

# IT-SIKKERHEDEFTERSYN

Baseret på ISO27000 og praktisk erfaring

## Hvordan sikrer jeg, at min organisations IT-sikkerhed er tilstrækkelig?

### HVORFOR ET IT-EFTERSYN?

Virksomheder og organisationer er afhængige af, at IT-systemerne virker. Altså, at man kan kommunikere og arbejde digitalt internt i organisationen og i cyberspace. At man gennem anvendelse af netværk, servere, printere, computere og applikationer mv. kan løse de opgaver, som gør at organisation fungerer. At det kan ske uforstyrret og sikkert, uden at andre kan misbruge ens data og systemer.

Spørgsmålet er, om IT-systemerne og den tilhørende organisation er robust og sikker nok, hvis der skulle ske et databas, kompromittering af data eller et systemnedbrud, enten ved et uheld eller tilsigtet. Dette vil et IT-sikkerhedseftersyn give svar på.

### FORMÅLET MED ET IT-EFTERSYN

Formålet med Search IT Consult IT-sikkerhedseftersyn er at afdække de områder som virksomheden skal fokusere på for at opnå en tilfredsstillende IT-sikkerhed. Samtidig bliver IT-sikkerheden sat i system gennem etablering af et information security management system (ISMS).

Desuden kan formålet være at forberede virksomheden på en egentlig ISO27000 certificering.

### HVAD ER ET IT-EFTERSYN?

Search IT Consult IT-sikkerhedseftersyn består af en gennemgang af virksomhedens IT-mæssige forhold, herunder organisering, politikker, regler, processer, adfærd mv. Dette med henblik på at afdække de områder, hvor organisationen bør foretage forbedringer.

IT-sikkerhedseftersynet giver forslag til forbedringer og opstiller en konkret handlingsplan, samtidig med at virksomheden får en række værktøjer til at opnå og vedligeholde IT-sikkerheden.

Efter aftale kan IT-sikkerhedseftersynet suppleres med en gennemgang af virksomhedens GDPR-forhold.

### SEARCH IT CONSULT IT-SIKKERHEDEFTERSYN KOMMER RUNDT OM ALLE DE VIGTIGE OMRÅDER



Fig. 1: Komponenter der er indeholdt i IT-sikkerhed

## HVORDAN GENNEMFØRES ET IT-SIKKERHEDSEFTERSYN?

Sikkerhedseftersynet indledes med en afdækning af organisationens overordnede rammer og nuværende IT-forhold. Der tages udgangspunkt i en ISMS-skabelon, der eksemplificerer en SMV-virksomhed med typiske IT-forhold, trusler og kontroller.

Herefter følger en gennemgang af de områder, der har særlig betydning for virksomhedens IT-sikkerhed, og for hvert område foretages en afdækning af omfang og tilstrækkelighed via en risikovurdering.

Der udarbejdes en analyse, der fremhæver de områder, hvor virksomheden afviger fra ISMS-skabelonens virksomhed, en såkaldt GAP analyse.

Sidste del af processen er en afklaring af, hvad organisationen bør gøre for at opnå, vedligeholde og bevare en tilfredsstillende IT-sikkerhed, et ISO27000 relateret ISMS-system.

## OMFANG

Sikkerhedseftersynets omfang og varighed vil være afhængig af organisationens størrelse og kompleksitet, men et standardforløb for en ikke for kompleks SVM-virksomhed vil kunne gennemføres inden for 50-60 konsulenttimer.

1.fase	2.fase	3.fase	4. fase	5.fase
Introduktion af proces og ISMS-skabelon	Introduktion af proces og ISMS-skabelon. Præsentation af parter	Search IT Consult analyserer resultat af interviewfasen	Search IT Consult udarbejder HANDLEPLAN	Kunde drøfter HANDLEPLAN internt
Kortlægning af virksomhedens IT-forhold	Detaljeret gennemgang af ISMS-skabelon, identifikation af GAPS. Eventuel GDPR-proces	Search IT Consult angiver en række prioriterede tiltag og kontroller, som lukker GAPS og giver det ønskede risikoniveau	Search IT Consult og kunde aftaler de sidste ændringer i HANDLEPLAN	Kunde beslutter, hvilket tiltag der skal implementeres af kunden, alternativt af Search IT eller tredjepart
Dialog om proces og omfang		Search IT Consult og kunde drøfter de foreslåede tiltag og lægger grundlaget for HANDLEPLANEN	Search IT Consult udarbejder endelig HANDLEPLAN	Kunde iværksætter tiltag i rammen af ISMS
Fremsendelse af tilbud			HANDLEPLAN forelægges for kundens beslutningstagere. ISMS etableres hos kunden. Handleplanens tiltag er udestående	
Accept af tilbud				

Fig. 2: Generisk tidsplan

	Search IT Consult
	Kunden og Search IT Consult
	Kunden

### **AFGRÆNSNING**

Den proces som Search IT Consult gennemfører med kunden, er ikke en ISO-certificering, men en proces der i praksis vedrører alle de elementer som ISO27000 omhandler, samt de elementer der evt. tilføjes som særlige områder af interesse i forbindelse med den enkelte virksomhed.

### **HVORDAN KOMMER JEG VIDERE?**

For yderlig information og vejledning:



Henning Søgaard  
+45 22 14 61 23  
hsn@searchitpeople.dk



Lars Bæhr  
+45 28 30 16 77  
lb@searchitconsult.dk