KOMBIT

Version 2.4

Instruks til systemspecifik ISAE 3402-erklæring

Indholdsfortegnelse

1. Instruks til systemspecifik ISAE 3402-erklæring

Denne instruks er udarbejdet af KOMBIT til brug for KOMBITs kontrakter med leverandører om levering af drift, vedligeholdelse mm. af de enkelte it-systemer (i de enkelte kontrakter benævnt "Systemet").

Instruksen skal følges af leverandørerne og dennes revisor ved levering af ISAE 3402 revisionserklæringer under den enkelte kontrakt med KOMBIT.

Formålet med revisionserklæringen er, at kommunerne i deres revision af, at der er foretaget lovmedholdelige transaktioner og beregninger, kan anvende denne revisionserklæring som en del af dokumentation for systemets korrekte håndtering af økonomiske transaktioner og beregninger.

Alle revisionserklæringer skal være afgivet med en høj grad af sikkerhed.

2. Omfang

ISAE 3402 erklæringen skal omfatte en beskrivelse af leverandørens system med tilhørende relevante kontrolmål og kontroller.

Ved vurdering af, om serviceleverandørens beskrivelse af sit system er retvisende, skal revisor som minimum anvende de almindelige kriterier i ISAE 3402, herunder

- hvorvidt beskrivelsen viser, hvordan serviceleverandørens system blev udformet og implementeret, herunder når det er relevant:
    - de typer af ydelser, der er leveret, herunder, når det er relevant,
        - de grupper af transaktioner, der er behandlet
        - de procedurer i såvel it som manuelle systemer som leverer ydelserne, herunder, når det er relevant, procedurer, som igangsatte, bogførte, behandlede, om nødvendigt rettede og overførte transaktioner til rapporter og anden information, der er udarbejdet til modtagerne af revisionserklæringen.
    - tilknyttede registreringer og underliggende information, herunder, når det er relevant, regnskabsregistreringer, underliggende information og specifikke konti, der anvendes til at igangsætte, bogføre, behandle og rapportere transaktioner; dette omfatter rettelse af fejlinformation, og hvordan information overføres til rapporter og anden information, der udarbejdes til modtagerne af revisionserklæringen.

    - hvordan leverandørens system behandler andre betydelige begivenheder og forhold, som ikke er transaktioner.
    - den proces, der anvendes til at udarbejde rapporter og anden information til modtagerne af revisionserklæringen.
    - de anførte kontrolmål og kontroller, der er udformet til at nå disse mål
    - komplementerende kontroller hos modtagerne af revisionserklæringen der er lagt til grund ved kontrollernes udformning, herunder angivelse af hvorvidt KOMBIT eller kommunerne er ansvarlige for den komplementære kontrol, og
- andre aspekter ved leverandørens kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågnings- kontroller, der er relevante for de leverede ydelser.

Generelle it-kontroller

Det er forventningen, at erklæringen som minimum vil omfatte kontrolmål og kontroller relateret til generelle it-kontroller for systemet, samt de manuelle og automatiske kontroller der er relevante for at sikre fuldstændig og nøjagtig processering af transaktioner i systemet.

De generelle kontroller skal forholde sig til:

- It-sikkerhedspolitik
- Change management
- Adgangsstyring, herunder
    - funktionsadskillelse
    - adgangskontrol
- Backup
- Hændelsesstyring
- Patch Management
- Fysisk sikkerhed
- Adskillelse af drifts- test- og udviklingsmiljøer
- Håndtering af testdata
- Sikker udviklingspolitik

De gennemførte test af de generelle kontroller skal være målrettet systemet.

Det nøjagtige omfang aftales jævnfør nedenstående afsnit om planlægningsmøde.
Revisionserklæringen skal være systemspecifik, og der kan derfor ikke anvendes en generel erklæring dækkende flere systemer.

Identificerede forhold, forbehold og findings

Såfremt revisionserklæringen indeholder forbehold, fremhævelse af forhold eller bemærkninger til kontrollernes design, implementering eller effektivitet, skal leverandøren samtidig med fremsendelsen af revisionserklæringen til KOMBIT fremsende en fyldestgørende handlingsplan, som beskriver, hvordan og hvornår de omhandlede forhold bringes i orden.

