ISO 27001:2013 - Sertifikat Sistema menadžmenta bezbednošću informacija

Uvod

Ovaj međunarodni standard pripremljen je da pruži zahteve za uspostavljanje, primenu, održavanje i kontinuirano unapređivanje sistema upravljanja informacionom sigurnošću. Usvajanje sistema upravljanja informacionom sigurnošću je strateška odluka za organizaciju. Na uspostavljanje i primenu sistema upravljanja informacionom sigurnošću organizacije utiču potrebe i ciljevi organizacije, zahtevi za bezbednošću, korišćeni organizacioni procesi i veličina i struktura organizacije. Očekuje se da će se svi ovi faktori uticaja vremenom promeniti.

Sistem upravljanja informacionom sigurnošću čuva poverljivost, integritet i dostupnost informacija primenom procesa upravljanja rizicima i daje poverenje zainteresovanim stranama da se rizicima adekvatno upravlja.

Važno je da je sistem upravljanja informacionom sigurnošću deo i integrisan sa procesima organizacije i celokupnom upravljačkom strukturom i da se informaciona sigurnost uzima u obzir pri dizajniranju procesa, informacionih sistema i kontrola. Očekuje se da će primena sistema upravljanja informacionom sigurnošću biti skalirana u skladu sa potrebama organizacije.

Ovaj međunarodni standard mogu koristiti unutrašnje i spoljne strane za procenu sposobnosti organizacije da ispuni sopstvene zahteve za informacionom sigurnošću.

Redosled kojim su zahtevi predstavljeni u ovom međunarodnom standardu ne odražava njihov značaj niti podrazumeva redosled kojim se oni moraju primeniti. Stavke na spisku nabrojane su samo u svrhu referenci.

ISO / IEC 27000 opisuje pregled i rečnik sistema za upravljanje informacionom sigurnošću, pozivajući se na porodicu standarda sistema upravljanja informacionom sigurnošću (uključujući ISO / IEC 27003 [2] , ISO / IEC 27004 [3] i ISO / IEC 27005 [4]), sa srodnim terminima i definicijama.

Primena

Ovaj međunarodni standard precizira zahteve za uspostavljanje, primenu, održavanje i kontinuirano unapređivanje sistema upravljanja informacionom sigurnošću u kontekstu organizacije. Ovaj međunarodni standard takođe uključuje zahteve za procenu i tretman rizika od informacione bezbednosti prilagođene potrebama organizacije. Zahtevi navedeni u ovom međunarodnom standardu su generički i namenjeni su primeni u svim organizacijama, bez obzira na vrstu, veličinu ili prirodu. Izuzimanje bilo kog zahteva navedenog u članovima 4 do 10 nije prihvatljivo kada organizacija tvrdi da je u skladu sa ovim međunarodnim standardom.