Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Zavedení Incident managementu ve středně velké společnosti

Bc. Radoslav Nagy

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Radoslav Nagy

Informatika

Název práce

Zavedení Incident managementu ve středně velké společnosti

Název anglicky

Implementation of Incident Management in mid-size company

Cíle práce

Hlavním cílem diplomové práce je navržení komplexního Incident managementu pro středně velikou společnost působící v ICT, který bude splňovat požadavky jak technické, tak i legislativní.
Dílčí cíle práce jsou:
- analýza vhodných nástrojů pro správu incidentů
- návrh a zavedení vhodných workflow, nezbytných pro efektivní zpracování příchozích požadavků.

Metodika

Práce je založena na studiu vědecké a odborné literatury v oblasti Incident management. Dále pak bude využita teorie vícekriteriální analýzy variant a následně sestavení aktuálního modelu Incident managementu ve vybrané společnosti. V rámci analýzy proběhne identifikace míst, u kterých je možný návrh pro zlepšení. na základě literární rešerše a získaných poznatků budou navrženy postupy pro práci s incidenty pomocí definování nových postupů zpracování (workflow) ve vhodném nástroji.

Doporučený rozsah práce

60 – 80 stran

Klíčová slova

ICT, informační technologie, ISO/IEC 27000, ISO/IEC 27001, kybernetická bezpečnost, ITIL, Incident, ticket, workflow, SLA, KPI

Doporučené zdroje informací

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE. PROVOZNĚ EKONOMICKÁ FAKULTA, – BROŽ, S. – ŠVARCOVÁ, I. *Vliv řízení informačních technologií na chování organizace : [disertační práce].* 2005.

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE. PROVOZNĚ EKONOMICKÁ FAKULTA, – HAVLÍČEK, Z. *Informační technologie v řízení.* Praha: Credit, 2000. ISBN 80-213-0688-2.

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE. PROVOZNĚ EKONOMICKÁ FAKULTA, – TESAŘ, Š. – HAVLÍČEK, Z. *Řízení životních cyklů produktů informačních a komunikačních technologií v servisních organizacích [rukopis] : disertační práce.* Disertační práce. Praha: 2013.

HOUŠKA, M. – ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE. KATEDRA OPERAČNÍ A SYSTÉMOVÉ ANALÝZY, – BROŽOVÁ, H. – ŠUBRT, T. *Modely pro vícekriteriální rozhodování.* Praha: Credit, 2003. ISBN 80-213-1019-7.

Introduction to the ITIL service lifecycle. London: TSO(The stationery office), 2010. ISBN 978-0-11-331131-6.

ITIL. *Key element guide service strategy.* London: TSO(The stationery office), 2008. ISBN 978-0-11-331119-4.

ITIL V3 foundation handbook. London: TSO(The stationery office), 2009. ISBN 978-0-11-331197-2.

VELKÁ BRITÁNIE. OFFICE OF GOVERNMENT COMMERCE. *ITIL : service operation..*

VYSOKÁ ŠKOLA EKONOMICKÁ V PRAZE, – VOŘÍŠEK, J. – BASL, J. *Principy a modely řízení podnikové informatiky.* V Praze: Oeconomica, 2008. ISBN 978-80-245-1440-6.

Předběžný termín obhajoby

2018/19 LS – PEF

Vedoucí práce

Ing. Alexandr Vasilenko, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 11. 9. 2018

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 19. 10. 2018

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 25. 03. 2019

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Zavedení Incident managementu ve středně velké společnosti" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 25.3.2019 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Alexandru Vasilenkovi, Ph.D. jakožto vedoucímu této diplomové práce a panu Sakenzo Tavataki za poskytnutí technických informací a možnost konzultování problematiky Incident Managementu.

Zavedení Incident managementu ve středně velké společnosti

Abstrakt

Diplomová práce se zabývá ICT bezpečností, která vychází z ekonomických požadavků podniku, požadavků na platnou legislativu, které s bezpečnostním managementem souvisejí, rovněž vychází i z požadavků na normy a doporučené metody, které jsou celosvětově uznávané a které jsou v této oblasti zavedené.

Klíčová slova: ITIL, GDPR, Incident Management, Helpdesk, Vícekriteriální analýza variant, ISO 20000, workflow, tiketovací systém, IT, ICT, proces

Implementation of Incident Management in a mid-sized company

Abstract

This thesis is focused to ICT security, which emerges from economic demand of a company as well as from requests to comply with legislation, which is in a line with Security management. Its content relies also on possible methods, recommendations and principles used in companies worldwide.

