ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

ISMS – Systém řízení bezpečnosti informací

ISMS, založený na mezinárodních normách ISO/IEC 27001 a ISO/IEC 27002, představuje **osvědčený způsob,** jak zajistit a řídit bezpečnost informací a integrovat ji do stávajícího systému řízení organizace.

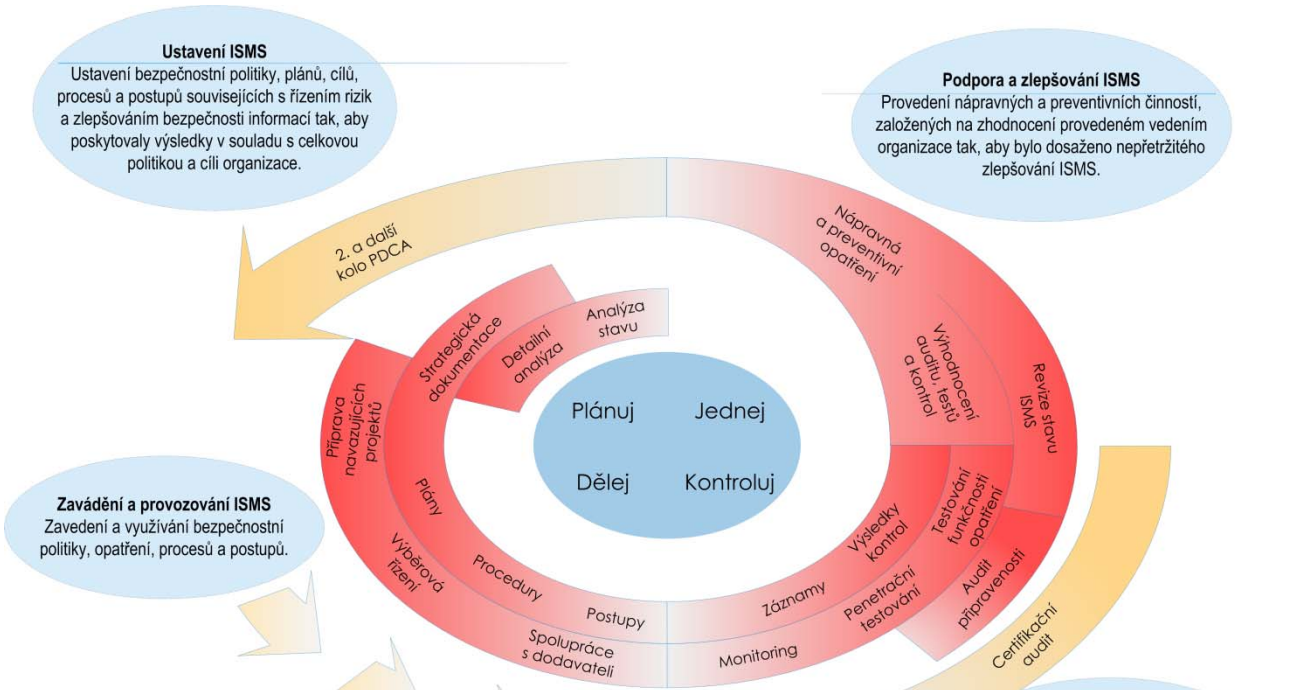
Cílem ISMS je **aktivně řídit rizika**, která pro organizaci vyplývají z využití informačních systémů a technologií a ze závislosti procesů na informacích.

Analogicky k ISO 9001 a systémům řízení kvality, je možné ISMS **certifikovat**, a to jak samostatně, tak v rámci integrovaného systému řízení. Certifikát, ověřený nezávislou autoritou, hraje roli prvku **důvěry** s partnery a zákazníky a vytváří konkurenční výhodu.

ISMS, postavený na normách ISO/IEC 27001 a ISO/IEC 27002, je **plně kompatibilní** s řízením kvality dle ISO 9001, systémem environmentálního managementu dle ISO 14001, směrnicemi OECD a je, jakožto jediný a ucelený popis bezpečnosti informací, významným tvůrcem požadavků a vztahů na evropské úrovni. Nadto, je-li rozumně zaveden, je ryze praktický a přispívá k efektivitě prostředků vynaložených na bezpečnost.

