

# System řízení bezpečnosti informací – mezinárodní normy a zkušenosti z praxe<sup>1</sup>

**Doucek Petr**

Vysoká škola ekonomická  
katedra systémové analýzy  
W. Churchilla 4, 130 67 Praha 3  
doucek@vse.cz

**Novák Luděk**

ISACA CRC  
Španělská 2, 120 00 Praha 2  
novak@isaca.cz

## **Abstrakt**

*Řízení bezpečnosti informací a systém řízení bezpečnosti informací (ISMS – Information Security Management System) jsou v permanentní pozornosti všech manažerů, kteří během své práce přicházejí do syku s daty, zpracovávanými pomocí informačních a komunikačních technologií. Článek obsahuje strukturu a nejdůležitější složky mezinárodně uznávaných a používaných norem rodiny ISO/IEC 27000, dále obsahuje prognózu jejich dalšího rozšiřování tak, jak je nabízí ISO na další roky. Kromě toho poskytuje článek stručný přehled praktických zkušeností autorů a problémů, které se vyskytují při zavádění, provozu a auditu ISMS v organizacích.*

## **Abstract**

*ISMS (Information Security Management System) and information security are hot topics for security and executive managers who are managing processes of data working out by information and communication technology. This contribution contents structure of family international standard ISO/IEC 27000 and future expected development of it as well. It deals also with practical experience with ISMS improvement, operating and main problems connected to ISMS audit in the second part.*

## **Klíčová slova**

System řízení bezpečnosti informací, audit, normy ISO/IEC

## **Keywords**

Information security management system, audit, standards ISO/IEC

## 1 Úvod

Neustále pokračující rozšiřování informačních technologií do prakticky všech lidských činností a stejnou měrou rozšiřující se standardizace mají za následek, že řízení bezpečnosti informací získává charakter řízení služby nebo řízení atributu informačního systému. V minulosti byly návrhy postupů řízení bezpečnosti informací, navrhovaných organizací ISO, založeny na různých konceptech. V současné době, kdy dochází k propojování postupů mezi klasickými složkami integrovaného systému řízení organizace (rodinami norem ISO 9000 – systém řízení jakosti a ISO 14000 – systém řízení vztahu k okolí – environmentálního managementu), se řízení bezpečnosti informací zařazuje

