Moravská vysoká škola Olomouc

Ústav informatiky a aplikované matematiky

Šimon Fanta

Hodnocení bezpečnosti v podnikové informatice

The Security Assessment in Business Informatics

Bakalářská práce

Vedoucí práce: Mgr. Zdeňka Krišová

Olomouc 2014

Prohlášení

Prohlašuji, že jsem bakalářskou práci vypracoval(a) samostatně a použil(a) jen uvedené informační zdroje. Prohlašuji, že odevzdaná tištěná verze bakalářské práce se shoduje s elektronickou verzí vloženou do IS/STAG.

Olomouc: ……

Podpis

Poděkování

Zde bych velmi rád poděkoval vedoucí bakalářské práce Mgr. Zdeňce Krišové za trpělivé vedení a věcné připomínky při vedení mé bakalářské práce. Dále bych rád poděkoval též panu Ing. Miroslavu Hübnerovi, MBA ze společnosti Pražská energetika, a.s. za pomoc a rady při tvorbě bakalářské práce.

Obsah

1 Úvod

V současné době se množství zpracovávaných informací závratnou rychlostí zvětšuje. Proto se otázka ochrany takových informací stává naprosto nevyhnutelnou. Žádný podnik nebo organizace si nemůže dovolit, aby data, která jsou zpracovávána, ztratila svou dostupnost, integritu nebo dokonce důvěryhodnost. Tento problém byl důvodem, který mě vedl k vybrání tématu pro mou bakalářskou práci. V ní jsem se rozhodl rozebrat problematiku zajištění bezpečnosti informací.

2 Cíle

Cílem této mé práce je zhodnocení a analýza bezpečnosti Informatiky ve firmě Pražská energetika a.s. (dále jen „PRE, a.s.“) a návrh nových zlepšení nebo opatření ke zvýšení bezpečnosti ve spolupráci s managementem PRE, a.s. Dále v práci uvádím skutečnosti, které jsou v oblasti zajištění bezpečnosti důležité. Jako metody práce použiji analýzu stávajícího prostředí v PRE, a.s., v hodnocení bezpečnosti používám metodu komparace kladů a záporů jednotlivých metodik společnosti PRE, a.s. Nedílnou součástí je také definování základních pojmů, důležitý je i úvod do legislativy, přehled norem bezpečnosti informací a objasnění problematiky Systému řízení bezpečnosti informací (ISMS). Dalším cílem práce je zhodnocení zavedených bezpečnostních opatření v praxi. Pro zhodnocení jsem se rozhodl použít bezpečnostní opatření uvedené v normě ISO/IEC 27001. Hodnocení bezpečnosti informatiky ve společnosti Pražská energetika a.s. bylo prováděno na základě mých praktických zkušeností na pozici interního auditora bezpečnosti a kvality a konzultací se zaměstnanci Informatiky. Pro obě dvě odvětví – tedy bezpečnost i kvalitu – jsem certifikovaným auditorem.

Hodnocenou organizací je společnost Pražská energetika a.s., kde jsem zaměstnán od roku 2006 v sekci Informatika. Pozici jednoho z interních auditorů bezpečnosti a kvality zastávám od roku 2010. Hlavním impulsem pro provedení analýzy bezpečnosti informatiky v PRE, a.s. bylo mé přesvědčení, že její bezpečnost je na vysoké úrovni, a proto jsem chtěl provést rozbor, zdokumentovat jej a tuto práci předložit jako zpětnou vazbu managementu Informatiky. Tato zjištění mají usnadnit práci a postupy v dané oblasti budoucím čtenářům.

3 Základní pojmy

Pro správné vysvětlení a následné pochopení dané problematiky uvádím základní používané pojmy.

Informace

Wikipedia uvádí: „*Z lat.* ***in-formatio****, utváření, ztvárnění je velmi široký, mnohoznačný pojem, který se užívá v různých významech. V nejobecnějším smyslu je informace chápána jako údaj o prostředí, jeho stavu a procesech v něm probíhajících. Informace snižuje nebo odstraňuje neurčitost (entropii) systému (např. příjemce/uživatele informace). Množství informace lze charakterizovat tím, jak se jejím přijetím změnila míra neurčitosti přijímajícího systému.*

Užší významy informace lze roztřídit takto:

- ***V běžné řeči****:*
  - *informace jako vědění, které lze předávat, jako obsah zprávy či sdělení;*
  - *informace (plurál) místo, kde se lze o něčem informovat.*
- ***Ve vědě*** *je informace vnímaným údajem o vlastnostech a uspořádání objektu (negentropie).*
- *V* ***informatice*** *tvoří informaci kódovaná data (protiklad šumu), která lze vysílat, přijímat, uchovávat a zpracovávat technickými prostředky. Množství informace je rozdíl mezi neurčitostí (entropií) informace (nebo stavu) před a po zprávě. Občas je slovo informace chybně zaměňováno s pojmem data, který spíše představuje „to, z čeho informaci získáváme“ (například číslo na konkrétní osobu z telefonního seznamu). Nosičem informace je signál.“*[1]

Informační systém (IS)

Informační systém zajišťuje správné uvedení informací, práci s informacemi a v rámci nějakého systému jejich posun dále. Základem celého IS je

- Vstup (input) – zahrnuje prvky, umožňující zachytit informační a další vstupy, které mají být předmětem zpracování, případné vstupy, vzájemně propojit.
- Zpracování (processing) – zahrnuje prvky, které zajišťují transformaci vstupů do požadovaného výstupu.

[1]WIKIPEDIA. *Infromace*, http://cs.wikipedia.org/wiki/Informace

- Výstup (output) – představuje prvky, které jsou schopny převést informační a další výstupy k jeho příjemci (uživateli).[2]

Takový systém je pak rozšířen o komponenty, které zajišťují jeho řízení (kontrolu) o zpětnou vazbu (feedback).

Bezpečnost

Dle Ministerstva vnitra ČR lze bezpečnost definovat jako: „*Stav, kdy je systém schopen odolávat známým a předvídatelným vnějším a vnitřním hrozbám, které mohou negativně působit proti jednotlivým prvkům (případně celému systému) tak, aby byla zachována struktura systému, jeho stabilita, spolehlivost a chování v souladu s cílovostí. Je to tedy míra stability systému a jeho primární a sekundární adaptace.*“[3]

Bezpečnost informací

Internetové stránky ITIL uvádějí: *„V dnešní době, kdy platí, že informace mají cenu zlata, neexistuje organizace (ať už se jedná o komerční subjekt nebo orgán veřejné správy), která by nějakými důležitými informacemi nedisponovala. Mohou to být informace z oblasti technického know-how, obchodní informace nebo jen osobní údaje zaměstnanců. Jedno však mají společné – je nutné je chránit. Není těžké si představit, co se může stát, pokud důležité informace (např. databáze klientů) budou nenávratně zničeny, nebo bude originální výrobní postup zaměstnancem vyzrazen konkurenci. Bezpečnost informací se zabývá právě způsoby zajištění takové ochrany.*

Bezpečnost informací si klade za cíl chránit informace v jakékoliv podobě. Je zcela nepodstatné, jakou mají formu (listinnou nebo elektronickou), kde se uchovávají (zdali v trezoru nebo ve vzdáleném informačním systému). To co je podstatné, je hodnota chráněných informací, případně velikost škody vzniklé v souvislosti s „poškozením“ těchto informací.“[4]

Bezpečnostní politika

Dle AEC je bezpečnostní politika popisována takto: *„Bezpečnostní politika organizace tvoří jeden ze základních pilířů, na kterém stojí systém řízení informační bezpečnosti. Bezpečnostní politika určuje rámec informační bezpečnosti organizace a je po schválení vedením závazná pro všechny zaměstnance a je směrodatná i pro všechny externí subjekty, které přicházejí do kontaktu s ICT službami organizace*.

[2] Srov. Gála, L., Pour, J., Šedivá, Z., *Podniková informatika*, s. 47.

[3] MVČR. *Bezpečnost*, http://www.mvcr.cz/clanek/pojmy-bezpecnost.aspx

[4] ITIL/ITSM. *Bezpečnost informací,* http://www.itil.cz/index.php?id=933

Bezpečnostní politika musí být v souladu s politikou celé organizace, definuje základní strategii, cíle, postoje, role, zodpovědnosti a zásady týkající se činností spojených s informační bezpečností.“[5]

Důvěrnost

Norma ČSN ISO/IEC 27001 uvádí: *„Důvěrnost znamená zabezpečení, že informace jsou přístupné, nebo sděleny pouze těm, kteří jsou k tomu oprávněni.“*[6]

Dostupnost

Norma ČSN ISO/IEC 27001 uvádí: *„Dostupnost znamená zabezpečení, že informace je pro oprávněné uživatele přístupná v okamžiku její potřeby.“*[7]

Integrita

Norma ČSN ISO/IEC 27001 uvádí: *„Integrita znamená zabezpečení správnosti a úplnosti informací.“*[8]

Systém managementu bezpečnosti informací

Norma ČSN ISO/IEC 27001 uvádí: *„Přeloženo z anglického originálu, který zní Information Security Management System – ISMS. ISMS je základním kamenem současného trendu řízení bezpečnosti informací dle ISO/IEC 27001, kde jsou definovány pravidla pro zavádění ISMS.*

Část systému řízení organizace, založená na přístupu (organizace) k rizikům činnosti, která je zaměřena na ustanovení, zavádění, provoz, monitorování, přezkoumání, údržbu a zlepšování bezpečnosti informací.“

Portál Risk Analysis Consultants popisuje Systém managementu bezpečnosti informací takto: *„Systém řízení bezpečnosti informací (ISMS) je dokumentovaný systém prokazující, že popsaná informační aktiva jsou chráněna, rizika bezpečnosti informací jsou řízena, jsou zavedena opatření s požadovanou úrovní záruk a ta jsou kontrolována. ISMS může být zaveden pro specifický IS, jednotlivé části IS nebo může zahrnovat celou organizaci.*

Řada organizací, pro které jsou informace a informační technologie klíčovou součástí podnikatelských procesů, se rozhoduje, jak efektivně zajistit jejich bezpečnost.

---

[5] AEC. *Bezpečnostní politika organizace,* http://www.aec.cz/cz/sluzby/bezpecnostni-politika-organizace

[6] ČNI, *Informační technologie - Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky, s. 8.*

[7] ČNI, *Informační technologie - Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky, s. 8.*

[8] ČNI, *Informační technologie - Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky, s. 8.*

Řešení této problematiky vyžaduje odpovídající systémové a komplexní přístupy, proto jsou základním vodítkem pro tuto oblast ISO normy ISO/IEC 27001 (BS 7799-2) a ISO/IEC 27002. Obě normy jsou úzce propojeny, každá z nich však plní jinou roli. Zatímco norma ISO 27002 poskytuje podrobný přehled (katalog) bezpečnostních opatření, které mohou být vybrány při budování ISMS, norma ISO 27001 specifikuje požadavky na to jak v organizaci správně ustavit, zavést, monitorovat, udržovat a zlepšovat systém pro řízení bezpečnosti informací organizace (ISMS organizace). Případná certifikace ISMS pak probíhá podle ISO 27001.“[9]

Aktivum

Norma ČSN ISO/IEC TR 13335:1998 uvádí: *„Aktivum je komponenta nebo část celkového systému, které organizaci přímo přiřazuje hodnotu a pro kterou tudíž organizace požaduje ochranu.*

Druhy aktiv mohou být následující:

- *Informace/data (např. soubory obsahující podrobnosti o platbách, informace o produktech)*
- *Hardware (PC, tiskárna atd.)*
- *Software, včetně aplikací*
- *Komunikační zařízení*
- *Dokumenty (např. smlouvy)*
- *Personál*
- *Know-how*
- *Atd.“*[10]

Aktivum je cokoliv, co má nějakou hodnotu.

4 Legislativa zabývající se bezpečností informací

V této kapitole chci vysvětlit problematiku legislativy, jejímž obsahem je bezpečnost informací. Při řešení bezpečnosti informací bývají hlavním pilířem právě legislativní opatření, proto považuji za důležité se o nich zmínit.

Tvorbu a vydávání legislativy můžeme rozdělit do dvou základních skupin. Je to jednak legislativa zákonná, jež je vydávána místními zákonnými orgány, což je v České

[9] RAC. *Zavedení systému řízení bezpečnosti informací*, http://www.rac.cz/rac/homepage.nsf/CZ/ISMS

[10] ČNI, *Informační technologie*, s. 7.

republice Parlament ČR, Senát a další. Dále pak je legislativa vydávána organizacemi, které se zabývají vytvářením a publikováním různých směrnic, norem, doporučení či nařízení.

Uvádím tedy tuto problematiku rozdělenou do dvou částí – právě dle způsobu vydávání legislativy. V části první je popisována legislativa zákonná (ve zkratce jsou popsány dva české zákony) a v části druhé pak jsou uváděny normy a vydavatelé norem.

Závěrem této části je uvedeno shrnutí legislativy.

4.1 Zákonná legislativa

Pojem zákonná legislativa zahrnuje zákony, vyhlášky či místní nařízení, vydávané zákonnými organizacemi. Společnosti, na něž má tato legislativa dopad, jsou povinny se jimi řídit. V případě neplnění této povinnosti jsou společnosti postihovány podle zákona. Dva hlavní zákony, které s touto problematikou přímo souvisí, jsou následující:

- Zákon č. 412/2005 Sb., o ochraně utajovaných informací
- Zákon č. 101/2000 Sb., o ochraně osobních údajů

4.1.1 Zákon č. 412/2005 Sb., o ochraně utajovaných informací

Tento zákon upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy.
Zákon definuje následující stupně utajení:

- ***„Přísně tajné**, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit mimořádně vážnou újmu zájmům České republiky*
- ***Tajné**, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit vážnou újmu zájmům České republiky,*
- ***Důvěrné**, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit prostou újmu zájmům České republiky,*
- ***Vyhrazené**, jestliže její vyzrazení neoprávněné osobě nebo zneužití může být nevýhodné pro zájmy České republiky.“*[11]

Tyto stupně utajení se přímo dotýkají i osob, jež mají k informacím přístup.

