

Outsourcing

Erklæring om generelle it-kontroller og applikationskontroller

IT-Revision & Risikostyring

Rammerne for it-anvendelsen

Det er nu blevet almindeligt, at virksomheder outsourcer it-opgaver og aktiviteter til outsourcingleverandører, som har den pågældende it-ydelse som deres fokusområde. Dermed kan virksomheden øge fokuseringen på egne kerneaktiviteter, ligesom der ofte kan være økonomiske og kompetencemæssige fordele ved at outsource til en ekstern leverandør.

Der er ikke to outsourcingopgaver, der er ens. Derfor udfærdiges der normalt en kontrakt mellem parterne, hvori det blandt andet aftales, hvilke it-ydelser der skal leveres hvornår, hvor længe og hvordan. I kontrakten aftales det normalt også, hvilke kontroller og andre forhold, som leverandøren skal efterleve.

Virksomheden kan dog have svært ved efterfølgende at sikre sig, at outsourcingleverandøren lever op til de aftalte betingelser i kontrakten. Derfor kan leverandøren få udarbejdet en revisorerklæring til eget og / eller til brug overfor leverandørens kunder vedrørende de generelle it-kontroller og applikationskontroller m.v. i forbindelse med de ydelser, der leveres. Leverandøren kan herefter vælge at bruge erklæringen overfor sine kunder som dokumentation for de etablerede kontroller i relation til den indgåede outsourcingkontrakt.

Nogle kunder har endvidere brug for en revisorerklæring som følge af, at de dele, som er outsourcet, vedrører væsentlige dele af deres regnskabsrapportering. Danske kunder vil normalt efterspørge en erklæring



baseret på revisionsstandard 3411, mens udenlandske og især amerikanske kunder ofte vil efterspørge en erklæring udarbejdet i henhold til den amerikanske revisionsstandard SAS70. Grant Thornton udfører begge typer af erklæringer.

Hvad indeholder en erklæring efter revisionsstandard 3411?

En 3411 erklæring kan gennemføres som en Type A eller en Type B erklæring. Ved en Type A erklæring udtaler revisor sig om udformningen og implementeringen af de aftalte interne kontroller hos leverandøren. Ved en Type B erklæring udfører revisor det samme som ved Type A, men derudover udtaler revisor sig også om funktionaliteten af de interne kontroller. Det vil sige, at revisor foretager test af de etablerede kontroller for at konstatere, om de fungerer effektivt. Det er aftalen mellem kunden og leverandøren, som afgør, om der skal udarbejdes en Type A eller Type B erklæring.

Udgangspunktet for erklæringen er aftalen mellem leverandøren og dennes kunde(r) samt relevant lovgivning. Revisor skal indhente et tilstrækkeligt og egnet revisionsbevis for manuelle og programmerede kontroller.

En gennemgang kan vedrøre generelle it-kontroller og / eller applikationskontroller alt efter typen af outsourcing.

Generelle it-kontroller - overblik

Generelle it-kontroller er politikker og procedurer, der vedrører mange applikationer og understøtter, at applikationskontrollerne fungerer effektivt ved at hjælpe med at sikre behørig drift af informationssystemer. Ved en gennemgang af de generelle it-

kontroller udføres der normalt revision af:

- drift af datacentre og netværk
- anskaffelse, ændring og vedligeholdelse af systemsoftware
- adgangssikkerhed.

Applikationskontroller - overblik

Applikationskontroller anvendes typisk på forretningsprocesniveau, og er manuelle eller programmerede procedurer, der skal være med til at sikre, at transaktioner har fundet sted, er godkendte og er fuldstændigt og nøjagtigt bogført og behandlet.

Ved en gennemgang af applikationskontrollerne skal revisor undersøge, hvorvidt:

- applikationskontroller sikrer en fuldstændig, nøjagtig og rettidig behandling af stedfundne og godkendte transaktioner
- applikationskontroller forhindrer, at fejl opstår, eller sikrer, at opståede fejl opda- ges og foranlediges korrigeret
- der er dokumentation for den foretagne databehandling og de udførte applikationskontroller.

Derudover skal revisor indhente tilstrækkeligt og egnet bevis for kontroller inden for følgende områder i det omfang, funktionerne er omfattet aftalen:

- adgangsrettigheder og funktionsadskillelse
- databehandling, herunder transaktions- og kontrolspor
- vedligeholdelse af stamdata
- grænseflader, herunder dataoverførsel
- eventuelle datakonverteringer
- dokumentation
- relevante generelle it-kontroller, herunder sikkerhed i anvendte databaser.

