ISAE 3000
ISAE 3402

Revisorerklæringer om informationssikkerhed og databehandleraftaler (GDPR)

En uafhængig revisorerklæring om virksomhedens informationssikkerhed er stærk dokumentation i forhold til kunder og samarbejdspartnere. Samtidig skærper erklæringsarbejdet jeres fokus på solide og effektive it-procedurer.

INDHOLD

- Indledning
- Hvad er en it-revisorerklæring?
- Hvilke typer it-revisorerklæringer findes der?
- Hvem har brug for en it-revisorerklæring?
- Hvordan kan en it-revisorerklæring styrke din virksomhed?
- Hvordan får man en it-revisorerklæring?
- Høj kvalitet, effektiv proces og minimalt ressourcetræk

Indledning

Solide procedurer og sikker behandling af personfølsomme data er vigtigere end nogensinde.

Stadig oftere bliver man som databehandler eller serviceleverandør bedt om at levere uafhængig dokumentation for, at man har styr på informationssikkerheden. I nogle brancher og sektorer er det et decideret krav, at man kan fremvise en it-revisorerklæring.

Men overalt i samfundet har den stigende digitalisering øget opmærksomheden om it- og informationssikkerhed. Emnet er rykket ind i direktions- og bestyrelseslokalerne, og myndighederne vedtager løbende ny lovgivning og udsteder bøder til dem, der ikke efterlever reglerne.

I bund og grund handler it-revision om at kunne vise kunder, samarbejdspartnere og omverden, at man har orden i penalhuset og har en professionel tilgang til virksomhedens styring af informationssikkerhed. Det gælder ikke kun større foretagender. I praksis er det et krav eller en forventning, der stilles til alle virksomheder, som leverer it-serviceydelser eller håndterer persondata som databehandler. Og det er flere, end mange af os går og tror.

Her kan du få mere at vide om, hvad en it-revisorerklæring er, hvem der kan eller bør få den udarbejdet, og hvordan det foregår.

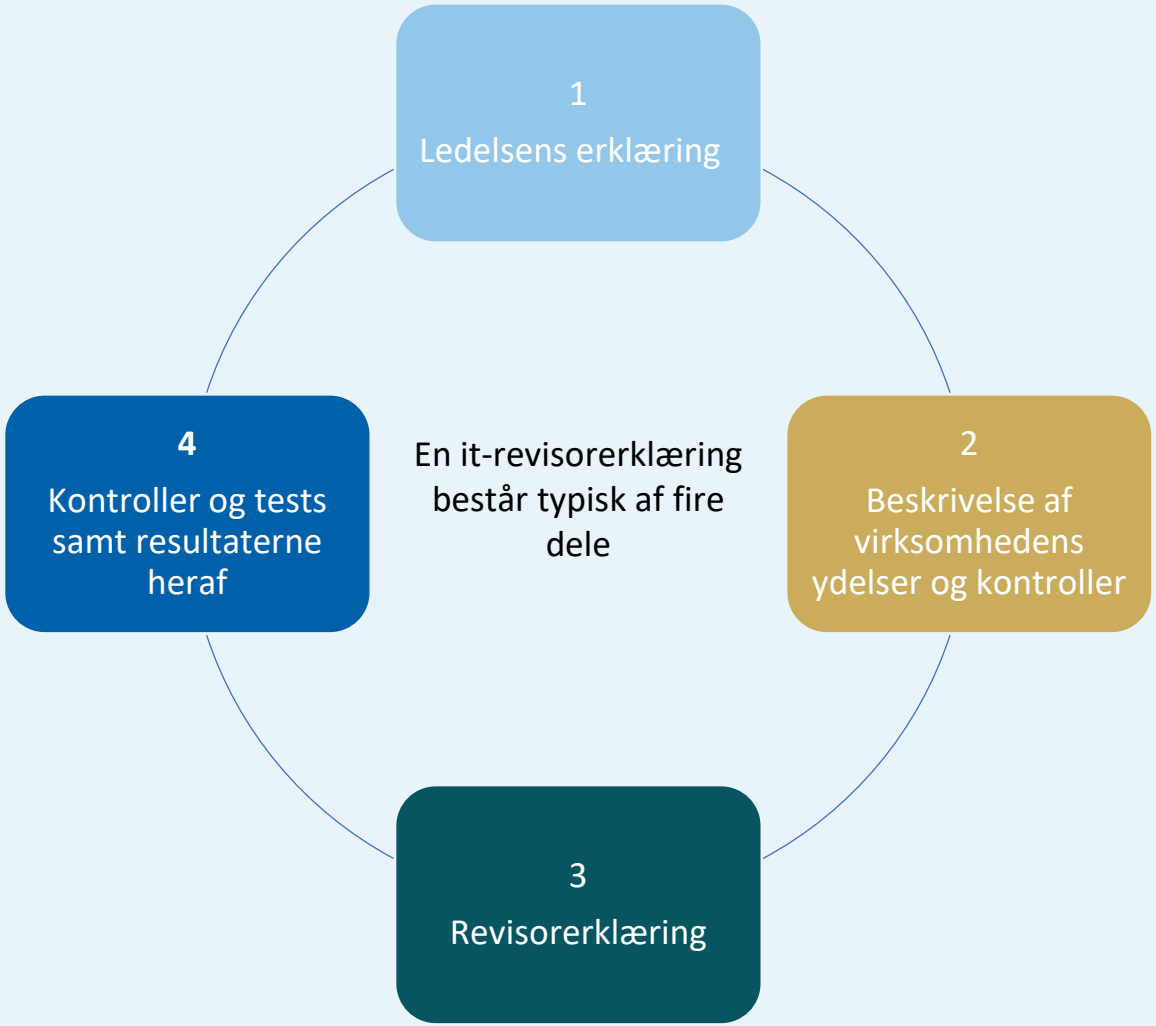
Hvad er en it-revisorerklæring?

