SECURITY 2011

19. ročník konference o bezpečnosti v ICT

Co je a co není implementace ISMS dle ISO 27001 a jak měřit její efektivnost.

Ing. Václav Štverka, CISA

Versa Systems s.r.o.

OBSAH

- Co je implementace ISMS dle ISO 27001
- Proč měřit ISMS?
- Zdroje pro měření ISMS
- Co znamená měřit efektivnost ISMS?
- Metody měření
- Nástroje pro měření ISMS
- Závěr

Co je implementace ISMS dle ISO 27001?

- Zavedení **řízení** ochrany informačních aktiv v celém jejich životním cyklu, které jsou důležité pro organizaci, na základě **procesního** přístupu
- **Integrace** bezpečnostních procesů **napříč všemi procesy** v organizaci
- Implementace vybraných **opatření k řízení rizik** na základě výsledků hodnocení rizik jako součást **managementu rizik**
- Aplikace **P-D-C-A** cyklu do všech „bezpečnostních procesů a činností“ napříč organizací

Co je implementace ISMS dle ISO 27001?

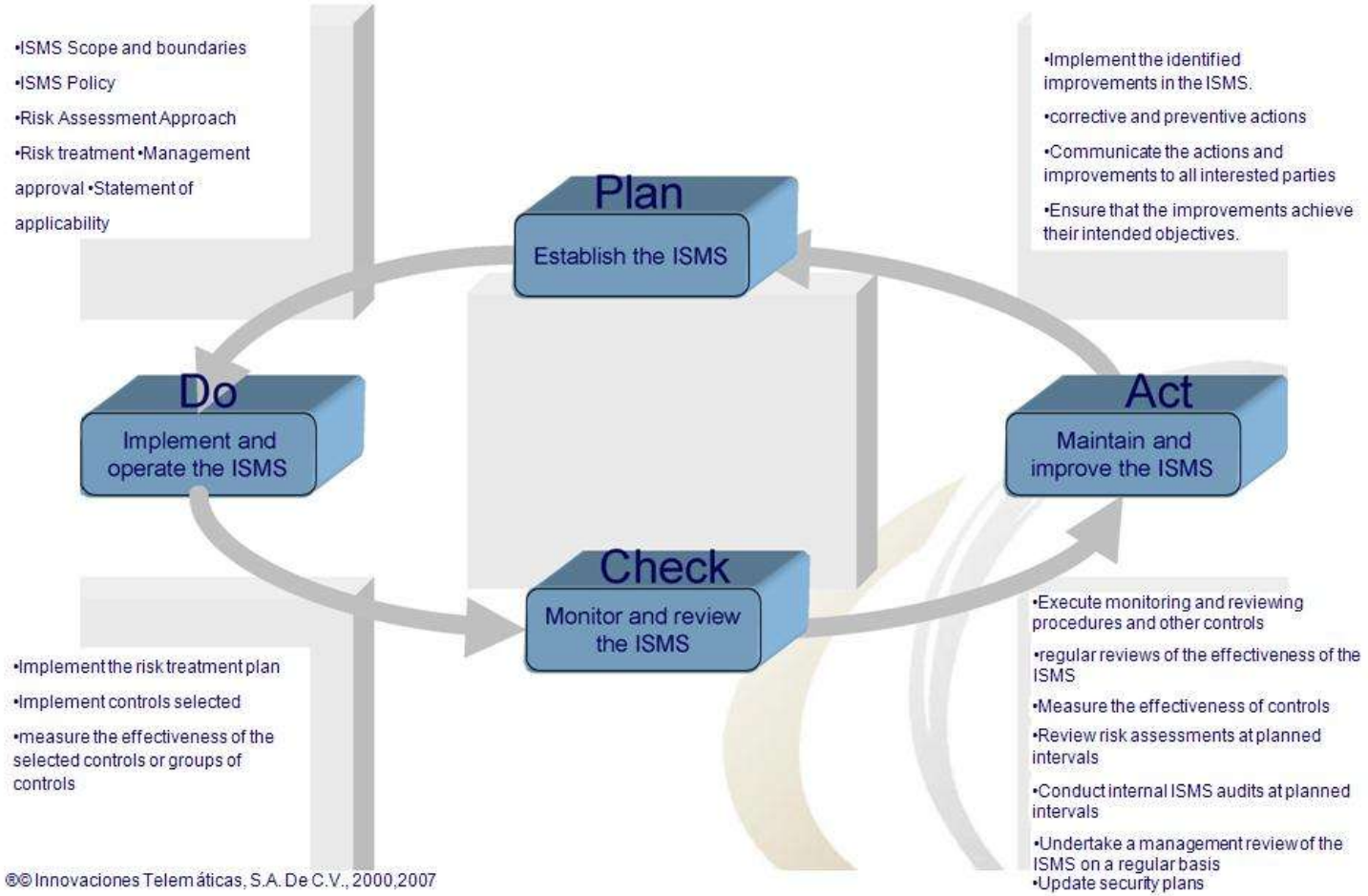
- Pro systematické řízení bezpečnosti informačních aktiv se dnes organizace rozhodují implementovat ISMS dle ISO/IEC 27001

- ISMS je, stejně jako ostatní systémy řízení (ISO 9001, ISO 14001, ISO 20000 aj.), založen na definování a řízení procesů týkajících se informační bezpečnosti.

- U všech systémů založených na procesech musíme tyto procesy monitorovat a měřit, abychom zajistili jejich efektivitu

- **Platí, že:** Co nemůže být měřeno, nemůže být efektivně řízeno!!

Information Security



Co není implementace ISMS dle ISO 27001?

Implementací ISMS **NENÍ**:

- Instalace Firewalu nebo antiviru
- Instalace technologických prostředků realizovaná útvarem IT
- Projektem, který se **netýká** vrcholového vedení
- Investování do bezpečnostních opatření bez zdůvodnění oprávněnosti investic na základě provedené analýzy rizik
- ….atd

Měření efektivnosti ISMS dle ISO 27001?