[11] NBU. *Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů*, http://www.nbu.cz/cs/pravni-predpisy/zakon-c-4122005/

4.1.2 Zákon č. 101/2000 Sb., o ochraně osobních údajů

Zákon č. 101/2000 Sb. uvádí: *„Osobní údaje jsou jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.“*[12]

Dle tohoto zákona existují tzv. správci nebo zpracovatelé osobních údajů a pak osoby, jejichž osobní údaje jsou zpracovávány, tzv. subjekty údajů.

Pro správce a zpracovatele jsou stanovovány a ukládány povinnosti, subjektům jsou přiznávána práva. Aby tato práva byla dodržována, byl zřízen Úřad na ochranu osobních údajů, jež má také dohlížet na plnění povinností správců a zpracovatelů. Neplnění těchto povinností podléhá sankcím. Správci a zpracovatelé musejí své povinnosti dobře znát.

4.1.3 Zákon o kybernetické bezpečnosti

Národní bezpečnostní úřad (NBÚ) připravil návrh zákona o kybernetické bezpečnosti, který je v současné době v připomínkovém řízení. Zákon by měl nabýt účinnosti 1. 1. 2015. Návrh naplňuje a rozvádí zejména první pilíř zákona o kybernetické bezpečnosti. Ten tvoří bezpečnostní opatření, tj. požadavky na standardizaci kritické informační infrastruktury a významných informačních systémů.

Riziko incidentu hrozí všem subjektům, které pracují s větším množstvím osobních údajů, které jsou chráněny zákonem č. 101/2000 Sb., o ochraně osobních údajů, a v případě jejich úniku, krom ztráty dobrého jména, existuje zákonná odpovědnost vedení společnosti.

4.2 Normy a směrnice

Další legislativou v oblasti bezpečnosti informací jsou normy a směrnice, které jsou vydávány orgány, jež mohou být, státní, soukromé, národní či mezinárodní.

Normy jsou definovány jako směrnice, pravidlo, jehož zachování je závazné, např. mravní, právní, technické. Norma technická přesně stanovuje požadované vlastnosti, provedení, tvar nebo uspořádání opakujících se předmětů nebo způsobů a postupů práce, popř. vymezuje všeobecně užívané technické pojmy.

[12] OOU. *Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů*, http://www.oou.cz/index.php?file=personal_data_protection_zakon_101

Hlavní úkoly normy jsou:

- zjednodušování a snižování rozmanitosti výrobků a činností,
- dorozumívací funkce mezi výrobcem a zákazníkem a mezi výrobci v národním i mezinárodním měřítku,
- zavádění symbolů a kódů ke zjednodušení obchodního styku a překonání potíží způsobených rozdílností jazyků,
- zlepšení hospodárnosti,
- zlepšení bezpečnosti a ekologie,
- ochrana spotřebitele.

4.2.1 Instituce vydávající normy

Drtivou většinu norem vydávají organizace a instituce, které jsou zakládány státem, respektive vládami jednotlivých států, nebo minimálně jsou pod jejich vlivem a podporou. Pro detailní popis jsem vybral tyto instituce, které jsou spojené s problematikou normy ISO/IEC 27001

- Český normalizační institut,
- Úřad pro technickou normalizaci, standardizaci, metrologii a státní zkušebnictví,
- International Organization for Standardization.

4.2.1.1 Český normalizační institut

Český normalizační institut byla státní příspěvková organizace**,** která byla v roce 2008 zrušena rozhodnutím Ministra průmyslu a obchodu ČR. Díky rozhodnutí Ministerstva obchodu a průmyslu byla tato příspěvková organizace pověřena zajišťovat tvorbu, vydávání a pravidelné zveřejňování českých technických norem. V současné době zajišťuje tuto činnost Úřad pro technickou normalizaci, standardizaci, metrologii a státní zkušebnictví.[13]

4.2.1.2 Úřad pro technickou normalizaci, standardizaci, metrologii a státní zkušebnictví

Úřad pro technickou normalizaci, metrologii a státní zkušebnictví (ÚNMZ) zřídila Česká národní rada zákonem č. 20/1993 Sb., o zabezpečení výkonu státní správy v oblasti technické normalizace, metrologie a státního zkušebnictví. Spadá pod působnost Ministerstva průmyslu a obchodu ČR. Jeho hlavním úkolem je zabezpečovat úkoly, které stanovují zákony České republiky upravující technickou normalizaci, metrologii a státní

[13] Srov. CSNI, *Český normalizační institut.*

zkušebnictví a úkoly v oblasti technických předpisů a norem uplatňovaných v rámci členství ČR v Evropské unii. Od roku 2009 zajišťuje také tvorbu a vydávání českých technických norem.[14]

Aktuálně je předsedou úřadu Mgr. Viktor Pokorný.

4.2.1.3 International Organization for Standartization

V překladu Mezinárodní organizace pro standardizaci. Jedná se o největší organizaci ve světě, která se zabývá tvorbou a vydáváním mezinárodně platných norem. V ISO jsou organizovány národní instituty pro standardizaci z celkem 163 zemí. Sídlo ISO je ve švýcarské Ženevě. Je to nevládní organizace, která – přeloženo z ISO je mostem mezi veřejným a soukromým sektorem.

Mezinárodní organizace pro normalizaci se zabývá tvorbou mezinárodních norem ISO a jiných druhů dokumentů ve všech oblastech normalizace kromě elektrotechniky. Jsou to např.:

- TS – technické specifikace
- TR – technické zprávy
- PAS – veřejně dostupné specifikace
- TTA – dohody o technických trendech
- IWA – dohody z pracovní konference průmyslu
- Pokyny ISO.

Na pracích technických komisí je možno se podílet jako aktivní členové (P – členové – participating members), kteří mají povinnost účastnit se zasedání a hlasovat k dokumentům, nebo jako pozorovatelé (O – členové – observer members), kteří dostávají pracovní dokumenty a mají právo, nikoliv povinnost účastnit se zasedání a hlasovat.[15]

4.3 Shrnutí legislativy

Je nezbytné průběžně sledovat legislativu jako takovou, tedy kterým směrem se ubírá, mít přehled o jednotlivých úpravách – dodatcích, a to v obou typech legislativy, což je ale mnohdy složité, zvláště pak pro čtenáře bez příslušného vzdělání. Legislativa je psána jako vysoce odborný text, ve kterém se laik poměrně těžko orientuje, což platí obzvláště pro legislativu zákonnou. Navíc celou situaci komplikuje fakt, že jednotlivé

[14] Srov. UNMZ, *O úřadu.*

[15] Srov. WIKIPEDIA, *International Organization for Standartization*

zákony se často liší v různých státech a zemích. Mohou se dokonce lišit i uvnitř státu např. mezi jednotlivými kraji.

5 Rozbor normy ISO 27001

Norma ISO/IEC 27001:2005 byla přeložena do českého jazyka prostřednictvím Českého normalizačního institutu. Tato norma má ovšem stejný status jako oficiální verze. Předchozí norma ČSN BS 7799-2 (36 9790) z prosince 2004 je touto normou v plném rozsahu nahrazena.

5.1 Předmět normy

5.1.1 Všeobecně

Norma ČSN ISO/IEC 27001 má mezinárodní platnost a mohou se jí řídit všechny organizace, tedy např. vládní úřady a agentury, organizace obchodní, soukromé i státní, neziskové organizace. Norma konkretizuje požadavky na zavedení bezpečnostních opatření v přímé souvislosti s potřebami jednotlivých organizací. Specifikuje požadavky na ustavení, zavedení, provoz, a zlepšování dokumentovaného ISMS se zohledněním celkových rizik činností organizace.

Princip ISMS je takový, že zajišťuje odpovídajícím a přiměřeným způsobem bezpečnostní opatření. Současně ochraňuje informační aktiva. Je zárukou jistoty pro zúčastněné strany.

5.1.2 Použití normy

Normou ČSN ISO/IEC 27001 se mohou řídit obecně všechny organizace, nezávisle na předmětu jejich činnosti, typu organizace a jejich velikosti. Vyloučení jakýchkoli požadavků, které jsou specifikovány níže, je nepřijatelné, pakliže chce společnost dosáhnout souladu s touto normou.

Požadavky normy, které nelze vyloučit:

- Systém managementu bezpečnosti informací
- Odpovědnost vedení
- Interní audity ISMS
- Přezkoumávání ISMS vedením organizace
- Zlepšování ISMS.

Jakákoli vyloučení opatření, která byla stanovena jako nezbytná pro snížení rizik, jsou přijatelná pouze v případě, že rizika, která jsou s tím spojená, byla akceptována odpovědnou osobou. Tato akceptace musí být doložena.

Pokud budou taková vyloučení opatření provedena, lze toto akceptovat jako soulad s normou. Podmínkou ale je, že takováto vyloučení opatření neovlivní schopnost organizace nebo její odpovědnost zajistit bezpečnost informací. Taková bezpečnost musí být v souladu s bezpečnostními požadavky.

5.1.3 Termíny a definice normy ISO 27001 - ISMS

- **Aktivum (asset)**

  Cokoliv, co má pro organizaci nějakou hodnotu.

- **Dostupnost (availability)**

  Zjištění, že informace je pro oprávněné uživatele přístupná v okamžiku její potřeby.

- **Důvěrnost (confidentiality)**

  Zajištění, že informace jsou přístupné nebo sděleny pouze těm, kteří jsou k tomu oprávněni.

- **Bezpečnost informací (information security)**

  Zachování důvěrnosti, integrity a dostupnosti informací a dalších vlastností, jako např. autentičnost, odpovědnost, nepopiratelnost a spolehlivost.

- **Bezpečnostní událost (information security event)**

  Identifikovaný stav systému, služby nebo sítě, ukazující na možné porušení bezpečnostní politiky nebo selhání bezpečnostního opatření. Může se také jednat o jinou předtím nenastalou situací, která může být důležitá z pohledu bezpečnosti informací.

- **Bezpečnostní incident (information security incident)**

  Jedna nebo více nechtěných nebo neočekávaných bezpečnostních událostí, u kterých existuje vysoká pravděpodobnost kompromitace činností organizace a ohrožení bezpečnosti informací.

- **Systém managementu bezpečnosti informací ISMS (information security management system)**

  Část celkového systému managementu organizace založená na přístupu (organizace) k rizikům činností, která je zaměřena na ustavení, zavádění, provoz, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací.

- **Integrita (integrity)**
  Zajištění správnosti a úplnosti informací.
- **Zbytkové riziko (residual risk)**
  Riziko zbývající po uplatnění zvládání rizik.
- **Akceptace rizik (risk acceptance)**
  Rozhodnutí přijmout riziko.
- **Analýza rizik (risk analysis)**
  Systematické používání informací k odhadu rizika a k identifikaci jeho zdrojů.
- **Hodnocení rizik (risk assessment)**
  Celkový proces analýzy a vyhodnocení rizik.
- **Vyhodnocení rizik (risk evaluation)**
  Proces porovnávání odhadnutého rizika vůči daným kritériím pro určení jeho významu.
- **Management rizik (risk management)**
  Koordinované činnosti sloužící k řízení a kontrole organizace s ohledem na rizika.
- **Zvládání rizik (risk treatment)**
  Proces výběru a přijímání opatření ke změně rizika.
- **Prohlášení o aplikovatelnosti (statement of applicability)**
  Dokumentované prohlášení popisující cíle opatření a jednotlivá bezpečnostní opatření, která jsou relevantní a aplikovatelná v rámci ISMS organizace.

5.1.4 Metodiky normy

5.1.4.1 Interní audity ISMS

Interní audity ISMS musí být v každé organizaci prováděny v daných plánovaných termínech. Cílem těchto auditů je zjistit, jestli cíle opatření, jednotlivá bezpečnostní opatření, procesy a postupy ISMS:

- Vyhovují požadavkům této normy.
- Vyhovují daným požadavkům na bezpečnost informací.
- Jsou zavedeny a efektivně udržovány.
- Fungují tak, jak se očekává.

Jednotlivé audity musí být naplánovány s ohledem na stav a význam auditovaných oblastí. V úvahu je potřeba brát i výsledky předchozích auditů. Musí být předem dána kritéria auditů, metody a četnost. Rovněž je předem dán rozsah auditů. Při výběru auditorů

a provádění auditů musí být zajištěna objektivita, přičemž auditoři nesmí provádět audit na své vlastní práci.

Všechny tyto požadavky musí být dány dokumentovaným postupem. Vedoucí pracovníci v oblasti, která byla auditována, musí zajistit, aby byly bez odkladu odstraněny nedostatky a jejich příčiny.

