordnede ansvaret er ivaretatt.

Kjøp og bruk av standard regnskapssystemer eller oppdragsstyringssystemer vil være utkontraktering av IKT-virksomhet dersom dette kjøpes sammen med løsninger for lagring av opplysninger (regnskapsinformasjon, oppdragsdokumentasjon eller annet) eller hvis leverandøren påtar seg drift av IKT-systemene (sikkerhet og vedlikehold). Bruk av fildelings- og oppbevaringstjenester (som for eksempel Jottacloud, Dropbox, OneDrive, iCloud), innebærer også utkontraktering av virksomhet.

Ved utkontraktering må regnskapsførerselskapet vurdere om de lovmessige kravene er oppfylt, særlig overholdelse av taushetsplikt, behandling av personopplysninger og risikostyring av virksomhet som er utkontraktert. For fildelings- og oppbevaringstjenester (som for eksempel Jottacloud, Dropbox, OneDrive, iCloud) må vurderingen også inkludere risikoen for at medarbeidere på eget initiativ benytter denne type løsninger i sitt arbeid, uten at det foreligger en skriftlig avtale mellom regnskapsførerselskapet og leverandøren, og dermed er utenfor regnskapsførerselskapets styring og kontroll.

Regnskapsførerselskapenes muligheter til å styre og kontrollere IKT-risikoen knyttet til utkontraktert virksomhet, vil være avhengig av de kontraktene som systemleverandørene tilbyr. Det er derfor nødvendig å ha kontraktene tilgjengelig når spørsmål 4.7 – 4.12 skal besvares.

Dersom svarene i tematilsynet viser at kontraktene ikke gir regnskapsførerselskapene slik styring og kontroll som er nødvendig, vil Finanstilsynets samlerapport kunne være nyttig for bransjens vurdering av om det er behov for justeringer i de standardkontraktene som leverandørene tilbyr. Det er derfor viktig at disse spørsmålene besvares ut fra hva som står i kontraktene, ikke hva systemleverandørene har gjort eller sier seg villig til å gjøre utover det som er kontraktsfestet.

Utarbeidet 24.09.2015.