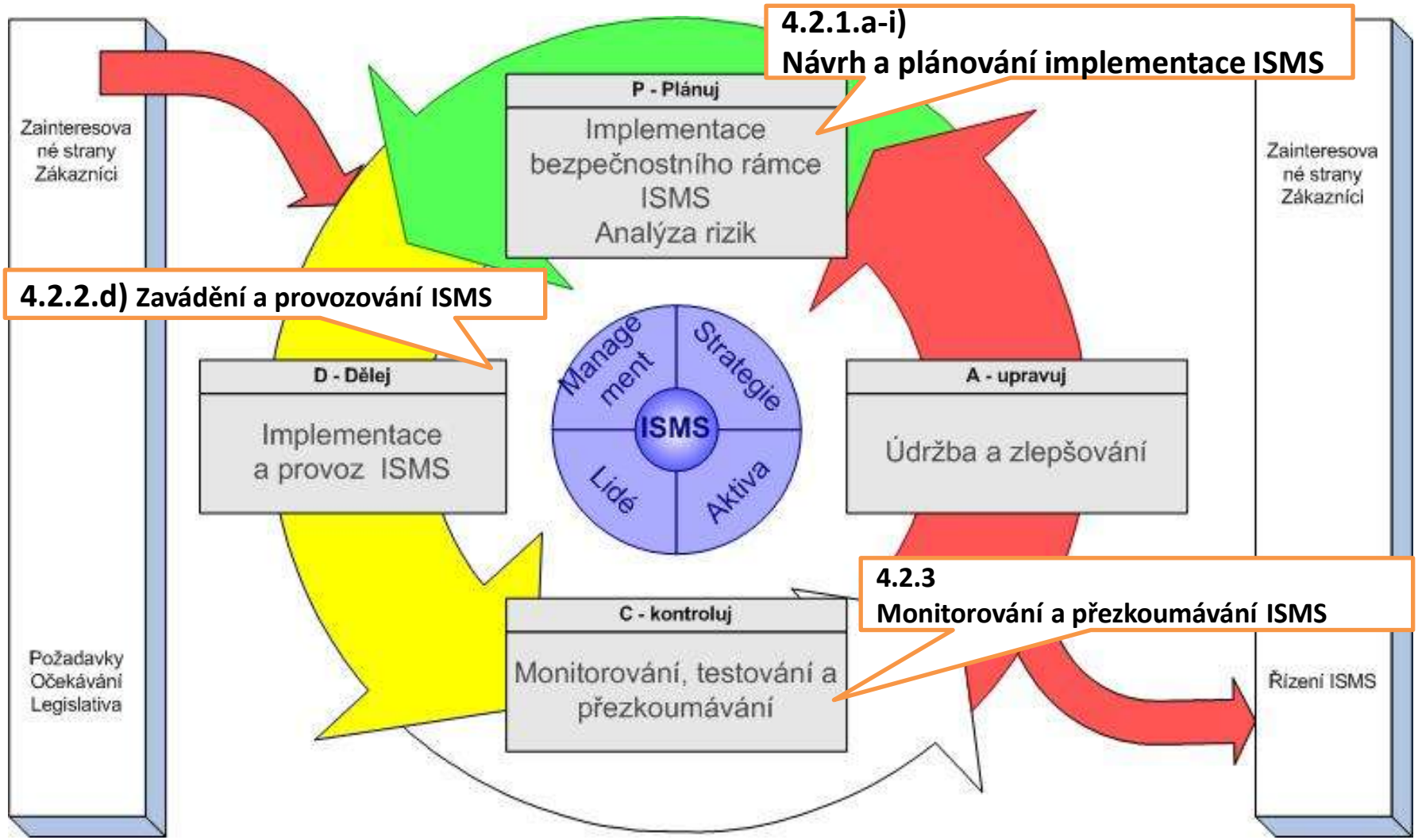
PROČ MĚŘIT ISMS?

Měření efektivnosti ISMS dle ISO 27001?

V ISMS (ale i v ostatních systémech řízení) platí ZÁSADA:

- Abychom byli schopni úspěšně implementovat ISMS a dlouhodobě jej efektivně provozovat a zlepšovat, musíme měřit ISMS procesy a přijatá opatření
- **Co nemůže být měřeno, nemůže být efektivně řízeno!!**
- Pokud neměříme výsledky práce bezpečnostních expertů, nemůžeme říci, zda jsou úspěšní.
- Pokud neměříme efektivnost procesů ISMS, nemůžeme říci, zda dosahují předpokládaných (plánovaných) hodnot

27001 - (PDCA) model v ISMS



Požadavky na monitorování a měření

4.2.2 Zavádění a provozování ISMS (ISO 27001)

- **Čl. (4.2.2 (d)) -** Určit jakým způsobem se bude měřit účinnost vybraných opatření nebo skupin opatření a stanovit jakým způsobem budou tato měření použita k vyhodnocení účinnosti opatření tak, aby závěry hodnocení byly porovnatelné a opakovatelné

Jinými slovy to znamená:

- Definovat soubor měření a zvolit soubor metod pro měření účinnosti implementovaných opatření – po implementaci a dále v pravidelných intervalech
- Specifikovat, jak měřit účinnost vybraných opatření a skupin opatření
- Specifikovat, jak tato měření budou účinná k hodnocení účinnosti opatření
- Zajistit porovnatelné a opakovatelné výsledky těchto měření

Požadavky na monitorování a měření

4.2.3.a-f Monitorování a přezkoumávání – ISO 27001

- Monitorovat, přezkoumávat a zavést další opatření….
- Pravidelně přezkoumávat účinnost ISMS s ohledem na výsledky bezpečnostních auditů, incidentů, výsledků měření účinnosti opatření, návrhů a podnětů….
- Měřit účinnost zavedených opatření……
- V plánovaných intervalech provádět přezkoumání hodnocení rizik…..
- Provádět interní audity ISMS v plánovaných intervalech…
- Pravidelně přezkoumávat ISMS na úrovni managementu organizace…..

Měření efektivnosti ISMS dle ISO 27001?

ZDROJE PRO MĚŘENÍ ISMS?

Zdroje pro měření ISMS

- Nejznámější návody standardy a postupy, kde získat informace o tom, jak měřit efektivnost ISMS:
  - ISO/IEC 27004 (ČSN ISO 27004) – Information security management Measurements
  - BIP 0074 - Průvodce měřením účinnosti ISMS implementace
  - „Security Metrics Guide for Information Technology systems“ (2003) NIST Special publication 800-55

ISO/IEC 27004

ISO/IEC 27004:2009 Information security management Measurements

ČSN ISO/IEC 27004:2011

Doporučení pro vývoj a použití metrik a měření pro hodnocení účinnosti ISMS a měření opatření uvedených v ISO 27001 příl. A

ISO/IEC 27004

- Cílem normy ISO/IEC 27004 bylo vytvořit základní rámec pro management měření informační bezpečnosti, který se zaměřuje na to, jak měřit **EFEKTIVITU** implementace, provozu a zlepšování ISMS (procesů a opatření)

- Návod ***Co měřit, jak měřit a kdy měřit***

- Norma vyšla v ČR 1.2. 2011 (ČSN ISO/IEC 27004)

