
# VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

## FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

## ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS


# NÁVRH ZAVEDENÍ ITSM S VYUŽITÍM RÁMCE ITIL SE ZAMĚŘENÍM NA BEZPEČNOST

DIPLOMOVÁ PRÁCE
MASTER'S THESIS


AUTOR PRÁCE
AUTHOR
Bc. Dominik Antalík

VEDOUCÍ PRÁCE
SUPERVISOR
Ing. Petr Sedlák


BRNO 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

# Zadání diplomové práce

| | |
|---|---|
| Ústav: | Ústav informatiky |
| Student: | **Bc. Dominik Antalík** |
| Studijní program: | Systémové inženýrství a informatika |
| Studijní obor: | Informační management |
| Vedoucí práce: | **Ing. Petr Sedlák** |
| Akademický rok: | 2017/18 |

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

## Návrh zavedení ITSM s využitím rámce ITIL se zaměřením na bezpečnost

**Charakteristika problematiky úkolu:**

Úvod
Vymezení problému a cíle práce
Teoretická východiska
Analýza současného stavu
Vlastní návrh řešení
Zhodnocení a přínosy práce
Závěr
Seznam použité literatury
Přílohy

**Cíle, kterých má být dosaženo:**

Optimalizované řízení služeb informačních technologií na základě normy ČSN ISO/IEC 20000 – Informační technologie – Management služeb (ITSM).
Přijetí a přizpůsobení rámce ITIL (IT Infrastructure Library), který napomáhá zvládnout IT v organizaci, pojednává komplexně o službách a zaměřuje se na neustálé měření a zlepšovaní kvality poskytovaných služeb IT.
Sladění ITSM s funkčním systémem řízení bezpečnosti informací (ISMS) dle normy ČSN ISO/IEC 27013:2015 – Pokyn pro integrovanou implementaci ISO/IEC 27001 a ISO/IEC 20000–1.

**Základní literární prameny:**

BUCKSTEEG, Martin. ITIL 2011. Brno: Computer Press, 2012. ISBN 978-80-2513-732-1.

ČSN ISO/IEC 27001. Informační technologie - Bezpečnostní techniky - Systém managementu bezpečnosti informací - Požadavky. Praha: Český normalizační institut, 2014.

ISO/IEC 27013. Information technology - Security techniques - Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1. Geneva: ISO Office, 2015.

ITIL – výkladový slovník a zkratky v češtině, v1.1, 6. ledna 2012. ITIL [online]. [cit. 2018-02-21]. Dostupné z:

https://itsmf.cz/wp-content/uploads/2017/08/itil_2011_czech_glossary_v2.0.pdf

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2017/18

V Brně dne 28.2.2018

L. S.

| | |
|---|---|
| doc. RNDr. Bedřich Půža, CSc.<br>ředitel | doc. Ing. et Ing. Stanislav Škapa, Ph.D.<br>děkan |

## Abstrakt

Diplomová práca sa zaoberá návrhom pre zlepšenie kvality poskytovaných služieb IT a ich optimalizáciou v záujme podniku a jeho obchodných cieľov. Pre potreby užívateľsky prívetivého poskytovania služieb IT s optimalizovanými nákladmi musia byť procesy, funkcie, role pracovníkov a technológii zosúladené tak, aby boli pre podnik prínosom.

Prijatím a prispôsobením rámcu ITIL bude možné zvýšiť efektívnosť a účinnosť poskytovaných služieb IT, jasne definovať správu služieb IT a vymedziť hlavné procesy s príslušnými cieľmi. Rámec ITIL využíva osvedčené praktiky, ktoré už boli úspešne použité v iných organizáciách. Prakticky overené procesy, zvyšovanie kvality služieb a dlhodobá optimalizácia s neustálym zlepšovaním ponúkajú potenciál pre zníženie nákladov.

K udržaniu integrity funkčného systému riadenia bezpečnosti informácií s navrhovaným riadením služieb informačných technológií bude nápomocná norma ČSN ISO/IEC 27013:2015 – Pokyn pre integrovanú implementáciu ISO/IEC 27001 a ISO/IEC 20000-1.

## Abstract

The diploma thesis solves proposals for improving the quality of providing IT services and their optimization in the interest of the company and its business goals. For the needs of user-friendly IT services with optimized cost, the processes, functions, roles of employees and technology need to be a benefit for the business.

By adopting and adapting the ITIL framework, it will be possible to increase the efficiency and effectiveness of providing IT services, to clearly define the IT service management and to define the main processes with the relevant objectives. The ITIL framework uses best practices that have been successfully used in other organizations. Practically proven processes, improved service quality and long-term optimization with continuous improvement offer cost-cutting potential.

ISO/IEC 27013:2015 provides guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 will be helpful in maintaining the integrity of the current information security management system with the design of IT services management.

## Kľúčové slová

ITSM, ITIL, ISMS, GDPR, Riadenie služieb IT

## Key words

ITSM, ITIL, ISMS, GDPR, IT Service Management

## Bibliografická citácia

ANTALÍK, D. *Návrh zavedení ITSM s využitím rámce ITIL se zaměřením na bezpečnost.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2018. 75 s. Vedoucí diplomové práce Ing. Petr Sedlák.

## 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 21. května 2018

.....

podpis studenta

## Poďakovanie

Ďakujem pánovi Ing. Petrovi Sedlákovi, že bol ochotný viesť moju záverečnú prácu, ústretový prístup, promptné reakcie na moje otázky, návrhy na zlepšenie a dotiahnutie diplomovej práce do výslednej podoby. Taktiež ďakujem oponentovi, ktorý mi predložil nápad na túto tému a vďaka jeho vysokej pracovnej pozícii v danom podniku som mohol nahliadnuť na detailnejší na chod spoločnosti.

# OBSAH

# ÚVOD

Vďaka neustále sa zvyšujúcej potrebe a významnosti informačno-komunikačných technológii (ICT) v obchodných jednotkách a celej spoločnosti, rastú požiadavky na riadenie ich prevádzky z pohľadu služieb, ktoré by mohli ponúknuť ostatným oddeleniam podniku. Závislosť podnikových procesov na informačných technológiách sa tak neustále prehlbuje. Pohľad na ICT ako len na prevádzku technologických komponentov je už zastaralý a nie je postačujúcim pre efektívne využitie v podnikaní.

Práve kvôli tomu je potrebné zmeniť pohľad na ICT v podniku a vnímať ich viac ako jednotlivé služby, ktoré vďaka procesnému riadeniu a zákaznícky orientovanému prístupu poskytnú konkurenčnú výhodu, zlepšenú odolnosť a dostupnosť služieb, ktoré povedú k vyššej spokojnosti zákazníkov a samotnému znižovaniu nákladov pre podnik.

# ZADANIE

Medzi úlohy, ktoré majú byť dosiahnuté patrí transformácia oddelenia, resp. oddelení informatiky do jednotného európskeho IT oddelenia so zameraním na optimalizáciu a správu služieb IT pomocou rámcu ITIL za účelom diverzifikovať riziká, určiť role vlastníkov a správcov jednotlivých služieb so zreteľom na bezpečnú a odolnú infraštruktúru informačných technológií a s tým spojenými procesmi.

Okrem toho je nutné integrovať súčasný systém riadenia bezpečnosti informácií do komplexného systému riadenia IT služby, ktorý bude spĺňať požiadavky normy ČSN ISO/IEC 20000-1.

# 1 TEÓRIA

## 1. 1 Slovník pojmov

V prvom rade je potrebné definovať pojmy používané v tejto záverečnej práci a celkovo v reálnom prostredí, ktoré sa zaoberajú problematikou riadenia služieb IT a rámcom ITIL, ktoré vychádzajú z oficiálnej dostupnej literatúry. [1]

- Activity (činnosť) – množina akcií navrhnutá tak, aby sa dosiahlo určité výsledky. Činnosti sú zvyčajne definované ako časť procesov alebo plánov a sú dokumentované v postupoch. [1]
- Asset (aktívum) – čokoľvek v organizácii, čo má nejakú cenu (hmotné a nehmotné) - všetok hmotný a nehmotný majetok. [2]
- Audit (audit) – systematický, nezávislý a zdokumentovaný proces slúžiaci k objektívnemu hodnotenia podľa vopred stanovených kritérií. Je to nezávislý a dokumentovaný proces s hodnotením kritérií. Môže byť interný, vykonaný poverenou osoby z podniku, externý alebo certifikačný. [3]
- Availability (dostupnosť) – Z pohľadu služby: Schopnosť plniť požadovanú funkčnosť v určitý čas, resp. po určitú dobu. Vyjadruje sa ako percentuálny podiel medzi rozdielom doby prevádzky služby a dobou výpadku s dobou prevádzky služby. Z pohľadu bezpečnosti informácií: zabezpečenie dostupnosti informácií pre oprávnených používateľov v okamihu potreby. [3], [4]
- Confidentiality (dôvernosť) – Z pohľadu služby: služby sú prístupné alebo oznámené len tým, ktorí sú na to oprávnení. Z pohľadu bezpečnosti informácií: zabezpečenie prístupu k informáciám a poskytnutie iba oprávneným osobám. [3], [4]
- Countremeasure (opatrenie) – akákoľvek aktivita, zariadenia, technika či postup znižujúce silu hrozby alebo zabránenie účinku hrozby. [2]
- Customer (zákazník) – zákazníkom pre poskytovateľa IT služieb je akákoľvek osoba, skupina, organizačný útvar, atď, ktorí platí za poskytnuté služby. Nerozlišuje sa medzi poskytovaním služieb pre interného zákazníka (v rámci jedného podniku) alebo pre externého zákazníka (iný podnikateľský subjekt). [4]
- Effectiveness (efektivita) – požiadavky na včasné doručovanie relevantných služieb v správnom, konzistentnom a použiteľnom spôsobe. [5]

- Efficiency (účinnosť) – požiadavky na správu služieb najekonomickejším a najproduktívnejším spôsobom prostredníctvom optimálneho využívania zdrojov informatiky. [5]
- Event (udalosť) – zmena stavu, ktorá je významná z hľadiska riadenia konfiguračnej položky alebo IT služby. Pojem je tiež používaný vo význame výstrahy alebo upozornenia pochádzajúcich od IT služby, konfiguračnej položky alebo monitorovacieho nástroja. Udalosti zvyčajne vyžadujú, aby pracovník prevádzky IT vykonal nejakú činnosť, a často vedú k registrácii incidentu.
- GDPR (GDPR) – Všeobecné nariadenie o ochrane osobných údajov [2]
- Chain of Trust (reťazec dôvery) – Reťazec, ktorý zabezpečí dôvernosť údajov počas celého životného cyklu a mapuje ako sa prenášajú, kto ich spracúva a ako sa zhromažďujú alebo archivujú. [2]
- Impact (dopad) – vznik škody v dôsledku hrozby. [2]
- Incident (incident) – neplánované prerušenie IT služby alebo obmedzenie kvality služby IT. Incidentom je tiež porucha konfiguračnej položky, ktorá doteraz neovplyvnila službu - napríklad porucha jedného zo zrkadlených diskov. [1]
- Integrity (integrita) – zaistenie správnosti a úplnosti informácií
- Maintainbility (udržateľnosť) – Ako rýchlo a efektívne je možné po výpadku obnoviť službu. [4]
- Manager (správca) – Správca procesu nesie operatívnu zodpovednosť za daný proces. Zameriava sa na realizáciu činností v každodennej prevádzke a sleduje koordináciu, eskaláciu a komunikáciu. [4]
- Operation Level Agreement (dohoda o úrovni prevádzkových služieb) – dohoda medzi poskytovateľom IT a ďalšie súčasťou tej istej organizácie. Dohoda definuje tovar alebo služby, ktoré by mali byť poskytnuté, a zodpovednosti oboch strán. [1]
- Owner (vlastník) – Rozlišuje sa vlastník procesu a vlastník služby. Vlastník služby zodpovedá za službu ako celok v priebehu jej životného cyklu a je členom poradného výboru. Vlastník procesu je zodpovedný za návrh, zavedenie, implementáciu a výsledky procesu, tak aby bolo dosiahnutých stanovených cieľov. [5]
- Problem (problém) – príčina jedného alebo viacerých incidentov. Príčina zvyčajne nie je známa v čase vytvorenia záznamu o probléme a proces správy problémov je zodpovedný za jeho ďalšie skúmanie. [1]

- Process (proces) – štruktúrovaná množina činností navrhnutá pre dosiahnutie určitého špecifického cieľa. Proces má jeden alebo viac definovaných vstupov a pretvára ich do definovaných výstupov. Môže obsahovať akékoľvek role, zodpovednosti, nástroje a manažérske kontrolné mechanizmy požadované pre spoľahlivú dodávku výstupov. Proces môže v prípade potreby definovať politiky, normy/štandardy, smernice, činnosti a pracovné inštrukcie. [1]
- RACI matrix (matica zodpovednosti) – Popisuje zodpovednosti za rôzne činnosti a úlohy so štyrmi stavovými hodnotami. [2]

A: Accountable, zodpovedá

C: Consulted, konzultovaný

I: Informed, informovaný

R: Responsible, realizuje

- Reliability (spoľahlivosť) – Ako dlho je po dohodnutý časový rámec služba bez problémov k dispozícií. [2]
- Risk (riziko) – kombinácia hrozby a zraniteľnosti [2]
- Service (služba) – prostriedok poskytovanie hodnoty zákazníkovi prostredníctvom výstupov, ktorých zákazník chce dosiahnuť bez vynaloženia špecifických nákladov a rizík. [1]
- Service desk (service desk) – jediné kontaktné miesto medzi poskytovateľom služieb a užívateľmi. Typický service desk spravuje incidenty a požiadavky na službu a zabezpečuje komunikáciu s užívateľmi. [1]
- SLA, Service Level Agreement (dohoda o úrovni služieb) – dohoda medzi poskytovateľom IT a zákazníkom. Dohoda o úrovniach služieb opisuje službu IT, dokumentuje ciele úrovňou služieb a špecifikuje zodpovednosti poskytovateľa IT služieb a zákazníka. Jedna dohoda o úrovni služieb môže pokrývať rad služieb IT, alebo viac zákazníkov. [1]
- Threat (Hrozba) – akcia alebo udalosť, ktorá môže ohroziť bezpečnosť (zneužitie zraniteľnosti). [2]
- Vulnerability (zraniteľnosť) – akékoľvek slabé miesto aktíva. [2]

## 1. 2 ITSM – IT Service Management

ITSM predstavuje spôsob riadenia informačných a komunikačných technológií, ich prevádzky a rozvoja, ktorý využíva princípy riadenia na báze služieb, zahŕňa teda pohľad zákazníkov aj poskytovateľa samotných IT služieb. [4]

Snaží sa definovať a popísať služby, ktoré podniková informatika poskytuje zamestnancom, naučiť zamestnancov s týmito službami pracovať v kontexte ich každodenných činností a následne tieto služby kontinuálne riadiť, a to ako na operatívnej, tak aj taktickej a strategickej úrovni. Pokrýva predovšetkým operatívni prevádzku dodávaných služieb a dlhodobejšie budovanie vzťahu informačných a komunikačných technológií s obchodnými útvarmi v oblasti synchronizácie dopytu a dodávky IT služieb. [3]

ITSM predstavuje:

- súčinnosť ľudí – z oblasti ICT aj podnikateľskej činnosti
- pracujúcich na základe definovaných procesov – so stanovenými cieľmi, zodpovednosťami a spôsobmi vyhodnocovania výsledkov svojej činnosti
- za podpory zodpovedajúcich technologických nástrojov – implementovaných v zmysle definovaných procesov
- Jedným z najpoužívanejších prístupov k ITSM (definícia procesov, ich vlastníkov, požiadavky na zodpovedajúce nástroje, apod.) je v dnešnej dobe ITIL – the IT Infrastructure Library. [5]

Pre ITSM existuje norma ČSN ISO/IEC 20000. Tento štandard definuje súbor vzájomne prepojených radiacich procesov. Prostredníctvom súladu s ISO 20000 organizácia získa ďalšie možnosti a bude viesť niektoré organizačné zmeny. Ďalšie výhody, ktoré dosiahne organizácia z preukázateľného súladu s best practice sú:

- konkurencie schopnejší biznis
- súlad IS/IT stratégie s celkovou biznis stratégiou
- manažované a redukované riziká
- manažované a znížené náklady
- rýchlejšia implementácia zmien
- zlepšená odolnosť a dostupnosť služieb vedúca k vyššej spokojnosti zákazníkov
- integrovaní a na služby orientovaní dodávatelia a partneri
- možnosť porovnania s inými organizáciami [5]

## 1. 3 Vzťah ITSM a ISMS

Information Security Management System (systém riadenia bezpečnosti informácií, ISMS) je podmnožinou celkovej správy IT služieb, teda ITSM. Túto správu je možné v podnikoch nasadiť a certifikovať samostatne bez riadenia ostatných služieb. na ISMS sa vzťahuje norma ČSN IEC/ISO 27001.

Norma ČSN ISO/IEC 27013:2015 poskytuje návod pre integrovanú implementáciu ISO 27001 a ISO 20000-1 pre organizácie, ktoré zamýšľajú:

- implementovať ISO 27001 po predchádzajúcej implementácií ISO 20000-1 alebo opačne,
- implementovať súčasne ISO 27001 a ISO 20000-1,
- integrovať existujúce ISO 27001 a ISO 20000-1 manažérske systémy. [2]

Obe správy obsahujú návod pre cyklické a neustále sa zlepšujúce riadenie, ktorým je Demingov PDCA cyklus, ktorý je popísaný nižšie.

## 1. 4 ITIL

Popis najlepších skúseností a osvedčených postupov, ako efektívneho riadenia služieb IT dosiahnuť, je uvedený v sade knižných publikácií, ktoré sa súhrnne nazývajú ITIL (IT Infrastructure Library, voľný preklad: Knižnica Infraštruktúry Informačných Technológií). [3]

ITIL poskytuje rámec pre zvládnutie IT v organizácii, pojednáva komplexne o službách a zameriava sa na neustále meranie a zlepšovanie kvality dodávaných služieb IT, a to ako z pohľadu biznisu, ako z pohľadu zákazníka. Toto zameranie je hlavnou príčinou celosvetového úspechu ITIL a prispelo k rozšírenému využitie a prínosom, ktorých organizácie, ktoré aplikovali tieto techniky a procesy vo svojich štruktúrach, dosiahli. [3]

V súčasnej verzii knižnice už nie je pôvodný význam týchto štyroch písmen uvádzaný, dokonca ani v oficiálnom výkladovom slovníku ITIL dostupnom na http://www.itil-officialsite.com/. To je zapríčinené pravdepodobne tým, že sa obsah knižnice infraštruktúre informačných technológií venuje len z pohľadu jej riadenia, a to ešte len vo vzťahu k službám IT, nie k technológiám ako takým.

### 1. 4. 1 História

Vznik procesného riadenia ITIL je v literatúre často spájaný s historickou udalosťou z druhej polovice 20. storočia. V roku 1982 vypukla vojna medzi Veľkou Britániou a Argentínou o Falklandské ostrovy. Cez obrovskú technologickú prevahu britského námorníctva vybaveného najmodernejšími informačnými a komunikačnými technológiami nebol vývoj tohto vojenského stretu úplne jednoznačný. Britskému námorníctvu napríklad trvalo celé dva týždne, než prvá loď opustila domovský prístav a mohla sa zapojiť do bojov. Podľa niektorých prameňov boli na vine predovšetkým problémy s modernými informačnými a komunikačnými technológiami, respektíve s ich riadením a koordináciou požiadaviek na ne kladenými. Po skončení vojny britská vláda bezodkladne začala kroky k náprave a poverila jednu zo svojich agentúr – Central Computer and Telecommunications Agency – tým, aby **vytvorila určitý štandard pre riadenie ICT služieb**, ktorého používanie vo vládnom sektore by bolo záväzné. [4]

Toto pozadie vzniku ITIL však podľa dostupných informácií sa nedá preukázateľne potvrdiť, okrem skutočnosťou, že britské námorníctvo bezprostredne po vypuknutí vojenského konfliktu malo nešpecifikované ťažkosti a že krátko po skončení vojny bola agentúra Central Computer and Telecommunications Agency vládou poverená vytvorením záväzného štandardu riadenie ICT služieb a ICT infraštruktúry. Je pravdepodobné, že súvislosť medzi týmito dvoma faktami v skutočnosti neexistuje. Jednak ťažkosti námorníctva neboli spôsobené nefunkčnými ICT službami, ako skôr nedostatočnú koordináciu logistických zložiek armády a tiež vtedajšia konzervatívna vláda, vedená Margaret Thatcherovou, mala vytýčený hlavný cieľ v zastavení ekonomického prepadu, zoslabenie úlohy štátu v národnom hospodárstve a obmedzenie celkových výdavkov. Vládni úradníci si tak nemohli nevšimnúť veľkej miery neefektivity a vysokých nákladov oddelenia informačných technológií pri jednotlivých vládnych úradov. [4]

Kľúčové historické momenty spojené s vývojom ITIL:

- Po roku 1982 vzrastajú hlasy na britských ostrovoch proti nízkej efektivite správy ICT pri jednotlivých vládnych úradov. Riešením tejto situácie je poverená Central Computer and Telecommunications Agency. [3], [4], [5]
- V roku 1986 britská Central Computer and Telecommunications Agency zostavuje tím odborníkov pod vedením Johna Stewarta a Peta Skinnera, ktorá v nasledujúcich mesiacoch vykonáva rozsiahly výskum v oblasti organizácie správy ICT u mnohých úspešných podnikov. [3], [4], [5]

- V roku 1988 na základe skúseností získaných týmto výskumom vydáva publikácie, pre ktorých je použitý súhrnný názov Government Infrastructure Management Method (Gitmo), ktorý je v roku nasledujúcom (1989) zmenený na Information Technology Infrastructure Library (ITIL), neskôr označovaný ITIL V1. Tieto publikácie sú určené ako metodika pre správu IT britského verejného sektora. [3], [4], [5]
- V rokoch 1989 - 1994 je publikované viac ako 40 kníh ITIL V1. [3], [4], [5]
- V roku 1991 vzniká IT Service Management Forum (itSMF), medzinárodná nezávislá organizácia zložená z profesionálov a odbornej verejnosti, účelovo sa venujúca všetkým aspektom riadenia služieb informačných a komunikačných technológií. Predovšetkým vďaka tejto komunite sa aj širšia verejnosť začína hojne zoznamovať s rámcom ITIL. [3], [4], [5]
- V tomto roku sa tiež začína s vydávaním prvých certifikátov odbornej spôsobilosti pre oblasť IT Service Management podľa ITIL. [3], [4], [5]
- V roku 1999 začínajú prvé revízie ITIL V1, tentoraz v silnom obsadení medzinárodných firiem a konzultantov z celého sveta, začína sa pracovať na ITIL V2. [3], [4], [5]
- V roku 2000 vzniká Office of Government Commerce (OGC), a to zlúčením troch britských vládnych agentúr vrátane Central Computer and Telecommunications Agency, ktorá týmto zaniká. OGC tak preberá zodpovednosť za správu ITIL a púšťa sa do prepracovania pôvodnej kníh ITIL V1 a začína vydávať publikácie ITIL V2. [3], [4], [5]
- V rokoch 2002 - 2006 vychádza kompletná publikácia ITIL V2, ako posledné v roku 2006 je vydaný ITIL Glossary V2 (Výkladový slovník ITIL V2). Táto druhá verzia začala byť univerzálne akceptovaná v mnohých krajinách tisíckami organizáciami, ako základňa pre efektívne poskytovanie služieb IT. [3], [4], [5]
- V roku 2004 tím pod vedením Sharon Taylorovej začína pracovať na ITIL V3. [3], [4], [5]
- V roku 2007 bol ITIL V2 vystriedaný rozšírenú a konsolidovanú verziou ITIL V3, skladajúci sa z piatich kľúčových kníh pokrývajúcich životný cyklus služieb, spoločne s oficiálnym úvodom. Avšak tým rozvoj knižnice ITIL V3 zďaleka neskončil, postupne boli vydávané ďalšie doplňujúce a rozširujúce publikácie. [3], [4], [5]
- V roku 2011 prebehla zatiaľ posledná aktualizácia piatich ústredných publikácií ITIL V3 a výkladového slovníka, táto verzia je označovaná ako ITIL 2011 Edition. [3], [4], [5]

## 1. 5 Charakteristické rysy ITIL

ITIL sa za dobu svojej existencie stal medzinárodne uznávaný štandard pre riadenie ICT služieb a ICT infraštruktúry a v dnešnej dobe predstavuje najrozšírenejšie nástroj používaný v procesne riadených organizáciách. K samotnému vývoju ITIL prispeli mnohí odborníci, experti, čelné praktici a významné osobnosti z odvetvia informačných technológií. Tvorcovia si uvedomovali, že neexistuje univerzálne riešenie pre návrh a implementáciu optimalizovaného procesu pre správu a dodávku kvalitných IT služieb.