Keywords: ITIL, GDPR, Incident Management, Helpdesk, multi-criteria analysis, ISO 20000, workflow, IT, ICT, process

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Prudký rozvoj a globalizace trhu probíhající na celém světě nutí podniky k neustálému zdokonalování procesů a nástrojů k tomu používaných. Tyto nástroje a procesy v případě nedostatku pracovní síly můžou přispívat k alespoň dočasné konkurenční výhodě. Neustále probíhá zavádění nových produktů, zlepšování a zvyšování efektivity ve spolupráci s partnery i se samotnými zákazníky. Probíhající změny a výzvy se zákonitě projevují nejen u podniků dodávaných své zboží a služby do zahraničí, ale logicky i u společností působících jenom lokálně. Míra zvyšování konkurenční výhody, kterou stanovuje právě technologie, je stále vyšší, jelikož lidské zdroje a pracovní efektivitu se daří zvedat jenom pomalu a v mnoha případech vůbec. Proto je důležitost zvyšování efektivity procesů, zlepšování služeb, zrychlování dodávek a zlevňování práce stále vyšší a je hlavním tématem z důvodu, aby ve společnosti nevládla stagnace anebo i dokonce úpadek.

Flexibilitu rozhodování, který lze dostatečně rychle přizpůsobit aktuálním potřebám zákazníků a trhu, už nelze dosáhnout bez flexibilního informačního systému. Je jasné, že vzniká potřeba koncipovat systémy a procesy tak, aby byly jednoduše uchopitelné a ohybatelné k aktuálním potřebám, které jsou v moha případech především maximalizace zisku. Nezřídka je to i požadavek zákonný, který určuje, a někdy i limituje, možnosti nasazení pracovní síly, nebo způsobu uchování dat.

Standardní podpora uživatelů a řešení problémů systémů mají společného jmenovatele, kterým je právě systém pro správu jednotlivých požadavků. V hantýrce IT může mít vícero názvů a podob, zaužívané jsou primárně pojmy „Helpdesk“, anebo „Incident Management“, který může mít mnoho podob a stanovení cesty k nalezení ideálního řešení není ani z pohledu odborníka z praxe lehkou úlohou. Proto je vytvoření návodu pro zjednodušení cesty k finálnímu řešení vyústěním této logické úlohy.

2 Cíl práce a metodika

Tato diplomová práce má jako hlavní cíl navržení komplexního Incident managementu pro středně velikou společnost působící v ICT[1], který bude splňovat požadavky jak technické, tak i legislativní. Dotýká se témat procesů použitých v rámci toku informací ve společnosti, ze kterých vyplývají dílčí cíle, kterým je analýza a výběr vhodných nástrojů pro správu incidentů a návrhu zavedení vhodných pracovních postupů nezbytných pro efektivní zpracování příchozích požadavků.

2.1 Metodický postup

Řešení této diplomové práce využívá metodiku, která je založena na analýze jak dostupných zdrojů, tak především informací a postupů získaných a zaznamenaných v různých publikacích věnujících se problematice incident managementu, společenských a technologických normách a studiem současných trendů.

Jednou z množiny publikací, která se zabývá a doporučuje zavedené postupy a praktiky v oblasti ICT, se nazývá ITIL[2]. Analyzováním části této publikace lze získat sadu informací, které budou uplatněné při modelování vzorového Incident Managementu.

Analýzou GDPR[3] získám nutné informace, které definují zákonné požadavky na plnění ochrany dat a soukromí, které můžou být nezbytné při zavádění Incident Managementu. Důvodem je především jasná vazba této problematiky na lidi a data, které s nimi souvisejí.

Jednoduchým hledáním pomocí internetu a následným náhodným výběrem několika nástrojů pro správu incidentů, zvolím pomocí vícekriteriální analýzy variant jeden konkrétní nástroj, ve kterém bude vymodelován způsob správy a práce s incidenty. Vymodelování procesů a nakonfigurovaní takovéhoto nástroje pak poslouží jako ukázka použití teorie v praxi.

2.2 Vícekriteriální analýza variant

Při řešení rozhodovacích problému se lze setkat s případy, kdy rozhodnutí závisí na více než jenom jednom kritériu. Kritéria mohou být různé a lze je kategorizovat, příkladem může být

[1] Information and Communication Technology – informační a komunikační technologie
[2] Information Technology Infrastructure Library – Soubor praxí a doporučení při zavádění informačních technologií do podniku, více v kapitole 4 - ITIL
[3] General Data Protection Regulation – norma regulace ochrany dat a soukromí v EU

vyžadovaná nejrychlejší odezva a co nejnižší nároky na výkon, můžou být různého typu a druhu, jak uživatelský komfort oproti ceně a můžou být navzájem konfliktní použití SaaS[4] k potřebě vlastních programový úprav. Úlohy vícekriteriálního rozhodování lze klasifikovat podle způsobu zadání množiny variant, které jsou přípustné varianty anebo připadají k úvahu. Pokud je tato množina definovaná konečným seznamem variant, jedná se o vícekriteriálním hodnocení variant. Je-li množina přípustných variant zadána podmínkami, které musí být při výběru optimální varianty splněny, jde o úlohy vícekriteriálního programování. Teorie a model vícekriteriální analýzy variant lze využít na jako řešení problému, jak vybrat jednu nebo více variant z množiny přípustných variant a doporučit je k realizaci. Cílem je najít variantu, která je podle všech kritérií celkově hodnocena co nejlépe, variantu kompromisní, případně seřadit varianty od nejlepší po nejhorší, nebo vyloučit neefektivní varianty. [1]

