CERTIFIKÁCIA PODĽA ISO 27001

Produktový list

PRÍPRAVA ZÁKAZNÍKA NA CERTIFIKÁCIU PODĽA STN ISO/IEC 27001

S prehlbujúcou sa informatizáciou spoločnosti sú v organizáciách zavádzané zložité informačné systémy. Ak informačné systémy obsahujú aj informácie iných právnických respektíve fyzických osôb je potrebné o bezpečnosti systémov uistiť aj zákazníkov.

Zavedením systému manažérstva informačnej bezpečnosti (SMIB) spoločnosť preukazuje dôveryhodnosť všetkým dotknutým stranám organizácie, že so získanými informáciami a údajmi narába obozretne, spravuje ich v zmysle zadefinovaných bezpečnostných pravidiel a zvláda riziká spojené s hrozbami, ktoré sú identifikované v procesoch.

Tiež sa zavedením SMIB implicitne deklaruje súlad s legislatívnymi požiadavky na informačnú bezpečnosť (napríklad zákon č. 122/2013 Z.z. o ochrane osobných údajov). Zavedenie systému je výhodné z pohľadu presvedčenia vedenia spoločnosti o existencii interných procesov na zvládanie rizík informačnej bezpečnosti.

Najvhodnejší spôsob ako to dokázať pre zákazníka alebo pre komunitu, ktorej údaje spravujeme, je certifikácia na SMIB.

Úloha manažmentu

Pre zavedenie SMIB je v prvom rade potrebné, aby o tomto kroku bol presvedčený vrcholový manažment.

Manažment si musí byť vedomý potrebných organizačných, personálnych a technických opatrení, ktoré je potrebné splniť, aby bol systém úspešne implementovaný. Okrem toho musí sám zabezpečiť vyžadovanie plnenia požiadaviek SMIB a aj sám tieto požiadavky dodržiavať.

KOŠICE
Gavlovičova 9
040 17 Košice
T: +421 55 727 17 17
E: lynx@lynx.sk

BRATISLAVA
Jelačičova 8A
821 08 Bratislava
T: +421 2 501 065 11
E: lynxba@lynx.sk

SMIB ako modelové riešenie

SMIB vo svojej podstate poskytuje celistvý model upravujúci hodnotenie rizík, návrh a zavedenie bezpečnosti informácií, riadenie bezpečnosti informácií a opätovné hodnotenie bezpečnosti informácií na neustále zlepšovanie informačnej bezpečnosti.

Štandard je zostavený tak, že dokáže pokryť potreby ľubovoľného typu organizácie, od súkromných spoločností až po štátne inštitúcie. Podstatou štandardu je cyklický model neustáleho zlepšovania, z histórie najčastejšie používaný model PDCA (Plan-Do-Check-Act) – Plánuj-Vykonaj-Kontroluj-Prevádzkuj, ktorého cieľom je vytváranie, budovanie, monitorovanie a neustále zlepšovanie SMIB v rámci organizácie.

Cyklus zlepšovania je vhodné nastaviť na obdobie jedného roka a tým prispôsobiť termíny systému auditov požadovaných certifikačnou spoločnosťou. Samotná certifikácia zavedeného systému vyžaduje každoročne vykonávať externý audit. Prvý je certifikačný audit, nasledujúce dva roky kontrolné audity a po nich opäť recertifikačný audit a potom ďalšie dva kontrolné audity.

Zavedenie SMIB

Zavedenie SMIB je vhodné načasovať po implementácii ISO 9001, prípadne súčasne s ním a zaviesť takzvaný integrovaný systém manažérstva.

Takouto postupnosťou implementácií sa zjednoduší zavedenie SMIB vzhľadom na opísané procesy riadenia manažérstva kvality a ich využitie pri implementácii SMIB.