ČSN ISO/IEC 27001:2014 a zákon o kybernetické bezpečnosti

Ing. Daniel Kardoš, Ph.D

4.11.2014

ČSN ISO/IEC 27001:2006	ČSN ISO/IEC 27001:2014	Poznámka
0 Úvod	0 Úvod	
1 Předmět normy	1 Předmět normy	
2 Normativní odkazy	2 Citované dokumenty	
3 Termíny a definice	3 Termíny a definice	
4 Systém managementu bezpečnosti informací	4 Kontext organizace	Mnohem stručnější
4.1 Všeobecné požadavky	4.1 Porozumění organizaci a jejímu kontextu	Důraz na externí aspekt
4.2 Ustavení a řízení ISMS	4.2 Porozumění potřebám a očekáváním zainteresovaných stran	Nová norma končí kapitolu 4 stejnou větou, kterou stará začínala.
4.2.1 Ustavení ISMS	4.3 Stanovení rozsahu systému řízení bezpečnosti informací	PDCA přesunuto z 4.2 do kapitoly 6, 8, 9, 10
4.2.2 Zavádění a provozování ISMS	4.4 Systém řízení bezpečnosti informací	
4.2.3 Monitorování a přezkoumání ISMS		
4.2.4 Udržování a zlepšování ISMS		
4.3 Požadavky na dokumentaci		Integrace ISMS do procesů organizace
5 Odpovědnost vedení	5 Vůdčí role	
5.1 Závazek vedení	51 Vůdčí role a závazek	Podáváním zpráv o výkonnosti řízení
5.2 Řízení zdrojů	5.2 Politika	
	5.3 Role, odpovědnosti a pravomoci organizace	

ČSN ISO/IEC 27001:2006	ČSN ISO/IEC 27001:2014	Poznámka
6 Interní audity ISMS	**6 Plánování**	
	6.1 Opatření zaměřená na rizika a příležitosti	4.2.1 Analýza rizik, opatření, prohlášení o aplikovatelnosti
7 Přezkoumání ISMS vedením organizace	6.2 Cíle bezpečnosti informací a plánování jejich dosažení	
7.1 Všeobecně	**7 Podpora**	
7.2 Vstup pro přezkoumání	7.1 Zdroje	
7.3 Výstup z přezkoumání	7.2 Kompetence	5.2, 4.3 a jiné. Kompetence (role), komunikace
	7.3 Povědomí	
	7.4 Komunikace	
	7.5 Dokumentované informace	
	8 Provozování	
8 Zlepšování ISMS	8.1 Plánování a řízení provozu	
8.1 Neustálé zlepšování	8.2 Posuzování rizik bezpečnosti informací	4.2.2 Velmi stručná kapitola
8.2 Opatření k nápravě	8.3 Ošetření rizika bezpečnosti informací	
8.3 Preventivní opatření	**9 Hodnocení výkonnosti**	
	9.1 Monitorování, měření, analýza a hodnocení	
	9.2 Interní audit	4.2.3, 6, 7
	9.3 Přezkoumání vedením organizace	
	10 Zlepšování	
	10.1 Neshody a nápravná opatření	4.2.4, 8
	10.2 Neustálé zlepšování	

Normativní příloha A

ISO/IEC 27001:2013	ISO/IEC 27001:2005
A.5 Politiky bezpečnosti informací	A.5 Politiky bezpečnosti informací
A.6 Organizace bezpečnosti informací	A.6 Organizace bezpečnosti informací
A.7 Bezpečnost lidských zdrojů	A.8 Bezpečnost lidských zdrojů
A.8 Řízení aktiv	A.7 Řízení aktiv
A.9 Řízení přístupu	A.11 Řízení přístupu
A.10 Kryptografie	A.12.3 Kryptografická opatření
A.11 Fyzická bezpečnost a bezpečnost prostředí	A.9 Fyzická bezpečnost a bezpečnost prostředí
A.12 Bezpečnost provozu	A.10 Řízeni komunikací a řízení provozu A.10.1 Provozní postupy a odpovědnosti
A.13 Bezpečnost komunikací	A.10 Řízeni komunikací a řízení provozu A.10.6 Správa bezpečnosti sítě
A.14 Akvizice, vývoj a údržba systémů	A.12 Akvizice, vývoj a údržba informačních systémů
A.15 Dodavatelské vztahy	A.6.2 Externí subjekty A.10.2 Řízení dodávek služeb třetích stran
A.16 Řízení incidentů bezpečnosti informací	A.13 Zvládání bezpečnostních incidentů
A.17 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací	A.14 Řízení kontinuity činnosti organizace
A.18 Soulad s požadavky	A.15 Soulad s požadavky

Politika BI v ISO 17799:2005

a) definici bezpečnosti informací, její cíle, rozsah a její význam – mechanizmus umožňující sdílení informací
(viz Úvod);
b) prohlášení vedení organizace o záměru podporovat cíle a principy bezpečnosti informací;
c) rámec pro stanovení cílů opatření a opatření včetně jednotného přístupu k hodnocení a řízení rizik;
d) stručný výklad bezpečnostních zásad (politik), principů, standardů a norem a požadavků na soulad, kterým organizace přikládá zvláštní význam, například:

1) dodržování zákonných, regulatorních a smluvních požadavků;
2) požadavky na vzdělávání, školení a zvyšování povědomí v oblasti bezpečnosti;
3) zásady plánování kontinuity činností organizace;
4) důsledky porušení bezpečnostních zásad;

e) stanovení obecných a konkrétních odpovědností pro oblast řízení bezpečnosti informací včetně hlášení bezpečnostních incidentů;
f) odkazy na dokumentaci, která může bezpečnostní politiku podporovat, například na detailnější bezpečnostní politiky a postupy zaměřené na konkrétní informační systémy nebo bezpečnostní pravidla, která by měli uživatelé dodržovat.

