



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



**FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY**

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

POSOUZENÍ A NÁVRH INFORMAČNÍ BEZPEČNOSTI V ORGANIZACI

ASSESSMENT AND A PROPOSAL FOR INFORMATION SECURITY IN THE ORGANIZATION

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE

AUTHOR

Bc. ALENA RYBÁKOVÁ

VEDOUCÍ PRÁCE

SUPERVISOR

Ing. VIKTOR ONDRÁK, Ph.D.

BRNO 2015

ZADÁNÍ DIPLOMOVÉ PRÁCE

Rybáková Alena, Bc.

Informační management (6209T015)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává diplomovou práci s názvem:

Posouzení a návrh informační bezpečnosti v organizaci

v anglickém jazyce:

Assessment and a Proposal for Information Security in the Organization

Pokyny pro vypracování:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

ČSN ISO/IEC 27001:2006 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací – Požadavky. Český normalizační institut, 2006.

ČSN ISO/IEC 27002:2005 Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací. Český normalizační institut, 2005.

DOBDA L. Ochrana dat v informačních systémech. Praha: Grada Publishing, 1998. ISBN 80-716-9479-7.

DOUCEK P., L. NOVÁK a V. SVATÁ Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.

POŽÁR J. Základy teorie informační bezpečnosti. Praha: Vydavatelství PA ČR, 2007. ISBN 978-80-7251-250-8.

POŽÁR J. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

Vedoucí diplomové práce: Ing. Viktor Ondrák, Ph.D.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2014/2015.

L.S.

doc. RNDr. Bedřich Půža, CSc.
Ředitel ústavu

doc. Ing. et Ing. Stanislav Škapa, Ph.D.
Děkan fakulty

V Brně, dne 28.2.2015

Abstrakt

Tato diplomová práce pojednává o problematice informační bezpečnosti v organizaci. Snahou autorky je získat široký přehled souvislostí, které potom budou zhodnoceny v závěrečné části, při poskytování konkrétních doporučení. V této práci je tedy rozebírán systém řízení bezpečnosti informací, systém managementu služeb a kybernetická bezpečnost jak v teoretické rovině, tak z hlediska reálné aplikace v konkrétní organizaci. Cílem práce je poskytnutí vlastních doporučení na zlepšení.

Abstract

This diploma thesis deals with the issue of information security in the organization. Author's effort is to gain a broad overview of connections, which will then be evaluated in the final section, providing concrete recommendations. In this thesis it is discussed information security management system, service management system and cyber security, both in theory and in terms of real application in a particular organization. The aim is to provide own recommendations for improvement.

Klíčová slova

ISMS, ITSM, bezpečnost informací, kybernetická bezpečnost, IT služby

Keywords

ISMS, ITSM, information security, cyber security, IT services

Bibliografická citace

RYBÁKOVÁ, A. Posouzení a návrh informační bezpečnosti v organizaci. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2015. 79 s. Vedoucí diplomové práce Ing. Viktor Ondrák, Ph.D.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 28. května 2015

.....
podpis studenta

Poděkování

Tímto bych ráda poděkovala panu Ing. Petru Sedlákoví za jeho cenné rady a připomínky. Také chci poděkovat pracovníkům Generálního ředitelství cel, za umožnění spolupráce a poskytnutí důležitých informací potřebných pro realizaci této práce.

Obsah

Úvod.....	11
Cíle práce	13
Metody a postupy zpracování	13
1 Teoretická východiska práce	14
1.1 Informační bezpečnost	14
1.2 Strategické řízení.....	14
1.3 Procesní přístup.....	15
1.4 Model PDCA.....	15
1.5 Systém řízení bezpečnosti informací ISMS	16
1.5.1 Důvody zavedení ISMS	16
1.6 Řada norem ISMS a jejich vztahy.....	17
1.6.1 ISO 27000:2014.....	19
1.6.2 ČSN ISO/IEC 27001:2014.....	20
1.6.3 ČSN ISO/IEC 27002:2014.....	23
1.6.4 ČSN ISO/IEC 27005:2013.....	27
1.7 Systém managementu služeb ITSM.....	29
1.7.1 Důvody zavedení systému řízení služeb.....	29
1.8 Normy ISO/IEC 20000	29
1.8.1 Norma ISO/IEC 20000-1	30
1.8.2 Norma ISO/IEC 20000-2	31
1.9 ITIL	32
1.10 Kybernetická bezpečnost	33
1.10.1 Zákon o kybernetické bezpečnosti.....	35
1.10.2 Management kybernetické bezpečnosti	37
2 Analýza současného stavu	38

2.1	Požadavky zadavatele	38
2.2	Celní správa České republiky.....	38
2.2.1	Seznámení se s organizací	39
2.2.2	Historické hledisko bezpečnosti informací a kvality služeb.....	45
2.3	Systém řízení informační bezpečnosti v Celní správě České republiky	48
2.3.1	Kontext organizace	49
2.3.2	Vůdčí role	49
2.3.3	Plánování	50
2.3.4	Podpora	50
2.3.5	Provozování	51
2.3.6	Hodnocení výkonnosti	52
2.3.7	Zlepšování.....	52
2.4	Systém managementu služeb informačních technologií v Celní správě České republiky	52
2.4.1	Všeobecné požadavky na systém.....	52
2.4.2	Návrh služeb a přechod na nové nebo změněné služby.....	54
2.4.3	Proces dodávky služby.....	54
2.4.4	Procesy řízení vztahů	55
2.4.5	Procesy zajišťující řešení	55
2.4.6	Řídící procesy	56
2.5	Kybernetický zákon	56
2.6	Shrnutí aktuálního stavu.....	58
2.6.1	ISMS	58
2.6.2	ITSM.....	59
2.6.3	Kybernetický zákon	59
2.6.4	Silné stránky	59

2.6.5	Slabé stránky	60
3	Vlastní návrhy řešení	61
3.1	Návrhy na změnu	61
3.1.1	Budování bezpečnostního povědomí	65
3.1.2	Plán obnovy	68
3.2	Ekonomické zhodnocení	70
	Závěr	71
	Seznam zkratk	73
	Seznam použitých tabulek, obrázků a grafů	74
	Seznam použitých zdrojů	75
	Seznam příloh	79

Úvod

S pokrokem a globalizací lidstvo sbírá, spravuje, vyhodnocuje a ukládá mnohem více dat, informací a zpráv, než kdykoliv dříve. Vyrůstá množství kanálů, kterými se data v kybernetickém prostoru mohou přenášet, což přináší zvýšení komfortu uživatelů, zároveň ale neustále vyrůstá riziko napadení a zneužití dat nejen na úrovni špatně zabezpečených individuálních uživatelů, ale i relativně dobře chráněných firemních sítí.

Na jedné straně je tak kladen požadavek na maximální dostupnost dat nehledě na geografickou vzdálenost, různorodost aplikací a schopnosti uživatelů.

Na straně druhé je nutné nezapomínat ani na různá rizika, která vyplývají z takovéto dostupnosti a otevřenosti systémů.

Existují-li například v organizaci obchodní tajemství, je potřeba tato tajemství pečlivě chránit před jejich znehodnocením (např. zničení živelnou pohromou či prodejem citlivých informací konkurenci z řad vlastních zaměstnanců), které by mělo fatální vliv na budoucí existenci firmy. Dále je důležité dbát i na bezpečnost citlivých údajů, které společnost sbírá nejen o svých zaměstnancích, ale i dodavatelích, odběratelích včetně zákazníků v podobě fyzických osob. Kdyby byly informace, které společnost udržuje snadno získatelné, znamenalo by to konkurenční výhodu pro ostatní společnosti, kdy by například mohly cílit na zákazníky lepší nabídkou a navíc společnost sama by se mohla stát pro ostatní nedůvěryhodná. Nikdo si nepřeje, aby jeho citlivé informace byly volně šířené a dostupné.

Podle toho, s jakými informacemi jednotlivé subjekty až celé organizace včetně států zacházejí, je třeba přemýšlet nad tím, jak tyto informace ochránit. Existuje mnoho možností, jak informační bezpečnost zajišťovat – od antivirů, šifrování, zálohování dat po řízení přístupu a další. Pokud tedy vyžadujeme maximální možné bezpečí pro citlivé informace, je třeba na tuto problematiku nahlížet co nejkomplexněji. Hledáním takového řešení se zabývá i systém managementu bezpečnosti informací ISMS, jehož problematika bude podrobněji rozebírána v této práci.

Dne 1. 1. 2015 navíc nabyl účinnosti zákon č. 181/2014 Sb., zákon o kybernetické bezpečnosti a změně souvisejících zákonů (zákon o kybernetické bezpečnosti) zabývající se kybernetickou bezpečností, který je reakcí na vzrůstající hrozby kybernetických útoků na tzv. prvky kritické infrastruktury. Definování jasných pravidel a postupů je tak v souvislosti s ochranou informací v kyberprostoru, některým významným institucím, přímo nařízeno.

Cíle práce

V této diplomové práci se věnuji bezpečnosti informací v konkrétní organizaci. Jedná se o orgán výkonné moci Celní správu České republiky (dále také jen „CS“).

Za cíl vycházející z požadavků samotné organizace jsem si vytyčila vypracovat soubor návrhů a doporučení, jež by společnosti pomohla lépe čerpat výhody a přínosy, které jí certifikovaný systém managementu bezpečnosti informací (dále také jen „ISMS“) nabízí.

Výstup této práce by měl zainteresovaným osobám pomoci dosáhnout prosazení efektivnějšího systému řízení bezpečnosti informací tak, aby organizace lépe plnila podmínky pro jeho certifikaci, tím dojde i k snazšímu plnění podmínek kybernetického zákona. Důležitou součástí jsou i návrhy na změny v praktické aplikaci bezpečnosti informací.

Metody a postupy zpracování

Svá stanoviska budu tvořit na základě historických faktů z minulých let, z existující dokumentace, kterou si Celní správa České republiky zpracovala či pro ni byla vytvořena. Dále budu čerpat informace jak od příslušných zaměstnanců CS, tak od odborníků z praxe. Hlavními vodítky při formulaci vlastních návrhů a závěrů mi přitom budou normy, které se danou problematikou zabývají.

1 Teoretická východiska práce

V této části diplomové práce se zabývám studiem důležitých pojmů. Ze získaných znalostí pak budu čerpat v analytické a návrhové části práce.

1.1 Informační bezpečnost

Jsme závislí na informacích a většina z nich je uchovávána a zpracována v elektronické podobě. Záplava nových technologií a jejich rozšiřující se využití v pracovním i běžném životě na jednu stranu zvyšuje jistý komfort a přispívá k pokroku, na straně druhé, přináší také nová bezpečnostní rizika, která ještě pár let zpátky neexistovala, či nebyla natolik závažná jako nyní (7).

Informace jsou aktiva představující hodnotu a je důležité je chránit před širokým spektrem hrozeb jako je poškození, zničení, zcizení nebo ztráta. Odborně řečeno informační bezpečnost je cílená snaha o zajištění *integrity, dostupnosti a důvěrnosti* informací (1, str. 18).

1.2 Strategické řízení

Strategické řízení je oblastí řízení organizace zohledňující dlouhodobé plánování a směřování organizace jako celku nebo její části. Strategické řízení v organizaci zajišťuje, že se věci nedějí nahodile, ale podle předem naplánovaných, dlouhodobých záměrů. Zásadní pro strategické řízení je definice cílů a stanovení způsobu jejich dosažení (8).

„Strategické řízení slouží jednak pro přenášení požadavků vlastníků na management organizace (tzv. governance) a jednak managementu organizace pro uspořádání, sjednocení a usměrnění chování všech lidí ve všech částech organizace“ (8, odst. 3).

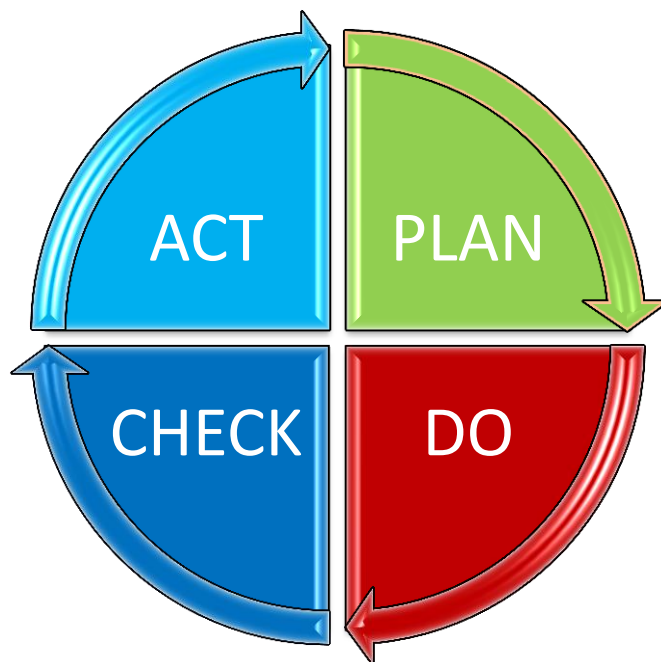
Informační strategie je označení pro dlouhodobý plán vytvořený k dosažení cílů organizace v oblasti nakládání se znalostmi, informacemi či daty (8).

1.3 Procesní přístup

Procesní přístup znamená, že na jednotlivé činnosti probíhající v organizaci je nahlíženo jako na soustavný tok činností, které přeměňují vstupy na výstupy (1, str. 19).

1.4 Model PDCA

Zkratka *PDCA* vznikla z anglických slov Plan–Do–Check–Act, do češtiny se překládá jako Plánuj–Jednej–Kontroluj–Dělej. Jde o cyklus změn, které jsou prováděny ve čtyřech krocích stále dokola a dochází tak k neustálému zlepšování (6, str. 24).



Obr. 1: PDCA cyklus (Upraveno dle 6, str. 25)

1.5 Systém řízení bezpečnosti informací ISMS

Český název vznikl překladem z anglického „Information security management system“, ve zkratce ISMS. Jedná se o součást celkového systému řízení, a jak jeho název napovídá, zabývá se řízením bezpečnosti informací v organizacích a je založený na hodnocení rizik (7).

Než přikročíme k důkladnému seznámení se s managementem bezpečnosti informací, uvedu několik hlavních důvodů, proč by organizace, bez ohledu na svůj typ a velikost, o ISMS měly uvažovat a případně i si tento systém managementu nechat certifikovat (certifikace není podmínkou jeho používání).

1.5.1 Důvody zavedení ISMS

Výhod řízení bezpečnosti informací existuje celé množství, mezi ty nejdůležitější důvody integrace systému řízení bezpečnosti informací do firemní politiky patří (11):

- Požadavky zákonů a regulačních orgánů - především od 1. 1. 2015, kdy vešel v účinnost zákon č. 181/2014 Sb., o kybernetické bezpečnosti, který od organizací, jejichž informační a komunikační systémy splňují kritéria (pevně daná legislativou) vyžaduje zavedení řízení kybernetické bezpečnosti, případně zavedení ISMS a jeho certifikaci.
- Zajištění kontinuity podnikání – společnost pracuje s riziky a jejich možnými dopady a je vyvíjena neustálá snaha o jejich eliminaci, tak aby byla minimalizována rizika ztráty dat při vynaložení optimálních nákladů.
- Vytváření vztahů důvěry a jejich udržení - demonstrace mechanismů sloužících k zabezpečení důvěrných informací, které společnosti udržují o zákaznících, odběratelích, dodavatelích a obchodních partnerech.

V průběhu let vznikla řada vzájemně propojených **norem, které se problematikou ISMS zabývají**. Tyto normy jsou průběžně aktualizovány a překládány do různých jazykových mutací, včetně češtiny (1, str. 2).

1.6 Řada norem ISMS a jejich vztahy

Jde o normy sloužící jako návody pro ustavení, implementaci, udržování a zlepšování ISMS, stanovující požadavky na ISMS v organizaci. Také zadávají požadavky na pracovníky, kteří provádějí jeho certifikaci, či slouží jako vodítka pro tvorbu směrnic pro ISMS v různých odvětvích a zabývají se kontrolou shody ve vztahu k ISMS (1, str. 6).

Na tomto místě uvádím přehled nejdůležitějších norem zabývajících se problematikou ISMS. Nejedná se však o kompletní výčet všech norem (1, str. 23 – 27):

- *ISO/IEC 27000* – obsahuje definice a slovník,
- *ISO/IEC 27001* – určuje seznam požadavků, jak aplikovat ISO/IEC 27002 v rámci procesu ustavení, provozu, údržby a zlepšování systému řízení bezpečnosti informací,
- *ISO/IEC 27002* – návod na implementaci opatření – kontrolní seznam všeho, co je nutno pro bezpečnost informací v organizaci udělat,
- *ISO/IEC 27003* – poskytuje návod pro návrh a implementaci ISMS v souladu s ISO 27001,
- *ISO/IEC 27004* – podpora pro měření a prezentaci efektivity jejich ISMS, zahrnující řídicí procesy definované v ISO/IEC 27001 a opatření z ISO/IEC 27002,
- *ISO/IEC 27005* – doporučení pro řízení rizik bezpečnosti informací s ohledem na požadavky ISMS dle ISO/IEC 27001,
- *ISO/IEC 27006* – stanovuje požadavky na certifikační orgány provádějící auditu systémů řízení,
- *ISO/IEC 27007* – postup pro audit ISMS,

- *ISO/IEC 27008* – směrnice pro audit opatření ISMS,
- *ISO/IEC 27010* – obsahuje doporučení pro sdílení informací mezi organizacemi a/nebo státy, které spadají do „kritické infrastruktury“. Jedná se například o informace týkající se bezpečnostních rizik, opatření, problémů a/nebo incidentů,
- *ISO/IEC 27013* – směrnice pro integraci ISO/IEC 27001 a ISO/IEC 20000-1.

