

ISO 27001 kan være grundlaget for din nye it-sikkerhedsstrategi



Men vær opmærksom på, at den øgede fleksibilitet ikke giver ratslø.

ISO 27001 og 2 giver mere fleksibilitet end DS 484, men stiller også nye krav. Har du helt styr på forskellen? Ellers læs videre her.

Hvad er egentlig forskellen?

DS 484 tager udgangspunkt i ISO standarden og er i sin opbygning identisk hermed. Man kan altså uden videre referere mellem de to. Men i DS 484 har man gjort en række af kravene obligatoriske.

ISO standarden er mere fleksibel, og du vælger selv, hvad der er relevant for jer. Til gengæld skal valg og fravalg begrundes og dokumenteres i en særlig erklæring.

Generelt vil erklæringen tage afsæt i:

- En risikovurdering
- Kontraktlige forpligtelser
- Lovbestemte krav
- Branchenormer/god skik.

INFO OM

Maj 2011

KONTAKT



Anders Ganer
Chefrevisor
Tlf. 24 29 50 38
aga@bdo.dk



Erik Sørup Andersen
Chefkonsulent
Tlf. 51 58 60 35
esa@bdo.dk

Et ISMS (Information Security Management System) er den organisatoriske struktur med tilhørende ansvarsfordeling, procedurer og metoder til at gennemføre risikovurdering, fastsætte mål, planlægge, gennemføre, overvåge og optimere - i en tilbagevendende cyklus

Denne publikation er skrevet i generelle vendinger og skal alene betragtes som generel vejledning. Publikationen dækker ikke specifikke situationer, og du bør ikke handle - eller undlade at handle - uden at have fået professionel rådgivning. Kontakt venligst BDO for at drøfte de specifikke problemstillinger. BDO, vores partnere og medarbejdere påtager os ikke ansvar for tab foranlediget af en handling, der er taget - eller ikke er taget - på grund af oplysningerne i denne publikation.

WWW.BDO.DK

Skifter I til den internationale standard, skal I beskrive et såkaldt ISMS.

Populært sagt er erklæringen sammen med ISMS'et din garanti mod "ratslør".

For at kunne udnytte fleksibiliteten kan en differentieret it-sikkerhedsstrategi være relevant. Skal forvaltningerne/direktørområderne have deres eget ISMS, eller skal it-sikkerhed styres centralt? Hvad skal gælde for skoler, biblioteker, kultursteder mv.?

ISO 27001 tvinger kommunen gennem en række overvejelser. Processen er ikke nødvendigvis nem, men kan være nyttig, og hvis I har oplevet det som en udfordring at implementere DS 484, kan et skift være anledningen til at starte på en frisk.

Hvad kan BDO hjælpe med?

Hvis I overvejer at skifte til ISO 27001/2, kan vi hjælpe med:

- at afklare, hvad et skift konkret betyder for jer
- at udarbejde en erklæring om anvendelse, og om nødvendigt hjælpe med at foretage risikovurderingen
- at beskrive et ISMS og tjekke, at jeres ISMS lever op til ISO 27001
- at udarbejde en gap analyse og en implementeringsplan.

Få mere at vide

I er altid velkomne til at kontakte os. Vi fortæller gerne om vores løsninger og fremlægger konkrete eksempler, der har hjulpet andre kommuner.



BDO Statsautoriseret revisionsaktieselskab og BDO Kommunernes Revision, Godkendt revisionsaktieselskab, begge danskejede revisions- og rådgivningsvirksomheder, er medlemmer af BDO International Limited - et UK-baseret selskab med begrænset hæftelse - og dele af det internationale BDO netværk bestående af uafhængige medlemsfirmaer. BDO er varemærke for både BDO netværket og for alle BDO medlemsfirmaerne. BDO i Danmark beskæftiger godt 1.100 medarbejdere, mens det verdensomspændende BDO netværk har over 46.000 medarbejdere i 115 lande.