ČESKÁ TECHNICKÁ NORMA

ICS 35.040

Říjen

2006

Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky	ČSN ISO/IEC 27001 36 9790

Information technology - Security techniques - Information security management systems - Requirements

Technologies de l'information - Techniques de sécurité - Systémes de gestion de sécurité de l'information - Exigences

Tato norma je českou verzí mezinárodní normy ISO/IEC 27001:2005. Překlad byl zajištěn Českým normalizačním institutem. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 27001:2005. It was translated by Czech Standards Institute. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN BS 7799-2 (36 9790) z prosince 2004.

Národní předmluva

Změny proti předchozím normám

Oproti předchozímu vydání normy ČSN BS 7799 bylo z Přílohy A odstraněno devět bezpečnostních opatření a sedmnáct nových jich přibylo.

Informace o citovaných normativních dokumentech

ISO 9001:2000 zavedena v ČSN EN ISO 9001:2001 (01 0321) Systémy managementu jakosti - Požadavky

ISO 14001 zavedena v ČSN EN ISO 14001:2005 (010901) Systémy environmentálního managementu - Požadavky s návodem pro použití

ISO/IEC 13335-1:2004 dosud nezavedena

ISO/IEC TR 13335-3:1998 zavedena v ČSN ISO/IEC TR 13335-3:2000 (36 9786) Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 3: Techniky pro řízení bezpečnosti IT

ISO/IEC 17799:2005 zavedena v ČSN ISO/IEC 17799:2006 (36 9790) Informační technologie - Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací

EN ISO 19011:2002 zavedena v ČSN EN ISO 19011:2003 (01 0330) Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu

Souvisící ČSN

ČSN ISO/IEC 17799 (36 9790) Informační technologie - Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací

Vysvětlivky k textu převzaté normy

Nesoulad v překladu jednotlivých kapitol v Příloze C je způsoben různými překlady předchozích vydání norem ČSN EN ISO 9001 a ČSN EN ISO 14001.

Vypracování normy

Zpracovatel: Risk Analysis Consultants, s.r.o., IČ 63672774, Ing. Libor ©iroký

Technická normalizační komise: TNK 20 Informační technologie

Zaměstnanec Českého normalizačního institutu: Ing. Petr Wallenfels

MEZINÁRODNÍ NORMA
Informační technologie - Bezpečnostní techniky — ISO/IEC 27001
Systémy managementu bezpečnosti informací - Požadavky — První vydání 2005-10

ICS 35.040

ISO copyright office
Case postale 56, CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.ch
Web www.iso.ch

Obsah

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém celosvětové normalizace. Národní orgány, které jsou členy ISO nebo IEC, se podílejí na vypracování mezinárodních norem prostřednictvím technických komisí zřízených příslušnou organizací k tomu, aby se zabývaly určitou oblastí technické činnosti. V oblastech společného zájmu technické komise ISO a IEC spolupracují. Práce se zúčastňují i jiné mezinárodní organizace, vládní i nevládní, s nimiž ISO a IEC navázaly pracovní styk. V oblasti informačních technologií zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC 1.

Návrhy mezinárodních norem jsou zpracovány v souladu s pravidly uvedenými v části 2 Směrnic ISO/IEC.

Hlavním úkolem společné technické komise je připravovat mezinárodní normy. Návrhy mezinárodních norem přijaté společnou technickou komisí se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících členů.

Pozornost je třeba věnovat možnosti, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nenesou odpovědnost za identifikaci všech patentových práv nebo kteréhokoliv z nich.

Mezinárodní norma ISO/IEC 27001 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Information technology*, subkomise SC 27, *IT Security techniques.*

---

0 Úvod

0.1 Všeobecně

Tato mezinárodní norma byla připravena proto, aby poskytla podporu pro ustavení, zavádění, provozování, monitorování, udržování a zlepšování systému managementu bezpečnosti informací (Information Security Management System nebo ISMS). Přijetí ISMS by mělo být strategickým rozhodnutím organizace. Návrh a zavedení ISMS v organizaci je podmíněno potřebami a cíli činností (business), požadavky na bezpečnost, dále pak používanými procesy a velikostí a strukturou organizace. Všechny tyto a jejich podpůrné systémy podléhají změnám v čase. Předpokládá se, že jednoduché situace vyžadují jednoduchá řešení ISMS.

