

3402-ERKLÆRINGER

IT-systemer og applikationer bliver løbende mere komplekse – både i selve systemernes struktur, men også i forhold til de IT-sikkerhedsmæssige krav – krav om generelle IT-kontroller og overholdelse af GDPR-lovgivningen.

Af revisionsbekendtgørelsen fremgår, at ” Det påhviler den enkelte institutions ledelse at sikre, at der foreligger systemrevisionserklæringer for de i pkt. 2.2-2.5 nævnte systemer og tilhørende databehandling, medmindre de anvendte systemer eller databehandlingen varetages af Statens It eller andre myndigheder, der revideres af Rigsrevisionen.” Men skal man som ledelse så alene sikre, at der foreligger systemrevisionserklæringer? Skal de også forstås? Og hvilke systemer skal der foreligge erklæringer på?

Det er en kompleks øvelse at læse sig igennem disse erklæringer, hvis ikke der er en vis systemmæssig indsigt og forståelse.

For at erklæringerne har den nødvendige relevans, så skal de være underskrevet af en godkendt revisor med en særlig IT-revisionsuddannelse.

Revisors arbejde er sat på spidsen at sikre, at der foreligger politikker og forretningsgange på et givet tidspunkt vedrørende IT-området (Type 1), og at disse politikker og forretningsgange har været efterlevet af IT-leverandøren igennem den periode, som testes (type 2). Revisionsmæssigt er alene en type 2-erklæring egnet som revisionsbevis.

Men er den hellige grav så velbevaret med en type 2-erklæring?

Det korte svar er nej. Der står typisk en lang række forhold som skal håndteres hos de enkelte institutioner. Det er typisk forhold knyttet til brugeradministration, dvs. hvem der har adgang til hvilke systemer og i hvilket omfang, samt sikring af løbende versionsopdatering.

Mange systemer genererer herudover en lang række kontrolrapporter og LOG's som det er institutionens ansvar løbende at gennemgå og følge op på. Sker dette ikke, så bortfalder den opfattede IT-sikkerhed, da de generelle IT-kontroller er baseret på denne opfølgning mv.

Ingen systemer er ens og det er forskellige ting som der skal følge op på.

Hos Beierholm gennemgår vi hvert år de relevante IT-revisionserklæringer og følger op på de forhold som det er de enkelte institutioners ansvar at håndtere lokalt. Er I i tvivl om kravene til jer, så kontakt os gerne for assistance.

Partner, statsautoriseret revisor

Uffe Black Jensen, Tlf. 25 29 30 16, ubj@beierholm.dk