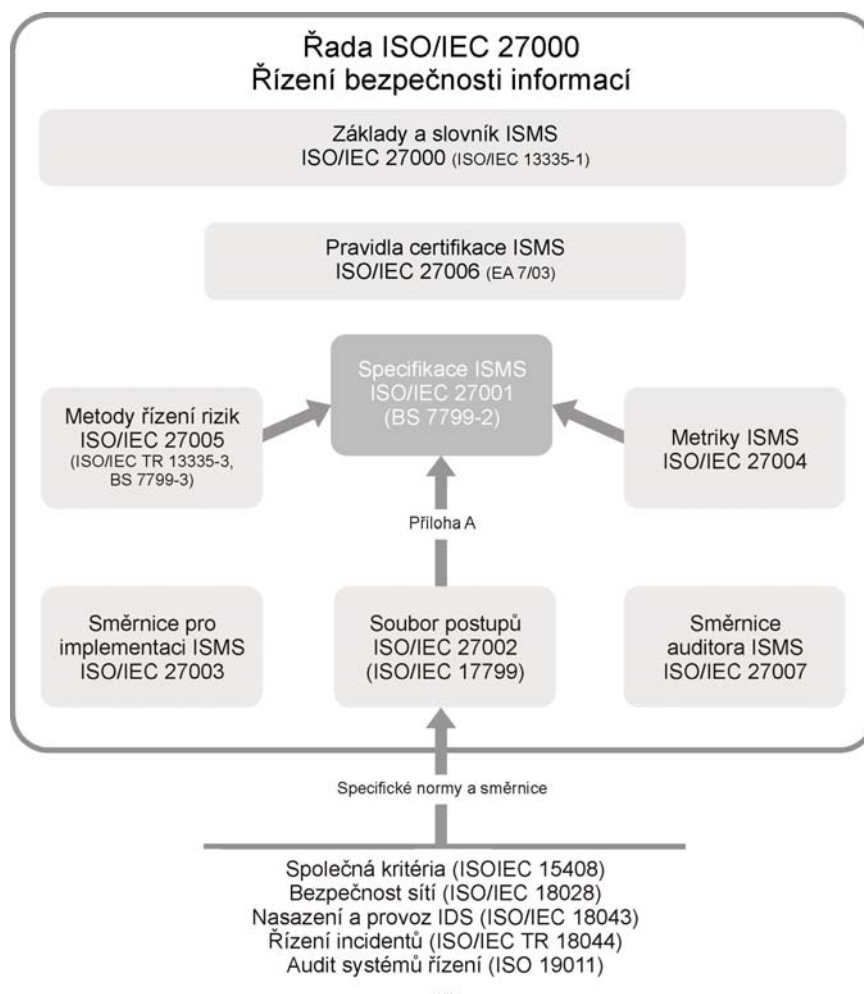
---

<sup>1</sup> Příspěvek byl zpracován v rámci řešení grantu GAČR – 201/07/0455 – Model vztahů mezi výkonností podnikání, účinností podnikových procesů a efektivností podnikových procesů.

mezi jeho složky. Všechny, takto definované systémy řízení, vycházejí ze společného konceptu řízení PDCA [1].

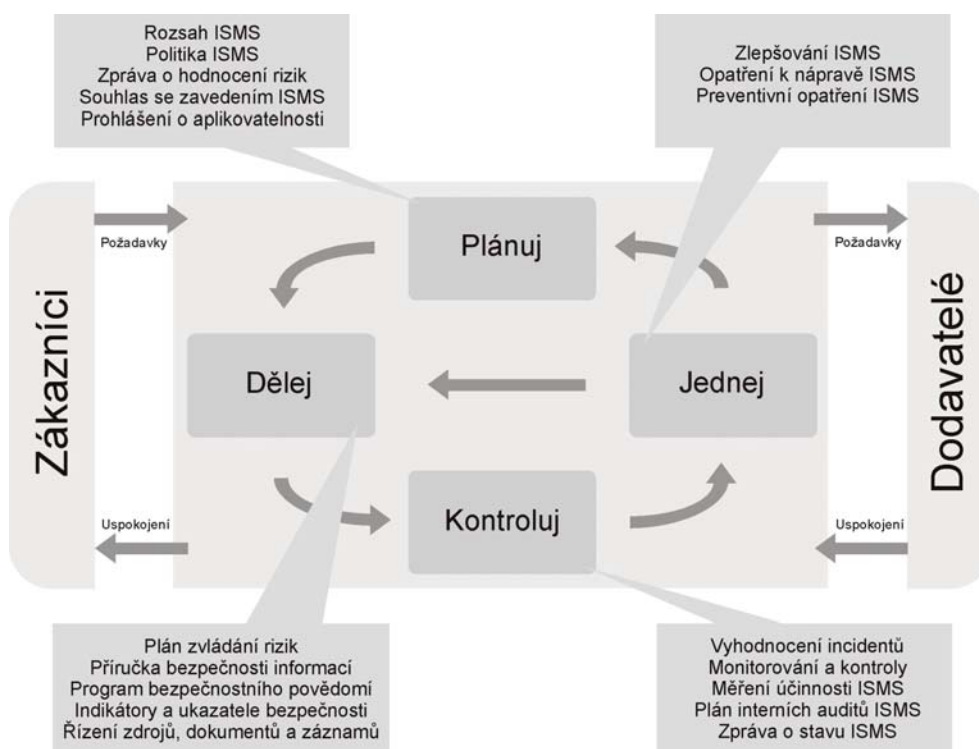
## 2 Mezinárodní normy pro řízení bezpečnosti informací

Na jaře roku 2005 organizace ISO ohlásila zavedení nové řady norem ISO/IEC 27000, která se bude věnovat problematice řízení bezpečnosti informací.