Politika BI v ISO 27002:2013

Politika bezpečnosti informací by měla obsahovat prohlášení týkající se (Vyhláška o bezpečnostních opatřeních…. Příl.č.4 - PKB 1+2, systému + organizační):

a) **definice bezpečnosti informací, cílů a principů, které nasměrují veškeré činnosti související s bezpečností informací;**

b) **přiřazení obecných a specifických odpovědností pro řízení bezpečnosti informací k definovaným rolím;**

c) **postupy pro zacházení s odchylkami a výjimkami.**

Politika BI v ISO 27002:2013

Na nižší úrovni by měla být politika bezpečnosti informací podporována prostřednictvím politik se specifickými tématy:

a) **řízení přístupu (viz kapitola 9); (PKB č. 7)**
b) **klasifikaci informací (a zacházení s informacemi) (viz 8.2) (4);**
c) **fyzickou bezpečnost a bezpečnost prostředí (viz kapitola 11) (16);**
d) **témata orientovaná na koncového uživatele, jako jsou (8):**
    1) **přijatelné použití aktiv (viz 8.1.3);**
    2) **čistý stůl a čistý displej (viz 11.2.9);**
    3) **přenos informací (viz 13.2.1);**
    4) **mobilní zařízení a práce na dálku (viz 6.2);**
    5) **omezení týkající se instalací a použití softwaru (viz 12.6.2);**

Politika BI v ISO 27002:2013

Na nižší úrovni by měla být politika bezpečnosti informací podporována prostřednictvím politik se specifickými tématy:

e) zálohování (viz 12.3) (9);
f) přenos informací (viz 13.2) (10);
g) ochrana před malwarem (viz 12.2) (18);
h) správa a řízení technických zranitelností (viz 12.6.1) (11);
i) kryptografická opatření (viz kapitola 10) (21);
j) bezpečnost komunikací (viz kapitola 13) (6 + provozu);
k) soukromí a ochrana osobních údajů (viz 18.1.4) (15);
l) dodavatelské vztahy (viz kapitola 15) (3).

Důvodová zpráva A / I.
7.7.2 Shrnutí významných zjištění

„Velmi pozitivním zjištěním je skutečnost, že metodika norem pro řízení informační bezpečnosti ISO/IEC 27001, 27002, z níž vychází návrh zákona, je již nyní využívána pro řízení informační bezpečnosti u 80% subjektů spravujících důležité informační a komunikační technologie státu.“

Důvodová zpráva
A / I. /1.6 Zhodnocení rizika

1.6.2 Technická a ekonomická náročnost zavádění bezpečnostních opatření u povinných osob

„U orgánů a osob, které se prokážou certifikací podle shora uvedených mezinárodních norem, se má za to, že splnily standardy bezpečnostních opatření podle zákona o kybernetické bezpečnosti.“

Důvodová zpráva
A / V. / 6 Korupční rizika

„Zavedení bezpečnostních opatření přitom nebude podléhat (na rozdíl od předmětné normy) žádnému certifikačnímu nebo akreditačnímu řízení. Orgány a osoby budou vést o zavedených bezpečnostních opatřeních příslušnou bezpečnostní dokumentaci a jejich aplikace bude podléhat pouze kontrole ze strany Úřadu, respektive Ministerstva vnitra.“

Přechodná ustanovení § 29 – 32

§ 31 Orgány a osoby uvedené v § 3 písm. e)

a) oznámí kontaktní údaje podle § 16 nejpozději do 30 dnů ode dne naplnění určujících kritérií významného informačního systému jejich informačních systémů,

b) začnou plnit povinnost stanovenou v § 8 (Hlášení kybernetického bezpečnostního incidentu) odst. 1 a 3 nejpozději do 1 roku ode dne naplnění určujících kritérií významného informačního systému a

c) zavedou bezpečnostní opatření podle § 4 odst. 2 nejpozději do 1 roku ode dne naplnění určujících kritérií významného informačního systému.

BS 7799:1995
ISO/IEC TR 13335-1:1996

- **individuální zodpovědnost** (accountability): vlastnost zajišťující, že činnosti určité entity mohou být sledovány jedinečně pro tuto entitu (ISO 7498-2:1989)
- **autenticita** (authenticity): vlastnost zajišťující, že identita subjektu nebo zdroje je taková, za kterou je prohlašována. Autenticita je aplikována na entity, jako jsou uživatelé, procesy, systémy a informace
- **spolehlivost** (reliability): vlastnost, zajišťující konzistentní zamýšlené chování a jeho výsledky

Děkuji za pozornost