$$\begin{array}{c} \\ a_1 \\ a_2 \\ \vdots \\ a_p \end{array} \begin{array}{c} \begin{array}{cccc} f_1 & f_2 & \cdots & f_k \end{array} \\ \begin{pmatrix} y_{11} & y_{12} & \cdots & y_{1k} \\ y_{21} & y_{22} & \cdots & y_{2k} \\ \cdots & \cdots & \cdots & \cdots \\ y_{p1} & y_{p2} & \cdots & y_{pk} \end{pmatrix} \end{array}$$

Obrázek 1: Kritéria (sloupce) a varianty (řádky) v maticovém obecném tvaru

Celkové hodnocení variant závisí na důležitosti jednotlivých kritérií, které jsou k posuzované (interkriteriální preference) a na hodnocení jednotlivých variant (intrakriteriální preference). Důležité jsou právě typy informací o důležitosti jednotlivých kritérií a o hodnocení variant podle každého kritéria. [2]

Z hlediska rozdělení lze proto klasifikovat kritéria následovně do několika skupin, které zle jednoduše definovat a aplikovat:

- Dle povahy
    - Maximalizační
    - Minimalizační
- Dle kvalifikovatelnosti

[4] Software as a Service – softvérová služba za kterou se platí při užívání a kterou spravuje společnost, která ji poskytuje. Typická implementace je v cloudovém prostředí.

    - Kvantitativní
    - Kvalitativní
- Preference kritéria
    - Aspirační úroveň
    - Pořadí kritérií
    - Váhy kritérií
    - Kompenzace kriteriálních hodnot

Existují varianty, které mají speciální vlastnosti. Radí se mezi ně dominovaná varianta; Paretovská, nedominovaná varianta; ideální varianta; bazální varianta; kompromisní varianta. Vlastnosti, které musí tyto varianty splňovat jsou pak nedominovanost; invariance k pořadí; invariance k měřítku kriteriálních hodnot; nezávislost na identických hodnotách; invariance k dominovaným variantám; determinovanost; jednoznačnost.

Hledané řešení lze najít, pokud bude výchozím krokem analýzy modelu vícekriteriální analýzy variant stanovení vah, které je nutné zvolit na základě interních preferencí a především, relevantnosti požadovaných vlastností výsledného produktu, který je posuzovaný. Po určení vah, je nutné zvolit metodu, která bude pro posouzení použitá. Nelze obecně určit, která metoda je nejpřesnější, nebo nejvhodnější, vždy záleží od konkrétní situace, která nastane a která použití některé z metody předurčuje. Na základě subjektivních nebo objektivních preferencí se proto určí vhodná metoda. Z důvodu potvrzení správnosti výsledků lze použít i metod několik a ověřit si tak jednoduše správnost výsledku. Pro toto ověření správnosti je může být zvolena metodika, která využívá několik stanovení vah kritérií, kterými jsou například:

- Metoda pořadí;
- Saatyho metoda;
- Metoda AHP;
- Bodovací metoda;
- Fullerova metoda;
- Lexikografická metoda;
- Metoda TOPSIS;
- Permutační metoda ORESTE;
- Metoda preferenčních relací ELECTRE, PROMETHEE;
- A další.

2.2.1 **Metoda pořadí**

Metoda pořadí je založena na převedení kriteriální matice na matici pořadí, kterou lze vyhodnotit. To znamená, že se postupně podle všech kritérií přiřadí pořadí jejich variantám. Pokud je známa ordinální informace, kterou lze hodnotit dle jednoho kritéria, je možné informaci vyjádřit pořadím variant, a to celými čísly mezi *1* a *p*. P představuje počet variant. Varianta, která je nejdůležitější (nejhodnotnější), bude ohodnocena číslem *p* (počtem variant), druhou nejlepší číslem *p-1*, atd. až do poslední, do té, která je nejhorší. Variantám, které jsou rovnocenné, je přiřazeno číslo průměrného pořadí.

Kritéria je potřeba seřadit nejprve podle pořadí od nejdůležitějšího po nejméně důležité. Nejdůležitější kritérium je potřeba ohodnotit *k* body ($bi = k$), druhé nejdůležitější $k - 1$ body ($bi = k - 1$), atd. až poslední (nejméně důležité) jedním bodem ($bi = 1$). V případě, že by některá kritéria byla stejně důležitá, lze je obodovat příslušným průměrem. [2]

$$yy = \sum_{j=1}^{k} bij$$

V dalším kroku pak budou varianty uspořádané sestupně podle hodnot b_i, a nejlepší variantu lze vypočíst ze vztahu:

$$a_1 : b_1 = \max_{i=1,\dots,s} (b_i)$$

2.2.2 **Bodovací metoda**

Kvantifikaci hodnocení variant podle kritéria předchází stanovení bodovací stupnici. Rozmezí, které je nejvíce vhodné pro určování pořadí, může být od 0 do 10. Podle tohoto kritéria se pak hodnotí každé z variant a je tak vyjádřeno určitým počtem bodů. Při maximalizačním typu ohodnocení se nejlepší varianta ohodnotí počtem bodů, který je nejvyšší. V případě minimalizačního ohodnocení je nejlepší varianta ohodnocena nejnižším počtem bodů.

