

Sistem menadžmenta bezbednošću informacija

Značaj bezbednosti informacija

Usled sve veće zavisnosti od informacionih tehnologija, otvorenosti organizacija i porasta značaja informacija u modernom poslovanju, kreirani su standardi ISO/IEC 27001 i ISO/IEC 27002 za menadžment bezbednošću informacija, sa željom da se uredi i standardizuje oblast bezbednosti informacija u organizacijama.

Standardi predstavljaju upravljačke alate koji su nezavisni od pojedinačnih tehnoloških rešenja i nude sveobuhvatan pregled bezbednosti informacija tokom poslovanja organizacije. Ocenjivanje rizika u vezi sa informacijama je osnova za uspostavljanje sistema menadžmenta bezbednošću informacija i predstavlja njegovu osnovnu karakteristiku.

Standard ISO/IEC 27002 nudi niz mera za kontrolu identifikovanih rizika, a koje su se tokom godina korišćenja u različitim organizacijama širom sveta pokazali kao primeri dobre prakse. U 14 poglavlja je opisano 113 kontrola koje su namenjene ostvarivanju 35 različitih ciljeva.

Standard ISO/IEC 27001 je napisan u formi zahteva koje mora da ispuni organizacija ukoliko želi da dobije sertifikat. Poglavlja 4, 5, 6, 7 i 8 morate da razmotrite bez ikakvih isključenja i u potpunosti. Pored pomenutih poglavlja, standard sadrži i prilog A koji predstavlja rezime 113 kontrola iz standarda ISO/IEC 27002. Za svaku kontrolu koja je isključena je potrebno da se navede razlog za isključenje.

Standardi su sveobuhvatni u smislu bezbednosti informacija. To znači da ne uzimaju u obzir samo informacione tehnologije i informacije u elektronskom obliku, već i informacije u svim mogućim oblicima i na svim medijima. U tom smislu, mnoge od opisanih kontrola su u potpunosti organizacione prirode i nisu povezane sa tehnologijom (npr. klasifikacija informacija, politika praznog stola, fizičko obezbeđenje objekata ili opis bezbednosti informacija u ugovorima o zapošljavanju).

Zašto dobiti sertifikat?

Poslovne koristi:

- identifikacija i smanjenje bezbedonosnih rizika na željeni nivo,
- poboljšavanje poslovnih partnerstava (veća poverljivost međusobno razmenjenih informacija),
- investiranje u prava (akutna) mesta,
- konkurentska prednost prilikom sklapanja poslovnih partnerstava,
- uređeno upravljanje procesima u vezi sa bezbednošću informacija.

ISO/IEC 27001

Postupak sertifikacije

Postupak sertifikacije obuhvata pregled dokumenata i sertifikacionu proveru, koja se sastoji iz dva dela. U prvom delu se fokusiramo na uspostavljenost i dokumentovanost sistema menadžmenta bezbednošću informacija. Tokom provere sprovodimo pregled:

- politike i ciljeva bezbednosti,
- predmeta i područja sertifikacije, pratećih procedura i kontrola,
- izveštaja o proceni rizika,
- izjave o primenljivosti (eng. "Statement of applicability") itd.

U drugom delu je akcenat na primeni i efikasnosti sistema menadžmenta bezbednošću informacija, ispunjavanju zahteva standarda ISO/IEC 27001, zakonskih zahteva i zahteva zainteresovanih strana.

Nakon dodele sertifikata, nadzornim proverama pojedinih delova sistema se jednom godišnje proverava da li vaša organizacija i dalje ispunjava propisane zahteve. Sertifikat važi tri godine.

Usluge iz oblasti bezbednosti informacija:

- proveravanje i sertifikacija,
- predprovera,
- ocena stanja,
- ocena stanja kod vaših isporučilaca.

Saradnja sa organizacijom tokom postupka sertifikacije

Organizacija koja je u postupku proveravanja dobija:

- stručna pojašnjenja i odgovore u vezi sa zahtevima standarda i postupkom sertifikacije,
- potvrdu (ako je potrebno) da je organizacija u postupku sertifikacije ili postupku procene stanja.
- 10% popusta za seminare i kurseve koje izvodi SIQ.

Zašto SIQ?

Proveravanje i sertifikaciju sistema menadžmenta bezbednošću informacija prema tehničkoj specifikaciji ISO/IEC 27001 mogu da sprovode samo akreditovana sertifikaciona tela.

Naša stručnost je potvrđena saradnjom sa sertifikacionim telom CIS-Certification & Information Security Services iz Beča, sa kojom zajedno izdajemo akreditovan sertifikat za sistem menadžmenta bezbednošću informacija.

Informacije: SIQ d.o.o. Beograd

Cara Dušana 266
11080 Beograd - Zemun
Srbija
Tel: + 381 11 316 21 62
Faks: + 381 11 261 52 33
E-pošta: siq.beograd@siq.si
www.siq.rs