ČESKÁ TECHNICKÁ NORMA

ICS 03.100.70; 35.030 **Březen 2018**

# Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Monitorování, měření, analýza a hodnocení

ČSN ISO/IEC 27004

36 9790

Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation

Technologies de l,information – Techniques de sécurité – Management de la sécurité de l,information – Surveillance, mesurage, analyse et évaluation

Tato norma je českou verzí mezinárodní normy ISO/IEC 27004:2016. Překlad byl zajištěn Českou agenturou pro standardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 27004:2016. It was translated by the Czech Standardization Agency. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO/IEC 27004 (36 9790) z ledna 2011.

Národní předmluva

Změny proti předchozí normě

Ve druhém vydání normy byla zcela změněna struktura dokumentu, protože byl modifikován účel dokumentu – poskytnout návod k ISO/IEC 27001:2013, 9.1 – který v době předchozího vydání normy neexistoval.

Koncepty a procesy byly modifikovány a rozšířeny. Avšak teoretický základ (ISO/IEC 15939) zůstává stejný a několik příkladů uvedených v předcházejícím vydání je zachováno, i když jsou aktualizovány.

Souvisící ČSN

ČSN ISO/TR 10017 (01 0336) Návod k aplikaci statistických metod v ISO 9001:2000

ČSN EN ISO/IEC 27000 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

ČSN EN ISO/IEC 27001:2014 (36 9797) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky

Vysvětlivky k textu převzaté normy

Pro účely této normy byl použit:

– překlad anglického termínu „management“ jako „řízení“ s ohledem na jeho preferované používání v oblasti IT a v návaznosti na vydané normy z oblasti IT, zejména norem řady 27XXX;

– překlad anglického termínu „control“ jako „opatření“, „řízení“ nebo „kontrola“ s ohledem na význam v textu normy.

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČO 61470716

Technická normalizační komise: TNK 20 Informační technologie

Pracovník České agentury pro standardizaci: Ing. Miroslav Škop

Česká agentura pro standardizaci je státní příspěvková organizace zřízená Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví na základě ustanovení § 5 odst. 2 zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Monitorování, měření, analýza a hodnocení

ISO/IEC 27004
Druhé vydání
2016-12-15

ICS 03.100.70; 35.030

Obsah

Strana

# 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 svých technických komisí ustavených příslušnými organizacemi pro jednotlivé obory technické činnosti. Technické komise ISO a IEC spolupracují v oborech společného zájmu. Práce se zúčastňují také další vládní i nevládní mezinárodní organizace, s nimiž ISO a IEC navázaly pracovní styk. V oblasti informační technologie zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC 1.

Postupy použité při tvorbě tohoto dokumentu a postupy určené pro jeho další udržování jsou popsány ve směrnicích ISO/IEC, část 1. Zejména se má věnovat pozornost rozdílným schvalovacím kritériím potřebným pro různé druhy dokumentů ISO. Tento dokument byl vypracován v souladu s redakčními pravidly uvedenými ve směrnicích ISO/IEC, část 2 (viz www.iso.org/directives).

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědnými za identifikaci jakéhokoliv nebo všech patentových práv. Podrobnosti o jakýchkoliv patentových právech identifikovaných během přípravy tohoto dokumentu budou uvedeny v úvodu a/nebo v seznamu patentových prohlášení obdržených ISO (viz www.iso.org/patents).

Jakýkoliv obchodní název použitý v tomto dokumentu se uvádí jako informace pro usnadnění práce uživatelů a neznamená schválení.

Vysvětlení významu specifických termínů a výrazů ISO, které se vztahují k posuzování shody, jakož i informace o tom, jak ISO dodržuje principy WTO týkající se technických překážek obchodu (TBT), jsou uvedeny na tomto odkazu URL: www.iso.org/iso/foreword.html.

Za tento dokument je odpovědná komise ISO/IEC JTC 1 *Informační technologie*, Subkomise SC 27 *IT Bezpečnostní techniky*.

Toto druhé vydání ISO/IEC 27004 zrušuje a nahrazuje první vydání (ISO/IEC 27004:2009), které bylo technicky zrevidováno.

Toto vydání zahrnuje oproti předchozímu vydání následující hlavní změny:

Úplná restrukturalizace dokumentu, protože má nový účel – poskytnout návod k ISO/IEC 27001:2013, 9.1 – který v době předchozího vydání neexistoval.

Koncepty a procesy byly modifikovány a rozšířeny. Avšak teoretický základ (ISO/IEC 15939) zůstává stejný a několik příkladů uvedených v předcházejícím vydání je zachováno, i když jsou aktualizovány.

# Úvod

Tento dokument má pomoci organizacím při hodnocení výkonnosti bezpečnosti informací a efektivnosti systému řízení bezpečnosti informací, aby splnily požadavky ISO/IEC 27001:2013, 9.1: Monitorování, měření, analýza a hodnocení.

Výsledky monitorování a měření systému řízení bezpečnosti informací (ISMS) mohou podporovat rozhodnutí týkající se správy, managementu, provozní efektivnosti a neustálého zlepšování ISMS.

Jako je tomu u jiných dokumentů ISO/IEC 27000, měl by být tento dokument zvažován, interpretován a upravován tak, aby vyhovoval konkrétní situaci v každé organizaci. Koncepty a přístupy jsou určeny k široké aplikaci, ale konkrétní míry, které jakákoliv organizace požaduje, závisí na kontextových faktorech (jako je její velikost, odvětví, vyzrálost, rizika bezpečnosti informací, povinnost zajistit soulad a styl řízení), které se v praxi hodně mění.

Tento dokument se doporučuje organizacím implementujícím ISMS, které splňují požadavky ISO/IEC 27001. Nestanoví však pro ISMS žádné nové požadavky, které by odpovídaly ISO/IEC 27001 nebo ukládaly organizacím jakékoliv povinnosti ve věci dodržování předložených směrnic.

# 1 Předmět normy

Tento dokument poskytuje směrnice, jejichž cílem je pomáhat organizacím při hodnocení výkonnosti bezpečnosti informací a efektivnosti systému řízení bezpečnosti informací, aby splnily požadavky ISO/IEC 27001:2013, 9.1. Stanoví:

a) monitorování a měření výkonnosti bezpečnosti informací;

b) monitorování a měření efektivnosti systému řízení bezpečnosti informací (ISMS) včetně jeho procesů a opatření;

c) analýzu a vyhodnocení výsledků monitorování a měření.

Tento dokument mohou používat všechny druhy a velikosti organizací.