ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Prosinec 2011**

Informační technologie – Bezpečnostní techniky – Směrnice pro implementaci systému řízení bezpečnosti informací

ČSN ISO/IEC 27003
36 9790

Information technology – Security techniques – Information security management system implementation guidance

Technologies de l,information – Techniques de sécurité – Lignes directrices pour la mise en ouvre du systeme
de management de la sécurité de l,information

Tato norma je českou verzí mezinárodní normy ISO/IEC 27003:2010. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 27003:2010. It was translated by Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Národní předmluva

Informace o citovaných normativních dokumentech

ISO/IEC 27000:2009 zavedena v ČSN ISO/IEC 27000:2010 (369790) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

ISO/IEC 27001:2005 zavedena v ČSN ISO/IEC 27001:2006 (369790) Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky

Souvisící ČSN

ČSN EN ISO 9001:2009 (01 0321) Systémy managementu jakosti – Požadavky

ČSN EN ISO 14001:2005 (01 0901) Systémy environmentálního managementu – Požadavky s návodem pro použití

ČSN ISO/IEC 15026:2000 (36 9030) Informační technologie – Úrovně integrity softwaru a systému

ČSN ISO/IEC 15408-2:2010 (36 9789) Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 2: Bezpečnostní funkční komponenty

ČSN ISO/IEC 15408-3:2010 (36 9789) Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 3: Komponenty bezpečnostních záruk

ČSN ISO/IEC 15939:2011 (36 9040) Softwarové inženýrství – Proces měření

ČSN ISO/IEC 20000-1:2006 (36 9074) Informační technologie – Management služeb – Část 1: Specifikace

ČSN ISO/IEC 27001:2006 (369790) Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky

ČSN ISO/IEC 27004:2011 (36 3790) Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Měření

ČSN ISO/IEC 27005:2009 (36 3790) Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací

ČSN ISO/IEC 27006:2008 (36 9790) Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací

Vypracování normy

Zpracovatel: Risk Analysis Consultants, s.r.o., IČ 63672774

Technická normalizační komise: TNK 20 Informační technologie

Zaměstnanec Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Petr Wallenfels

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – ISO/IEC 27003
Směrnice pro implementaci systému řízení bezpečnosti informací První vydání
2010-02-01

ICS 35.040

Obsah

Strana

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.org

Web www.iso.org

Published in Switzerland

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.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědné za identifikaci libovolného patentového práva nebo všech takových patentových práv.

Mezinárodní norma ISO/IEC 27003 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie*, subkomise SC 27, *IT Bezpečnostní techniky*.

Úvod

Účelem této mezinárodní normy je poskytnout praktická doporučení při vývoji plánu implementace pro systém řízení bezpečnosti informací (ISMS) v organizaci v souladu s ISO/IEC 27001:2005. Skutečná implementace ISMS se obvykle provádí jako projekt.

Proces popsaný v této mezinárodní normě byl navržen tak, aby poskytoval podporu pro zavedení ISO/IEC 27001:2005 (příslušné části z kapitol 4, 5, a 7 včetně) a zdokumentoval:

a) přípravu zahájení plánu implementace ISMS v organizaci, definování organizační struktury pro projekt a získání souhlasu vedení organizace;

b) kritické činnosti pro projekt ISMS; a

c) příklady naplnění požadavků normy ISO/IEC 27001:2005.

Použitím této mezinárodní normy bude organizace schopna zavést proces řízení bezpečnosti informací poskytující zainteresovaným stranám ujištění o tom, že rizika působící na informační aktiva jsou neustále udržována v rámci přijatelných hranic bezpečnosti informací stanovených organizací.

Tato mezinárodní norma nepokrývá činnosti spojené s provozem ISMS. Poskytuje však doporučení k činnostem, které vyplynou ze zahájení provozování ISMS. Výsledkem této koncepce je finální plán implementace projektu ISMS. Skutečné provedení specifické části projektu ISMS organizace je mimo rozsah této mezinárodní normy.

Implementace projektu ISMS by se měla provádět za použití standardních metodik řízení projektů (více informací naleznete v ISO a ISO/IEC normách, které se týkají řízení projektů).

1 Předmět normy

Tato mezinárodní norma se zaměřuje na kritické aspekty nutné pro úspěšný návrh a implementaci systému řízení bezpečnosti informací (ISMS) v souladu s ISO/IEC 27001:2005. Popisuje proces

specifikace a návrhu ISMS od počátku do vytvoření implementačních plánů. Popisuje proces získání souhlasu vedení organizace k zavedení ISMS, definuje projekt, jak implementovat ISMS (tento projekt je dále v této mezinárodní normě uváděn jako projekt ISMS) a poskytuje doporučení, jak plánovat projekt ISMS, aby výsledkem byl finální plán implementace projektu ISMS.

Tato mezinárodní norma je určena pro organizace, které zavádějí ISMS. Je aplikovatelná pro všechny typy
organizací (například: obchodní podniky, vládní organizace, neziskové organizace) všech velikostí. Složitost a rizika každé organizace jsou jedinečná a její specifické požadavky budou hnací silou pro implementaci ISMS. Menší organizace shledají, že činnosti zmíněné v této mezinárodní normě jsou pro ně použitelné a lze je ještě zjednodušit. Velké společnosti mohou shledat, že pro účinné řízení činností popsaných v této mezinárodní normě bude zapotřebí víceúrovňová organizační struktura nebo systém řízení. V obou případech však lze plánovat příslušné činnosti za použití této mezinárodní normy.

Tato mezinárodní norma dává doporučení a vysvětlení; nespecifikuje žádné požadavky. Tato mezinárodní norma je určena pro použití v souvislosti s ISO/IEC 27001:2005 a ISO/IEC 27002:2005, ale není určena k tomu, aby měnila a/nebo redukovala požadavky specifikované v ISO/IEC 27001:2005 nebo doporučení uvedená v ISO/IEC 27002:2005. Vyžadování shody s touto mezinárodní normou není vhodné.