Tato norma je určena k posuzování souladu ze strany zainteresovaných interních i externích stran.

0.2 Procesní přístup

Tato mezinárodní norma prosazuje přijetí procesního přístupu pro ustavení, zavádění, provozování, monitorování, udržování a zlepšování ISMS v organizaci.

Aby organizace fungovala efektivně, musí identifikovat a řídit mnoho vzájemně propojených činností. Činnost, která využívá zdroje a je řízena za účelem přeměny vstupů na výstupy, může být považována za proces. Výstup z jednoho procesu často přímo tvoří vstup pro následující proces.

Aplikace systému procesů v organizaci, spolu s identifikací těchto procesů, jejich vzájemným působením a řízením může být označováno jako „procesní přístup“.

Při použití procesního přístupu pro management bezpečnosti informací tak, jak je prezentován v této normě, je kladen důraz na:

a) pochopení požadavků na bezpečnost informací organizace a potřebu stanovení politiky a cílů bezpečnosti informací;

b) zavedení a provozování opatření pro management bezpečnosti informací v kontextu s řízením celkových rizik činností organizace;

c) monitorování a přezkoumání výkonnosti a účinnosti ISMS;

d) neustálé zlepšování založené na objektivním měření.

Model známý jako „Plánuj-Dělej-Kontroluj-Jednej“ (Plan-Do-Check-Act nebo PDCA) může být aplikován na všechny procesy ISMS tak, jak jsou zavedeny touto normou. Obrázek 1 znázorňuje, jak ISMS přijímá požadavky bezpečnosti informací a očekávání zainteresovaných stran jako vstup, a jak pomocí nezbytných činností a procesů vytváří výstupy bezpečnosti informací, které splňují tyto požadavky a očekávání. Obrázek 1 také znázorňuje propojení procesů uvedených v kapitolách 4, 5, 6, 7 a 8.

Zavedení modelu PDCA bude také odrážet principy, které jsou popsány ve směrnici OECD (2002)[1] pro řízení bezpečnosti informačních systémů a sítí. Norma ISO/IEC 27001 poskytuje celistvý model pro zavedení principů popsaných v této směrnici, které upravují hodnocení rizik, návrh a zavedení bezpečnosti, management bezpečnosti a opětovné hodnocení bezpečnosti.

PŘÍKLAD 1

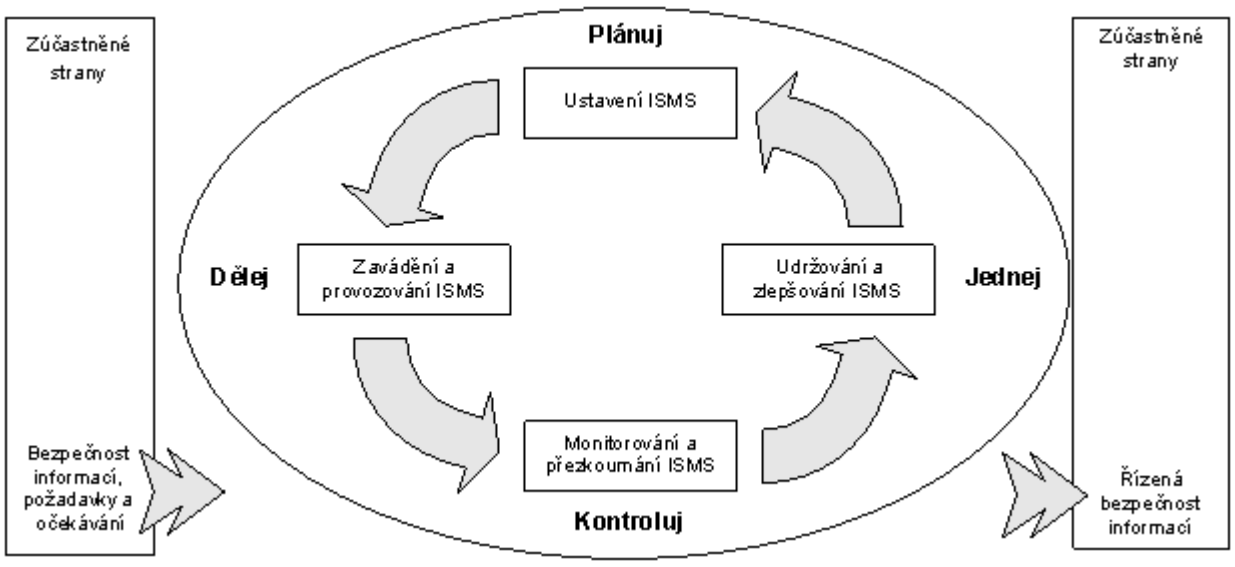
Může být například požadováno, aby v případě narušení bezpečnosti nebyly způsobeny organizaci vážné finanční škody ani jiné těžkosti (např. ztráta image).