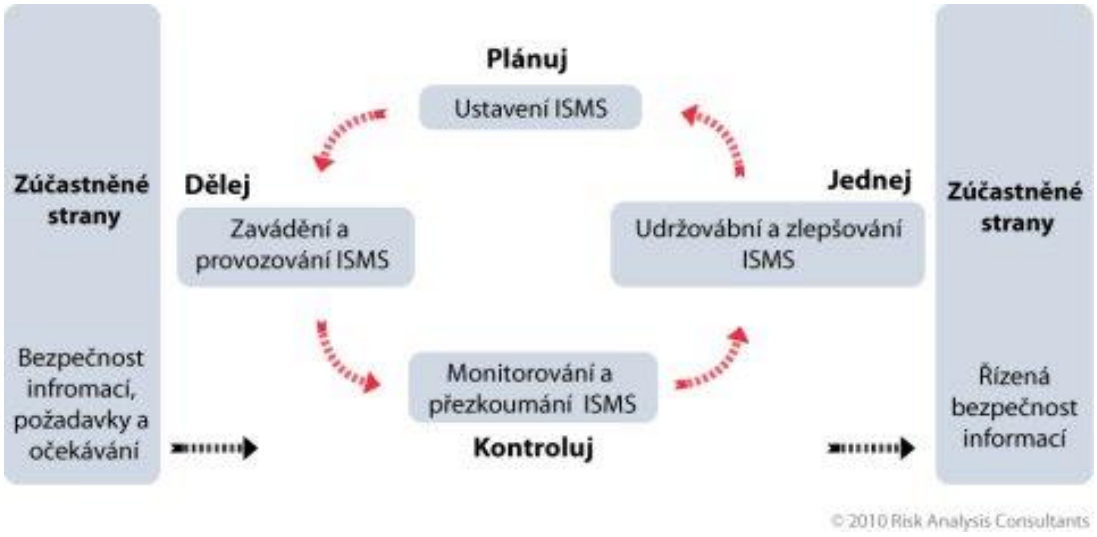
5.1.4.2 Přezkoumávání ISMS vedením organizace

Pravidelně, minimálně jednou ročně, musí být prováděno přezkoumání ISMS organizace. Účelem těchto přezkoumání je zajištění přiměřenosti a účinnosti ISMS a také vyhodnocení případných zlepšení a potřebných změn v ISMS.

O výsledcích takových přezkoumání musí být v organizaci vedeny záznamy.

5.1.4.3 Zlepšování ISMS

Cílem organizace musí být neustále zvyšování ISMS. Je nezbytné brát při tom v úvahu výsledky auditů, analýz jednotlivých událostí, nápravných opatření atd. Princip neustálého zlepšování je znázorněn na následujícím obrázku Demingova PDCA cyklu.



Obrázek č. 1 – PDCA cyklus použitý na procesy ISMS[16]

[16] Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/ISMS [online]. [cit. 2014-01-18]

Opatření k nápravě

Povinností organizace je přijmout taková opatření, aby došlo k odstranění nedostatků, které jsou spojeny s implementací a provozem ISMS. Tato opatření musí zabránit také opětovnému výskytu těchto nedostatků.

Pro názornost uvádím několik požadavků definovaných normou:

- Identifikace nesouladu v zavedení a/nebo provozu ISMS,
- určení příčin nesouladu,
- vyhodnocení potřeby, kterým se zajistí, že se nesoulad znovu nevyskytne,
- určení a zavedení potřebných opatření k nápravě.

Preventivní opatření

Jednou z povinností organizace je stanovit opatření, aby se zabránilo opakovanému výskytu nesouladu s požadavky ISMS. Taková opatření musí být přiměřená problémům. Postup aplikace preventivních opatření musí být zdokumentován.

Pro názornost uvádím některé požadavky definované touto normou:

- Identifikace potenciálních nesouladů a jejich příčin,
- vyhodnocení potřeby provedení činností k zamezení opětovného výskytu nesouladu,
- určení a zavedení potřebných preventivních opatření,
- zaznamenání výsledků podniknutých opatření,
- přezkoumání provedení preventivních opatření.

5.1.5 Názory na metodiky

Význam auditů v rozsahu, který popisuje tato norma, je jasný a naprosto nezpochybnitelný. Řadě lidí se někdy může na první pohled zdát, že se jedná o ztrátu času. Samozřejmě, že interní audity znamenají náklady na lidské zdroje na straně zaměstnanců, ale jedná se o dobrý feedback pro management v dané oblasti. Auditoři dokáží podle typizovaných dotazů a podnětů odhalit bezpečnostní rizika v systémech a procesech, která by jinak nemusela být odhalena. V takových případech by se stávala hrozbou pro organizaci. Zároveň ve spolupráci s řešitelem v auditované oblasti navrhnou potřebná opatření. Interní audity by neměly být brány jako „bič na zaměstnance a jejich pracovní výsledky“, nýbrž jako nástroj na zlepšení a podnět pro management – v čem jsou rezervy a kde je zapotřebí nápravy. Organizace pak může svoji certifikaci na ISO 27001 používat např. při soutěžích o veřejné zakázky, což může poskytovat další výhody.

Metodika zlepšování je nedílnou součástí interních auditů a je samostatně těžko oddělitelná. O přijatých opatřeních musejí být vedeny záznamy a jejich plnění je auditory kontrolováno, což je důkazem toho, že management v dané oblasti má zájem ve své působnosti neustále věci zlepšovat a posouvat dále. Management vidí posun organizace, což mu může pomáhat při strategických rozhodnutích.

6 Případová studie

6.1 Výběr společnosti Pražská energetika, a. s.

V této kapitole popisuji zajištění bezpečnosti informací v organizaci Pražská energetika, a.s. prostřednictvím metodik, které tato společnost používá. Zdrojem informací budou oficiální dokumenty, které mi poskytla Informatika společnosti vedená Ing. Miroslavem Hübnerem, MBA.

Společnost PRE, a.s. provádí zpracování a distribuci elektrické energie, jejíž spotřebu není možné omezovat. Je na českém trhu stabilní společností s dlouholetou tradicí, jejíž význam pro obchodní partnery neustále roste. Nedílnou součástí, je Informatika a informatické služby. Informatické služby procházejí napříč celou Skupinou PRE a jsou nepostradatelné v podstatě pro všechny podnikové útvary. Logické je, že požadavky jednotlivých útvarů mají různé nároky (v oblasti ekonomiky, strategie atd.) a tyto nároky mají rostoucí tendenci.

Podíváme-li se na podnikání PRE, a.s. z hlediska informačních technologií, aplikací a služeb, je evidentní, že právě Informatika toto podnikání podporuje. Informatika zajišťuje konkrétně:

- přístup k informacím a jejich zpracování,
- spolehlivou dodávku informatických služeb,
- predikci budoucích požadavků a hledání potenciálu informatiky,
- provoz infrastrukturních systémů,
- kontrolu efektivnosti portfolia informatických služeb[17].

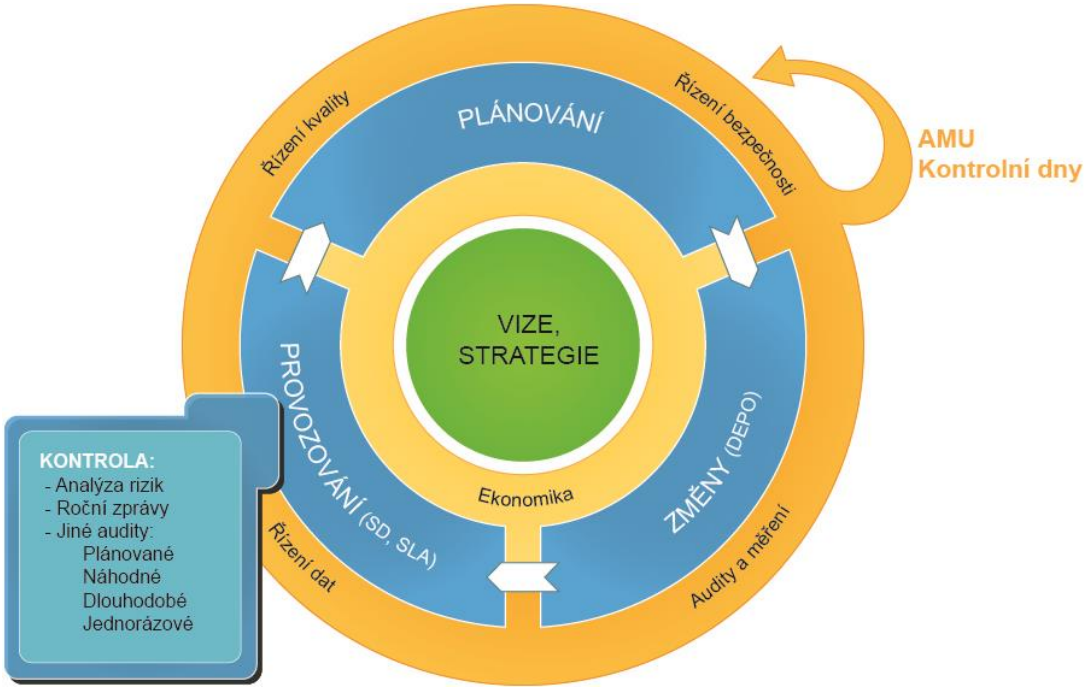
[17] Srov. PRAŽSKÁ ENERGETIKA, a. s., *Výroční zpráva,* s. 84

6.2 Popis nástrojů používaných v PRE, a.s.

Informatika ve společnosti PRE, a.s. používá pro zajištění a zlepšení bezpečnosti na poli informatických služeb následující nástroje:

- Interní audity ISMS a QMS,
- Analýzu rizik,
- Externí audity ISMS a QMS,
- Roční zprávu,
- Analýzu mimořádné události.

Jejich znázornění a využití je popsáno na obrázku č. 2 Využití nástrojů v IT službách.



Obrázek č. 2 – Využití nástrojů v IT službách PRE, a.s.[18]

6.2.1 Interní audity ISMS a QMS

Interní audity v sekci Informatika probíhají od dubna do konce června. Konají se pravidelně každý rok. Za průběh těchto auditů jsou odpovědni určení pracovníci z Informatiky, kteří byli na danou problematiku vyškoleni a certifikováni. Audit probíhá po oblastech, které se nazývají Kompetenční centra. Smysl tohoto rozdělení je v jeho větší přehlednosti a tím i snazší řiditelnosti a kontrole. O průběhu Interních auditů je informován manažer Informatiky, který také musí jednotlivé audity odsouhlasit. Veškeré podklady

[18] Vlastní zpracování

z interních auditů jsou posléze svázány do jedné knihy, která se předkládá při Recertifikačním a dozorovém externím auditu, jako podklad pro auditory.

Pro přehlednost uvádím vysvětlení pojmu Kompetenční centrum (dále jen „KC“).

6.2.1.1 Kompetenční centra

Název sice vypadá poněkud složitě, ale je to poměrně logický název. Jedná se o pravidelné setkávání lidí, kteří jsou kompetentní k rozhodování za určitou oblast. V Pražské energetice, a. s. většinu informatických služeb řídíme napříč liniovým řízením, daná kompetenční centra tak mohou řídit některé oblasti relativně samostatně.

Cílem kompetenčního centra je zajistit efektivní chod a rozvoj služeb v oblasti IT, ale musí respektovat požadavky uživatelů dotčených oddělení.

Mezi hlavní činnosti kompetenčního centra patří:

- zajišťování koordinace mezi jednotlivými službami,
- vytváření a schvalování koncepce a strategie v oblasti IT služeb,
- hospodaření s penězi, které kompetenční centrum pro danou IT oblast dostalo přiděleno,
- kontrola hospodaření s přidělenými finančními prostředky,
- určování priorit rozvoje a návrh plánu pro danou IT oblast,
- určování konkrétních pravidel práce a rozhodování pro danou IT oblast.

V současné době oblast Informatiky v PRE, a.s. zajišťují následující KC:

- Řídící služby,
- Bezpečnost a kvalita,
- Průřezové služby,
- Telekomunikace,
- Pracoviště,
- Infrastruktura,
- SAP,
- Zákaznické systémy,
- Řízení dat,
- Trh s elektřinou,
- Řízení sítě,
- Měření,
- Správa distribuční sítě,
- WEB,

- SW ostatní,
- Kompost.

6.2.1.2 Role v kompetenčním centru

Pro správné procesní řízení služeb máme v Pražské energetice, a. s. nadefinované určité role. Každá role se týká určité oblasti. Zpřehledňuje to tak činnost celého kompetenčního centra.

Pro kompetenční centra máme stanovené tyto role:

- **Vlastník služby**

  Představitel business, který rozhoduje o službě s ohledem na naplňování potřeb daného procesu.
- **Správce služby**

  Vždy je ze sekce informatika, jedná se o IT specialistu, který zajišťuje provoz dané služby.
- **Metodik služby**

  Jde vždy o zkušeného uživatele služby, který metodicky řídí její provoz, rozvoj a nastavení. Má velmi dobrou znalost procesů a služby, která je podporuje.
- **Odborný metodik služby**

  Jedná se o metodika služby, který koordinuje implementaci a schvaluje nasazení dokončených požadavků na změnu.
- **Technolog**

  Vždy je ze sekce Informatika, jedná se o IT specialistu, který je pověřen nasazováním realizovaných požadavků na změnu.
- **Klíčový uživatel**

  Je to zkušený uživatel služby, který spolupracuje s Metodikem služby.
- **Vedoucí kompetenčního centra**

  Osoba odpovědná za organizaci kompetenčního centra, připravuje podklady pro rozhodování, dobře zná koncepci celé oblasti.
- **Správce oblasti**

  Vždy je ze sekce Informatika, prezentuje a obhajuje stanovisko Informatiky, snaží se o efektivní působení z technického hlediska.
- **Vlastník dat**

  Zástupce konkrétní společnosti, která je majitelem „obsahu dat“. Odpovídá za způsob nakládání s daty a určuje pravidla pro přístup k těmto datům.