Terminologie	27000 Přehled a slovník	
Požadavky	27001 Všeobecné požadavky	27006 Požadavky na auditory
Obecné směrnice	27002 Soubor postupů a opatření	TR 27008 Směrnice auditu opatření
	27003 Implementace	27013 Integrace s ISO 20000-1
	27004 Měření	27014 Správa
	27005 Řízení rizik	TR 27016 Organizační ekonomika
	27007 Směrnice pro audit ISMS	
Specifické směrnice	27010 Komunikace – mezi org.	TR 27015 Pro finanční služby
	27011 Pro telekomunikace	27001 Při cloud computingu
Specifická opatření	2703x	2704x

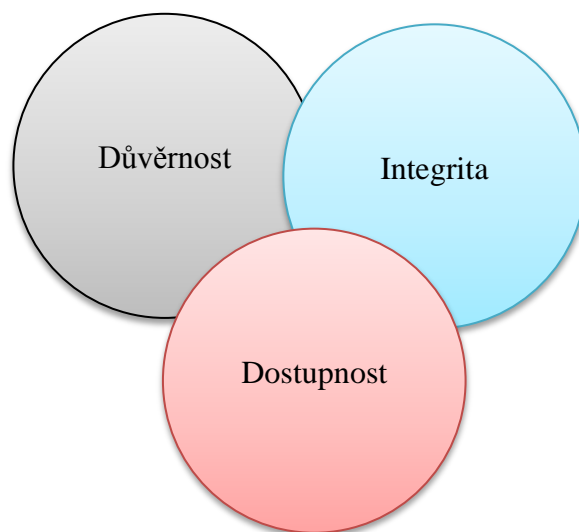
Obr. 2: Vztahy mezi normami ISMS (Upraveno dle 1, str. 24)

1.6.1 ISO 27000:2014

Tato norma slouží k seznámení s problematikou ISMS, udává důvody, proč management bezpečnosti v organizaci implementovat, jeho zařazení do celkového managementu, dále přináší přehled dalších norem a jejich charakteristik a slovník pojmů (1, str. 8).

Nejdůležitější pojmy zahrnuté v této normě (1, str. 8 – 17):

- *Aktivum* – je pojato jako cokoliv, co představuje pro organizaci hodnotu.
- *Bezpečnost informací* – zachování důvěrnosti, integrity, dostupnosti informací, případně i dalších požadovaných vlastností.
- *Dostupnost* – požadované informace jsou v okamžiku potřeby dostupné oprávněným uživatelům a procesům.
- *Dopad* – je výsledkem nežádoucího incidentu.
- *Důvěrnost* – zajištění, aby přístup k informacím, měly jen oprávněné osoby, entity nebo procesy.
- *Integrita* – správnosti a úplnosti informací.
- *Hrozba* – potenciální příčina nechtěného incidentu, která by mohla vést k nežádoucímu stavu.
- *Incident bezpečnosti informací* – nechtěná nebo neočekávaná událost bezpečnosti.
- *ISMS* – část managementu organizace, přístup k rizikům činností.
- *Management rizik* – koordinované činnosti k práci s riziky.
- *Riziko* – účinek nejistoty na dosažení cílů.
- *Událost bezpečnosti informací* – stav, kdy hrozí riziko narušení bezpečnosti.
- *Zvládnání rizik* – proces výběru a přijímání opatření.
- *Zranitelnost* – slabé místo aktiva nebo opatření, které může v případě naplnění hrozby, představovat slabé místo.



Obr. 3: Informační bezpečnost (Vlastní zpracování)

1.6.2 ČSN ISO/IEC 27001:2014

Tato norma nahrazuje předcházející ČSN ISO/IEC 27001:2005 – došlo k nahrazení termínů a definic, včetně změn obsahu (2, str. 1).

Jedná se o podrobnou specifikaci normativních požadavků při ustavení, zavádění, provozování, monitorování, přezkoumávání, udržování a zlepšování systému managementu bezpečnosti informací (2, str. 6).

Norma je využitelná všemi organizacemi neohledně na jejich typ, velikost a organizační uspořádání. Jedná se tedy o univerzální normu, která dává všem organizacím návod, avšak je třeba jednotlivé předložené části touto normou, přizpůsobit konkrétnímu prostředí. Pokud by došlo k vyloučení kteréhokoliv z požadavků této normy, jednalo by se o nepřijatelný krok, v případě, že se organizace snaží o shodu s touto normou, například pro důvody certifikace (2, str. 6).

Požadavky stanovené ČSN ISO/IEC 27001:2014 (2, str. 7 – 13):

Kontext organizace

- *Porozumění organizaci a jejímu kontextu* (určení aspektů, které ovlivňují dosažení výstupů ISMS),
- *Porozumění potřebám a očekáváním zainteresovaných stran* (určení těch, kteří mají vztah k ISMS a jejich požadavků),
- *Stanovení rozsahu systému řízení bezpečnosti informací* (určení hranic aplikovatelnosti),
- *Systém řízení bezpečnosti informací* (požadavek na ustanovení, implementaci, udržování a neustálé zlepšování ISMS v souladu s touto normou).

Vůdčí role

- *Vůdčí role a závazek* (vyjádření podpory a její demonstrace vrcholovým vedením),
- *Politika* (stanovení politiky bezpečnosti informací, která musí splňovat požadavky jako přiměřenost, její dostupnost a komunikace, zahrnovat závazky, cíle),
- *Role, odpovědnosti a pravomoci organizace* (jejich přiřazení pro shodu s touto normou a podávání zpráv o výkonnosti ISMS).

Plánování

- *Opatření zaměřená na rizika a příležitosti* (určení rizik a příležitostí v kontextu organizace, posouzení a ošetření rizik) – *blíže bude probráno později*,
- *Cíle bezpečnosti informací a plánování jejich dosažení* (definuje požadavky na cíle bezpečnosti informací a jejich plánování např. měřitelnost, aplikovatelnost požadavků, komunikace, aktualizace, určení zdrojů, kompetencí, hodnocení výsledků a podobně).

Podpora

- *Zdroje* (určení a zajištění zdrojů ISMS),
- *Kompetence* (stanovení kompetencí, včetně zajištění prokázání kompetencí)
- *Povědomí* (všichni v organizaci musí znát politiku bezpečnosti, svoji roli a důsledky nepřizpůsobení se),
- *Komunikace* (zajištění komunikace – co, kdy, kde, kým, procesy a podobně)
- *Dokumentované informace* (co musí být dokumentováno v kontextu organizace, zajištění odpovídající identifikace, popisu, formátu, média, přezkoumání, schválení, aktualizace a řízení distribuce, přístupu, ukládání, změn, uchovávání likvidace a podobně).

Provozování

- *Plánování a řízení provozu* (implementace, plánování a řízení procesů a implementace opatření a plánů – požadavek na dokumentaci, řízení plánovaných změn, určení a řízení outsourcovaných procesů),
- *Posuzování rizik bezpečnosti informací* (stanovení termínů),
- *Ošetření rizik bezpečnosti informací* (požadavek na implementaci plánu ošetření rizik bezpečnosti informací a úschovu dokumentovaných výsledků).

Hodnocení výkonnosti

- *Monitorování, měření, analýza a hodnocení* (určení rozsahu a metod měření, stanovení monitorování, analýz, hodnocení, včetně kompetencí a požadavku na uchovávání),
- *Interní audit* (v plánovaných termínech zjišťovat, zda nedochází k chybám vzhledem k požadavkům organizace, této normy a zda je ISMS efektivní – nutno definovat kritéria a rozsah auditu, auditory, komu budou výsledky předkládány a jejich uložení, sloužící jako důkaz o provedení),
- *Přezkoumání vedením organizace* (v naplánovaném intervalu vrcholový management posuzuje ISMS organizace za účelem zjištění vhodnosti, přiměřenosti a efektivnosti, výstup je nutno zdokumentovat a uschovat).

Zlepšování

- *Neshody a nápravná opatření* (reakce na neshodu, implementace opatření, vyhodnocení potřeby a efektivnosti opatření, provedení změn v ISMS, pokud je to nezbytné, nutno zdokumentovat),
- *Neustálé zlepšování* (požadavek na neustálé zlepšování vhodnosti, přiměřenosti a efektivnosti ISMS organizace).

1.6.3 ČSN ISO/IEC 27002:2014

Tato norma úzce souvisí s ISO/IEC 27001 a slouží jako opora pro výběr opatření v rámci procesu integrace ISMS. Definuje 14 kapitol ohledně bezpečnostních opatření. Kapitoly jsou podrobněji rozpracovány na 35 kategorií. Každá kategorie má určený cíl a jedno nebo více opatření, jak ho dosáhnout a dále obsahuje pokyny k implementaci (3, str. 7).

Tab. 1: Přehled ČSN ISO/IEC 27002:2014 (Zpracováno dle 3, str. 10 až 72)

Kategorie bezpečnostních opatření:	Počet kategorií	Počet opatření
<i>Politiky bezpečnosti informací</i> - Směřování bezpečnosti informací vedením organizace	1	2
<i>Organizace bezpečnosti informací</i> - Interní organizace, - Mobilní zařízení a práce na dálku	2	7
<i>Bezpečnost lidských zdrojů</i> - Před vznikem pracovního vztahu, - Během pracovního vztahu, - Ukončení a změna pracovního vztahu,	3	6
<i>Řízení aktiv</i> - Odpovědnost za aktiva, - Klasifikace přístupu, - Manipulace s médii,	3	10
<i>Řízení přístupu</i> - Požadavky organizace na řízení přístupu,	4	14

<ul style="list-style-type: none"> - Řízení přístupu uživatelů, - Odpovědnosti uživatelů, - Řízení přístupu k systémům a aplikacím, 		
Kryptografie <ul style="list-style-type: none"> - Kryptografická opatření, 	1	2
Fyzická bezpečnost a bezpečnost prostředí <ul style="list-style-type: none"> - Bezpečné oblasti, - Zařízení, 	2	15
Bezpečnost provozu <ul style="list-style-type: none"> - Provozní postupy a odpovědnosti, - Ochrana proti malwaru, - Zálohování, - Zaznamenávání formou logů a monitorování, - Správa provozního software, - Řízení technických zranitelností, - Hlediska auditu informačních systémů, 	7	14
Bezpečnost komunikací <ul style="list-style-type: none"> - Správa bezpečnosti sítě, - Přenos informací, 	2	7
Akvizice, vývoj a údržba systémů <ul style="list-style-type: none"> - Bezpečnostní požadavky informačních systémů, - Bezpečnost v procesech vývoje a podpory, - Data pro testování, 	3	13
Dodavatelské vztahy <ul style="list-style-type: none"> - Bezpečnost informací v dodavatelských vztazích, - Řízení dodávek služeb dodavatelů, 	2	5
Řízení incidentů bezpečnosti informací <ul style="list-style-type: none"> - Řízení incidentů bezpečnosti informací a zlepšování 	1	7
Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací <ul style="list-style-type: none"> - Kontinuita bezpečnosti informací, - Redundance, 	2	4
Soulad s požadavky <ul style="list-style-type: none"> - Soulad s právními a smluvními požadavky, - Přezkoumání bezpečnosti informací. 	2	8
Celkem:	35	114

Bezpečnostní politika

Základním z požadavků při zavádění ISMS je stanovení a přijetí bezpečnostní politiky. Jedná se o dokument, jehož cílem je závazek vedení k vytvoření podmínek pro podporu bezpečnosti informačních aktiv a určení bezpečnostní politiky jako takové.

Předmětem bezpečnostní politiky je ochrana informací a prostředků pro zpracování těchto informací (15).

Politika bezpečnosti informací by měla zahrnovat tyto klíčové části (16, str. 5 – 6):

- Definice bezpečnosti informací, cílů a principů, které nasměrují veškeré činnosti, související s bezpečností informací,
- Přiřazení obecných a specifických odpovědností pro řízení k definovaným rolím,
- Postup pro zacházení s odchylkami a výjimkami.

Politiky nižší úrovně by měly řešit (16, str. 6 – 9):

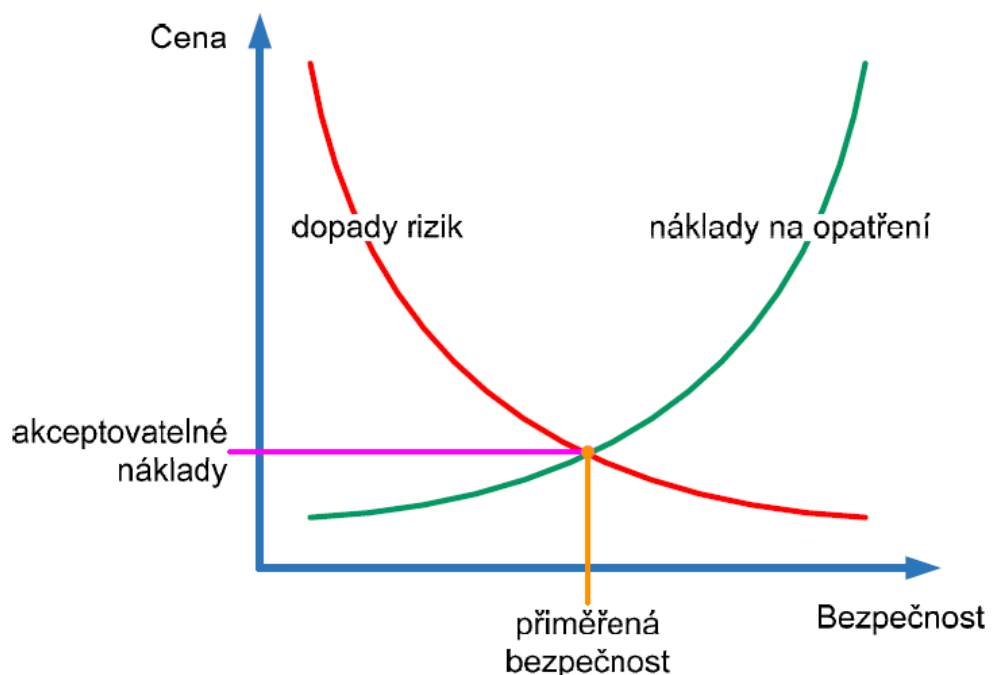
- Řízení přístupu,
- Klasifikace informací,
- Fyzická bezpečnost a bezpečnost prostředí,
- Problematika řešící koncového uživatele,
 - Přijatelné použití aktiv,
 - Čistý stůl a čistý displej,
 - Přenos informací,
 - Mobilní zařízení a práce na dálku.
- Omezení týkající se instalací a použitelnosti software
- Zálohování,
- Přenos informací,
- Ochrana před malwarem,
- Správa a řízení technických zranitelností,
- Kryptografická opatření,
- Bezpečnost komunikací,
- Soukromí a ochrana osobních údajů,
- Dodavatelské vztahy.

Disaster recovery plan

„Disaster recovery plan“, česky plán obnovy, by měl poskytnout jasné, srozumitelné a stručné avšak úplné instrukce, co je potřeba vykonat, nastane-li situace, která se vymyká stavu běžného provozu a dojde k narušení bezpečnosti informací (3, str. 68).

Zdrojem těchto situací může být například havárie, živelná pohroma nebo lidské pochybení. Někdy je možné takovým situacím předcházet, jindy náklady na opatření převyšují dopady na tolik, že se zkrátka nevyplatí proti těmto rizikům bojovat a riziko můžeme snížit (například pojištěním), či ho jen akceptovat a doufat, že tato situace nenastane (6, str. 35).

V každém případě je přínosné, aby organizace přijala taková bezpečnostní opatření, která těmto situacím zabrání. Někdy opatření nelze realizovat, či je příliš nákladné vzhledem k dopadu rizik. Viz graf přiměřené bezpečnosti (6, str. 35).



Graf 1.: Vztah mezi dopady rizik a náklady na opatření (Zdroj 6, str. 36)

1.6.4 ČSN ISO/IEC 27005:2013

Tato norma předkládá, jak by organizace měla řídit rizika, je zde zdůrazněn systematický přístup k této problematice a nechybí ani připomínka, že se jedná o cyklický proces. Riziko je touto normou definované jako účinek nejistoty na dosažení cílů (4, str. 7 - 10).

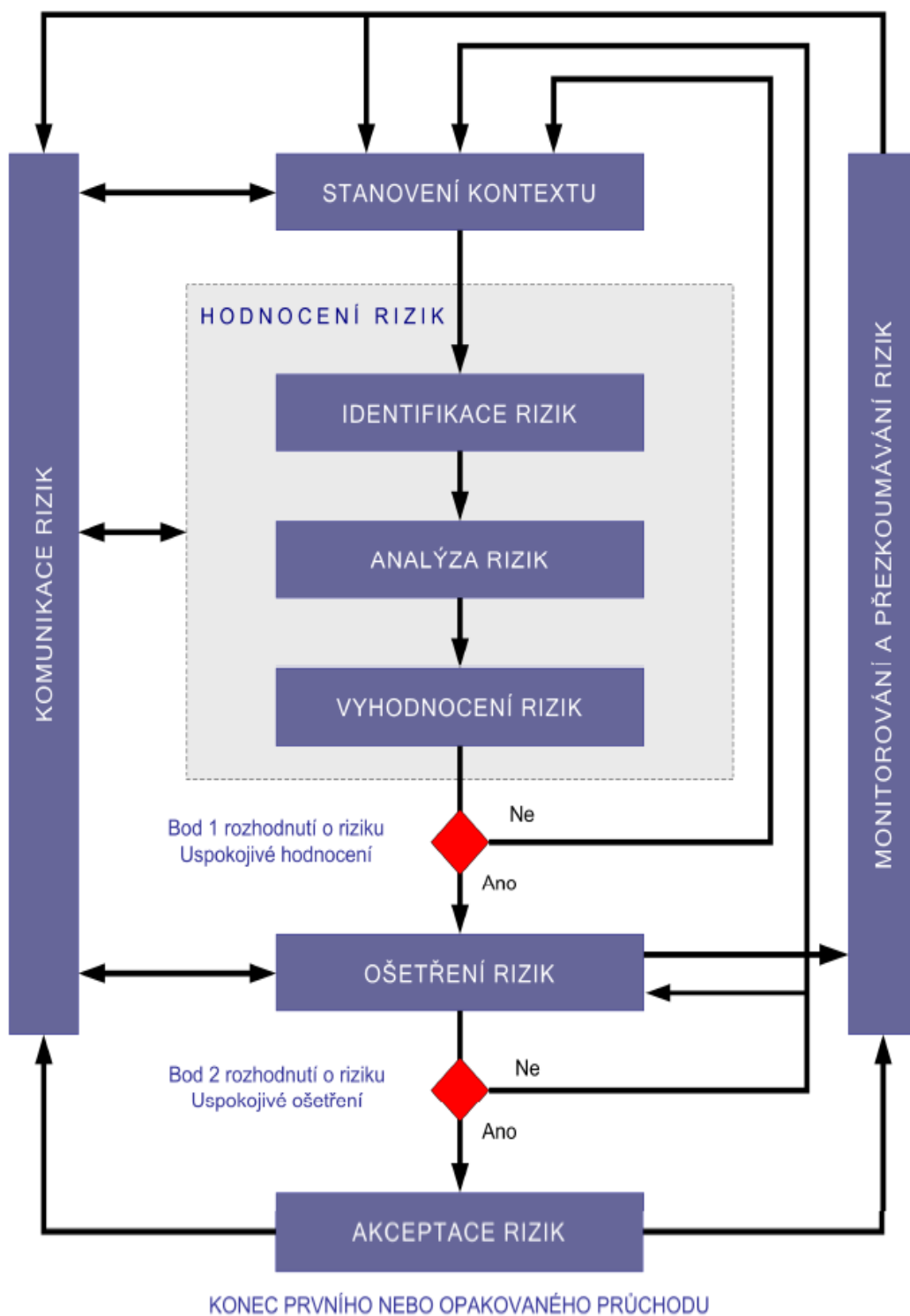
Řízení rizik bezpečnosti informací

Systematická činnost řízení rizik zahrnuje nezbytné kroky jako je identifikace a posouzení rizik z hlediska důsledků na činnosti organizace a pravděpodobnosti výskytu těchto rizik. Neméně důležitá je komunikace a pochopení pravděpodobnosti a důsledků těchto rizik. Dalším krokem je stanovení pořadí priorit při ošetření rizik a stanovení priorit u činností vedoucích k redukci výskytu rizik.

