Webinar ISO/IEC 27002 – kom på forkant med de nye sikkerhedsforanstaltninger

4. juni 2021

Spørgsmål fra chatten i relation til Dansk Standards oplæg:

Hvordan hænger temaerne sammen med SOA-dokumentet?
SoA-dokumentet skal opdateres til den nye struktur, når ISO/IEC 27001's Anneks A er blevet opdateret efter ISO/IEC 27002.

Hvordan hænger de valgte standarder på cybersecurity i den nye ISO 27002 sammen med CIS20 standarden?
CIS20 er en kondenseret, mere konkret og fortrinsvis teknisk rettet sæt af sikkerhedsforanstaltninger, hvis kobling til ISO/IEC 27002 kan findes i forskellige mapninger på nettet.

Hvornår forventes det at standarden kommer på dansk?
Forventet medio/ult. 2022

Er GDPR-relaterede foranstaltninger blevet indarbejdet i 27002 eller er der fortsat behov for 27701?
Der er ganske vist blevet tilføjet et par nye foranstaltninger, som må siges at have en stor rolle for privatlivsbeskyttelse (Data Deletion og Data Masking), men standardens fokus er stadig informationssikkerhed ift. forretningsmål og ikke privatlivsbeskyttelse ift. GDPR. ISO/IEC 27701 er langt mere omfattende og præcis i sit sæt af foranstaltninger til beskyttelse af privatlivet ved behandling af personoplysninger.

Hvad med GDPR (27701) bliver de en del af 27001/27002?
Nej. ISO/IEC 27701 bliver ikke en del af ISO/IEC 27001/27002. ISO/IEC 27701 bliver på et tidspunkt opdateret, så den er korrekt i sin privatlivsvejledning til ISO/IEC 27002.

Er det korrekt forstået at 27002 erstatter 27001, således at man på sigt ikke kan blive certificeret under 27001?
Nej, det er ikke korrekt. ISO/IEC 27001 er kravstandarden og ISO/IEC 27002 er en vejledende standard knyttet til anneks A i ISO/IEC 27001. ISO/IEC 27001 vil også fremover være den standard, man bliver certificeret efter.

Hvis man er i gang med at få ledelsen til at beslutte et SOA-dokument - hvad er så jeres anbefaling af proces i virksomheden?
Først og fremmest at få besluttet og defineret risikovilligheden for forretningen i ens organisation. Ledelsen skal, baseret på de fundne risici og deres risikoappetit, afgøre behovet for foranstaltninger i SoA-dokumentet. Dog vigtigt at understrege, at kvalificeringen af de forskellige foranstaltningers nødvendighed kræver teknisk indsigt fra forretningen og støttefunktioner. Ledelsen vil alt andet lige forholde sig til et udkast vedr. SoA-dokumentet og de tilhørende forretningsmæssige implikationer heraf. Går spørgsmålet på om man skal afvente den nye ISO/IEC 27002's udgivelse, er svaret nej: SoA-dokumentet følger jo opdateringen af ISO/IEC 27001 og her går der yderligere et år. Samtidig indeholder ISO/IEC 27002 jo en mapning til den gamle struktur, hvorved intet af det nuværende arbejde bliver forgæves.

Hvordan bliver risiko og risikoejer adresseret/behandlet i den reviderede udgave?
ISO/IEC 27002 beskæftiger sig med passende sikkerhedsforanstaltninger til håndtering af risici. Således er vejledning til risikostyring (ISO/IEC 27005) stedet at lære om risici og roller i forbindelse med risikostyring.

Kommer der en opdateret implementeringsguide til SOA dokumentet?
Man kan forvente, at der på sikkerdigital.dk vil tilgå en række opdateringer, der som i dag hjælper myndigheder og andre organisationer med at følge principperne i ISO/IEC 27000-serien. ISO/IEC 27003, som er en implementeringsvejledning til det samlede ledelsessystem efter ISO/IEC 27001, vil også blive opdateret. Her er SoA-dokumentet dog kun en af mange aktiviteter.