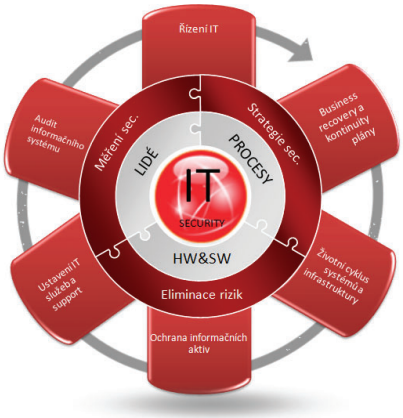
AUTOCONT

Zavedení systému řízení bezpečnosti informací (ISMS)

CO PŘINÁŠÍ SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ?

- Jistotu, že data jsou dostupná v potřebném rozsahu a čase
- Zajištění, že data jsou přístupná pouze tomu, komu jsou určena
- Ochranu informací takovým způsobem, aby nemohlo dojít k jejich neoprávněné změně
- Jednotný způsob ochrany dat a prostředků ICT
- Úspory nákladů na zabezpečení i na řešení bezpečnostních incidentů a havárií



AutoCont SECURITY bezpečnostní cyklus

Chcete vědět, jak řídit bezpečnost interních informací, které zásadním způsobem vaše ovlivňují podnikání?

Chcete vybudovat, případně certifikovat systém řízení bezpečnosti interních informací v souladu s normou ISO 27001?

Chcete zajistit ochranu dat a bezpečnost ICT (informační a komunikační technologie)?

Chcete efektivně využívat prostředky vynaložené na bezpečnost?

Popis řešení

Naše řešení ISMS nabízíme na základě přání a požadavků našich zákazníků jak formou komplexní dodávky tzv. ”na klíč“, tak i prostřednictvím výběru jednotlivých požadovaných služeb. Zákazníkům jsme schopni poskytnout i služby metodického vedení a konzultace s našimi odborníky a specialisty na oblast bezpečnosti informací, které zahrnují témata:

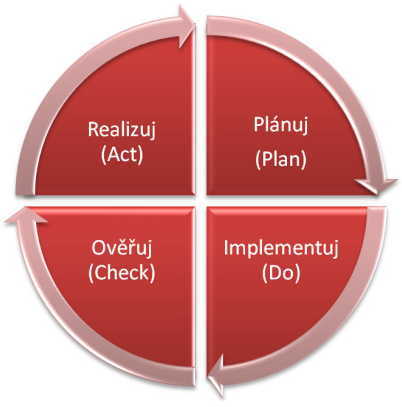
- Získání podpory managementu pro zavádění ISMS (např. v oblasti schvalování, přidělení pravomocí, prosazování ISMS)
- Definice rozsahu implementace ISMS
- Identifikace klíčových aktiv organizace
- Identifikace a hodnocení možných rizik
- Přípravy prohlášení o aplikovatelnosti
- Přípravy plánu zvládání/ošetření rizik
- Vytvoření programu implementace ISMS

PRAKTICKÉ PŘÍNOSY

Základním cílem tohoto řešení je vybudovat a úspěšně certifikovat systém řízení bezpečnosti v souladu s normou ISO 27001. Přínosem našich služeb jsou především znalosti a praktické zkušenosti se zaváděním a provozováním systému a s přípravou organizací na úspěšný audit implementace ISMS.

Mezi další přínosy řešení patří:

- zavedení systému a pořádku v řízení bezpečnosti interních informací
- vysoké bezpečnostní povědomí zaměstnanců-uživatelů
- efektivně vynakládané prostředky na bezpečnost ICT prostředí
- eliminace rizik a výskytu incidentů s negativním dopadem na bezpečnost klíčových informací
- ochrana ICT a citlivých dat organizace, které ovlivňují podnikání
- důvěryhodnost a dobré jméno vaší společnosti



Komu je řešení určeno

Řešení je určeno všem společnostem, které chtějí úspěšně řídit bezpečnost svých interních informací, které zásadním a klíčovým způsobem ovlivňuji podnikání organizace (informace o zákaznicích, projektech, rozvojových strategiích apod.) Dále zákazníkům, kteří chtějí získat certifikaci systému řízení bezpečnosti v souladu s normou ISO 27001 a tento systém nadále udržovat a neustále zlepšovat. Zavedení ISMS je určeno všem státním, veřejným i soukromým organizacím, které usilují o účinný, jednotný a systematický přístup k ochraně dat a ICT prostředků.

Způsob řešení

Komplexní služby spojené se zaváděním ISMS poskytujeme v rámci následujících kroků:

- Analýza rizik, včetně vytvoření metodiky, příp. realizace penetračních testů
- Vypracování plánu bezpečnosti, tj. harmonogramu realizace přijatých bezpečnostních opatření
- Vypracování potřebné bezpečnostní dokumentace (politika, směrnice, metodické materiály)
- Vytvoření havarijních plánů
- Zpracování prohlášení o aplikovatelnosti
- Příprava na interní audit
- Bezpečnostní školení a vzdělávání

Pod naším odborným dohledem a za aktivního přispění zákazníka k realizaci všech uvedených kroků jsme schopni garantovat úspěšné absolvování certifikačního auditu a získání certifikátu ISMS podle normy ISO 27001.

Podporované nástroje

Při poskytování služeb souvisejících s implementací ISMS se opíráme o požadavky, doporučení a obecné principy uvedené v normách:

- **ISO 27001** - Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky
- **ISO 27002** - Informační technologie - Soubor postupů pro řízení informační bezpečnosti

Reference

ÚKZÚZ - Re-audit informační bezpečnosti vč. penetračních testů