Jako nutná součást řízení rizik je bráno i zapojení zainteresovaných stran a jejich informování. Předem stanovená ošetření rizik je třeba neustále sledovat a přitom se nesmí zapomenout ani na přezkoumávání sledování rizik a procesů sledování. Vhodné je neustále získávat informace vedoucí ke zlepšení přístupu k řízení rizik a pravidelně provádět školení vedoucích pracovníků a zaměstnanců v oblasti rizik (4, str. 12).

Tab. 2: Aplikace modelu PDCA při řízení rizik (Zpracováno dle 4, str. 15)

Proces ISMS	Proces řízení rizik bezpečnosti informací
Plánuj	Stanovení kontextu, Posouzení rizik, Příprava plánu ošetření rizik, Akceptace rizik.
Dělej	Implementace plánu ošetření rizik.
Kontroluj	Kontinuální monitorování a přezkoumávání rizik.
Jednej	Udržování a zlepšování procesu řízení rizik a bezpečnosti informací.



Obr. 4: Procesní pohled na řízení rizik (Zdroj 4, str. 14)

1.7 Systém managementu služeb ITSM

Obecně je jako služba považováno dodávání hodnoty zákazníkovi (tj. tomu, kdo službu odebírá), přičemž tato hodnota spočívá v dosahování takových výsledků, které zákazník potřebuje, avšak bez toho, aby se sám stal vlastníkem specifických nákladů a rizik spojených s poskytnutím a dodávkou. Služba IT je speciální případ služby založené na použití informačních technologií (10).

„Služba IT v podniku = Explicitně definovaná a popsána funkcionalita, poskytovaná informačními technologiemi, která podporuje, či přímo umožňuje chod nějakého podnikového procesu, resp. podnikové činnosti“ (10, odst. 2).

Systém managementu služeb přispívá k neustálému zlepšování poskytovaných služeb díky trvalému řízení (5, str. 8 – 9).

1.7.1 Důvody zavedení systému řízení služeb

Systém řízení služeb přispívá k minimalizaci výpadků a zvýšení dostupnosti IT služeb, snížení nákladů na vývoj a dodávku IT služeb, zlepšení komunikace mezi poskytovatelem IT služeb a odběratelem daných služeb. Další výhodou je například schopnost rychle reagovat na velké množství změn a pružně přizpůsobovat IT služby požadavkům podnikání a zákazníků či certifikace celosvětově uznávaným standardem (12).

1.8 Normy ISO/IEC 20000

Pro organizaci může implementace normy ISO/IEC 20000 znamenat například zefektivnění činnosti při poskytování služeb v oblasti ICT. Následně pak snížení výskytu incidentů, nedostupnosti služeb ICT a snížení finančních ztrát (9).

Český překlad Informační technologie – řízení služeb vznikl z anglického Information management – Service management (dále jako zkratka „ITSM“). Pro zavádění,

integraci a neustálé zlepšování služeb vyžaduje používat již několikrát zmíněný PDCA cyklus. Podporováno a umožněno je bližší sladění s jinými normami, například s ISO/IEC 27001 (5, str. 8).

1.8.1 Norma ISO/IEC 20000-1

ISO/IEC 20000 je norma se zpřesněním a zpřísněním systémových norem pro služby ICT. Získání certifikace dle této normy přináší záruku, že prostředí, ve kterém jsou služby poskytovány je řízené a kontrolované (5, str. 8).

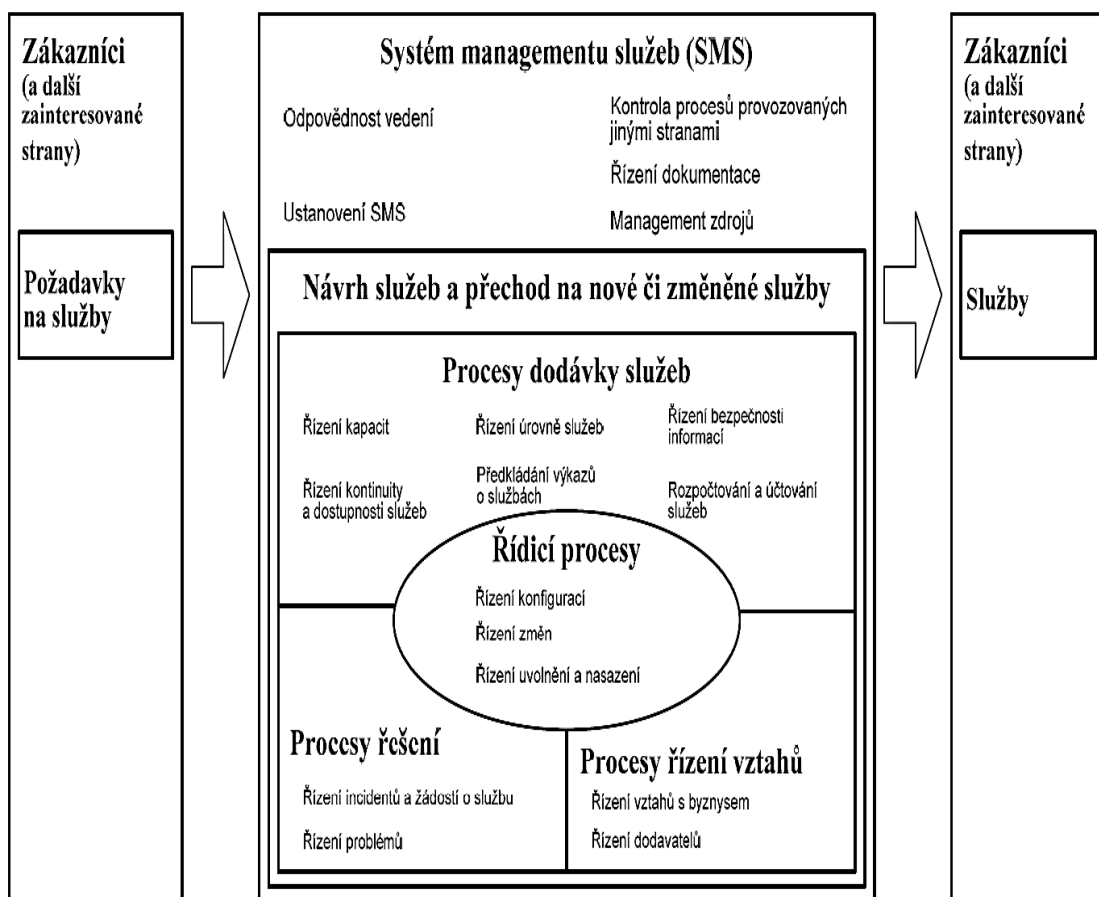
Tato část normy může být například použita organizací využívající službu jako ujištění naplnění požadavků služeb. Dále poskytovatelem služeb, který tak může prokázat svůj zájem o neustálé zlepšování jím poskytovaných služeb. Je vhodná pro monitorování, měření a přezkoumání procesů managementu služeb v organizaci. Auditor ji využije jako kritérium pro hodnocení. (5, str. 9)

- **Požadavky na ITSM, stanovené touto normou** (5, str. 18 – 39):
- **Odpovědnost vedení** - Vrcholové vedení musí být angažované a aktivní, zajistit správnost a úplnost politiky managementu služeb, stanovit pravomoci, odpovědnost a komunikaci.
- **Kontrola procesů provozovaných jinými stranami** (interní skupiny, zákazníci, dodavatelé) – neboli poskytnutí důkazů kontroly těchto procesů,
- **Řízení dokumentace** – je vyžadováno řízení, tvorba a údržba dokumentů a záznamů.
- **Management zdrojů** – určení a poskytování lidských, technických, finančních a informačních zdrojů.
- **Ustanovení a zlepšování SMS** – znamená vymezení rozsahu, plánování, zavádění a provozování, monitorování a přezkoumání, udržování a zlepšování SMS.
- **Návrh služeb a přechod na nové nebo změněné služby**

- **Proces dodávky služby** – je nutné zavést management úrovně, kontinuity, dostupnosti a bezpečnosti včetně rozpočtování a účtování.
- **Procesy řízení vztahů** – s rozlišením vztahů s byznysem a s dodavateli.
- **Procesy zajišťující řešení** – sem spadá řízení incidentů, žádostí o služby a řízení problémů.
- **Řídící procesy** – řízení konfigurací, změn, řízení uvolnění a nasazení služby.

1.8.2 Norma ISO/IEC 20000-2

Tato norma obsahuje doporučení, která je vhodné realizovat, aby bylo dosaženo požadovaných požadavků uvedených v první části (5, str. 9).



Obr. 5: Procesní pohled na systém řízení služeb (Zdroj 5, str. 11)

1.9 ITIL

ITIL je lehce upravitelný rámec „best practice“, založený na nejlepších zkušenostech z praxe, s pomocí kterého byznys organizace dosáhne požadovanou kvalitu IT služeb a překoná překážky, související s rozvojem svých IT systémů.

Fyzicky jde o sadu knižních publikací, která obsahuje sbírku nejlepších zkušeností z oboru řízení služeb informačních technologií. Název ITIL vznikl jako zkratka anglických slov „Information Technology Infrastructure Library“ (12).

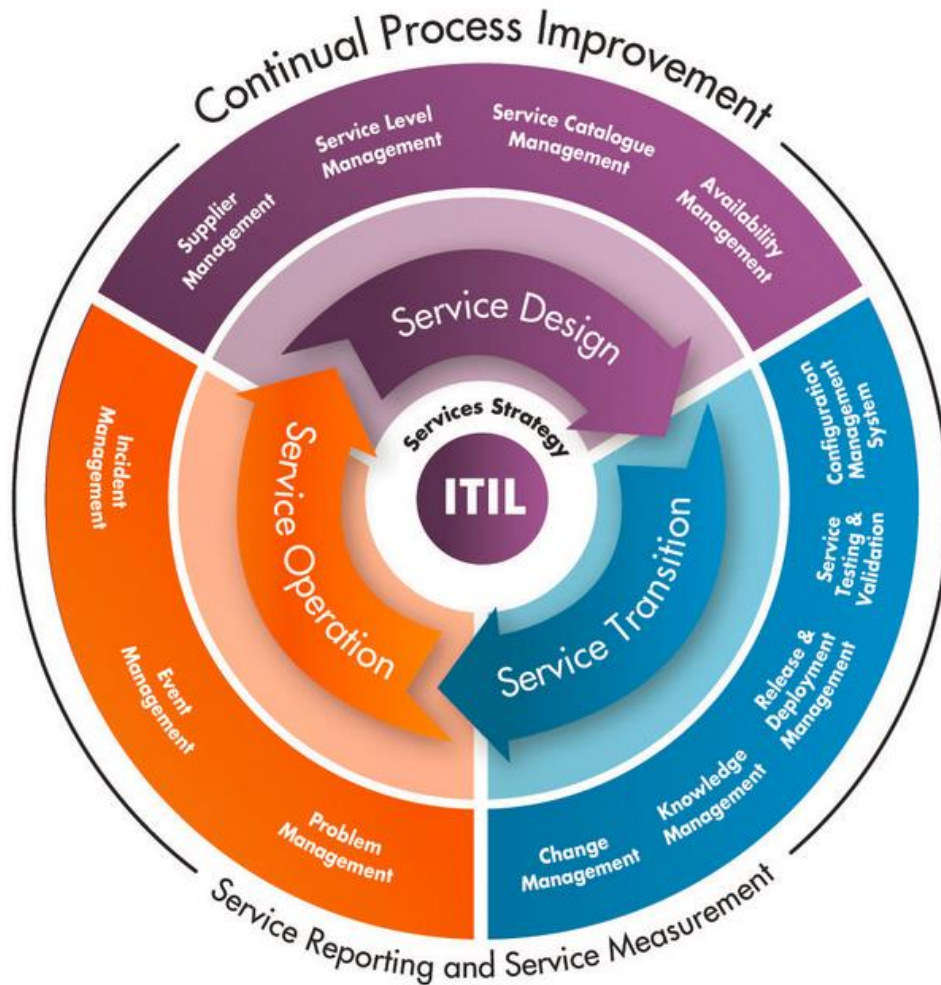
Ve své současné verzi obsahuje pět ústředních publikací, které se dají s výhodou využít pro zkvalitnění služeb a zajištění shody s ISO/IEC 20000.

Ústředních publikace ITIL (12):

- Service Strategy – strategické procesy,
- Service Design – návrh služeb,
- Service Transition – uvedení služby do provozu,
- Service Operation – provoz služeb,
- Continual Service Improvement – neustálé zlepšování.

Nespornou výhodou ITIL je nezávislost na platformě, která umožňuje široké využití ve všech oborech (12).

Přehled některých procesů a vztahů k publikacím, je znázorněn na obrázku níže.



Obr. 6: ITIL (Zdroj 16)

1.10 Kybernetická bezpečnost

Bezpečnost informací je přeneseně zakotvena i v Ústavě České republiky v čl. 1 a čl. 3, dle kterého je součástí ústavního pořádku České republiky Listina základních práv a svobod (dále jen „Listina“). V Listině není právo na respekt k soukromému životu garantováno v jednom všezahrnujícím článku, samotné právo na informační sebeurčení lze dovodit z čl. 10 odst. 3 Listiny, garantujícího jednotlivci právo na

ochranu před neoprávněným shromažďováním, zveřejňováním a-nebo jiným zneužíváním údajů o své osobě, a to ve spojení s čl. 13 Listiny, chránícím listovní tajemství a tajemství přepravovaných zpráv, ať již uchovávaných v soukromí, nebo zasílaných poštou, podávaných telefonem, telegrafem nebo jiným podobným zařízením anebo jiným způsobem. Svou povahou i významem tak právo na informační sebeurčení spadá mezi základní lidská práva a svobody, neboť spolu se svobodou osobní, svobodou v prostorové dimenzi (domovní), svobodou komunikační a zajisté i dalšími ústavně garantovanými základními právy dotváří osobnostní sféru jedince, jehož individuální integritu jako zcela nezbytnou podmínku důstojné existence jedince a rozvoje lidského života vůbec je nutno respektovat a důsledně chránit; zcela právem jsou proto respekt a ochrana této sféry garantovány ústavním pořádkem (40).

Parlament České republiky schvaluje a vydává různé právní předpisy a nařízení k posílení důvěry, integrity a dostupnosti dat, informací, systémů a dalších prvků. Dává tím jasně najevo, že si uvědomuje závislost na ICT, kdy by případné narušení bezpečnosti mohlo mít kritické následky (17).

Zákony, které tuto problematiku upravují, či zmiňují (17):

- zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti),
- zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích),
- zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti,
- zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu),
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů,
- zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů,
- zákon č. 40/2009 Sb., trestní zákoník,

- zákon č. 89/2012 Sb., občanský zákoník,
- zákon č. 90/2012 Sb., o obchodních korporacích.

1.10.1 Zákon o kybernetické bezpečnosti

Zákon č. 181/2014 Sb. O kybernetické bezpečnosti a o změně souvisejících zákonů.

Tento zákon zavádí jednotná řešení a bezpečnostní standardy pro komplexní oblast informační bezpečnosti. Vztahuje se především na takové systémy, kde by narušení jednoho ze základních bezpečnostních aspektů (důvěrnosti, dostupnosti nebo integrity) mohlo způsobit ohrožení státu a jeho občanů (18).

Jedná se o reakci na nedostatek koordinace v této problematice v rámci organizací. Tento zákon nepůsobí plošně – jsou definována jasná kritéria, která musí být naplněna (podle nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury), aby se organizaci zákon vztahoval. Myšleny jsou zde nejen o organizace zřizované státem, ale i o soukromoprávní (např. energetické společnosti, banky aj.) (17).

„Významný informační systém je informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci“ (19, str. 1).

Bližší informace o kritériích pro stanovení významného informačního systému lze najít ve vyhlášce č. 317/2014 Sb., o významných informačních systémech a jejich určující kritéria.

„Kritickou informační infrastrukturou je prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti“ (19, str. 1).

Prioritou zákona je zajistit, aby si dané organizace a jejich zaměstnanci uvědomovali všechna bezpečnostní rizika informací a především, aby byla nalezena a zavedena vhodná opatření s dostatečnou bezpečnostní úrovní. Organizace také musí zajistit detekci a hlášení bezpečnostních incidentů. Cílem tedy není zasahovat do obsahu, ale to, aby organizace zajistily integritu, důvěrnost a dostupnost informací (17).

Předmět úpravy:

„1. Tento zákon upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti“ (19, str. 1).

„2. Tento zákon se nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi“ (19, str. 1).

Zákon pro dotčené subjekty, mimo jiné, stanovuje:

Povinnosti – podle typu subjektu (19, str. 3 – 9):

- *základní* (hlásit kontaktní údaje, detekovat kybernetické bezpečnostní události, hlásit kybernetické bezpečnostní incidenty, zavádět bezpečnostní opatření),
- *při stavu kybernetického nebezpečí* (hlásit kontaktní údaje, provádět reaktivní opatření, zpracovávat bezpečnostní dokumentaci, hlásit kybernetické bezpečnostní incidenty, zavádět bezpečnostní opatření),
- *nahlášení kontaktních údajů, hlášení incidentů, zavedení bezpečnostní opatření, činit opatření.*

Postihy – podle nesplněné podmínky (19, str. 16 – 17):

Za neplnění povinností, které zákon č. 181/2014 Sb. přináší, hrozí finanční postih. Pro významné informační systémy je nastaveno pět typů sankcí s hodnotou do 100 000 Kč.

1.10.2 Management kybernetické bezpečnosti

Management kybernetické bezpečnosti je specifikován Vyhláškou č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti).