I tuto metodu lze použít pro výpočet, kterým určujeme váhy kritérií, které může hodnotit vícero expertů najednou. Pro toto použití je nutné zvolit bodovou stupnici a každé kritérium ohodnotit určitým počtem bodů, na základě preferencí nebo důležitosti, tj. čím je kritérium víc preferované nebo důležité, tím víc bodů dostane. Výpočet vah se z bodového hodnocení provede stejně jako u metody pořadí.

3 Teoretická východiska

Zkoumáním teorie analýzy variant lze pochopit a popsat možný způsob výběru vhodného nástroje pro Incident management. Ten musí splňovat určité vlastnosti a funkcionalitu, která vychází doporučení se všeobecným názvem ITIL.

Informační technologie hrají stále více zásadnější roli při vytváření nových příležitostí a poskytování konkurenční výhody podnikům. Proto podnikání zaměřené na oblast řízení IT zdrojů je vysoce ceněno. Vzhledem k tomu, že IT oddělení a organizace přecházejí z technologií do modelů řízení založených na službách, investování do důvěryhodného rámce osvědčených postupů, jako je knihovna informačních infrastrukturních infrastruktur (ITIL), je stále důležitější.

3.1 ITIL

ITIL – Information Technology Infrastructure Library (Soubor svazků popisujících Infrastrukturní řešení a procesy informačních technologií) je soubor svazků popisující rámec praktických zkušeností pro poskytování IT služeb, které se v praxi ukázaly jako nejlepší a fungující.

V ITILu se lze jednoduše inspirovat při vývoji a implementaci podnikových systémů. Důvodem je obsah, který vychází z předešlých zkušeností jak z pohledu potřeb zákazníka, tak i z různých vnitřních událostí a fungování společností. Hlavním důvodem implementace postupů na základě těchto doporučení je, že lze očekávat zvýšení produktivity společnosti a zlepšení ve spolupráci, komunikaci i v obchodních stycích s dodavateli nebo i zákazníky. Důležitá je společná terminologie, kterou ITIL přináší a popisuje. [3]

ITIL není jednoduché uchopit, vzhledem na fakt, že se jedná pouze o hypotetické doporučení a nezabývá se řešením konkrétních událostí. Existují proto různé školení a certifikace, které se snaží společnostem objasnit důležité principy fungování ICT, obsažené v jednotlivých svazcích. Stává se, že některé implementace ITILu v společnostech ne zcela vyřeší nedostatky a ITIL se tak stává kontraproduktivním přínosem do organizace. Různé publikace popisují jak zdárné, tak i nezdárné případy zavedení těchto doporučení v společnostech a jsou dobrým vodítkem pro jakékoliv zahájení změn v procesech týkajících se IT ve společnosti. [3]

Jako každé doporučení, i u ITILu lze popsat charakteristické rysy, které provázejí toto doporučení v podstatě od jeho založení. Celosvětově jsou tyto pravidla uznávaná právě

proto, že jsou univerzální a lze je použít téměř na jakékoliv řešení v každé společnosti, bez ohledu na politickou, geolokační anebo kulturní rozličnost. Je vhodné vyjmenovat některé charakteristické rysy [18]:

- **Procesní řízení** – ITIL používá procesně orientovaný přístup k řízení IT služeb. Proces je logický sled úkolů transformujících nějaký vstup na nějaký výstup, přičemž plnění jednotlivých úkolů v procesu je zajišťováno rolemi s jasně definovanými odpovědnostmi. Celý proces je řízen, monitorován, měřen, vyhodnocován a neustále vylepšován, což je odpovědností vlastníka procesu.
- **Zákaznicky orientovaný přístup** – všechny procesy jsou navrženy s ohledem na potřeby zákazníka, tzn. každá aktivita a úkon v procesu musí přinášet nějakou přidanou hodnotu pro zákazníka. Pokud tuto funkci neplní, je tato činnost nadbytečná.
- **Jednotná terminologie** – málo doceňovaná, nebo úplně opomíjená charakteristika ITILu, která je však podstatnou součástí. Vynechání této součásti zpravidla vede k prodlužování a prodražování projektů a rovněž i při natahování času při řešení incidentu, které plynou z prostého nedorozumění.
- **Nezávislost na platformě** – rámec procesů managementu IT služeb podle ITIL je nezávislý na jakékoliv platformě. Dokonce je možné ITIL použít i pro navrhování procesů v jakékoliv organizaci, která nepodniká v IT.
- **Public domain**[5] – knihovna je volně dostupná, což znamená, že za užití a inspiraci při zavádění procesů a struktury vlastní IT se lze libovolně inspirovat v libovolně velkém rozsahu, jak z volně dostupných zdrojů, tak i z placených publikací, které vydává organizace, která zaštiťuje ITIL [18].