Obr.1 Koncept řady ISO/IEC 27000 pro řízení bezpečnosti informací

Nová řada norem pro řízení bezpečnosti informací ISO/IEC 27000 vychází ideově z konceptu PDCA a jejím základem jsou normy, jež jsou uvedeny na obrázku Obr.1. Podobně jako u jiných systémů řízení (např. ISO 9001, ISO 14001) je za jádro normalizace považována definice systému. V případě ISMS se tak stává klíčovým prvkem mezinárodní norma **ISO/IEC 27001:2005 – Information security management system – Requirements (Systém řízení bezpečnosti informací – Požadavky)**, která vychází ze známého britského standardu BS 7799-2 a která byla vydána v říjnu roku 2005. Nosné prvky, které norma vyžaduje pro budování ISMS, jsou vidět na následujícím obrázku.

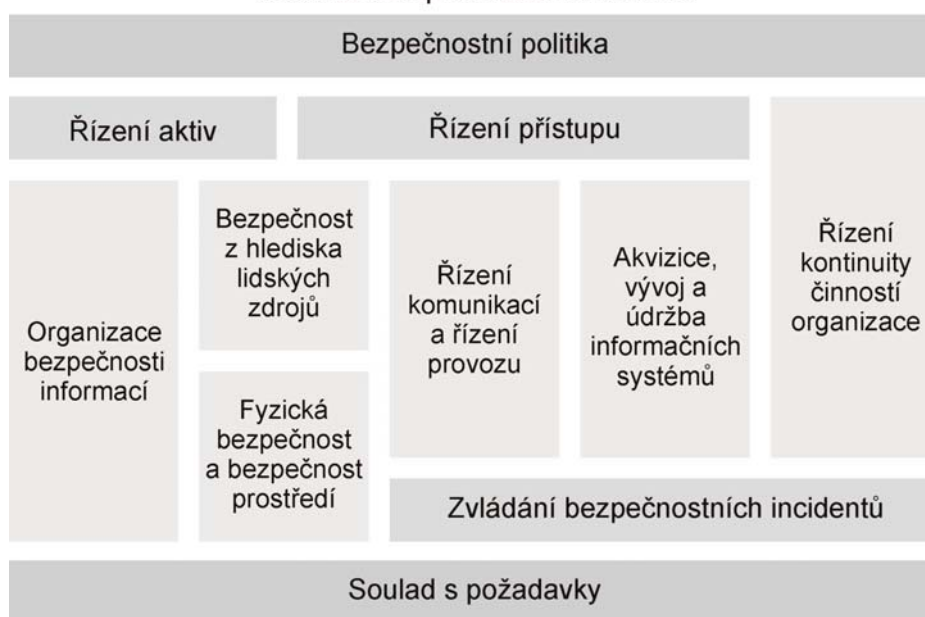


Obr.2 PDCA Model pro bezpečnost informací [4]

Druhou nejdůležitější normou této řady je norma **ISO/IEC 27002 – Code of practice for information security management (Soubor postupů pro řízení bezpečnosti informací)**, která obsahuje podrobný výklad vhodných bezpečnostních opatření. Tato norma byla vydána již v polovině roku 2005 a to ještě s označením ISO/IEC 17799:2005.

Ta obsahuje tzv. nejlepší praxi řízení bezpečnosti informací a doporučení normy definuje 133 bezpečnostních opatření, která jsou rozdělena do 11 oblastí (viz následující obrázek).

### Oblasti bezpečnosti informací



Obrázek 1: Oblasti bezpečnosti informací [5]

Na začátku roku 2009 byl spuštěn proces aktualizace obou norem (tj. ISO/IEC 27001 a ISO/IEC 27002), který bude uzavřen v roce 2011 vydáním nových verzí.