Preto pri tvorbe vychádzali predovšetkým z najlepších praktických skúseností, pričom ponechali veľkú voľnosť pri implementácii jednotlivých procesov. Každá organizácia, či už sa jedná o poskytovateľa interných služieb alebo o externého poskytovateľa služieb, tak mohla aplikovať koncepciu ITIL a prispôsobiť si ju svojmu vlastnému jedinečnému prostrediu. Ide o princíp, ktorý býva v angličtine označovaný ako adopt and adapt (prijať a prispôsobiť).

### 1. 5. 1 Procesné riadenie

Jedným z najvýznamnejších charakteristických rysov rámca ITIL je procesne orientovaný prístup k riadeniu IT služieb. Filozofia procesného prístupu vychádza z predpokladu, že základným objektom riadenia je popísaný, definovaný, štruktúrovaný, zdrojovo a vstupmi zabezpečený proces, ktorý je uskutočňovaný pre konkrétneho zákazníka a má jednoznačne, vytýčeného vlastníka. Preto sa v ITIL objavujú procesy, ich **vlastníci, role a zodpovednosti**. [3], [6]

ITIL bol vyvinutý tak, aby bol procesne orientovaný a napriek tomu škálovateľný a dostatočne flexibilné, aby bol vhodný pre akúkoľvek organizáciu od malých a stredných až po globálne medzinárodné organizácie. [3], [6]

### 1. 5. 2 Zákaznícky orientovaný prístup

Rámec ITIL pristupuje k činnosti IT oddelení v organizácii ako ku vzťahu dodávateľa a zákazníka. Teda **IT oddelenie preberá úlohu dodávateľskej firmy**, zatiaľ čo **ostatné oddelenia organizácie vystupujú ako zákazníci IT oddelenia**, ktorí dopytujú jeho služby. Všetky procesy sa tak navrhujú s ohľadom na jednotlivé potreby zákazníka, každá aktivita, ktorákoľvek činnosť v každom procese tak musí prinášať nejakú pridanú hodnotu pre zákazníka, v opačnom prípade je tento úkon nadbytočný. [3], [5]

### 1. 5. 3 Jednoznačná terminológia

Jednoznačná terminológia je často zanedbávaná a nedocenený charakteristika rámcovo ITIL. Často však práve zlá komunikácia spôsobená rozdielnou terminológie býva zdrojom množstva najrôznejších problémový. Táto vlastnosť tak uľahčuje komunikáciám nielen v rámci organizácii, ale aj s obchodnými partnermi. [3], [5]

### 1. 5. 4 Nezávislosť na platforme

Rámec procesov podľa ITIL je nezávislý na akékoľvek použitej platforme, a preto jeho výstupy je možné aplikovať pre navrhovanie procesov v akejkoľvek spoločnosti pohybujúcej sa v službách, dokonca aj mimo oblasti informačných a telekomunikačných technológií. [3], [5]

### 1. 5. 5 Dostupnosť

Na rozdiel od celého radu iných metodík a prístupov pre riadenie služieb informačných technológií, je knižnica ITIL voľne dostupná širokej verejnosti. Každý si tak môže publikácie ITIL zakúpiť a používať návody a rady vzniknuté na základe najlepších praktických skúseností. Táto skutočnosť veľkou mierou prispela celosvetovému rozšíreniu ITIL. [3], [5]

## 1. 6 Čo očakávať a neočakávať od ITIL

### ITIL nie je norma

V knižnici ITIL sa objavuje len veľmi málo imperatívov, ITIL málokedy niečo priamo striktne predpisuje.

*„Jeden príklad za všetky: ITIL hovorí, že procesy Incident Management a Problem Management by nemali byť nikdy zlúčené do jedného procesu, a takisto manažéri týchto dvoch procesov by mali byť dve rôzne osoby.“* [7]

Takýchto nariadenie sa nachádza v celej knižnici naozaj len niekoľko. Väčšinou sa jedná o sadu praktických odporúčaní, ktorá by mala byť v organizácii uplatňovať, pretože s najväčšou pravdepodobnosťou je to na základe skúseností z iných firiem potreba. Rozhodne sa však nedá očakávať, že ITIL ponúkne univerzálne riešenie, pretože skúsenosti, z ktorých ITIL vzišiel, pochádzajú z veľmi heterogénneho prostredia. Každá organizácia je unikátna svojimi, zvyky, odborom pôsobnosti, filozofiou a pod., A preto je nutné riešenie potrebám danej spoločnosti prispôsobiť. [7]

**ITIL je rámec ITSM, nie presný pracovný postup pre ITSM**

ITIL nedáva presné inštrukcie ako konkrétne jednotlivé činnosti vykonávať, akú mať organizačnú štruktúru, aké pripraviť pracovné toky, či ako obsadiť role konkrétnymi pracovnými pozíciami. Dáva iba rámcové návody. [7]

*„Jeden príklad za všetky: ITIL hovorí, že všetky incidenty majú byť prioritný vzhľadom na vplyv, ktorý má ich existencia na biznis a naliehavosť, s ktorou ich vyriešenie požaduje užívateľ, tj. podľa aktuálnej potreby pracovať so službou, na ktorej incident vznikol. Ďalej ITIL obsahuje jednu ukážku jednoduchého systému skladania priorít na základe dopadu a naliehavosti. A to je všetko. ITIL nepredpisuje, koľko má byť stupňov pre dopad a naliehavosť, ani aké majú byť výsledné priority pre jednotlivé kombinácie ich hodnôt. ITIL nehovorí, aké konkrétne časy riešenia incidentu majú reprezentovať jednotlivé stupne priorít. Tiež nie je jasne uvedené, na základe akých konkrétnych kritérií sa má vyhodnocovať, akú hodnotu dopadu a naliehavosti má mať daný incident.“* [7]

V minulosti sa síce objavovali určité pokusy o vytvorenie jednotnej komplexnej metodiky v riadenia služieb informačných technológií, ktoré by predpisovala aj také detaily popísané vo vyššie uvedenom príklade, avšak každý takýto pokus bol neúspešný. Univerzálna metodika riadenia služieb informačných technológií použiteľná celosvetovo pre všetky podnikateľské obory (sa zdá) nemôže nikdy existovať. [7]

**Podľa ITIL nemožno systém riadenia služieb informačných technológií objektívne auditovať**

Pretože v rámci ITIL sa takmer nič nepredpisuje, ale skoro všetko je založené na odporúčaní z praxe, nedá sa u konkrétneho systému riadenia služieb informačných technológií v konkrétnom podniku objektívne prehlásiť, či jednotlivý prvok je zle alebo dobre.

Existuje síce celý rad rôznych pomocných („self-assessment“) dotazníkov, ktoré umožňujú vyhodnotiť, v ktorých procesoch je aplikované aké množstvo prvkov „Best practice“, ale už nie je možné len na základe ITIL objektívne posúdiť, či sú tieto prvky implementované správne či zle.

**Pre skutočné objektívne hodnotenie systému riadenia služieb informačných technológií slúži medzinárodná norma ISO / IEC 20000.**

**ITIL neobsahuje žiadne nové prevratné myšlienky**

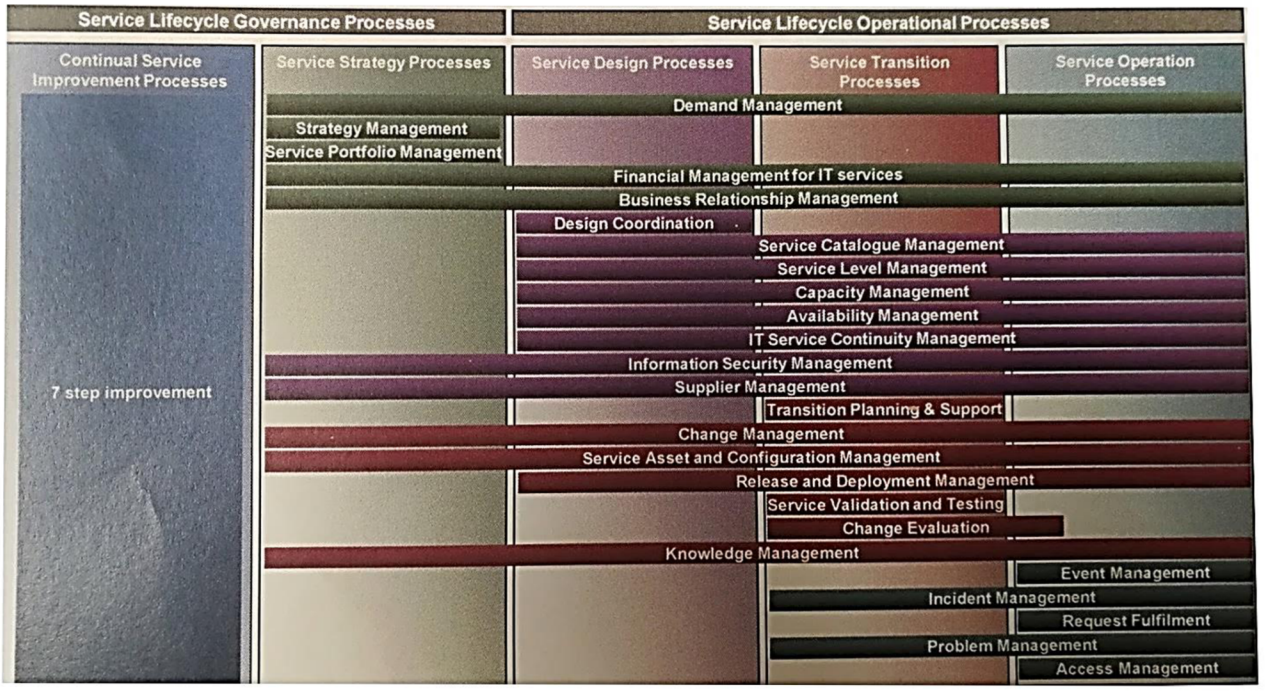
V spojitosti s ITIL sa často hovorí nielen o „best practice“, ale takisto aj o „common sense“ (zdravý rozum). Aj v organizáciách, kde o ITIL nikdy nikto nepočul, môže existovať systém riadenia služieb informačných technológií, ktorý bude obsahovať mnoho prvkov opísaných v ITIL publikáciách, a to jednoducho preto, že manažéri a odborníci v tomto podniku dospeli k tým samým poznatkom, ako mnohí iní pred nimi. Toto by však nemal byť dôvodom na to, aby sa od ITIL odvracalo. Samotná prevádzka informačných technológií v podnikovom prostredí je konfrontovaná s veľmi tvrdými požiadavkami na kvalitu, spoľahlivosť, náklady a výkon. ITIL môže v tomto prípade pomôcť manažérom a IT špecialistom **nájsť inšpiráciu či návod pre riešenie každodenných problémov**.

## 1. 7 Životný cyklus

Životný cyklus služieb, ktorý zobrazuje nasledujúci obrázok, sa skladá celkom z piatich fáz a každá z ústredných piatich publikácií opisuje práve jednu z týchto fáz: Service Strategy, Service Design, Service Transition, Service Operation, Continual Service Improvement. Kniha Service Strategy začína životný cyklus služby, kde sa plánuje stratégia businessu (vrátane zberov požiadaviek, budovanie portfólia služieb a finančných súvah) a z nej vyplývajúce stratégie služieb informačných technológií. Nadväzujúca publikácia Service Design definuje vlastný návrh služieb vrátane podporných procesov, infraštruktúry, metrík a podporných systémov. Service Transition pokrýva implementáciu (prechod) služby do prevádzkového prostredia a zahŕňa také kroky ako testovanie, vlastné nasadenie, školenia a validáciu. Ďalšia kniha v poradí Service Operations potom popisuje všetky prevádzkové aspekty služby. Celý životný cyklus je logicky zakončený knihou Continual Service Improvement, ktorá sa zaoberá aspektmi priebežného vylepšovania v oblasti businessu, technológií a procesov. [3]

Celkom je v týchto piatich knihách ITIL popísaných 26 kľúčových procesov a k nim mnoho desiatok ďalších aktivít, z ktorých mnohé majú charakter celých procesov, a ďalej 4 komplexné funkcie a asi stovka rolí, ktoré sa vzťahujú ako priamo k jednotlivým procesom, tak súhrnne k celým fázam životného cyklu služby. [3]


**Obrázok č. 1: Životný cyklus služby.**
[Zdroj: 3]




**Obrázok č. 2: Životný cyklus služieb**
[Zdroj: 3]

### 1. 7. 1 Service Strategy (Stratégia služieb)

Poskytuje praktický rámec k návrhu, vývoji a implementácii riadenia služieb nielen z pohľadu organizačného, ale aj ako zdroja strategickej výhody. Dá sa povedať, že je do istej miery skôr učebnicou ekonómie a obchodnej stratégie, než publikácií o správe služieb informačných technológií. Je skutočným jadrom ITIL.

Kniha nie je primárne určená pre technických odborníkov alebo vedúci prevádzky IT, ale skôr pre riaditeľov informatiky, finančných riaditeľov alebo finančných analytikov.

Obsahuje definície služieb, stratégiu IT Service Managementu a plánovanie pridanej hodnoty, IT Governance, definície typov poskytovateľov služieb a obchodných stratégií, respektíve stratégiou služieb. Jej účelom je pomáhať oddeleniam IT stať sa dôležitou súčasťou celej firmy. Spôsob jej fungovania na základe správy služieb by tak mal byť hlavným princípom a súčasťou jej celkovej stratégie. [8]

Pre dosiahnutie poznania a predovšetkým porozumenie potrieb zákazníka, ktoré musia byť základom stratégie služieb všetkých poskytovateľov, je potrebné jasne analyzovať, kto je existujúci a potenciálny zákazník, čo sú jeho potreby a akým spôsobom môže poskytovateľ dosiahnuť ich uspokojenie. Poskytovateľ tak musí porozumieť situácii aktuálnych trhov, na ktorých operuje, aj potenciálnych trhov, na ktorých chce pôsobiť.


**Obrázok č. 3: Popis aktivít a očakávaných výsledkov**
[Zdroj: 8]

## Stratégia 4P v Service Strategy

- perspektíva: príznačná vízia a smer
- pozícia: základňa, kedy bude poskytovateľ pôsobiť
- plán: ako poskytovateľ dosiahne svoje vízie
- profil: charakteristické správanie pri rozhodovaní a správanie v priebehu doby

1) Konkurencia a priestor na trhu – poskytovateľ sa musí oproti svojim konkurentom snažiť lepšie porozumieť trhovému priestoru, jeho zákazníkom a kritickým faktorom úspechu.

2) Hodnota služby – je ako strategické aktívum opísané pomocou dvoch základných charakteristík - užitočnosť služby a záruka služby. Užitočnosť služby označuje to, čo zákazník dostáva v zmysle podporovaných výstupov alebo odstránených obmedzení. Záruka služby predstavuje spôsob, akým je služba dodávaná a jej vhodnosť na použitie. Vytvorenie hodnoty služby tak môže priniesť trvalé výhody a nárast potenciálu poskytovateľa.

3) Typy poskytovateľov služieb – tu je potrebné rozlišovať, či poskytovateľ dodáva službu pre jeden alebo viac útvarov podniku, či pôsobí ako externý dodávateľ pre viac externých zákazníkov.

4) Správa služieb ako strategické aktívum – ITIL môže viesť k nárastu potenciálu poskytovateľa služieb taktiež prostredníctvom použitia zdrojov (finančných, kapitálových, informačných, personálnych) a schopnosťou koordinovať, kontrolovať a implementovať tieto zdroje.

5) Kritické faktory úspechu – pre úspešnú implementáciu stratégie služieb je tiež potrebné, aby poskytovateľ pravidelne identifikoval, analyzoval a revidoval kritické faktory úspechu.

6) Modely poskytovaných služieb – jedná sa o kategorizácii spôsobe získavania služby buď prostredníctvom financovania priamo zo zdrojov podnikovej jednotky pre seba samu (tzv. Spravovaná služba), prostredníctvom zdieľanej infraštruktúry a zdrojov pre zaistenie viac služieb (tzv. Zdieľaná služba), alebo poskytovanie služieb na základe toho, kedy, koľko a ako často ich zákazník požaduje (tzv. utilita).

7) Návrh a rozvoj organizácie – dosiahnutie priebežné podoby a štruktúry organizácie, ktoré umožňujú stratégiu služieb. Ide o:

i) štádia rozvoja organizácie: všetka dodávka závislá na vývojovom stave organizácie prostredníctvom siete delegovania, spolupráca a koordinácia.

ii) stratégia výberu zdrojov: rozhodnutie, či sa bude jednať o zdieľanú službu, spravovanú službu alebo outsourcovanie služieb.

iii) analytika služby: porozumenie výkonnosti služby prostredníctvom analýzy.

iv) rozhranie služby: ustálené procesy, prostredníctvom ktorých používatelia spolupracujú s každou službou.

v) správa rizík: správa portfólia rizík, ktoré vychádzajú z portfólia služieb.

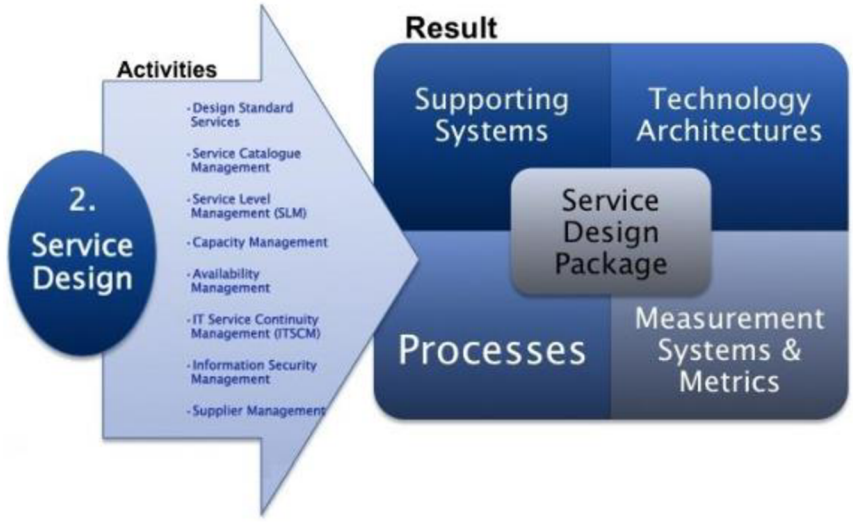
### 1. 7. 2 Service Design (Návrh služieb)

Kniha Service Design predstavuje druhú fázu životného cyklu služby a jej hlavným zámerom je návrh, vývoj služieb a súvisiacich procesov pre ich uvedenie do produkčného prostredia. Poskytuje všeobecný základ pre vytvorenie návrhu súčasných a budúcich obchodných požiadaviek, zahŕňa princípy a metódy pre prevod strategických cieľov do portfólia služieb. Nezameriava sa len na nové služby, ale pokrýva aj procesy zmeny a priebežného zlepšovanie existujúcich služieb, ich pridanej hodnoty pre zákazníka a v neposlednom rade aj ich súlad s právnymi predpismi a normami. [8]
Hlavné ciele tejto knihy by sa dali zhrnúť do nasledujúcich bodov:

- Návrh služieb vyhovujúcich dohodnutým výstupom biznisu.
- **Návrh bezpečnej a odolnej infraštruktúry informačných technológií.**
- **Identifikácia a správa rizík.**
- **Návrh procesov pre podporu životného cyklu služby.**
- Návrh metód pre meranie a návrh metrík.
- Rozvoj zručností, schopností a všeobecné zlepšenie kvality služieb informačných technológií. [3], [8]

**Stratégia 4P v Service Design**

- personál: ľudia, zručnosti a kompetencie, ktoré sú potrebné pre poskytovanie služieb informačných technológií.
- produkty: technologické systémy a systémy správy používané pre dodávku služieb informačných technológií.
- procesy: procesy, úlohy a činnosti, ktoré sa týkajú zabezpečovania služieb IT.
- partneri: predajcovia, výrobcovia a dodávatelia využívaní pri asistencii a podpore poskytovania služieb informačných technológií. [3], [8]




**Obrázok č. 4: Popis aktivít a očakávaných výsledkov**
[Zdroj: 9]

### 1. 7. 3 Service Transition (Prechod služieb)

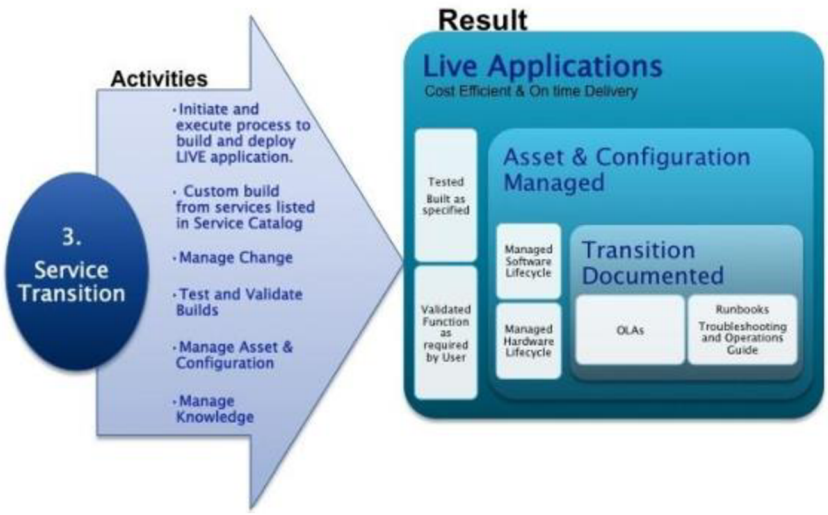
Popisuje fázu prevodu služby z jednej fázy svojho životného cyklu do ďalšej. Poskytuje rady pre riadenie projektu tak, aby výsledná nová alebo upravená služba bola čo najspôsobilejšie pre odovzdanie do produkčného prostredia, aby pri odovzdaní došlo k čo najmenej chybám, obmedzením aktuálnych služieb a prejavením čo najmenej rizík. Vstupom do tejto fázy je kompletná špecifikácia čo je potrebné urobiť, kúpiť, nainštalovať, naprogramovať a otestovať, a výstupom je fungujúca služba informačných technológií v produkčnom prostredí. [8]

Service Transition je podporovaný základnými princípmi uľahčujúcimi efektívne a hospodárne využitie nových alebo upravených služieb. Medzi kľúčové princípy v tejto fáze životného cyklu kniha zahŕňa:

- Porozumenie všetkým službám, ich užitočnosti a zárukám – pre efektívny prechod služby je podstatné poznať jej podstatu, účel, užitočnosť pre business a mať záruku, že táto užitočnosť bude dodaná v patričnej kvalite.
- Zriadenie formálnej politiky a spoločného rámca pre implementáciu všetkých potrebných zmien – tento rámec musí spĺňať vlastnosti ako konzistentnosť, úplnosť a zaručiť, že sa nezabudne žiadna služba, zainteresovaná osoba, príležitosť atď. Nespôsobí sa tak porucha služby.
- Podpora prenosu znalostí, podpora rozhodovania a opätovného použitia procesov, systémov a ďalších elementov – efektívne prechod služieb prebieha za účasti všetkých

zainteresovaných strán, pri zabezpečení dostupnosti potrebných znalostí a možnosti opakovaného použitia za podobných okolností v budúcnosti.