- **Metodik dat**

  Osoba, která zajišťuje nastavení pravidel za účelem dosažení stanovené úrovně kvality dat.

- **Správce dat**

  Vždy je ze sekce Informatika, jde o IT specialistu, který má přehled, kde jsou jednotlivá data uložena v systémech, posuzuje realizovatelnost požadavků.

- **Manažer dat**

  Jde o vlastníka procesů, který připravuje metodiku a další dokumenty v oblasti řízení.

6.2.1.3 Ostatní role

V Pražské energetice, a. s. máme definovány ještě role ve vztahu k řízení IT, které vyplývají z organizační struktury. Jsou to role: Vedoucí informatiky, Ekonom informatiky, IT architekt, Projektová kancelář, Hotline, Manažer bezpečnosti, Manažer kvality a Analytik. Tyto role se bezpodmínečně podílejí na procesním řízení v oblasti IT.

6.2.2 Interní audit ISMS a QMS Kompetenčního centra SAP

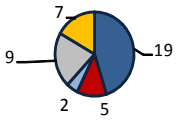
Průběh interních auditů v PRE, a.s. názorně ukážu na jednom vybraném kompetenčním centru (KC). Pro ukázku mi poslouží KC SAP.

6.2.2.1 Chod KC

V této části auditu jednotliví auditoři sbírají podkladová data, která vyznačují chod daného KC. Jedná se o statistiku z aplikace LogIT ve zobrazovaném období – viz obrázek č. 3 níže, kde se přesně zobrazuje počet akcí, které ovlivňovaly chod daného KC. Jednotlivé akce do této aplikace zapisují řešitelé pro dané oblasti. Současně také rozebírají a popisují příslušnou akci (odstávka, výpadek, restart, ostatní, změna konfigurace).

LogIT statistika 1.3.2012 - 1.3.2013

	odstávka	výpadek	restart	ostatní	změna konfigurace
SAP - Financování	-	-	-	-	-
SAP - Logistika	-	-	-	1	-
SAP - Mobilní čety	4	2	-	-	1
SAP - Personalistika	-	-	-	-	3
SAP - Řízení insvestic	-	-	-	-	-
SAP - SAP Režie	15	2	2	1	3
SAP - Účetnictví	-	1	-	1	-
SAP - Údržba(PM)	-	-	-	6	-
Celkem	19	5	2	9	7



odstávka
výpadek
restart
ostatní
změna konfigurace

Obrázek č. 3 – LogIT statistika[19]

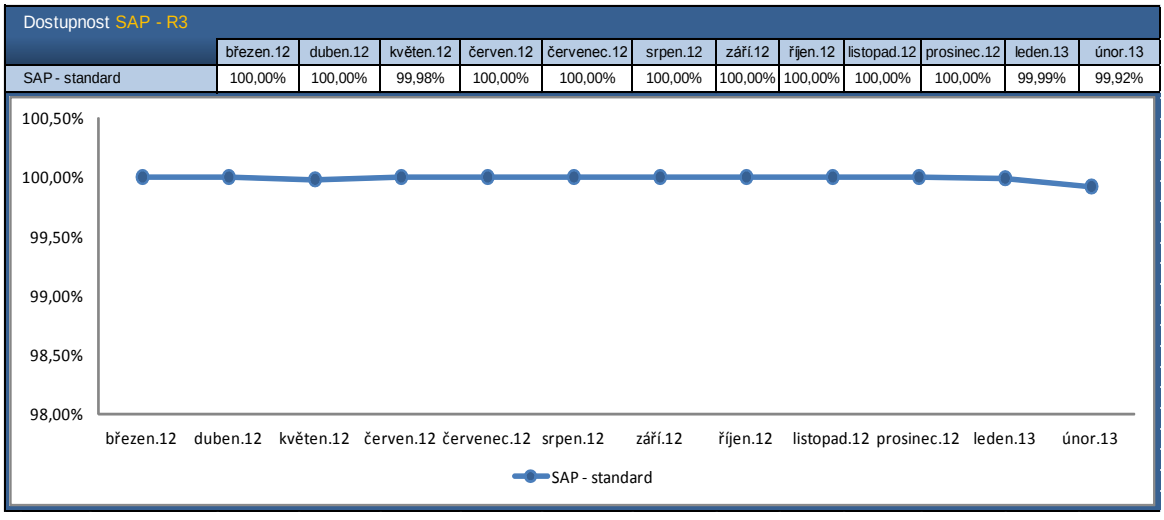
[19] Interní audity Kompetenčních center, interní dokument PRE, a.s.

Další částí chodu KC je popis výpadků, který vychází z aplikace LogIT. V této části jsou detailně popsány jednotlivé výpadky, které se za sledované období odehrály, včetně jejich opatření a dopadů na počty uživatelů. V této části je statistika výpadků zobrazována podle jednotlivých oblastí tak, jak jsou součástí systémů např. SAP – SAP Režie. Znázornění je v obrázku č. 4.

LogIT - Výpadky		
SAP - SAP Režie		
	datum	5.10.2012
	popis	V ELFA došlo k problému při rozesílání mailů schvalovatelům (3x denně jsou rozesílány systémem). Docházelo k chybnému přepínání schvalovatele na systémového uživatele, který maily rozesílá.
	opatření	Po zjištění problému jsme dávková rozesílání faktur ke schvalování zastavili, opravili a opět zprovoznili.
	datum	23.10.2012
	popis	Několika uživatelům zmizelo nastavení přístupu do systému.
	opatření	Nastavena nová hesla.
	datum	3.12.2012
	popis	Došlo k zaplnění log area v datbázi CS.
	opatření	K problému nedochází v běžném provozu, jednalo se o hromadný import dat.
	datum	16.1.2013
	popis	Nebylo funkční propojení mezi IT kancelářskou sítí a sítí cety.pre.
	opatření	Na straně infrastruktury.
	datum	20.2.2013
	popis	Na telefonní ústředně v místnosti B217 došlo k nechtěnému odpojení napájení pro komunikační technologie.
	opatření	Opatrnost při pracích v telefonní ústředně.

Obrázek č. 4 – LogIT výpadky[20]

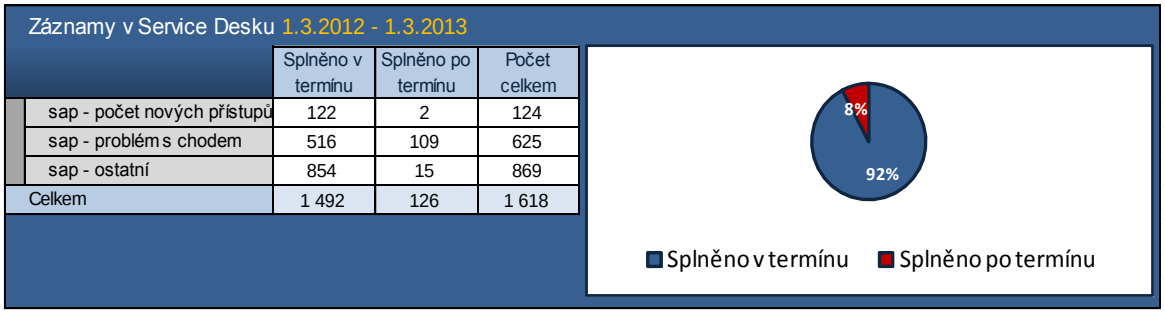
Další oblastí této části je dostupnost KC. Dostupnosti jsou měřeny a kontrolovány pravidelně každý měsíc a jejich hodnoty jsou zapisovány do Excelu. Pakliže se některá dostupnost (nedostupnost) systémů propadne pod hranici definovanou vedením Informatiky, je na tuto konkrétní záležitost napsána analýza mimořádné události, která musí být schválena vedením Informatiky a z pozice zákazníka též vedoucím pracovníkem dané oblasti. Dostupnosti jsou pravidelně doplňovány a vyhodnocovány. Tyto hodnoty jsou poskytovány auditorům pro jejich další práci. Názorná ukázka na obrázku č. 5, kde je patrné, že dostupnost služby ve sledovaném období nikdy neklesla pod hodnotu **99,9 %.**



Obrázek č. 5 – Dostupnost KC[21]

[20] Interní audity Kompetenčních center, interní dokument PRE, a.s.

Poslední součástí chodu KC je statistika požadavků a problémů, které byly zadány ve sledovaném období do aplikace Service Desk. Jedná se o aplikaci, se kterou pracuje především služba Hotline z pohledu zapisovatele požadavků nebo problémů. Záznamy jsou prostřednictvím aplikace předávány příslušným řešitelům, kterým je v ten samý okamžik odesílána e-mailová notifikace s předáním záznamu. Každý záznam v této aplikaci má své jedinečné „Id“ a je tak bez problémů kdykoliv dohledatelný. E-mailovou notifikaci dostává i nahlašovatel záznamu, který má tak prostřednictvím e-mailu či telefonátu přehled o řešení záznamu po celou dobu jeho trvání. V jednotlivých requestech jsou evidovány veškeré činnosti řešitelů, schvalovatelů či operátorů na Hotline. Jelikož jsou všechny záznamy dohledatelné, mají auditoři možnost si některé requesty nechat namátkově zobrazit. Statistiku z aplikace Service Desk pro potřeby interních auditů ukazuje obrázek č. 6.



Obrázek č. 6 – Záznamy ze Service Desku[22]

6.2.2.2 DEPO požadavky

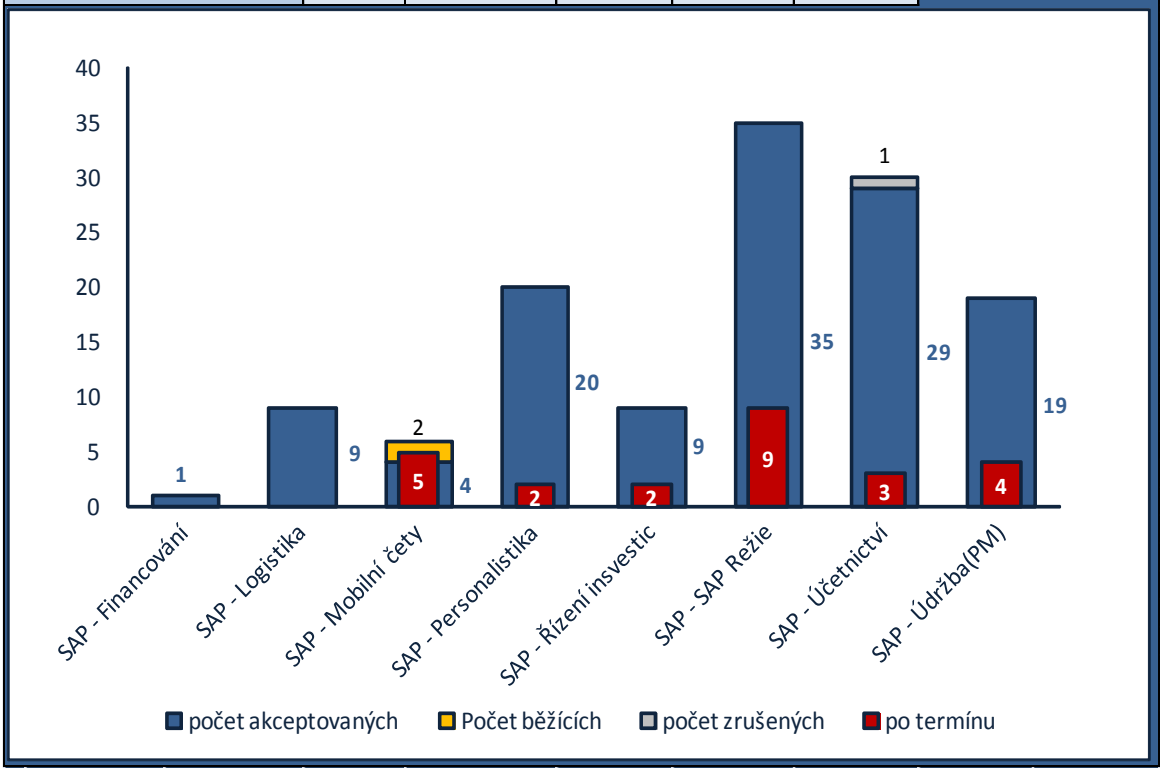
Jedná se o statistiku podnětů zadaných do aplikace DEPO, která slouží k evidenci nápadů, myšlenek a požadavků na rozvoj nějaké konkrétní aplikace nebo služby či HW. Jedná se o aplikaci, která byla naprogramována přímo podle potřeb Informatiky v PRE, a.s. Opět má každý záznam, který je do této aplikace zadaný, svoje vlastní jedinečné „Id“. Součástí aplikace je i schvalovací workflow. Aplikace rovněž poskytuje managementu PRE, a.s. vidět tok peněz na rozvoj jednotlivých oblastí tzv. online. Pro potřeby auditu je vytvářena statistika z této aplikace, která i graficky znázorňuje přehled o jednotlivých požadavcích. Statistika je znázorněna na obrázku č. 7.

[21] Interní audity Kompetenčních center, interní dokument PRE, a.s.

[22] Interní audity Kompetenčních center, interní dokument PRE, a.s.