Od počátku roku 2007 se dalším přírůstkem řady ISO/IEC 27000 stala norma **ISO/IEC 27006 – Requirements for the accreditation of bodies providing certification of information security management systems** (Požadavky na akreditaci orgánů provádějících certifikaci systémů řízení bezpečnosti informací) [8]. Ta upřesňuje pravidla pro udělování certifikací ISMS a podle ní musí postupovat certifikační orgány, které služby spojené s certifikací ISMS poskytují. Norma nahradila již poměrně zastaralý evropský dokument EA 7/03 z roku 2000.

Poslední již vydanou je **ISO/IEC 27005:2008 – Information security risk management (Řízení rizik bezpečnosti informací)** [7], která podrobně definuje pravidla a postupy řízení rizik a nahradila již zastaralou normu ISO/IEC TR 13335-3. Kromě doporučení spojených s řízením rizik tato norma obsahuje i rozsáhlé katalogy hrozeb a zranitelností.

Novými příspěvky řady ISO/IEC 27000 by se v blízké budoucnosti mělo stát několik dalších mezinárodních norem. Mezi prvními by měla být norma **ISO/IEC 27004 – Information security management measurements (Měření účinnosti řízení bezpečnosti informací)** [6], která upřesní pravidla a způsoby využití nástrojů pro sledování účinnosti a efektivnosti zavedení a prosazení ISMS. Norma především předepisuje strukturu ukazatelů pro měření ISMS, upřesňuje pravidla pro definici a využívání bezpečnostních ukazatelů a doporučuje některé obecné ukazatele pro sledování účinnosti ISMS.

Mezi nimi by se měla objevit norma **ISO/IEC 27000 – Information security management system fundamentals and vocabulary (Základy a slovník systému řízení bezpečnosti informací)**, jejímž úkolem je sjednotit odborný slovník a definovat základní modely uplatňované při řízení bezpečnosti informací. Tato norma nahradí ISO/IEC 13335-1 a tím zanikne řada ISO/IEC 13335.

Novou normou bude **ISO/IEC 27003 – Information security management system implementation guidance (Směrnice pro implementaci systému řízení bezpečnosti informací)**. Ta bude obsahovat doporučení a návody, které jsou pro zavádění ISMS sice vhodné, nicméně nemají podobu závazných pravidel.

Posledním, v současnosti známým příspěvkem řady ISO/IEC 27000, by se měla stát norma **ISO/IEC 27007 – ISMS Auditor Guidelines (Směrnice auditora ISMS)**, která by měla upřesnit pravidla a postupy spojené s prováděním interních i externích auditů ISMS.

Během několika málo let by celá řada ISO/IEC 27000 měla obsahovat devět následujících dokumentů:

- ISO/IEC 27000 – Základy a slovník pro systém řízení bezpečnosti informací (vydání je plánováno na rok 2009),
- ISO/IEC 27001:2005 – Systém řízení bezpečnosti informací – Požadavky (vydáno v říjnu 2005 a jako ČSN v říjnu 2006),
- ISO/IEC 27002:2005 (dříve označovaná jako ISO/IEC 17799:2005) – Soubor postupů pro řízení bezpečnosti informací (vydáno v červnu 2005 a jako ČSN v srpnu 2006),
- ISO/IEC 27003 – Příručka pro zavádění systému řízení bezpečnosti informací (vydání je plánováno na rok 2009),
- ISO/IEC 27004 – Měření řízení bezpečnosti informací (vydání plánováno na rok 2009),
- ISO/IEC 27005:2008 – Řízení rizik bezpečnosti informací (vydáno v červnu 2008 a jako ČSN v tisku),
- ISO/IEC 27006:2007 – Pravidla certifikace ISMS (vydáno v únoru 2007),
- ISO/IEC 27007 – Směrnice auditora ISMS (vydání je plánováno na rok 2010),
- ISO/IEC TR 27008 – Příručka pro audity o opatřeních ISMS (vydání je plánováno na rok 2012).

