

# ISO 27001 – vlastnosti a prínosy

Organizácie sa čoraz častejšie zaoberajú návrhom, realizáciou a certifikáciou systémov riadenia informačnej bezpečnosti (ISMS – Information security management system). ISO 27001 sa v súčasnosti pokladá za najdôležitejšiu a najspoľahlivejšiu normu pre tieto systémy. Obsahuje špecifikáciu požiadaviek na informačnú bezpečnosť, ktoré musí certifikovaná organizácia spĺňať. Každá organizácia, usilujúca o rast a posilnenie pozície na trhu, by takýto certifikát mala získať.



**Peter Manda**  
Nezávislý IT konzultant

[peter.manda@fidecon.sk](mailto:peter.manda@fidecon.sk)

## ČO JE ISO 27001?

Norma ISO 27001 sa pokladá za primárnu normu z rodiny ISO 27000. Vychádza z pôvodného štandardu platného vo Veľkej Británii pod označením BS 7799-2 a po mnohých certifikovaných revíziách a úpravách ju v roku 2005 publiko-

vali pod názvom ISO/IEC 27001:2005. Predstavuje štandard informačnej bezpečnosti, oproti ktorému môže byť systém riadenia informačnej bezpečnosti auditovaný a certifikovaný. Je zosúladená s ostatnými systémami riadenia ako napr. ISO 9001 a ISO 14001.

V prílohe normy je popísaných jedenásť radiácií oblastí (control sections), medzi ktoré patrí organizácia informačnej bezpečnosti, manažment aktív, bezpečnosť ľudských zdrojov, riadenie prístupov, obstarávanie informačných systémov, ich rozvoj a údržba, a ďalšie.

### VLASTNOSTI NORMY

Hlavným cieľom zavedenia ISO 27001 je podpora pri návrhu, zavedení a manažmente efektívneho systému riadenia informačnej bezpečnosti. Cieľom tohto systému

### PRÍNOSY ZAVEDENIA ISO 27001

Kvantifikovať prínosy zavedenia ISO 27001, rovnako ako pri mnohých iných investíciách do IT, nie je jednoduché. Napriek tomu organizácie, ktoré majú túto normu zavedenú, môžu preukázať prínosy v nasledujúcich oblastiach:

- Zvýšená spoľahlivosť a bezpečnosť informačných systémov. Využívanie nezávislého medzinárodného štandardu vytvára predpoklad na aplikovanie primeraných a efektívnych postupov v oblasti bezpečnosti a stability systémov.

## Hlavným cieľom zavedenia ISO 27001 je podpora pri návrhu, zavedení a manažmente efektívneho systému riadenia informačnej bezpečnosti.

je ochrana informácií, ktoré organizácia má, pred ľubovoľným rizikom. Taktiež pomáha pri dodržiavaní etických princípov pri manipulovaní s informáciami, napr. s osobnými údajmi zákazníkov a pod.

Norma bola vyvinutá tak, aby spĺňala požiadavky na informačnú bezpečnosť organizácií všetkých typov a veľkostí. Je dôležité vedieť, že pokrýva všetky typy informácií (elektronických aj papierových) a preto nie je limitovaná technológiami. Štandard neobsahuje zoznam krokov, po ktorých realizácii bude mať organizácia systémy zabezpečené. Poskytuje však metodiku na realizáciu špecifického posúdenia rizík v organizácii a definíciu bezpečnostných cieľov.

Podobne ako v prípade iných ISO noriem, má aj ISO 27001 zakomponovaný cyklický PDCA model (plan-do-check-act). Cieľom je vytvoriť a prevádzkovať ISMS v súlade s pravidlami informačnej bezpečnosti a v prípade zmien zabezpečiť jeho aktualizáciu. Cyklický PDCA model je jedným z kľúčových nástrojov poskytnutých štandardom ISO 27001 na priebežnú aktualizáciu rizík a bezpečnostných cieľov vyplývajúcich z neustále sa meniacich podmienok v informačnej bezpečnosti.

- Nárast zisku. Navyše štandardným prístupom v oblasti bezpečnosti informačných systémov organizácia demonštruje navonok pre svojich obchodných partnerov spoľahlivosť pri manipulovaní s obchodnými, prípadne osobnými informáciami. Takto môže organizácia zlepšiť svoju schopnosť udržiavať si existujúcich zákazníkov a získavať nových.

- Splnenie legislatívnych a odvetvovo-špecifických požiadaviek. Zavedenie ISMS a jeho certifikácia môže podstatným spôsobom zjednodušiť splnenie súčasných, ale aj pripravovaných legislatívnych a odvetvovo-špecifických požiadaviek. Táto oblasť sa dostáva do pozornosti vo viacerých odvetviach, ktoré pracujú s osobnými údajmi svojich zákazníkov, ako napr. finančný sektor, sektor verejných služieb alebo verejnej správy.

- Kvalitnejší interný manažment. Znalosť toho, čo a ako má byť spravované a aké informácie majú byť zabezpečené, zvyšuje úroveň riadenia informačných zdrojov v organizácii. Certifikácia ISO 27001 napomáha aj zosúladiť biznis a IT cieľov, nakoľko do prípravy býva zapojený biznis aj IT manažment.

V hlavnej časti normy sú uvedené povinné časti ISMS, najmä oblasť posúdenia rizík. Posúdenie rizík (risk assessment) a z neho vyplývajúca definícia jednotlivých bezpečnostných cieľov, je podstatnou časťou tohto štandardu.