3.1.1 Historie ITIL

Tyto postupy byly vytvořené britskou vládní agenturou Central Computer and Telecommunications Agency (CCTA) a byly postupně doplňované na více než 30 knih. Tyto svazky obsahovaly praktické zkušenosti z oblasti informačních technologií, které byly nashromážděny z řady zdrojů, a to i včetně interních zkušeností dodavatelů informačních technologií a poradenských firem z celého světa.

[5] Volně přeloženo jako veřejně dostupné, nebo „příslušné k volnému užívání“

V letech 2000 - 2001 byly svazky ITILu revidovány, označeny jako verze 2 a jejich počet se snížil ze třiceti na uspořádaných 9. V květnu 2007 je pak vydaná verze 3, která obsahuje popis 26 procesů a funkcí, seskupených do pěti svazků.
Výrazná změna nastává v roce 2011, kdy proběhlo oživení některých částí a tato publikace je poslední známou změnou. Další naplánované změny jsou očekávané v průběhu roku 2019. [4]

3.1.2 **ITIL v současné době**

Základní cíl ITIL je pořád poskytnout rámec osvědčených postupů a doporučení, které podniky mohou využít jako vodítko pro řízení IT. ITILv3 má pět základních svazků, které jsou [12]:

- Service Strategy (strategie služeb)
- Service Design (návrh služeb)
- Service Transition (uvedení služeb do provozu)
- Service Operation (provoz služeb)
- Continual Service Improvement (neustálé zlepšování služeb)

I když se tyto svazky věnují různým oblastem v rámci IT, tak je mezi nimi vzájemné propojení, jak ve jmenné konvenci, tak i tím, že počítají s určitým řešením, které je rozebíráno v předešlém svazku. Stejně tak se vzájemně doplňují. Implementace jenom separátního svazku v rámci jedné společnosti tedy možné je, výsledná efektivnost takového řešení je pak sporná. Krátké představení jednotlivých svazků pomáhá k pochopení ITILu a k vytvoření ucelené představy.

3.1.3 **Strategie služeb**

Service (IT Service, IT Service Management, ITSM) v terminologii ITIL vyjadřuje určitou přidanou hodnotu, která je poskytována zákazníkům (uživatelům) a jejímž cílem je podpořit obchodní, strategické, nebo jiné cíle, kterých chce organizace dosáhnout. Ve této fázi se doporučení pro podnik týká vytvoření strategie poskytování služeb IT tak, aby vedla k vytvářením určité přidané hodnoty, a definování strategie řízení těchto služeb, které jsou nezbytné pro úspěšný chod společnosti [13].
Přínosem fáze pro ITSM je ovládnutí znalostí, týkajících se:

- porozumět tomu, jak aktivity související s poskytováním služeb ovlivňují celkovou hodnotu společnosti;
- optimalizace kvality a úrovně, různých typů služeb, které jsou přínosem pro zákazníky;
- zvýšit konkurenční výhodu rychlým a efektivním rozhodováním, které se děje při změnách podmínek v byznysu;
- zajistit návrat co nejvíc z investic do služeb a snažit se o největší zisk;
- dosáhnout souznění ve spolupráci mezi poskytovatelem a zákazníkem v otázce toho, co je požadavek a co a jak bude dodané;
- plánování efektivní a účinné poskytování veškerých služeb [13].

3.1.4 **Návrh služeb**

V této fázi je navrženo, jak bude vybraná služba vypadat a z jakých technologií se bude skládat. Fáze návrhu služeb může popisovat i definování změn stávajících služeb IT, politik, procesů a ITSM strategií a dále popisuje implementování a uplatnění v praxi všech navržených změn [14].

Přínosem pro ITSM je zisk následujícího a za pomocí:

- minimalizace nákladů vhodně provedeným návrhem služeb IT, procesů a souvisejících technologií;
- zvyšování kvality poskytovaných služeb IT prostřednictvím použití sofistikovaných metod při návrhu;
- vytváření konzistentního návrhu služeb, které se prolíná se strategií společnosti;
- usnadnit a zjednodušit zavádění navržených změn;
- zvýšit povědomí a proškolení pracovníků, aby navržené služby poskytovaly odpovídající úroveň, která je požadovaná zákazníky;
- zvýšit přínos služeb IT zohledněním možných kapacit a dostupností služeb ve fázi jejího návrhu;
- snažit se zvyšovat výkon ITSM zapracováváním kontrolních prvků a metrik v nových procesech [14].