- Predvídanie a riadenie „korekcií smeru“ – v tejto fáze životného cyklu je nevyhnutné zisťovať pravdepodobné požiadavky na korekciu smeru, a pokiaľ je nutné prvky služieb doladiť, je potreba k tejto úlohe pristupovať logicky a s kompletnou dokumentáciou. [3], [8]




**Obrázok č. 5: Popis aktivít a očakávaných výsledkov**
[Zdroj: 10]

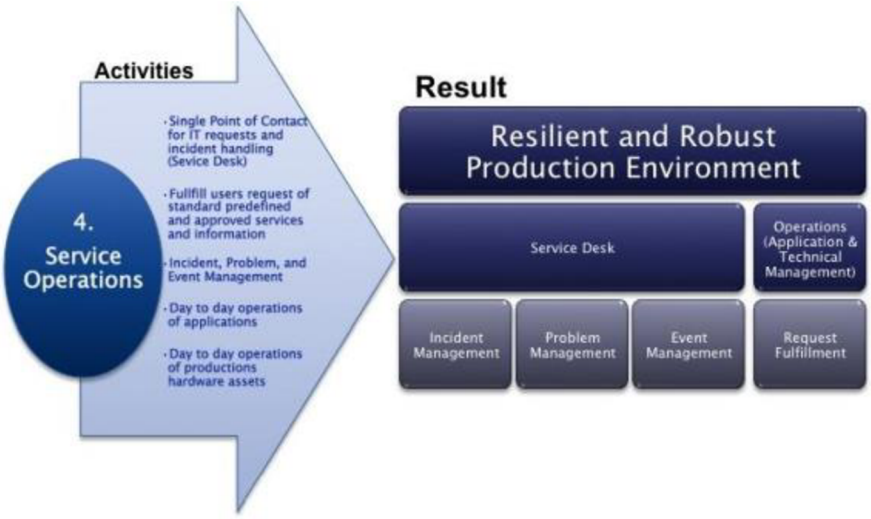
### 1. 7. 4 Service Operations (Prevádzka služieb)

Service Operations sa priamo zameriava na prevádzku služieb businessu. Popisuje priamu dodávku služieb, ale tiež monitoruje problémy, rovnováhu medzi spoľahlivosťou služby a jej cenou. Jej hlavným cieľom je podať návod, ako dosiahnuť efektivity a pridanej hodnoty ako pre zákazníka, tak pre poskytovateľov služieb a túto pridanú hodnotu udržať aj v prípade služieb, ktoré prechádzajú zmenou. Jedná sa o životný cyklus IT služby, ktorý má za úlohu prevádzkovať IT služby tak, aby z nich podnik mal väčší alebo prinajmenšom rovnaký úžitok a poskytovali podporu jej užívateľom. [8], [11]
V rámci Service Operations je teda dôležité vyvážiť konfliktné ciele, ktoré by inak mali za následok zlú službu. Týmito konfliktnými cieľmi sú:

- Vnútorný pohľad IT × vonkajší pohľad businessu
- Stabilita × vnímavosť
- Kvalita služby × náklady na službu

- Reaktívne × proaktívne činnosti

Prevádzka služieb zahŕňa procesy, ktorých cieľom je udržiavať spokojnosť zákazníkov na vysokej úrovni, a to predovšetkým tým, že služby budú dosahovať nimi požadované kvality. Jedná sa o všetky procesy zahŕňajúce monitoring služby, jej zlepšovanie a reporting. Sústredí sa aj na každodenné skvalitňovania služieb a podporu informačných technológií. [8]




**Obrázok č. 6: Popis aktivít a očakávaných výsledkov**
[Zdroj: 11]

## 1. 7. 5 Demingov (PDCA) Cyklus

Používa sa ako presne stanovený a cyklicky sa opakujúci sled krokov a činností pri zavádzaní inovácií a zvyšovanie kvality.

P: Plan (plán) – identifikácia procesov a služieb. Ustanovenie.

D: Do (robiť) – popísanie a zdokumentovanie procesov a služieb. Zavedenie a prevádzka.

C: Check (kontrolovať) – riadenie na základe dokumentov. Monitorovanie a prevádzka.

A: Act (jednať) – následná optimalizácia. Údržba a zlepšenie. [2]


**Obrázok č. 7: PDCA cyklus**
[Zdroj: 13]

Plán:

- ciele manažmentu služieb, ktorých chce poskytovateľ služby dosiahnuť,
- požiadavky na služby,
- známe obmedzenia, ktoré môžu ovplyvniť systém managementu služieb (SMS),
- politiky, štandardy, zákonné a regulačné požiadavky a zmluvné záväzky,
- zodpovednosti a úlohy v rámci procesov,
- ľudské, technické, informačné a finančné zdroje potrebné na dosiahnutie cieľov SMS,
- iné zúčastnené strany v procese návrhu a prechodu nových alebo zmenených služieb,
- rozhrania medzi procesmi a ich integráciou s ďalšími súčasťami SMS,
- prístup k manažmentu rizík a kritériá pre akceptovanie rizík,
- technológie využívané pre podporu SMS,
- spôsob merania, auditovanie, vykazovanie a zlepšovaniu efektívnosti SMS a služieb. [13]

Robiť:

- pridelenie a riadenie finančných zdrojov a rozpočtov,
- splnomocnenia, zodpovednosti a úlohy v rámci procesov,
- riadenie ľudských, technických a informačných zdrojov,
- identifikácia, vyhodnotenie a manažment rizík služieb,
- riadenie procesov manažmentu služieb,
- monitorovanie a vykazovanie výkonnosti činností v rámci manažmentu služieb. [13]

Kontrolovať:

- spätná väzba od zákazníkov,
- výkonnosti služieb a procesov,
- súčasné a budúce odhadované úrovne ľudských, technických, informačných a finančných zdrojov,
- riziká,

- výsledky a následné opatrenia z interných auditov a z preskúmaní manažmentu,
- zmeny, ktoré by mohli ovplyvniť SMS a služby,
- príležitosti pre zlepšenie. [13]

Jednať:

- stanovenie cieľov pre zlepšovanie v jednej alebo viacerých oblastiach týkajúcich sa kvality, hodnôt, kapacít, nákladov, produktivity, využívania zdrojov a zníženie rizík,
- zaistenie, že schválené zlepšenia sú implementované,
- aktualizácia politiky manažmentu služieb, plánov, procesov a postupov tam, kde je to potrebné,
- meranie implementovaných zlepšení oproti stanoveným cieľom a tam, kde nie sú ciele dosiahnuté, prijímanie potrebných opatrení,
- reportovanie implementovaných zlepšenie. [13]

# 2 ANALÝZA SÚČASNÉHO STAVU

Kapitola obsahuje stručnú charakteristiku podniku, jeho hierarchiu a súčasný stav podniku so zameraním na procesy a služby oddelenia IT.

## 2. 1 Charakteristika spoločnosti

Spoločnosť je vedúci poskytovateľ produktov, služieb, a riešení v oblasti tlače, dokumentov, a ich spracovania. Osobitný dôraz kladie na celkové riešenie tlače a správy obehu dokumentov v kancelárskom a produkčnom prostredí. Okrem toho ponúka online a cloudové služby, automatizáciu podnikových procesov a implementáciu ERP a CRM riešení spojené s technickou a servisnou podporou.

Spoločnosť sa vývoju a inováciám venuje už od svojho vzniku, teda už viac ako 145 rokov. Stále si však udržuje dynamiku mladej firmy. Ich sľub zákazníkom „Dávame myšlienkam tvar“ je vedúcim princípom všetkých aktivít. Tento podnik zjednodušuje pracovný život s ohľadom na budúci rozvoj a vytvára pozoruhodné a pritom udržateľné riešenia s prípravou na úplnú digitalizáciu a „paper-less“ kancelárie v najbližších rokoch.

## 2. 2 Charakteristika oddelenia Informatika – INF

V súčasnej dobe sa oddelenie Informatiky zaoberá podporou a správou pracovných staníc, mobilných zariadení a softvérového vybavenia zamestnancov, vrátane podpory komunikačnej infraštruktúry, aplikačných serverov, ďalších informačno-komunikačných zariadení, zabezpečením, bezpečnosťou informácií a evidenciou IT aktív. Zoznam činností, resp. služieb, ktoré v súčasnosti oddelenie informatiky ponúka je uvedený spoločne s priradenými zodpovednosťami uvedený v kapitole 2. 6 Matica zodpovednosti RACI.

Oddelenie Informatiky v súčasnej dobe tvorí desať zamestnancov usporiadaných do troch vetví na základe špecializácie, ktoré sa orientujú na rozdielne typy podpory a správy a popri tom niektorí členovia oddelenia sa nachádzajú v geograficky inej lokácií na inej pobočke, kde ponúkajú primárne technickú podporu pre zamestnancov z iných oddelení. **Problematickou tak je vzájomná zastupiteľnosť a zdieľanie informácií v rámci tímu ako celku.**

Oddelenie sa schádza na pravidelných mesačných schôdzach, kde sa prediskutovávajú kľúčové udalosti za posledný mesiac v starostlivosti o vyššie uvedené a smerovaniu tímu v nasledujúcom období, prípadne iné aktuálne témy. Tieto stretnutia

sa sústreďujú skôr na chod tímu ako celku a oznamujú sa prípadné ďalšie strategické rozhodnutia zo strany vedenia.

Celé oddelenie zastrešuje hlavný IT manažér, ktorý zabezpečuje koordináciu celého oddelenia a komunikáciu naprieč ďalšími oddeleniami na úrovni manažmentu.

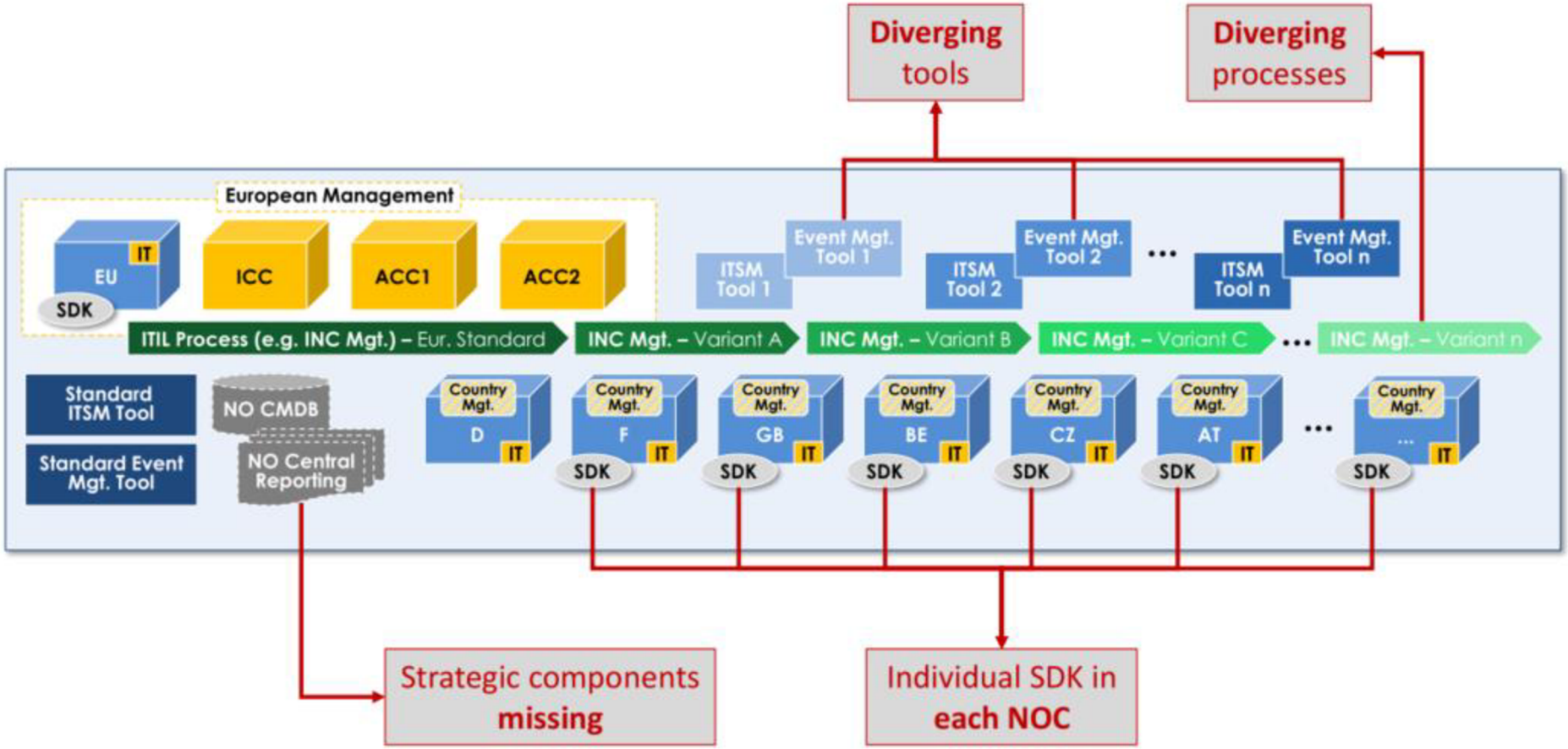
### 2. 2. 1 Súčasný stav

V súčasnosti jednotlivé oddelenia IT v jednotlivých krajinách fungujú samostatne podľa vlastných plánov a cieľov nezávisle od ostatných krajín. Každé oddelenie IT má svoje vlastné procesy a spôsoby realizácie plánov, podporné nástroje, individuálne služby a ich riadenie, vlastné helpdesky, ktoré slúžia na podporu zákazníkov, samostatne zakupované softvérové licencie a duplikácie zamestnancov, ktorí vykonávajú tie isté činnosti, len v iných krajinách.

Už teraz existuje pomaly vznikajúce európske IT, ktoré plánuje zjednotiť a zintegrovať ostatné krajinné oddelenia IT. Aktuálne vykonáva úlohy vrcholového IT managementu s víziami a strategickými plánmi na päť a viac rokov dopredu a je do neho začlenená celoeurópska podpora aplikácií pre externých zákazníkov z krajín Európy.

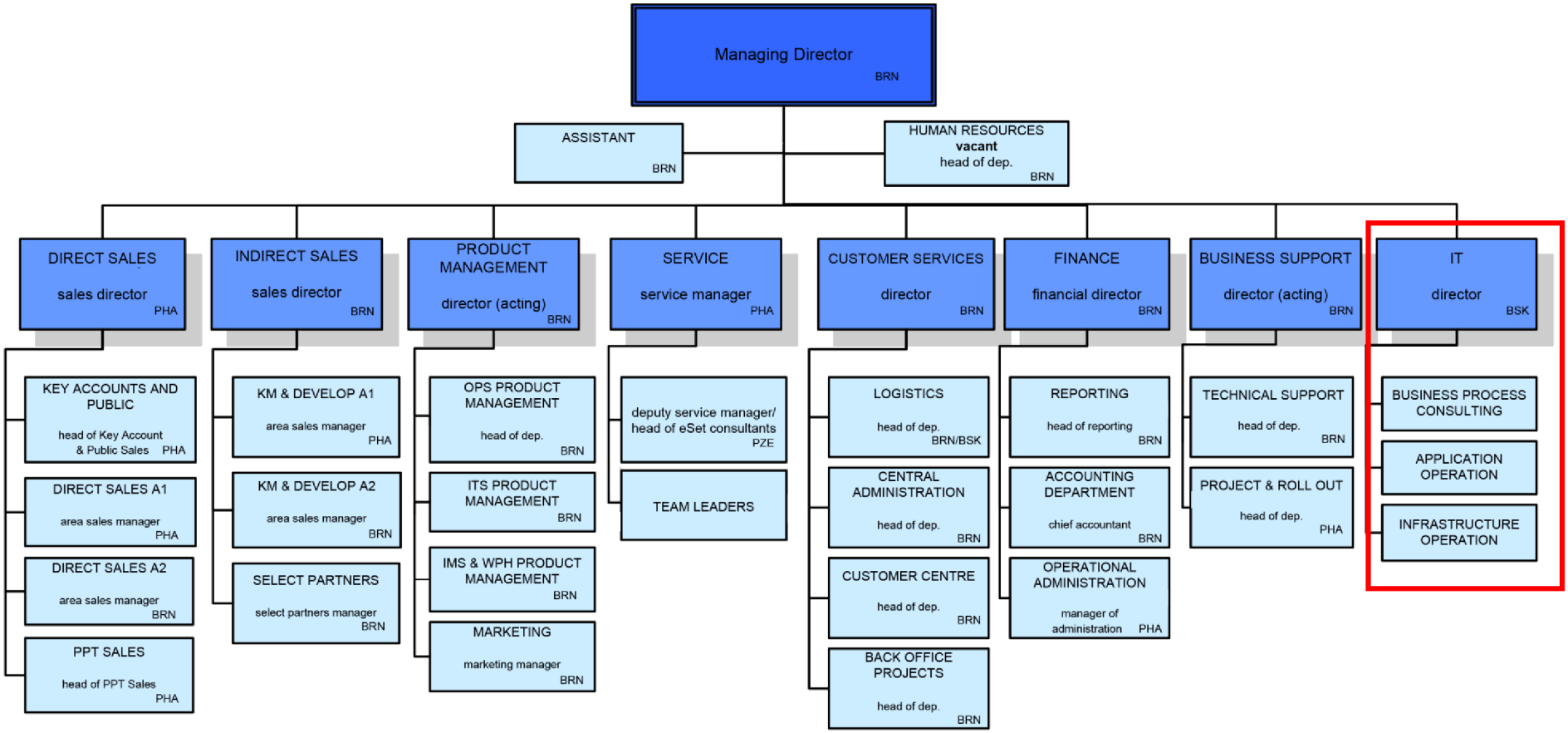
Chýbajú predovšetkým hlavné strategické komponenty pre unifikáciu ako napríklad centrálny informačný systém pre reporting, konfiguračná databáza, centrálny service desk, správa úrovní služieb a ďalšie komponenty, ktoré sú popísané v samostatnej kapitole návrhu riešenia.

Súčasný stav prevádzky s hlavnými nedostatkami sa nachádza v prehľadnej schéme na nasledujúcej strane.