Tato vyhláška stanovuje

1) Bezpečnostní opatření (20, str. 2 – 17):

- *Organizační* – řízení aktiv, řízení rizik, bezpečnostní politika,
- *Technická* – fyzická bezpečnost, nástroje ochrany, ověřování a řízení, nástroje detekce, aplikační bezpečnost, kryptografické prostředky, bezpečnost průmyslových a řídicích systémů.

2) Bezpečnostní dokumentaci a její obsah (20, str. 18):

- Bezpečnostní dokumentace vychází z ISO/IEC 27001 a dá se říct, že subjekt, který splňuje certifikaci dle ISMS s velkou pravděpodobností splňuje i podmínku na soulad se zákonem o kybernetické bezpečnosti, ale pouze v případě, že určený prvek kritické informační infrastruktury je zahrnut do rozsahu ISMS.

3) Kybernetické bezpečnostní incidenty (20, str. 19 – 20)

- Kybernetické bezpečnostní incidenty jsou rozděleny podle typů příčin a dopadů. Například bezpečnostní incident způsobený škodlivým kódem, překonáním technických opatření nebo porušením organizačních opatření. Podle dopadu byly stanoveny tyto typy kybernetických bezpečnostních incidentů – narušením důvěrnosti aktiv, narušením integrity aktiv, narušením dostupnosti aktiv či jejich kombinací.
- Následně jsou kybernetické bezpečnostní incidenty kategorizovány (jako velmi závažný kybernetický bezpečnostní incident, závažný kybernetický bezpečnostní incident a méně závažný kybernetický bezpečnostní incident).

2 Analýza současného stavu

Tato část práce obsahuje požadavky, které zadavatel, Celní správa České republiky, stanovil k provedení. Poté následuje krátké všeobecné seznámení se s organizací, jako takovou. Dále je prošetřen aktuální stav v organizaci vzhledem ke stanoveným požadavkům. Poslední podkapitola obsahuje shrnutí nabytých poznatků.

Při zpracování jsem vycházela z reálných podkladů, tedy na základě mnou vyhodnocených dotazníků, předložené dokumentace a z poznatků, které jsem získala od pověřených osob.

2.1 Požadavky zadavatele

Hlavním přáním zadavatele je posouzení, zda jsou plněna kritéria normy ČSN ISO/IEC 27001:2014 (ISMS), včetně návaznosti na normu ČSN ISO/IEC 20000-1:2012. V souvislosti s problematikou managementu bezpečnosti si organizace přeje posoudit, zda její bezpečnostní dokumentace vyhovuje nově schválenému kybernetickému zákonu.

V případě, že odhalím pochybení, především proti požadavkům normy ČSN ISO/IEC 27001:2014, žádá Celní správa České republiky o označení konkrétního problému a navržení možností pro jeho napravení. Organizace sama přiznává, že si uvědomuje vlastní rezervy v managementu bezpečnosti, především, co se jeho praktické aplikace v reálném prostředí týká.

2.2 Celní správa České republiky

Celní správa České republiky je soustavou správních orgánů a ozbrojeným bezpečnostním sborem s mnoha kompetencemi svěřenými za účelem prosazování ekonomického zájmu státu a jeho občanů a ochrany národního i evropského

mezinárodního trhu. Dále se i aktivně podílí na zajišťování bezpečnosti v rámci evropského prostoru (23).

2.2.1 Seznámení se s organizací

Orgány Celní správy České republiky jsou Generální ředitelství cel (dále také „GŘC“) a jemu podřízené celní úřady, které jsou správními úřady. Celních úřadů je celkem 15. Jejich územní působnost se kryje s vyššími územněsprávními celky – kraji (24).

Rozmístění a organizační struktura (Stav k 15. 4. 2015):

Hlavní sídlo: Budějovická 7, 14096 Praha 4

Vedení: Generální ředitel Generálního ředitelství cel
brig. gen. Mgr. Petr Kašpar

Rozmístění a organizační struktura jsou vyobrazeny na následujících dvou stranách.



CELNÍ SPRÁVA
ČESKÉ REPUBLIKY

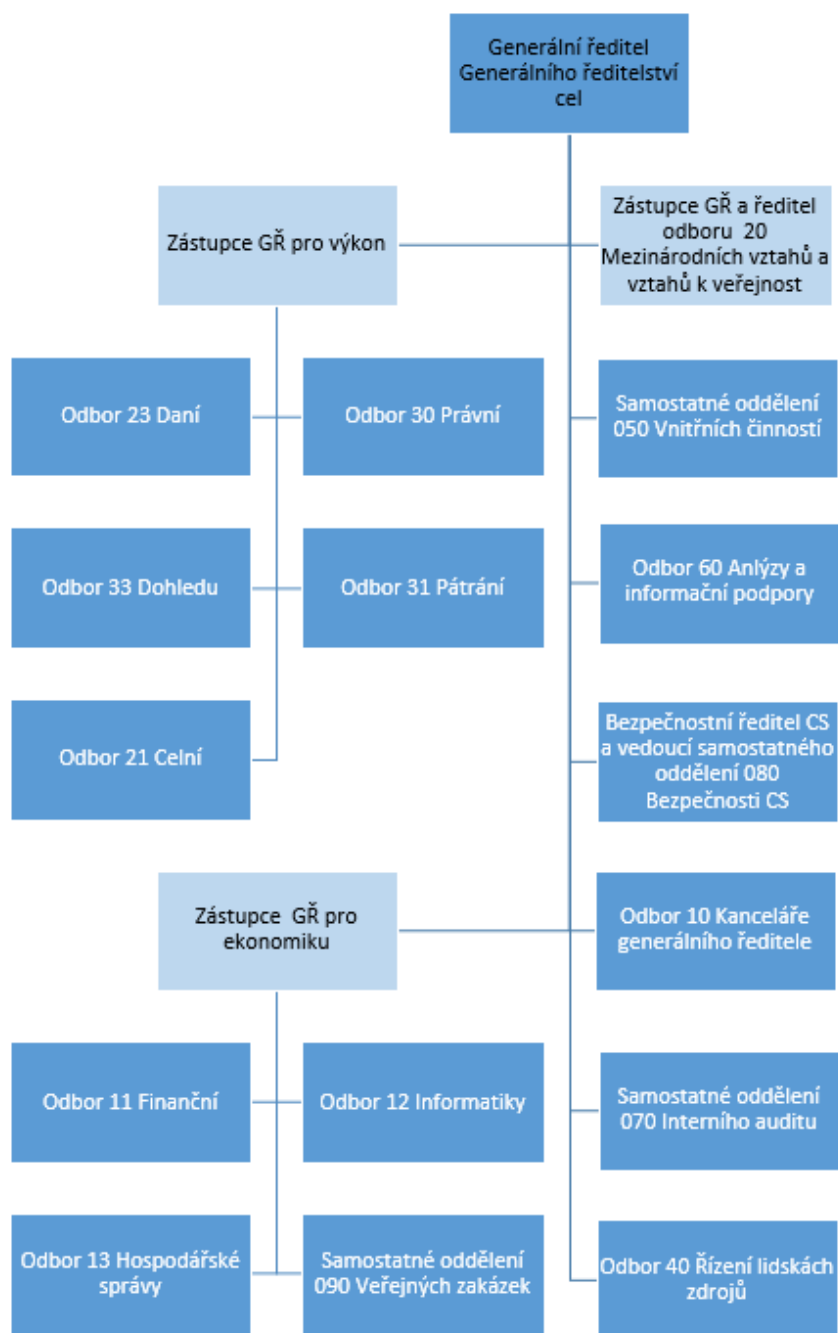
www.celnisprava.cz

THE CUSTOMS ADMINISTRATION
OF THE CZECH REPUBLIC

www.czechcustoms.eu



Obr. 7: Mapa sídel Celní správy České republiky (Zdroj 24)



Obr. 8: Organizační struktura Generálního ředitelství cel (Upraveno dle 24)

Kompetence CS

Mezi hlavní kompetence patří správa cel a některých daní, především spotřebních, celní dohled nad pohybem zboží, ochrana práv duševního vlastnictví, odhalování trestné činnosti, boj proti organizovanému zločinu a globálnímu terorismu, výběr a vymáhání poplatků, kontrola zaměstnávání cizinců, kontrola povinného značení lihu, řízení o přestupcích ve své kompetenci a další (25).

Legislativní vymezení CS

Existence a rozsah působení jsou přesně vymezeny legislativou české republiky, zejména předpisem č. 17/2012 Sb., zákonem o Celní správě České republiky, ve znění pozdějších předpisů (23).

Vize

Vizí Celní správy České republiky je být moderní, strategicky a procesně řízenou organizací, která ve svých kompetencích odvádí kvalitní a účinné výsledky (23).

Mise

Prosazování ekonomických zájmů státu a jeho občanů, ochrana národního a evropského trhu, podílení se na zajištění bezpečnosti státu, občanů a evropského bezpečnostního prostoru na základě přidělených kompetencí (23).

Strategické cíle

Pro období 2013 – 2017 byly mimo jiné vymezeny tyto strategické cíle (23):

- Dosáhnout nulové tolerance obchodním podvodům,
- Zvýšit dobrovolné plnění daní a cel,
- Efektivnější nastavení nosných procesů (zjednodušení, napřímení a integrace),
- Zavést systém řízení jakosti v Celní správě České republiky.

Informační systém Celní správy České republiky ISCS

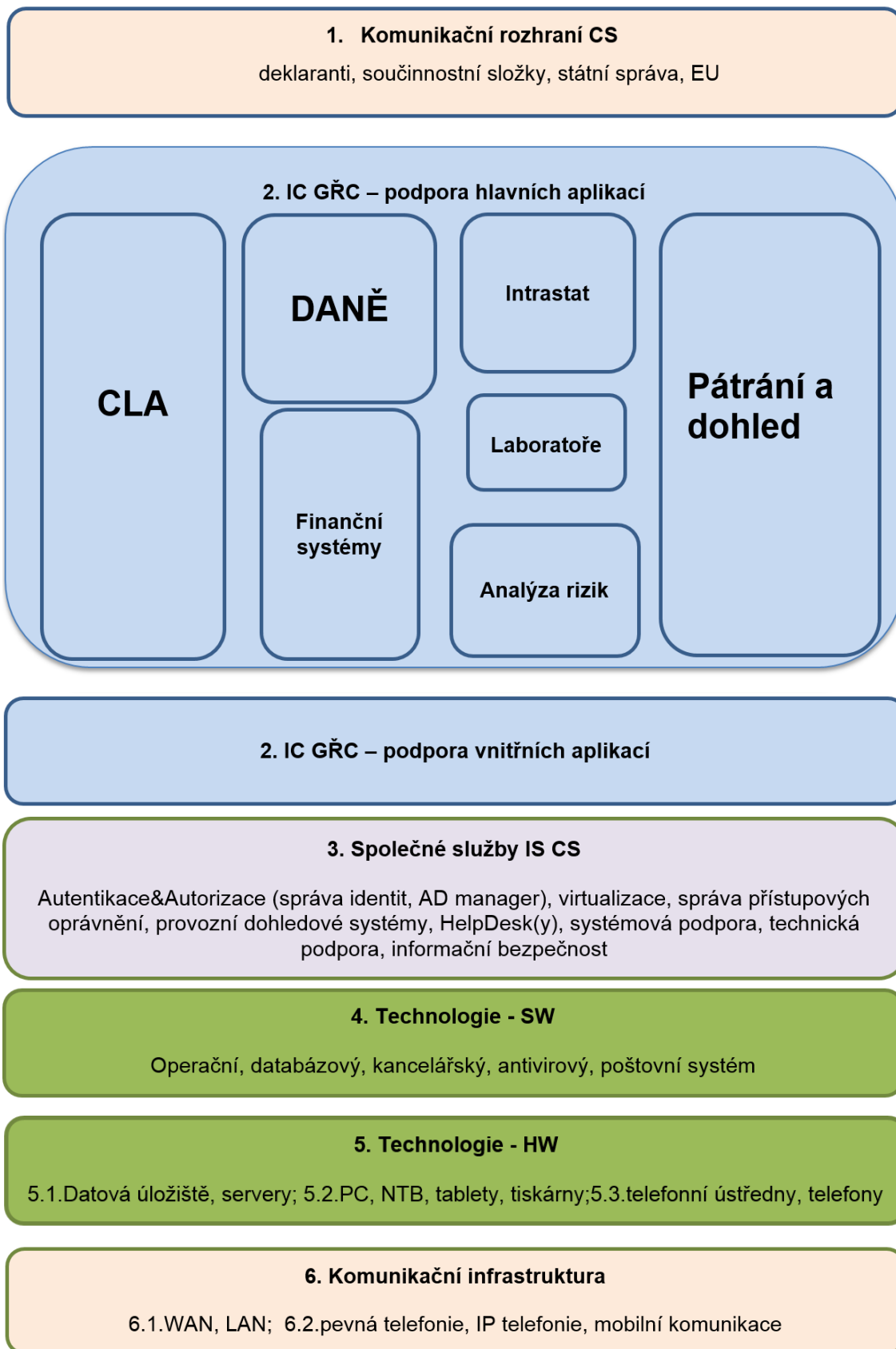
Jak je patrné z výše uvedeného, Celní správa České republiky zpracovává a schraňuje enormní množství dat a informací. Za tímto účelem využívá a spravuje informační systém (dále „ISCS“). Správou tohoto systému je pověřen Odbor 12 Informatiky (26).

Odbor 12 Informatiky

Tento odbor je začleněn do organizační struktury GŘC a společně s dalšími tzv. „back office“ odbory přímo podléhá zástupci generálního ředitele pro ekonomiku. V jeho kompetencích jsou společné činnosti jako nákup, vývoj SW, bezpečnost ISCS, komunikace s evropskými systémy cla a daní a provoz centrálních aplikací včetně výpočetního centra zajišťují oddělení dislokované na GŘC v Praze. Provoz ISCS včetně uživatelské podpory jednotlivých celních úřadů pak zajišťuje osm detašovaných oddělení Odboru 12 geograficky rozmístěných po celém území ČR. Tato detašovaná oddělení mají také některé celorepublikové kompetence, například DO 128.8 Ústí nad Labem zodpovídá za provoz systému e-learningu, DO 128.1 Brno za provoz centrálního číselníkového řetězce, jehož výstupy používají všechny celní aplikace (26).

Architektura ISCS

Schématické zobrazení architektury ISCS je na obrázku č. 9. *„ISCS je na vnější okolí (deklaranti, státní správa, součinnostní složky, EU) připojen prostřednictvím komunikačních bran (1). Na tyto komunikační brány je napojeno informační centrum GŘC (pozn. dále v textu jen „IC“), kde jsou provozovány centrální aplikace v architektuře klient-server (2). Aplikace pro pátrání a dohled jsou z bezpečnostních důvodů provozovány mimo IC GŘC. Aplikace jsou provozovány na HW- aplikačních a databázových serverech s využitím ukládání dat na diskových polích (5.1). Aby zaměstnanci CS mohli využívat aplikací provozovaných v IC GŘC, musí být k dispozici společné služby (3). Konektivita ze všech regionů CS je zabezpečena komunikační infrastrukturou (6.1) z lokálních pracovišť vybavených odpovídajícím SW (4) a HW (5.2). Hlasové služby jsou zabezpečeny prostřednictvím HW (5.3) a komunikační infrastruktury (6.2).“*, (27, str. 9).



Obr. 9: Schéma informačního systému CS (Upraveno dle 27, str. 8)

ICT strategie Celní správy České republiky (27, str. 9 – 15):

Strategie ISCS pro roky 2014 – 2016 a strategické cíle ISCS jsou stanoveny v návaznosti na Strategii Celní správy České republiky pro roky 2013 – 2017 a pro ICT byly definovány tyto hlavní strategické cíle:

- Zabezpečit vysokou kvalitu a dostupnost ICT služeb,
- Realizovat rozvoj technologické základny ISCS,
- Zabezpečit vysokou úroveň bezpečnosti ISCS,
- Zabezpečit vysoký stupeň integrace ISCS.

Stanovením těchto cílů se Celní správa České republiky zavázala například k dalšímu zlepšování poskytovaných služeb v oblasti ICT dle normy ČSN ISO/IEC 20000. (Základem pro poskytování služeb je schválený Katalog služeb a klíčovou službou je dostupnost a spolehlivost aplikací IC GŘC.)

Dále modernizovat technologickou základnu ISCS jako základní předpoklad udržení vysoké úrovně poskytování požadovaných služeb. V tomto období se CS chce také věnovat přechodu na mobilní zařízení a mobilní komunikace.

Ke strategickému cíli zabezpečit vysokou úroveň bezpečnosti ISCS je stanoven požadavek trvale zvyšovat bezpečnost provozu a ochranu informací při poskytování služeb a dosažení vyšší úrovně provázání metodických podkladů a konkrétních bezpečnostních opatření.

2.2.2 Historické hledisko bezpečnosti informací a kvality služeb

Aktuální stav je výsledkem postupné mnohaleté snahy zavést certifikaci podle norem ČSN ISO/IEC 2000:1 a ČSN ISO/IEC 27001.

O certifikaci Celní správa České republiky začala uvažovat v roce 2007 a v roce 2010 proběhla první certifikace podle normy ČSN ISO/IEC 20000:1. K certifikaci byly

navrženy procesy z oblasti poskytování služeb IT, zajištěné v souladu s organizačním řádem CS, odborem 12 GŘC (26).

V roce 2010 došlo ke standardizování pracovních postupů v jednotlivých procesech v rámci ISCS. Nezávislý audit byl proveden společností Tayllor&Cox s.r.o a následně vydán certifikát podle ISO/IEC 20000-1.

V témže roce nadále pokračovaly přípravy i pro certifikaci dle ČSN ISO/IEC 27001 – postupné zpracovávání potřebné dokumentace, byla provedena kontrola ISCS v Plzni a v Praze a začaly být plněny související úlohy jako kontrolní dny, porady, školení zpracování posudků analýz, stanovisek a podobně. Došlo k prvnímu zpracování akvizičních a vývojových bezpečnostních záměrů a budování základů pro havarijní plánování (26).

Pro rok 2011 byl vytyčen cíl zavedení ISMS v rámci GŘC odboru 12, spočívající v dopracování chybějící dokumentace a implementace chybějících bezpečnostních opatření dále novelizace již některých vydaných dokumentů v předchozích letech. Úkol byl splněn a úspěšně získán certifikát pro poskytování systémových integrovaných IT služeb ve shodě s požadavky normy ČSN ISO/IEC 27001. Nezávislý audit byl proveden společností Tayllor&Cox s.r.o a následně byl touto společností vydán certifikát dle ČSN ISO/IEC 27001 :2005 (26).

