Henrik Gudme, Formand for DFK, skriver her i Magasinet Kvalitet omtaler af bøger, som skønnes at være relevante eller på anden vis være interessante for DFK-medlemmer. Du er velkommen til at foreslå bøger ved at skrive til DFKs sekretariat.

DET STORE ROVDYR – GDPR

Titel: Ledelsessystemer for informationssikkerhed i praksis
Undertitel: Gennemgang og fortolkning af kravene i DS/En ISO/IEC 27001:2017
Forfatter: Torben Abildgaard Pedersen
Sprog: Dansk
Forlag: Forlaget Dansk Standard
ISBN-978-87-7193-086-3
Sider: 233
Udgivet: 2018

Deadline den 25/5-18 er for længst passeret, og det nye store rovdyr, der sad i udkanten af skoven og hvæssede sine klør, er lusket ind mellem træerne og har fundet sig en god plads med fred og ro, og er faldet i dyb søvn. Sådan ser det i hver fald ud ved en hurtig helikoptertur hen over nyhedssites og sociale medier. Jeg har hørt tilsvarende fra nogen konsulenter, som havde "tusind" travlt op til den 25. maj, men som fra den ene dag til den anden har haft lige så tomme ordrebøger.

Denne bog fra DS har fokus på ISO 27001, den standard der dækker informationssikkerhed og som derfor også er relevant i forhold til GDPR. ISO 27001 er dog meget mere end lige GDPR.

Men er denne bog relevant, nu det store rovdyr har lagt sig? Ja, det mener jeg bestemt. Dels er jeg overbevist om, at selv om fokus på GDPR er landet på et leje noget under hvad det var, har det alligevel givet en opmærksomhed på hvor vigtigt det er, at vi passer på vores oplysninger, ikke kun de personfølsomme, men sandelig også på de forretningsfølsomme. Og her er ISO 27001 er rigtigt godt afsæt, præcis som ISO 9001 er det til kvalitetsarbejdet generelt.

Bogen er ligesom bogen fra DS om ISO9001 (tidligere omtalt), også delt i to (dog her i ét bind).

Begge dele er bygget op med farvekoder, sådan at det er meget hurtigt at afkode, hvor du skal læse afhængig af, hvad du søger.

Del 1 – Først, i blåt, standardens tekst punkt for punkt. Derefter følger et afsnit i grønt, nok det mest interessante, forfatterens forklaringer og fortolkninger af det berørte afsnit. Derefter, i lilla, bemærkninger og eksempler. Til sidst, i rødt, kommer forfatterens eksempler på hvordan et informationssikkerhedsledelsessystem kan bygges op.

Del 2 – er en gennemgang af det normative Anneks A. Igen anvendes de samme farvekoder. Blå for teksten i Anneks A, lilla for bemærkninger og eksempler og i rød, eksempel på dokumenter til et informationssikkerhedsledelsessystem. Her er den grønne del – forfatterens forklaringer og fortolkninger – udgået.

Både i del 1 og 2 er eksemplerne på dokumenter til et informationssikkerhedsledelsessystem meget fyldige og efter mit skøn meget anvendelige. For den, der for første gang står overfor at skulle indføre et certificerbart informationssikkerhedsledelsessystem i en virksomhed, er denne bog absolut prisen værd.

God læselyst
Henrik

”

EFTERLEVER VIRKSOMHEDEN ALLE RELEVANTE OG ANVENDELIGE CONTROLS, VIL ORGANISATIONEN VÆRE I STAND TIL AT FORSVARE SIG MOD ALLE IKKE BLOT TEKNOLOGBASEREDE RISICI, MEN OGSÅ MOD ANDRE MERE ALMINDELIGE TRUSLER, SÅSOM UFORSIGTIG ADFÆRD, FOR RINGE INFORMERET PERSONALE OG INEFFEKTIVE DRIFTSPROCEDURER.