ČESKÁ TECHNICKÁ NORMA

ICS 35.020; 03.100.01 **Prosinec 2004**

	Systém managementu bezpečnosti informací - Specifikace s návodem pro použití	ČSN BS 7799-2 36 9790

Information Security Management Systems - Specification with guidance for use

Tato norma je českou verzí britské normy BS 7799-2:2002. Britská norma BS 7799-2:2002 má statut české technické normy.

This standard is the Czech version of the BS 7799-2:2002. The British Standard BS 7799-2:2002 has the status of a Czech Standard

71613

Národní předmluva

Citované normy

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

ISO/IEC 17799:2000 zavedena v ČSN ISO/IEC 17799:2005 (36 9790) Informační technologie - Soubor postupů pro management bezpečnosti informací

ISO Guide 73:2002 dosud nezaveden

Vypracování normy

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

Technická normalizační komise: TNK 20 Informační technologie

Zaměstnanec Českého normalizačního institutu: Ing. Petr Wallenfels

---

BRITSKÁ NORMA
Systém managementu bezpečnosti informací - 7799-2 **BS**
Specifikace s návodem pro použití Druhé vydání

2002-09-05

ICS 03.100.01;35.020

Norma BS 7799-2 byla připravena výborem BDD/2, Information security management, reprezentovaném zástupci následujících organizací:

@stake

Articsoft Ltd

Association of British Insurers

British Computer Society

British Telecommunications plc

British Security Industry Association

Department of Transport and Industry - Information Security Policy Group

EDS Ltd

Experian

Gamma Secure Systems Limited

GlaxoSmithKline plc

HMG Protective Security Authority

HSBC

I-Sec Ltd

Institute of Chartered Accountants in England and Wales

Institute of Internal Auditors - UK and Ireland

KPMG plc

Lloyds TSB

Logica UK Ltd

London Clearing House

Marks & Spencer plc

National Westminster Group

Nationwide Building Society

QinetiQ Ltd

Shell UK

Unilever

Wm. List & Co

XiSEC Consultants Ltd/AEXIS Security Consultants

Norma BS 7799-2, připravená pod dohledem komise BSI-DISC, byla publikována se souhlasem Standards Policy and Strategy Committee a byla vydána dne 5.září 2002.

poprvé publikováno jako část 2 v únoru 1998

aktualizace, květen 1999

ISBN 0 580 40250 9

Obsah

Předmluva

Tato část BS 7799 byla připravena výborem BDD/2, Information security management. Nahrazuje BS 7799-2:1999. Toto nové vydání bylo vytvořeno za účelem harmonizace s dalšími normami systému managementu jako např. EN ISO 9001:2000 a EN ISO 14001:1996 proto, aby zajistilo důslednou a sjednocenou implementaci a využití systémů managementu. Také zavádí model Plánuj-Dělej-Kontroluj-Jednej (Plan-Do-Check-Act nebo zkratkou PDCA) jako součást přístupu systému managementu k vývoji, implementaci a zlepšování efektivnosti systému managementu bezpečnosti informací v organizaci.

Zavedení modelu PDCA bude také odrážet principy, které jsou stanoveny ve směrnicích OECD (2002)[1] pro řízení bezpečnosti informačních systému a sítí. Toto nové vydání především poskytuje celistvý model pro zavedení principů ve směrnicích, které upravují hodnocení rizik, návrh a zavedení bezpečnosti, management bezpečnosti a opětovné hodnocení bezpečnosti.

Cíle kontrol a jednotlivé kontroly, kterých se to týká, jsou v tomto vydání odvozeny a uspořádány přímo podle těch, které jsou uvedeny v ISO/IEC 17799:2000. Seznam cílů kontrol a jednotlivých kontrol v této normě není vyčerpávající a organizace by měla brát v úvahu, že mohou být nezbytné i další cíle kontrol a jednotlivé kontroly. Ne všechny kontroly zde popsaná se budou týkat všech situací, nemohou ani přihlížet k omezením místního prostředí nebo technologií, nebo se vyskytovat ve formě, která vyhovuje každému případnému uživateli v organizaci.

Tato publikace nemůže obsáhnout všechna opatření z oblasti jejího určení. Uživatelé jsou sami odpovědni za její správné použití.

Shoda s normou sama o sobě neposkytuje ochranu před plněním zákonných závazků.

---

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

0 Úvod

0.1 Všeobecně

Tato norma je určena pro podnikové manažery a jejich zaměstnance, aby poskytla model pro zavedení a správu efektivního 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 cíly činností (business) organizace a z toho vyplývajících požadavků 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.

Tuto normu mohou využívat interní i externí subjekty, včetně certifikačních orgánů, k hodnocení schopnosti organizace splnit vlastní požadavky, stejně jako jakékoli zákonné požadavky nebo požadavky zákazníků.

