# ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Leden 2011**

Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Měření

**ČSN**
**ISO/IEC 27004**
36 9790

Information technology – Security techniques – Information security management – Measurement

Technologies de l,information – Techniques de sécurité – Management de la sécurité de l,information – Mesurage

Tato norma je českou verzí mezinárodní normy ISO/IEC 27004:2009. 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 27004:2009. 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 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

ISO/IEC 27001:2005 zavedena v ČSN ISO/IEC 27001:2006 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky

Souvisící ČSN

ČSN EN ISO 9000:2005 (01 0300) Systémy managementu kvality – Základní principy a slovník

ČSN ISO/IEC 15504-3:2004 (36 9027) Informační technologie – Posuzování procesu – Část 3: Návod na realizaci posouzení

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

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

ČSN ISO/TR 10017:2004 (01 0336) Návod k aplikaci statistických metod v ISO 9001:2000

Vysvětlivky k textu převzaté normy

Vzhledem k vývoji terminologie v oblasti IT, se slovo management přeládá podle kontextu, ve kterém bylo použito. V tomto případě bylo slovo management v názvu této normy nahrazeno slovem řízení, což je v souladu s procesem vytváření názvů pro normy řady ČSN ISO/IEC 27000. U norem ČSN ISO/IEC 27001 a ČSN ISO/IEC 17799 (ISO/IEC 27002) bube úprava provedena při jejich revizi.

Termín **byznys (e-byznys)** je v prostředí tvorby norem a normalizačních dokumentů chápán jako série procesů, z nichž každý má zřejmý a srozumitelný účel; je realizovaná pomocí výměny informací, směrovaná ke vzájemně odsouhlasenému cíli, probíhá po určitý časový úsek a zahrnuje více než jednu stranu.

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 27004
Řízení bezpečnosti informací – Měření První vydání
2009-12

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, 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 27004 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie*, subkomise SC 27, *IT Bezpečnostní techniky*.

## 0 Úvod

### 0.1 Všeobecně

Tato mezinárodní norma poskytuje doporučení zaměřená na vývoj a používání metrik a měření za účelem hodnocení účinnosti zavedeného systému řízení bezpečnosti informací (ISMS) a účinnosti opatření nebo skupin opatření, jak je uvedeno v ISO/IEC 27001.

Doporučení se týkají politiky, řízení rizik bezpečnosti informací, cílů opatření, opatření, procesů a postupů a podporují proces revize, který napomáhá určit, zda některé procesy nebo opatření ISMS vyžadují změnu nebo zlepšení. Vždy je nutné mít na paměti, že měření účinnosti opatření samo o sobě nemůže zaručit úplnou bezpečnost.

Implementace těchto doporučení je předmětem programu měření bezpečnosti informací. Program měření bezpečnosti informací napomáhá vedení organizace při identifikaci a vyhodnocení nevyhovujících a neúčinných procesů a opatření ISMS a při stanovení priorit činností spojených se zlepšováním nebo změnou těchto procesů a/nebo opatření. Může rovněž pomáhat organizaci při demonstrování shody s ISO/IEC 27001 a poskytovat další důkazy pro procesy přezkoumání vedením organizace a pro řízení rizik bezpečnosti informací.

Tato mezinárodní norma předpokládá, že výchozím bodem pro rozvoj metrik a měření je dobré porozumění rizikům bezpečnosti informací, kterým organizace čelí, a že činnosti hodnocení rizik organizace byly provedeny správně (tj. na základě ISO/IEC 27005), jak to vyžaduje ISO/IEC 27001. Program měření bezpečnosti informací napomáhá organizaci poskytovat příslušným zainteresovaným stranám spolehlivé informace týkající se svých rizik bezpečnosti informací a stavu zavedeného ISMS k řízení těchto rizik.

Účinně zavedený program měření bezpečnosti informací zvyšuje důvěru zainteresovaných stran ve

výsledky měření a umožňuje zainteresovaným stranám využívat tyto metriky k uskutečňování neustálého zlepšování bezpečnosti informací a ISMS.