DEPO Požadavky Sumarizace

	Počet běžících	počet akceptovaných	počet zrušených	Počet celkem	po termínu
SAP - Financování	0	1	0	1	0
SAP - Logistika	0	9	0	9	0
SAP - Mobilní čety	2	4	0	6	5
SAP - Personalistika	0	20	0	20	2
SAP - Řízení insvestic	0	9	0	9	2
SAP - SAP Režie	0	35	0	35	9
SAP - Účetnictví	0	29	1	30	3
SAP - Údržba(PM)	0	19	0	19	4
Celkem	2	126	1	129	25



Obrázek č. 7 – DEPO Požadavky[23]

Poslední oblastí z této části je termínové hodnocení jednotlivých požadavků. Tato statistika sleduje dodržování termínů řešení u jednotlivých požadavků a rozděluje je do skupin:

- po termínu – akceptované,
- po termínu – běžící,
- referuje se MB (MB – manager bezpečnosti),
- priorita kritické.

Auditoři zde mohou vidět jednotlivou prodlevu u záznamů s prošlým termínem. U těchto záznamů musí být uveden důvod zpoždění, který je důležitý zejména proto, že pouhým porovnáním plánovaného termínu dodání a skutečného termínu dodání může docházet ke zkreslování skutečností. Tuto statistiku znázorňuje další obrázek č. 8.

[23] Interní audity Kompetenčních center, interní dokument PRE, a.s.

DEPO požadavky Po termínu - Akceptované					
ID	Název	Datum zadání	Datum akceptace	Zpoždění (dny)	Důvod zpoždění
19310	FLS VISITOUR - doplnění seznamu s informacemi o zakázce v týdenním plánu	21.6.2011	14.8.2012	105	Zpoždění způsobeno dlouhým testováním.
22001	Změnit neodpovídající popisy položek	29.11.2011	10.8.2012	87	Zpoždění způsobeno dlouhým testováním.
25250	Servery pro VisiTour	31.5.2012	28.2.2013	27	Pozdě odklikáno v DEPU. Realizováno před koncem termínu.
22980	Ukládání nahrávek BCM	24.1.2012	17.5.2012	16	Způsobeno řešením hlavního projektu BCM - vyšší priorita.
23962	PS - úprava programu ZPSR_WF_KONTROLA pro posílání zpráv do SAP pošty	15.3.2012	15.5.2012	15	Nedostatečné kapacity pro testování, což protáhlo celou realizaci.
25225	SAP CRM - oprava generování korespondenčních dopisů	29.5.2012	27.8.2012	12	Zpoždění bylo na straně dodavatele – na straně PRE byla zajišťována poze technická podpora.
23770	Úprava programů na unicode (ext)	7.3.2012	9.10.2012	11	Zpoždění bylo způsobeno dořešováním některých chyb po migraci SAP na Unicode ze strany externistů.
25581	Oprava fungování ZCDSAGRBILL	15.6.2012	11.12.2012	11	Souběh s upgr. SAP, nedostatečné kapacity na straně PRE.
25360	TM Kabelové tunely a kabely 110kV	6.6.2012	9.10.2012	9	Zpoždění nastalo ve fázi testování, řešeny záznamy s vyšší prioritou.
27301	PM - promítnutí údajů z VT při změně fixované práce	19.9.2012	7.10.2012	9	Úloha se zdržela ve fázi testování. V té době byl odstaven testovací systém PRQ z důvodů upgrade, systém se přesouval na řadu PRX – PRY. Prodleva způsobena problémy s přístupy.

Obrázek č. 8 – DEPO Požadavky po termínu[24]

V této části se snaží auditoři o ucelení představy o stavu bezpečnosti a kvality pro sledovanou oblast. Otázky se mohou prolínat jednotlivými procesy, protože velmi často dochází k propojování – integraci systémů. Auditoři se mohou zaměřit např. na vedení dokumentace k jednotlivým systémům, či na průběh zálohy dat a její frekvenci. Velmi často se ovšem auditor zajímá o téma vytvoření havarijních plánů, nebo správu uživatelských účtů. Z pohledu bezpečnosti (ale i kvality) je pro auditory důležitá rovněž správa dat, zejména pokud se jedná o systém, který má více prostředí (vývojové, testovací a produktivní). Pro oblast bezpečnost a kvalita máme několik desítek otázek. Na ukázku přikládám část otázek z oblasti bezpečnosti (ISMS) – obrázek č. 9 a z oblasti kvality (QMS) – obrázek č. 10.

P33 Provoz a poskytování aplikačního SW - Seznam otázek ISMS					
Relevantní požadavek ISO 27001		Otázka	Odpověď – poznámka	Hodnocení	
				Stanoveno v ISMS	Prokázáno v praxi
		Byly identifikovány nějaké neshody při posledním interním auditu? Jsou tyto neshody vyřešeny a jak byly řešeny?	Nebyly identifikovány žádné neshody	A	A
A.10.1.1	Dokumentace provozních postupů	Jaká provozní dokumentace existuje a kde je uložena?	Dle normy pro SAP, uložena na OSS, Nová dokumentace k PM a k tiskům	A	A
A.10.5.1	Zálohování informací	Kdy a jak proběhlo zálohování informací?	Zálohování probíhá v rámci zálohování infrastruktury a obnova 1x ročně při kopii systému	A	A
A.10.7.4	Bezpečnost systémové dokumentace	Jak je chráněna systémová dokumentace proti neoprávněnému přístupu?	Na OSS je přístup pouze pro registrované účastníky, řízen i přístup na portál	A	A
A.10.9.3	Veřejně přístupné informace	Jak je zabezpečen přístup do administrace proti zneužití, kdo může získat administrátorská práva a jaké byly v této oblasti provedeny kontroly?	Podle oprávnění, lze získat pouze po souhlasu VO G34 400 a jejich kontrola se provádí v rámci inventury. Proběhl audit Delloite.	A	A
A.11.2.3	Správa uživatelských hesel	Jak často je uživatel povinen měnit heslo?	Každých 180 dnů	A	A

Obrázek č. 9 – Seznam otázek ISMS[25]

[24] Interní audity Kompetenčních center, interní dokument PRE, a.s.

[25] Interní audity Kompetenčních center, interní dokument PRE, a.s.

P33 Provoz a poskytování aplikačního SW - Seznam otázek QMS				
Relevantní požadavek ISO 9001		Otázka	Odpověď – poznámka	Hodnocení
				Stanoveno v QMS / Prokázáno v praxi
		Byly identifikovány nějaké neshody při posledním interním auditu? Jsou tyto neshody vyřešeny a jak byly řešeny?	Nebyly žádné neshody.	
4.1	Všeobecné požadavky	Kde jsou popsány odpovědnosti a činnosti kompetenčních center (KC)?	Dle normy pro SAP, uloženo na OSS	A / A
4.2.1 - 4.2.3	Požadavky na dokumentaci	Jak je tato dokumentace řízená? Pro jaké aplikace jsou definována pravidla pro jejich poskytování, provozování a používání?	Dle normy pro SAP o provozování je popis dohledu (portál), administrační příručky - online na OSS	A / A
4.2.4	Požadavky na dokumentaci	Existují provozní záznamy v tomto KC? Jak jsou řízeny?	Záznamy jsou v SD a řízeny jsou přes DEPO	A / A
5.5.1	Odpovědnost a pravomoc	Kdo odpovídá za provoz, poskytování a využívání jednotlivých aplikací?	Správci dle služeb	A / A
6.3	Infrastruktura	Je infrastruktura pro toto KC dostatečná?	ano	A / A

Obrázek č. 10 – Seznam otázek QMS[26]

Během interních auditů se používá i sumarizační tabulka z Analýzy rizik. Této části bude věnována samostatná následující kapitola. Ukázka této sumarizační tabulky je na následujícím obrázku č. 11.

Oblast/Typ aktiva	Hodnota	Hrozba	Frekvence hrozby	Komentář k hrozbě a frekvenci hrozby	HR 2011	HR 2012	HR 2013	Trvalé opatření	Opatření	Účinnost opatření	Současná hodnota rizik	SR 2011	SR 2012	SR 2013	ID opatření
					27	27	27				5				
SAP - režie															
HW	3	1	1	Nedostupnost služeb, nedodržení zákonné povinnosti	12	12	3	HW, databáze a operační systém je ve správě odd. G 34 300, LogIT, is901	obměna HW	95%	0	A	A	A	
SW	3	3	3	Nutné změny, legislativní požadavky, chyby systému, vypršela podpora části CRM verze 5.0	27	27	27	is920, iis22-1, is940, is941, is 901	DEPO, LogIT, OSS, kompetenční centrum SAP, testovací systémy, plán SP a upgrade, Outsoursing	85%	4	S	A	A	
Lidé	2	2	2	Nemáme plně pokryto vlastními lidmi, není zástupnost	8	8	8		Outsoursing, personální politika	80%	2	A	A	A	
Lokality	0	1	1	provoz pouze v základních lokalitách PRE bez lokálních instalací (mimo Mobilní čety údržby)	0	0	0				0	M	M	M	
Organizace	3	3	3	Velké množství zapojených útvarů a rozhodovacích center	27	27	27	is920, is940, iis22-1, is941, is 901	KC, DEPO, AMU	95%	1	A	A	A	
Projekty	4	4	1	Omezení business aktivit z důvodu velkých systémových změn	16	16	16	is920, iis22-1, is941	Dlouhodobý plán, DEPO, KC	70%	5	A	A	S	u563
Data	3	2	2	Potenciál ztráty či chyby	12	12	12	is920, is940, is923, is 901	Zálohy, oprávnění, monitoring na vyžádání, inventury přístupu k datům, SD, AMU	85%	2	A	A	A	

Obrázek č. 11 – Analýza rizik[27]

6.2.3 Analýza rizik

Jedna z nejdůležitějších metod je vytvoření správné Analýzy rizik. Z této analýzy získáváme rizika, jež by mohla přímo ohrozit činnost organizace. Toto je důvod, proč je

[26] Interní audity Kompetenčních center, interní dokument PRE, a.s.

[27] Analýza rizik IT, interní dokument PRE, a.s.

potřeba je řídit. Analýza rizik se musí provádět v pravidelných intervalech každý rok, je tudíž nezbytné takovou metodiku dobře znát a správně umět používat.

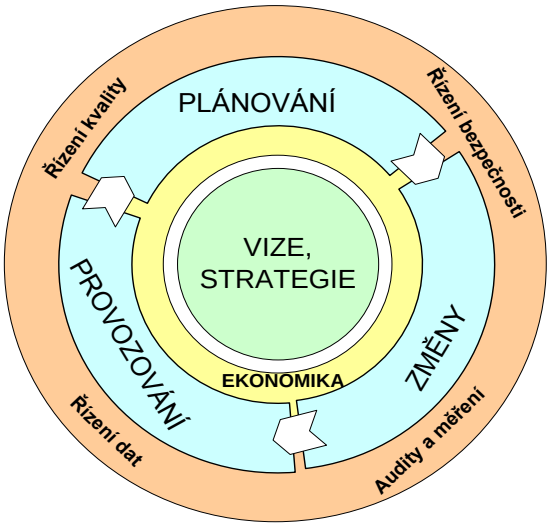
Ve firemním prostředí Skupiny PRE, a.s. se nachází velké množství informačních aktiv vysoké hodnoty. Pro jejich ochranu máme definovanou a implementovanou bezpečnostní politiku. Nástrojem umožňujícím poznat aktuální situaci a potřeby v této oblasti a na jejich základě vytvářet a kontinuálně zlepšovat bezpečnostní opatření je analýza rizik a implementace systému řízení IT rizik – postupy k tomuto bodu jsou podrobněji popsány v samostatné normě Informatiky PRE, a.s. (NorIIS 121 – Řízení rizik IT).

Zavedení relevantních bezpečnostních opatření a kontrola jejich dodržování umožňuje zajištění potřebné úrovně bezpečnosti poskytovaných IT služeb naplňujících potřeby zákazníka a zabezpečení důvěrnosti, dostupnosti a integrity zpracovávaných informací. Nesmíme ale zapomínat, že důležitým opatřením je neustálé a kontinuální zvyšování bezpečnostního povědomí uživatelů IT služeb.

6.2.3.1 Definice aktiv

Nejprve je potřeba specifikovat, co je vlastně aktivum. V PRE, a.s. aktiva znamenají určité prvky systému, které je zapotřebí chránit proti možným rizikům, za použití daných opatření.

Jako základní mapu pro definici aktiv jsme zvolili službu IT, která je základní jednotkou pro řízení ICT činností. Jedná se o ucelenou část ICT, ve které lze a je smysluplné definovat cíl, zákazníky a jednoznačné kompetence. Zajištění chodu a rozvoje služeb a jejich oblastí vyžaduje značné množství dílčích činností, které jsme rozdělili do několika částí (procesů) dle obrázku č. 12.



Obrázek č. 12 – Činnosti služeb IT[28]

Seznam aktiv dle organizace PRE, a.s.

- HW
- SW
- Lidé
- Lokality
- Organizace
- Projekty
- Data

6.2.3.2 Určení hodnoty aktiva

Hodnota aktiva je složena ze zbytkové ceny z částky, kterou by mohla organizace tratit, při případném nesplnění smluvních podmínek apod. Hodnoty aktiv organizace provádí kvalifikovaným odhadem. Jednotlivé hodnoty používané v organizaci uvádí následující Tabulka č. 1.

0	Bez dopadu	----
1	Zanedbatelná	Hodnota do 100 000 Kč
2	Nízká	Hodnota 100 000 – 300 000 Kč
3	Střední	Hodnota 300 000 – 1 000 000 Kč
4	Vysoká	Hodnota 1 000 000 – 10 000 000 Kč
5	Velmi vysoká	Hodnota 10 000 000 Kč a výše

Tabulka č. 1 – Hodnota aktiv[29]

[28] Analýza rizik IT, interní dokument PRE, a.s.