En it-revisorerklæring viser kunder, samarbejdspartnere og interessenter, at I har beskrevet alle it-procedurer og -processer på en måde, der afspejler virkeligheden i jeres virksomhed. I får med andre ord papir på, at I gør dét, I har skrevet, at I vil gøre.

Som it-revisorer kigger vi også på, om I lever op til eventuelle krav, regler og retningslinjer på jeres område.

Formålet er at få et uafhængigt og retvisende billede af jeres styring af informations-sikkerhed, og hvordan I arbejder med informationer og persondata. Det giver gennemsigtighed, så kunder og samarbejds-partnere nemt kan se, hvad I gør, og hvor godt I har tjek på tingene.

Ofte giver it-revision også overblik over, hvor I kan forbedre og effektivisere arbejdsgange og procedurer. Undervejs kan vi hjælpe med faglig sparring om, hvordan I kan udvikle jeres set-up.



Hvilke typer it-revisorerklæringer findes der?

Der findes flere typer it-revisorerklæringer, der bruges til forskellige formål og virksomheder. De kan også omfatte forskellige tidsperioder.

Erklæringerne har dog det til fælles, at de er internationale erklæringsstandarder. Derfor fungerer de også som dokumentation over for kunder og samarbejdspartnere i udlandet.

To af de mest almindelige it-revisorerklæringer er:

- ISAE 3000 – Databehandlererklæring
- ISAE 3402 - Generelle IT-kontroller

Erklæringerne udarbejdes som enten et øjebliksbillede (type 1) eller en periodeerklæring (type 2).

ISAE 3000 Databehandler-erklæring

- *Databehandlere:* Vi udtaler os her med høj grad af sikkerhed om de tekniske og organisatoriske sikkerhedsforanstaltninger, I som databehandlere har indført for at beskytte de oplysninger, I håndterer på vegne af jeres kunder.

ISAE 3402 Generelle it-kontroller

- *It-serviceleverandører* Denne erklæring afgiver vi, hvis din virksomhed er it-serviceleverandør – det kan fx være hosting, drift af en it-funktion, opbevaring af data for kunder eller levering af Software as a Service (SaaS). En ISAE 3402-erklæring giver et billede af den generelle tilstand af jeres styring af informationssikkerheden og spænder bredt – fra de it-relaterede forretningsgange, der kan påvirke den finansielle rapportering til den fysiske placering af jeres servere. Udgangspunktet for vores arbejde er ISO 27001, den internationale ledelsesstandard for informationssikkerhed.

Et øjebliksbillede (Type 1)

- Denne erklæring handler om, hvordan jeres kontroller er udformet (designet) og implementeret. Som it-revisorer udfører vi en række handlinger, så vi kan udtale os med høj grad af sikkerhed om, hvorvidt jeres beskrivelse af ydelserne og kontroller i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er udformet hensigtsmæssigt.

Periodeerklæring (Type 2)

- Periodeerklæringen handler om jeres udformning (design), implementering og effektivitet af beskrevne kontroller i en specifik periode, typisk 12 måneder. Også her udfører vi som it-revisorer en række handlinger, så vi med høj grad af sikkerhed kan udtale os om, hvorvidt jeres beskrivelser af ydelser og kontroller er retvisende i alle væsentlige henseender. Vi efterprøver også, om kontrollerne er udformet hensigtsmæssigt, og om kontrollerne i alle væsentlige henseender har fungeret effektivt i perioden.



Hvem har brug for en it-revisorerklæring?

Når virksomheder og offentlige instanser sender opgaver i udbud - typisk outsourcing af it-ydelser og lignende – er der et stort fokus på, om leverandørerne kan dokumentere informationssikkerheden.

Desuden er der som følge af GDPR lovgivningen krav om indgåelse af databehandleraftale, hvis du som leverandør har med dine kunders persondata at gøre. Dataansvarlige skal føre tilsyn med sine databehandlere, og her fungerer erklæringerne som redskab for det årlige tilsyn.

Erklæringerne kan også bruges som et internt redskab for ledelsen til at få en status på virksomhedens styring af informationssikkerheden, og få et overblik over styrker og svagheder samt muligheder for forbedringer.