**Obrázok č. 8: Súčasný stav**
[Zdroj: Interný dokument spoločnosti]

## 2. 3 Organizačná štruktúra




**Obrázok č. 9: Organizačná štruktúra. Zvýraznené oddelenie INF**
[Zdroj: Interný dokument spoločnosti]

## 2. 4 Prehľad aktív

**Tabuľka č. 1: Prehľad aktív**
[Zdroj: Vlastné spracovanie]

| Kategória aktíva | P.č. | Aktívum | Hodnota aktíva | Vlastník aktíva (z hľadiska zodpovednosti) |
|---|---|---|---|---|
| Informačné | 1 | Data na PRINT servere | 4 | Vedúci IT oddelenia, riaditeľ KAC |
| | 2 | Data na zálohovacom serveri pre pracovníkov | 5 | Vedúci IT oddelenia, riaditeľ KAC |
| | 3 | Data na poštovnom exchange serveru a sharepoint serveri | 5 | Evropská centrála |
| | 4 | Data na ostatných PC | 3 | Všetci pracovníci |
| | 5 | Data na prenosných diskoch (externý vymeniteľný disk, šifrovaný flash disk) | 5 | Všetci pracovníci |
| | 6 | Zálohované data | 2 | Všetci pracovníci, ved. IT odd. |
| | 7 | Prenášená data na prenosných pamäťových nosičoch od zákazníkov | 5 | Všetci pracovníci |
| | 8 | Zmluvy so zákazníkmi v listinnej podobe | 5 | Všetci pracovníci |
| | 9 | Zmluvy s dodávateľmi v listinnej podobe | 3 | Asistentka odd. KAC |
| | 10 | Dokumentácia k zakázkám v listinnej podobe | 3 | Všetci pracovníci |
| | 11 | Ponuky a objednávky so zákazníkmi v listinnej podobe | 4 | Všetci pracovníci |
| | 12 | Objednávky na dodávateľov v listinnej podobe | 1 | Asistentka odd. KAC |
| | 13 | Prevádzková dokumentácia | 2 | Asistentka odd. KAC |
| | 14 | Personálna agenda (pracovné zmluvy, osobné listy zamestnancov, podklady pre mzdy apod.) | 3 | Vedúci HR oddělení |
| | 15 | Data prístupné na bezdrôtovej sieti Wi-Fi | 5 | Ved. IT odd., Všetci pracovníci |
| | 16 | Data v mobilných telefónoch | 2 | Ved. IT odd., Všetci pracovníci |
| SW | 17 | Operačné systémy | 5 | Vedúci IT oddelenia |
| | 18 | Programy a aplikace | 2 | Vedúci IT oddelenia, Evropská centrála |

| Kategória aktíva | P.č. | Aktívum | Hodnota aktíva | Vlastník aktíva (z hľadiska zodpovednosti) |
|---|---|---|---|---|
| Fyzické | 19 | Notebooky zamestnancov | 3 | Všetci pracovníci, ved. IT odd. |
| | 20 | PRINT server | 2 | Vedúci IT oddelenia |
| | 21 | Zálohovací server pre zamestnancov | 2 | Vedúci IT oddelenia |
| | 22 | Šifrované flashdisky | 1 | Všetci pracovníci, ved. IT odd. |
| | 23 | Mobilné telefóny | 1 | Všetci pracovníci, ved. IT odd. |
| | 24 | Prenosné pamäťové nosiče | 1 | Vedúci IT oddelenia |
| | 25 | Ostatné zariadenia (tablety, multifunkčné zariadenia, projektory, GPS, apod.) | 1 | Vedúci IT oddelenia |
| | 26 | Automobily | 1 | Všetci pracovníci, ved. IT odd. |
| | 27 | Priestory oddelení vrátane serverovien v lokalitach | 3 | riaditeľ odd. KAC, ved. IT oddelenia |
| Ľudské zdroje | 28 | Riaditeľ a asistentka | 5 | riaditeľ odd. KAC |
| | 29 | IT oddelenie | 5 | riaditeľ odd. KAC |
| | 30 | Ostatní zamestnanci | 3 | riaditeľ odd. KAC |
| | 31 | Služby vzťahujúce sa k oddeleniu a pobočkám (technické služby budovy, úklid, apod.) | 1 | riaditeľ odd. KAC |
| | 32 | Tretie strany | 3 | Vedúci IT oddelenia |
| Ostatné | 33 | Image spoločnosti | 5 | všetci pracovníci, vedúci oddelení |

## 2. 5 Analýza rizík

**Tabuľka č. 2: Analýza rizík**
[Zdroj: Vlastné spracovanie]

| Riziko | Aspekt | Dôvod vzniku | Vlastník rizika | Potenciálny dopad, pokiaľ riziko nastane | Reálna pravdepo-dobnosť výskytu rizika* | Úroveň rizika/kritéria pre akceptáciu rizika** | Súčin pravdepo-dobnosti a úroveň rizika*** |
|---|---|---|---|---|---|---|---|
| špecifická hrozba pre bezpečnosť informácií spoločnosti spojená so stratou dôvernosti, integrity a dostupnosti informácií; účinok neistoty na dosiahnutie cieľov | E = externé, I = interné | | ten, kto je oprávnený riadiť riziko | | 1 - nízka<br>2 - stredne vysoká<br>3 - vysoká | 1 - nízka<br>2 - stredne vysoká<br>3 - vysoká | <5 - netreba prijať opatr.<br>=>6 - je nutné prijať opatr. |
| nekvalitne odvedená práca zamestnancom | I | | riaditeľ oddelenia | poškodenie mena spoločnosti, možná strata zákazníka | 2 | 3 | **6** |
| nekvalitne odvedená práca externým dodávateľom | E | | riaditeľ oddelenia | poškodenie mena spoločnosti, možná strata zákazníka | 2 | 3 | **6** |
| zneužitie prístupu do dystému spoločnosti | I | | všetci zamestnanci | strata dát, neoprávnený prístup k informáciám, neoprávnené akcie pod cudzou indetitou | 2 | 3 | **6** |
| vykradnutie oddelenia | E | | riaditeľ oddelenia | strata vybavenia kancelárií, súvisiacich dokumentovaných informácií, poškodenie mena spoločnosti, ak by došlo k zneužitiu | 2 | 2 | 4 |
| prezradenie dôverných informácii zamestnancom na verejnosti | I, E | | všetci zamestnanci | poškodenie mena spoločnosti, ak by došlo k zneužitiu zistených informácií | 1 | 3 | 3 |
| strata alebo poškodenie dát z pracovnej stanice (notebook) | I | | všetci zamestnanci | dáta sú pravidelne zálohované, následkom je len časová strata než dôjde k obnove dát | 1 | 2 | 2 |
| strata dát z pracovnej stanice (notebook) | E | | všetci zamestnanci | dôjde k strate dát, v prípade, že nedošlo k ich uloženie na server, dôjde k časovej strate než budú opäť obnovené | 1 | 2 | 2 |
| zámena dát predávaných zákazníkovi | I | | všetci zamestnanci | porušenie dôvernosti, nutné ihneď riešiť so subjektom, s ktorým k zámene došlo, prijatie nápravných opatrení | 1 | 2 | 2 |
| nedodržania NDA zo strany zákazníka | E | | riaditeľ oddelenia | poškodenie mena spoločnosti | 1 | 2 | 2 |
| akýkoľvej novo prijatý zamestnanec | I | | riaditeľ oddelenia | poškodenie mena spoločnosti | 1 | 2 | 2 |
| zneužitie informácií spoločnosti | I | | všetci zamestnanci | strata dát | 2 | 3 | 2 |
| strata alebo poškodenie dát z pracovnej stanice (desktop) | E | | všetci zamestnanci | dochádza iba k strate alebo poškodeniu dát na pracovných staniciach, následkom je len časová strata než dôjde k obnove dát | 1 | 1 | 1 |
| strrata alebo poškodenie dát na serveroch | I, E | | administrátor | dáta sú pravidelne zálohované mimo HDD servera, následkom je len časová strata než dôjde k obnove dát | 1 | 1 | 1 |
| strata alebo poškodenie dát na zálohovacom serveri | E | | riaditeľ oddelenia | dáta sú pravidelne zálohované mimo HDD servera, následkom je len časová strata než dôjde k obnove dát | 1 | 1 | 1 |
| strata dát zo zálohovacieho serveru | E | | administrátor | okamžitá výmena administrátorských hesiel, ak dôjde k útoku z vonku | 1 | 1 | 1 |
| strata šifrovaných diskov | I | | vlastník disku | šifrovaný disk je bez kódu nepoužiteľný, pre majiteľa disku sa jedná o finančnú stratu | 1 | 1 | 1 |

### 2. 5. 1 Kritériá pre hodnotenie rizík bezpečnosti informácií

1) riziká sú priebežne posudzované bezpečnostným manažérom (BM), v prípade výskytu nového rizika, alebo opakovania sa existujúceho rizika zvoláva BM bezpečnostnú poradu za prítomnosti ďalších pracovníkov podľa charakteru rizika (administrátor, vlastníci rizík a pod.) a prijímajú príslušné opatrenia.

2) kritériá na posudzovanie rizík sú dané číselnými stupnicami v stĺpcoch „reálna pravdepodobnosť výskytu rizika“ a „úroveň rizika / kritérium pre akceptáciu rizika“.

3) v analýze rizík sú zahrnuté iba riziká, ktoré môžu skutočne nastať, nezahrnujeme sem riziká s nereálnou pravdepodobnosťou.

Medzi hlavné aspekty systému riadenia bezpečnosti informácií patrí:

- harmonizácia s normami pre ďalšie systémy riadenia (ISO 9001)
- kontinuálne zabezpečenie procesu zlepšovania riadenia manažérstva bezpečnosti informácií
- zabezpečenie súladu s právnymi predpismi

Medzi interné aspekty ďalej patrí:

- stálosť v stave kľúčových zamestnancov oddelenia KAC vrátane vedúceho pracovníka
- oddelenie KAC spoločnosti sídli stále v rovnakých priestoroch zabezpečených preverenýmspôsobom
- oddelenie KAC spoločnosti využíva profesionálne HW a SW, ktorý je aktualizovaný vždy po starostlivom uvážení a po konzultácii s IT oddelením
- dodržiavanie všetkých požiadaviek podľa zavedených a neustále zlepšovanie systémov podľa ČSN EN ISO 9001: 2009 a ČSN ISO/IEC 27001: 2014

Medzi externé aspekty ďalej patrí:

- stála, dlhodobá a bezproblémová spolupráca s IT a HR oddelením
- stála a dlhodobá spolupráca s poradcom vo veci neustáleho zlepšovania zavedeného ISMS
- stála, dlhodobá a bezproblémová spolupráca s internými dodávateľmi
- stála a dlhodobá spolupráca s V.I.P. zákazníkmi
- sledovanie legislatívnych požiadaviek a ich napĺňanie v rozsahu vzťahujúcim sa k činnosti oddelenia KAC našej spoločnosti
- služby recepcie a ostrahy majiteľa budovy

## 2. 6 Matica zodpovednosti RACI

**Tabuľka č. 3: RACI matica**

[Zdroj: Vlastné spracovanie na základe interného dokumentu]

| IT Service Catalog (or Activity) / Role / Name | | Zamestnanec I | Zamestnanec II | Zamestnanec III | Zamestnanec IV | Zamestnanec V | Zamestnanec VI | Zamestnanec VII | Zamestnanec VIII | Zamestnanec IX | Zamestnanec X | Riaditeľ IT | ACC2 oddelenie | ICC oddelenie | OPS oddelenie |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | **Infrastructure Operation** | | | | | **Aplication Operation** | | | | **Business Process Consulting** | **CIO** | **L2 Support** | | |
| Central | **SharePoint - Central** | I | R | | | | | | | | | I | | A/R/C | |
| Central | **Business Warehouse** | | | | | | I | | | | | A/C | | | |
| Central | **Corporate Website Hosting** | I | I | | | | | | | | | I | | A/R/C | |
| Central | **CRM** | | | | | | | | I | | R/C | A | | | |
| Central | **CSES** | | A | | | | | R/C | | | | I | | | |
| Central | **eCON** | | I | R | | | I | I | R | | | A | C | | |
| Central | **ECS** | | I | R | | | I | I | R | | | A | C | | |
| Central | **Exchange** | A/R/C | | I | | | | | | | | I | | C | |
| Central | **InfoPortal** | | I | I | | | | | R | | | A | | C | |
| Central | **Lighthouse** | | | | | | | | | | | A | | R | |
| Central | **Lync** | A/R/C | | I | I | I | | | | | | I | | C | |
| Central | **Myinfohub external** | | A | | | | | | | | | I | R/C | | |
| Central | **Myinfohub internal** | | A | | | | | | | | | I | R/C | | |
| Central | **NAV Mobile Technician (LMobile)** | | R | | | | I | I | | | | A | C | | |
| Central | Mobile Technician INFRA | I | A/R | | | | I | I | | | | I | C | | |
| Central | Mobile Technician APP | | A/R | | | | I | R | | | | I | C | | |
| Central | **Navision C** | I | I | | | | R | I | | | | A | C | | |
| Central | **eInvoice** | | R | | | | C | | A/R | | | I | I | | |
| Central | **OPS C** | | I | | | | | R | | | | A | | | C |
| Central | OPS CSRC | | I | | | | | R | | A | | I | | | C |
| Central | OPS CSRC 4Mobile | | I | | | | | R | | A | | I | | | C |
| Central | OPS CSRC Device Checker | | I | | | | | R | | A | | I | | | C |
| Central | OPS CSRC Remote Panel | | I | | | | | R | | A | | I | | | C |
| Central | OPS DRMS | | I | | | | | R | | A | | I | | | C |
| Central | OPS IDQM | | I | | | | | R | | A | | I | | | C |
| Central | OPS M2M GPRS Solution | | I | | | | | R | | A | | I | | | C |
| Central | OPS PrintFleet | | I | | | | | R | | A | | I | | | C |
| Central | **Remedy** | | | R | I | | | | | | | A | | | C |
| Central | **Central Proxy** | R | | | | | | | | | | I | | A/C | |
| Central | **Client to Site VPN** | A/R | | R | R | R | | | | | | | | C | |
| Central | **Data Center Network** | I | | | | | | | | | | I | | A/R/C | |
| Central | **Citrix** | | | | | | | | | | | | | A/R/C | |
| Central | **Active Directory** | I | I | | | | | | | | | | | A/R/C | |
| Central | **Group Policies** | A/R/C | I | | | | | | | | | I | | C | |
| Central | **Data Archiving** | | | | | | | | | | | | | A/R/C | |
| Central | **Data Center Housing** | | | | | | | | | | | I | | A/R/C | |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Central | **Server (virtual)** | A | | | | | | | | | | | | R/C | |
| Central | **Server Management** | A | | | | | | | | | | | | R/C | |
| Central | **Storage** | A | | | | | | | | | | | | R/C | |
| Local | **Intranet - Sharepoint 2013** | | A/R | | | | | | | | | C/I | | | |
| Local | **Pivotal CRM** | | | | | | | | I | | A/R | C/I | | | |
| Local | Pivotal training I | | | | | | | | A/R | | C | I | | | |
| Local | Pivotal training II | | | | | | | | I | | A/R/C | I | | | |
| Local | **Přístup na internet (www, ftp)** | A/R | | | | | | | | | | I | | | |
| Local | **SQL server** | | A/R | | | | C/I | | | | | I | | | |
| Local | **Tiskové služby přes alikaci SafeQ** | | A/R | R | | | | | | | | I | | | |
| Local | **Nástup nového zaměstnance** | A/R | | R | R | R | R | R | R | | R | I | | | |
| Local | **Servis HW** | A/R | | R | R | R | | | | | | I | | | |
| Local | **Nákup HW** | R | | R | R | R | | | | | | A | | | |
| Local | **Mzdy** | | A/R | | | | | | | | | I | | | |
| Local | **EZS, vstupní systém** | | A/R | R | | | | | | | | I | | | |
| Local | **PBX** | | A/R | R | | | | | | | | I | | | |
| Local | **správa Active Directory** | A/R | R | | | | | | | | | | | | |
| Local | **aplikačná podpora Navision** | I | I | | | | R | I | | | | A | | | |
| Local | Navision INFRA | A/R | R | | | | I | | | | | I | C | | |
| Local | Navision Finance | | | | | | A/R | R | | | | I | C | | |
| Local | Navision Sales | | | | | | A/R | R | | | | I | C | | |
| Local | Navision Service | | | | | | R | A/R | | | | I | C | | |
| Local | Navision Logistics | | | | | | A/R | R | | | | I | C | | |
| Local | Navision Other | | | | | | A/R | R | | | | I | C | | |
| Local | **podpora VT, MT** | R | R | R | R | R | | | | | | A | | | |
| Local | **správa serverů v správě BCZ IT** | A/R | R | | | | | | | | | I | | | |
| Local | **přídělování přístupů práv** | R | R | R | R | R | R | | R | | R | A | | | |
| Local | **Evidence aktiv IT** | R | | R | R | R | | | | | | A | | | |
| Local | **IT Asset managament** | R | | R | R | R | | | | | | A | | | |
| Local | Nákup VT | R | | R | R | R | | | | | | A | | | |
| Local | Odkup vyřazené VT | R | | R | R | R | | | | | | A | | | |
| Local | **aplikace Zoner pro eshop KMBCZ** | R | A/R | | | | | | | | | I | | | |
| Local | **LAN + Wifi** | A/R | | R | R | R | | | | | | I/C | | | |
| Local | **Vývojové prostřední DataSpring, DEMO hosti** | A/R | | | | | | | | | | I/C | | | |
| Local | **VPN v mobilu** | A/R | | | | | | | | | | I | | | |
| Local | **FileSharing Replicas for Service** | A/R | | | R | | | | | | | I | | | |
| Local | **CarControl** | | A/R | | | | | | | | | I | | | |
| Local | **Testovaní bezkontatních karet pro MFP** | | | A/R | | | | | | | | I | | | |
| Local | **Generování licencí pro OBCH a ECM** | | C | | | | | | R | | A/R | I | | | |
| Local | **Synology NAS** | R | | | | | | | | | | A | | | |
| Local | **Software** | R | | R | R | R | | | | | | A | | | |
| Local | **BCZ DataWarehouse** | | R | | | | R | | | | | A | | | |
| Local | **Datamining** | | | | | | A/R | R | | | R | I | | | |
| Local | **dokoniCASE** | | R | R | | | | | | | | A/I/C | | | |
| Local | **podpora OBCH ECM** | | | | | | | | | | | A/I/C | | | |
| Local | **IT školení** | R | R | R | R | R | | | | | | A | | | |

# 3 VLASTNÝ NÁVRH RIEŠENIA

Samotný návrh využíva rámec ITIL, vďaka ktorému je možné diverzifikovať dopad rizika, lepšie určiť zodpovednosti a rozčleniť činnosti oddelenia do samostatných procesov, a vytvoriť príslušné funkcie. Samotné vytvorenie správ služieb zabezpečení lepšie zmapovanie procesov a určenie vlastníkov a správcov pre dané procesy.

Vďaka pôsobeniu spoločnosti naprieč celou Európou je možné vytvoriť jedno veľké IT oddelenie, pod ktoré budú spadať jednotlivé oddelenia z rôznych štátov a súčasní pracovníci budú začlenení do tímov v rámci Európy, tzv. kompetenčných centier. Tým pádom sa vytvoria tímy, ktorých členovia budú mať príbuzné vedomosti a orientáciu na podobné problémy.

Táto distribúcia zabezpečí predovšetkým zastupiteľnosť jednotlivých zamestnancov, lepšiu komunikáciu a lepšie zdieľanie informácií v rámci tímu, vrátane využitia podporných nástrojov, ktoré budú popísané neskôr.

## 3. 1 Business Relationship Management

Vytvorenie tohto oddelenia spája procesy a funkcie, ktoré majú na starosti obchodné vzťahy z IT pohľadu.

Funkcia pre riadenie obchodných vzťahov zabezpečuje prepojenie medzi IT a ostatnými oddeleniami, resp. zákazníkmi, ktorých potreby sa menia. Manažér obchodných vzťahov rozumie všetkým obchodným procesom a poskytuje technologické usmernenia na zabezpečenie maximálnej návratnosti investícií.

Riadenie obchodných vzťahov pomáha pri obchodnej analýze a preklade zákazníckych požiadaviek do zrozumiteľného jazyka pre spoločnosť. Pre každú službu IT poskytovanú zákazníkovi by mala existovať zmluva. Je potrebné zriadiť centrálne úložisko všetkých zmlúv, aby ich bolo možné zmysluplne spravovať.

Kľúčovou úlohou BRM je znižovanie obchodných a IT bariér.

### 3. 1. 2 Správa úrovní služieb (Service level management)

Cieľom týchto ujednaní je zaistiť parametrizovanú podporu, kvalitu a kvantitu služieb a kontrolu ich prisľúbenej úrovne a reportovanie.

Reporty budú obsahovať nasledujúce informácie:

- Počet a percento incidentov s nedodržanou dobou reakcie
- Počet a percento incidentov s nedodržanou dobou k vyriešeniu
- Počet a percento incidentov s nedodržanou dobou dodania náhradného zariadenia

Má na starosti dohodnutie, schvaľovanie a dokumentovanie cieľov služieb informačných technológií s businessom, nastavuje merateľné ciele pre všetky aktivity zaisťované podnikovú informatikou, ktoré sa priamo podieľajú na dodávke služieb informačných technológií. Úlohou Service Level Managementu je dojednávať Service Level Agreement (dohoda o úrovni služieb) s dosiahnuteľnými parametrami a zodpovedať za zabezpečenie ich plnenia.

Ďalej potom dojednať Operation Level Agreement (dohoda o úrovni prevádzkových služieb) a zmluvy s externými dodávateľmi služieb, a to s takými parametrami a takým plnením, aby s ich pomocou bolo možné dosiahnuť splnenie parametrov Service Level Agreement.

### 3. 1. 3 Správa dodávateľov (Supplier Management)

Tento proces zabezpečuje, aby dodávatelia a služby, ktoré poskytujú, boli riadené tak, aby podporovali ciele služieb informačných technológií a očakávania businessu.

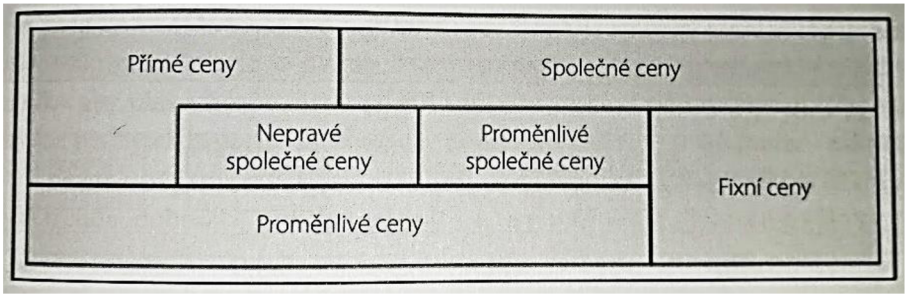
Účelom správy dodávateľov je získať od dodávateľov hodnotu za peniaze a zabezpečiť, aby dodávatelia plnili ciele obsiahnuté v ich kontraktoch a dohodách pri zachovaní všetkých termínov a podmienok. Databáza dodávateľov a kontraktov je rozhodujúcim zdrojom informácií o dodávateľoch a kontraktoch, a mala by obsahovať všetky informácie potrebné pre správu dodávateľov, kontraktov, a s nimi spojených služieb.

Medzi aktivity patrí definovanie dodávateľov a definovanie nových zmluvných požiadaviek, hodnotenie nových zmlúv a dodávateľov, kategorizácia dodávateľov a zmlúv, tvorba nových zmlúv a dodávateľských vzťahov, samotné spravovanie, a obnovenie alebo ukončenie zmluvy. Jedným z hlavných bezpečnostných požiadaviek na dodávateľa bude požiadavka o preukázanie súladu s GDPR v tom prípade, ak bude dodávateľ pri svojej práci prichádzať do styku s osobnými údajmi

Pri správe dodávateľov a dodávateľsko-odberateľských vzťahov sa taktiež uplatňujú politiky pre bezpečnosť informácií a ochranu osobných údajov, ktoré sú popísané v samostatných kapitolách: *Správa bezpečnosti informácií* a *Ochrana osobných údajov.*

### 3. 1. 4 Správa financií služieb IT (Financial Management)

Správa financií služieb IT je zodpovedná za ekonomické zváženie vytvorenia služby. Skutočné náklady na vytvorenie služby a správu služieb IT zvyčajne nie sú dostatočne rozpísané. Tomuto stavu sa vytvorenie správy financií snaží zabrániť. Cieľom je zaistiť prijateľný účtovný model a dokázať kvantifikovať hodnotu služieb. Následne je poskytovateľ služieb schopný dosiahnuť rovnováhy medzi nákladmi a kvalitou služieb a zaistiť zhodu s finančnými predpismi.




**Obrázok č. 10: Rozdelenie nákladov podľa pridelenia a variability**
[Zdroj: 3, s. 53]

Medzi vstupy pre vytvorenie správy patrí portfólio služieb, ktoré obsahuje informácie o výnosoch a nákladoch konkrétnych služieb. Ďalej tu patria predpisy, normy a postupy dané legislatívou a riadiacimi úrovňami podniku.

Výstupom správy financií sú: výpočet ROI, resp. TCO jednotlivých služieb, optimalizácia nákladov, hodnotenie služby a analýza dopadu na business.