V následujících letech došlo k řadě změn, které se promítaly do procesů organizace a mnoho dokumentů muselo projít revizemi a následně být aktualizováno – například v roce 2012 došlo k významné změně organizační struktury. Celní správa aktivně rozšířila rozsah ISMS (26). V roce 2013 došlo k úspěšné recertifikaci ITSM dle ISO/IEC 20000-1:2011. O rok později byl úspěšně recertifikován i ISMS podle ISO/IEC 27001:2013.

V průběhu roku 2014 se Celní správa začala připravovat na chystaný kybernetický zákon, který jí, jako významnému informačnímu systému, ukládá náležitě povinnosti, které k 1. 1. 2015 nabyly účinnosti. Nyní má Celní správa České republiky

rok na to, aby řádně splnila veškeré požadavky tohoto zákona. Pokud by od 1. 1. 2016 byla zjištěna pochybení, pak může následovat peněžité postih (26).

Aplikace v rámci CS

Celní správa České republiky využívá okolo 180 aplikací. Kdyby mělo dojít k jejich pomyslnému seřazení podle priorit, pak nejdůležitějšími jsou ty, které slouží pro odvod peněz ze cla do EU. Dále aplikace určené ke komunikaci s ostatními státními orgány, například daňovou správou či policií. Důležité jsou aplikace pro přímou komunikaci s veřejností, sloužící například k podávání celních prohlášení a komunikaci ohledně daní, a aplikace pro interní komunikaci.

Aplikace je možné rozdělit podle typu služby na

- *aplikační* – ASEO, EMCS, ETK, ZAR a mnoho dalších,
- *informační* – zajištění provozu e-learningu, datový sklad, správa identit a podobně,
- *infrastrukturní* – zde se jedná převážně o služby sítě, např. správa aktivních a pasivních prvků lokální sítě CS,
- *podpůrné* – různé dohledové, správní, zálohovací aplikace,
- *vývojové* – pro tvorbu aplikací a maker, analýzu, vývoj a testování.

Významné aplikace:

- *ASEO* – slouží k jednotné správě celních povolení a následnému ověřování uživatelů.
- *EMCS* – elektronický systém, který slouží pro přepravu a sledování výrobků podléhajících spotřební dani. Zavedení EMCS umožňuje zjednodušení pohybu zboží mezi členskými zeměmi EU. Podstatou tohoto systému je nahrazení papírových průvodních dokladů elektronickými.
- *ETK* – tato aplikace slouží pro sledování a řízení tranzitních a vývozních operací.
- *NWKII* – aplikace pro deklaranty umožňující podání celních prohlášení do režimu tranzitu, vývozu, umožňuje sledovat stav čerpání záruk a povolení.

- *ICS* – aplikace pro sledování a řízení dovozních operací.
- *ZAR* – aplikace zajišťuje elektronickou výměnu informací o zárukách se všemi zeměmi Úmluvy o společném tranzitu, s uživateli záruk a s emitenty záručních dokladů a spravuje záruky a registruje jejich použití.
- *ECDC* - modulová aplikace pro evidenci cla a daní, odvod cla do EU, spojení s pokladnou a bankami.

2.3 Systém řízení informační bezpečnosti v Celní správě České republiky

Systém managementu bezpečnosti ISCS je ustanoven v rozkazu č. 92/2014 Politika kybernetické bezpečnosti informačního systému Celní správy České republiky. Tento rozkaz byl schválen generálním ředitelem GŘC a následně publikován. V rozkazu je ředitel odboru 12 informatiky GŘC stanoven jako správce ISCS ve smyslu zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Pověřenou osobou k jednání ohledně tohoto zákona je pak stanoven vedoucí referátu bezpečnosti informací GŘC.

Politika kybernetické bezpečnosti ISCS je uvedena v Příloze č. 1 k rozkazu GŘC č. 92/2014.

Rozsah systému řízení bezpečnosti informací

Rozsah systému se vztahuje na všechny oblasti a procesy ISMS na Odboru 12 GŘC Informatiky. Dále na Odbor 60 GŘC Analýzy a informační podpory. Odbor 12 GŘC provádí řízení ICT v rámci Celní správy České republiky prostřednictvím detašovaných oddělení informatik v Brně, Českých Budějovicích, Hradci Králové, Olomouci, Ostravě, Plzni, Praze a Ústí nad Labem. Tyto lokality jsou rozděleny do bezpečnostních domén s označením BD 01 až BD 09. Samostatná a bezpečnostní doména BD 10 je provozována nezávisle Odborem 60 GŘC, který má speciální postavení.

Služební předpis č. 9/2012 stanovuje rozsah ISMS na informace a prostředky pro jejich zpracování v rámci ISCS. Hranice ISMS je tvořena vstupními a výstupními místy mezi ISCS a externími počítačovými sítěmi

2.3.1 Kontext organizace

Kontext organizace byl popsán v předcházejících kapitolách, kde došlo k seznámení s organizací.

2.3.2 Vůdčí role

Bezpečnostní politika doplňuje závazek Strategie rozvoje Informačního systému Celní správy České republiky na roky 2014-2016, kde je jako jeden z cílů i zabezpečení vysoké úrovně bezpečnosti ISCS (trvale zvyšovat bezpečnost informací a prostředků pro zpracování informací CS tak, aby byla v souladu s certifikáty ISMS a ITSM). Další vytyčený cíl k bezpečnosti informací zní – Trvale zvyšovat úroveň bezpečnosti ISCS v souladu s ČSN ISO/IEC 27001 zabezpečit požadavky dohledových (recertifikačních) auditů.

Vedení Odboru 12 informatiky GŘC schválením těchto dokumentů deklaruje svůj zájem o rozvoj a neustálé zlepšování informační bezpečnosti ISCS. V návaznosti na nový zákon č. 181/2014 Sb., o kybernetické bezpečnosti navíc vedení CS schválilo vytvoření specializovaného útvaru ISCS, referát Bezpečnosti IS CS, založený za účelem kompletního řešení problematiky ISMS pro CS.

Vedení CS jsou ve stanovených intervalech předkládány zprávy o fungování ISMS, které jsou dále komunikovány v ohledu na Politiku kybernetické bezpečnosti informačního systému Celní správy České republiky.

Zmíněnou politiku ISCS stanovuje a schvaluje vedení a to ve stanovených intervalech. Tato politika musí být průběžně zkoumána, a je vyhodnocováno, zda jsou naplňovány její vytyčené cíle. Tato politika je dokumentovaná a dostupná zainteresovaným stranám, za účelem zlepšování daných procesů.

Zřízení a obsazení bezpečnostních rolí v působnosti odboru 12 GŘC je stanoveno v interním příkazu č. 15/2014.

2.3.3 Plánování

Bezpečnostní rizika jsou stanovena, posuzována, identifikována, analyzována a hodnocena na základě metodiky Riziková analýza ISCS. Riziková analýza je vykonávána v souladu s Vnitřním pokynem č. 13/2010 – Pravidla řízení rizik informačního systému CS České republiky. Nevyhnutelná zbytková rizika jsou schvalována ředitelem odboru 12 GŘC v rámci analýzy.

Bezpečnostní cíle ISCS jsou stanoveny na základě plánu zvládnutí reálných rizik ISCS pro období 2014 – 2016, který je konzistentní s politikou ISCS a dalšími procesy minimalizace rizik bezpečnosti schraňovaných informací. Tyto cíle jsou v Knihovně ISCS. Cíle jsou vzájemně doplňující se s politikou kybernetické bezpečnosti ISCS a v případě potřeby aktualizovány.

2.3.4 Podpora

Kompetence a kompetentní osoby - Odbor 12 GŘC má rozsah, odpovědnost a určení do bezpečnostních rolí stanovené interním příkazem ředitelem odboru 12 č. 15/2014 Zřízení a obsazení bezpečnostních rolí v působnosti odboru 12 GŘC. Odbor 60 GŘC má rozsah, odpovědnost a určení do bezpečnostních rolí stanovené interním příkazem ředitelem odboru 60 č. 2/2014 Zřízení a obsazení bezpečnostních rolí v působnosti odboru 60 GŘC.

Pro zvyšování povědomí o ISMS zaměstnanců CS slouží e-learningové proškolení, které je prováděno jednou ročně na základě přílohy č. 2 k vnitřnímu pokynu č. 96/2012 Řízení bezpečnosti informačního systému Celní správy České republiky. Výsledky tohoto kurzu jsou analyzovány a dále komunikovány, za účelem neustálého zlepšování, v souhrnné zprávě, která je uložena a archivována stanoveným způsobem.

Termíny zasedání a porad jsou pevně dané a dokumentované. Na poradách se komunikuje směřování bezpečnosti informací Celní správy, jsou vyhodnocovány dosavadní kroky a jsou schvalovány a řešeny další postupy. Veškeré informace ze zasedání a schůzí jsou uchovávány v dokumentované podobě.

Veškeré potřebné informace týkající se bezpečnosti informací Celní správy České republiky jsou dokumentovány a řízeny. Dokumenty, které musí být vzhledem k ISMS vytvořeny jsou stanoveny v příloze č. 3 služebního předpisu č. 9/2012 a v metodice Správa bezpečnostní dokumentace ISCS.

2.3.5 Provozování

Všechny procesy potřebné ke splnění požadavků bezpečnosti jsou plánovány a implementována taková opatření a plány, které pomáhají předcházet nechtěným situacím. Dále jsou přijímána opatření ke snížení nepříznivých dopadů bezpečnostních incidentů.

Outsourcové procesy jsou řízeny formou vzorových smluvních dodatků a akceptačních listů. Dokumenty, které musí být vzhledem k ISMS vytvořeny jsou stanoveny v Příloze č. 3 Služebního předpisu 9/2012.

Pro podporu ISMS je vytvořeno fórum ISMS tvořené manažerem ISMS, auditorem ISMS a doménovými manažery ISMS. Fórum se schází nejméně dvakrát ročně. Jsou stanoveny pravidelné porady správce ISMS se správci bezpečnostních domén ISCS. Z jednání jsou pořizovány záznamy v podobě zápisů. Posuzování rizik bezpečnosti informací je stanoveno ve Vnitřním pokynu č. 9/2012 – Pravidla zvládání bezpečnostních incidentů ISCS a v metodice Zvládání bezpečnostních incidentů ISCS.

2.3.6 Hodnocení výkonnosti

Účinnost bezpečnostních opatření ISMS je pravidelně hodnocena v rámci kontrol bezpečnostních opatření ISCS. Všechny dokumenty a záznamy jsou řízeny manažerem ISMS. Opatření k nápravě z auditů a dohledů jsou uváděna v dokumentu Nápravná a preventivní opatření v oblasti řízení bezpečnosti ISCS, která tak slouží zainteresovaným osobám (manažer ISCS, správci bezpečnostních domén) k neustálému zlepšování. Vnitřní audit je implementován, ustanovován a plánován Odborem 12 GŘC.

2.3.7 Zlepšování

Vhodnost, přiměřenost a efektivnost ISMS je neustále zvyšována na základě získaných praktických poznatků a zkušeností, výsledků interních a externích auditů, školení. Jsou přijímána taková opatření, která snižují nedostatky, tak aby bylo dosahováno neustálého zlepšování v oblasti bezpečnosti informací.

2.4 Systém managementu služeb informačních technologií v Celní správě České republiky

Tato podkapitola slouží ke zjištění aktuálního stavu ITSM v Celní správě České republiky.

2.4.1 Všeobecné požadavky na systém

Rozsah systému managementu – IT služby jsou poskytovány GŘC Odborem 12 a odběratelem je Celní správa České republiky. Tyto služby (Helpdesk) jsou v poskytovány v oblasti provozu a podpory centrálních aplikací a slouží jak pro interní, tak externí uživatele informačního centra a centrálních aplikací. Podpora a správa aplikačních služeb je poskytována z lokalit Budějovická 7, 140 96 Praha 4 a z Nám. Svatopluka Čecha 4, 702 00 Ostrava – Přívoz.

Rozsah a úroveň služeb IT vymezuje Katalog služeb, který zahrnuje úplný výčet služeb a činností odboru 12 GŘC, jakožto poskytovatele. Katalog služeb je pravidelně,

nejméně jedenkrát ročně aktualizován odborem 12 GŘC na základě požadavků vlastníků hlavních a podpůrných procesů CS.

Odpovědnost vedení – Vrcholové vedení CS je plně angažované, politika managementu služeb je nastavena, schválena a pravidelně konzultována s vedením. Tato politika slouží k podpoře a trvalému prosazování principů managementu služeb IT podle normy ČSN ISO/IEC 20000 v kontextu realizace CS jako plně procesně řízené organizace.

Politika je stanovena služebním předpisem č. 12/2013 Systém managementu služeb informačních technologií v Celní správě České republiky a její znění je v příloze č. 1 k tomuto předpisu.

Interní předpisy a dokumentace – Uplatňování politiky ITSM, dokumentace procesů a způsob realizace jsou dány služebním předpisem č. 12/2013 Systém managementu služeb informačních technologií v Celní správě České republiky. Jsou vytvořeny webové stránky Fórum ITSM, obsahující veškeré dokumenty vytvořené ohledně ITSM. Web je dostupný v rámci CS. Dokumentace je rozdělena na dokumenty a záznamy.

Kontrola procesů provozovaných jinými stranami – Jde vidět snaha o řešení pomocí SLA smluv. Vzor podoby SLA smluv je daný. Podpora SLA smluv se ale v minulosti nesečkala s plnou podporou vedení.

Řízení dokumentace – Řízení, tvorba a údržba dokumentů a záznamů probíhá v souladu se stanovenými požadavky.

Management zdrojů – Určení a poskytování lidských, technických, finančních a informačních zdrojů je ve shodě s normou ISO/IEC 20000-1.

Ustanovení a zlepšování ITSM – Vymezení rozsahu, plánování, zavádění a provozování, monitorování a přezkoumání, udržování a zlepšování je aplikováno na všechny procesy ITSM. Jsou plněny všechny základní požadavky. Služby jsou

monitorovány. Monitoruje se například dostupnost služby, dostatek kapacit a podobně. Následně je prováděn rozbor příčin (za využití statistických metod). Služby jsou monitorovány na základě SLA smluv a na základě monitorování jsou navrhována zlepšení služeb. Všechny podstatné záležitosti v rámci procesu jsou konzultovány a schvalovány fórem ITSM.

2.4.2 Návrh služeb a přechod na nové nebo změněné služby

Nové služby a požadavky na změny ve službách jsou plánovány a implementovány v souladu s ISO/IEC 20000. Je využívána aplikace Business Mashups. Služby jsou definované prostřednictvím SLA mezi dodavatelem a zákazníkem. Rozšiřování probíhá podle požadavků, kapacit a schváleného rozpočtu.

2.4.3 Proces dodávky služby

Management úrovně služeb – K některým službám v rámci ITSM jsou vypracovány a uzavřeny SLA smlouvy, které jsou pravidelně přezkoumávány. Existují problémy týkající se SLA smluv. SLA smlouvy nejsou dostatečně využívány jako prostředek uzavírání interních dohod o úrovni poskytovaných služeb.

Předkládání výkazů o službách – Jsou prováděny pravidelné měsíční reporty zavedených služeb, výstupy jsou k zobrazení na webu ITSM. Některé reporty jsou automatické (reakční doby, doby řešení a podobně) prostřednictvím aplikace HelpLine.

Management kontinuity a dostupnosti služeb – Servery informačního centra jsou virtualizovány, je provozováno 108 virtuálních serverů. Tři fyzické servery jsou využívány pro ostrý provoz a další dva pro testování.

Hlavní novinkou v této oblasti je schválený projekt realizace záložního informačního centra v datovém centru Státní tiskárny cenin. Toto záložní informační centrum je zároveň nutnou podmínkou pro poskytování IT modulů formou služby ostatním členským státům EU.

Rozpočtování a účtování služeb – Tento proces je prováděn v souladu s legislativou a interními předpisy organizace. Stav rozpočtu je reportován, plánován a schvalován.

Management kapacit – Je prováděn v rámci svěřené rozpočtové částky a jednotlivé položky jsou plánovány v ohledu na průběh výdajů v minulosti a s maximálním zohledněním všech požadavků organizace.

Management bezpečnosti informací – Organizace vlastní v této oblasti managementu certifikaci dle ISO/IEC 27001. Proces evidence bezpečnostních incidentů je realizován prostřednictvím samostatného modulu HelpLine.

2.4.4 Procesy řízení vztahů

Management vztahů s byznysem – CS má k dispozici technologie, pomocí kterých zjišťuje spokojenost zákazníků. Využívá Business Mashup aplikaci k dokumentování vztahů mezi zákazníkem a dodavatelem vztahů.

Management vztahů s dodavateli – Vztahy s dodavateli jsou řízeny pomocí standardních smluv. Existuje celá řada dodavatelů. Na všechny dodávky jsou uzavřeny smlouvy, které se jednou za rok přezkoumávají a vyhodnocují a podle potřeb upravují.

2.4.5 Procesy zajišťující řešení

Řízení incidentů a žádostí o služby a Management problémů – Řízení problémů je navázáno na proces řízení incidentů. Mezi těmito procesy probíhá přenos informací. Management problémů je řešen aplikačně, spravován může být prostřednictvím nastavení přehledného work-flow pro jednotlivé procesy.

2.4.6 Řídící procesy

Management konfigurací – Konfigurační databáze je spravována a aktualizována poměrně vyspělými prostředky. Databáze je nezávisle zálohovaná a umožňuje správcům přehlednou vizualizaci infrastruktury a poskytuje informace o všech infrastrukturních položkách v rámci serverovny GŘC.

Řízení uvolnění a nasazení – Tento proces je zdokumentován a v souladu s vnitřními předpisy. Každému uvolnění služby do ostrého provozu předchází testování. CS má k dispozici testovací prostředí, které neovlivňuje ostrý provoz. CS se může pochlubit sto procentní úspěšností v případě uvolnění služeb.

2.5 Kybernetický zákon

Povinnosti Celní správy České republiky, jakožto významného informačního systému, vzhledem ke kybernetickému zákonu (17):

- Hlášení kontaktních údajů národnímu CERT týmu.
- Detekce kybernetických bezpečnostních událostí.
- Implementace a provádění bezpečnostních opatření.
- Provádění ochranných opatření.
- Provádění reaktivních opatření.
- Hlášení kybernetických bezpečnostních incidentů vládnímu CERT týmu.
- Oznámení o provedení reaktivních opatření vládnímu CERT týmu.

