

# System managementu bezpečnosti informací dle ISO 27001



A1Q, S.R.O.  
ING. RICHARD MIKULČÍK

**A1**  
**Q**

A1Q, s.r.o.  
jednoduchá a poctivá řešení



## Naše poslání

- ❖ neustále nabízet jednoduchá a poctivá řešení
- ❖ šířit dobou náladu.

# A1Q, s.r.o. se specializuje



- ISO 9001 Systémy managementu kvality
- ISO 14001 Systémy environmentálního managementu
- OHSAS 18001 Systém managementu bezpečnosti a ochrany zdraví při práci
- ISO/IEC 27001 Systém managementu bezpečnosti informací
- TS 16949 zvláštní požadavky používání ISO 9001 v organizacích zajišťujících výrobu dílů v automobilovém průmyslu.

# Hlavní důvody proč ISO 27001 zavádět



- Zákazník
- Vlastní firma - organizace
- Zákon

## Další důvody proč ISO 27001 zavádět



- Certifikát zlepšuje pozitivní pohled na organizaci
- Ochrana dat znamená ochranu investic
- Provedení analýzy bezpečnostních rizik
- Míň než polovina krádeží dat není způsobena zvenčí firmy

## Další důvody proč ISO 27001 zavádět



- Riziko porušení zákonných povinností a s tím spojené sankce
- Velká část ztráty dat je způsobena neznalostí základních bezpečnostních pravidel
- Únik, ztráta nebo jiné zneužití informací, může znamenat velkou diskreditaci firmy

# Přínosy



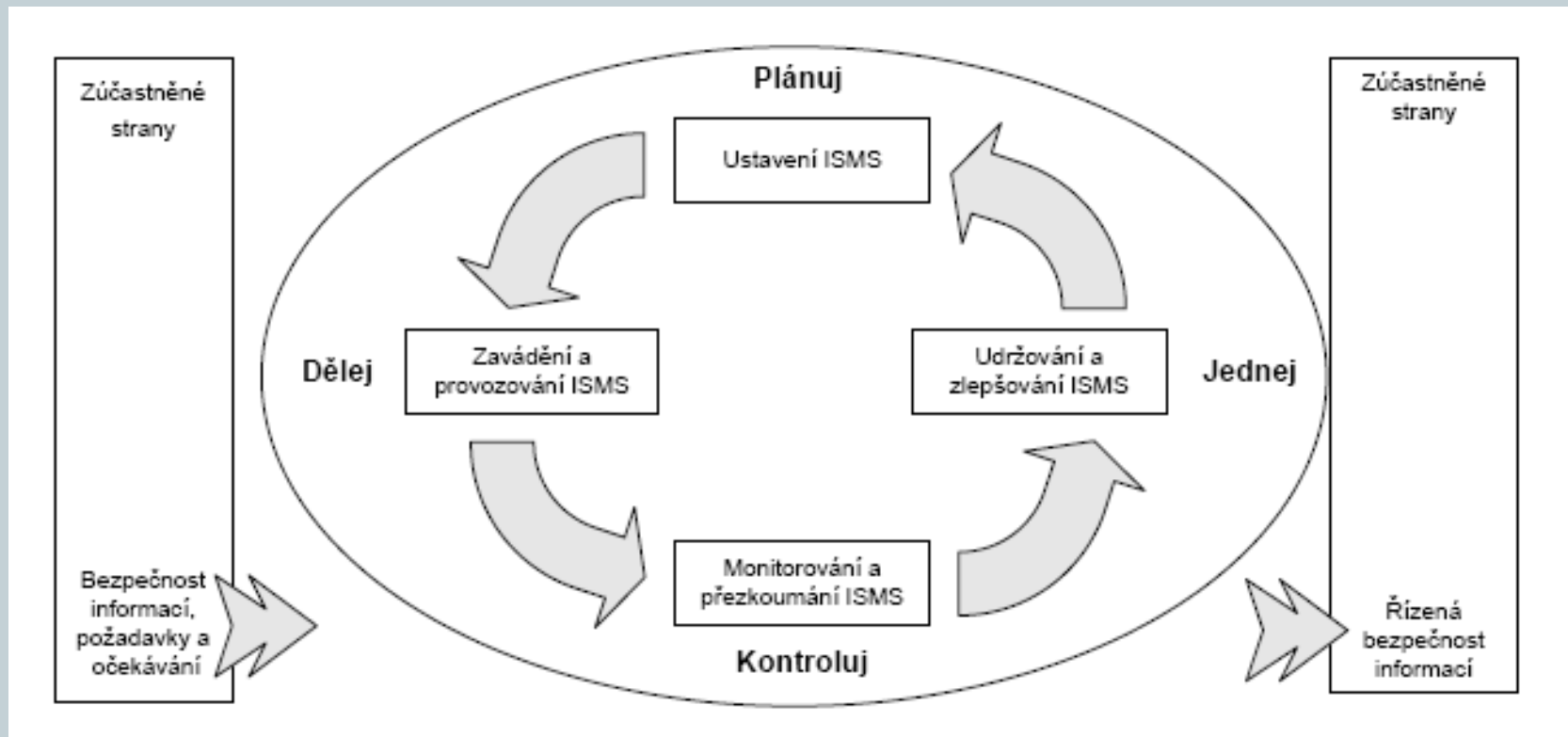
- Prestiž
- Prevence před nechtěnou medializací
- Prevence před postihy ze zákona
- Výběrová řízení tam kde je certifikát požadován
- Definice pravomocí a odpovědností pracovníků

# Iso normy – normy se špatnou pověstí



- papírování
- investice
- ztráta času
- stojí to moc peněz

# PDCA



# Plánuj



- Politika ISMS
- Cíle ISMS
- Rozsah ISMS
  
- ANALÝZA

# Dělej



- Zavedení dokumentovaných postupů
- Instruktaž personálu
- Záznam skutečných stavů

# Kontroluj



- Interní audity
- Externí audity
- Přezkoumání
- Vyhodnocení nežádoucích stavů
- Kontrola shody s požadavky

# Jednej



- Nápravná opatření
- Preventivní opatření
- Změny dokumentovaných postupů
- Školení personálu
- Neustálé zlepšování

# Co musí být definováno



- Politika ISMS
- Cíle ISMS
- Registr Aktiv
- Registr rizik a plán zvládnání rizik
- Prohlášení o aplikovatelnosti
- Role a odpovědnosti pracovníků
- Záznamy

# Výsledek zavedeného ISMS



- Dostupnost
- Integrita
- Důvěryhodnost

# Nesprávná aplikace ISMS



- Bezpečnost pouze IT
- Zodpovědnost pouze IT manažera
- Zabezpečení pouze elektronických dat

# Kdo ISMS zavádí a praktikuje



- Zdravotnické a farmaceutické organizace
- Státní organizace
- Softwarové firmy
- Energetické firmy
- Stavební firmy

# Jak to probíhá



- Zavádění ISMS
- IA
- CA I. Stupně
- CA II. Stupně
- Dozorové audity

# Proč právě A1Q, s.r.o.



- Připravujeme naše klienty pro všechny významné certifikační organizace
- Nabízíme jednoduchá a poctivá řešení
- Snažíme se šířit dobrou náladu

A1Q, s.r.o.



- DĚKUJI ZA POZORNOST

- Ing. Richard Mikulčík