## Matica zodpovednosti pre obstarávanie nového hardvéru[1]

**Tabuľka č. 4: RACI matica pre kúpu nového HW**
[Zdroj: Vlastné spracovanie]

| činnosť / zodpovednosť | IT | ZAS/OÚ | CON | VED | LOG |
|---|---|---|---|---|---|
| Vytvorenie a predanie požadavky | I | R | - | - | - |
| Prevzatíe a evidovanie požadavky | R | I | - | - | - |
| Upresnenie požiadavky | R | C | - | - | - |
| Aktualizácia stavu požiadavky v IT HelpDesk | R | I | - | - | - |
| Technické posúdenie požadavky | R | I | - | - | - |
| Finančné posúdenie požadavky | I | I | R | - | - |
| Rozhodnutie vedenenia spoločnosti | I | I | I | R | - |
| Predanie požadavky k nákupu | R | I | - | - | C |
| Realizácia nákupu | C | I | I | - | R |
| Kompletizácia, inštalácia | R | I | - | - | - |
| Evidencia | R | I | C | - | - |
| Testovanie | R | C | - | - | - |
| Predanie do užívania | R | C | - | - | - |

## Matica zodpovednosti pre obstarávanie nového softvéru[1]

**Tabuľka č. 5: RACI matica pre kúpu nového SW**
[Zdroj: Vlastné spracovanie]

| činnosť / zodpovednosť | IT | ZAS/OÚ | CON |
|---|---|---|---|
| Vytvorenie a odovzdanie požiadavky | I | R | - |
| Prevzatie a evidovanie požiadavky | R | I | - |
| Posúdenie požiadavky | R | I | I |
| Zostavenie tímu | R | C | - |
| Analýza | R | C | - |
| Spracovanie návrhu riešenia | R | C | I |
| Posúdenie návrhu riešenia | R | C | C |
| Testovanie | C | R | - |
| Posúdenie testovanie | R | C | I |
| Zabezpečenie realizácie | R | C | - |
| Vytvorenie postupu realizácie | R | C | I |
| Realizácia | R | C | C |
| Zaistenie školenia | C | C | C |
| Evidencia SW | R | - | C |
| Posúdenie skúšobnej prevádzky | R | C | - |
| Údržba | R | C | - |
| Sledovanie prevádzky | R | C | - |

Zodpovednosť za Správu financií IT však nie je iba v kompetencii financií a účtovania IT, ale aj ostatných útvarov organizácie. Hlavný prínos tohto procesu je

[1] IT – IT oddelenie; ZAS – zastúpenie; OÚ – organizačný útvar; CON – riaditeľ controllingu; VED – vedenie spoločnosti; LOG – poverený pracovník z oddelenia logistiky

možné vidieť v jednoduchším, rýchlejším a dôkaznejším zostavovaniam rozpočtov útvaru podnikovej informatiky. Vďaka tomu tak môžu byť náklady na služby informačných technológií premietnuté do nákladov výrobkov a služieb poskytovateľa. Absencia procesu naopak znemožňuje kalkulovať skutočnú ziskovosť poskytovaných služieb. [14]

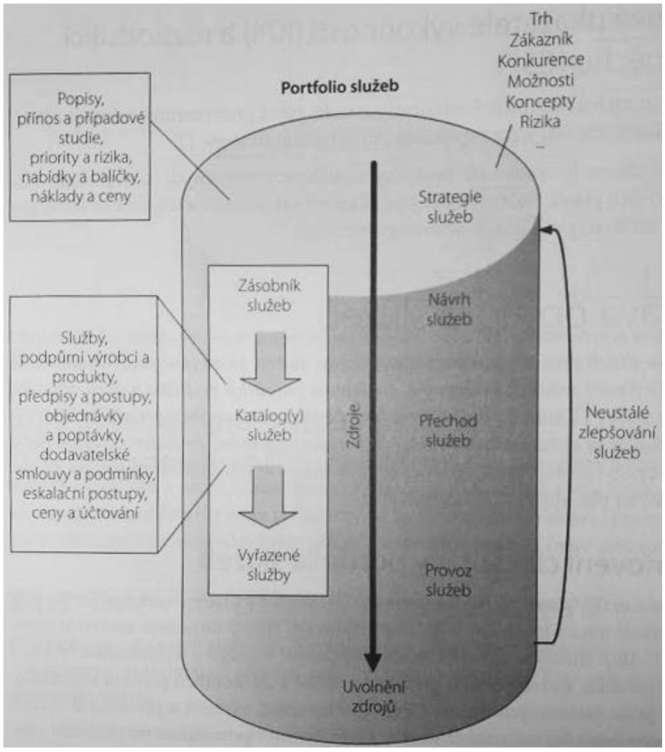
### 3. 1. 5 Správa portfólia služieb (Service Portfolio Management)

V rámci portfólia služieb sú zdokumentované všetky služby, ktoré poskytovateľ služieb IT navrhol, vyvinul vytvoril alebo už poskytoval. Portfólio služieb predstavuje ústrednú dokumentáciu a rozhodovaciu platformu pre prevádzku a rozvoj všetkých služieb. Tvorí zoznam všetkých služieb poskytovateľa, vrátane služieb, ktoré sú stále v štádiu plánovania či vývoja, tak aj služby, ktoré už boli zastavené (služby, ktoré neodpovedajú požiadavkám). Dáva odpovede na otázky:

- Ktoré služby IT má podnik poskytovať?
- Prečo by mal zákazník tieto služby využívať?
- Ako vyzerajú cenové modely pre tieto služby?

Správa portfólia služieb je strategickým procesom, ktorý pôsobí na všetky fázy životného cyklu, pretože s jej pomocou sa všetky služby po celú dobu ich životného cyklu riadia a spravujú.

Od tohto procesu sa odvíjajú strategické plánovanie celého portfólia služieb konkrétneho poskytovateľa, vrátane prideľovania zdrojov. Správa portfólia služieb zaisťuje, že poskytovateľ služieb disponuje správnou kombináciou služieb. Cieľom je rozpoznať, vytvoriť a prevádzkovať také služby, ktoré vyhovujú kritériám o zhode s obchodnou stratégiou a dohodnutou tvorbou hodnôt.




**Obrázok č. 11: Portfolio služieb**
[Zdroj: 3, s. 46]

Správa portfólia služieb funguje vo forme podobný Demingovmu PDCA cyklu:

1. Definície: dokumentácia a zhodnotenie požiadaviek
2. Analýza: do akej miery prispieva služby k zvýšeniu pridanej hodnote a optimalizácia medzi nákladmi na poskytnutie a vyvolaním služby. Obsahuje prípadovú štúdiu každej služby a investičnú analýzu.
3. Schválenie: Nastáva po overení prípadovej štúdiu a zaistení uskutočniteľnosti
4. Zámer

Jedná sa o kombináciu služieb vo vývoji pre rôzne typy zákazníkov a katalógu služieb, ktoré je jedinou časťou portfólia viditeľnou pre zákazníka. Katalóg služieb je podmnožinou portfólia a je pre zákazníka ukazovateľom, že daný poskytovateľ je schopný ponúkať služby. Jedná sa teda o nepretržitý proces, pozostávajúci z:

- definovania katalógových služieb, potvrdenia dát v portfóliách
- analýzy maximalizácie hodnoty portfólia a vyváženie dopytu a ponuky
- schválenie – dokončenie portfólia
- stanovenie – priradenie zdrojov a dohodnutých služieb, komunikácia rozhodnutí

### 3. 1. 6 Správa katalógu služieb (Serivce Catalogue Management)

Na rozdiel od správy portfolia služieb SCM riadi aktuálne ponúkané služby pre zákazníkov, ktoré môžu využiť. Katalóg služieb je podmnožinou portfólia a je pre zákazníka ukazovateľom, že daný poskytovateľ je schopný ponúkať služby. Umožňuje úseku businessu získať presný a konzistentný obraz o dostupnosti služieb, o ich detailoch a stavu. Jeho účelom je poskytnúť jediný ucelený zdroj informácií o všetkých dohodnutých službách tým osobám, ktoré majú k nemu povolený prístup.

### 3. 1. 7 Kľúčové úlohy a zodpovednosti

S realizáciou úspešnej vytvorenia oddelenia pre správu vzťahov s biznisom sú spájané špecifické úlohy a zodpovednosti.

Jedná sa o role:

**Business Relationship Manager** – ktorého úlohou je vytváranie vzťahu so zákazníkom na základe pochopenia jeho businessu.

**Product Manager** – ktorého hlavnou úlohou je zodpovedať za rozvoj a správu služieb počas životného cyklu a za produkčnú kapacitu podnikovej jednotky. Dôležitá je tiež spolupráca s Business Relationship Managerom v rámci výrobnej kapacity.

**Chief Sourcing Officer** – ktorý je zodpovedný za nasmerovanie a vedenie útvarov zdrojov a rozvíja tiež stratégiu zdrojov.

**Service Level Manager** – zodpovedný za dohodnutie a dosiahnutie požadovanej úrovne služieb.

**Supplier Manager** – zodpovedný predovšetkým za to, že za peniaze organizácia získa adekvátnu hodnotu od všetkých dodávateľov informačných technológií za súlad podporných zmlúv a dohôd s potrebami biznisu.

### 3. 1. 8 Odporúčanie

O1 – Vytvorenie funkcie pre riadenie obchodných vzťahov – znižovanie obchodných a IT bariér.

O2 – Zriadiť centrálne úložisko všetkých zmlúv pre každú službu IT.

O3 – Definovať zainteresované strany, portfólio zákazníkov, obchodné výsledky a spokojnosť zákazníkov.

O4 – Založenie zoznamu ponúkaných služieb – identifikácia služieb

O5 – Správa financií služieb IT – kvantifikovanie hodnoty služieb

## 3. 2 IT Strategy & Governance Europe

Vytvorenie tohto oddelenia slúži pre vyhodnotenie, smerovanie a efektívne, účinné a akceptovateľné využívanie IT a IT služieb v rámci organizácií. Zriaďuje štatutárne resp. vedúce orgány spoločnosti, dopĺňa koncept riadenia IT služieb o celkové fungovanie IT v organizácii a definuje ich kompetencie.

Hlbšie sa problematikou IT Governance zaoberá norma pre riadenie IT – ISO/IEC 38500:2015. Norma pokrýva vyššiu úroveň riadenia IT prostredia a služieb, vrátane manažmentu podnikových procesov a strategických cieľov organizácie.

### 3. 2. 1 Správa stratégie služieb IT (Strategy Management for IT services)

Tento proces definuje a stará sa o perspektívu, pozíciu, plán a vzorce chovania organizácie (podľa 4P stratégie služieb) vo vzťahu k službám a ich správe v organizácii IT. Tiež zaoberá misiou a víziou.

Cieľom tohto procesu je vytvoriť stratégiu služieb v súlade s celkovou obchodnou stratégiou. Popisuje ako poskytovateľ služieb prispôsobí svoju organizáciu k dosiahnutiu obchodných cieľov. Proces poskytuje rozhodujúci návod pre vytvorenie služby v podobe smerníc a plánov. Hľadajú sa odpovede na nasledujúce otázky:

- O ktoré časti trhu má podnik záujem?
- Aké sú priority pri investovaní?
- Ako môže najlepšie vytvoriť a prevádzkovať svoje služby?

Medzi vstupy patria už existujúce plány a stratégie, budúce požiadavky, audity a správy a taktiež sa jedná s dodávateľmi. Ako spúšťať tohto procesu slúži výročná plánovacia schôdza, nové obchodné možnosti, rozsiahle organizačné zmeny alebo zmeny v okolí.

Aktivity sa delia nasledovne:

- Strategické posúdenie (Strategic Assessment)
- Generovanie stratégie (Strategy Generation)
- Dodržiavanie stratégie (Strategy Execution)
- Meranie a vyhodnocovanie (Measurment and Evaluaton)
- Expanzia a rast (Expansion and Growth)

Výstup správy stratégie služieb IT pozostáva z aktualizovaných alebo nových pokynov, strategických a taktických plánov, vízií a úloh. Rovnako aj strategické požiadavky na nové služby alebo požiadavky na zmeny súčasných služieb. Tieto výstupy predstavujú podklady pre nasledujúce fázy životného cyklu služby a pre súvisiace procesy.

### 3. 2. 2 Kľúčové role a zodpovednosti

**Service Design Manager** - jeho zodpovednosť spočíva v celkovej koordinácii a rozšírenie kvalitných návrhov riešenia pre služby a procesy.

**IT Architect** - zodpovedný za koordináciu a zhodnotenie potrebných technológií, architektúr, návrhov a plánov.

### 3. 2. 3 Odporúčanie

O4 – ustanovenie IT Architecture Review Board (IT Management) – kladie si za cieľ definovať plán pre budúci rozvoj technologického prostredia, s prihliadnutím k stratégii služby a novo dostupných technológií.

O5 – ustanovenie poradného výboru pre IT technológie – členmi sú jednotliví vlastníci pre konkrétne služby, ktorí za ne zodpovedajú

## 3. 3 IT Service Management

Toto oddelenie zahŕňa služby, ktoré slúžia k udržovaniu stabilného stavu prevádzky IT.

### 3. 3. 1 Správa incidentov (Incident Management)

Poskytuje prvú pomoc a prípadne koordinuje ďalšie spracovanie následnými úrovňami podpory. Hlavným cieľom je čo najrýchlejšia obnova postihnutej služby pre návrat k normálnej prevádzke s minimálnymi negatívnymi dopadmi na prevádzku podniku.

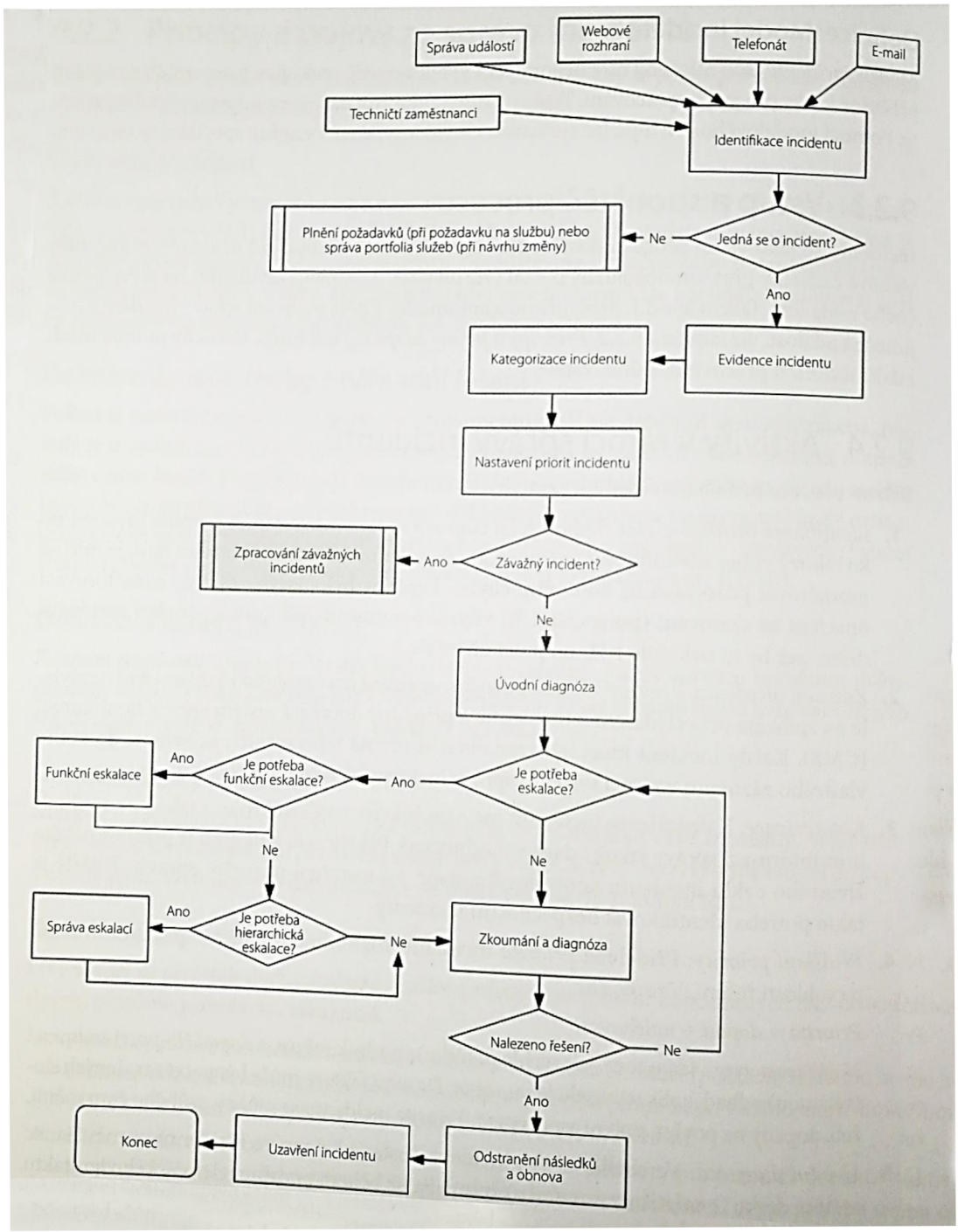
Zaisťuje, aby všetci zúčastnení v rámci aktivít procesu používali štandardizované metódy a postupy, zdieľanie incidentov podpore IT a zákazníkovi s cieľom zlepšiť tok informácií a udržanie, resp. zvýšenie, spokojnosti zákazníka pomocou kvality služieb IT.

Incidenty sa ako vstup procesu dostávajú k správe incidentov od užívateľov cez webové rozhranie cez samoobslužný portál, zavolaním/správou (e-mail) na service desk alebo priamo automaticky cez rozhranie správy incidentov

Medzi výsledky patrí predovšetkým obnovená služba a uzavretý, vyriešený incident. Patrí k nim aj pozitívna spätná väzba po informovaní zákazníka o ukončení.

Schopnosť rozpoznať incidenty a rýchle ich riešiť vedie k nízkym časom odstávky a k vyššej dostupnosti služby. Zásadný význam má schopnosť rozoznať dôležitosť aktivít IT pre podporu procesov, podnikových aktivít a vyvodiť z toho priority.

K rozhodujúcim faktorom úspechu procesu patria **ustanovenie service desk-u ako jediného kontaktného miesta** a záznamy všetkých incidentov.




**Obrázok č. 12: Proces správy incidentov**
[Zdroj: 3, s. 156]

### 3. 3. 2 Riadenie bezpečnostných incidentov v rámci IT

Riadiaci systém pre bezpečnostné incidenty v rámci IT

1. Bezpečnostný technik IT určí vedúcich pracovníkov zodpovedných za bezpečnostné incidenty v rámci IT ("vedúci pre bezpečnostné incidenty IT") a určí riadiaci systém pre reagovanie na tieto incidenty.

Riadenie bezpečnostných incidentov v rámci IT

1. Vedúci pre bezpečnostné incidenty musia predvídať vznik bezpečnostných incidentov a musí jasne zaviesť komunikačný plán a postupy na reakciu. Títo vedúci budú tiež tieto postupy pravidelne a včas preverovať. Medzi tieto postupy musia patriť nasledujúce:

1) Čo najvčasnejšie nahlásenie incidentu v súlade s komunikačným plánom. To isté platí pre hlásenie výsledkov opatrení reagujúcich na incident.

2) Stanovenie a analýza príčin incidentu.

3) Realizácia vhodných protiopatrení, vrátane opatrení, ktoré majú zabrániť opakovanému vzniku incidentu podľa závažnosti incidentu.

4) Zber a uchovanie protokolov z auditov a ďalších relevantných podkladov.

5) Zavedenie mechanizmov potrebných pre kvantifikáciu typu incidentu, jeho závažnosti a súvisiacich nákladov.

2. Vedúci pre bezpečnostné incidenty v rámci IT musia podať užívateľom nasledujúce pokyny, ktorými sa používatelia budú riadiť.

1) Dodržujte postupy stanovené v odseku 1 tohto článku vyššie, keď v oblasti IT vznikne bezpečnostný incident.

2) Buďte si stále vedomí slabín zabezpečenia IT a súvisiacich hrozieb. Pokiaľ si užívateľ všimne niečoho podozrivého, musí to okamžite hlásiť v súlade s komunikačným plánom.

3. Ak bola získaná certifikácia ISO / IEC 27001, je nutné realizovať riadenie reagujúce na incidenty v súlade s príslušnými normami, a to bez ohľadu na ustanovenia položky 1 a 2.

Uvedený postup zabezpečí, že:

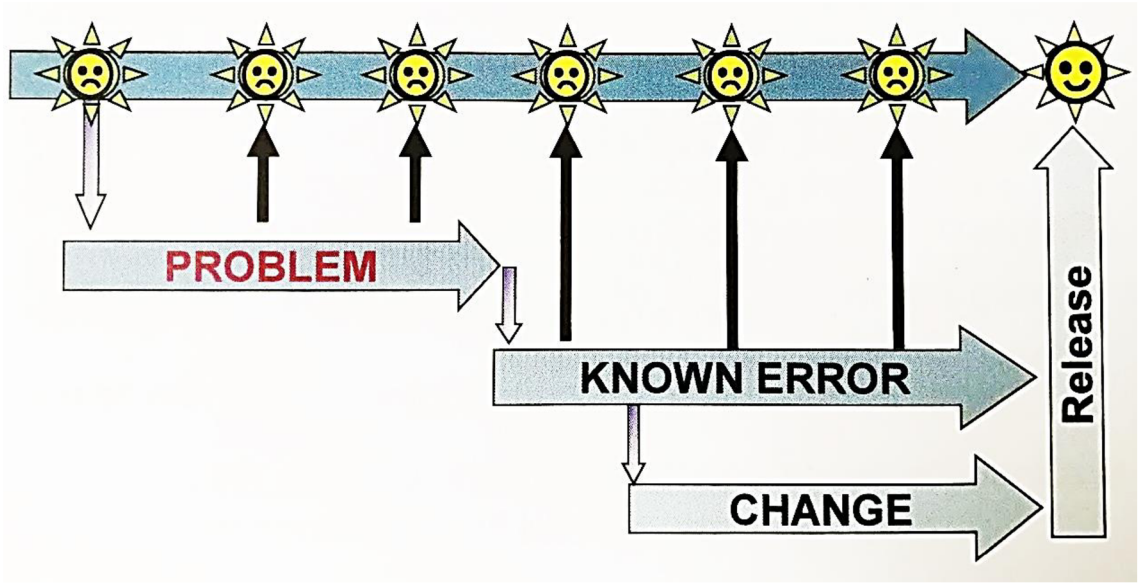
- vedenie organizácie bude o incidente informované,
- procesy ošetrovania bezpečnostných incidentov budú vopred stanovené,
- pre tieto procesy bude vopred určený a vyškolený okruh zodpovedných zamestnancov.

### 3. 3. 3 Správa problémov (Problem Management)

Správa problémov úzko súvisí so správou incidentov, keď spúšťačom procesu je najčastejšie jeden alebo viac incidentov. Následne správa problémov pomocou zisťovania a odstraňovania príčin sa odstraňujú opakujúce sa incidenty a minimalizujú sa dopady nevyhnutných incidentov. Známa príčina problému sa nazýva *známa chyba*, ktorá je zaznamenaná do databázy známych chýb (KEDB, Known Error Database), kde sa nachádzajú náhradné riešenia.

K rozhodujúcim faktorom úspechu procesu patria efektívny a účinný proces správy incidentov, odpovedajúca podpora nástrojov a prepojenie s ostatnými procesmi.

Cieľom je vytvoriť, čo najväčšiu databázu známych chýb a prejsť na proaktívne riadenie problémov, ktoré zaistí identifikáciu a vyriešenie problémov predtým ako nastane incident a identifikovať náchylné komponenty, resp. časti procesov, ktoré sú najčastejšie zodpovedné za vzniknuté incidenty a neskôr problémy.




**Obrázok č. 13: Procesy zmeny problému**
[Zdroj: 3, s. 157]

### 3. 3. 4 Správa aktív služieb a konfigurácie (Service asset & configuration management)

Proces zodpovedajúci za zabezpečenie, že aktíva požadované pre dodávku služieb sú správne riadené, a že o týchto aktívach sú k dispozícii presné a spoľahlivé informácie kedykoľvek a kdekoľvek sú potrebné. Tieto informácie zahŕňajú detaily o konfiguráciách aktív a o vzájomných vzťahoch medzi nimi.