[29] Vlastní zpracování

Abychom se vyhnuli zbytečně složitým „nekonečným“ seznamům aktiv, je nutné jednotlivá drobná aktiva slučovat do větších celků a u těch dbát na snižování rizik.

6.2.3.3 Identifikace hrozeb a zranitelnost

K tomu, abychom mohli odhalit případné hrozby, potřebujeme získat příslušné informace, ty nám mohou poskytnout jednak přímo vlastníci, nebo uživatelé aktiv, dále pak pracovníci personálního oddělení, nebo experti na bezpečnost či plánování.

Určitým zdrojem informací mohou být také externí subjekty, které nám pomohou s identifikací pravděpodobných hrozeb. V současné době společnost PRE, a.s. používá tyto hrozby, jež jsou uvedeny v následující tabulce č. 2.

1	Zanedbatelný
2	Malý
3	Střední
4	Velký
5	Zničující

Tabulka č. 2 – Hodnocení hrozeb[30]

Zranitelnost je v podstatě důsledkem slabých míst v organizaci ať už v oblasti managementu, administrativě, IT prostředků atd. Výskyt zranitelnosti sám o sobě škodu nezpůsobí, tu způsobuje až přítomnost hrozby, která zranitelnosti využije. Z toho důvodu také za přítomnosti zranitelnosti ale bez přítomné hrozby není nutné implementovat ochranná opatření. Zranitelnosti je však nutné monitorovat. Ve společnosti PRE, a.s. zranitelnosti definujeme dle období, kdy mohou nastat – tedy dle frekvence viz tabulka č. 3.

1	Občasná – jednou za více let
2	Nízká – jednou ročně
3	Střední – jednou měsíčně
4	Vysoká – jednou za několik dní
5	Mimořádně vysoká – denně, trvale

Tabulka č. 3 – Frekvence zranitelnosti[31]

6.2.3.4 Odhad rizika

Kombinací jednotlivých vah u kritérií se dosáhne hodnoty hrubého rizika. Jedná se o riziko, u kterého je zapotřebí ještě opatření pro eliminaci rizik.

[30] Vlastní zpracování

[31] Vlastní zpracování

Rizika eliminujeme:

- dlouhodobým trvalým opatřením,
- dočasným úkolem.

Současnou hodnotou rizika rozumíme rizikové číslo snížené v závislosti na aktuální míře účinnosti opatření k eliminaci konkrétního rizika.

Stav	Riziko	Poznámka
K (>31)	Kritické (katastrofální)	Řídí vedení společnosti
R (16-30)	Řízené	Opatření se eviduje v IT Úkolníku, sleduje mng. IT
S (5-15)	Sledované	Opatření se eviduje v IT Úkolníku, sleduje určený vedoucí kompetenčního centra nebo člen 6IIS
A (1-4)	Akceptované	
M (0)	Malé	
Z	Zrušené	

Tabulka č. 4 – Seznam hodnocení rizik[32]

6.2.4 Externí audity ISMS a QMS

Vedení Informatiky PRE, a.s. odsouhlasilo plán konání externích auditů v periodě 1x ročně ISO 27 001 – ISMS a 1x ročně ISO 9001 – QMS.

V této společnosti probíhají 2 typy auditů:

- recertifikační,
- dozorový.

Audity jsou prováděny nezávislými externími auditory ve spolupráci s vedením Informatiky, manažerem bezpečnosti, interními auditory a osobami odpovědnými za auditované oblasti.

Auditování probíhá v jednotlivých procesech, jimiž jsou Strategie a marketing Integrovaného informačního systému (dále jen „IIS“); Systémy řízení IIS; Management zdrojů IIS; Měření, analýza a zlepšování; Obsluha zákazníků; Řízení a realizace/změn projektů; Zajištění infrastruktury ICT; Provoz a poskytování aplikačního SW; Poskytování ostatních služeb IIS.

Auditorům jsou předloženy výsledky interních auditů a kniha Interní audity Kompetenčních center IIS, kterou mají k nahlédnutí po celou dobu průběhu auditu. Je vypracován detailní harmonogram auditů, který odsouhlasí obě zúčastněné strany.

Samotné audity probíhají za účasti dvou až třech externích auditorů, odpovědné osoby za danou oblast ze sekce Informatiky a jednoho až dvou interních auditorů. Auditoři

[32] Analýza rizik IT, interní dokument PRE, a.s.

se dotazují dle typizovaných otázek pro danou oblast. Dle normy ISO 27001 má totiž každá ze sledovaných oblastí za povinnost evidovat všechny potřebné nástroje k zajištění vyšší bezpečnosti informací. Např. provozní deník, plány kontinuity, záloha dat atd. Auditoři zejména požadují dostatek hmatatelných důkazů (např. záznamy v Service Desku, kde si mohou poznamenat unikátní číslo záznamu nebo ID z aplikace LogIT – aplikace na evidenci výpadků a odstávek), které se probírané problematiky dotýkají, či ji dokonce řeší. Auditoři se rovněž zaměřují na úkoly, které vyplynuly z předešlých auditů.

Případné vzniklé neshody jsou zaprotokolovány a jejich kontrola proběhne v následujícím externím auditu. O výsledcích auditu jsou seznámeni všichni účastníci na společném jednání. Informatika dostane o výsledcích auditu protokol a následně i certifikát podepsaný externími auditory. V současné době je Informatika PRE, a.s. certifikována na ISO 27001 – ISMS a ISO 9001 – QMS. Nyní management Informatiky uvažuje o zavedení certifikace na ISO 20000.

6.2.5 Roční zpráva

Jedná se o shrnutí daného roku po jednotlivých odděleních sekce Informatika. Dokument obsahuje manažerské shrnutí roku i plán na následující období. Rovněž je zde uváděna roční statistika jednotlivých částí Informatiky, která se během roku dodává po jednotlivých měsících. Statistika obsahuje např. grafický výstup počtu záznamů v aplikaci Servicedesk (požadavky uživatelů, ale i problém, incidenty a reklamace), počty realizovaných projektů v oblasti informatických služeb, počty výběrových řízení, které Informatika za uvedený rok vypisovala.

Zpráva obsahuje i možné bezpečnostní problémy, které byly objeveny při auditech, penetračních testech apod. Dokument je pak schválen manažerem IT a předložen vedení PRE, a.s.

6.2.6 Analýza mimořádné události

Analýza mimořádné události (dále jen „AMU“) je dokument, který sbírá podklady o mimořádné události (výpadku, špatné časové dostupnosti aplikace) v provozu IT, resp. poskytovaných službách Informatiky. Jde o nezávislou analýzu a zhodnocení příčin, průběhu odstraňování a přijetí opatření k minimalizaci dopadů a opakování obdobné události. O tuto analýzu může požádat kterýkoliv zaměstnance PRE, a.s. V tomto dokumentu jsou Normou (NorIIS 144 – Analýza mimořádných událostí, je přílohou č. 2 této práce, s jejím zveřejněním souhlasilo vedení Informatiky PRE, a.s.) striktně definovány odpovědnosti.

Odpovědnosti:

- Vedoucí IT – vydává pokyn ke zpracování AMU, schvaluje zejména navržená opatření, má právo kdykoli na základě nových skutečností nebo opakujících se problémů stejného charakteru, změnit hodnocení příčin v jednotlivých oblastech, a to i zpětně.
- Zpracovatel AMU – analytik pověřený zpracováním dané AMU, sbírá podklady, analyzuje, navrhuje hodnocení a opatření, včetně osob odpovědných za jejich realizaci a termín realizace, zajišťuje evidenci a uložení schválení AMU.
- Kontrolor – člen vedení IT, který je zpravidla nadřízeným určeného řešitele, zajišťuje informování ostatních členů vedení Informatiky.
- Řešitel – osoba odpovědná za provedení opatření.

6.3 Hodnocení nástrojů a bezpečnosti Informatiky

Cílem této kapitoly je krátké shrnutí osobních názorů na používané nástroje ve společnosti PRE, a.s. z pohledu interního auditora pro oblast ISMS a QMS. Pro vedení Informatiky má eminentní přínos dlouhodobé sledování odchylek opatření na určitá rizika. Podklady pro hodnocení bezpečnosti získáváme z dílčích anomálií. Hodnocení bezpečnosti probíhá dvakrát do roka v podobě Analýzy rizik a Zprávě o bezpečnosti. Oba dokumenty pak představitelé Informatiky poskytují vrcholovému vedení PRE, a.s. Pro přehlednější zhodnocení bezpečnosti Informatiky ve skupině PRE, a.s. jsem se rozhodl použít jednoduchou metodu komparace kladů a záporů, jak uvádím níže.

6.3.1 Interní a externí audity

Důležitost a význam pravidelného provádění jak interních, tak i externích auditů je naprosto nezpochybnitelná.

6.3.1.1 Klady

+ Pomáhají odhalovat eventuální nedostatky, které by mohly do budoucna ohrozit správný chod organizace.
+ K odstranění nedostatků dochází podstatně rychleji.
+ Rychlejší odhalení zranitelností při běžném provozu generuje ušetřené náklady.
+ Rychlým a včasným odstraněním nedostatků se minimalizují škody (ztráta zákazníků atd.).
+ Certifikací se zvyšuje prestiž značky Pražská energetika, a.s. na trhu.

+ Při provádění interních auditů se zapojují zaměstnanci napříč sekcí Informatika, což pomáhá zvýšit jejich znalosti.

6.3.1.2 Zápory

- Zvýšení nákladů (např. tisk knihy, náklady na certifikaci).
- Časová náročnost (jak na interní auditory, tak na zaměstnance).
- Narůstající požadavky na evidenci, která ne vždy může být elektronická.

6.3.2 Analýza rizik IT

Analýzou rizik zjišťujeme, k čemu všemu může v organizaci dojít, důvod proč k tomu může dojít, jakým způsobem a kde k tomu může dojít a koho se to bude týkat. Analýza rizik nám pomůže odhalit hrozby, kterým je společnost vystavena a zranitelnost aktiv. Touto analýzou zjistíme také výši pravděpodobnosti a dopad na společnost v případě, že zmíněná hrozba určitou zranitelnost zneužije.

6.3.2.1 Klady

+ V rámci společnosti PRE, a.s. pomáhá Analýza rizik zvýšit prestiž a zdůraznit důležitost práce Informatiky.
+ Zaměstnanci si uvědomí význam a důležitost služby v případě jejího výpadku.
+ Dochází k eskalaci problémových záležitostí managementu PRE, a.s., což vyvolá řídící dohled kompetentní osobou.

6.3.2.2 Zápory

- Časová náročnost na vytvoření podkladů a tvorbu analýzy.

6.4 Osobní zkušenosti s užívanými nástroji

Během mého působení ve společnosti PRE, a.s. jsem se setkal s praktickým používáním všech mnou uvedených nástrojů. Osobně mám největší praktické zkušenosti s Analýzou rizik, Interními a Externími audity a Zprávou o bezpečnosti IT.

V počátcích tvorby Analýzy rizik jsme se museli vyrovnat s problémy definování jednotlivých aktiv a zároveň s vysvětlením těchto aktiv zainteresovaným osobám. Tyto problémy představovaly při tvorbě enormní časovou náročnost na vytvoření celistvého dokumentu. Postupně ovšem přešla tvorba Analýzy rizik do rutiny. Je to jedna z nejlepších zpětných vazeb pro vedení Informatiky. Její platnost v oblasti hodnocení bezpečnosti je zejména v tom, že se jedná o dlouhodobé sledování oblastí. Správné hodnocení bezpečnosti rovněž probíhá dlouhodobě.

Interní a externí audity se ve společnosti PRE, a.s. dělají jeden krát za rok. Nejprve provádíme s vedoucími KC interní audity, kde se pomocí cílených dotazů zaměřujeme na určité části oblasti bezpečnosti. Výsledky interních auditů následně konzultujeme s vedením Informatiky, které přijímá opatření na vzniklá/odhalená rizika. Tyto výstupy poté slouží jako podklad pro nezávislé externí auditory. Externí audity probíhají v letních měsících po dobu tří dnů. Informatika PRE, a.s. je v současnosti certifikována na ISO 27001 a ISO 9001. Certifikáty mají vždy omezenou dobu platnosti na 12 měsíců.

Zpráva o bezpečnosti Informatiky je dokument, který vytváří tým auditorů, pod vedením manažera bezpečnosti, pro manažera Informatiky. Tento dokument následně manažer IT předkládá ke schválení vrcholovému vedení PRE, a.s. Zpráva obsahuje celkové zhodnocení po jednotlivých oblastech, vize a dlouhodobé cíle, preventivní opatření, rutinní opatření při vzniku incidentu. Používaná metodika je znázorněna v tabulce v Příloze.

6.5 Návrhy na zlepšení

Hlavním návrhem na zlepšení je zapracování změn spojených s aktualizací normy ISO/IEC 27001:2013. Momentálně ještě nebyla vydána verze s českým překladem. Následná implementace by měla proběhnout co nejdříve. Nová norma klade vyšší důraz na vyhodnocení toho, jak dobře společnost ISMS provádí. Celkově je tato norma navržena tak, aby lépe spolupracovala s normami ISO 9001 a ISO 20000.

Dalším podnětem ke zlepšení je rozvoj bezpečnostního monitoringu HP ArcSight (SIEM), který má na starosti monitoring činnosti uživatele na všech účtech (i administrátorských), aplikacích a systémech. Obohacuje protokol událostí a poskytuje informace, které dávají ucelený obraz o činnosti uživatelů. Výsledkem je nižší vnitřní hrozba a lepší řízení přístupů.