ISO/IEC 27004

ČSN ISO/IEC 27004:2011

Norma dává doporučení, jak splnit požadavky měření dle ISO/IEC 27001, které se týkají 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;

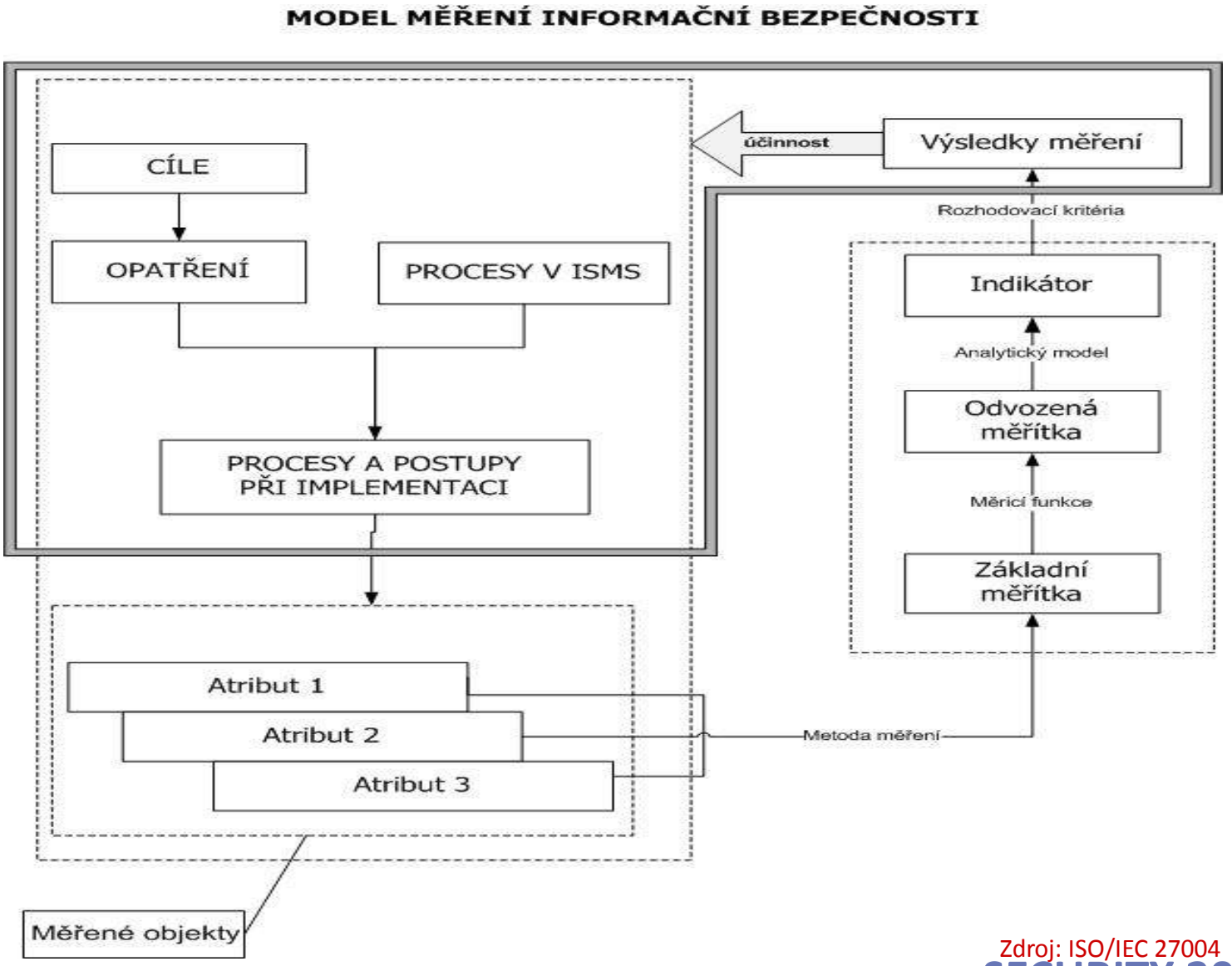
g) použití výsledků měření k identifikaci potřeb pro zlepšování zavedeného ISMS, včetně jeho rozsahu, politik, cílů, opatření, procesů a postupů; a

h) napomáhání neustálému zlepšování programu měření bezpečnosti informací.

Zdroje pro měření ISMS

- ISO/IEC 27004 - poskytuje doporučení pro vývoj a používání metrik a pro měření účinnosti zavedeného systému řízení bezpečnosti informací (ISMS) a účinnosti opatření, jak je požadováno v ISO/IEC 27001.
- Norma obsahuje následující hlavní sekce:
  - Přehled o měření informační bezpečnosti (5)
  - Odpovědnosti managementu (6)
  - Vývoj metrik a měření (7)
  - Provádění měření (8)
  - Analýza dat a reportování o výsledcích měření (9)
  - Vyhodnocování a zlepšování programu měření bezpečnosti informací (10)
- Příloha A – příklad šablony karty metrik
- Příloha B – příklady metrik

Zdroje pro měření ISMS



Zdroj: ISO/IEC 27004

Měření efektivnosti ISMS dle ISO 27001?

CO ZNAMENÁ MĚŘIT EFEKTIVNOST ISMS?

Jak zjistíme míru bezpečnosti?

Management – Otázka:

„Zlepšily změny, které byly implementovány a stály nemalé finanční prostředky, naši bezpečnostní situaci?“

Bezpečnostní ředitel:

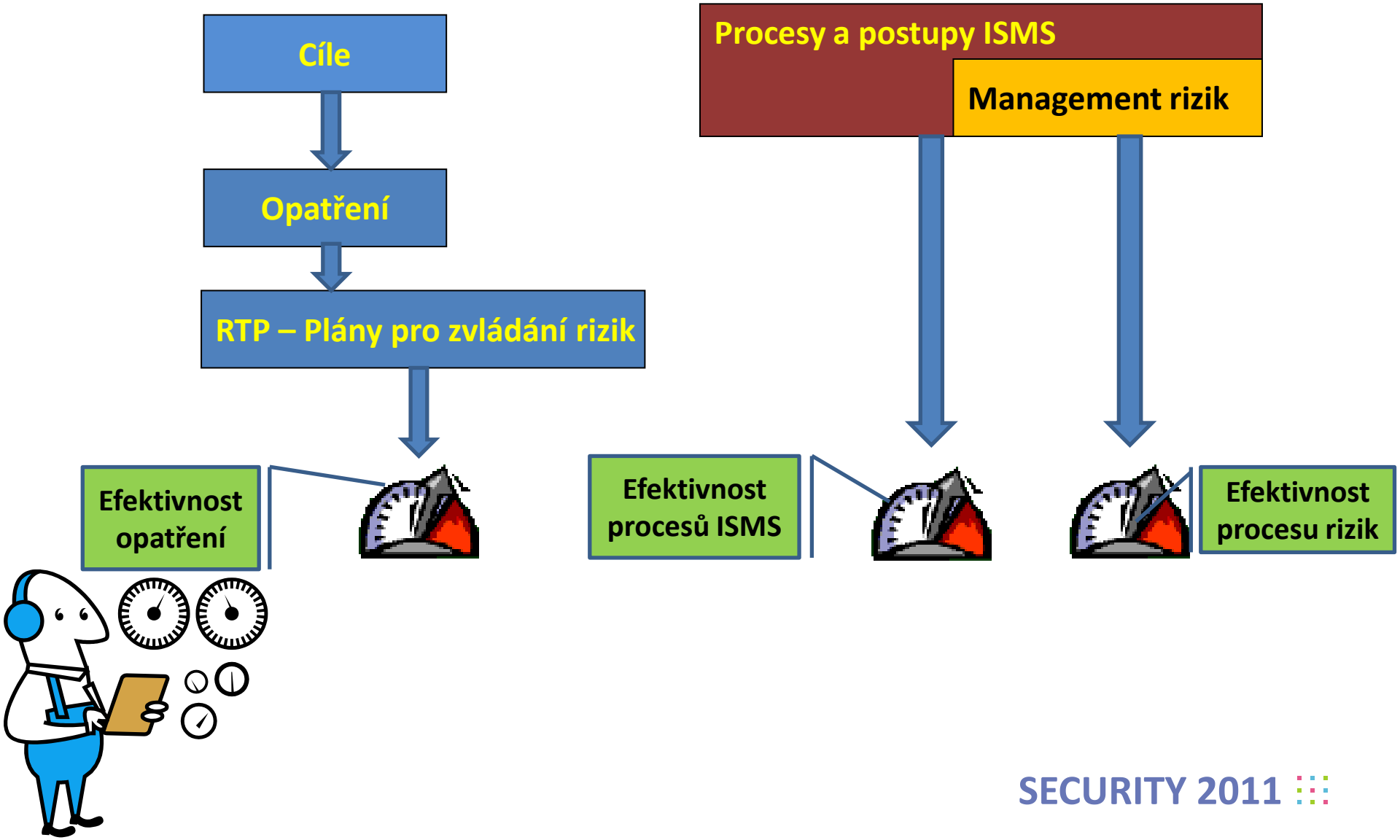
- ***Bez metrik:***

  „Ano, jistě, zlepšili jsme zabezpečení, používáme nové technologie“ (o kolik jsme bezpečnější? Jak mi to dokážete?)

- ***S metrikami:***

  „Ano. Podívejte se na naše hodnoty rizik před implementací opatření a po provedení navrhovaných změn. Nyní dosahují hodnoty o 25 bodů menší. Bezpochyby, změny redukovaly naše bezpečnostní rizika, náš **bezpečnostní index se zlepšil**).

Měření efektivnosti ISMS dle ISO 27001?



Měření efektivnosti ISMS

Měření stavu (pokroku) při implementaci ISMS:

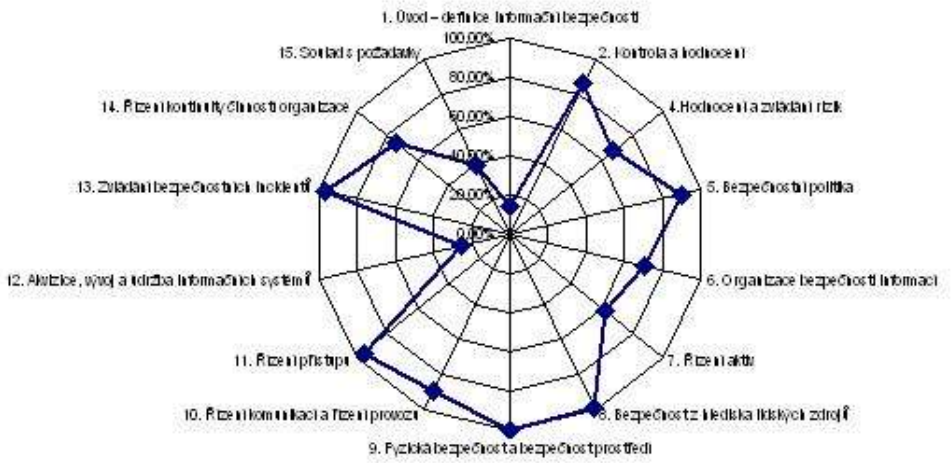
- Zjistit pokrok při implementaci ISMS, např. kolik dokumentů je již vypracováno nebo kolik opatření je již realizováno
- Zjistit pokrok ve výkonnosti ISMS (např. porovnáním tohoto ukazatele v čase)
- Jiné možnosti měření pokroku (vyzrálosti) např. model vyzrálosti (CMM)

Měření efektivnosti ISMS

Název kapitoly	Cílový stav	Metrika	Stav						
			Neexistuje	Zadání (1)	Definováno (2)	Navrženo (3)	Schváleno (4)	Řízeno (4)	Koeficient
	souladu s autorským zákonem, zajištění kompatibility a kontinuity vývoje, stanovení odpovědnosti	Definice pravidel externí správy (outsourcing)	0	1	2	3	4	4	100,00%
10. Řízení zachování kontinuity provozu	1. Dokumentovaný, platný a aktualizovaný havarijní plán pro ICT 2. Dokumentované zásady bezpečnosti a provozní předpisy - pravidla pro řešení krizových situací a havárií týkajících se ICT a ostatních s ohledem na jejich provázanost, koordinace činností 3. Dokumentované kritické procesy závislé na ICT zohledněné v havarijním plánu ICT	Havarijní plán ICT	0	1	2	3	4	2	85,71%
		Definice pravidel testování a aktualizace Havarijního plánu	0	1	2	3	2		57,14%
		Priority procesů dle požadavků na kontinuitu provozu	0	1	2	2			35,71%
11. Řízení shody se zákonnými požadavky	1. Zpracování postupu kontroly shody s legislativními požadavky	Definice postupu kontroly shody s legislativními požadavky (atestace, certifikace, ISVS, ochrana osobních údajů)	0	1	2	3	2	2	71,43%