3.1.5 **Uvedení služby do provozu**

Cílem převádění služby do provozu je vybudování a spuštění procesu pro udržení této služby v chodu. V návaznosti na tento proces je vybudován i postup a způsob, jak služby udržovat v chodu koordinovaně (řízení změn a incidentů), případně určit celý životní cyklus [15].
Cílem fáze pro ITSM je:

- zvýšit množství změn, které pozitivně ovlivňují chod systému a různé služby;
- sdílet potřebné pomůcky a mechanizmy přechodu mezi službami a projekty;
- zvýšit pravděpodobnost, že provedení změny negativně neovlivní ostatní služby, nebo systémy;
- garantovat udržitelnost a cenovou efektivitu služeb;
- vyladit kontrolu nad službami, aktivy a konfiguracemi [15].

3.1.6 **Provoz služeb**

Fáze provozu služeb má za cíl udržovat službu v provozu, přičemž ty mají stanovené podmínky fungování, jako jsou například maximální povolená míra odstávky, nebo doba zprovoznění služby při výpadku. Dle zkušeností z praxe, lze provoz udržet správným koordinováním všech aktivit, které se službou souvisejí. Důležité je dodržování navržených procesů, stanovených při uvedení služby do provozu, rovněž funkční monitorování, kontrola metrik a jejich vyhodnocování [16].
Přínosem fáze pro ITSM je získání schopnosti:

- omezit práce nad plánovaný rámec a výdaje spojené s IT plánováním odstávek a identifikací příčin odstávek neplánovaných;
- omezit frekvenci a délku odstávek;
- zvýšit celkovou dostupnost služeb;
- neustále zlepšovat služby za pomocí vyhodnocování různých metrik a měření;
- urychlit a zefektivnit dodávku služeb k zákazníkům;
- zvýšit celkovou spokojenost pravidelným reportováním a informováním o průběhu řešení všech požadavků;
- zvýšit efektivitu přerozdělováním zdrojů na přínosnější a více inovativní práci, a případnou automatizací prací [16].

3.1.7 **Kontinuální zlepšování služeb**

Fáze kontinuálního zlepšování služeb je přizpůsobení IT služeb neustále se měnícím potřebám podniku, který vyplývá z požadavků jak právních, tak i obchodních. Není to ale v čase omezená část životního cyklu, protože se doplňuje společně s fázemi strategie služeb, návrhu služeb, uvedením služeb do provozu a samotným provozem. Během fáze provozu jsou příznačné události, které jsou spouštěčem pro zahájení všech změn. Neustálé hledání možností, jak lze zefektivnit služby a všechno kolem IT, je přesně to, co charakterizuje tuto fázi. Realizace zlepšování probíhá pomocí cyklu „plánuj – dělej – kontroluj – jednej“ jinak známého jako Demingova životního cyklu [17].

Využití je možné:

- postupné zlepšování kvality služeb;
- zefektivnění dodávky služeb, zrychlení procesů a snižování výdajů;
- při hledání možností ke zlepšování všech dodávek služeb [17].

3.2 **ITSM**

IT Service Management (ITSM) - obvykle se nepřekládá a používá se zkratka. Je to souhrn nejlepších praxí a referenčních modelů procesů řízení služeb IT. ITSM představuje způsob řízení informačních a komunikačních technologií, jejich provozu i rozvoje, který využívá principů řízení na bázi služeb, zahrnuje tedy pohled zákazníků i poskytovatele IT služeb. Pojem IT Service management vychází z rámce ITIL, ve kterém byl koncept řízení IT pomocí služeb poprvé použit, ale není s ním výlučně spjat.

ITSM jako manažerská disciplína zahrnuje tři relativně samostatné, ale přesto navzájem propojené a na sobě závislé oblasti. Tuto závislost lze znázornit jako vzájemně propojené vrcholy jednoho trojúhelníku [11]:

1. **Lidé** – všichni zaměstnanci podniku, kteří přicházejí do kontaktu se službami IT, tj. uživatelé, kteří se službami IT pracují na denní bázi, jejich manažeři, kteří s útvarem podnikové informatiky vyjednávají parametry služeb IT, interní podnikoví IT specialisté, kteří zajišťují dodávku a podporu služeb IT, a v neposlední řadě externí dodavatelé.
2. **Nástroje** – nástroje usnadňující řízení služeb a infrastruktury IT a nástroje automatizující rutinní činnosti a spolupráci různých lidí. Zejména sem tedy patří nástroje pro monitorování, správu a řízení komponent infrastruktury IT, nástroje pro

řízení životního cyklu incidentů, požadavků, problémů, změn a dalších entit, knihovny elektronické dokumentace a software, a nástroje pro ukládání a sdílení dat, informací a znalostí, a v neposlední řadě nástroje pro komunikaci.