Hvad enten man er motiveret af den ene eller den anden årsag, så vil en erklæring alt andet lige kunne anvendes som et konkurrenceparameter, og under alle omstændigheder en kilde til mere kvalitet i styring af informationssikkerheden.

Hvordan kan en it-revisorerklæring styrke din virksomhed?

Udadtil

- Jeres kunder får uafhængig dokumentation for, at I passer godt på deres data.
- I signalerer, at I er en professionel virksomhed med fokus på kvalitet og sikkerhed.
- Erklæringen bygger på internationale standarder og gælder også jeres udenlandske aktiviteter.
- Med en it-revisorerklæring kan I skille jer ud fra konkurrenterne i fx udbud og markedsføring.

Indadtil

- Ledelse og medarbejdere får et skærpet fokus på og forståelse for it-informationssikkerhed og persondata.
- Jævnlige fornyelser af erklæringen sikrer, at der er fokus på tidssvarende processer.
- I får overblik over svagheder og afledte forbedringsmuligheder.
- It-revisionen er en oplagt lejlighed til at få professionel, faglig sparring om jeres informationssikkerhed.

Hvordan får man en it-revisorerklæring?

Det er med it-revision som med almindelig revision: Jo bedre styr I har på bilag og dokumentation, desto smidigere går revisionsprocessen.

Derfor er det vigtigt, at I har styr på it-politikker og procedurer for informationssikkerhed, og at udførelsen står højt på to-do-listen.

Når I første gang får udarbejdet en erklæring, kan der forud for erklæringsprocessen være en modningsfase. I har sikkert nogle fornuftige processer, men det er ikke sikkert, at de er skrevet ned eller at udførelsen er veldokumenteret. Her står vi klar til at guide jer på rette vej.

De følgende år kommer I hurtigere frem til erklæringsprocessen. Til gengæld er der her mere fokus på, at I kan bevise og dokumentere, at jeres processer og kontroller har fungeret i perioden. En stærk erklæring kræver derfor løbende fokus på styring af informationssikkerheden i løbet af året.

Erklæringsprocessen afrundes altid med en gennemgang af vores observationer, anbefalinger og kommentarer.



Sådan forløber processen i overordnede træk

AFKLARING

- Vi drøfter jeres behov og afklarer, hvilken type it-revisorerklæring(er) der passer til netop jeres virksomhed.

FORBEREDELSE

- Sammen med jer får vi overblik over materialerne. Hvad har I af relevante politikker, procedurebeskrivelser m.v., som vi kan læse og revidere? Og er der noget, der bør implementeres, inden vi går i gang med selve erklæringsarbejdet?

REVISION

- I revisionsprocessen gennemgår vi materiale og dokumentation for jeres kontroller og procedurer. I løbet af processen vil der være 2-4 audit møder, hvor vi gennemgår spørgsmål og requests. Møderne forgår enten fysisk hos jer eller digitalt.

ERKLÆRING

- Vi udsteder en erklæring, der beskriver de kontroller vi har testet for at kunne udtale os med høj grad af sikkerhed

TILSYN

- En it-revisorerklæring har altid en udløbsdato og skal derfor jævnligt fornyes. Som regel er det en gang om året. Vi aftaler, hvornår det passer jer bedst.

Selve erklæringsprocessen forløber typisk over 3-4 uger, afhængig af hvor mange ressourcer I kan stille til rådighed undervejs.

Høj kvalitet – effektiv proces – minimalt ressourcetræk

I inforevision trækker vi på viden og erfaring fra en bred vifte af brancher. Men vores udgangspunkt er altid virkeligheden i netop jeres virksomhed.

Vi står klar til at sparre med jer om mulighederne og om, hvordan vi bedst kan gribe opgaven an. Vores mål er at sikre høj kvalitet og en effektiv proces med et minimalt ressourcetræk hos jer som kunde.

Vil du vide mere om de forskellige erklæringstyper, hvad de kræver, og hvordan de kan løfte sikkerhed og kvalitet i virksomheden, så kontakt os for et uforpligtende sparringsmøde.

inforevision er et revisions- og konsulenthus med 140 medarbejdere. Vi betjener cirka 3100 mindre og mellemstore virksomheder inden for mange brancher, og vores ydelser omfatter revision og regnskab, skat og moms, internationale forhold, corporate finance, transaction services, erhvervsservice, it og interimydelser. inforevision er etableret i1986 og ligger i Søborg.

Kontakt



John Richardt Søbjærg er statsautoriseret revisor med indgående kendskab til mindre og mellemstore virksomheder i mange brancher. Han har mange års erfaring i at rådgive virksomheder og afgive revisorerklæringer.

John Richardt Søbjærg
Partner, statsautoriseret revisor
Tel. 24 21 15 71
Mail: jr@inforevision.dk



Simon Okkels er Certified Information Systems Auditor (CISA®) – en global certificering, der garanterer dyb viden om bl.a. audit-processer, afrapportering og compliance-procedurer inden for it-revision og it- og informationssikkerhed.

Simon Okkels
Partner, CIO, Certified Information Systems Auditor (CISA®)
Tel. 21 71 99 25
Mail: so@inforevision.dk