PŘÍKLAD 2

Vyskytne-li se závažný incident, například napadení (hacking) eBusiness systému organizace (web site) očekává se, že pro minimalizaci dopadů incidentu budou k dispozici dostatečně vyškolení zaměstnanci.

---

[1] OECD. OECD Guidelines for the Security of Information systems and Network – Towards a Culture of Security.
Paris: OECD, July 2002. www.oecd.org.



Obrázek 1 - PDCA model aplikovaný na procesy ISMS

Plánuj (ustavení ISMS)	Ustavení politiky ISMS, cílů, procesů a postupů souvisejících s managementem rizik a zlepšováním bezpečnosti informací tak, aby poskytovaly výsledky v souladu s celkovou politikou a cíli organizace.
Dělej (zavádění a provozování ISMS)	Zavedení a využívání politiky ISMS, opatření, procesů a postupů.
Kontroluj (monitorování a přezkoumání ISMS)	Posouzení, kde je to možné i měření výkonu procesu vůči politice ISMS, cílům a praktickým zkušenostem a hlášení výsledků vedení organizace k přezkoumání.
Jednej (udržování a zlepšování ISMS)	Přijetí opatření k nápravě a preventivních opatření, založených na výsledcích interního auditu ISMS a přezkoumání systému řízení ze strany vedení organizace tak, aby bylo dosaženo neustálého zlepšování ISMS.

0.3 Kompatibilita s jinými systémy managementu

Tato mezinárodní norma je propojena s normami ISO 9001:2000 a ISO 14001:2004 tak, aby bylo podpořeno jejich konzistentní a jednotné zavedení a provoz. Jeden vhodně navržený systém managementu tak může naplnit požadavky všech těchto norem. Tabulka C.1 znázorňuje vztah mezi kapitolami této normy, ISO 9001:2000 a ISO 14001:2004.

Tato norma je navržena tak, aby organizaci umožnila propojit nebo integrovat ISMS s odpovídajícími požadavky systému managementu.

Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky

Důležité upozornění - Tato publikace nemůže obsáhnout všechna opatření z oblasti jejího určení. Uživatelé jsou odpovědni za její správné použití. Shoda s normou sama o sobě nezbavuje organizaci odpovědnosti za splnění závazků vyplývajících ze zákona.

1 Předmět normy

1.1 Všeobecně

Tato mezinárodní norma je použitelná pro všechny typy organizací (např. komerční organizace, vládní agentury a úřady, neziskové organizace). Norma specifikuje požadavky na ustavení, zavedení, provoz, monitorování, přezkoumání, udržování a zlepšování dokumentovaného ISMS v kontextu celkových rizik činností organizace. Specifikuje požadavky na zavedení bezpečnostních opatření, upravených podle potřeb jednotlivých organizací nebo jejich částí.

ISMS je navržen tak, aby zajistil odpovídající a přiměřená bezpečnostní opatření chránící informační aktiva a poskytující odpovídající jistotu zainteresovaným stranám.

POZNÁMKA 1 Slovo „business“ je v textu normy překládáno jako „činnost organizace“, v kontextu celé normy jsou činnostmi organizace myšleny veškeré aktivity, které jsou důležité pro existenci organizace a naplňování jejích cílů.

POZNÁMKA 2 ISO/IEC 17799 poskytuje doporučení, která mohou být použita při návrhu a realizaci jednotlivých opatření.

-- Vynechaný text --