3411 Erklæringen

På baggrund af vores arbejde udarbejder vi en erklæring til leverandøren og dennes kunder, hvori vi beskriver det udførte arbejde og vores konklusion vedrørende kontrolmiljøet. I et tillæg til erklæringen udarbejder vi normalt et bilag, hvor det identificeres hvilke test af kontroller, der er udført og de tilknyttede resultater.



Vores erfaring viser, at der er flere og flere leverandører, der får udarbejdet en 3411 erklæring med den begrundelse, at virksomhederne / kunderne i den indgåede outsourcingkontrakt stiller krav om en 3411 erklæring fra en uafhængig revisor.

Udarbejdelse af en 3411 erklæring sker med udgangspunkt i den indgåede aftale mellem leverandøren og virksomheden. Der foretages interview af de it-ansvarlige hos leverandøren, ligesom der foretages tests af relevante kontroller.

Hvorfor vælger nogle outsourcingleverandører at få udarbejdet en 3411 erklæring uden at en kunde direkte har stillet krav herom?

I de tilfælde hvor der i stort omfang leveres ydelser efter en standardkontrakt, vælger mange outsourcingleverandører at få en uafhængig revisor til at udarbejde en 3411 erklæring, fordi leverandøren på den måde kan dokumentere, at de har etableret et tilfredsstillende internt kontrolmiljø, der er gennemgået og vurderet af en uafhængig revisor. Leverandøren kan benytte erklæringen overfor eksisterende kunder og i salgsøjemed overfor nye kunder.

Hvornår kan man få udarbejdet en 3411 erklæring?

Udarbejdelse af en 3411 erklæring kan i princippet udføres på et hvilket som helst tidspunkt på året. Ligesom erklæringen kan omfatte bestemte perioder af kortere eller længere varighed, dog maksimalt og typisk for et år ad gangen.

Der er dog en tendens til, at leverandørerne ønsker erklæringen udarbejdet for et år ad gangen i forbindelse med årets udløb. Dermed kan leverandøren videregive erklæringen til kunderne med revisors udtalelse om det interne kontrolmiljø for det forløbne år.

SAS70

SAS70 er den amerikanske revisionsstandard for erklæring fra en leverandør til en eller flere kunder. Krav om en SAS70 erklæring kommer typisk fra en amerikansk kunde, der er børsnoteret i USA.

Der er visse ligheder mellem 3411 og SAS70 erklæringen, men SAS70 erklæringen er reelt en egentlig rapport og væsentlig mere omfangsrig og kompleks end den danske 3411 erklæring. Der er en række specifikke amerikanske krav til omfanget af revisors arbejde, til de beskrivelser som skal være med i rapporten, og hvordan arbejdet dokumenteres i rapporten og ikke mindst hos revisor. For at det kan kaldes en SAS70 erklæring, skal det endvidere være en revisor med amerikansk statsautoriseret revisoreksamen, der underskriver erklæringen.

I Danmark udfører vi en SAS70 erklæringsopgave i samarbejde med Grant Thornton i USA, som har stor ekspertise på området.

Hvad er resultatet?

Rapporteringen sker efter aftale, og på den måde, som passer bedst til Deres virksomhed.

Vi udarbejder dog altid en erklæring, hvor vi beskriver, hvad der er udført af arbejde samt om de undersøgte kontroller fungerer som forudsat, herunder om de lever op til kontrakten. Herudover kan der udarbejdes en rapport med tilhørende observationsskema med detaljeret beskrivelse af identificerede risici og med vores tilhørende anbefalinger og prioritering indenfor de nævnte områder.



Hvordan kommer jeg videre?

Hvis en 3411 erklæring er relevant for jer, eller hvis I vil vide mere om erklæringsopgaver i forbindelse med generelle it-kontroller og applikationskontroller, så kontakt venligst Grant Thorntons afdeling for It-revision & Risikostyring.

Michael Clement

Director
T +45 35 27 12 36
mic@grantthornton.dk



Klaus Myssen

Manager
T +45 35 27 12 33
kmy@grantthornton.dk



grantthornton.dk
Statsautoriseret Revisionsaktieselskab

Stockholmsgade 45 • DK-2100 København Ø
Tlf. 35 27 11 00 • Fax 35 27 11 01
Hjulmagervej 8 K • DK-7100 Vejle
Tlf. 76 43 25 00 • Fax 76 43 25 01