Dne 19. 12 2014 byl generálním ředitelem cel vyhlášen rozkaz č. 92/2014 Politika kybernetické bezpečnosti informačního systému Celní správy České republiky. Tímto rozkazem byl nahrazen rozkaz č. 29/2014 Bezpečnostní politika informačního systému Celní správy České republiky. Příloha č. 1 (Politika kybernetické bezpečnosti ISCS) k rozkazu č. 92/2014 vychází z Vyhlášky č. 316/014 Sb. a stanovuje (28, str. 2-12):

a) Organizační opatření

1. *Opatření organizačně personální bezpečnosti*

- Bezpečnostní role, řízení bezpečnosti lidských zdrojů, řízení uživatelů, vracení svěřených aktiv a odebrání přístupových práv, řízení dodavatelů, smluvní bezpečnost.

2. *Opatření administrativně procedurální bezpečnosti*

- Bezpečnostní standard, řízení kybernetické bezpečnosti, správa kybernetické bezpečnosti, řízení aktiv, řízení rizik, řízení zvládání kybernetických bezpečnostních incidentů, řízení kontinuity provozu, řízení ochrany osobních údajů, řízení bezpečnosti provozně technické správy (akvizic, vývoje a údržby).

b) Technická opatření

3. *Opatření počítačové bezpečnosti*

Prováděcí ochrany (řízení přístupu, antivirová ochrana, bezpečná výměna dat, šifrovaná ochrana, zálohování)

4. *Opatření fyzické bezpečnosti*

Fyzická bezpečnost

c) Bezpečnostní dokumentace

5. *Řízení bezpečnostní dokumentace (předpisy související s kybernetickým zákonem, ČSN ISO/IEC 27001, rozkazy, služební předpisy a vnitřní pokyny v působnosti odboru 12 GŘC, vnitřní akty řízení, příkazy ředitele odboru 12 GŘC, rozkazy ředitele odboru 60 GŘC, realizační projekty, prováděcí metodiky, zprávy, záznamy, plány a přehledy, stanoviska a vyjádření)*

d) Certifikace podle ČSN ISO/IEC 27001

6. *Řízení ISMS (audit a externí audit)*

2.6 Shrnutí aktuálního stavu

Významnou měrou se na stávajícím stavu bezpečnosti informací podepisuje historický kontext, kdy byla koncepce vnitřních předpisů týkajících se bezpečnosti IS několikrát změněna. To je patrné zejména na nejednotné terminologii a různé úrovni podrobnosti jednotlivých předpisů. Dále měly vliv například změny organizační struktury, které v průběhu let v Celní správě České republiky proběhly, včetně změn klíčových zaměstnanců. I přes to se podmínky pro interní i externí audity dařilo plnit a recertifikace proběhly relativně úspěšně.

2.6.1 ISMS

První certifikace proběhla v roce 2011, o rok později než ITSM. Poslední recertifikační audit dle ISO/IEC 27001 byl proveden v roce 2014 a společnost Tayllor&Cox s.r.o. nezjistila žádné závažné nedostatky. V rámci prověřování byl auditován stanovený rozsah ISMS – Odbor 12 Informatika GRČ. Rozsah auditu je poskytování systémových integrovaných IT služeb. Audit byl proveden dle revidované normy ISO/IEC **27001:2013** a jednotlivé oblasti přílohy A normy ISO/IEC 27001 proběhly v souladu s Plánem auditu – uvádí certifikační orgán.

Zde si dovoluji tvrdit, že certifikační autoritou měla být minimálně navržena taková opatření, která by pomohla Celní správě České republiky zlepšit aktuální stav bezpečnosti informací. Dost možná recertifikace neměla být dopuštěna. Je zřejmé, že společnost provádějící externí audit musela o pochybení, která vzhledem k ISO/IEC 27001:2013 v organizaci panují, vědět a je tedy na místě navrhnout i změnu tohoto externího auditora. Náročnější podmínky externího auditu by mohly pomoci zajistit zvýšení kvality ISMS v organizaci. Nedostatky, které jsem našla vůči ISO/IEC 27001:2013, jsou popsána ve třetí kapitole této práce.

2.6.2 ITSM

Generální ředitelství cel, Odbor 12 informatiky získalo certifikáte ISO/IEC 20000-1:2011 pro následující rozsah služeb a činností:

- Poskytování systému integrovaných IT služeb
- podpora uživatelů ICT,
- řízení a realizace projektů ICT včetně projektů EU,
- zajišťování síťových služeb,
- podpora a správa aplikačního SW.

Tento certifikát byl vydán společností Tayllor&Cox s.r.o v roce 2013 a je platný do roku 2016. První zavedení ITSM a certifikace proběhly v roce 2010.

2.6.3 Kybernetický zákon

Kybernetický zákon přináší organizaci změnu ve vztahu k problematice informační bezpečnosti. Původně byla informační bezpečnost brána jako součást ITSM, přičemž se organizace více soustředila na celkový management služeb. Poté, co bylo zjištěno, že se chystá nový zákon, vztahující se k informační bezpečnosti, začala snaha o zefektivnění ISMS a začala mu být věnována náležitá pozornost. Ve třetí fázi se organizace začala koncentrovat na požadavky kybernetického zákona, dokonce vytvořila prostor pro nezávislý referát, který se kybernetickou bezpečností v rámci organizace zabývá.

Z mého pohledu se to jeví tak, že nezávislý referát spíše slovíčkaří, místo toho, aby se aktivně snažil zlepšit současný stav ISMS a tím zároveň vyhovět kybernetickému zákonu.

2.6.4 Silné stránky

- Neustálé zlepšování kvality ISMS díky dlouholeté praxi,

- vytvoření nezávislého referátu pro organizaci bezpečnosti informací v organizaci,
- provádění školení,
- vedení podporující ISMS.

2.6.5 Slabé stránky

- Z části je ISMS prováděno „papírovou“ formou,
- odtržení hlavních pracovníků zabývajících se ISMS od reality praxe,
- upřednostňování Prahy na úkor ostatních detašovaných pracovišť Odboru 12,
- bezpečnostní povědomí ostatních zaměstnanců na velmi nízké úrovni,
- nepřehledná dokumentace,
- některé uveřejněné dokumentace si protirečí, nevhodné křížové odkazy – certifikace podle ISO/IEC 27001 versus ISO/IEC 20000 versus kybernetický zákon,
- část dokumentace ISMS není ještě podřízená ČSN ISO/IEC 27001:2014 a z toho plynoucí dva důležité závěry:
 - organizace nevyhovuje kybernetickému zákonu,
 - bylo by vhodné uvažovat o změně externího auditora.

3 Vlastní návrhy řešení

V této části práce čerpám z předcházejících kapitol, kde jsem se věnovala jak teoretické přípravě, tak zkoumání stavu problematiky v organizaci. Jsou zde shrnuta nejzásadnější pochybení, u kterých je potřeba sjednat nápravu, tak aby Celní správa České republiky plnila nejenom nároky ISMS, ale i kybernetického zákona. V některých případech pak podávám návrhy, jak konkrétní změny provést.

3.1 Návrhy na změnu

Obecně lze shrnout, že hlavním nedostatkem je postoj personálu ISCS k ISMS. Ten je potřeba změnit tak, aby pro ně ISMS netvořilo „nutné“ povinnosti, ale aby bylo přínosem ve všech rutinních oblastech provozu.

Tato změna nemůže být provedena den ze dne, nýbrž postupnými kroky především ze strany vedení Odboru 12, které by mělo navíc jít příkladem všem zaměstnancům Celní správy České republiky a informační bezpečnost více prosazovat. Do dnešního dne bylo ISMS zavedeno jako služba navíc a Celní Správa byla uspokojena jeho certifikací, nyní, díky kybernetickému zákonu, vznikla nutná potřeba napravit všechna pochybení, která byla dosud tolerována i ze strany externího auditora, jinak hrozí finanční pokuty. Postupné vylepšování bude zahrnovat řadu dílčích úkolů, které vyplynou z detailní analýzy jak celého systému ISMS, tak konkrétního provozu.

Dalším všeobecným poznatkem je, že organizace se soustředí na slovíčkaření a na minimální konkretizaci na úkor praktickému využití. Většina dokumentace je psána co nejobecněji. V takovéto dokumentaci se pochybení hledají těžko, na druhou po bližším prozkoumání problematiky je jasné, že tento přístup je velmi nevhodný. Větší specifikace by přinesla jasnější pravidla a návody na praktické nasazení ISMS.

V následujících odstavcích uvádím nalezená významná pochybení:

A.7.1.2 Povědomí, vzdělávání a školení bezpečnosti informací:

Je potřeba zlepšit povědomí o ISMS u všech zaměstnanců CS. Navrhuji změnit podmínky e-learningového školení tak, aby vystihovalo podstatu bezpečnosti informací (znalost problematiky), nikoliv pouze znalost formulací uvedených ve vnitřních předpisech bez návaznosti na praxi.

Toho lze dosáhnout vyšším využitím možností moderní výpočetní techniky např. začleněním obrazových materiálů, animací, ozvučením výkladu, interaktivním výkladem (např. jednoduchou „hrou“) případně využitím uživatelského počítače k demonstraci některých situací. Velmi vhodným prvkem je zařazení osobního kontaktu, kdy je lektor schopen individuálně reagovat na stav pochopení problematiky uživatelem.

Problematiku zvyšování povědomí rozeberu v podkapitole 3.2.1

A.9.2.1 Správa uživatelských přístupů:

V této souvislosti by bylo vhodné vytvořit jednotnou směrnici procesu registrace uživatele. Na směrnici může navazovat jednoduchá webová aplikace, která provede personál ISCS celým procesem zřízení nového uživatelského účtu a tím bude zajištěno, že některá část nebude zapomenuta – např. vytvoření Home adresářů na fileserveru. Tato aplikace bude centrálně aktualizována tak, aby reflektovala změny směrnice. Zároveň může obsahovat uživatelský výstup log záznamů pro audit. Tímto krokem by došlo k přínosnému zjednodušení pro personál a navíc k zajištění vyšší bezpečnosti.

A.11.1.2 Fyzické kontroly vstupu:

Lépe zajistit kontroly fyzického vstupu. Například uvádím detašované pracoviště GŘC v Brně – zde je jedna budova sdílená s Finančním úřadem. Zcela chybí zamezení pohybu po budově nepovolaným osobám.

Nevhodně řešenou záležitostí je i vstup do serveroven. Přístup je chráněn pouze fyzicky – bezpečnostním zámekem, vhodnější by bylo využití přístupových karet a zaznamenávat i konkrétní časy a jména osob při vstupu.

Proto, především na těch detašovaných lokalitách, kde je CS pouze v nájmu a nemá v místě personál ISCS, by bylo na místě vytvořit projekt, který by se fyzickou bezpečností zabýval ve vztahu k možnostem ICT technologií – například použití tzv. RODC, tj. domain kontrolerů, které umožňují pouze čtení, a přesunout tak data z lokality, kde je fyzické zabezpečení velmi složité nebo nákladné, do místa s vhodnějšími podmínkami.

A.11.2 Zařízení:

Zde je potřeba přepracovat plány kontinuity a upravit bezpečnostní plány. Jedná se o velmi slabé místo. Stávající plány a dokumentace jsou příliš obecné a ve výsledku zcela nevhodné v případě, že by opravdu nastal bezpečnostní incident a bylo by potřeba je využít.

Stále existuje mnoho klíčových informací pouze ve hlavách personálu ISCS. Ty jsou ohroženy při případném odchodu pracovníka nebo jeho dlouhodobé nemoci. Je nutné upravit reálně existující pracovní postupy s ohledem na tuto skutečnost.

Návrh pro tvorbu plánu, uvádím v podkapitole 3.2.2

A.11.2.4 Údržba zařízení:

Pro podporu správného zajištění dostupnosti a integrity doporučuji využívat více SLA místo vlastních zaměstnanců. Spoluprací s externími subjekty dojde k přenesení zodpovědnosti a na základě SLA smlouvy ke specifikaci jak potřebných služeb, tak případných sankcí a tím i zajištění vyšší kvality. SLA smlouvy je vhodné využívat v rámci organizace.

V informačním centru probíhá profylaxe jedenkrát ročně. Ostatní bezpečnostní domény údržbu systému provádí dle svého nejlepšího vědomí a zkušeností. Praxe je

tedy velmi rozdílná. Je nutné vydat vnitřní předpis, co má údržba obsahovat a kdy a jak ji provádět. To platí nejen pro servery, ale i aktivní prvky, kabeláž, kontroly konfigurací a podobně.

A.15.2 Řízení dodávek služeb dodavatelů

Znovu zdůrazňuji výhody využívání SLA smluv, kdy se specifikují jak přesná kritéria služby, tak i sankce za nedodržení, čímž je zajištěna kvalita.

A.16.1.1 Odpovědnosti a postupy:

Je potřeba detailněji propracovat postupy pro zvládání incidentů bezpečnosti informací. Podrobně je rozpracován postup informace, že k incidentu došlo a následné schvalování kroků k nápravě služebními funkcionáři.

Bohužel funkcionáři, kteří jsou do tohoto procesu zahrnuti, nejsou technici, musí proto naprosto důvěřovat svému personálu a jejich schválení je tedy jen formálního charakteru. Většinu rozhodnutí při řešení krizového stavu je nutné provést na co nejnižší úrovni, pouze incidenty velkého rozsahu by měly být eskalovány až na top management.

Naproti tomu samotné postupy nápravy co, kdy a jak provést, zkontrolovat, zdokumentovat a jaké zdroje použít jsou nedostatečné. Viz A.11.2.

Dále navrhuji upravit povinnosti zaměstnanců ISCS vzhledem k ISMS a konkretizovat zodpovědnosti správců na nižší úrovni. Nyní jsou jejich kompetence popsány příliš povrchně, což vede k jejich nechuti ISMS praktikovat.

A.18.1.1 Identifikace odpovídající legislativy a smluvních požadavků:

Zde je potřeba neustále sledovat změny zákonných norem a reagovat na ně, pokud možno s předstihem. V této souvislosti je nutné zmínit kybernetický zákon, který k 1. 1. 2015 identifikoval Generální ředitelství cel jako významný informační systém. Do 1. 1. 2016 musí CS vytvořit vhodné podmínky pro kybernetickou bezpečnost, které jsou pro ni tímto zákonem pevně stanovené. Poté, pokud by byly zjištěny nedostatky, hrozí finanční pokuty až do 100 000Kč.

Přitom, pokud by CS začala lépe využívat ISMS a upravila dokumentaci, tak aby plně vyhovovala ISMS, dá se říct, že by snadno plnila podmínky i z pohledu kybernetického zákona.

3.1.1 Budování bezpečnostního povědomí

Protože i systém managementu bezpečnosti informací je tak silný, jako jeho nejslabší článek, je žádoucí tvořit bezpečnostní povědomí u všech zaměstnanců, protože právě oni často bývají touto slabinou. Bezpečnostní povědomí by měli mít všichni zaměstnanci bez ohledu na vztah k ISMS.

Podstatné přitom je pracovat s různými zaměstnanci odlišně, tak aby uživatelé ISCS nebyli zahlceni přemírou nepodstatných informací, a tím demotivováni a obráceně, aby výkonní zaměstnanci z řad IT manažerů a techniků získali dostatečné množství kvalitních informací, které potřebují pro výkon svěřené práce.

Problematice bezpečnostního povědomí se velmi vhodně věnuje například americká **norma NIST SP 800-50 - Building an Information Technology Security Awareness and Training Program**, pomocí které může organizace vytvořit a implementovat školicí program.

Možný způsob implementace bezpečnostního povědomí v Celní správě České republiky:

Ze všeho nejdříve je nutné zaměstnance rozdělit do skupin, podle jejich vztahu k ICT technologiím vzhledem k pracovní náplni a svěřeným kompetencím, dostupným například z pracovních smluv.

Navrhuji tyto tři skupiny zaměstnanců:

- a) *Běžný uživatel* (IT technologie využívá jako prostředek k vykonávání jiné činnosti)

- b) *ICT zaměstnanec* (aktivně s ICT technologiemi pracuje, jsou jeho pracovní náplní)
- c) *Bezpečnostní specialista, manažer* (ICT zaměstnanec podílející se na zvyšování úrovně bezpečnosti informací ve společnosti)

Následně je vhodné definovat příslušný typ vzdělávání na základě požadovaných dovedností a znalostí, které by měly jednotlivé skupiny zaměstnanců ovládat. Jako příklad může posloužit tabulka níže, kterou jsem vytvořila na základě NIST SP 800-50.

Tab. 3: Tabulka srovnání (Zpracováno dle 39)

<i>Typ:</i>	Povědomí	Školení	Vzdělání
<i>Atribut k bezpečnosti:</i>	„Co“	„Jak“	„Proč“
<i>Úroveň:</i>	Informativní	Znalostní	Porozumění
<i>Cíl vzdělávání:</i>	Rozpoznání a retence	Dovednost	Pochopení
<i>Vhodné metody:</i>	Videokurzy, Letáky, Interaktivní aplikace Praktická ukázka	Lekce, Případové studie, Praktická ukázka	Semináře, Přednášky, Výzkum
<i>Výstupní dovednosti:</i>	Identifikace	Aplikace	Interpretace
<i>Časová náročnost:</i>	Krátká	Střednědobá	dlouhodobá
<i>Skupina:</i>	Běžný uživatel, IT zaměstnanec, Bezpečnostní specialista, manažer	IT zaměstnanec, Bezpečnostní specialista, manažer	Bezpečnostní specialista, manažer
<i>Prokázání dosažené úrovně:</i>	Test ano/ne, výběr z více možností	Řešení případové studie	Esej

Dalším krokem je otestování vstupních znalostí zaměstnanců v jednotlivých typech kurzů a jejich následné rozdělení do znalostních skupin, například začátečník, středně-pokročilý, pokročilý.

Nyní, když jsou zaměstnanci rozdělení ve znalostních skupinách, je potřeba blíže specifikovat cíle a rozsah vzdělávání. Na základě zjištěných skutečností vytvořit materiály jako:

- témata, která je potřeba řešit,
- metodiky,
- dokumentace, zajištění zpětné vazby, doložení výstupu,
- vyhodnocení a aktualizace materiálů.

Nakonec je ještě potřeba určit četnost výuky a jejího opakování a vytvořit cenovou kalkulaci.

Na tomto místě uvádím příklad obsahu letáku, který slouží pro budování bezpečnostního povědomí:

Bezpečnostní povědomí pro uživatele:

1. Používejte silné heslo, bez významu.
2. Heslo si zapamatujte, nikam nepište (využijte např. počáteční písmena v první sloce oblíbené básničky).
3. Heslo pravidelně měňte.
4. Dodržujte zásadu prázdného stolu a obrazovky při odchodu z pracoviště.
5. Neotevírejte podezřelé e-maily a v žádném případě jejich přílohy.
6. Pravidelně zálohujte.
7. Na internetu nenavštěvujte podezřelé stránky, které by mohly být nebezpečné, nestahujte neznámé soubory.
8. Používejte jen legální a aktualizovaný software.
9. Mějte zapnutý firewall.
10. Používejte antivir, povolte jeho update.
11. Bezpečnostní problémy okamžitě hlaseť pověřenému správci.