Cieľom je identifikácia, kontrola, riadenie, dokladanie stavu, verifikácia a podávanie správ o službách a komponentoch infraštruktúry IT vrátane ich verzií

a atribútov. SACM poskytuje ostatným procesom logický model organizácie IT z hľadiska správy služieb IT.

Využíva systém správy konfigurácií (configuration management system, CMS) a konfiguračnú databázu (configuration management database, CMDB). CMS je súbor nástrojov, dát a informácií, ktorý slúži na podporu aktív služieb a správy konfigurácií. CMS je súčasťou celkového systému manažmentu znalostí služieb a zahŕňa nástroje pre zber, ukladanie, správu, aktualizáciu, analýzu a prezentáciu dát o všetkých konfiguračných položkách a ich vzťahoch. CMS tiež zahŕňa informácie o incidentoch, problémoch, známych chybách, atď. CMS je udržiavaný správou aktív služieb a konfiguráciou a je využívaný všetkými procesmi správy služieb IT.

CMDB je využívaná pre uloženie konfiguračných záznamov počas ich životného cyklu. Systém správy konfigurácií obsahuje jednu alebo viac konfiguračných databáz, a v každej databáze sú zaznamenané atribúty konfiguračných položiek a väzby s ďalšími konfiguračnými položkami.

Medzi správu aktív patrí aj správa softvérových aktív vrátane licencií. K hlavným činnostiam správy aktív prináleží aj riadené vyradenie aktív.

### 3. 3. 5 Správa bezpečnosti informácií (Information Security Management)

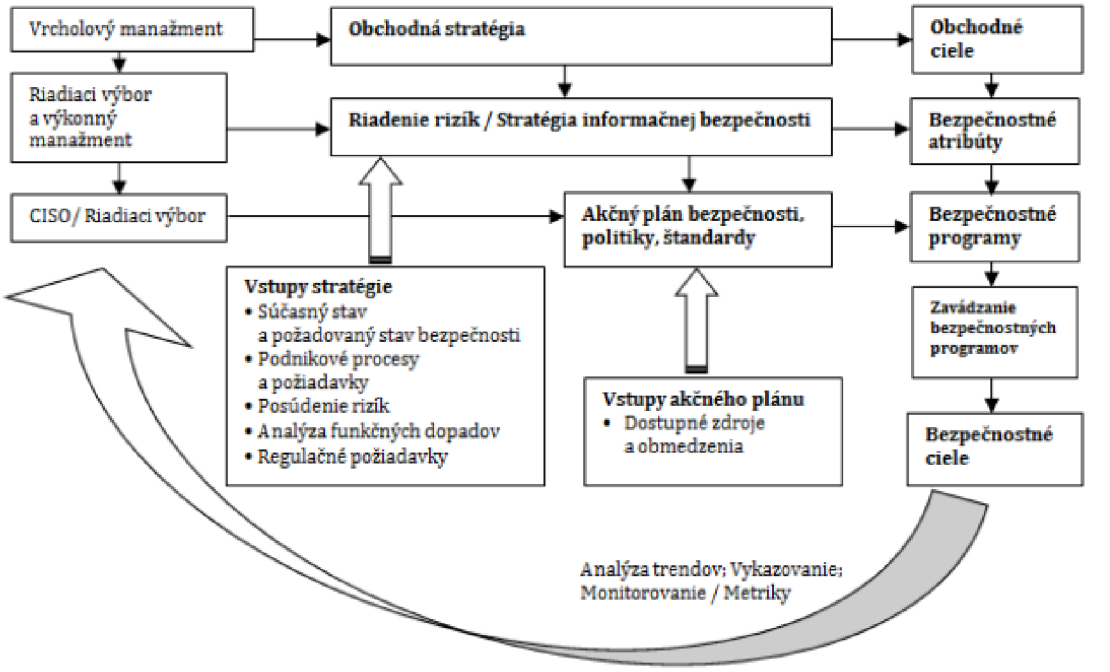
*„Vzhľadom na rastúce riziká a zvýšenie výdavkov na informačnú bezpečnosť, spolu s čoraz prísnejšími predpismi a rastúcimi záväzkami, je nevyhnutné, aby sa informačná bezpečnosť stala záležitosťou na prerokovanie na najvyššej organizačnej úrovni. Akonáhle vrcholový manažment a predstavenstvo pochopí požiadavky a výhody integrácie informačnej bezpečnosti do štruktúry riadenia organizácie, môžu sa pozerať na svoju budúcnosť v podnikaní s väčšou istotou. V súčasnej dobe je už nutnosťou pre vrcholový manažment integrovať informačnú bezpečnosť do celkového organizačného riadenia na najvyššej úrovni.“* [15]

Cieľom je vytvoriť a udržovať definovanú bezpečnosť informácií. Bezpečnosť IT sa pritom musí riadiť podľa podnikovej bezpečnosti. U aktív, informácií, dát a služieb IT ide o triádu CIA – dôvernosť, integrita a dostupnosť (Confidentiality, Integrity and Availability). Pre možnosť neustáleho hodnotenia a zlepšovania je dôležité nepretržité sledovanie bezpečnostných opatrení. To zahrňuje napríklad zachádzanie s prípadmi porušenia bezpečnosti, správu dodávateľov a **integráciu bezpečnostných aspektov do všetkých procesov ITSM.** Efektívna bezpečnosť vyžaduje aktívnu účasť vrcholového

manažmentu na posúdenie vznikajúcich hrozieb a poskytnutie silného vodcovstva v oblasti kybernetickej bezpečnosti. [16]

Nosnou súčasťou správy bezpečnosti informácií v podniku sa stáva funkčný certifikovaný systém riadenia bezpečnosti informácií (Information Security Management System – ISMS). Pre zosúladenie s osvedčenými postupmi z rámca ITIL je nutné použiť normu ČSN ISO/IEC 27013:2015 – Pokyn pre integrovanú implementáciu ISO/IEC 27001 a ISO/IEC 20000-1. [16]

Zladenie už existujúceho ISMS podľa ISO 27001 a chystaného ISO 20000-1 zabezpečí: spoločný slovník, spoločný audit, systém prepojených procesov či prepojený systém riadenia procesov. V konečnom dôsledku by to malo viesť k zvýšeniu účinnosti a efektívnosti systémov riadenia. [16]




**Obrázok č. 14: Konceptuálny rámec riadenia informačnej bezpečnosti**
[Zdroj: 15]

### 3. 3. 6 Zásady zachovania dôvernosti informácií a zaistenie ochrany dát

Používateľ berie na vedomie, že všetky informácie, ktoré získal alebo získa v súvislosti so svojou pracovnou činnosťou:

- Nesmie sprístupniť akejkoľvek tretej strane, ani ich nebude akýmkoľvek spôsobom bez právneho dôvodu a/alebo v rozpore s internými predpismi uchovávať, rozširovať, spracovávať, využívať či združovať s inými informáciami
- ďalej sa zaväzuje, že tieto informácie bez zbytočného odkladu odovzdá svojmu priamemu nadriadenému a v období, kedy bude s nimi sám nakladať, zabezpečí ich

dostatočnú ochranu pred akoukoľvek stratou, odcudzením, zničením, neoprávneným prístupom, náhodným či iným poškodením či iným neoprávneným používaním alebo spracovaním.

Povinnosťou zamestnanca je chrániť informácie tak, aby nemohli byť zneužité treťou stranou, ktorá nie je oprávnená pristupovať k daným informáciám.

Správca sleduje nové možnosti zabezpečenia informácií i nové hrozby a podniká potrebné opatrenia na zníženie hrozby straty informácií.

Správca informuje pracovníka o prípadných hrozbách straty informácií. Správca informuje zamestnancov o potrebách prijať opatrenia vedúce k zníženiu hrozby straty informácií.

Používanie, evidencia a zálohovanie médií s dátami kategórie dôverné je riešené zavedením riadeného systému zálohovania dát užívateľov na diskový priestor spoločnosti.

Vhodným podporným nástrojom je využitie služby ThreatGuard od spoločnosti Comguard, ktorý funguje ako virtuálny bezpečnostný analytik. Jeho cieľom je získavanie a systematizácia aktuálnych IT hrozieb. Služba vznikla na základe dopytu a záujmu zákazníkov. ThreatGuard zhromažďuje aktuálne hrozby a zraniteľnosti z overených zdrojov, vyhodnocuje ich relevantnosť a navrhuje nápravné riešenia.

Identifikácia hrozieb prebieha na základe rôznych kritérií, ako sú napríklad možnosť zneužitia, slabiny pre firemný segment, lokalizácia a dôraz na dôležité segmenty siete. S ohľadom na rastúce požiadavky na bezpečnosť a ochranu dát v oblasti IT je služba ThreatGuard vhodným nástrojom, ktorý ocenia najmä IT manažéri.

Ak chce manažment dosiahnuť významné zlepšenie bezpečnosti informácií, musí byť neoddeliteľnou súčasťou riadenia podniku. Informačná bezpečnosť sa musí posudzovať vo všetkých stratégiách riadenia a musí byť vrcholovým manažmentom uznaná ako rozhodujúci prispievateľ k úspechu.

Viac o ochrane osobných údajov s dôrazom na všeobecné nariadenie o chrane osobných údajov je popísané v samostatnej kapitole *Ohrana osobných údajov*.

### 3. 3. 7 Kľúčové role

**Security Manager** – zodpovedný za zabezpečenie súladu bezpečnostných informačných technológií s rizikami, dopady a požiadavkami dohodnutými v bezpečnostnej politike podnikania.

**Service Desk Manager** – V rámci riadenia incidentov je zodpovedný za kompletný priebeh procesu správy incidentov na všetkých úrovniach podpory, za spracovanie veľkých incidentov a prevádzkovú zodpovednosť za service desk.

### 3. 3. 8 Odporúčanie:

O6 – Zriadenie centrálneho service desk-u ako je ako jediného kontaktného miesta

O7 – Založenie databázy známych chýb

O8 – Vytvorenie konfiguračnej databázy a systém správy konfigurácií

O9 – Spravovanie aktív

O10 – Zosúladenie správy bezpečnosti ITIL s fungujúcim ISMS podľa normy ČSN ISO/IEC 27013.

## 3. 4 IT Infrastructure Management

Nasledujúce oddelenie si stanovilo za cieľ plánovať, vykonávať a riadiť služby s cieľom zabezpečiť včasné poskytovanie kvalitnej IT infraštruktúry z rozpočtu, rozsahu, podľa dohodnutých noriem a osvedčených postupov.

Služby riadenej infraštruktúry znižujú náklady a zvyšujú výkonnosť prostredníctvom technologických inovácií a zameranie na návrh vysoko kvalitných služieb. Umožňuje zostaviť plán optimalizácie infraštruktúry IT, ich prevádzky a priestorov. Ponúka prepojenie na jasne definované obchodné stratégie, ktoré možno sledovať po celú dobu životného cyklu.

### 3. 4. 1 Správa kapacít (Capacity Management)

Zaisťuje, aby kapacity služieb IT a infraštruktúry IT efektívnym spôsobom splňovali dohodnuté požiadavky týkajúce sa kapacít a výkonnosti. K cieľu správy kapacít patrí vytvorenie informačného systému správy kapacít (CMIS, Capacity Management Information System), kapacitný plán a prevádzanie proaktívnych meraní s cieľom zlepšiť výkonnosť.

Prekročenie stanovených prahových hodnôt alebo informácie z kontrolných hlásení sú hlavnými spúšťačmi tohto procesu.

- včasné naplánovanie dostatočnej kapacity IT k podpore nových alebo upravených požiadaviek
- identifikácia služieb IT a očividných pascí
- optimálne použitie hardvérových a softvérových komponentov

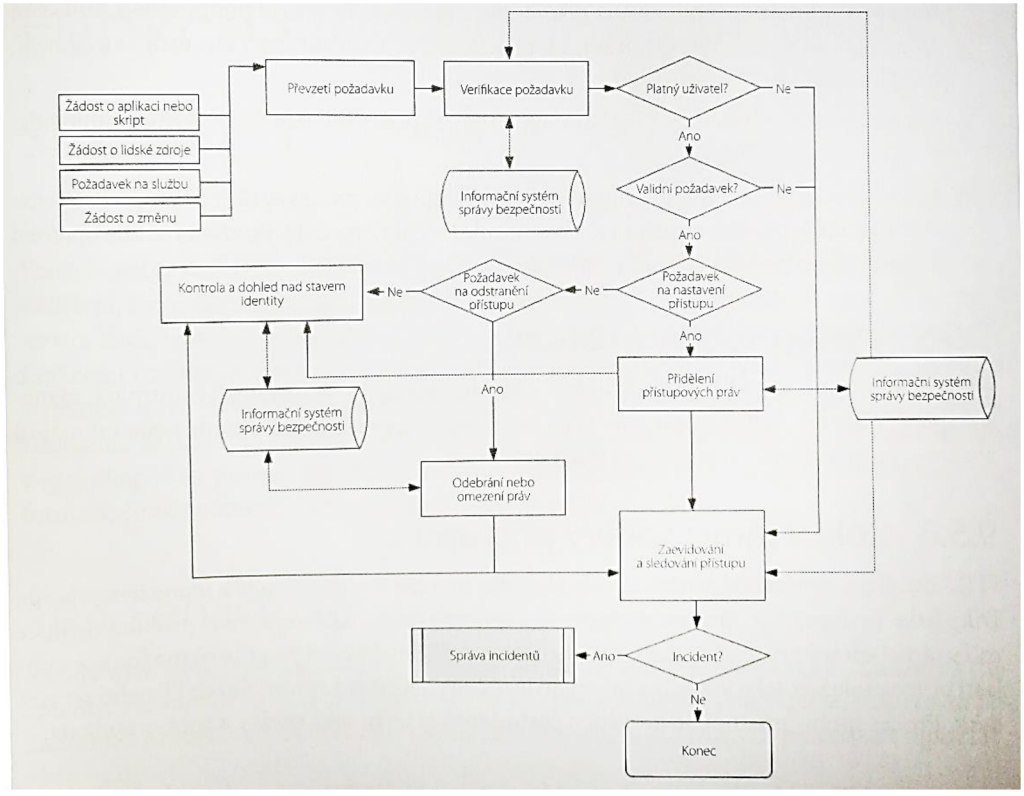
- predpoveď správania sa služieb IT pri danom objeme a rozdielnych formách použitia (simulácie a benchmarking)
- rieši úzke hrdlá (bottleneck) výkonnosti

### 3. 4. 2 Správa prístupu (Access Management)

Cieľom procesu je realizovať definovaný prístup na základe pravidiel a preddefinovaných akcií správy bezpečnosti informácii (*kapitola: Správa bezpečnosti informácií*). Jedná sa o účinnú reakciu na žiadosť o prístup k službám, o korektné zmeny prístupových práv alebo o ich obmedzenie.

- Žiadosť o pridelenie prístupových práv prostredníctvom service desk-u
- verifikácia
- poskytnutie práv
- kontrola a sledovanie stavu služby
- zaznamenanie a sledovanie prístupu
- odstránenie alebo obmedzenie prístupových práv

K rozhodujúcim faktorom úspechu procesu patria jasné úlohy zo strany správy bezpečnosti informácií, mechanizmy verifikácie, školení pracovníci a sledovanie aktuálnych prístupových práv. Je tak možné zaistiť, ktorý užívateľ má aké prístupové práva a kedy mu boli na základe nejakého schválenia alebo úlohy udelené.




**Obrázok č. 15: Zobrazenie procesu správy prístupov**
[Zdroj: 4, s. 167]

### 3. 4. 3 Správa dostupnosti (Availability Management)

Správa dostupnosti zaisťuje, aby služby odpovedali schválenej úrovni dostupnosti. Nezaoberá sa len meraním a udržaním celkovej dostupnosti, ale aj jej definíciou, plánovaním a implementáciou. Taktiež musí byť adekvátne navrhnutá infraštruktúra IT, procesy, nástroje a role k zaisteniu dostupnosti.

Hlavným cieľom je vytvorenie plánu dostupnosti, ktorý odráža súčasné i budúce obchodné požiadavky. Správa dostupnosti poskytuje pre podnik a IT pomoc a poradenstvo k všetkým relevantným aspektom dostupnosti, s ohľadom na dostupnosť služieb a výkonu, vrátane posúdenia zmien s ohľadom na ich dopad na dostupnosť.

Správa dostupnosti obsahuje reaktívne a proaktívne aktivity a ich výsledky bývajú zahrnuté do vhodného informačného systému správy dostupnosti (AMIS, Availability Management Information System), ktorý slúži ako úložisko relevantných informácií.
Reaktívne činnosti:

1. Monitorovanie, meranie, analýza a hlásenie dostupnosti
2. Analýza nedostupnosti a vyšetrovanie rušivých zásahov
3. Analýza výpadku služieb

Proaktívne činnosti:

1. Plánovanie a koncepcia nových alebo upravených služieb
    a. Zaistenie požiadaviek na dostupnosť
    b. Identifikácia životne dôležitých funkcií
    c. Návrh dostupnosti
    d. Modelovanie
2. Analýza rizík a správa bezpečnosti
    a. Implementácia protiopatrení
3. Kontrola nových a upravených služieb, dostupnosti a odolnosti proti výpadkom
4. Priebežné hodnotenie a zlepšovanie

Výsledkom procesu správy dostupnosti je napr. AMIS (Availability Management Information System), plán dostupnosti, kritéria dostupnosti a návrh obnovenia. Môže taktiež obsahovať plány testov a možnosti zlepšenia do budúcna.

### 3. 4. 4 Správa udalostí (Event Management)

Ponúka možnosť včasného odhalenia incidentov, dokonca aj problémov, niekedy aj ich príčinu. Identifikuje možné nasadenie automatizácie a tým znižuje časy výpadkov

a vďaka upozorneniam na odchýlky šetrí čas a náklady. Pre včasné zachytenie stavových informácií a vznikajúcich problémov sa odporúča začleniť správu udalostí do ostatných procesov prevádzky služby a súvisiacich procesov v životnom cykle služby (napr. správa incidentov, problémov, kapacity, dostupnosti alebo bezpečnosti informácií).

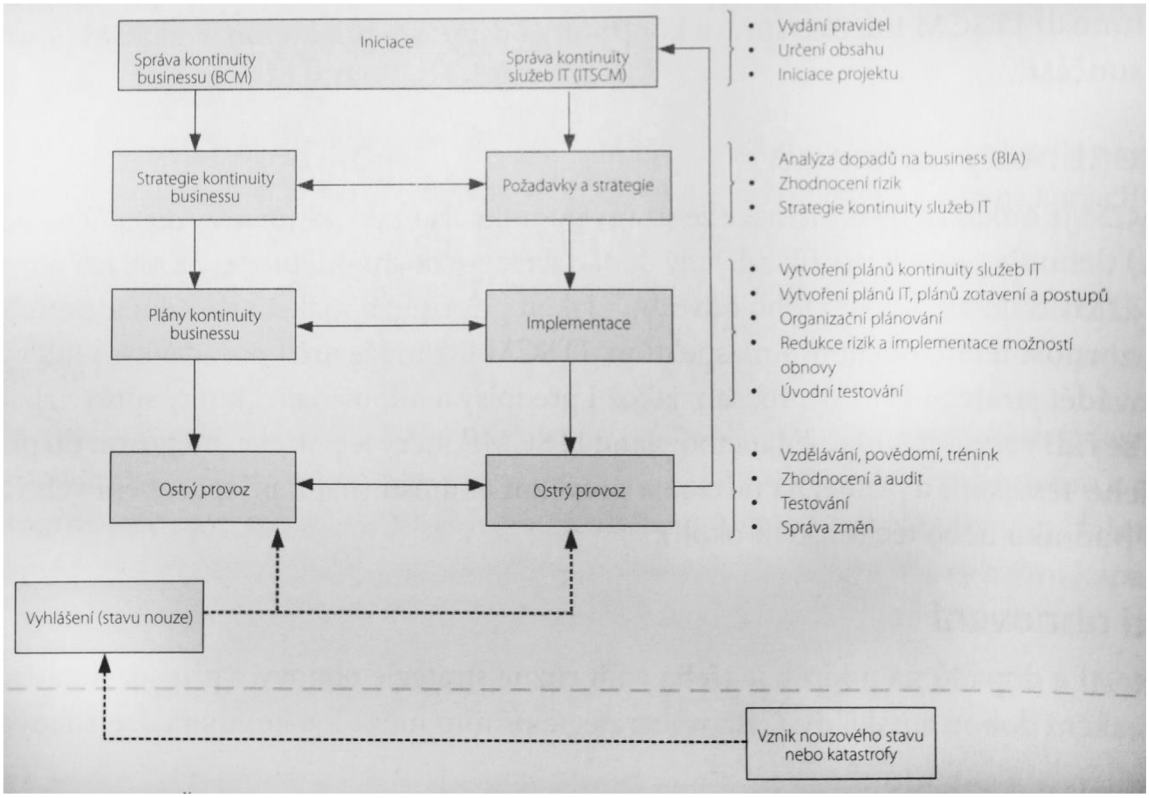
K rozhodujúcim faktorom úspechu procesu patria zaistenie komunikácie s relevantnými a definovanými funkčnými oblasťami s ohľadom na (pre nich) dôležité udalosti a overené, a schválené predpisy týkajúce sa korelačných a eskalačných postupov ako aj prevedenie odpovedajúcej konfigurácie alarmu.

### 3. 4. 5 Správa kontinuity služieb IT (IT Service Continuity Management)

Správa kontinuity služieb IT (ITSCM) podporuje technickú podporu pre správu kontinuity podniku (business continuity plan/management) a zaisťuje v prípade mimoriadnych udalostí alebo katastrof prežitie služieb a infraštruktúry IT, resp. podľa priorít ich obnovenia v určitom čase. Pre prežitie podniku sú kľúčovými odolné a vysoko dostupné služby IT, ktoré sú zabezpečené pomocou opatrení k zníženiu rizík, správou rizík a možnosťami obnovy.

Cieľom plánu kontinuity je brániť prerušeniu prevádzkových činností IT, chrániť kritické procesy pred následkami závažných zlyhaní a zaistiť včasnú obnovu činností.

K preventívnym opatreniam pre zamedzenie núdzových stavov a kritických situácií slúži prevencia a redukcia rizika na akceptovateľnú úroveň. Správa kontinuity služieb IT umožňuje udržania, čo najnižších dopadov na oblasť obchodu a rýchly návrat k normálnej prevádzke podľa SLA.

