BEZPEČNOSTNÍ AUDIT

SPRÁVNĚ ROZHODNOUT ZNAMENÁ ZNÁT REALITU

Bezpečnostní audit zkoumá a identifikuje skutečný aktuální stav procesů a opatření v určených oblastech bezpečnosti: organizační, administrativní, personální, fyzické, počítačové a komunikační a porovnává ho s požadovanými kritérii auditu.

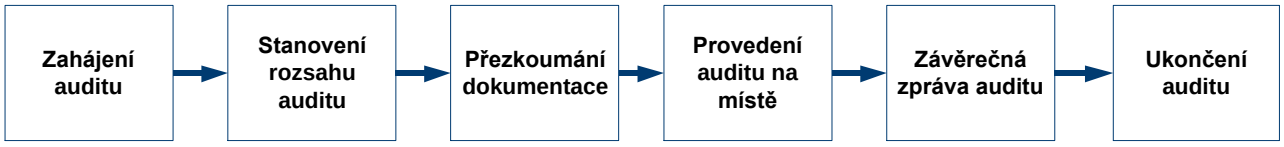
Cílem bezpečnostních auditů je porovnat a posoudit míru dosažené shody aktuálního stavu procesů a opatření bezpečnosti informací vůči požadovaným kritériím (definovanému optimálnímu stavu / etalonu), zdokumentovat nalezené rozdíly a nedostatky, navrhnout doporučení a upozornit na potenciální rizika.

Kritérii bezpečnostních auditů mohou být jednak interní bezpečnostní dokumentace organizace (politiky, směrnice, nařízení), národní / EU legislativa nebo vybrané normy, metodické pokyny, odborná a technologická doporučení institucí, výrobců a autorit.

„Nabízíme bezpečnostní audit systémů, aplikací, technické infrastruktury, všech oblastí ochranných opatření informačního systému a stavu bezpečnosti informací či kontinuity činností organizace.“

„Bezpečnostní audity provádíme především v souladu s mezinárodními standardy, interní dokumentací organizace a s „de-facto“ standardy danými ověřenou praxí.

Šest kroků auditu



Audity stavu bezpečnosti informací

Tyto audity jsou zaměřeny na posouzení dosaženého stavu bezpečnosti informací v souladu s **požadavky norem ISO/IEC 27001 a ISO/IEC 27002** na řízení systému bezpečnosti informací (**ISMS**) v organizacích.

Komplexní audit dle ISO/IEC 27001 a ISO/IEC 27002

Cíl: nezávislé prověření aktuálního stavu bezpečnosti informací organizace s požadavky norem pro řízení bezpečnosti informací.

Využití: získat jistotu, že bezpečnost informací je komplexně zvládána a zlepšována; získat konkurenční výhodu a záruky pro partnery, klienty a orgány státní správy. Audit může být i přípravou na získání či udržení certifikátu ISMS.

Přehledový audit systému řízení bezpečnosti informací

Cíl: rychlý přehled o stavu organizace z hlediska zavedení a provozu systému řízení bezpečnosti informací dle požadavků ISO 27001.

Využití: podklad pro plánování, zavádění nebo rozvoj ISMS v organizaci; nástroj a metodika pro periodickou kontrolu stavu a údržby ISMS v organizaci.

BEZPEČNOSTNÍ AUDIT

Audity stavu kontinuity činností

Tyto audity jsou zaměřeny na posouzení dosaženého stavu kontinuity činností v souladu s požadavky norem **ISO 22301 a ISO 22313** na řízení systému kontinuity činností (**BCMS**) v organizacích.

Komplexní audit dle norem ISO 22301 a ISO 22313

Cíl: nezávislé prověření aktuálního stavu kontinuity činností organizace s požadavky norem pro řízení kontinuity činností.

Využití: získat jistotu, že kontinuita činností je komplexně zvládána a zlepšována; získat konkurenční výhodu a záruky pro partnery, klienty a orgány státní správy. Audit může být i přípravou na získání či udržení certifikátu BCMS.

Přehledový audit BCMS

Cíl: rychlý přehled o stavu organizace z hlediska zavedení a provozu systému řízení kontinuity činností dle ISO 22301.

Využití: podklad pro plánování, zavádění nebo rozvoj BCMS v organizaci; nástroj a metodika pro periodickou kontrolu stavu a údržby BCMS v organizaci.

Specializované typy auditů bezpečnosti informací

Tyto audity jsou zaměřeny na posouzení souladu bezpečnosti informací s požadavky vybrané národní či EU legislativy (ochrana osobních údajů, klasifikovaných dat) nebo s dalšími normami pro bezpečnost informací (BASEL III, ITIL, COBIT, ISM3…).

Audit zajištění provozních rizik týkajících se bezpečnosti IS dle požadavků BASEL III

Cíl: prověřit aktuální stav řízení provozních rizik a souvisejících opatření dle požadavků BASEL III.

Využití: podklad pro plánování, zavádění nebo rozvoj ISMS v institucích finančního a bankovního sektoru a kontrola dosaženého souladu s požadavky BASEL III.

Audit zabezpečení informací a dat v organizaci dle požadavků národní / EU legislativy, požadavků organizace či smluvních závazků.

Cíl: prověřit stav ochrany informací jako například ochrany osobních údajů a /nebo utajovaných informací dle požadavků legislativy.

Využití: nezávislý posudek o plnění požadavků národní / EU legislativy na ochranu informací.

Audit bezpečnosti informačních systémů

Tyto audity jsou zaměřeny na zjištění souladu bezpečnosti informačních systémů nebo jejich částí ve zvolených oblastech bezpečnosti IS (oblasti ICT, fyzické, personální nebo administrativní) s požadovanými kritérii (normy, soubory nejlepších praktik, politikami, standardy a doporučenými postupy organizace,…) s cílem posoudit, zda informační systémy adekvátně ochraňují aktiva, zabezpečují integritu dat a poskytují spolehlivé a relevantní informace.

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.