3.1.2 Plán obnovy

V následující části práce uvádím příklad, jak by organizace mohla vypracovat plán obnovy, který stanoví jasný a stručný návod, co je v konkrétních situacích potřeba udělat a v jakém pořadí.

Z bezpečnostních důvodů bylo výslovným přáním CS, aby mnou zpracovaný plán neobsahoval detailnější postupy, jména osob a podobně.

Plán obnovy po havárii systému

Popis: Tento plán určuje přesný postup jak jednat v případě havárie systému. Určuje postup prací nutných k co nejrychlejšímu obnovení provozu. Dále určuje postupy obnovy dat.

Hlavní cíl: Minimalizace dopadu na činnost organizace.

Díličí cíle: Minimalizace ekonomických nákladů.
Zajištění rychlé obnovy činnosti.
Zajištění alternativ pro provoz činností po dobu nezbytně nutnou.
Zabránění zvyšování rozsahu škod.

Součástí plánu musí uveden kontakt na **všechny zodpovědné osoby**, minimálně v rozsahu, jak je naznačeno v následujících tabulkách.

Tab. 4: Zodpovědné osoby – zaměstnanci (Zdroj Vlastní zpracování)

Jméno a příjmení	Pozice	Rozsah zodpovědností	Kontaktní adresa	Kontakt (telefon; e-mail)

Tab. 5: Zodpovědné osoby externí spolupráce (Zdroj Vlastní zpracování)

Jméno a příjmení	Firma	Rozsah zodpovědností	Kontaktní Adresa	Kontakt (telefon; e-mail)

1. Inicializační část:

- Podstatou této části je zjištění předběžného rozsahu škod, zabránění jejich dalšímu šíření a informování zainteresovaných stran. Seznam činností, které je potřeba vykonat:
 - a) Neprodleně informovat vedení a svolat pracovníky krizového týmu.
 - b) Určit zasažené oblasti a stupeň poškození.
 - c) Kontaktovat související externí organizace.
 - d) Upřesnění rozsahu zhroucení a zjištění přibližné doby obnovy, přerušení procesů, které zjevně zhoršují aktuální stav, bezpečné ukončení spuštěných relací, aby došlo k jejich uložení.
 - e) Informování uživatelů o přerušení služeb a přibližné době trvání (např. telefonicky informovat vedoucí jednotlivých oddělení).

2. Plán obnovy

- Nyní by měly začít práce na obnově, k tomu složí následující body:
 - a) Sestavení týmu pro obnovu (seznam osob, včetně telefonních kontaktů).
 - b) Rozdělení úkolů a sestavení časového harmonogramu.
 - c) Zajištění nezbytných financí.
 - d) Zajištění vybavení, dopravy, stravy, ubytování (podle závažnosti).
 - e) Přesun do záložního pracoviště, je-li to potřeba.
 - f) Zprovoznění záložního pracoviště a spuštění záložního systému.

3. Ukončení plánu obnovy

- Tato část nesmí být vynechána, nyní by měli být všichni informováni o tom, že systém pracuje jak má a vydána zpráva informující o příčině havárie. Havárie by měla být zdokumentována a postup vyhodnocen, klady i zápory, poučení se z chyb a nesmí chybět ani úprava plánu obnovy.
 - a) Informování všech zasažených o obnovení systému (minimálně vedení, vedoucí oddělení).
 - b) Vyhodnocení akce, včetně důvodu havárie, zdokumentování, kalkulace škod, podání zpětné vazby.
 - c) Úprava plánu obnovy, je-li to potřeba.

3.2 Ekonomické zhodnocení

Ztráty, které by mohly nastat, pokud by organizace nedbala na dostupnost, integritu a důvěrnost informací, by mohly zapříčinit významné škody nejen pro ni samotnou, ale především pro stát a jeho občany. Jak jsem zmínila v popisu organizace, mezi její nejdůležitější kompetence patří správa cel a některých daní, a to i v celoevropském kontextu.

V roce 2013 vybrala Celní správa České republiky na daních a clech celkem 164, 7 miliardy Kč (41, str. 3). S přihlédnutím k tomu, že většina údajů je již zpracovávána elektronicky, pak smazání dat v elektronicky vedeném spisu by mohlo znemožnit vyměření cla nebo daně v konkrétní věci v řádech miliónů korun. K tomu by mohlo postačit nabourání se do systému a „smazat“ doručenkou. Jednoduchým výpočtem se dá zjistit, že CS v roce 2013 průměrně za den vybrala 451,2 miliónu korun. Tedy pokud by došlo k fatálnímu výpadku systému na jeden den, ztráty by se mohly vyšplhat až k této částce. Přičemž celoroční kapitálové výdaje na ICT tvořily v tomto roce „jen“ 197 miliónů Kč.

V případě dlouhodobého výpadku systému by tak došlo k pozastavení importu zboží ze zahraničí, dovozci by buď museli čekat, až se systémy obnoví, nebo by se někteří mohli rozhodnout zboží neproclít (nebylo by to dohledatelné) a tím by hrozil růst nežádoucí šedé ekonomiky.

Další pravomocí Celní správy je kontrola povinného značení lihu. Pokud by se například neoprávněná osoba dostala do systému a mohla tyto údaje spravovat, kromě ekonomických ztrát by mohly nastat i ztráty na životech, protože by líh nebyl dostatečně kontrolován a hrozily by další „metanolové“ kauzy.

Těmito příklady poukazují na to, že ztráty, které by hrozily v modelových situacích, by mnohokrát předčily náklady, které jsou spojeny s bezpečným provozem ICT.

Závěr

Problematika systému managementu bezpečnosti je velmi rozsáhlá a zahrnuje prakticky veškeré činnosti oddělení IT. V Celní správě České republiky je vytvořen solidní základ podložený získanými certifikáty.

Jako člověk nezatížený interními předsudky a rutinou jsem měla možnost projít většinu systému ISMS v Celní správě České republiky a nestranně vidět, jak zpracovanou dokumentaci, tak reálnou praxi. Na základě těchto poznatků jsem vznesla návrhy na zlepšení, které se opírají především o normativní doporučení, názory odborníků v této problematice a přáními samotných zaměstnanců.

Pokud organizace mnou předložené návrhy na zlepšení přijme za své a upraví dotčené části ISMS, pak to pro ni bude velký krok k vytvoření silné vazby s reálným provozem ISCS. Díky tomu dojde jak v informačním centru, tak na detašovaných pracovištích k synergickému efektu, který měli tvůrci normy zejména na mysli.

CS poté využije plně potenciál nejen formálního vlastnictví certifikátů ISO, ale i know-how těchto norem vedoucího k neustále se zdokonalujícímu, pružnému a modernímu ISCS. Na základě toho pro ni nebude problém projít bezpečnostní prověrkou ohledně kybernetického zákona, která po roce 2015 může kdykoliv nastat.

Přínos návrhu řešení

V této práci jsem si kladla za cíl vypracování návrhů a doporučení, která budou pro Celní správu České republiky přínosná. Tyto návrhy jsou zpracovány v kapitole 3.1.

Věřím, že v případě zvážení mých návrhů a opravy jednotlivých částí ISMS, dojde ke zlepšení v podobě nejen snazšího plnění certifikačních podmínek a kybernetického zákona, ale především v praktické bezpečnosti, o kterou tu hlavně jde.

Hlavní přínosy mých návrhů na zlepšení:

- Zvýšení bezpečnostního povědomí zaměstnanců,

- lepší připravenost v podobě podrobných plánů a směrnic,
- snížení administrativní zátěže pracovníků ICT,
- vyšší využití SLA a tím zabezpečení určení rolí, povinností a zodpovědností,
- úspěšná implementace podmínek dle ISO/IEC 27001:2013,
- splnění podmínek kybernetického zákona,
- zvýšení bezpečnosti informací,
- vyšší ochota vedení organizace uvolnit finance na ICT a jeho zabezpečení.

Seznam zkratek

AD	Active Directory
BD	Bezpečnostní doména
CS	Celní správa České republiky
ČSN	Česká technická norma
IEC	International Electrotechnical Commission
GŘ	Generální ředitel
GŘC	Generální ředitelství cel
HW	Hardware
IC	Informační centrum
ICT	Informační a komunikační technologie
ISCS	Informační systém Celní správy České republiky
ISMS	Systém řízení bezpečnosti informací
ISO	International Organization for Standardization
IT	Informační technologie
ITIL	Information Technology Infrastructure Library
ITSM	Systém řízení služeb v IT
LAN	Lokální síť
NTB	Notebook
PDCA	Plan-Do-Check-Act model
SLA	Service Level Agreement (Smlouva mezi poskytovatelem služby a zákazníkem)
SW	Software
WAN	Počítačová síť na dlouhou vzdálenost

Seznam použitých tabulek, obrázků a grafů

Tab. 1: Přehled ČSN ISO/IEC 27002:2014 (Zpracováno dle 3, str. 10 až 72).....	23
Tab. 2: Aplikace modelu PDCA při řízení rizik (Zpracováno dle 4, str. 15)	27
Tab. 3: Tabulka srovnání (Zpracováno dle 39).....	66
Tab. 4: Zodpovědné osoby – zaměstnanci (Zdroj Vlastní zpracování)	68
Tab. 5: Zodpovědné osoby externí spolupráce (Zdroj Vlastní zpracování)	68
Obr. 1: PDCA cyklus (Upraveno dle 6, str. 25).....	15
Obr. 2: Vztahy mezi normami ISMS (Upraveno dle 1, str. 24).....	18
Obr. 3: Informační bezpečnost (Vlastní zpracování).....	20
Obr. 4: Procesní pohled na řízení rizik (Zdroj 4, str. 14).....	28
Obr. 5: Procesní pohled na systém řízení služeb (Zdroj 5, str. 11).....	31
Obr. 6: ITIL (Zdroj 16).....	33
Obr. 7: Mapa sídel Celní správy České republiky (Zdroj 24)	11
Obr. 8: Organizační struktura Generálního ředitelství cel (Upraveno dle 24).....	41
Obr. 9: Schéma informačního systému CS (Upraveno dle 27, str. 8).....	44
Graf 1.: Vztah mezi dopady rizik a náklady na opatření (Zdroj 6, str. 36).....	26

Seznam použitých zdrojů

1. ČSN ISO/IEC 27000. *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník*. 2014. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.
2. ČSN ISO/IEC 27001. *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky*. 2014. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.
3. ČSN ISO/IEC 27002. *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací – Soubor postupů pro opatření bezpečnosti informací*. 2014. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.
4. ČSN ISO/IEC 27005. *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací – Řízení rizik bezpečnosti informací*. 2013. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.
5. ČSN ISO/IEC 20000-1. *Informační technologie – Management služeb – Část1: Požadavky na systém managementu služeb*. 2012. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.
6. ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Vyd. 1. Brno: CERM, 2013, 377 s. : il, grafy, tab. ISBN 978-80-7204-872-4.
7. Informační bezpečnost. ČERMÁK, Miroslav. *Clever and Smart* [online]. 2009 [cit. 2015-04-20]. Dostupné z: <http://www.cleverandsmart.cz/informacni-bezpecnost/>
8. Strategické řízení. *Management mania* [online]. 2010 [cit. 2015-04-20]. Dostupné z: <https://managementmania.com/cs/strategicke-rizeni>
9. ISO/IEC 20000. ŠKÁLA, Jiří. *Bestpractice.cz: IT and Management Knowledge Base* [online]. 2011 [cit. 2015-04-20]. Dostupné z: <http://www.bestpractice.cz/cs/Best-practice/-ISO20000.alej>

10. ISO/IEC 20000. ŠKÁLA, Jiří. *Bestpractice.cz: Co je to služba IT* [online]. 2011 [cit. 2015-04-20]. Dostupné z: <http://www.bestpractice.cz/cs/Best-practice/-ITSM-ITIL--Co-je-to-sluzba-IT.alej>
11. Ochrana informací. *Information security management system* [online]. 2015 [cit. 2015-05-25]. Dostupné z: www.isms.cz
12. ISO/IEC 20000-1: - Informační technologie, management služeb. ŠKÁLA, Jiří. *LRQA: Lloyd's Register* [online]. 2013 [cit. 2015-04-20]. Dostupné z: <http://www.lrqa.cz/standardy-a-schemata/iso-iec20000-1/>
13. Zákon č.181/2014Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ze dne 23. července 2014
14. Bezpečnostní politika. *Clever and Smart* [online]. 2015 [cit. 2015-05-25]. Dostupné z: <http://www.cleverandsmart.cz/bezpecnostni-politika/>
15. KARDOŠ, Daniel. ČSN ISO/IEC 27001:2014 Systém řízení bezpečnosti informací a zákon o kybernetické bezpečnosti. In: *Nekomerční konference pro popularizaci systému řízení IT* [online]. 2014 [cit. 2015-05-25]. Dostupné z: http://www.kardos.cz/konf/2014/Kardos_2014.pdf
16. ITIL methodology. *SoftCat* [online]. 2015 [cit. 2015-05-25]. Dostupné z: <http://www.softcat.com/what-we-do/managed-services/helpdesk-remote-support-services>
17. KUČÍNSKÝ, Adam. *Určování KII a VIS*. Seminář k zákonu o kybernetické bezpečnosti. Brno: Fakulta Podnikatelská, VUT v Brně, 21. 5. 2015
18. Bezpečnost. *Zákon o kybernetické bezpečnosti* [online]. 2015 [cit. 2015-05-25]. Dostupné z: <https://www.kybez.cz/bezpecnost/zkb>
19. Zákon č.181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ze dne 23. července 2014
20. Vyhláška č.316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti) ze dne 15. prosince 2014
21. Vyhláška č.317/2014 Sb., o významných informačních systémech a jejich určujících kritériích ze dne 15. prosince 2014

22. Předpis č. 432/2010 Sb., nařízení vlády o kritériích pro určení prvku kritické infrastruktury ze dne 22. prosince 2010
23. O nás Celní správa ČR. *CELNÍ SPRÁVA ČESKÉ REPUBLIKY*[online]. 2014 [cit. 2015-04-20]. Dostupné z: <https://www.celnisprava.cz/cz/o-nas/Stranky/celni-sprava.aspx>
24. Organizační struktura Celní správy České republiky. *CELNÍ SPRÁVA ČESKÉ REPUBLIKY*[online]. 2014 [cit. 2015-04-20]. Dostupné z: <https://www.celnisprava.cz/cz/o-nas/organizacni-struktura/Stranky/organizacni-struktura-celni-spravy-ceske-republiky1.aspx>
25. Kompetence – čím se zabývá celní správa. *CELNÍ SPRÁVA ČESKÉ REPUBLIKY*[online]. 2014 [cit. 2015-04-20]. Dostupné z: <https://www.celnisprava.cz/cz/o-nas/kompetence/Stranky/default.aspx>
26. ŠARBORT, J. Osobní sdělení. Celní správa České republiky. Koliště 17, 602 00 Brno. 24. 3. 2015
27. GENERÁLNÍ ŘEDITELSTVÍ CEL. *Strategie rozvoje Informačního systému Celní správy České republiky na roky 2014-2016*. Praha, 2013.
28. GENERÁLNÍ ŘEDITELSTVÍ CEL. *Rozkaz č. 92/2014: Politika kybernetické bezpečnosti informačního systému Celní správy České republiky*. Praha, 2014.
29. GENERÁLNÍ ŘEDITELSTVÍ CEL. *Služební předpis č. 9/2012: Systém managementu bezpečnosti informací v Celní správě České republiky*. Praha, 2013.
30. GENERÁLNÍ ŘEDITELSTVÍ CEL. *Interní příkaz č. 15/2014: Zřízení a obsazení bezpečnostních rolí v působnosti odboru 12 GŘC*. Praha, 2014.
31. GENERÁLNÍ ŘEDITELSTVÍ CEL. *Riziková analýza ISCS: METODIKA*. Praha, 2015.
32. GENERÁLNÍ ŘEDITELSTVÍ CEL. *Zvládání reálných rizik ISCS v období 2014 - 2016: PLÁN*. Praha, 2015.
33. GENERÁLNÍ ŘEDITELSTVÍ CEL. *Správa bezpečnostní dokumentace ISCS: METODIKA*. Praha, 2014.
34. GENERÁLNÍ ŘEDITELSTVÍ CEL. *Vnitřní pokyn č. 9/2012: Pravidla zvládání bezpečnostních incidentů ISCS*. Praha, 2013.

35. GENERÁLNÍ ŘEDITELSTVÍ CEL. *Služební předpis č. 12/2013: Systém managementu služeb informačních technologií v Celní správě České republiky*. Praha, 2013.
36. GENERÁLNÍ ŘEDITELSTVÍ CEL. *Závěrečná zpráva z vnitřního auditu Informačního systému Celní Správy České republiky dle ČSN ISO/IEC 27001 za rok 2014*. Praha, 2014.
37. GENERÁLNÍ ŘEDITELSTVÍ CEL. *Recertifikační auditní zpráva: Norma ISO/IEC 27001:13*. Praha, 2014.
38. GENERÁLNÍ ŘEDITELSTVÍ CEL. *Certifikát: ISO/IEC 20000-1:2011*. Praha, 2013.
39. *Building an Information Technology Security Awareness and Training Program: Computer security*. Gaithersburg, U.S.: National Institute of Standards and Technology, 2003.
40. *Nález pléna Ústavního soudu č. 94/2011 Sb.* 2011 [cit. 2015-05-01].
41. *Zpráva o činnosti Finanční správy České republiky a Celní správy České republiky za rok 2013*[online]. 2014 [cit. 2014-05-01].
42. GENERÁLNÍ ŘEDITELSTVÍ CEL. *HelpLine Katalog Služeb*. Praha, 2015.
43. GENERÁLNÍ ŘEDITELSTVÍ CEL. *Zvládání bezpečnostních incidentů ISCS: METODIKA*. Praha, 2014.