I tillæg til erklæringen skal leverandøren udlevere en oversigt fra revisor over revisors findings, som ikke indgår i revisionserklæringen (prioritet 3 findings) som følge af at disse vurderes at udgøre en mindre risiko/svaghed. Listen med revisors prioritet 3 findings skal give KOMBIT et mere komplet overblik over svagheder i Systemet.

Kommunerne anvender revisionserklæringen som dokumentation for systemets korrekte håndtering af økonomiske transaktioner og beregninger, og kommunerne har derfor ret til at få ISAE 3402-erklæringer med besvarelse af supplerende instrukser udleveret.

3. Anvendelse af underleverandører

I det omfang der anvendes underleverandører i forbindelse med levering af ydelsen, herunder eksempelvis til hosting, drift, behandling af data mv., er det leverandørens ansvar at sikre, at den pågældende underleverandør har implementeret relevante kontroller i forhold til de leverede ydelser til kommunerne. Leverandøren kan vælge enten direkte at inkludere underleverandørens systembeskrivelse med tilhørende kontrolmål og kontroller i ISAE 3402 erklæringen (helhedsmetoden) eller udelade dette fra erklæringen (partielmetoden).

Hvis partielmetoden vælges, skal ISAE 3402 erklæringen som minimum indeholde kontrolmål og kontroller til monitorering af underleverandørens kontroller. Det er forventningen, at denne monitorering vil omfatte indhentelse og gennemgang af revisorerklæringer med tilsvarende indhold og detaljeringsgrad som i en ISAE 3402 erklæring. Erklæringerne fra underleverandørerne skal enten omfatte samme periode eller en periode, der slutter højst 3 måneder tidligere end leverandørens egen erklæring. Leverandøren skal yderligere sikre, at erklæringer fra underleverandører kan stilles til rådighed for kommunerne.

4. Planlægningsmøde

Leverandører skal, som led i planlægningen af revisionen, sikre at der indkaldes til et møde med KOMBIT og leverandørens revisor (”3-partsmøde”). Formålet med mødet er at gennemgå revisionsforløbet og omfanget af erklæringen. Inden mødet fremsender leverandøren forslag til kontrolmål og kontroller der skal omfattes af erklæringen. På mødet drøftes blandt andet følgende:

- Hvorvidt der forefindes en transaktions- og beregningslog, som gør det muligt at revidere gennemførte transaktioner og beregninger samt kontrol af lovmedholdelighed samt ansvarsfordeling mellem kommuner og leverandøren
- Eventuelle eksterne kildedataleverandører, underleverandører hos leverandøren samt underleverandørers eventuelle under-underleverandører, som behandler data i forbindelse med systemets økonomiske beregninger og transaktioner.
- Gennemgang af den af leverandøren fremsendte oversigt over kontrolmål og kontroller der forventes omfattet af ISAE 3402-erklæringen
- Drøftelse af hvorledes en række specifikke kontrolområder forventes dækket af erklæringen, herunder:
    - At systemet og setup er tilstrækkelig robust i forhold til manipulation af beregningsmotor samt transaktionslogik.
    - At der foretages validering af data fra eksterne kilder.
    - At der ikke foretages økonomiske transaktioner eller beregninger uden nødvendigt datagrundlag samt nødvendige godkendelser fra brugerne samt myndigheder.
    - At brugere samt systemadministratorer af systemet er valideret i tilstrækkelig grad for at undgå uautoriserede transaktioner og beregninger.
    - At der kan foretages nødvendig genopretning ved eventuelle fejl i transaktioner og beregninger.
- Hvorledes KOMBITs ønsker til specifikke kontroller og andre områder kan indarbejdes i revisionserklæringen.
- Proces for at sikre involvering af KOMBIT inden underskrift af revisionserklæring med henblik på at afklare eventuelle anmærkninger fra revisor.

5. Versionshistorik

Version:	Dato for revidering:	Revideret af:
2.3	16/08/2023	Service Management
2.4	12/05/2025	Drift – præcisering ift. generelle it-kontroller og komplementerende kontroller