Kromě nich jsou v současné době připravovány další dokumenty této řady. Jejich názvy jsou velmi často pracovní, a proto jsou uvedeny pouze v anglickém originále. Jedná se o následující normy, které by se měli věnovat doporučení a výkladu ISMS pro specifické použití:

- ISO/IEC 27010 – Information security management for inter-sector communications (vydání je plánováno na rok 2011),
- ISO/IEC 27011:2008 – Information security management guidelines for telecommunications,
- ISO/IEC 27012 – Information security management guidelines for e-government services (vydání je plánováno na rok 2011),
- ISO/IEC 27013 – Guidance on the integrated implementation of 20000-1 and 27001 (realizace projektu je zvažována),
- ISO/IEC 27014 – Information security governance framework (realizace projektu je zvažována),
- ISO/IEC 27015 – Information security management guidelines for financial and insurance services (realizace projektu je zvažována),
- ISO/IEC 27799:2008 - Security Management in Health using ISO/IEC 27002.

Kromě doporučení pro specifické použití ISMS jsou připravovány normy, které se budou podrobněji věnovat určitým bezpečnostním okruhům. Jedná se především o následující normy:

- ISO/IEC 27031 – Specification for ICT Readiness for Business Continuity (tato norma bude navazovat na britské normy BS 25999 – Business Continuity Management resp. BS 25777 Information and communication technology continuity management – Code of Practice, která byly postupně vydány v letech 2006 až 2008)
- ISO/IEC 27032 – Guidelines for cybersecurity,
- ISO/IEC 27033 – IT network security (nahradí všechny díly ISO/IEC 18028),
- ISO/IEC 27034 – Application security,
- ISO/IEC 27035 – Information Security Incident Management (nahradí ISO/IEC TR 18044).

Směr rozvoje bezpečnostních standardů je patrný ze vzniku dalších rodin norem. Jedná se o rodinu norem ISO/IEC 29000, která se zabývá problematikou **soukromí (Privacy)** a o rodinu norem ISO/IEC 24000 a ISO/IEC 19000, které se zabývají novými trendy v řízení přístupů k aktivům informačních systémů – **biometrikou (Biometrics)**.

Další, nově vznikající, rodinou norem je ISO/IEC 31000, jejímž obsahem je řízení rizik na obecné úrovni. S ní potom musí být harmonizovány speciální normy pro řízení rizik jako např. ISO/IEC 27005.

Všechny tyto rodiny norem pak mají vazby na ostatní rodiny norem, které vymezují integrovaný systém řízení ISO 9000 a ISO 14000.

### 3 Zkušenosti s budováním systému řízení bezpečnosti informací

V následujícím textu se budeme podrobněji zabývat zkušenostmi se zaváděním normy ISO/IEC 27001, podle které je možné provádět certifikaci systému řízení bezpečnosti informací. Shromážděné zkušenosti byly z části získány při provádění auditů ISMS, které jsou základem pro udělení certifikace a z části byly získány sledování různých názorů v českém prostředí.

#### 3.1 Nedostatečná kompetence odborníků na ISMS

Jednou z nejvíce problematických oblastí je **odborná kompetence pracovníků**, kteří jsou zavedením ISMS pověřeni. Je potřeba zdůraznit, že vlastní norma ISO/IEC 27001 obsahuje pouze ty nejnужnější požadavky, které je potřeba naplnit. Podrobné vysvětlení, co tyto požadavky v praxi znamenají, v normě nalézt nelze a řada souvislostí bývá pro čtenáře normy skrytá. Zde je prostor pro dobrá školení, ale i těch je v České republice poskromnu.

Vzpomínáme si na jednu prezentaci odborníka z USA a překvapilo nás s jakou samozřejmostí hovořil o tom, že ještě před rozhodnutím o zavedení ISMS v bance, kde pracoval, byl tým odborníků vyslán do Londýna na školení BSI. Sám si toto školení chválil, protože mu dovolilo pochopit souvislosti při zavádění ISMS a, jak sám uvádí, bylo základem pro úspěšné dokončení celého projektu.