3. **Procesy** – veškeré organizačně-procesní prvky systému řízení služeb IT, zejména definice pojmů, vymezení aktivit, rolí a jejich odpovědností, definice vstupů a výstupů aktivit a procesů, definice komunikačních kanálů, metrik, reportování a dokumentace celého systému. Tímto aspektem rozumíme jak jednotlivé ITSM procesy či jejich dílčí aktivity, resp. jejich ostatní prvky (role, metriky atd.), tak celé systémy řízení služeb IT, které se skládají ze všech těchto organizačně-procesních prvků.

3.3 ISO/IEC 20000

ITIL tvoří v podstatě celosvětově nejrozšířenější normu pro regulaci a poskytování IT služeb tak, jak to bylo popsané v jedné z předešlých kapitol této práce. Z principů stanovovaných v tomto rámci, vychází i norma ISO 20000 a která je jakýmsi uceleným souborem pravidel, na základě kterého lze určit správnost implementace procesů, metod, nebo technického vybavení, nebo jenom jednoduše certifikovat společnost, která se nachází v určitém (regulovaném) odvětví [18].

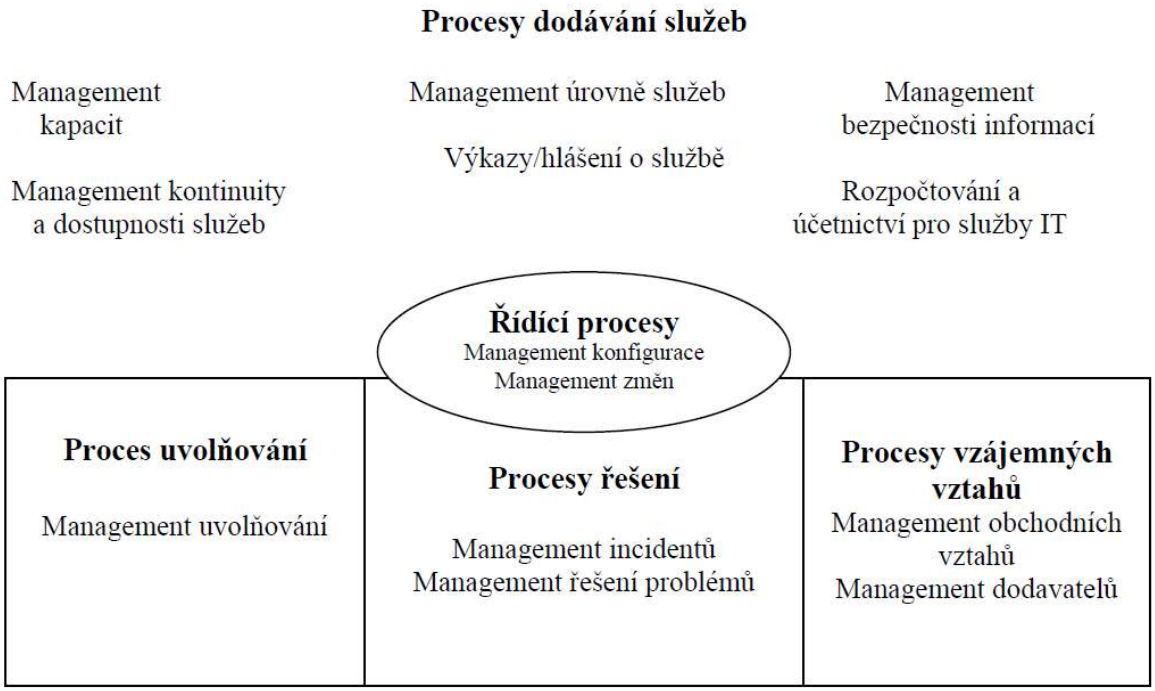
3.3.1 Procesy podle normy ISO 20000

Specifikace procesů podle ITIL respektive podle normy ISO 2000 stanovuje požadavky na organizaci s ohledem na dodání kontrolovaných informačních (IT) služeb v kvalitě přijatelné pro její zákazníky [18].

Může být použita [18]:

- Organizacemi, které vstupují do výběrových řízení se svými informačními (IT) službami;
- organizacemi, které vyžadují důsledný přístup od všech poskytovatelů služeb v dodavatelském řetězci;
- poskytovateli služeb pro ohodnocení výkonnosti jejich managementu IT služeb;
- jako základ ohodnocení, které může vést k formální certifikaci;
- organizací, která potřebuje prokázat schopnost poskytovat IT služby, které splňují požadavky zákazníků;

- organizací, která usiluje o zlepšení IT služeb pomocí efektivní aplikace procesů pro monitorování a zlepšování kvality služeb.



Obrázek 2: Rámcový model životního cyklu incidentu (zdroj: [18])

Norma ISO 20000 specifikuje několik vzájemně úzce souvisejících procesů managementu informačních (IT) služeb, jak je znázorněno na obrázku (Obrázek 2).

Vztahy mezi procesy závisejí na způsobu aplikace v rámci organizace a jsou obecně příliš složité na modelování, a proto nejsou vztahy mezi procesy v tomto diagramu ukázány.