Po určitou dobu získávané výsledky měření umožní srovnávání pokroku při dosahování cílů bezpečnosti informací jako součásti procesu neustálého zlepšování ISMS organizace.

## 0.2 Manažerský přehled

ISO/IEC 27001 vyžaduje, aby organizace „prováděla pravidelná přezkoumání účinnosti ISMS a brala přitom v úvahu výsledky měření účinnosti" a „měřila účinnost opatření, aby si ověřila, že požadavky na bezpečnost byly splněny". ISO/IEC 27001 rovněž vyžaduje, aby organizace „definovala, jakým způsobem bude měřit účinnost vybraných opatření nebo skupin opatření, a specifikovala, jak mají být tyto metriky použity k vyhodnocení účinnosti opatření, aby závěry hodnocení byly porovnatelné a opakovatelné".

Přístup přijatý organizací ke splnění požadavků na měření, které jsou specifikovány v ISO/IEC 27001, se bude lišit v závislosti na počtu významných faktorů, včetně rizik bezpečnosti informací, kterým organizace čelí, její organizační velikosti, dostupných zdrojích a platných právních, regulačních a smluvních požadavcích. Pečlivý výběr a zdůvodnění použité metody ke splnění požadavků na měření jsou důležité pro zajištění toho, aby těmto činnostem ISMS nebyly, na úkor jiných, věnovány nadměrné zdroje. V ideálním případě mají být probíhající činnosti měření zahrnuty do běžných činností organizace s minimálními dodatečnými požadavky na zdroje.

Tato mezinárodní norma poskytuje základní doporučení pro naplnění požadavků měření, jak je specifikuje ISO/IEC 27001 a týkají se následujících činností:

a. vývoje metrik (tj. základních metrik, odvozených metrik a indikátorů);
b. zavedení a provozování programu měření bezpečnosti informací;
c. sběru a analýzy dat;
d. získání výsledků měření;
e. sdělení získaných výsledků měření příslušným zainteresovaným stranám;
f. použití výsledků měření jako faktorů přispívajících k rozhodnutím souvisejících s ISMS;
g. použití výsledků měření k identifikaci potřeb pro zlepšování zavedeného ISMS, včetně jeho rozsahu, politik, cílů, opatření, procesů a postupů; a
h. napomáhání neustálému zlepšování programu měření bezpečnosti informací.

Jedním z faktorů, který bude mít vliv na schopnost organizace provádět měření, je její velikost. Obecně řečeno, velikost a složitost podnikání v kombinaci s důležitostí bezpečnosti informací ovlivňují rozsah potřebného měření, jak z hlediska počtu metrik, které mají být vybrány, tak z hlediska četnosti sběru a analyzování dat. U malých a středních organizací bude dostačující méně komplexní program měření bezpečnosti informací, zatímco velké organizace budou zavádět a provozovat četné programy pro měření bezpečnosti informací.

Pro malé organizace může stačit jeden program měření bezpečnosti informací, zatímco pro velké organizace může existovat potřeba několika programů pro měření bezpečnosti informací.

Doporučení, která poskytuje tato mezinárodní norma, povedou k vytvoření dokumentace, která přispěje k prokázání toho, že účinnost opatření je měřena a hodnocena.

## 1 Předmět normy

Tato mezinárodní norma poskytuje doporučení pro vývoj a použití metrik a měření za účelem hodnocení účinnosti zavedeného systému řízení bezpečnosti informací (ISMS) a opatření nebo skupin

opatření, jak je uvedeno v ISO/IEC 27001.

Tato mezinárodní norma je aplikovatelná na všechny typy a velikosti organizací.

POZNÁMKA Tento dokument používá slovesné tvary pro vyjádření ustanovení (například „musí”, „nesmí ”, „měl by”, „neměl by”, „smí”, „nemusí”, „může” a „nemůže”), které jsou specifikovány ve směrnicích ISO/IEC, Část 2, 2004, příloha H. Viz také ISO/IEC 27000:2009, příloha A.