Seznam příloh

Příloha č. 1: Ukázka části bezpečnostního auditu

Příloha č. 2: Ukázka návrhu Prohlášení o aplikovatelnosti

Příloha č. 1: Ukázka části bezpečnostního auditu

NORMA KAPITOLA	KONTROLNÍ OTÁZKY	HODNOCENÍ			
		1 - splněno	2 - splněno částečně	3 - nesplněno	N - neprováděno
KAP.4.3 (stanovení rozsahu systému řízení bezpečnosti informací)	Můžete nám doložit vnitřní předpis, který vám stanovuje váš rozsah systému managementu bezpečnosti informací ve vaší bezpečnostní doméně?	x			
KAP.5.3 (role, odpovědnosti a pravomoci organizace)	Můžete nám nějakým způsobem doložit, zda máte jasně definovanou odpovědnost v oblasti systému managementu bezpečnosti informací, například popisem pracovních činností?	x			
KAP.7.2 (kompetence)	Máte zajištěno, aby zaměstnanci, kteří mají povinnosti definované v systému managementu bezpečnosti informací byli odborně vyškoleni?	x			
KAP.7.3 (povědomí)	Můžete nám nějakým způsobem doložit, zda máte definovanou politiku bezpečnosti informací (systému managementu bezpečnosti informací)?	x			
	Můžete nějakým způsobem doložit, zda máte dokument systému managementu bezpečnosti informací Prohlášení o aplikovatelnosti (SoA) dle normy ISO/IEC 27001?	x			
Příloha A.6 (organizace a bezpečnost informací)	A.6.2.1 Můžete nám nějakým způsobem doložit, zda máte stanovená formální pravidla pro bezpečnost používání mobilní a komunikační zařízení?	x			
	A.6.2.2 Autentizujete přístup vzdálených uživatelů a využíváte kryptografické techniky?	x			
Příloha A.8 (řízení aktiv)	A.8.1.1 Máte aktuální a kompletní evidenci aktiv?		x		
	A.8.1.4 Můžete nám předložit metodiku nebo Vámi stanovené postupy při odchodu zaměstnance?	x			

Příloha č. 1: Ukázka části bezpečnostního auditu

Příloha A.9 (řízení přístupů)	A.9.2.2	Máte formalizovaný proces přidělování práv pro interní a externí zaměstnance, a to na základě oprávněné a odůvodněné potřeby?	x			
	A.9.4.1	Máte chráněnou systémovou dokumentaci proti neoprávněnému přístupu, například dokumentace k počítačovým sítím nebo bezpečnostní dokumentaci?	x			
	A.9.4.2	Máte přístup do systému a k datům umožněn pouze na základě jednoznačné identifikace a autorizace pracovníků a to včetně přístupů třetích stran?	x			
	A.9.4.3	Máte hesla uložená v počítači (databázích) ve chráněné podobě, například u vlastních vyvíjených aplikací (SW, WWW)?	x			
Příloha A.11 (fyzická bezpečnost a bezpečnost prostředí)	A.11.1.2	Máte stanoveny postupy (například provozní řády) u režimových místností (například serverovny) kde máte HW aktiva proti přístupu neoprávněných osob?	x			
	A.11.2.9	Dodržujete a jakým způsobem zásadu prázdného stolu a prázdné obrazovky monitoru?				x
Příloha A.12 (bezpečnost provozu)	A.12.1.1	Máte změny provozních postupů odsouhlaseno vedoucím zaměstnancem?	x			
	A.12.1.2	Provádíte řízení změn a jak?		x		
	A.12.1.4	Je oddělen vývoj a testování provozních prostředků od vlastního provozu, v případě, že ANO, tak uveďte konkrétně, jak to probíhá při zavádění nových programových verzí ?	x			
	A.12.2.1	Máte implementovanou ochranu proti škodlivým programům?	x			
	A.12.3.1	Provádíte zálohování dat?	x			
	A.12.4.1	Máte nastaveny auditní záznamy, obsahující chybová hlášení a jiné bezpečnostně významné události pro účely monitorování řízení přístupu a v jakém rozsahu?	x			
	A.12.4.1	Obsahují ID, datum a čas, identifikátor terminálu a záznam o úspěšných a odmítnutých pokusech o přístup k systému, datům a jiným zdrojů nebo změny konfigurace systému?	x			
	A.12.4.1	Máte stanovena pravidla pro monitorování použití prostředků pro zpracování informací, výsledky těchto monitorování pravidelně přezkoumávány?	x			
	A.12.4.3	Nemohou systémoví administrátoři vymazat záznamy anebo deaktivovat vytváření záznamů o své vlastní činnosti?		x		
	A.12.5.1	Máte zavedené postupy pro kontrolu instalace programového vybavení na provozních systémech?	x			
	A.12.6.1	Máte stanovené spojení na kontaktní osoby v případě neočekávaných systémových nebo technických potíží?	x			
	A.12.6.1	Máte zajištěna kritická aktiva a zdroje potřebné pro zajištění havarijních postupů?	x			

Příloha č. 1: Ukázka části bezpečnostního auditu

Příloha A.14 (akvizice, vývoj a údržba systémů)	A.14.2.2	Máte nastavena kritéria pro přejímání nových informačních systémů, jejich aktualizace a zavádění nových verzí a kdo je formálně schvaluje?		x		
	A.14.3.1	Jakým způsobem vybíráte data pro testování (aplikací, programů atd.), jak je máte chráněna a kdo provádí kontrolu (pokud toto provádíte)?	x			
Příloha A.16 (řízení incidentů bezpečnosti informací)	A.16.1.1	Máte systém hlášení bezpečnostních událostí a zainteresování uživatelů i smluvních stran a uživatele třetích stran (provedeno seznámení, měli by znát kontaktní místo pro hlášení)?	x			
Příloha A.17 (aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací)	A.17.1.1	Máte stanovenou odpovědnost za proces řízení kontinuity činností organizace/útvary?	x			
	A.17.1.2	Máte stanoveny provozní postupy (plány kontinuity) až do obnovení činností organizace?	x			
Příloha A.18 (soulad s požadavky)	A.18.1.2	Máte zavedené kontrolní mechanismy, zajišťující instalaci pouze schválených a licencovaných programových produktů?	x			
	A.18.1.4	Máte zavedená pravidla pro ochranu osobních dat (zákon č. 101/2000 Sb.)?	x			

Příloha č. 2: Ukázka návrhu Prohlášení o aplikovatelnosti

Prohlášení o aplikovatelnosti

Legenda (Vybrané opatření a důvod výběru)

PP: právní požadavky, SZ: smluvní závazky, OP/BP: obchodní požadavky /přijaty best practices, RA: risk analýza

ČSN ISO/IEC 27001:2014 Příloha A			Apliko váno	Cíl opatření	Důvod výběru opatření				Poznámky (Dokumentace)
Kapitola	Číslo	Opatření			PP	SZ	OP /BP	RA	
5 Politiky bezpečnosti informací	5,1	Směrování bezpečnosti informací vedením organizace							
	5.1.1	Politiky pro bezpečnost informací	ANO	Implementovaná sada politik pro bezpečnost informací, schválená, zveřejněná a daná na vědomí zaměstnancům a interesovaným stranám				Rozkaz č. 92/2014, Příloha č. 1	
	5.1.2	Přezkoumání politik pro bezpečnost informací	ANO	Revize a aktualizace BP je stanovena a v pravidelných intervalech prováděna, a to alespoň jednou za 2 roky					
6 Organizace bezpečnosti informací	6,1	Interní organizace							
	6.1.1	Role a odpovědnosti bezpečnosti informací	ANO	Všechny odpovědnosti za bezpečnost informací a provozu bezpečnosti informací v rámci organizace jsou ustanoveny				SP č. 29/2010, Pravidla bezpečného užívání ISCS Rozkaz GŘ č. 92/2014 Kybernetická bezpečnostní politika ISCS Interní pokyn ŘO 12 č.13/2013 Zřízení a obsazení bezpečnostních rolí v působnosti odboru 12 GŘC VP č. 96/2012 Řízení bezpečnosti ISCS společně VP č. 101/2012 Řízení a provádění ochrany ISCS	
	6.1.2	Oddělení povinností	ANO	Konfliktní povinnosti a oblasti působnosti jsou odděleny, aby se omezily příležitosti neoprávněné nebo neúmyslné změny nebo zneužití aktiv organizace					
	6.1.3	Kontakt s příslušnými orgány a autoritami	ANO	Udržování kontaktů s příslušnými autoritami				Příslušné autority jsou uveřejněny na webu, dále pak u manažera ISMS a místních správců BD	
	6.1.4	Kontakt se zájmovými skupinami	ANO	Kontakt se zájmovými skupinami je pravidelně udržován, tak aby docházelo k předávání zkušeností a vzájemné pomoci				Semináře, besedy, pozvání zájmových skupin	
	6.1.5	Bezpečnost informací v řízení projektů	ANO	Začlenění bezpečnosti informací do všech projektů				Součástí každého dokumentu je i informace o jaký typ informací se jedná	
	6,2	Mobilní zařízení a práce na dálku							

Příloha č. 2: Ukázka návrhu Prohlášení o aplikovatelnosti

	6.2.1	Politika mobilních zařízení	ANO						
	6.2.2	Práce na dálku	ANO						
	7,1	Před vznikem pracovního vztahu							
7 Bezpečnost lidských zdrojů	7.1.1	Prověřování	ANO	<p>Prověřování z hlediska bezpečnosti je ve spolupráci s odborem 40 GŘC prováděno na základě osobního pohovoru, vícenásobným ověřením totožnosti, doložením vzdělání a kvalifikace, dále například doložením dvou referencí, historie předchozích zaměstnání, kontroly životopisu, výpisu z rejstříku trestů, v případě potřeby se postupuje dle zákona č. 412/2005 Sb. a od roku 2012 dle zákona č.255/2011 Sb. Vždy je brán zřetel na ochranu OÚ a dodržení soukromí. Spolehlivost pracovníků třetích stran je zajištěna v rámci smluvních podmínek a dále také dle referencí, certifikací.</p>					<p>VP č.8/2012 Postup Centrálního náborového střediska odboru 40 GŘC při obsazování volných služebních a pracovních míst v celní správě</p>
	7.1.2	Podmínky pracovního vztahu	ANO	<p>Smlouvy obsahují ustanovení o povinnosti mlčenlivosti a dále u ATZ odkaz na Zákoník práce a u příslušníků CS odkaz Služební zákon a dále odvolání na platné právní předpisy. Jsou pravidelně proškolení v oblasti bezpečnosti informací. Odpovědnost za bezpečnost je určena odpovídajícími předpisy například Rozkaz GŘ č. 15/2012 Bezpečnostní politika ISCS. Odpovědnost třetích stran je začleněna do smluvních podmínek v rámci ITSM dle VP č. 12/2013 Systém managementu služeb informačních technologií v Celní správě České republiky.</p>				<p>Rozkaz GŘ č. 15/2012 Bezpečnostní politika ISCS VP č. 12/2013 Systém managementu služeb informačních technologií v Celní správě České republiky</p>	
	7,2	Během pracovního vztahu							
	7.2.1	Odpovědnosti vedení organizace							
	7.2.2	Povědomí, vzdělávání a školení bezpečnosti informací							
	7.2.3	Disciplinární řízení							
	7,3	Ukončení a změna pracovního vztahu							

Příloha č. 2: Ukázka návrhu Prohlášení o aplikovatelnosti

	7.3.1	Odpovědnosti při ukončení nebo změně pracovního vztahu							
8 Řízení aktiv	8,1	Odpovědnost za aktiva							
	8.1.1	Seznam aktiv							
	8.1.2	Vlastnictví aktiv							
	8.1.3	Přípustné použití aktiv							
	8.1.4	Navrácení aktiv							
	8,2	Klasifikace informací							
	8.2.1	Klasifikace informací							
	8.2.2	Označování informací							
	8.2.3	Manipulace s aktivy							
	8,3	Manipulace s médii							
	8.3.1	Správa výměnných médií							
8.3.2	Likvidace médií								
8.3.3	Přeprava fyzických médií								
9 Řízení přístupu	9,1	Požadavky organizace na řízení přístupu							
	9.1.1	Politika řízení přístupu							
	9.1.2	Přístup k sítím a síťovým službám							
	9,2	Řízení přístupu uživatelů							
	9.2.1	Registrace a zrušení registrace uživatele							
	9.2.2	Správa uživatelských přístupů							
	9.2.3	Správa privilegovaných přístupových práv							
	9.2.4	Správa tajných autentizačních informací uživatelů							
	9.2.5	Přezkoumání přístupových práv uživatelů							
	9.2.6	Odebrání nebo úprava přístupových práv							
	9,3	Odpovědnost uživatelů							
	9.3.1	Používání tajných autentizačních informací							
	9,4	Řízení přístupu k systémům a aplikacím							
	9.4.1	Omezení přístupu k informacím							
	9.4.2	Bezpečné postupy přihlášení							
	9.4.3	Systém správy hesel							
	9.4.4	Použití privilegovaných programových nástrojů							
9.4.5	Řízení přístupu ke zdrojovým kódům								

Příloha č. 2: Ukázka návrhu Prohlášení o aplikovatelnosti

10 Kryptografie	10,1	Kryptografická opatření							
	10.1.1	Politika pro použití kryptografických opatření							
	10.1.2	Správa klíčů							
11 Fyzická bezpečnost a bezpečnost prostředí	11,1	Bezpečné oblasti							
	11.1.1	Fyzický bezpečnostní perimetr							
	11.1.2	Fyzické kontroly vstupu							
	11.1.3	Zabezpečení kanceláří, místností a vybavení							
	11.1.4	Ochrana před vnějšími hrozbami a hrozbami prostředí							
	11.1.5	Práce v bezpečných oblastech							
	11.1.6	Oblasti pro nakládku a vykládku							
	11,2	Zařízení							
	11.2.1	Umístění zařízení a jeho ochrana							
	11.2.2	Podpůrné služby							
	11.2.3	Bezpečnost kabelových rozvodů							
	11.2.4	Údržba zařízení							
	11.2.5	Přemístění aktiv							
	11.2.6	Bezpečnost zařízení a aktiv mimo prostory organizace							
	11.2.7	Bezpečná likvidace nebo opakované použití zařízení							
11.2.8	Uživatelská zařízení bez obsluhy								
11.2.9	Zásada prázdného stolu a prázdné obrazovky								
12 Bezpečnost provozu	12,1	Provozní postupy a odpovědnosti							
	12.1.1	Dokumentované provozní postupy							
	12.1.2	Řízení změn							
	12.1.3	Řízení kapacit							
	12.1.4	Princip oddělení prostředí vývoje, testování a provozu							
	12,2	Ochrana proti malwaru							
	12.2.1	Opatření proti malwaru							
	12,3	Zálohování							
	12.3.1	Zálohování informací							
	12,4	Zaznamenávání formou logů a monitorování							
	12.4.1	Zaznamenávání událostí formou logů							
	12.4.2	Ochrana logů							

Příloha č. 2: Ukázka návrhu Prohlášení o aplikovatelnosti

provozu	12.4.3	Logy o činnosti administrátorů a operátorů							
	12.4.4	Synchronizace hodin							
	12,5	Správa provozního softwaru							
	12.5.1	Instalace softwaru na provozní systémy							
	12,6	Řízení technických zranitelností							
	12.6.1	Řízení technických zranitelností							
	12.6.2	Omezení instalace softwaru							
	12,7	Hlediska auditu informačních systémů							
	12.7.1	Opatření k auditu informačních systémů							
13 Bezpečnost komunikací	13,1	Správa bezpečnosti sítě							
	13.1.1	Opatření v sítích							
	13.1.2	Bezpečnost síťových služeb							
	13.1.3	Princip oddělení v sítích							
	13,2	Přenos informací							
	13.2.1	Politiky a přístupy při přenosu informací							
	13.2.2	Dohody o přenosu informací							
	13.2.3	Elektronické předávání zpráv							
	13.2.4	Dohody o utajení nebo o mlčenlivosti							
14 Akvizice, vývoj a údržba systémů	14,1	Bezpečnostní požadavky informačních systémů							
	14.1.1	Analýza a specifikace požadavků bezpečnosti informací							
	14.1.2	Zabezpečení aplikačních služeb ve veřejných sítích							
	14.1.3	Ochrana transakcí aplikačních služeb							
	14,2	Bezpečnost v procesech vývoje a podpory							
	14.2.1	Politika bezpečného vývoje							
	14.2.2	Postupy řízení změn systémů							
	14.2.3	Technické přezkoumání aplikací po změnách provozní platformy							
	14.2.4	omezení změn softwarových balíčků							
	14.2.5	Principy budování bezpečných systémů							
14.2.6	Prostředí bezpečného vývoje								
14.2.7	Outsourcingový vývoj								

Příloha č. 2: Ukázka návrhu Prohlášení o aplikovatelnosti

	14.2.8	Testování bezpečnosti systémů							
	14.2.9	Testování akceptace systémů							
	14,3	Data pro testování							
	14.3.1	Ochrana dat pro testování							
15 Dodavatelské vztahy	15,1	Bezpečnost informací v dodavatelských vztazích							
	15.1.1	Politika bezpečnosti informací pro dodavatelské vztahy							
	15.1.2	Bezpečnostní požadavky v dohodách s dodavateli							
	15.1.3	Dodatelský řetězec informačních a komunikačních technologií							
	15,2	Řízení dodávek služeb dodavatelů							
	15.2.1	Monitorování a přezkoumávání služeb							
	15.2.2	Řízení změn ve službách							
16 Řízení incidentů bezpečnosti informací	16,1	Řízení incidentů bezpečnosti informací a zlepšování							
	16.1.1	Odpovědnosti a postupy							
	16.1.2	Hlášení událostí bezpečnosti informací							
	16.1.3	Hlášení slabých míst bezpečnosti informací							
	16.1.4	Posouzení a rozhodnutí o událostech bezpečnosti informací							
	16.1.5	Reakce na incidenty bezpečnosti informací							
	16.1.6	Ponaučení z incidentů bezpečnosti informací							
	16.1.7	Shromažďování důkazů							
Aspekty řízení kontinuity činnosti organizace z hlediska bezpečnosti informací	17,1	Kontinuita bezpečnosti informací							
	17.1.1	Plánování kontinuity bezpečnosti informací							
	17.1.2	Implementace kontinuity bezpečnosti informací							
	17.1.3	Verifikace, přezkoumávání a vyhodnocení kontinuity bezpečnosti informací							
	17,2	Redundance							

Příloha č. 2: Ukázka návrhu Prohlášení o aplikovatelnosti

	17.2.1	Dostupnost vybavení pro zpracování informací							
18 Soulad s požadavky	18,1	Soulad s právními a smluvními požadavky							
	18.1.1	Identifikace odpovídající legislativy a smluvních požadavků							
	18.1.2	Ochrana duševního vlastnictví							
	18.1.3	Ochrana záznamů							
	18.1.4	Soukromí a ochrana osobních údajů							
	18.1.5	Regulace kryptografických opatření							
	18,2	Přezkoumání bezpečnosti informací							
	18.2.1	Nezávislá přezkoumání bezpečnosti informací							
	18.2.2	Shoda s bezpečnostními politikami a normami							
	18.2.3	Přezkoumání technické shody							