A ještě jedna poznámka. Někdy je vhodné si školením prověřit vhodnost poradce, kterého jste si vybrali pro zavedení ISMS. Když nebudete spokojeni se školením a tento partner vás nepřesvědčí o svých schopnostech, je nejvyšší čas se znovu porozhlédnout po někom lepším. Za tuhle zkušenost se školení určitě vyplatí.

### 3.2 Nedostatky při určení rozsahu ISMS

Další oblastí nedostatků je stanovení rozsahu a hranic, ve kterých je ISMS realizováno. Mohlo by se zdát, že nejjednodušším přístupem k řešení ISMS je stanovení jeho rozsahu na celou organizaci. Tím si sice usnadníme vymezení rozsahu systému, ale na druhou stranu si výrazně zkomplikujeme celý proces jeho zavádění.

Velmi málo se dnes pracuje s představami a plány o **řízení rozsahu ISMS**. V podstatě jde o to zvolit si vhodnou část organizace, ve které bude ISMS zavedeno s tím, že na základě zkušeností z takového zavedení bude jeho rozsah dále rozvíjen a upravován. Tento přístup dovoluje organizaci zjednodušit složitost zavádění ISMS. Zároveň přináší možnost pro pracovníky organizace „zvyknout“ si na fungování ISMS a získáním reálných zkušeností s jeho implementací a provozem významně zjednodušuje jeho další rozvoj.

### 3.3 Nedostatky při řízení rizik

Vlastní kapitolou v nasazování ISMS je **řízení rizik**, které je základem každého účinného ISMS. Z praxe se nám vybavují dvě dominantní zkušenosti. V prvním případě organizace identifikovala **jediné riziko**, které označila za „ohrožení bezpečnosti informací“. Druhá zkušenost byla prezentována jako konkurenční výhoda jednoho poradce, který se snaží „**věnovat i malým rizikům**, jejichž zvládnutí není tak náročné“.

Oba dva přístupy jsou v praxi nepoužitelné. Smyslem a cílem řízení rizik je hledání priorit při budování ISMS. Z jednoho identifikovaného rizika žádnou prioritu nevyčteme a malá rizika prioritami organizací opravdu nejsou. Cílem řízení rizik je vyhledání velkých rizik a jejich zvládnutí tak, aby nevedly k přímému ohrožení organizace. Zájem o malá rizika je pouhým plýtváním času, pozornosti i peněz.

Z pohledu certifikačního auditora je zajímavé, že stav řízení rizik hodně napovídá o celkovém fungování ISMS v organizaci. U organizací, která dobře identifikují svoje rizika, dochází i k jejich účinnému zvládnutí a tím je zajištěno účelná a účinná funkčnost ISMS. Organizace, které nemají přesnou představu o rizicích, kterým pomocí ISMS chtějí čelit, nejsou obvykle ISMS ani účinně zavést.

Z praktických zkušeností můžeme doporučit, aby ISMS na **počátku pracovalo s desítkami rizik** (cca 20 až 30 identifikovaných rizik). Tento počet je dán schopností manažera ISMS dobře se orientovat v dané množině rizik, což je v úvodních fázích ISMS zásadní. Teprve **s nabytými zkušenostmi je přijatelné „komplikovat“ si situaci i život navyšováním počtu rizik**.

### 3.4 Nedostatky v prohlášení o aplikovatelnosti

**Prohlášení o aplikovatelnosti** je divný pojem, že? V rámci poslední aktualizace normy ISO/IEC 27001 se hojně diskutovalo o tom, jak tento termín nahradit něčím srozumitelnějším. A výsledek. I nadále se budeme bavit o nesrozumitelném prohlášení o aplikovatelnosti, protože na toto označení si už část lidí zvykla.

Co se tedy za prohlášením o aplikovatelnosti skrývá? Jedná se o dokument, který je základem ISMS, protože jeho cílem je jasně stanovit a odůvodnit opatření, která jsou v ISMS zavedena a která zavedena

nejsou. Naplníme-li tuto představu normy, vznikne důležitá **mapa mezi identifikovanými riziky a realizovanými bezpečnostními opatřeními**. Což je důvod, proč je tento dokument tak důležitý.