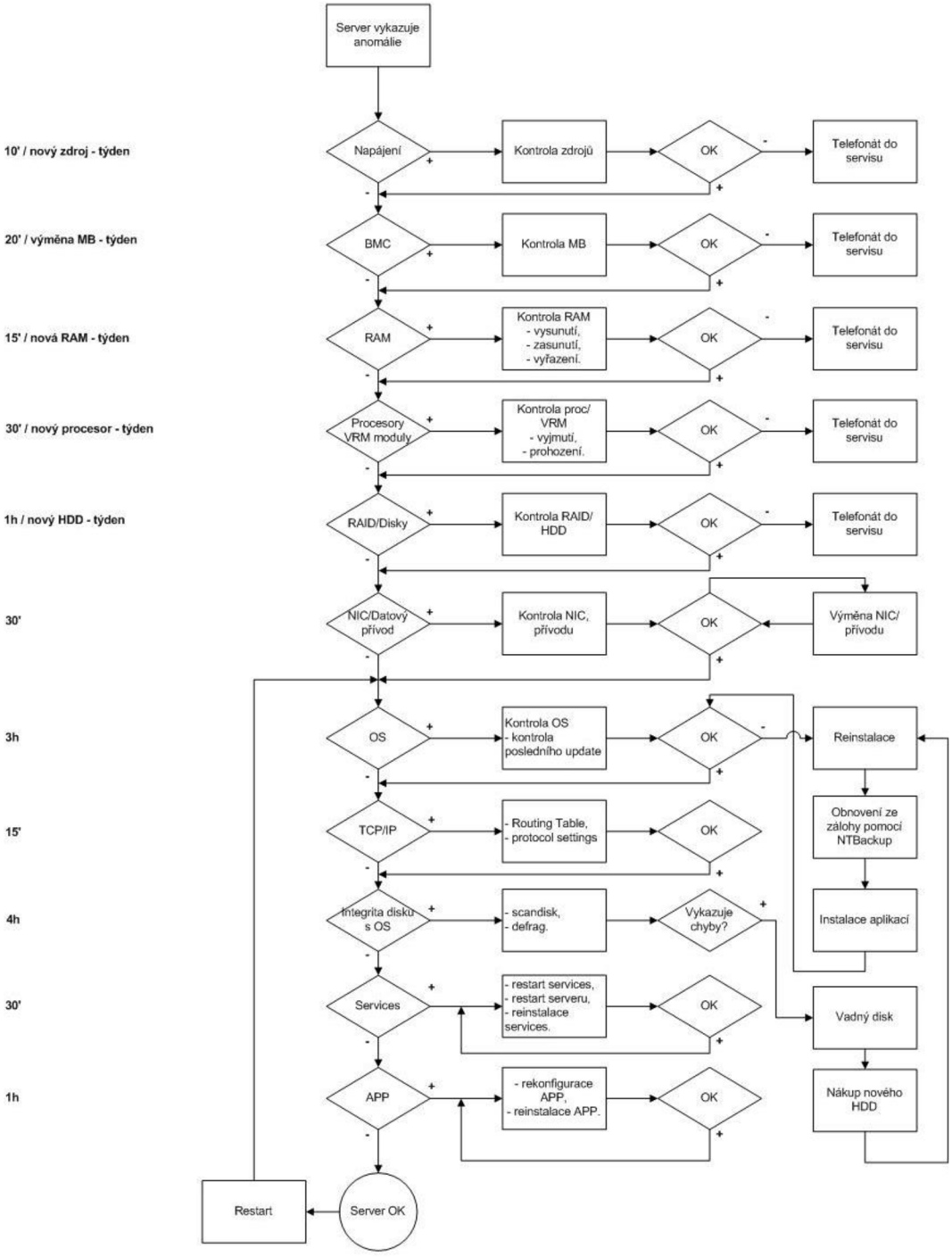



**Obrázok č. 16: Životný cyklus kontinuity služieb IT**
[Zdroj: 4, s. 96]

Správa kontinuity služieb IT funguje ako cyklický proces, ktorý sa skladá zo štyroch fáz.

1. Iniciácia: Špecifikuje sa pôsobnosť, rámcové podmienky a zodpovednosť ITSCM.
2. Požiadavky a stratégia: Požiadavky sú založené aj na výsledkoch BIA, ktoré kvantifikujú dopady na oblasť obchodu v prípade katastrof. O zavedenie možnosti obnovy sa neráta pre každú službu z dôvodu nákladnosti a preto je rozhodnutie založené aj na výsledkoch analýzy a správy rizík. Stratégia väčšinou obsahuje vyvážený pomer opatrení k zníženiu rizika a možností obnovy IT.
3. Implementácia: Implementácia opatrení pre zníženie rizík a možností obnovy a spolu s plánmi sa prevádza aj ich prvotné testovanie.
4. Bežná prevádzka: Zahŕňa revízie, audity a priebežné, resp. výročné, testovanie. Behom bežnej prevádzky je nevyhnutné udržiavať povedomie o postupoch, ktoré sa aktivujú v núdzových stavoch a taktiež je potrebné školiť zamestnancov.

Príklad postupu obnovenia funkčnosti serveru:




### 3. 4. 6 Kľúčové role

**Availability Manager** (manažer dostupnosti) – odpovědný za dosažení dohodnutých cílů dostupnosti u všech služeb.

**IT Service Continuity Manager** (manažer kontinuity služeb IT) – jeho odpovědnost spočívá v zajištění obnovy všech služeb v souladu s dohodnutými potřebami, požadavky a časovými plány businessu.

Capacity Manager (manažer kapacit) – odpovědný za dosažení souladu kapacity informačních technologií s dohodnutými a budoucími požadavky businessu.

### 3. 4. 7 Odporúčanie

O11 – Zriadenie informačného systému pre správu dostupnosti (AMIS) – obsahuje plán dostupnosti a monitoruje dostupnosť ostatných systémov a služieb.

O12 – Vytvorenie informačného systému pre správu kapacít (CMIS) – zaisťuje, aby kapacity služieb IT a infraštruktúry IT efektívnym spôsobom splňovali dohodnuté požiadavky týkajúce sa kapacít a výkonnosti s cieľom ich zlepšenia.

O13 – Sledovanie a zaznamenávanie poskytnutých a zamietnutých prístupov k službám.

O14 – Zriadenie AMIS, plánu dostupnosti a určenie kritérií dostupnosti.

O15 – Vytvárať záznamy udalostí, ktoré ukazujú na porušenie SLA alebo OLA a udalostí, ktoré poukazujú na ukončenie konkrétnej činnosti.

O16 - Vytvorenie scenárov obnovy každého zo spravovaných systémov v rôznych typoch krízových situácií (napr. nekonzistentné dáta v databáze).

O17 – Vytvorenie stratégie, pravidlá a schválené plány ITSCM

## 3. 5 Neustále zlepšovanie služieb (Continual Service Improvement)

Neustále zlepšovanie služieb je možné pojať z dvoch hľadísk – vylepšovanie a optimalizovanie služieb a podporných procesov pri zachovaní rovnakej ceny alebo poskytovanie rovnakej úrovne kvality pri nižších cenách. Zlepšovanie by nemalo byť náhodnou činnosťou. Rozhodnutie, čo zlepšiť a akým spôsobom, by malo byť vždy postavené na podložených tvrdeniach.

CSI dáva návod, ako môže organizácia riadiť proces zlepšovania svojej súčasnej pozície a porovnať ich s dlhodobými cieľmi pri súčasnom zachovaní vysokej kvality.

*„Čo nedokážeme definovať, nemôžeme merať.*
*Čo nedokážeme merať, nemôžeme kontrolovať.*
*Čo nedokážeme kontrolovať, nemôžeme riadiť.“*

### 3. 5. 1 Zlepšovací proces v siedmych krokoch

Týchto sedem krokov je nevyhnutných pre zber a analýzu dát, detegovanie problémov, návrh riešenia, jeho schválenie a implementáciu. Kroky musia byť v súlade so stratégiou

a prevádzkovými cieľmi spoločnosti. **Jedná sa o neustály proces, ktorý sa vracia späť na začiatok.**

1) Definícia toho, čo by sa malo merať
2) Definícia toho, čo je možné merať
3) Zhromaždenie dát – monitoring a zber dát zameraný na efektivitu služby, procesu a nástroja.
4) Spracovania dát
5) Analýza dát a odpoveď na otázku typu: Sú tu nejaké jasné trendy? Aké sú náklady?
6) Prezentácia a využitie informácií – informácie musia byť poskytnuté na správnej úrovni.
7) Implementácia nápravných akcií – získané znalosti sú využité pre zlepšenie služieb a procesov. [10]

### 3. 5. 2 Benchmarking

Meranie služieb definuje štyri základné dôvody pre monitorovanie a meranie služieb: potvrdenie predchádzajúcich rozhodnutí, smerovanie činností za účelom dosiahnutia stanovených cieľov, zdôvodnenie spôsobov realizácie, intervencia v správnom bode a realizácia nápravnej akcie.

Pre benchmarking musí existovať integrovaný rámec, ktorý zbiera dáta a podporuje ich vykazovanie. Medzi zbierané tipy metrík patria:

- Technologické metriky – založené na výkonnosti a dostupnosti
- Procesné metriky – získavanie vo forme kritických faktoroch úspechu
- Metriky služby – zamerané na užívateľa a výsledky služby z jeho pohľadu

### 3. 5. 3 Vykazovanie služby

IT oddelenie musí vykazovať skutočne dôležité informácie pre business. Musí byť schopné vysvetliť problémy, ktoré nastali a zaistiť nevyhnutné opatrenia, aby sa už daný problém neopakoval.

## 3. 6 Riadenie rizík

Táto kapitola nadväzuje na podkapitolu *Analýzy rizík* z kapitoly *Analýzy súčasného stavu.*

Akákoľvek organizácia, ktorá sa snaží o zvýšenie bezpečnosti, by sa mala zaoberať stratégiou riadenia rizík vhodnou pre dané prostredie a schopnou poukazovať na riziká efektívnym spôsobom. Je potrebné prijať stratégiu, ktorá by smerovala svoje úsilie na zvýšenie bezpečnosti tam, kde je to potrebné a kde to prináša lacný a časovo efektívny prístup.

### 3. 6. 1 Proces posudzovania rizík

1) Kritériá akceptácie rizika - zahrnuté do analýzy rizík pre daný kalendárny rok vrátane stupnice.

2) Kritériá pre hodnotenie rizík bezpečnosti informácií

a) Riziká sú priebežne posudzovaná BM, v prípade výskytu nového rizika alebo opakovania sa existujúceho rizika, zvoláva BM bezpečnostnú poradu za prítomnosti ďalších pracovníkov podľa charakteru rizika (správca, vlastníci rizík a pod.) a prijímajú príslušné opatrenia.

b) Kritériá na posudzovanie rizík sú dané číselnými stupnicami v stĺpcoch "reálna pravdepodobnosť výskytu rizika" a "úroveň rizika / kritérium pre akceptáciu rizika" u analýzy rizík.

U reálnej pravdepodobnosti výskytu rizika sa jedná o túto stupnici:

1 nízka = nikdy sa nevyskytlo alebo iba 1x za 12 mesiacov.

2 stredne vysoká = riziko sa vyskytlo opakovane 2x za 12 mesiacov.

3 vysoká = riziko sa vyskytlo opakovane 3x a viackrát za 12 mesiacov.

U úrovne rizika (kritériá pre akceptáciu rizika) sa jedná o túto stupnicu:

1 nízka = nie je potrebné zatiaľ riešiť.

2 stredne vysoká = priebežne sledovať, tiež zatiaľ nie je potrebné riešiť.

3 vysoká = je potrebné prijať opatrenia na zníženie rizika a ošetriť riziko.

Potom je vykonaný súčin hodnoty reálne pravdepodobnosti výskytu rizika a úrovne rizika:

do 5 = nie je potrebné prijímať opatrenia v pláne ošetrení rizík.

6-7 = vždy je nutné prijať opatrenia na zníženie rizika v pláne ošetrenie rizík, v prípade dosiahnutia týchto hodnôt musí byť v rámci porady KAC oddelenia prerokované návrhy

na opatrenia na zníženie hodnoty týchto rizík, na najbližšej porade – po skončení kvartáli – bude opatrenie preskúmané, či došlo k zníženiu rizika.
8-9 = vždy je nutné prijať opatrenia na zníženie rizika v pláne ošetrenie rizík, v prípade dosiahnutia týchto hodnôt musí BM prijať opatrenia najneskôr do piatich pracovných dní od vzniku rizika, v rámci najbližšej porady je posúdené, či došlo k zníženiu riziko vhodným prijatím opatrení. Pokiaľ nedošlo k zníženiu rizika alebo bolo naopak zvýšené, musia byť ihneď navrhnuté iné vhodnejšie opatrenia, ktoré bude vyhodnotené opäť do piatich pracovných dní. Pokiaľ došlo k zníženiu rizika do kategórie 6-7, bude postupované naďalej podľa tejto kategórie.

c) V analýze rizík sú zahrnuté iba riziká, ktoré môžu skutočne nastať, nezahrnujeme sem riziká s najväčšou pravdepodobnosťou nereálne. V spoločnosti sú identifikované riziká spojené so stratou dôvernosti, integrity a dostupnosti informácií v rozsahu systéme riadenia bezpečnosti informácií vrátane ich vlastníkov - časť analýzy rizík.

Pri spracovávaní analýzy rizík posudzujeme potenciálne následky, ktoré by nastali, ak by sa riziká realizovali, posudzujeme reálnu pravdepodobnosť výskytu rizík a úroveň rizika s prihliadnutím k interným a externým aspektom.

Výsledky analýzy rizík už obsahujú kritériá na akceptáciu a pre hodnotenie rizík. Stanovujeme priority pre ošetrenie rizika u analyzovaných rizík. Riziká, u ktorých je násobok hodnoty reálnej pravdepodobnosti výskytu rizika a úrovne rizika dosiahne hodnotu 6-9, presúvame do plánu na ošetrenie rizík, kde prijímame vhodné opatrenia na zníženie rizika.

Opakované posúdenie rizík bezpečnosti informácií produkujú konzistentné, opodstatnené a porovnateľné výsledky.

### 3. 6. 2 Proces ošetrenia rizík bezpečnosti informácií

Podľa charakteru rizika sú vyberané varianty pre jeho ošetrenie a ďalej sú určované všetky opatrenia potrebné na implementáciu vybranej varianty pre ošetrenie daného rizika. Riziká sú ošetrované za cieľom zníženia ich zníženia. Využívané sú priame opatrenia (napr.: obnova HW, nasadenie antivírusových programov a pod.) alebo nepriame (napr.: prenesenie rizika na inú osobu, školenia a pod.).
V nadväznosti na analýzu rizík je vytvorený a pravidelne aktualizovaný plán ošetrenia rizík bezpečnosti informácií vrátane súhlasu vlastníkov rizík ohľadom tohto plánu a prijatie zvyškových rizík bezpečnosti informácií.

### 3. 6. 3.Plán ošetrenia rizík

Pre známe riziká z kapitoly *Analýza rizík* je odporúčaný nasledovný plán pre ošetrenie týchto rizík:

**Tabuľka č. 6: Plán ošetrenia rizík**
[Zdroj: Vlastné spracovanie]

| Riziko k ošetreniu | Varianty k ošetreniu rizika | Poznámka |
|---|---|---|
| prezradenie dôverných informácií zamestnancom na verejnosť | doplnenie bezpečnostného povedomia u všetkých zamestnancoch | prebehne test znalostí každé dva mesiace (naposledy 10. 4. 2018) |
| | podľa rosahu a charakteru prezradenia informácií možno zahájiť okamžité prepustenie zamestnanca | nedošlo k žiadnemu prepusteniu zamestnanca |
| nekvalitne prevedená práca zamestnancom | doplnenie bezpečnostného povedomia u všetkých zamestnancoch | prebehne test znalostí každé dva mesiace (naposledy 10. 4. 2018) |
| | podľa rosahu a charakteru nekvalitne prevedenej práce finančný postih v súlade s platnou legislatívou | nebolo nutné dávať žiadny finančný postih pre zamestnanca |
| nekvalitne prevedená práca externým dodávateľom | výmena externého dodávateľa | nebolo nutné meniť žiadneho externého dodávateľa |
| zneužitie informácií spoločnosti v dôsledku nedodržania pravidiel prázdneho stolu a prázdnej obrazovky | doplnenie bezpečnostného povedomia u všetkých zamestnancoch | prebehne test znalostí každé dva mesiace (naposledy 10. 4. 2018) |
| | prevádzanie pravidelných týždenných kontrol dodržiavania pravidiel prázdneho stolu a prázdnej obrazovky | záznamy v information security incident book |
| zneužitie prístupu do systémov spoločnosti v dôsledku nedodržania pravidiel prázdneho stolu a prázdnej obrazovky | doplnenie bezpečnostného povedomia u všetkých zamestnancoch | prebehne test znalostí každé dva mesiace (naposledy 10. 4. 2018) |
| | prevádzanie pravidelných týždenných kontrol dodržiavania pravidiel prázdneho stolu a prázdnej obrazovky | záznamy v information security incident book |

## 3. 7 Ochrana osobných údajov

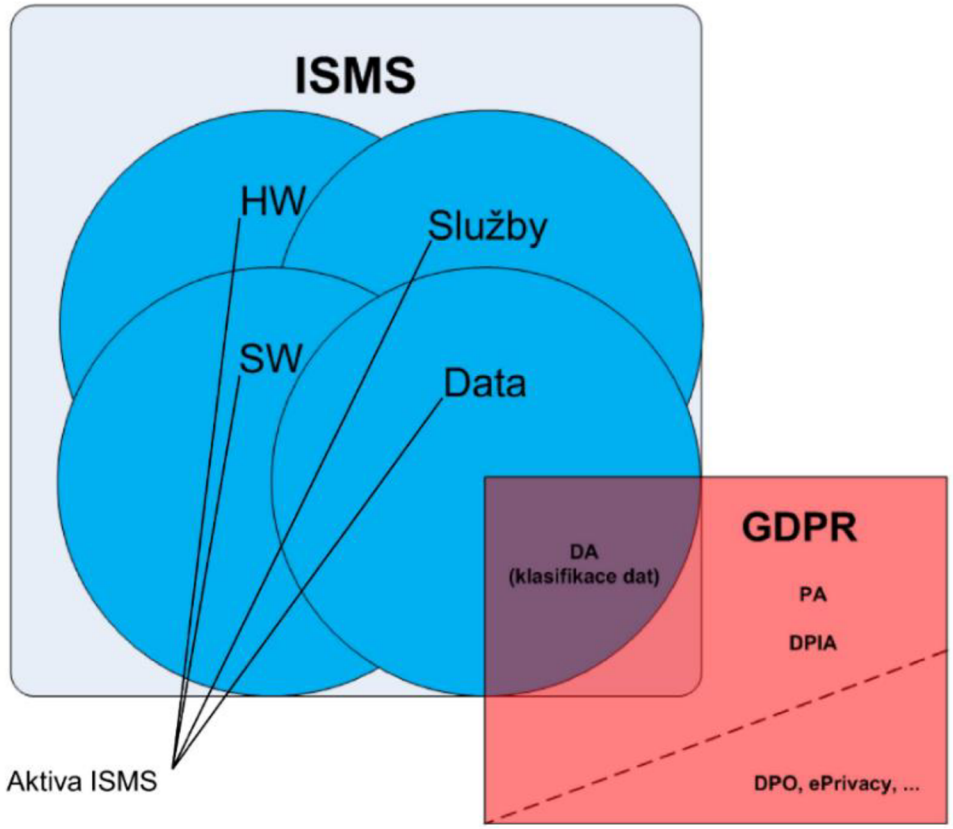
Dňa 25. 5. 2018 začne platiť Všeobecné nariadenie o ochrane osobných údajov (General Data Protection Regulation, GDPR), ktoré bolo schválené bolo 27.4.2016. Platiť bude bez výnimky pre všetky európske firmy, inštitúcie či online služby. Cieľom GDPR je dať ľuďom viac kontroly nad tým, ako sa zachádza s ich osobnými údajmi, zvýšiť samotnú úroveň ochrany a posilniť práva občanov Európskej Únie.

Pre firmy to znamená, že budú musieť aktualizovať informačné systémy, weby, archaické zaznamenávanie v tabuľkách atď. a zrevidovať procesy, pri ktorých manipulujú s citlivými údajmi zákazníkov.

**Súhlas so spracovaním údajov musí byť konkrétny, slobodný, jednoznačný, preukázateľný a ničím nepodmienený.** Prístup k citlivým údajom môžu mať len osoby, ktoré s nimi naozaj majú pracovať a len na dobu, počas ktorej existuje dôvod na ich spracovanie.

Občan EU získava tzv. „právo na zabudnutie“, aby požiadal o preverenie toho, čo o ňom spoločnosť eviduje a následne má právo na obmedzenie rozsahu spracovaných údajov a vymazanie týchto údajov, pokiaľ sa s nimi aktívne nepracuje, napr.: trestnoprávny proces, prenajatá služba (tarif od mobilného operátora).

Ak prevádzkovateľ spracúvajúci osobné údaje príde na porušenie ich ochrany, ktoré môže predstavovať riziko pre dotknuté osoby, musí o tom informovať Úrad na ochranu osobných údajov do 72 hodín od zistenia úniku. Následne musí opísať povahu úniku, jeho pravdepodobné následky a **prijať nápravné oprávnenia na zmiernenie dopadov**.




**Obrázok č. 17: Zaradenie GDPR v ISMS**
[Zdroj: 2]

### 3. 7. 1 Postup pri zavádzaní GDPR

Samotný postup sa dá zhrnúť do šiestich krokov, resp. blokov, z ktorých posledné dva kroky sú najpodstatnejšie, pretože sa musia vykonávať neustále a celý postup sa musí cyklicky opakovať podľa vzoru PDCA cyklu. Je to nikdy nekončiaci dynamicky samoučiaci sa cyklus.

1) Analýza a príprava plánu opatrení (asistovaná zhodnotenie, zistenie súčasného stavu a dátová analýza a klasifikácia dát)
2) Posúdenie vplyvu na ochranu osobných údajov (dopadová analýza)
3) Zmena procesov na dosiahnutie súladu s GDPR (procesná analýza, priradenie klasifikovaných dát užívateľom)
4) Tvorba orgánov na dodržiavanie zásad GDPR (zriadenie pozície DPO)
5) Kontrola dodržiavania zásad GDPR a hlásenie incidentov
6) Opakované testy bezpečnosti a aktualizácia predpisov (školenie zamestnancov podľa metodiky SAE)

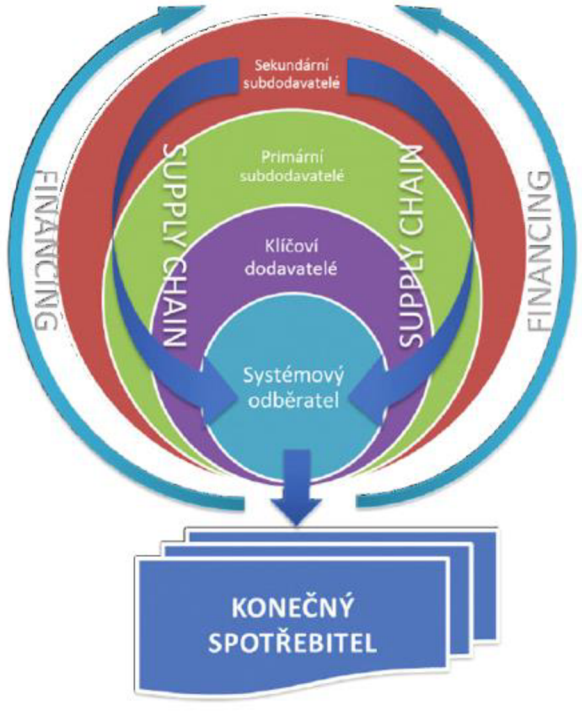
### 3. 7. 2 Realizácia DPO

Zmocnenec pre ochranu osobných údajov (Data Protection Officer, DPO) je osoba zodpovedná za školenie a zavedenie opatrení, kontaktná osoba v organizácií pre požiadavky na právne znalosti. DPO môže existovať v dvoch modeloch. Buď ako právne znalá osoba s podporou tretej strany, ktorá poskytuje technické zázemie (osoba s certifikátom ISMS) alebo osoba technicky zdatná v odbore ICT s podporou tretej strany, ktorá poskytuje právne zázemie.

