

Security Compliance



AEC disponuje stabilním týmem security specialistů. Klademe důraz na jejich specializaci, ale současně i široký přehled, který je v oblasti bezpečnosti nezbytný. I když prvořadé jsou pro nás praktické znalosti získané na projektech realizovaných pro naše zákazníky, řada našich specialistů se může pochlubit odbornými certifikacemi, jako např. CISA, CISSP, ITIL Foundation apod.



www.aec.cz

AEC

K problematice přistupujeme jak ze strany daných autoritativních zdrojů, tak i ze strany informačních technologií. Naším cílem není „jen zavést normy“, ale klademe důraz rovněž na optimální stanovení nutných procesů a vhodné použití konkrétních ICT technologií v souladu se zavedenými obchodními procesy a reálnými potřebami organizace.

V rámci našich projektů klademe velký důraz nejen na normativní základ (např. ISO/IEC 270xx), ale také na dodržování dalších známých technických standardů (např. ISO/IEC 15408, ISO 310xx atd.), využívané ICT technologie (např. OWASP, IETF, NIST, hardening atd.), řízení provozu ICT (např. ITIL, ISO/IEC 2000x, COBIT), projektové řízení (např. PRINCE2, PMI, TOGAF) a samozřejmě i soulad s „best-practices“.

Naše řešení je vždy v souladu s relevantní legislativou (např. se zákonem o ochraně osobních údajů č. 101/2000 Sb., zákonem o kybernetické bezpečnosti č. 181/2014 Sb. atd.).

Služby AEC v oblasti Security Compliance

- Budujete Systém řízení informační bezpečnosti (ISMS), připravujete se na certifikaci ISO/IEC 27001?
- Musíte být v souladu se Zákonem o kybernetické bezpečnosti?
- Chcete vyhovět požadavkům na ochranu osobních údajů (GDPR)? Potřebujete provést interní audit u dodavatele?
- Je pro vás velkým rizikem nedostupnost vašich služeb a informačních systémů a rozhodli jste se mu čelit zavedením systému Business Continuity Managementu?
- Manipulujete s platebními kartami a/nebo s transakcemi a vztahují se na vás požadavky PCI DSS?
- Provozujete systémy spadající do SWIFT infrastruktury a potřebujete ověřit plnění jeho bezpečnostního frameworku?

Pokud se potýkáte s těmito (nebo i dalšími) výzvami informační bezpečnosti, dokážeme vám účinně a efektivně pomoci!

Kde všude dokážeme pomoci?

- Systém řízení informační bezpečnosti (ISMS) dle norem řady ISO/IEC 270xx
- Zákon o kybernetické bezpečnosti (181/2014 Sb. a návazné vyhlášky)
- General Data Protection Regulation (EU 2016/679) a zákon o ochraně osobních údajů (101/2000 Sb.)
- Business Continuity Management Systems (ISO 22301)
- Payment Card Industry Data Security Standard (PCI DSS)
- SWIFT Customer Security Controls Framework

Přínosy našich služeb

- 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.
- Minimalizace rizik souvisejících s nedostupností informací a služeb, únikem nebo neoprávněným přístupem k informacím organizace aj.
- Úspora nákladů souvisejících s odstraňováním následků bezpečnostních incidentů.
- Zvýšení bezpečnostního povědomí zaměstnanců.

Z pohledu konkrétních činností poskytujeme:

■ Audit

Provedeme audit plnění požadavků v dané oblasti s ohledem na kontext organizace. Doporučíme vhodné kroky k nápravě nedostatků. V případě potřeby posoudíme i míru plnění požadavků u dalších zainteresovaných stran (např. dodavatelů).

■ Analýza

Provedeme analýzu rizik na základě identifikace aktiv organizace, relevantních hrozeb a existujících zranitelností (reálného pokrytí ochrannými opatřeními). Určíme míru závažnosti jednotlivých rizik a navrheme způsob jejich řešení.

■ Implementace

Pomůžeme vám s implementací opatření při budování informační bezpečnosti v souladu se stanovenou strategií, a to jak na úrovni procesů, tak i v oblasti technologií. V případě potřeby dovedeme klienta až k úspěšné certifikaci (např. ISMS).

■ Dokumentace

Vypracujeme potřebnou dokumentaci, která bude svým obsahem a formou odpovídat zvyklostem organizace, stejně jako dalším požadavkům v dané oblasti.

■ Outsourcing

Díky široké základně našich specialistů jsme schopni zajistit kontinuální podporu vaší organizace při řešení otázek informační bezpečnosti.

■ Školení

Zpracujeme vhodné edukační materiály pro všechny skupiny zaměstnanců. Školení provádíme jak prezenční formou, tak i pomocí e-learningu. Pro vyšší dopad školení doporučujeme zaměstnance otestovat např. metodami sociálního inženýrství.