Posledním návrhem je doporučení, aby se společnost vyvarovala přehnané integraci a propojení některých systémů PRE, a.s. což může mít za následek při eventuálním výpadku či nedostupnosti některého ze systémů mnohem vyšší dopady na některé části skupiny PRE, a.s. Vzhledem k tomu bych doporučil při implementaci dalších systémů neintegrovat je do systémů stávajících.

7 Závěr a vyhodnocení

Hlavním cílem této bakalářské práce bylo zhodnocení bezpečnosti Informatiky ve společnosti Pražská energetika, a.s. Práce má dvě části (teoretickou a praktickou). V teoretické části uvádím základní nástroje pro zajištění vyšší bezpečnosti v Informatice. Tento oddíl popisuji z důvodu lepšího pochopení praktické části bakalářské práce.

V druhé – praktické části se věnuji popisu a zhodnocení bezpečnosti Informatiky ve společnosti PRE, a.s. Definuji zde metodiky používané v této organizaci a následně je rovněž stručně hodnotím. Pro vedení Informatiky má eminentní přínos dlouhodobé sledování odchylek opatření na určitá rizika. Podklady pro hodnocení bezpečnosti poté získáváme z dílčích anomálií. Hodnocení bezpečnosti probíhá dvakrát do roka v podobě Analýzy rizik a Zprávy o bezpečnosti. Oba dokumenty pak představitelé Informatiky poskytují vrcholovému vedení PRE, a.s. Celkově je bezpečnost Informatiky v této společnosti na velmi vysoké úrovni i z toho důvodu, že PRE, a.s. úspěšně implementovala do provozu normu ISO/IEC 27001:2005 – Systém managementu bezpečnosti informací. Společnost se snaží maximálně využívat veškeré nástroje této normy. Přínosem je i používání metody Analýza rizik, která pomáhá odhalit managementu PRE, a.s. případné hrozby a rizika z toho plynoucí. Ve zhodnocení uvádím některé postřehy a podněty, které jsem v této oblasti získal.

Vedení Informatiky a ostatní vedoucí pracovníci jsou si plně vědomi, že jedním ze základních předpokladů pro prosperitu Informatiky a Pražské energetiky, a.s. je funkční a efektivní ISMS a jeho neustálé zlepšování.

Proto v tomto směru trvale působí na:

a) Zdokonalování mechanismů umožňujících neustálé zlepšování ISMS:
    a. řízením procesu,
    b. řízením politiky a cílů bezpečnosti,
    c. vnitřní komunikací,
    d. přezkoumáním ISMS,
    e. analýzou údajů,
    f. realizací zlepšování,
    g. nápravnými opatřeními,
    h. preventivními opařeními.

b) Podřízené zaměstnance:
    a. zvyšováním povědomí o důležitosti bezpečnosti informací,
    b. motivací a zapojením zaměstnanců Informatiky v rámci závazku vedení,
    c. seznamováním zaměstnanců s politikou bezpečnosti, návaznými cíli, opatřeními a úkoly,
    d. formou komunikace vedoucích pracovníků se zaměstnanci.

Hodnocení bezpečnosti ovlivňuje ve velké míře vývoj kultury podniku. Můžeme mít sebelepší normy a předpisy na zvýšení bezpečnosti, ale pokud v podniku bude fungovat špatně zaměstnanecká kultura, tak nám zaměstnanci bezpečnostní předpisy dodržovat nebudou. Správnému vývoji kultury můžeme pomoci používáním měkkých (např. motivaci) a tvrdých (např. měřitelné, tj. audity) řídících nástrojů. Ve společnosti PRE, a.s. je firemní kultura na vysoké úrovni a zaměstnanci dodržují nařízení a normy, které Informatika k zabezpečení informací a dat potřebuje.

Základním návrhem na zlepšení je zapracování změn, které vznikly aktualizací normy ISO/IEC 27001:2013. Aktualizovaná verze normy klade vyšší důraz na hodnocení správného používání ISMS společností. Dalším podnětem ke zlepšení je rozvoj SIEM, který má na starosti monitoring činnosti uživatele. Tento prostředek by společnosti PRE, a.s. poskytoval důležité informace o činnosti uživatelů. Na závěr doporučuji, důkladné sledování problematiky a vývoje Zákona o kybernetické bezpečnosti. Tento zákon ještě není v platnosti (očekávaná účinnost od 1. 1. 2015), proto není v této práci podrobněji popsán. Vzhledem k jeho rozsáhlé působnosti v oblasti bezpečnosti informatických dat jej ale není možné opomenout.

8 Anotace

Příjmení a jméno autora:	Šimon Fanta
Instituce:	Moravská vysoká škola Olomouc
Název práce v českém jazyce:	Hodnocení bezpečnosti v podnikové informatice
Název práce v anglickém jazyce:	The Security Assessment in Business Informatics
Vedoucí práce:	Mgr. Zdeňka Krišová
Počet stran:	51
Počet příloh:	2
Rok obhajoby:	2014
Klíčová slova v českém jazyce:	bezpečnost informací, systém řízení bezpečnosti informací, riziko, opatření, ISO/IEC 27001, PDCA cyklus, Kompetenční centrum
Klíčová slova v anglickém jazyce:	Information security, information security framework, risk, measures, ISO/IEC 27001, PDCA cycle, expert group

Obsahem této bakalářská práce je zhodnocení zajištění bezpečnosti informací v konkrétní organizaci. Práci jsem rozdělil na dvě části. V první části jsou rozebrány dostupné legislativní prostředky (norma ISO/IEC 27001:2005 a zákony České republiky). Druhá část obsahuje konkrétní metodiky ve společnosti Pražská energetika, a.s., jež jsou používány k zabezpečení informací.

Cílem této práce je analýza dostupných informací o zabezpečení dat, zhodnocení současného stavu zavedených bezpečnostních opatření ve společnosti Pražská energetika, a.s. a návrh na jejich zlepšení.

The content of this thesis provides a thorough analysis of information security framework in a given company. The thesis is divided into two parts. The first entails the description of the legislative framework (norm ISO/IEC 27001:2005 and laws of the Czech republic). The second one portrays the concrete measures utilized to secure information at Pražská energetika, a.s.

The aim of the thesis is to gather the analysis information regarding information security. Another aim is the evaluation of the current security measures in effect at Pražská energetika, a.s. and a subsequent summary. The contribution of this thesis should be the creation of a summary describing the security measures at the respective company and presentation of proposed remedies.

9 Literatura a prameny

GÁLA, L., POUR, J., ŠEDIVÁ, Z. *Podniková informatika*, Praha: Grada, 2009. 585 s. ISBN 978-80-247-2615-1

PRAŽSKÁ ENERGETIKA, a.s. *Analýza rizik IT*. Praha, 2013.

PRAŽSKÁ ENERGETIKA, a.s. *Roční zpráva 2012/2013*. Praha, 2013

PRAŽSKÁ ENERGETIKA, a.s. *Zpráva o bezpečnosti IT*. Praha, 2013

ČESKÝ NORMALIZAČNÍ INSTITUT. *Informační technologie - Bezpečnostní techniky – Systémy managementu bezpečnosti informací - Požadavky*. Praha, 2006

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů

DOUCEK, P., NOVÁK, L., SVATÁ, V.: *Řízení bezpečnosti informací*, Professional publishing, 2008, ISBN 978-80-86946-88-7

SMEJKAL, V., RAIS, K.: *Řízení rizik ve firmách a jiných organizacích*, Praha: Grada, 2010, ISBN 978-80-247-3051-6

10 Internetové zdroje

Wikipedie – Infromace [online]. 2014 [cit. 2014-01-18] Dostupné z: http://cs.wikipedia.org/wiki/Informace

Ministerstvo vnitra České republiky – Bezpečnost [online]. 2010. [cit. 2014-01-18] Dostupné z: http://www.mvcr.cz/clanek/pojmy-bezpecnost.aspx

ITIL – Bezpečnost informací [online]. 2013. [cit. 2014-01-18] Dostupné z: http://www.itil.cz/index.php?id=933

AEC – Bezpečnostní politika organizace [online]. 18. 1. 2014. [cit. 2014-01-18] Dostupné z: http://www.aec.cz/cz/sluzby/bezpecnostni-politika-organizace

ČSN ISO/IEC 27001:2005 – Informační technologie – Směrnice managementu řízení bezpečnosti informací – Požadavky [online]. 2006. [cit. 2014-01-18] Dostupné z: http://csnonlinefirmy.unmz.cz/html_nahledy/36/76533/76533_nahled.htm

Risk Analysis Consultants [online]. 2014. [cit. 2014-01-18] Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/ISMS

ČSN ISO/IEC TR 13335:1998 – Informační technologie – Směrnice pro řízení bezpečnosti IT – všechny části [online]. 2000. [cit. 2014-01-18] Dostupné z: http://csnonlinefirmy.unmz.cz/html_nahledy/36/58372/58372_nahled.htm

Národní bezpečnostní úřad - Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů [online]. 2005. [cit. 2014-01-18] Dostupné z: http://www.nbu.cz/cs/pravni-predpisy/zakon-c-4122005/

Ochrana osobních údajů - Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů [online]. c 2008. [cit. 2014-01-18] Dostupné z: http://www.oou.cz/index.php?file=personal_data_protection_zakon_101

Český normalizační institut – Český normalizační institut [online]. 24. 2. 2012. [cit. 2014-01-18] Dostupné z: http://csni.cz/

Úřad pro technickou normalizaci, metrologii a státní zkušebnictví – O úřadu [online]. 2013. [2014-01-18] Dostupné z: http://www.unmz.cz/urad/o-uradu

Wikipedie - Mezinárodní organizace pro normalizaci [online]. 7. 3. 2013. [cit. 2014-01-18] Dostupné z: http://cs.wikipedia.org/wiki/Mezin%C3%A1rodn%C3%AD_organizace_pro_normalizaci

Risk Analysis Consultants [online]. 2014. [cit. 2014-01-18] Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/371FBFBC600C1713C125773B00380DE8?OpenDocument

Pražská energetika, a.s. – Výroční zprávy [online]. 10. 5. 2013. [cit. 2014-01-19] Dostupné z: http://www.pre.cz/pre/nase-spolecnost/vice-o-pre/vyrocni-zpravy.html

11 Seznam zkratek

KC – Kompetenční centrum

PRE, a.s. – Pražská energetika, a.s.

AMU – Analýza mimořádné události

ISMS – Systém managementu bezpečnosti informací

QMS – Systém kvality služeb

ČNI – Český normalizační institut

NBÚ – Národní bezpečnostní úřad

ÚNMZ – Úřad pro technickou normalizaci, metrologii a státní zkušebnictví

SIEM – Bezpečnostní monitoring HP ArcSight

12 Seznam obrázků

13 Seznam tabulek

14 Seznam příloh

Příloha č. 1 – Metodika hodnocení bezpečnosti v PRE, a.s. – Zdroj: Zpráva o bezpečnosti IT, interní dokument PRE, a.s.

Příloha č. 2 – Analýza mimořádné události – Zdroj: Analýza mimořádných událostí, Norma PRE, a.s.

Příloha č. 1 – Metodika hodnocení bezpečnosti v PRE, a.s.

Hodnota	Stav oblasti	Opatření, hodnocení
0 - 20%	KRIZE - skutečný stav je velmi vzdálen od cílového stavu. V oblasti se vyskytl bezpečnostní problém, které by mohlo vážně ohrozit chod celé společnosti, nebo způsobit ztrátu dobrého jména společnosti	Ihned aplikovat krizové řízení pro neprodlené zajištění realizace nápravných opatření jsou projednávána vedením společnosti
21 - 40%	V oblasti nastal bezpečnostní problém, který narušil, nebo by mohl vážně narušit chod společnosti	Důležitá opatření, která vyžadují zásadní změny v chodu i nad rámec IIS případně velké finanční prostředky. Opatření řídí vedení Informatiky, je informován ředitel.
41 - 60%	V oblasti se vyskytl bezpečnostní podnět, jehož řešení naní možné řešit v rámci pracovního pořádku.	Opatření a rozhodnutí, která přesahují kompetence jednotlivých specialistů, rozhoduje se o nich na schůzi vedení Informatiky a jsou sledována v ročním hodnocení.
61 - 80%	V dané oblasti byly identifikovány problémy spojené s běžným chodem IT a jejich řešení je součástí rutinních činností skupiny či jednotlivce	Opatření typicky na úrovni lokální optimalizace nebo zlepšování na úrovni jednotlivců či menších týmů, charakter spíše preventivních opatření.
81 - 100%	V dané oblasti se nevyskytl žádný bezpečnostní problém, nenastal žádný bezpečnostní incident, ani slabina, která by představovala bezpečnostní problém, ani tento problém není očekáván.	Náměty na zlepšování, dominance preventivních opatření

Příloha č. 2 – Norma IIS č. 144 – Analýza mimořádných událostí

Zde uvádím jednotlivé části normy z interního dokumentu PRE, a.s. se souhlasem vedení Informatiky.

A. ÚVODNÍ A OBECNÁ USTANOVENÍ

A.1 Účel a cíl normy IIS

Definovat postup při analýze mimořádných událostí (dále jen „AMU“), včetně metodiky evidence a kontroly opatření vzniklých z AMU.