Ukázka měření úrovně informační bezpečnosti

Název kapitoly	Koeficient
1. Úvod – definice informační bezpečnosti	14,29%
2. Kontrola a hodnocení	85,71%
4.Hodnocení a zvládání rizik	67,86%
5. Bezpečnostní politika	89,29%
6. Organizace bezpečnosti informací	70,13%
7. Řízení aktiv	61,43%
8. Bezpečnost z hlediska lidských zdrojů	98,41%
9. Fyzická bezpečnost a bezpečnost prostředí	100,00%
10. Řízení komunikací a řízení provozu	88,10%
11. Řízení přístupu	96,29%
12. Akvizice, vývoj a údržba informačních systém	25,89%
13. Zvládání bezpečnostních incidentů	97,14%
14. Řízení kontinuity činností organizace	74,29%
15. Soulad s požadavky	39,29%



Měření efektivnosti ISMS

2. Všeobecný stav rizik ve společnosti

Ref	Popis	Odhad rizik					Trend	Komentář
		1	2	3	4	5		
1	Zákony na ochranu duševního vlastnictví	☐	☐	☐	☒	☐	↑	V současné době vysoký
2	Ochrana dat a osobních údajů	☐	☐	☐	☒	☐	↑	V současné době vysoký
3	Prevence zneužití prostředků pro zpracování informací	☐	☐	☒	☐	☐	↑	V současné době střední
4	Regulace kryptografických prostředků	☒	☐	☐	☐	☐	→	V současné době nízký
5	Dopad na podnikání:	☐	☐	☒	☒	☐	↑	V současné době střední až vysoký,
6	Bezpečnost informací z pohledu podnikání	☐	☐	☒	☒	☐	↑	V současné době střední až vysoký,

Odhad rizika:

1 - Velmi malé 2 - Malé 3 - Střední 4 - Vysoké 5 - Velmi vysoké

Měření efektivnosti ISMS

Měření stavu (pokroku) při implementaci ISMS pomocí modelu vyzrálosti (CMM):

Ref	Popis/ *Description*	Stav ISMS/ *Rating*					
		A	B	C	D	E	F
1	Bezpečnostní politika/ *Security policy*	☐	☐	☐	☐	☐	☒
2	Organizace ISMS/ *Organisation of information security*	☐	☐	☐	☐	☐	☒
3	Řízení aktiv/ *Asset management*	☐	☐	☐	☐	☒	☐
4	Bezpečnost lidských zdrojů/ *Human resource security*	☐	☐	☐	☐	☒	☐
5	Fyzická bezpečnost a bezpečnost prostředí/ *Physical and environmental security*	☐	☐	☐	☒	☐	☐
6	Řízení komunikace a provozu/ *Communications and operations management*	☐	☐	☐	☐	☒	☐
7	Řízení přístupu/ *Access control*	☐	☐	☐	☐	☒	☐
8	Sběr dat, vývoj a údržba IS/ *Information systems acquisition, development and maintenance*	☐	☐	☐	☐	☐	☒
9	Řízení bezpečnostních incidentů/ *Information security incident management*	☐	☐	☐	☐	☐	☒
10	Management kontinuity/ *Business continuity management*	☐	☐	☐	☐	☒	☐
11	Soulad s požadavky/ *Compliance with legal requirements*	☐	☐	☐	☐	☒	☐

Měření efektivnosti ISMS

Měření stavu (pokroku) při implementaci ISMS pomocí modelu vyzrálosti (CMM) - stupnice:

A	optimalizovaný, proces/prvek je pravidelně zlepšován na základě měření a monitorování „best practices"
	optimised, process/element is improved regularly, best practices are followed
B	plně řízený, proces/prvek je měřen a monitorován
	managed, process/element is measured/monitored
C	definován, prvek/proces je dokumentován, systémový přístup průkazný
	defined, process/element is documented, system approach evident
D	D-opakovatelný, prvek/proces je opakovatelný
	repeatable, process/element follow regular pattern
E	*počáteční fáze,* existují nesystémové, operativní náznaky řešení
	initial, non-systematic approach, processes are ad hoc
F	neexistence řízení, prvek/proces neřešen ani aplikován
	non-existent, element/process isn´t solved or applied

Měření efektivnosti ISMS

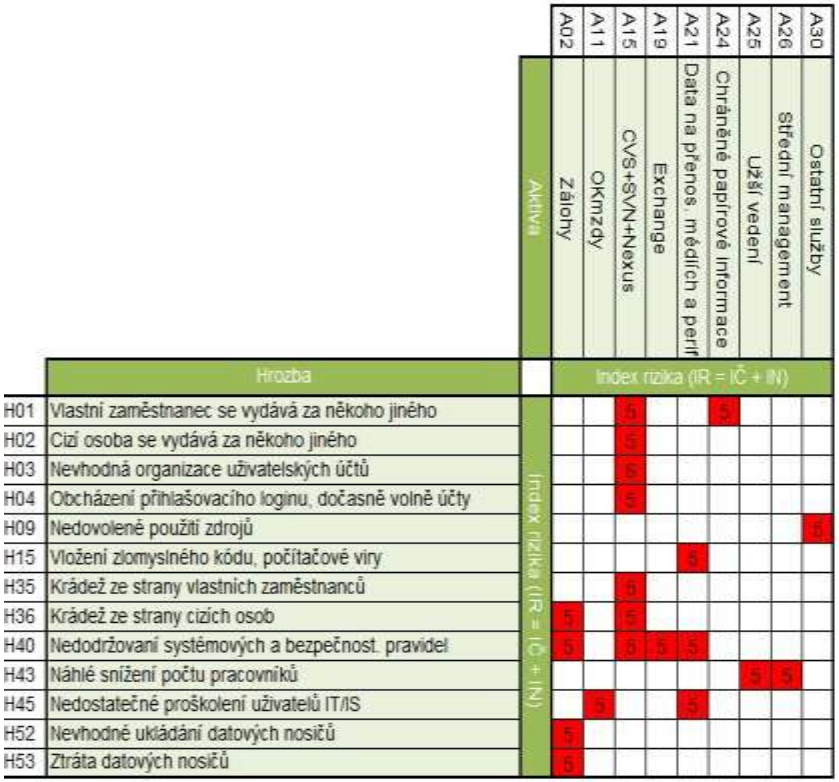
Měření efektivnosti implementovaných opatření ISMS - cíl:

- Zjistit, do jaké míry jsou implementovaná opatření účinná
- Zjistit dosažení cílů, kterých mělo být dosaženo implementací opatření
- Zjistit, zda opatření redukují/řídí rizika, jak bylo plánováno nebo plní identifikované požadavky

