Der findes forskellige typer erklæringer inden for it-revision. Her fortæller vi om forskellen på ISAE 3000, ISAE 3402, og ISRS 4400.

Forskellige erklæringer bruges til forskellige formål, og de kan dække alt fra et øjebliksbillede (point-in-time) til perioder på et års tid. Samtidig kan omfanget af erklæringerne variere – nogle erklæringer dækker hele it-brugen i en virksomhed, andre dækker et specifikt område, fx applikationssikkerhed, lovgivningsmæssige forhold eller fysiske forhold.

De tre mest udbredte erklæringstyper er ISAE 3000, ISAE 3402, og ISRS 4400. Fælles for dem alle er, at det er internationale erklæringsstandarder, som også er gældende i udlandet.

ISAE 3000

En 3000-erklæring er som regel en kortere erklæring, der dækker en konkret arbejdshandling, eksempelvis databeskyttelsesforordningen (GDPR), outsourcing-bekendtgørelsen, eller forpligtelser overfor en bestemt kunde.

I erklæringen gennemgår vi det udvalgte område samt relateret dokumentation, og giver en samlet vurdering af, hvor betryggende området håndteres hos virksomheden. Samtidig giver vi en vurdering for hvert delområde, så virksomheden præcist kan se, hvad der fungerer som det skal, og hvad der eventuelt skal arbejdes med.

Denne type erklæring kan afgives enten som et øjebliksbillede eller for en bestemt periode – fx et år.

ISAE 3402-I og 3402-II

3402 er en lidt længere erklæring, hvor en lang række af kontrolområder gennemgås, og den må betragtes som den klassiske it-revisionserklæring. 3402 forholder sig til alle forretningsgange omkring it-funktionen, som kan have indflydelse på den finansielle rapportering: Udvikling, drift, beredskab, dokumentation mv. Den forholder sig også til det helt lavpraktiske, som fx de fysiske forhold, såsom hvordan er servere/datacenter placeret.

Når vi laver en sådan erklæring for en virksomhed, gennemgår vi dokumentation og foretager stikprøvevis kontrol af de forskellige områder.

Det munder så ud i både en samlet konklusion, og en vurdering af hvert enkelt område. Samtidig giver vi også konstruktive anbefalinger til forbedring af de enkelte områder. Vi bruger ISO 27002-standarden som referenceramme for vores gennemgang.

3402-I viser et øjebliksbillede, og 3402-II dækker en periode, typisk et år.

3402-erklæringer bruges til at dokumentere, at sikkerhed og kvalitet af it-systemer og -forhold er i orden hos den pågældende virksomhed.

ISRS 4400

Denne erklæring er ikke så gængs, men benyttes i særlige tilfælde. Erklæringen bruges til aftalte arbejdshandlinger, og minder en del om ISAE 3000, men den kan i høj grad defineres af kunden selv.

Eksempelvis bruges den, hvis en virksomhed vil påvise, at de overholder certificeringskrav stillet af en brancheforening. Et andet eksempel er en virksomhed, der overfor en kunde skal påvise at de overholder nogle meget specifikke krav.

En ISRS 4400-erklæring bruges altså til verificering af, om en virksomhed lever op til specifikt udformede krav.

Hvad kan disse erklæringer så bruges til?

Man bruger de forskellige erklæringstyper i forskellige sammenhænge – afhængigt af, om man skal dokumentere sikkerheden i et bestemt område overfor kunder og samarbejdspartnere; have generel verifikation af, at ens it-organisation fungerer på betryggende vis; eller om man skal leve op til lovkrav eller certificeringskrav.

Hvis du vil vide mere om de forskellige erklæringstyper, er du meget velkommen til at kontakte os for et uforpligtende møde.

REVI-IT A/S • statsautoriseret revisionsaktieselskab
Jens Kofods Gade 1 • 1268 København K • Tlf. 3311 8100 • info@revi-it.dk • revi-it.dk • CVR-nr. 3098 8531