A.2 Související předpisy a řídicí dokumenty

Označení	*Název předpisu*
NorIIS 101	Příručka kvality IIS
NorIIS 102	Příručka bezpečnosti IIS
NorIIS 103	Dokumenty a záznamy v systémech řízení IIS
NorIIS 141	Řízení neshody a následných opatření

A.3 Klíčová slova

analýza, mimořádná událost, operativní zásah, nápravné opatření, preventivní opatření

A.4 Obsah

A.5 Seznam samostatných příloh

Číslo SP	*Název přílohy*	*Odkaz (soubor)*
1.	Šablona „Analýza mimořádné události“	PORTÁL/IIS/ISO/Šablony/AMU

B. Znění normy IIS

Výklad pojmů a zkratek

Pojem	*Význam*
Analýza mimořádné události	Sběr podkladů o mimořádné události v provozu IS/ICT, resp. poskytovaných službách IIS, nezávislá analýza a zhodnocení příčin, průběhu odstraňování apod. a přijetí opatření k minimalizaci dopadů a opakování obdobné události.

Zkratka	*Význam*
AMU	Analýza mimořádné události
NO	Nápravné opatření
OZ	Operativní zásah
PO	Preventivní opatření

Odpovědnosti v oblasti AMU

O provedení AMU může požádat na Hotline IIS kterýkoliv zaměstnanec PRE.

Vedoucí IIS

Vydává pokyn ke zpracování AMU (schvaluje/zamítá žádost o zpracování AMU).

Schvaluje první část AMU, zejména návrh opatření.

Má právo kdykoli na základě nových skutečností nebo opakujících se problémů stejného charakteru, změnit hodnocení příčin v jednotlivých oblastech a to i zpětně.

Zpracovatel AMU

Zaměstnanec G 34 100 pověřený vedoucím tohoto oddělení zpracováním určené AMU.

Sbírá podklady, analyzuje je, navrhuje hodnocení a opatření, včetně osob odpovědných za jejich realizaci a termín realizace.

Zajišťuje evidenci a uložení schválené AMU na určeném místě.

Kontrolor

Člen 6IIS, který u konkrétního schváleného opatření zajistí informování zbytku 6IIS o provedení opatření; standardně se jedná o nadřízeného řešitele.

Kontrolor může ověřením provedení opatření pověřit jinou osobu nebo s řešitelem komunikovat sám.

Řešitel

Osoba odpovědná za provedení opatření.

Struktura AMU

První část – Rozbor mimořádné události

Slouží jako finální závěry provedené AMU, stručné zhodnocení příčin a průběhu odstraňování události a především soupis přijatých opatření. Zpravidla by neměla překročit dvě strany.

Schválením vedoucím IIS se dosud nerealizovaná opatření stávají závaznými a zařadí se do evidence opatření dle kapitoly 0.

Položky první části

Popis	Stručná charakteristika problému.
Časový průběh	Časové aspekty vzniku a řešení mimořádné události (výběr)
Rozsah a dopady	Stručná charakteristika, například velikost poruchy, počet postižených uživatelů, finanční hledisko, pracnost, …)
Stručné hodnocení	Stručné zhodnocení a komentáře k příčinám vzniku mimořádné události a průběhu jejího odstraňování v jednotlivých kategoriích. Bodování (barvičky) slouží nejen k přehlednému zhodnocení „příspěvku“ jednotlivých aspektů ke vzniku či minimalizaci mimořádné události, ale též jako vodítko pro zlepšování a opatření v jednotlivých oblastech.
Příčiny	Stručný soupis hlavních příčin vzniku mimořádné události
Opatření	Soupis realizovaných a naplánovaných opatření k likvidaci příčiny, následků a prevenci mimořádné události (výběr).

Struktura tabulky pro hodnocení příčin a průběhu odstraňování:

Provoz (příčina)	**Technologie – HW**		Hodnota, včetně barvy
	Technologický SW (OS, DB, linky, …)		- „ -
	Aplikační SW		- „ -
	Celková architektura		- „ -
	Organizace práce		- „ -
	Zpracovatelé		- „ -
Havárie	**Organizace odstraňování**		- „ -
	Řešitelé		- „ -

V rámci tabulky se hodnotí na stupnici od 0 (nejhorší) do 9 (nejlepší) s touto interpretací a dopady:

0	kritické – černá	Aplikuje se krizové řízení pro neprodlené zajištění realizace nápravných opatření. Zásadní opatření jsou projednávána vedením společnosti.
1-3	závažné - červená	Stanovení opatření a jejich realizaci kontroluje vedoucí sekce IIS, řešení v rámci DEPO, nebo sledovaným úkolem v IT Úkolníku stanoveným vedoucím sekce IIS na prověření odstranění nedostatku.
4-6	rizikové - žlutá	Správce dotčené oblasti je povinen doložit opravu nedostatku formou DEPO požadavku nebo sledovaným úkolem v IT Úkolníku.
7-9	dobré - zelené	K oblasti není vážná výhrada, u hodnoty 7 se našla dílčí nesrovnalost (opatření se doporučuje zvážit).

Struktura tabulky opatření:

Operativní zásah (OZ)	Okamžitá opatření.
Nápravné opatření (NO)	Řešení problémů a odstraňování následků.
Preventivní opatření (PO)	Opatření k zamezení obdobných problémů v budoucnosti.
Další náměty a upozornění	Další zjištění či náměty zjištěné při analýze mimořádné události, které nebyly (zatím) uloženy jako konkrétní opatření.

Druhá část – Přílohy

Volitelně se dle charakteru mimořádné události doplňují další kapitoly, resp. přílohy s názory jednotlivých účastníků, skupin nebo názory nezávislých stran, důkazy o průběhu a řešení události, jejich dopadech a již realizovaných opatřeních.

Pojmenování souboru

AMU_RRRR(rok)-NNN(poř. číslo)_stručný název mim. události_RRRR-MM-DD(datum události).doc

Např. *AMU_2005-001_síť_2010-09-15.doc*

AMU_2005-002_platby_2010-09-15.doc

Metodika evidence a kontroly opatření vzniklých z AMU

Cílem evidence a kontroly nápravných a preventivních opatření (dále opatření) navržených a schválených v rámci analýz mimořádných událostí je zajistit, aby byla tato opatření skutečně realizována.

Postup

Zpracovatel AMU ve spolupráci s dotčenými osobami navrhne opatření včetně termínů realizace a řešitelů.

6IIS v rámci připomínkování AMU navržená opatření vč. řešitelů a termínů potvrdí, případně upraví. AMU s konečnou platností schválí vedoucí sekce IIS.

Přijatá opatření jsou zanášena do Tabulky opatření.

Každé opatření je zavedeno do aplikace IT Úkolník. Zadavatelem je 6IIS a opatření je označeno unikátním číslem úkolu, pod kterým je následně evidováno a monitorováno.

K jednotlivým opatřením je určen kontrolor. Kontrolor zajistí:

informování řešitele o povinnosti dané opatření realizovat;

komunikaci s řešitelem o stavu řešení problému (může být realizováno přes prostředníka, viz výše);

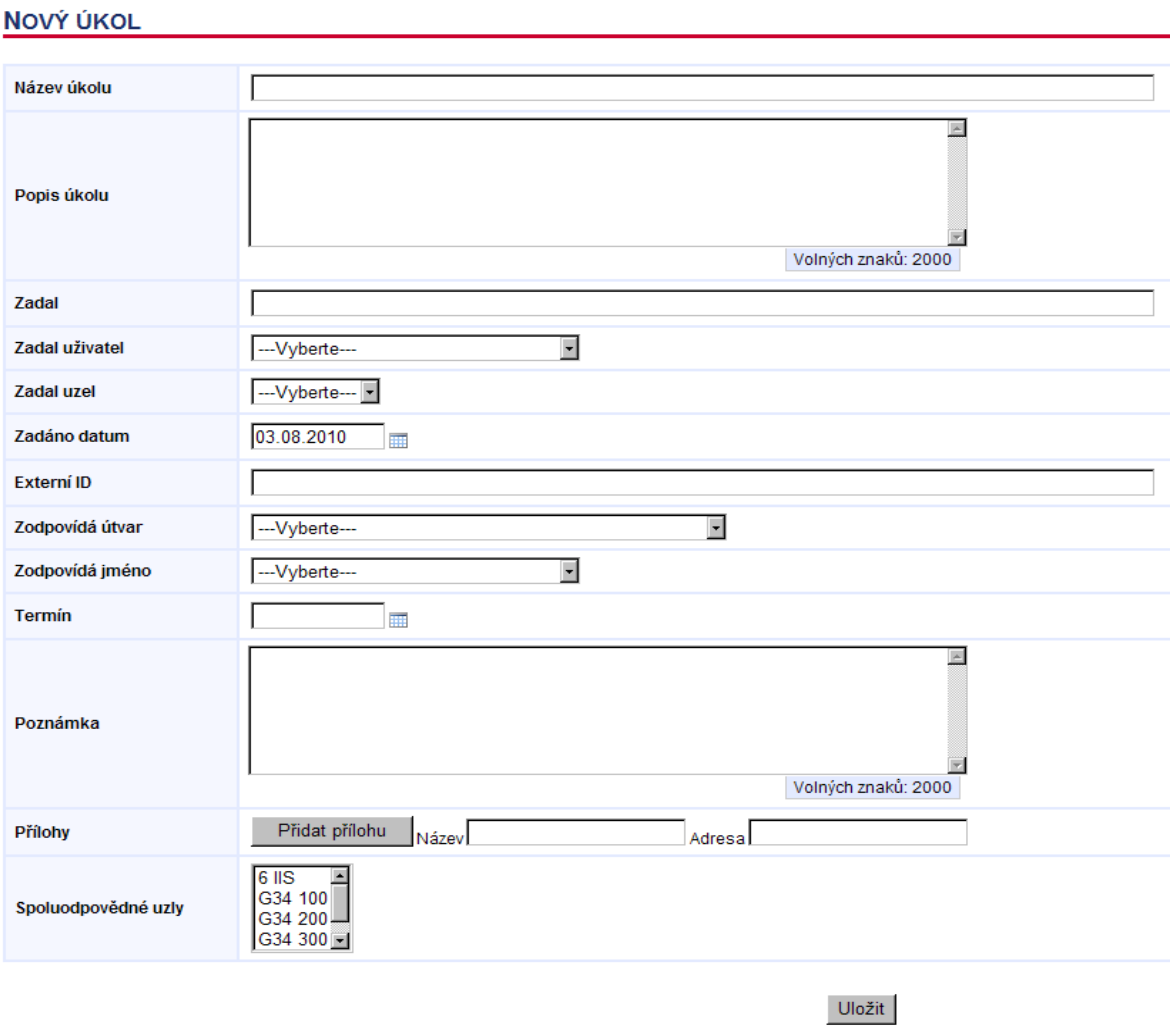
informování 6IIS o provedení či neprovedení daného opatření, nejlépe v rámci pravidelných týdenních porad;

sjednání nápravy v případě neprovedení daného opatření.

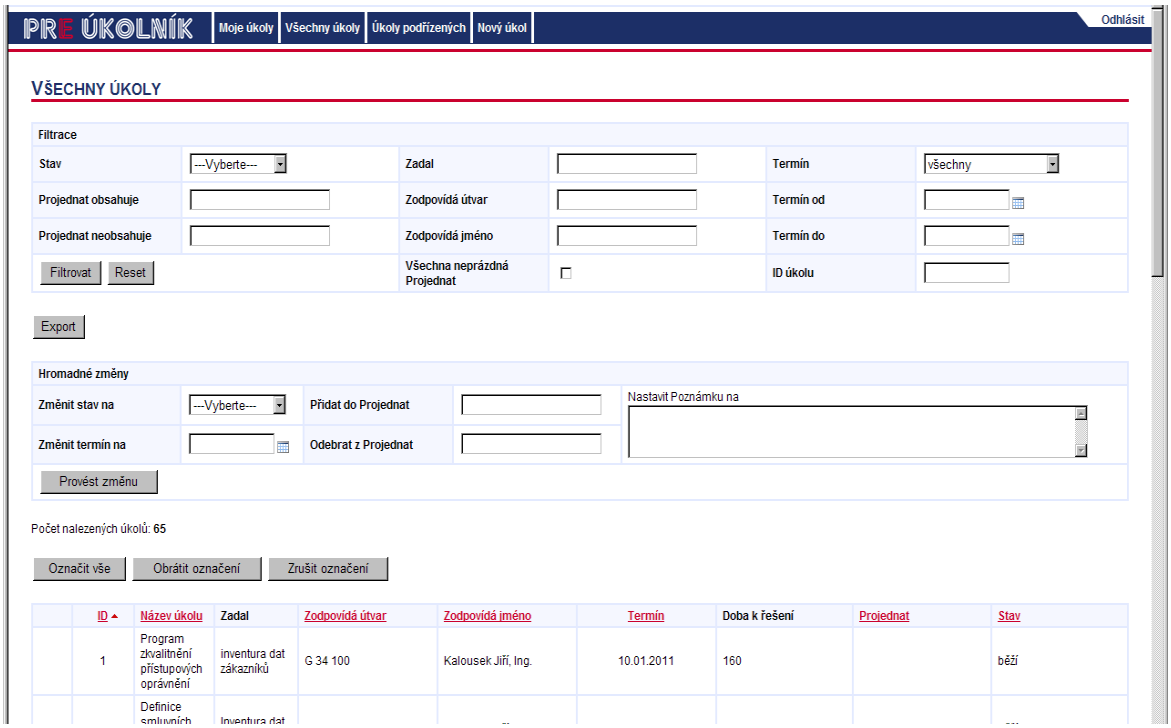
Pokud nastane situace, kdy se původně navržené a schválené opatření ukáže jako nevhodné či nerealizovatelné v daném termínu, je možné v rámci 6IIS schválit jeho změnu či zrušení. Takový návrh obvykle podává rovněž kontrolor.

Aplikace IT Úkolník

Zadání opatření do aplikace



Zobrazení úkolů



KONEC NORMY IIS