O jeho významu svědčí i skutečnost, že při certifikačním auditu tento dokument usnadňuje orientaci auditora v novém, často zcela neznámém prostředí. Podotýkáme, že úspěšná forma zpracování prohlášení o aplikovatelnosti se odráží v dobré a rychlé orientaci zejména externího auditora v daném ISMS při běžném i certifikačním auditu.

### 3.5 Nedostatky v dokumentaci ISMS

Při tvorbě dokumentace ISMS se často projevuje tendence k přílišné citaci požadavků normy bez vysvětlení, co určité skutečnosti znamenají pro danou organizaci a kdo je případně odpovědný za realizaci stanovených požadavků.

Je potřeba si uvědomit, že pro správné fungování ISMS je důležité systematické prosazování a realizace daných zvyklostí. Dokumentace je důležitým nástrojem, který by měl účinně pomáhat při prosazování zvolených bezpečnostních opatření. Nelze ale opomíjet skutečnost, že pro bezpečnost podstatným přínosem je situace, kdy všichni uživatelé umí bezpečně pracovat s hesly, ne pouhá existence dokumentu, který tuto problematiku popisuje. Jinými slovy existence rozsáhlé dokumentace automaticky nevede k praktické realizaci daných pravidel a často je vhodné praktické prosazování podpořit účinným školením o výkladu pravidel ISMS.

### 3.6 Nedostatky při měření účinnosti ISMS

Složitou oblastí pro praktickou realizaci se jeví i měření účinnosti ISMS, které bylo zásadní novinkou při vydání ISO/IEC 27001 v roce 2005. Toto je velmi komplikovaná a nová problematika, jejíž zvládnutí se projeví hlavně při prohlubování účinnosti ISMS tj. měření účinnosti by organizaci mělo dovolit realizovat ISMS s vyšší mírou bezpečnosti při nižší náročnosti na spotřebu zdrojů.

Z praktického hlediska je důležité s měřením nějak začít. Zde platí dvě důležité poučky. První se skrývá v přísloví „Méně někdy bývá více“. Zejména v počátku je důležité připravit méně metrik, které se soustředí na prioritní oblasti ISMS. A větší rozsah metrik připravit až po získání základních zkušeností. Ty jsou pro úspěšné měření nenahraditelné.

Druhou poučkou je omezení snahy o získávání absolutních ukazatelů. Pro kvalitní rozhodování je postačující relativní představa. Na vybrání nejvyššího žáka ve třídě není zapotřebí složitě používat centimetr. Stačí výšku žáků jednoduše porovnat s tím, že jistá míra nepřesnosti je tolerovatelná. A lze jen připomenout, že každé zvyšování přesnosti je spojeno s vyššími náklady.

Měření účinnosti ISMS má na rozvoj ISMS vliv i v tom, že při definování metrik jste nuceni definovat očekávaný výsledek měření. Již toto zamyšlení může vést k zajímavým podnětům. Po ukončení měření dostáváte možnost porovnávat očekávané a skutečné hodnoty. Vyhodnocení rozdílů opět vede k podnětům, které vám dovolí ISMS dále rozvíjet správným a žádoucím směrem.

### 3.7 Nedostatky při řízení záznamů ISMS

**Záznamy** jsou důležitým prvkem ISMS neboť prokazují, že daná činnost byla skutečně provedena. Například když existuje pravidlo, že se každý týden provádí zálohování serveru, musí být za rok shromážděno 52 záznamů o tom, jak tento proces každý týden dopadl.

Z hlediska ISMS **není důležité, zda bude záznam připraven písemně či elektronické formě**. Podstatně důležitější je schopnost odpovědných pracovníků všechny záznamy najít. Taktéž je důležité v rámci přezkoumání ISMS vyhodnotit, co tyto záznamy obsahují a jak vypovídají o zkoumaném opatření (procesu).