Měření efektivnosti ISMS

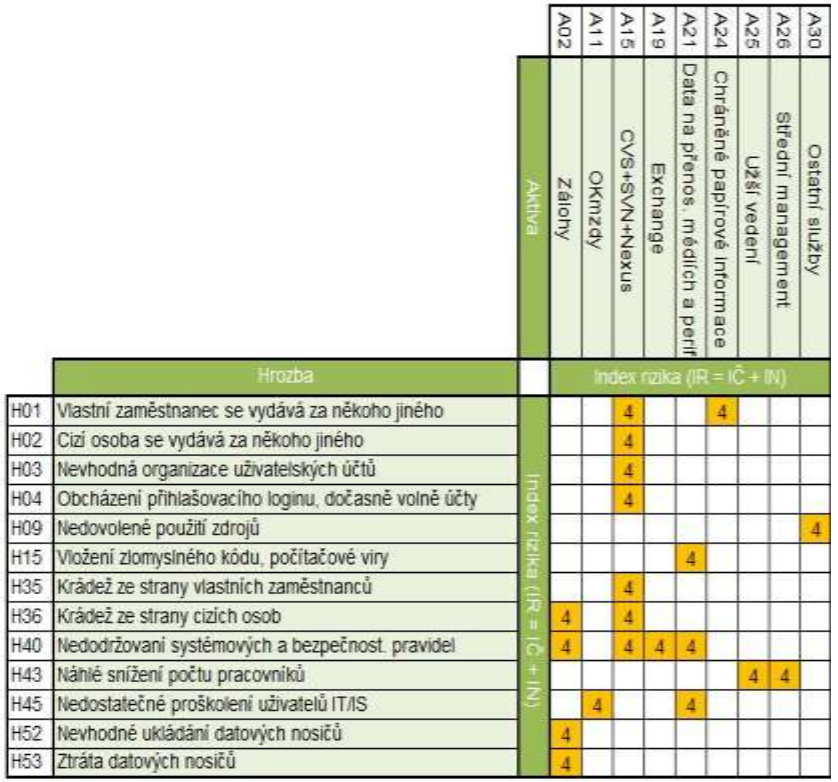
- Příklad měření efektivnosti realizovaných opatření pomocí opakované AR

Rizika před zavedením opatření



	Hrozba	Index rizika (IR = IČ + IN)										
	Aktiva		A02	A11	A15	A19	A21	A24	A25	A26	A30
			Zálohy	OKmzdy	CVS+SVN+Nexus	Exchange	Data na přenos. médiích a perif	Chráněné papírové informace	Užší vedení	Střední management	Ostatní služby
H01	Vlastní zaměstnanec se vydává za někoho jiného				5			5			
H02	Cizí osoba se vydává za někoho jiného				5						
H03	Nevhodná organizace uživatelských účtů				5						
H04	Obcházení přihlašovacího loginu, dočasně volně účty				5						
H09	Nedovolené použití zdrojů										5
H15	Vložení zlomyslného kódu, počítačové viry						5				
H35	Krádež ze strany vlastních zaměstnanců				5						
H36	Krádež ze strany cizích osob	5			5						
H40	Nedodržovaní systémových a bezpečnost. pravidel	5			5	5	5				
H43	Náhlé snížení počtu pracovníků								5	5	
H45	Nedostatečné proškolení uživatelů IT/IS		5				5				
H52	Nevhodně ukládání datových nosičů	5									
H53	Ztráta datových nosičů	5									

Plánované hodnoty rizik



	Hrozba	Index rizika (IR = IČ + IN)										
	Aktiva		A02	A11	A15	A19	A21	A24	A25	A26	A30
			Zálohy	OKmzdy	CVS+SVN+Nexus	Exchange	Data na přenos. médiích a perif	Chráněné papírové informace	Užší vedení	Střední management	Ostatní služby
H01	Vlastní zaměstnanec se vydává za někoho jiného				4			4			
H02	Cizí osoba se vydává za někoho jiného				4						
H03	Nevhodná organizace uživatelských účtů				4						
H04	Obcházení přihlašovacího loginu, dočasně volně účty				4						
H09	Nedovolené použití zdrojů										4
H15	Vložení zlomyslného kódu, počítačové viry						4				
H35	Krádež ze strany vlastních zaměstnanců				4						
H36	Krádež ze strany cizích osob	4			4						
H40	Nedodržovaní systémových a bezpečnost. pravidel	4			4	4	4				
H43	Náhlé snížení počtu pracovníků								4	4	
H45	Nedostatečné proškolení uživatelů IT/IS		4				4				
H52	Nevhodně ukládání datových nosičů	4									
H53	Ztráta datových nosičů	4									

