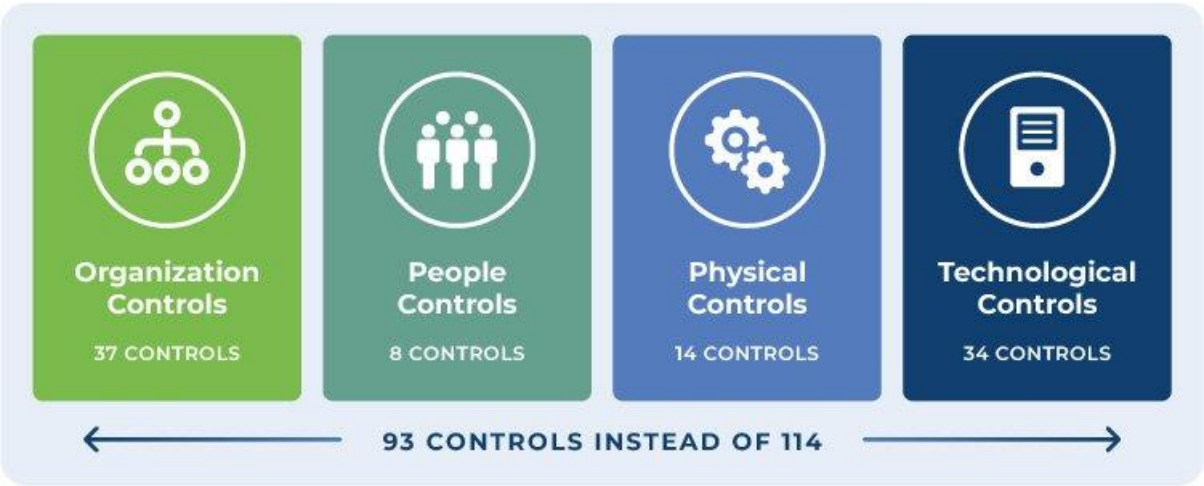
Što donosi revizija ISO 27002:2022?

ISO organizacija je 15.02.2022. godine objavila novo izdanje norme ISO 27002:2022 – Sigurnost informacija, cyber sigurnost i zaštita privatnosti - kontrole informacijske sigurnosti.

Ova norma nam daje smjernice kako ispuniti zahtjeve kontrola navedenih u Annexu A norme ISO 27001 koje su podijeljene u ukupno 14 grupa od A5 do A18.

Staro izdanje norme ISO 27002 je davalo smjernice kako ispuniti svaku od tih kontrola kroz 14 kategorija, a najveće promjene u novoj normi ISO 27002 je ta da ona grupira kontrole u 4 kategorije.

4 glavne kategorije su podijeljene obzirom na to prema čemu su kontrole usmjerene pa tako imamo organizacijske kontrole, kontrole ljudstva, fizičke i tehnološke kontrole.



Ukupan broj kontrola također se smanjio te ih sada imamo ukupno 21 manje u odnosu na prethodno izdanje. Obzirom da je u prethodnom izdanju norme dosta često bilo ponavljanja i redundancije 57 kontrola se spojilo u njih 24. Uvedeno je i potpuno novih 11 kontrola koje sada zaokružuju cijeli opseg kontrola informacijske i cyber sigurnosti.

S ciljem lakšeg shvaćanja uvodi se i element „svrhe“ pri opisu pojedinih kontrola u odnosu na prethodno izdanje gdje se za grupu kontrola definirao njihov cilj. Isto tako je uveden i pojam „atributi kontrolama“ kako bi se dodatno naglasio pristup procjene i tretiranja rizika. To će vam također omogućiti da stvorite različite poglede, tj. različite kategorizacije kontrola gledano iz različite perspektive u odnosu na teme kontrola.

ISO 27002:2022 ukupno ima 93 kontrole od kojih je 11 potpuno novih, 24 kontrola se spojilo (iz ukupno 57), 35 ostalo nepromijenjeno, a 23 kontrola su revidirane i nadopunjene kako bi se bolje prilagodile novom okruženju informacijske i cyber sigurnosti.

Uz glavne smjernice, norma ISO 27002:2022 ima i 2 aneksa; Annex A koji uključuje smjernice za primjenu atributa i Annex B koji povezuje kontrole s ISO 27001:2013.

Ono što se očekuje je da će sam Annex A norme ISO 27001:2013 doživjeti reviziju kroz dopunu koja bi trebala biti usklađena s novim ISO 27002:2022 što uključuje uvođenje novih 11 kontrola i reviziju postojećih.

Glavne prednosti koje nam je ovo novo izdanje dovelo je i smanjenje potrebe za dodatnim kontrolama koje su bile opisane kroz npr. ISO 27017 i ISO 27701. Smanjena je i redundancija te su sada logičnije grupirane kontrole jer se fokusiraju u samo 4 logičnije kategorije. Cyber sigurnost i zaštita privatnosti su sada predstavljene kroz nove i izmijenjene kontrole i u potpunosti zaokružuju priču o informacijskoj sigurnosti.

Osim pozitivnih strana nažalost suočeni smo i s time da nije paralelno izašla i nova norma ISO 27001 koja je i namijenjena za certifikaciju. To stvara brojne probleme jer će doći do

problema usklađivanja zahtjeva normi ISO 27001 i 27002 koja je sveobuhvatnija i daje širi pogled na informacijsku sigurnost. Srećom, norma ISO 27002 kroz Annex B povezuje kontrole opisane u ISO 27002:2022 s kontrolama u ISO 27001:2013 pa će to malo olakšati ovaj pomalo nelogičan redoslijed izdavanja smjernica prije promjene same norme sa zahtjevima.

Organizacije koje su usklađene i certificirane po normi ISO 27001:2013 će morati napraviti reviziju dokumentaciju i uskladiti se s novim zahtjevima tek kad službeno izađe novo izdanje norme ISO 27001 ili vjerojatnije samo dopuna Annexa A, a do tada je preporuka da se postojeći sustav nadogradi s novim i izmijenjenim kontrolama kako bi se podigao na višu razinu informacijske sigurnosti posebno u ovim nepredvidivim trenucima kojima svakodnevno svjedočimo.

Luka Kedmenec, Lead Auditor

email: luka.kedmenec@hr.urscertification.com

mob: 099/326-8121