

System managementu

BEZPEČNOSTI INFORMACÍ (ISMS)

Certifikace podle ISO/IEC 27001



ČESKÉ NÁRODNÍ
CERTIFIKAČNÍ FORUM

Informační technologie (zkr. IT) jako „červená nit“ prostupuje všemi procesy organizace. Management vaší společnosti používá informační technologie k řízení národních nebo mezinárodních firemních procesů. Vzdávající závislost na IT aplikacích znamená dramatický nárůst rizik a potřeb na systematickou každodenní ochranu dat. Řešení je prováděno systémem managementu bezpečnosti informací, který je přizpůsoben individuálním potřebám. Jak si mohu být jistý, že mám dnes optimální ochranu IT a že bude stále dobrá do budoucna? Jak mohu přesvědčit investory a klíčové zákazníky o spolehlivosti mého IT systému? Odpověď je jednoduchá:

- založte váš systém managementu bezpečnosti informací na splnění požadavků normy ISO/IEC 27001,
- dokumentujte jej a **certifikujte** oprávněným externím partnerem.

Koho se týká? Tato norma není specifická pro obor informačních technologií – je aplikovatelná stejně v logistickém odvětví, bankovníctví, u dodavatelů automobilových dílů, jako i ve zdravotnictví, kde je potřeba s údaji o vývoji, stejně jako s osobními údaji týkajícími se zákazníků, pacientů nebo personálu, zacházet a dále je zpracovávat s ohledem na jejich ochranu. Můžeme nalézt průkopníky v automobilovém průmyslu, kde se stále vyžaduje bezchybná harmonizace údajů s atributy integrity, důvěrnosti a dostupnosti.

Bezpečnost informací není svázána jen s informačními technologiemi. Informace jsou aktiva, která mají pro organizaci hodnotu. Mohou existovat v různých podobách (vytištěny nebo napsány na papíře, uloženy v elektronické podobě, posílány, zachyceny na film nebo vyřčeny při konverzaci).

Integrované systémy managementu? Systém managementu bezpečnosti informací je ideální kombinovat s již existujícími systémy managementu podle norem ISO 9001, ISO/TS 16949, ISO 14001, OHSAS 18001, ISO 20000 atd. Nezávisle na druhu certifikace - samotné nebo integrované, vám dle vašeho přání rádi vyjdeme vstříc a připravíme individuální certifikaci. Toto pro Vás znamená: služby zkušené mezinárodní certifikační společnosti, méně starostí s koordinací údajů a činností, využívání jednoho kontaktu při správě certifikace systému managementu a další výhody.

Kritéria pro certifikaci systému managementu bezpečnosti informací podle ISO/IEC 27001

- Politika bezpečnosti informací a organizace bezpečnosti.
- Klasifikace a monitorování systémů a hodnot.
- Personální, fyzická bezpečnost a bezpečnost prostředí.
- Administrace systémů, řízení přístupu, vývoj a údržba systémů.
- Plánování kontinuity.
- Soulad s mezinárodními a právními požadavky.

Norma ISO/IEC 27001 je mezinárodně uznávaný standard pro hodnocení bezpečnosti IT prostředí. Vedle informačních technologií, uvažuje zejména o relevantních podnikatelských procesech a stanovuje podmínky odpovídajícího monitorování. Norma ISO/IEC 27001 obsahuje souhrn praktických zkušeností a je úzce svázána s dalšími normami (dříve 2 díly, BS 7799-1 a BS 7799-2):

- ISO/IEC 27001 Systémy managementu bezpečnosti informací – Požadavky.
- ISO/IEC 17799 Informační technologie – Soubor postupů pro management bezpečnosti informací.



V oblasti norem ISO řady 27000 jsou využívány další normy, které již byly vydány, nebo se připravuje jejich vydání:

- ISO 27000 – ISMS, Základy a slovník.
- ISO 27001 – ISMS, Požadavky.
- ISO 27002 – ISMS, Soubor postupů (předchází ISO 17799).
- ISO 27003 – ISMS, Metriky a měření.
- ISO 27004 – ISMS, Návod pro implementaci.
- ISO 27005 – ISMS, Management rizik (předchází BS7799-3).

Přínos implementace mezinárodně uznávaného standardu ISO/IEC 27001 leží především na identifikaci rizik (týkajících se nakládání s informacemi) a jejich zvládnání. Tím je zajištěna spolehlivost informačních systémů včetně atributů bezpečnosti informací – integritou, důvěrností a dostupností.

Společnosti poskytující IT služby mají možnost implementovat systém managementu podle požadavků normy ISO 20000 a požadavky na bezpečnost prostřednictvím normy ISO/IEC 27001. Normy ISO řady 20000 nahrazují předchozí normu ISO 15001 a navazují na soubor postupů ITIL, které jsou zaměřeny na subjekty poskytující IT služby pro další podnikatelské subjekty.

TÜV NORD Czech, s.r.o. je váš partner, součást skupiny TÜV NORD AG, zajišťující provedení certifikací systémů managementu podle norem ISO 9001, ISO/TS 16949, VDA 6.1, VDA 6.4, HACCP, EN 3834, ISO 14001, BS OHSAS 18001, **ISO 27001**, ISO 20000 atd.

- ▶ Audity provádějí kvalifikovaní auditoři se způsobilostmi dle EAC klíčů.
- ▶ Naše certifikáty jsou vydávány ve standardních formátech a v jazycích německém, anglickém a českém.
- ▶ V dalších jazycích dle vašich požadavků.

KONKURENČNÍ VÝHODY – EXTERNÍ:

- Vzrůstající konkurenceschopnost.
- Oficiální potvrzení (certifikát) vydaný zkušenou mezinárodní a nezávislou certifikační společností, uznávaný zákazníky, partnery a legislativou.
- Redukce přístupových bariér trhu k činnostem na mezinárodních a národních trzích.
- Dlouhodobá a oboustranná loajální spolupráce se stávajícími zákazníky a stále získávání nových partnerů.

KONKURENČNÍ VÝHODY – INTERNÍ:

- Předcházení IT rizikům.
- Jasné struktury a odpovědnosti.
- Redukce problémů na přechodových místech systémů.
- Koncentrace informací.
- Přezkoumání interních bezpečnostních standardů.
- Objektivní hodnocení vlastního know-how.
- Proces neustálého zlepšování.
- Redukce ztrát z chyb.

Těšíme se na spolupráci s Vámi.

Vaše kontaktní osoba pro oblast certifikace systémů managementu bezpečnosti informací v TÜV NORD Czech, s.r.o.:

Ing. Tomáš Staněk

Pod Hájkem 406/1, 180 00 Praha 8

Tel: +420 296 587 201 - 9

Fax: +420 296 587 240

E-mail: stanek@tuev-nord.cz

www.tuev-nord.cz