0.2 Procesní přístup

Tato norma prosazuje přijetí procesního přístupu pro vybudování, zavedení, provozování, monitorování, udržování a zlepšování efektivnosti 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 je kladen důraz na:

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

b) zavedení a provádění kontrol v kontextu s řízením celkových rizik činností organizace;

c) monitorování a přezkoumání funkčnosti a efektivnosti ISMS;

d) neustálé zlepšování založené na objektivním měření.

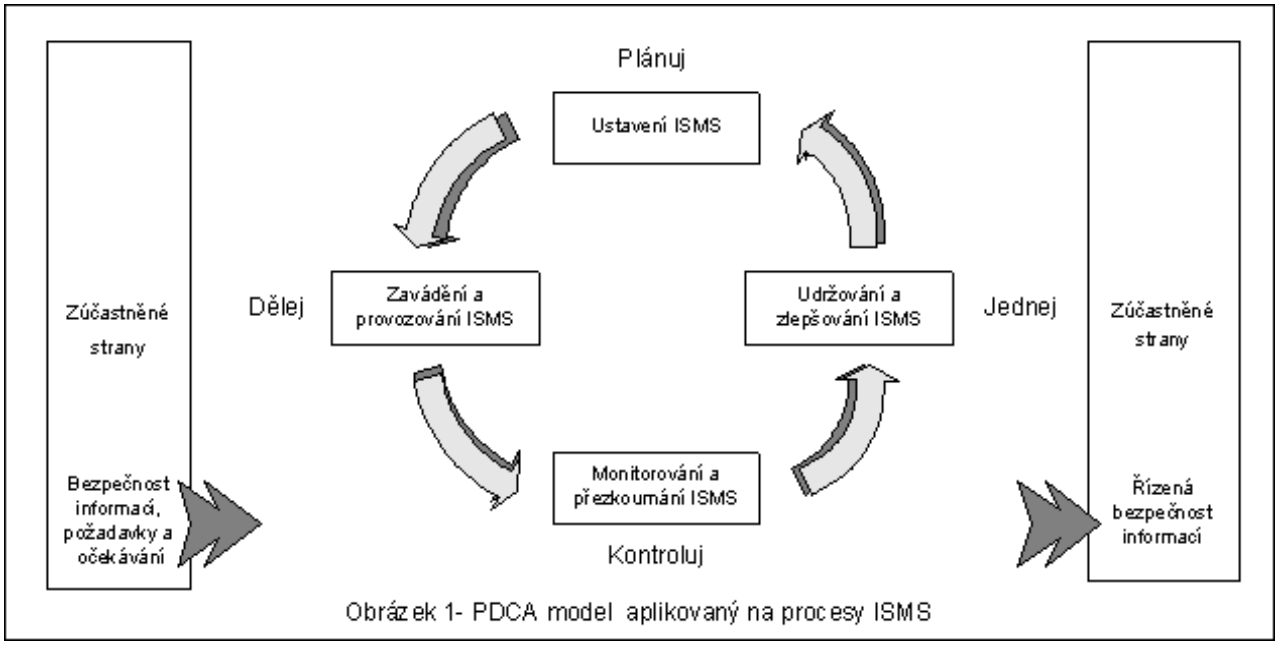
Model známý jako „Plánuj-Dělej-Kontroluj-Jednej“ (Plan-Do-Check-Act nebo PDCA) může být aplikován na všechny procesy ISMS tak, jak jsou zavedeny touto normou. Obrázek 1 znázorňuje, jak ISMS přijímá požadavky bezpečnosti informací a očekávání zainteresovaných stran jako vstup, a jak pomocí nezbytných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

PŘÍKLAD 1

Může být například požadováno, aby v důsledku bezpečnostních incidentů nebyly způsobeny organizaci vážné finanční škody ani jiné těžkosti.

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.



Obrázek 1- PDCA model aplikovaný na procesy ISMS

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

0.3 Kompatibilita s jinými systémy managementu

Tato norma je propojena s normami EN ISO 9001:2000 a EN ISO 14001:1996 tak, aby bylo podpořeno jejich konzistentní a jednotné zavedení a provoz.

Tabulka C.1 znázorňuje vztah mezi kapitolami této normy, EN ISO 9001:2000 a EN ISO 14001:1996.

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

1 Předmět normy

1.1 Všeobecně

Tato norma specifikuje požadavky na vybudování, zavedení, provoz, monitorování, přezkoumání, udržování a zlepšování dokumentovaného ISMS v kontextu celkových rizik činností organizace. Specifikuje požadavky na zavedení bezpečnostních kontrol, upravených podle potřeb jednotlivých organizací nebo jejich částí (viz přílohu B, která poskytuje informativní návod k používání této normy).

ISMS je navržen tak, aby zajistil odpovídající a přiměřené bezpečnostní kontroly, adekvátně chránící informační aktiva a poskytující odpovídající jistotu zákazníkům a dalším zainteresovaným stranám. Jinými slovy jde o udržování a zlepšování konkurenceschopnosti, oběhu hotovosti (cash flow), výnosů, zajištění souladu s právem a postavení na trhu.

-- Vynechaný text --