Měření efektivnosti ISMS

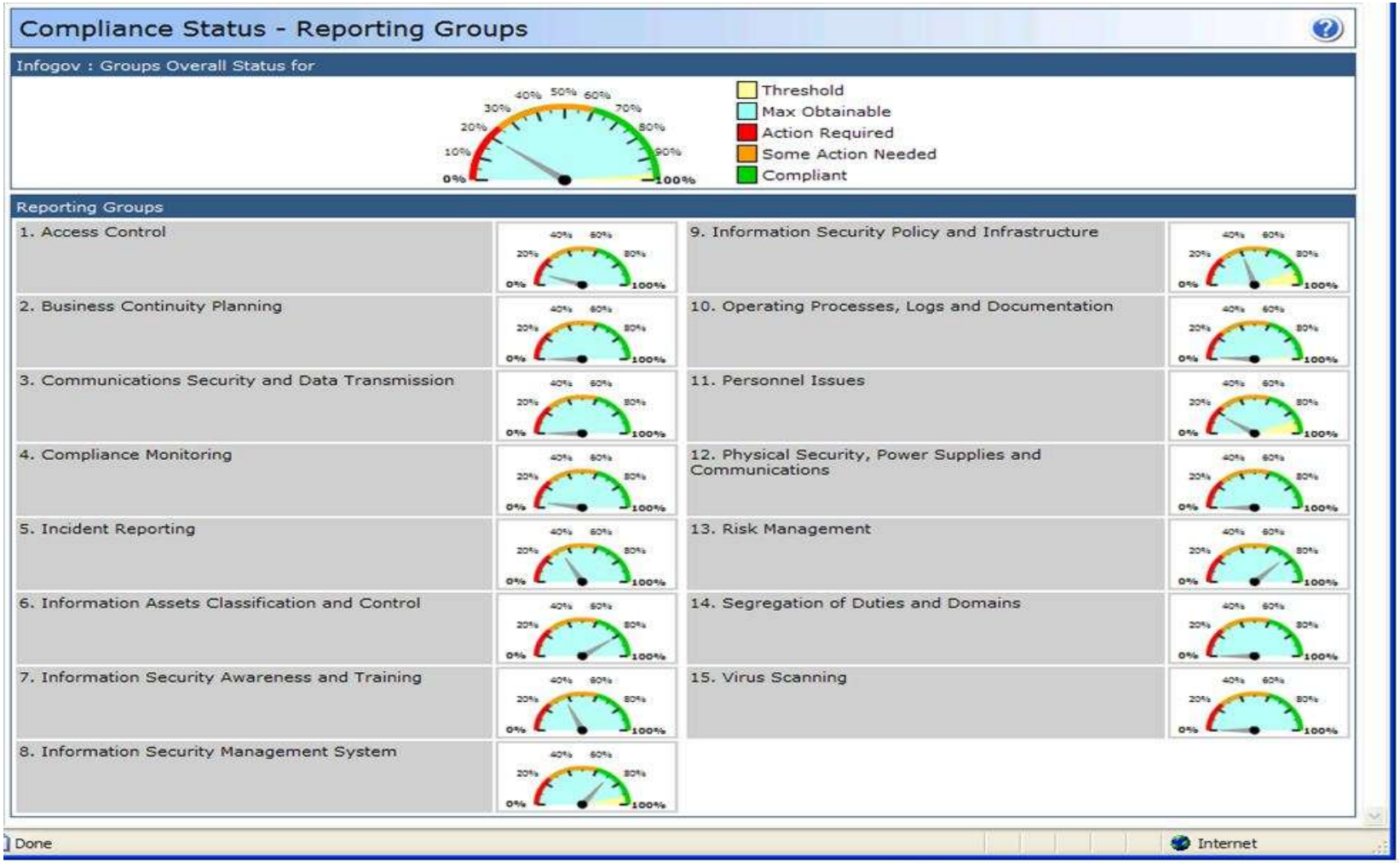
Celkový přehled metrik v organizaci - příklad

PŘEHLED METRIK - ISMS

Název ukazatele	Proces viz Mapa procesů	Co se dozvíme?	Způsob výpočtu - sledování	Zdroj dat	Odpovídá za sběr dat	Vyhodnocení dat	Perioda hodnocení	Cílová hodnota	Skutečnost
Podíl neidentifikovaných rizik v předchozí AR k identifikovaným rizikům	Management rizik	Schopnost kvalifikovaně posoudit a identifikovat rizika	Počet neident. rizik / celkový počet identifikovaných rizik za sledované období *100	protokoly z AR	Risk manager	Zpráva o stavu IMS	Vyhodnocováno 1x ročně	max. 10 % neident. rizik	splněno 1%
Zvládání rizik		Zda jsme schopni snižovat rizika dle schváleného plánu	počet rizik s plně implementovanými opatřeními/ celkový počet rizik, která mají být eliminována	RTP	Manager ISMS	Zpráva o stavu IMS	4x za rok	100%	nesplněno 90%
Shoda se systémovými požadavky na ISMS	Interní audity	Jak plníme požadavky normy ISO 27001	viz. metodika pro IA počet neshod	Protokoly z IA	Auditor ISMS	Zpráva z auditu	2 x ročně	< 5	nesplněno 10
Počet nevyřešených kritických zranitelností CVSS > 7 za kvartál	Management tech. Zranitelností	Jak rychle jsme schopni aplikovat relevantní patche	(Počet zranitelností nevyřešených/Celkový počet zranitelností)*100	VT Report	Securitz admin	Zpráva o stavu IMS	4x za rok	< 3%	splněno 1%