### 3. 7. 3 Reťazec dôvery

Potrebné je upraviť zmluvy v oblasti dodávateľsko-odberateľských vzťahov, tak aby vznikol kompletný reťazec dôvery, ktorý schvaluje každú dodávateľsko-odberateľskú entitu, počnúc od miesta, kde sa zaznamenávajú osobné údaje, cez to, ako sa prenášajú, kto ich spracúva a ako sa zhromažďujú alebo archivujú. Okrem iného vyžaduje aj evidenciu a spracovanie jednotlivých účtovných dokladov a údajov na nich uvedených. [18]

Vďaka nasadeniu reťazca dôvery bude možné zaistiť dôveryhodnosť získaných záznamov a kontrolu pravosti dát počas ich životného cyklu. V každej úrovni budú overené údaje.




**Obrázok č. 18: Odberateľsko-dodávateľský reťazec**
[Zdroj: 19]

### 3. 7. 4 Rady pre spoločnosť

Značná časť príjmov spoločnosti pochádza zo zákaziek dodávateľa zariadení na tlač, skenovanie a spracovanie dokumentov. Preto je nevyhnutné, aby procesy spojené so životným cyklom dokumentov spĺňali nasledujúce kritéria:

- Zabezpečená tlač a vyzdvihnutie vytlačených dokumentov možné výhradne po autentizácií cez prihlasovacími údajmi alebo cez čipovú kartu
- Mať možnosť bezpečného mazania pevného disku v tlačiarni a časovo definované zmazanie tlačených súborov
- Bezpečné ukladanie skenovaných úloh a zabezpečenie obsahu skenovaných súborov
- Bezpečné uchovávanie vytlačených dokumentov s osobnými údajmi
- Bezpečné skartovanie či iný spôsob likvidácie tlačených dokumentov s osobnými údajmi
- Zmapovať kompletný dodávateľsko-odberateľský reťazec za účelom vytvorenia reťazca dôvery

## 3. 8 Súhrn odporúčaní

O1 – Vytvorenie funkcie pre riadenie obchodných vzťahov – znižovanie obchodných a IT bariér

O2 – Zriadiť centrálne úložisko všetkých zmlúv pre každú službu IT

O3 – Definovať zainteresované strany, portfólio zákazníkov, obchodné výsledky a spokojnosť zákazníkov

O4 – Založenie zoznamu ponúkaných služieb – identifikácia služieb

O5 – Správa financií služieb IT – kvantifikovanie hodnoty služieb

O6 – Zriadenie centrálneho service desk-u ako je ako jediného kontaktného miesta

O7 – Založenie databázy známych chýb

O8 – Vytvorenie konfiguračnej databázy a systém správy konfigurácií

O9 – Spravovanie aktív

O10 – Zosúladenie správy bezpečnosti ITIL s fungujúcim ISMS podľa normy ČSN ISO/IEC 27013

O11 – Zriadenie informačného systému pre správu dostupnosti (AMIS) – obsahuje plán dostupnosti a monitoruje dostupnosť ostatných systémov a služieb.

O12 – Vytvorenie informačného systému pre správu kapacít (CMIS) – zaisťuje, aby kapacity služieb IT a infraštruktúry IT efektívnym spôsobom splňovali dohodnuté požiadavky týkajúce sa kapacít a výkonnosti s cieľom ich zlepšenia.
O13 – Sledovanie a zaznamenávanie poskytnutých a zamietnutých prístupov k službám.
O14 – Zriadenie AMIS, plánu dostupnosti a určenie kritérií dostupnosti.
O15 – Vytvárať záznamy udalostí, ktoré ukazujú na porušenie SLA alebo OLA a udalostí, ktoré poukazujú na ukončenie konkrétnej činnosti.
O16 - Vytvorenie scenárov obnovy každého zo spravovaných systémov v rôznych typoch krízových situácií (napr. nekonzistentné dáta v databáze).
O17 – Vytvorenie stratégie, pravidlá a schválené plány ITSCM

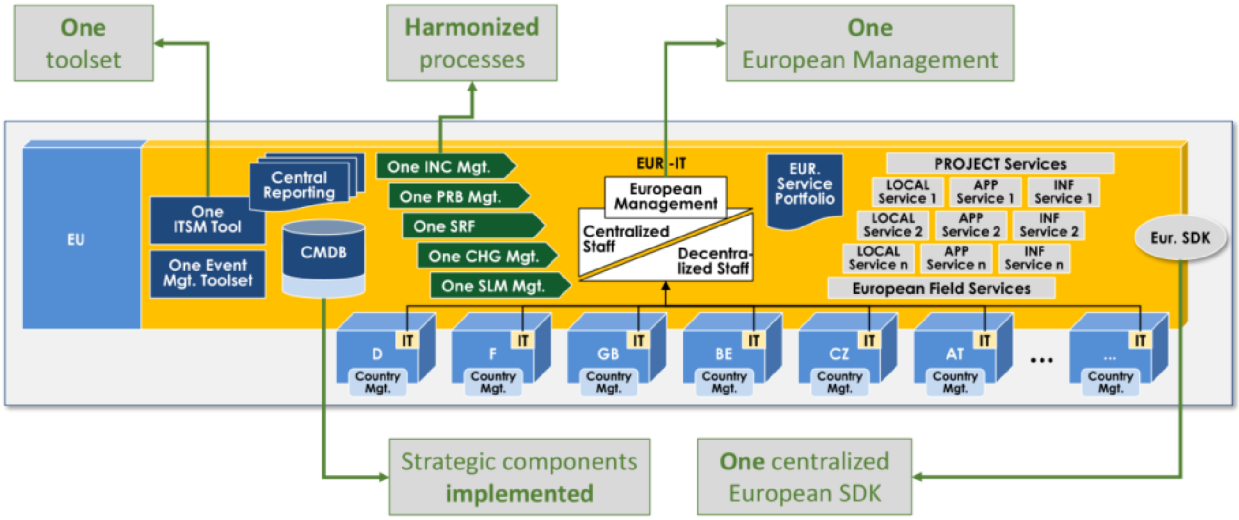
### 3. 8. 1 Odporúčané použitie podporných nástrojov

Krátky zoznam odporúčaných produktov, resp. softvérov, ktoré sa používajú na podporu správy procesov, ktoré boli spomenuté v predchádzajúcich kapitolách.

Celková správa služieb – K2: Workflow
Správa aktív služieb a konfigurácie – Flexera: IT Asset Management
Service Desk – BMC: Remedy Service Desk
Konfiguračná databáza – BMC: CMDB
Komunikácia – Microsoft: Skype for Business
Správa bezpečnosti informácií – Comguard ThreatGuard

## 3. 9 Konečný stav

Vďaka adaptácií rámca ITIL pre riadenie IT služieb a zjednotení viacerých krajinných oddelení IT do jedného európskeho oddelenia IT, sme dosiahli ucelené riadenie IT služieb v rámci všetkých krajín Európy.

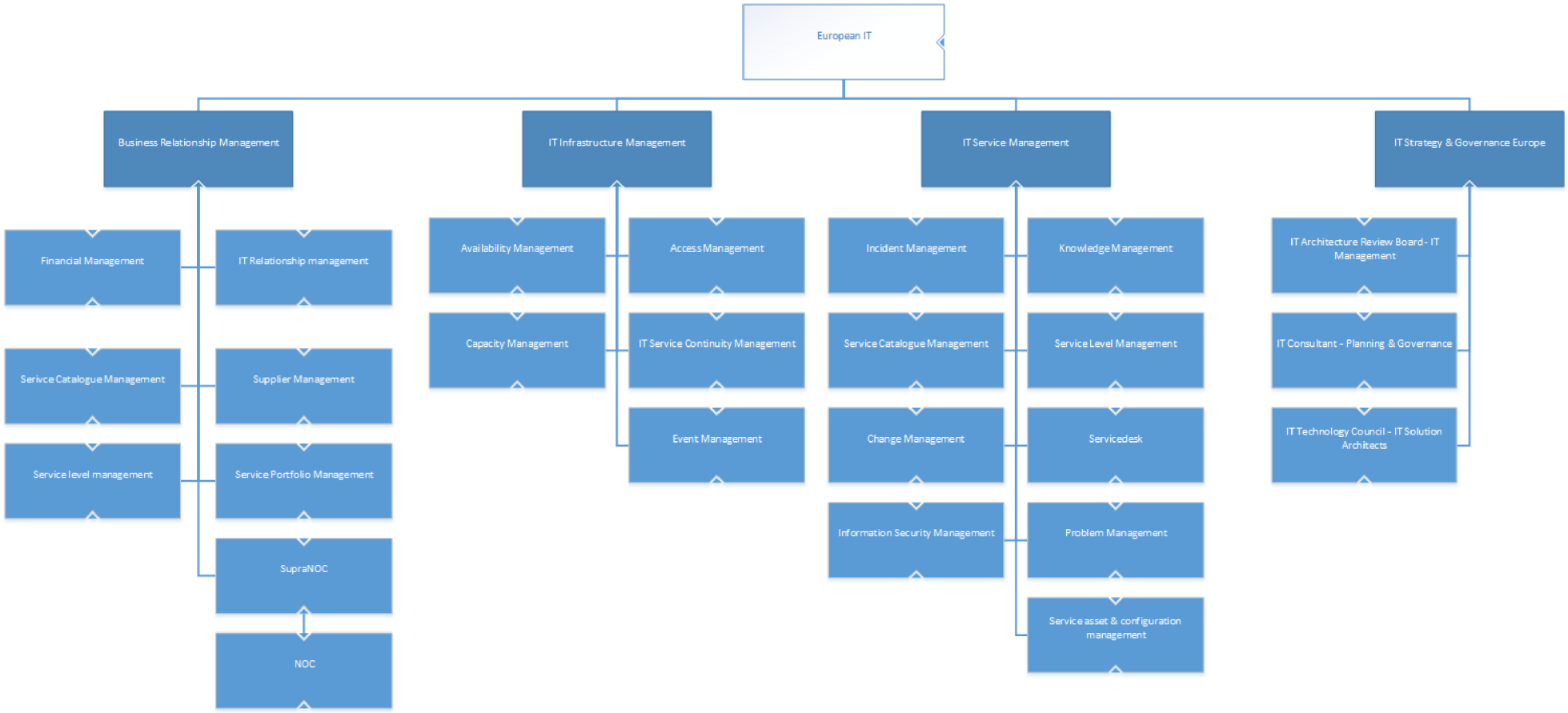



**Obrázok č. 19: Konečný stav**
[Zdroj: Vlastné spracovanie]

### 3. 9. 1 Organizačné zmeny

Po rozdelení do jednotlivých činností a začlenení ďalších pobočiek z ostatných krajín Európy vzniklo viacero samostatných oddelení a tímov, v ktorých sú zreteľne definované riziká, zodpovednosť a, predovšetkým, **určenie rolí vlastníka a správcu jednotlivých procesov.**

Organizačný diagram sa nachádza na nasledujúcej strane.




**Obrázok č. 20: Nová organizačná štruktúra**
[Zdroj: Vlastné spracovanie]

# 4 Zhodnotenie a prínosy práce

Zavedenie systému riadenia IT služieb prináša predovšetkým výhody v optimalizácií týchto služieb a možnosť ich neustáleho zlepšovania, resp. ponúkania rovnako kvalitnej služby s nižšími prevádzkovými nákladmi. Okrem toho boli zjednotené IT oddelenia zjednotené do jedného celoeurópskeho IT oddelenia, ktoré ponúka ucelené riadenie na všetkých vrstvách managementu a zosúladené procesy s možnosťou lepšej zastupiteľnosti členov tímov inými zamestnancami, ktorí majú na starosti tie isté aktivity v inej krajine.

Vzhľadom na blížiace sa všeobecné nariadenie o ochrane osobných údajov boli navrhnuté príslušné opatrenia vrátane zapojenia reťazca dôvery s dodávateľsko-odberateľským vzťahom. Navrhnutím bezpečnostných opatrení a odporúčaní dôjde k súladu s GDPR.

- Lepšia produktivita práce, využívanie a zdieľanie vedomostí v rámci oddelenia
- Lepšia konkurencieschopnosť spoločnosti
- spokojnejší zákazníci
- Zlepšenie komunikačných tokov v rámci organizácie
- Eliminácia zbytočnej práce jednotlivých zamestnancov
- Lepšie využitie ľudských zdrojov
- Vytvorenie reťazca dôvery

## 4. 1 Ekonomické zhodnotenie

Navrhované odporúčania a celkový návrh riešenia sa týkajú predovšetkým procesného fungovania, začlenenia súčasných zamestnancov do nového projektu, organizačných zmien v zmysle prerozdeľovania zamestnancov do tímov a iných oddelení a nie znižovania počtu zamestnancov. Preto jasná kvantifikácia – vyčíslenie nákladov a prínosov implementácie zmien – je trochu problematická. Finančné prostriedky nie sú priamo produkované. Celý návrh zmien je podporným prostriedkom pre zlepšenie chodu oddelenia.

Avšak, je možné približne určiť mzdové náklady spojené s projektom podľa toho, koľko zamestnancov sa ho zúčastní a koľko času vložia do samotného návrhu zmien naviac oproti svojej bežnej náplni práce.

Predpokladaná doba trvania projektu v krajinách, kde je počet všetkých zamestnancov nižší ako 500, sa odhaduje na 50 človekodní[2], v krajine od 500 do 1000 to činí 100 človekodní a v krajinách nad tisíc zamestnancov je odhad stanovený na 180 človekodní. Cena práce za jednu človekohodinu zo všetkých krajín bola spriemerovaná na 1 000 Kč.

**Tabuľka č. 7: Elementárny odhad ceny práce projektu v krajine**
[Zdroj: Vlastné spracovanie]

| počet zamestnancov | počet krajín | MD | Cena/krajina | Cena celkovo |
|---|---|---|---|---|
| do 500 | 18 | 50 | 400 000 Kč | 7 200 000 Kč |
| 500 - 1000 | 12 | 100 | 800 000 Kč | 9 600 000 Kč |
| nad 1000 | 6 | 180 | 1 440 000 Kč | 8 640 000 Kč |
| **Celkom** | | | | **25 440 000 Kč** |

Do kategórie menej ako 500 zamestnancov spadá aj česká pobočka spoločnosti a preto bude ekonomické zhodnotenie pre túto kategóriu rozobrané detailnejšie.

Vo väčších pobočkách sa očakáva priamo úmerná časová náročnosť s rovnakým pomerom.

**Tabuľka č. 8: Kalkulácia ceny práce pre českú pobočku**
[Zdroj: Vlastné spracovanie]

| Názov položky | Náročnosť v MD | Cena za položku |
|---|---|---|
| Identifikácia procesov a služieb | 10 | 80 000 Kč |
| Popísanie a zdokumentovanie procesov a služieb | 5 | 40 000 Kč |
| Návrhy na optimalizáciu | 15 | 120 000 Kč |
| Nasadenie | 20 | 160 000 Kč |
| **Celkom** | **50** | **400 000 Kč** |

[2] 1 manday (MD), človekodeň = 8 hodín

Okrem zamestnancov, ktorí budú pracovať na tomto projekte je potrebné poveriť samostatnú osobu (projektový manažér), ktorá bude mať na starosti celkovú koordináciu a komunikáciu a nebude sa venovať iným činnostiam v dôsledku plného nasadenia na daný projekt.

Predpokladá sa simultánna činnosť viacerých krajín súčasne a preto sa odhaduje celková dĺžka projektovej časti na 480 človekodní.

**Tabuľka č. 9: Celková cena práce projektovej časti**
[Zdroj: Vlastné spracovanie]

| | |
|---|---|
| Celková cena práce | 25 440 000 Kč |
| Cena práce projektového manažéra | 3 840 000 Kč |
| **Celkom** | **29 280 000 Kč** |

Samotný ITIL nerieši implementáciu spojenú s výberom konkrétneho softvéru a hardvéru, alebo iných technicky špecifických prostriedkov a podporných nástrojov. Z toho dôvodu náklady obsahujú len cenu práce zamestnancov.

# ZÁVER

Ciele práce boli splnené. Vďaka prijatiu a prispôsobeniu procesov a služieb podľa rámca ITIL bolo dosiahnuté efektívneho riadenia služieb IT a ich optimalizácia podľa najlepších skúseností a osvedčených postupov. Pridanou hodnotou je možnosť neustáleho zlepšovania zapojením PDCA cyklu, ktorý ponúka potenciál pre zníženie nákladov.

Hlavnou pridanou hodnotou navyše je, že návrh rieši aj zjednotenie viacerých krajinných oddelení IT do jedného európskeho oddelenia IT, ktoré prináša výhody v jednotnom riadení služieb na strategickej úrovni a odstránení redundantných aktivít, ktoré sa vyskytovali viacnásobne v samostatných oddeleniach.

Táto diplomová práca sa zaoberá momentálne najaktuálnejšími procesmi a službami vyžadujúce zmenu. Zďaleka však nepokrývajú úplnú implementáciu ITIL vo vybranej organizácii. Preto možno predpokladať, že je možné v budúcnosti ďalej pokračovať a viesť k ďalším procesným zmenám, ktoré by prospeli nie len európskemu oddeleniu pre IT, ale aj celej spoločnosti.

S ohľadom na obecné nariadenia na ochranu osobných údajov (GDPR), ktoré vstúpi do platnosti vo veľmi blízkej budúcnosti (25. 5. 2018) a týka sa každej organizácie, ktorá zhromažďuje alebo spracováva osobné údaje Európanov, bola tejto problematike venovaná pozornosť. Predovšetkým preto, že priamo súvisí so správou bezpečnosti informácií a úlohou integrovania súčasného systém riadenia bezpečnosti informácií do celkového riadenia služieb IT. Navrhnutím bezpečnostných opatrení a odporúčaní dôjde k súladu s GDPR.

V neposlednom rade bola venovaná pozornosť na vytvorenie reťazca dôvery a dodávateľsko-odberateľskému vzťahu z pohľadu bezpečnosti informácií s dôrazom na ochranu osobných údajov v rámci správy dodávateľov.

# ZOZNAM POUŽITEJ LITERATÚRY


[1] *ITIL – výkladový slovník a zkratky v češtině, v1.1, 6*. ledna 2012. ITIL [online]. [cit. 2018-02-21]. Dostupné z: <https://itsmf.cz/wp-content/uploads/2017/08/itil_2011_czech_glossary_v2.0.pdf>.

[2] SEDLÁK, Petr. *Management informační bezpečnosti* [prednáška]. Brno: VUT. 25. 9. 2017 - 18. 12. 2017.

[3] *IT Service Management Training: ITIL - IT Infrastructure Library*. 2016, 197s.

[4] BUCKSTEEG, Martin. *ITIL 2011*. Brno: Computer Press, 2012. ISBN 9788025137321.

[5] *IT & Management Knowledge Base: ITSM & ITIL* [online]. Bratislava: OMNICOM, 2008 [cit. 2018-05-14]. Dostupné z: <https://www.bestpractice.cz/cs/Best-practice/-ITSM-ITIL-.alej>.

[6] SKÁLA, Jiří. *ITIL - Best Practice řízení ICT služeb a ICT infrastruktury*. Praha: ČVUT, FEL a OMNICOM Praha. Řízení informačních a komunikačních technologií: 1. ročník konference ICTM. Praha: ČVUT, 2005, s. 28-37. ISBN 80-01-03259-0.

[7] *ITSM portal: Historie a vývoj ITIL*. [online]. Bratislava: OMNICOM, 2008 [cit. 2018-05-14]. Dostupné z: <https://www.bestpractice.cz/cs/Best-practice/-ITSM-ITIL-/-Historie-a-vyvoj-ITIL-.alej>.

[8] GRASSEOVÁ, Monika, a další: *Procesní řízení ve veřejném i soukromém sektoru*. Computer Press, 2008. 272 s. ISBN 978-80-251-1987-7.

[9] *ITSM portal: Co (ne)lze od ITIL® očekávat*. [online]. [cit. 2013-05-14]. Dostupné z: <https://www.bestpractice.cz/cs/Best-practice/-ITSM-ITIL-/-Co-nelze-od-ITIL-ocekavat.alej>.

[10] CARTIDGE, Alisona další. *Úvodní přehled ITIL V3.1.* : ItSMF Czech Republic, o.s., 2007. 58 s. ISBN 0-9551245-8-1.

[11] *ITIL Service Design - An Ephemeral Overview and Concepts Involved* [online]. Simpilearn, 2014 [cit. 2018-05-17]. Dostupné z: <https://www.simplilearn.com/itil-service-design-overview-rar62-article>.

[12] *ITIL Service Transition – Processes and Practices Involved* [online]. Simpilearn, 2014 [cit. 2018-05-17]. Dostupné z: <https://www.simplilearn.com/itil-service-transition-rar65-article>.

[13] SEDLÁČEK, Miroslav. *Demingův cyklus PDCA a norma ISO/IEC 20000-1:2011*. Systemonline [online]. SystemOnLine, 2011 [cit. 2018-05-17]. Dostupné z: <https://www.systemonline.cz/sprava-it/deminguv-cyklus-pdca.htm>

[14] *ITSM portal: Financial management for IT services*. [online]. [cit. 2018-05-14]. Dostupné z: <https://www.bestpractice.cz/cs/Best-practice/-ITSM-ITIL-/Klicove-procesy-ITIL-/Financial-management-for-IT-services.alej>.

[15] IT GOVERNANCE INSTITUTE. *Information security governance: guidance for boards of directors and executive management*. 2nd ed. Rolling Meadows. Ill: IT Governance Institute, 2006. ISBN 9781933284293.

[16] *ISO/IEC 27013:2015 Informační technologie - Bezpečnostní techniky. Norma stanovuje pokyny pro integrované použití ISO/IEC 27001 a ISO/IEC 20000-1 (standardů informační bezpečnosti a řízení IT služeb).*

[17] MALIŠ, Petr. *GDPR od A do Z*. SystemOnLine [online]. Systemonline, 2018 [cit. 2018-05-17]. Dostupné z: <https://www.systemonline.cz/clanky/vztah-spravce-a-zpracovatele-osobnich-udaju-podle-gdpr.htm>.

[18] CHLUMSKÝ, Pavel. *Dodavatelsko-odběratelské financování a jeho perspektivy v České republice (část 2/2)*. CAFIN [online]. AFIN, 2017 [cit. 2018-05-17]. Dostupné z: <http://news.cafin.cz/clanek/dodavatelsko-odberatelske-financovani-a-jeho-perspektivy-v-ceske-republice-cast-22>.

# ZOZNAM OBRÁZKOV

# ZOZNAM TABULIEK