

ISMS

Pomůžeme vám rychle a efektivně navrhnout a zavést systém řízení bezpečnosti informací (ISMS) i ICT napříč celou vaší organizací.

Zavedení **Information Security Management System** (ISMS) zahrnuje mj. definici chráněných informačních aktiv, **řízení bezpečnostních rizik** a zavedení a kontrolu bezpečnostních opatření. Máme dlouhodobé praktické zkušenosti s jeho nasazením do nejrůznějších prostředí.

ISMS je definováno normou např. ISO/IEC 27001 (resp. celou rodinou norem ISO/IEC 2700x), která je plně kompatibilní se systémy managementu jakosti (ISO/IEC 9001), systémy environmentálního

managementu (ISO/IEC 14001) nebo systémy bezpečnosti a ochrany zdraví při práci (OHSAS 18001), (ISO/IEC 9001). ISMS tedy lze jednoduše integrovat do celkového systému řízení organizace.

Naši specialisté vám **pomohou ve všech oblastech ISMS.**

Díky svým praktickým zkušenostem, které jsou kromě referencí z realizovaných projektů doloženy i vlastní **certifikací dle ISO/IEC 27001**, jsme schopni maximálně zohlednit specifika konkrétní organizace a komplexně implementovat její bezpečnostní procesy.



Co nabízíme?

Podporu zavedení ISMS v organizaci

Komplexní pomoc při budování ISMS včetně definice rozsahu systému, zpracování analýzy rizik, návrhu procesu řízení rizik, definice bezpečnostních opatření, zpracování bezpečnostní politiky a další bezpečnostní dokumentace, školení uživatelů, provedení interního auditu ISMS, případně dalších činností až po podporu ve fázi certifikace ISMS. Veškeré uvedené činnosti můžeme realizovat na klíč nebo formou konzultací či revizí výstupů.

Implementaci procesů ISMS

Konzultační podpora při návrhu a zavádění fragmentů (procesů) ISMS, jejich redesignu, optimalizaci apod.

Bezpečnostní dokumentaci

Návrh struktury a vypracování bezpečnostní dokumentace včetně bezpečnostní politiky, bezpečnostních směrnic, uživatelských a administrátorských příruček apod.

Audity řízení bezpečnosti

Realizace interních auditů ISMS, srovnávacích auditů vůči normě ISO/IEC 27002, procesních auditů ISMS anebo dílčích auditů zvolených oblastí ISMS, procesů apod.

Externí bezpečnostní správce

Specializovaný soubor služeb na podporu procesů řízení informační bezpečnosti organizace. Naši konzultanti a specialisté „externě“ pokrývají široké spektrum činností v rámci „údržby“ informační bezpečnosti, které organizace není schopna nebo nechce pokrývat vlastním personálem. V praxi se může jednat o přípravu a aktualizaci bezpečnostní dokumentace, školení uživatelů, vyšetření a vyhodnocení bezpečnostních incidentů, periodické technické prověrky bezpečnosti atd.

Další služby na klíč

Jsme schopni pokrýt také individuální požadavky zákazníků v oblasti ISMS i v souvisejících oblastech bezpečnosti informačních technologií.

Přínosy

- Stanovení optimálního poměru mezi náklady a dosaženou úrovní zabezpečení informačních aktiv organizace - maximální efektivita a přesné zacílení investic do bezpečnosti.
- Zvýšení důvěryhodnosti a kreditu organizace v očích zákazníků a partnerů.
- Zajištění souladu s požadavky legislativy.
- Snížení rizik souvisejících s nedostupností informací a služeb, únikem nebo neoprávněným přístupem k informacím organizace.
- Úspora nákladů souvisejících s odstraňováním následků bezpečnostních incidentů.
- Minimalizace nebezpečí úniku dat a ochrana stability organizace.
- Zvýšení bezpečnostního povědomí zaměstnanců - snížení chybovosti uživatelů.
- Průběžné sledování a hodnocení aktuální úrovně informační bezpečnosti organizace.

Náš přístup k ISMS

K problematice ISMS přistupujeme ze strany informačních technologií - **naším cílem není „jen zavést“ ISMS dle ISO norem, ale klademe důraz rovněž na konkrétní technologie a procesy IT** a jejich soulad s obchodními procesy a reálnými potřebami zabezpečení organizace.

Bezpečnost informačního systému řešíme tak, aby rizika byla prostřednictvím vhodně nastavených procesů řízena - **rizika musíme identifikovat, stanovit jejich dopad s ohledem na hodnotu aktiv a definovat vhodná protipatření**. Takové řešení pak zajistí efektivní eliminaci významné části rizik ještě před jejich reálným výskytem.