Charakteristika ISMS

- ***Prosazuje procesní přístup na základě Demingova cyklu Plánuj – Dělej - Kontroluj – Jednej***
- ***Je kompatibilní s ISO 9001, ISO 14001 a umožňuje integraci a sdílení společných zdrojů, principů a nástrojů (např. řízené dokumentace) a tím snížení nákladů na zavedení a provoz***
- ***Je součástí celkového systému řízení, která akcentuje důležitost ochrany informací, jakožto cenného aktiva organizace***
- ***Zahrnuje know-how – ověřenou nejlepší praxi bezpečnosti informací***



PDCA model ISMS

Model známý jako "**Plánuj-Dělej-Kontroluj-Jednej**" (Plan-Do-Check-Act nebo PDCA) je aplikován na všechny procesy ISMS tak, jak jsou zavedeny normou ISO/IEC 27001. **ISMS** je část celkového systému řízení organizace, založená na přístupu (organizace) k provozním rizikům, která je zaměřena na vybudování, zavádění, provoz, monitorování, přehodnocování, údržbu a zlepšování bezpečnosti informací.

ISMS „NA KLÍČ“ – ZAVEDENÍ A ZVYŠOVÁNÍ ISMS S MOŽNOSTÍ CERTIFIKACE

Přínosy ISMS

- Efektivní řízení rizik bezpečnosti informací
- Výrazné zvýšení efektivity investic vynakládaných na zajištění požadované míry bezpečnosti informací na základě znalosti rizik
- Integrace cílů a požadavků organizace s nároky na bezpečnost – bezpečnost z pohledu businessu
- Konkurenční výhoda – možnost prokazatelnosti úrovně bezpečnosti - „Ticket for business“
- Zvýšení důvěryhodnosti organizace pro partnery a zákazníky, ochrana pověsti a zavedené značky organizace
- Prokázání souladu s legislativou - např. ochranou osobních údajů
- Systémový přístup k problematice řízení bezpečnosti informací, její neustálé zlepšování a zlepšování fungování řídících procesů v rámci organizace
- Zvýšení bezpečnostního povědomí napříč organizací, nejen mezi technickými pracovníky
- Efektivní zvládání bezpečnostních incidentů
- Připravenost na mimořádné události díky plánování kontinuity činností

RAC - ISMS „na klíč“

- Analýza současného stavu a prostředí organizace
- Návrh rozsahu a Politiky ISMS
- Návrh organizace bezpečnosti, stanovení rolí a odpovědností
- Návrh systémové struktury dokumentace
- Provedení analýzy a vyhodnocení rizik
- Provedení výběru opatření
- Návrh Prohlášení o aplikovatelnosti
- Dokumentace „na klíč“
- Zpracování plánů implementace opatření
- Školení pracovníků organizace, manažera bezpečnosti a auditorů
- Postupy zvládání bezpečnostních incidentů
- Návrh a zavedení procesu plánování kontinuity činností organizace
- Nastavení procesu měření účinnosti ISMS
- Příprava přezkoumání ISMS managementem
- Podpora interních auditů ISMS včetně návrhu nápravných a preventivních opatření

RAC kompetence

- Pracovníci s rozsáhlými praktickými zkušenostmi a profesními certifikacemi
- Referenční projekty zahrnující mj. také první certifikaci ISMS v ČR
- Překlady norem ISO/IEC 27002 a ISO/IEC 27001, přijaty jako ČSN
- Metodika CRAMM pro analýzu rizik a současně schopnost využití různých metodik
- Zavedený integrovaný systém řízení (IMS), zahrnující řízení kvality podle ISO 9001:2008 a řízení bezpečnosti podle ISO 27001:2005, certifikovaný společností DNV pod britskou akreditací UKAS
- Pracovníci RAC a celá společnost je prověřena Národním bezpečnostním úřadem

Risk Analysis Consultants, s. r.o.
Španělská 2
120 00 Praha 2
Česká republika
+420 221 628 400
rac@rac.cz
www.rac.cz

Risk Analysis Consultants je nezávislá poradenská společnost poskytující služby a řešení ve všech oblastech bezpečnosti informací v souladu s mezinárodními normami, související národní legislativou a respektováním individuálních podmínek klientů. Od roku 1995 pomáhá zajišťovat bezpečnost informací v informačních systémech organizací státní správy, bank, finančních institucí, telekomunikačních společností a průmyslových podniků v České republice i v zahraničí.

QR kód RAC

V100521

© 2010 Risk Analysis Consultants