### 3.8 Nedostatky při komunikaci s auditory ISMS

Poslední oblastí nedostatků při certifikaci ISMS je způsob **komunikace s externími auditory**. Cílem či lépe řečeno očekávání těchto auditorů bývá **nalezení shody s danou normou**, ale ne vždy jsou na

tuto skutečnost auditované organizace dobře připraveni. Z toho pohledu by si odpovědní manažeři měli pohlídat schopnost organizace prezentovat shody ISMS s příslušnou normou – v tomto případě ISO/IEC 27001.

Dalším omylem auditovaných organizací je skutečnost, že auditoři mohou pracovat s domněnkami. Argumentace „... ale na mezinárodní odborné konferenci renomovaný expert prohlásil, že ..., a proto my jsme ...“ není vůbec relevantní tvrzení pro auditory. Ti pracují pouze s definovanými pravidly, což je auditovaná norma ISO/IEC 27001 nebo pravidla pro provádění auditů jako ISO/IEC 27006 či ISO/IEC 17021. Individuální výroky mezi uznávaná kritéria auditorů nepatří a obáváme se, že ani nikdy patřit nebudou.

## 4 Závěr

Přestože rodina norem IOS/IEC 27000 neslouží k řízení bezpečnosti informací dlouho, představuje, zejména v evropském prostředí, významný nástroj pro řízení jak pro manažery bezpečnosti, tak pro liniové manažery organizací. Rodina norem nemá ještě zdaleka svou konečnou podobu a článek poskytuje jak přehled současných vydaných norem, tak i perspektivy jejího rozvoje tak, jak jsou prezentovány organizací ISO. Nástroje a přednosti norem ISO/IEC 27000 jsou často využívány v praxi, ale ne vždy je jejich nasazení a prosazování bezproblémové. Protože zavádění ISMS patří mezi velmi složité procesy, správnou interpretaci doporučení, uvedených v normách, je dobré konzultovat nejen s externími odborníky, ale zejména s externími auditory ISMS, kteří mají zkušenosti s implementací i auditem systému řízení bezpečnosti informací v mnoha různých prostředích i organizacích. Výčet problémů, uvedených v tomto článku, není konečný, ale představuje špičku ledovce nejzávažnějších problémů a otázek spojených se zaváděním ISMS.

## 5 Literatura

- [1] DEMING, W., E.: Out of the Crisis, MIT, The MIT Press, Cambridge, MA, 1982, DEMOP 0-262-54115-7
- [2] DOUCEK, P., NOVÁK, L., SVATÁ, V.: Řízení bezpečnosti informací, Professional Publishing 2008, ss. 239, ISBN 978-80-86946-88-7
- [3] DOUCEK, P., NOVOTNÝ, O.: Standardy řízení podnikové informatiky, Standardy řízení podnikové informatiky. E+M. Ekonomie a Management, 2007, roč. X, č. 3, s. 132–146. ISSN 1212-3609.
- [4] ČSN ISO/IEC 27001:2006, Informační technologie – Bezpečnostní techniky – Systém managementu bezpečnosti informací – Požadavky.
- [5] ČSN ISO/IEC 27002:2006, Informační technologie – Soubor postupů pro management bezpečnosti informací.
- [6] ISO/IEC 27004, Information technology – Security techniques – Information security management measurements.
- [7] ISO/IEC 27005: 2008 – Information technology – Security techniques – Information security risk management
- [8] ISO/IEC 27006: 2007 – Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management system
- [9] ISO/IEC 27007 – Information technology – Security techniques – Guidelines for security management systems auditing (working draft)
- [10] ČSN ISO/IEC 20000:2006, Informační technologie – Management služeb.

[11] ŠABATOVÁ, I.: Systémy správy identity a řízení přístupu, In: VOŘÍŠEK, Jiří (ed.). Systems Integration 2005. Praha : KIT VŠE, 2005. ISBN 80-245-0895-8.

**Internet:**

[www.iso.org](http://www.iso.org) – 12.2. 2009

[www.isaca.org](http://www.isaca.org) – 12.2. 2009