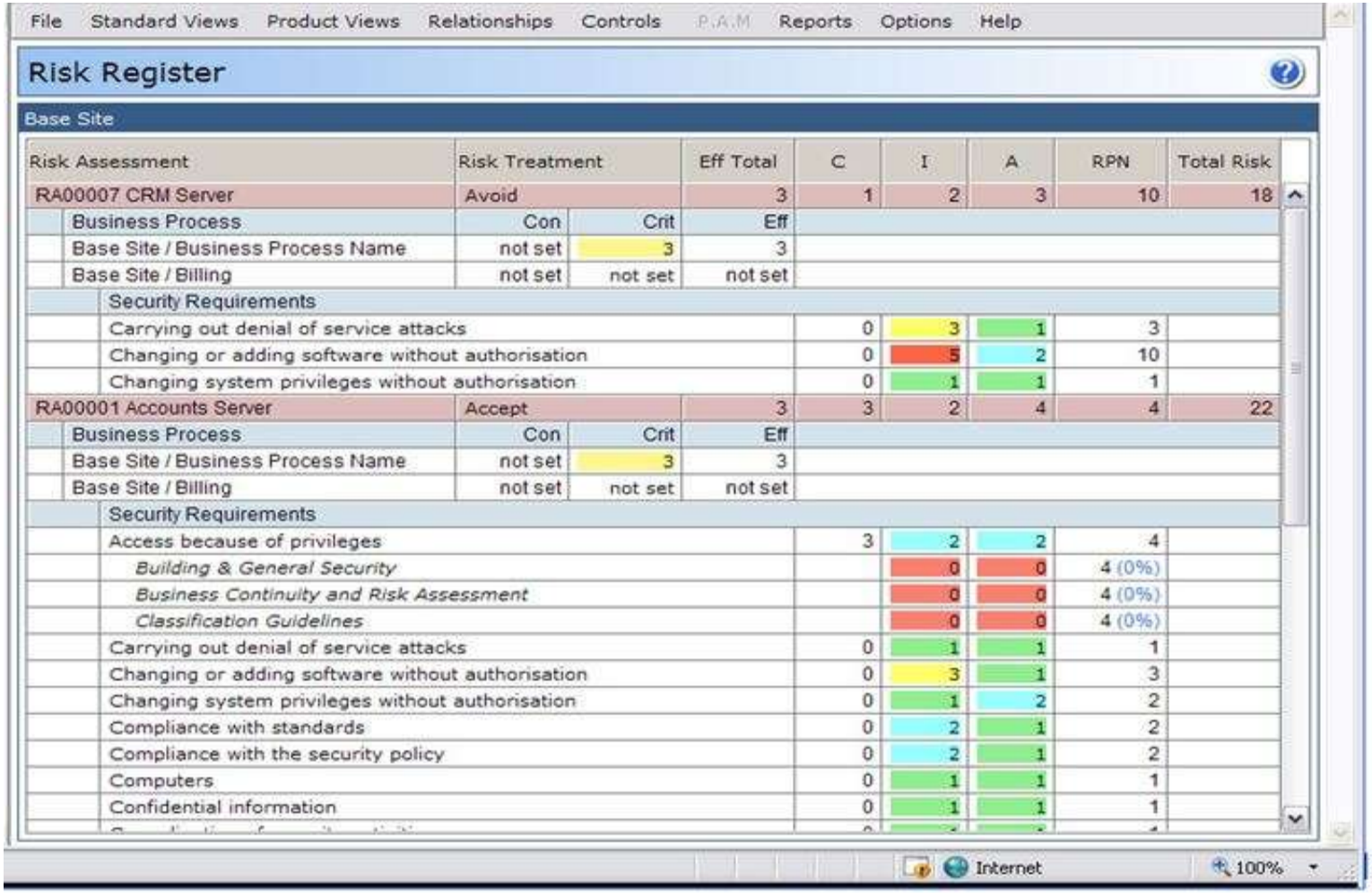
Měření efektivnosti ISMS

A nebo takhle automatizovaně…….



Měření efektivnosti ISMS

A nebo takhle automatizovaně…….



Risk Assessment	Risk Treatment		Eff Total	C	I	A	RPN	Total Risk
RA00007 CRM Server	Avoid		3	1	2	3	10	18
Business Process	Con	Crit	Eff					
Base Site / Business Process Name	not set	3	3					
Base Site / Billing	not set	not set	not set					
Security Requirements								
Carrying out denial of service attacks				0	3	1	3	
Changing or adding software without authorisation				0	5	2	10	
Changing system privileges without authorisation				0	1	1	1	
RA00001 Accounts Server	Accept		3	3	2	4	4	22
Business Process	Con	Crit	Eff					
Base Site / Business Process Name	not set	3	3					
Base Site / Billing	not set	not set	not set					
Security Requirements								
Access because of privileges				3	2	2	4	
Building & General Security					0	0	4 (0%)	
Business Continuity and Risk Assessment					0	0	4 (0%)	
Classification Guidelines					0	0	4 (0%)	
Carrying out denial of service attacks				0	1	1	1	
Changing or adding software without authorisation				0	3	1	3	
Changing system privileges without authorisation				0	1	2	2	
Compliance with standards				0	2	1	2	
Compliance with the security policy				0	2	1	2	
Computers				0	1	1	1	
Confidential information				0	1	1	1	

Měření efektivnosti ISMS

A nebo takhle automatizovaně…… stav plnění opatření

File Standard Views Product Views Relationships Controls P.A.M Reports Options Help

Compliance Status - Questionnaires ListView

IGL HQ (United Kingdom, Europe)

BS ISO/IEC 17799:2005 LITE (12/06)
Start - 14/03/2007
Interim - 20/04/2007
Completion - 01/06/2007
158 assigned, 130 outstanding

Control Status
Total Controls - 152
Failed Controls - 142
Question Status
Total Questions - 538
Answered - 28
Failed Questions - 20

Threshold
Max Obtainable
Action Required
Some Action Needed
Compliant

Sections: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Ctl Qtn	St	Name / Ans	Score	Justification	App User Name	Action Req Date	Verify Comment	Policies / History
1. Information Security Management System (ISMS)								
1.1. Establish the ISMS (PLAN)								
Fail		1.1.1. Define the scope of the ISMS			Yes	Yes	No	No
		1.1.1.1. Has the organisation defined and documented the scope of the ISMS?						
		Partly	0.50	Time	Firstname Surname	18/06/2007	The need for an ISMS within the company has been recognised and work in usderway to develop a suitable solution. It is intended to utilise the FSD department as a pilot and then roll out the ISMS across the business.	
		1.1.1.2. Has the scope been approved by management?						
		No	0.00	Environment	Firstname Surname	18/06/2007	The scope of the project has not been approved by the department heads. This work has not been started because the team was not aware until recently that is was a requirement.	
Fail		1.1.2. Define a systematic approach to risk assessment			Yes	Yes	No	No
		1.1.2.1. Has the organisation defined a systematic approach to risk management?						
		N/A	0.00	not set	Firstname Surname	not set		
		1.1.2.2. Does the approach determine criteria for accepting the risks and identify acceptable levels of risk?						
		No	0.00	Risk Budget	Firstname Surname	not set	This is a risky project becasue there is not sufficient budget	
Pass		1.1.3. Identify the risks			Yes	No	No	No
		1.1.3.1. Has the organisation identified the assets within the scope of the ISMS that may be subject to risk?						

Internet

Měření efektivnosti ISMS dle ISO 27001?

ZÁSADY PRO SEZNAMOVÁNÍ S DOSAŽENÝMI METRIKAMI:

- Vždy je nutné maximálně přizpůsobit zprávu o stavu metrik zvyklostem a kultuře organizace.
- Poskytovat pravidelnou zpětnou vazbu jednotlivcům a týmům, kteří sbírají data z pohledu jejich metrik.
- Nikdy nepoužívejte metriky k vyhrůžkám zaměstnancům nebo týmům

Měření efektivnosti ISMS dle ISO 27001?

ZÁSADY PRO SEZNAMOVÁNÍ S DOSAŽENÝMI METRIKAMI :

- Pracovníci musí být seznámeni s metrikami, musí je chápat a akceptovat, že jsou z jejich strany splnitelné

- Metriky, které indikují problematické oblasti by neměly být brány negativně, ale spíše jako pozitivní zjištění, že je prostor pro zlepšování daného procesu

- Je nutné vždy balancovat mezi tím, co ještě můžeme akceptovat jako únosnou míru neshody a kdy je nutno již přikročit k rázným opatřením (disciplinární proces, postihy atd.)

SECURITY 2011

19. ročník konference o bezpečnosti v ICT

SLOVO ZÁVĚREM

LITERATURA

- ISO/IEC 27004 (ČSN ISO 27004) – Information security management Measurements
- Manager ISMS dle ISO/IEC 27001 – Versa Systems, materiály z kurzu (2011)
- BIP 0074 - Průvodce měřením účinnosti ISMS implementace
- „Security Metrics Guide for Information Technology systems“ (2003) NIST Special publication 800-55
- White Paper - Measuring the Effectiveness of Security using ISO 27001 (Steve Wright, Senior Consultant)
- ISO/IEC 27001 & 27002 implementation guidance and metrics (www.ISO27001security.com)
- How can security Be Measured? (David A.Chapin, ISACA journ., vol. 2, 2005)

SECURITY 2011

19. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Václav Štverka
Versa Systems s.r.o.
stverka@versasys.cz