Norma nespecifikuje vyčerpávající seznam cílů a organizace může zvážit, zda existují další cíle a opatření nezbytné ke splnění jejich konkrétních podnikatelských potřeb. Podstata obchodního vztahu mezi poskytovatelem služeb IT a organizací využívající tyto služby určí, jak budou implementovány požadavky této normy, aby byly splněny celkové cíle [18].

3.4 Incident management

V případě požadavku na co nejrychlejší vyřešení výpadku, nebo omezení služeb, lze reagovat různým způsobem. Množství situací, které se stávají, je však natolik unikátních, že není možné popsat každou situaci separátně a vymyslet k ní nejoptimálnější přístup. Rysy každého takového požadavku mají mnoho společného, a to popsat lze. Jelikož už je možné popsat „co“, lze zkusit navrhnou způsob „jak“. Principy uvedené v následující části přímo i

nepřímo souvisí s problematikou správy incidentů a řešení různých požadavků a jsou tak popisem univerzálních črtů jednotlivých situací. Jejich popis je vhodný k plnému pochopení souvislostí a toho, jak lze vytěžit znalosti popsané v ITIL, které jsou doporučené k obsloužení těchto situací, tj. v případě incidentů, problémů, nebo jiných požadavků na službu.

Incident management je proces, který se věnuje celému životnímu cyklu incidentů. Další charakteristikou je taky nalezení vhodného popisu a postupu, aby byl provoz služeb IT, jejichž poskytování bylo přerušeno nebo omezeno, neprodleně obnoven na podle stanovené dohody a aby byl minimalizován negativní dopad na běh služby, kterou využívá zákazník anebo jakákoliv společnost [16].

3.4.1 Cíle Incident managementu

Jednoznačné cíle pro incident management lze definovat v pěti bodech, které jsou rovněž stěžejní téma ITILu a fáze provozu služeb:

- Nutnost existence procesu k zefektivnění a urychlení komunikace se zákazníky, analýze problémů, k vytváření dokumentace a zaznamenávání činností, rovněž i pro správu incidentů a následné reportování o stavu;
- Zlepšit přehlednost stavu řešení pro obě strany, jak pracovníky podpory, tak i zákazníky;
- Vylepšovat vjem z poskytovaných služeb profesionálním přístupem – informováním o nastalých incidentech a jejich rychlým vyřešením;
- Sladit prioritizaci řešení incidentů s prioritami zákazníků a dle dohodnutých pravidel;
- udržovat spokojenost zákazníků kvalitními dodávkami IT služeb [16].

3.4.2 Vnější předpoklady pro dodržení cílů

Existující předpoklady, které mají vnější vplyv na dodávky služeb v rámci Incident managementu:

- Součinnost s procesem, který je v rámci katalogizaci služeb;
- Učení se ze zpětné vazby z průběhu zpracování incidentů a vyhodnocování na základě podnětů z vnějška;

- Součinnost s procesem, který zaručuje korektnost databáze aktiv a katalogu služeb a konfigurací;
- Evidence veškerých změn konfiguračních položek, na základě které lze dohledat to, která změna způsobila výpadek [16].

3.4.3 Help desk a service desk

Helpdesk jako jedna z mála části podniku je v neustálé komunikaci jak interně v rámci podniku, ať už při snaze vyřešit zákaznický problém, nebo i požadavky zaměstnanců podniku, tak i externě se zákazníky. Funkčnost, spolehlivost, rychlost a efektivita jsou aspekty, které pomáhají značnou mírou k fungování podniku a zvyšování zisku, proto je správná implementace help desku v rámci služeb service desku velmi důležitou součástí běhu společnosti. Zároveň, je to jeden z nejsložitějších úkonů v rámci zprocesování podniku na základě doporučení ITILu. [9]

Služba service desk se obvykle soustřeďuje na správu životního cyklu incidentů a provádí následující primární funkce [10]:

- Zákaznické rozhraní
- Podpora podnikání
- Kontrola incidentů
- Informace o řízení.

Service desk je primárním kontaktním místem pro všechny interní a / nebo externí zákazníky. Dojem uživatelů ze služby service desk ovlivňuje celkový obraz IT služeb podniku a nálady zaměstnanců a zákazníků. Logicky, dobrý dojem a funkčnost service desku může získat větší podporu z vrcholového managementu, což bude velmi užitečné pro posílení implementace ITSM a zvýšení spokojenosti zákazníků.

Cílem tradičního service desku bylo v minulosti pouze obnovení služeb co nejrychleji, řídit životní cyklus incidentu (koordinovat řešení) a generovat reporty, komunikovat a propagovat. Stejně tak byla úloha vyřizovat, otázky, žádosti, stížnosti a řešit různé připomínky [5]. Nyní však podniky potřebují service desk s více funkcemi a silnějšími schopnostmi. Kvalitní service desk je základem při implementaci ITSM.

3.4.4 Životní cyklus incidentu

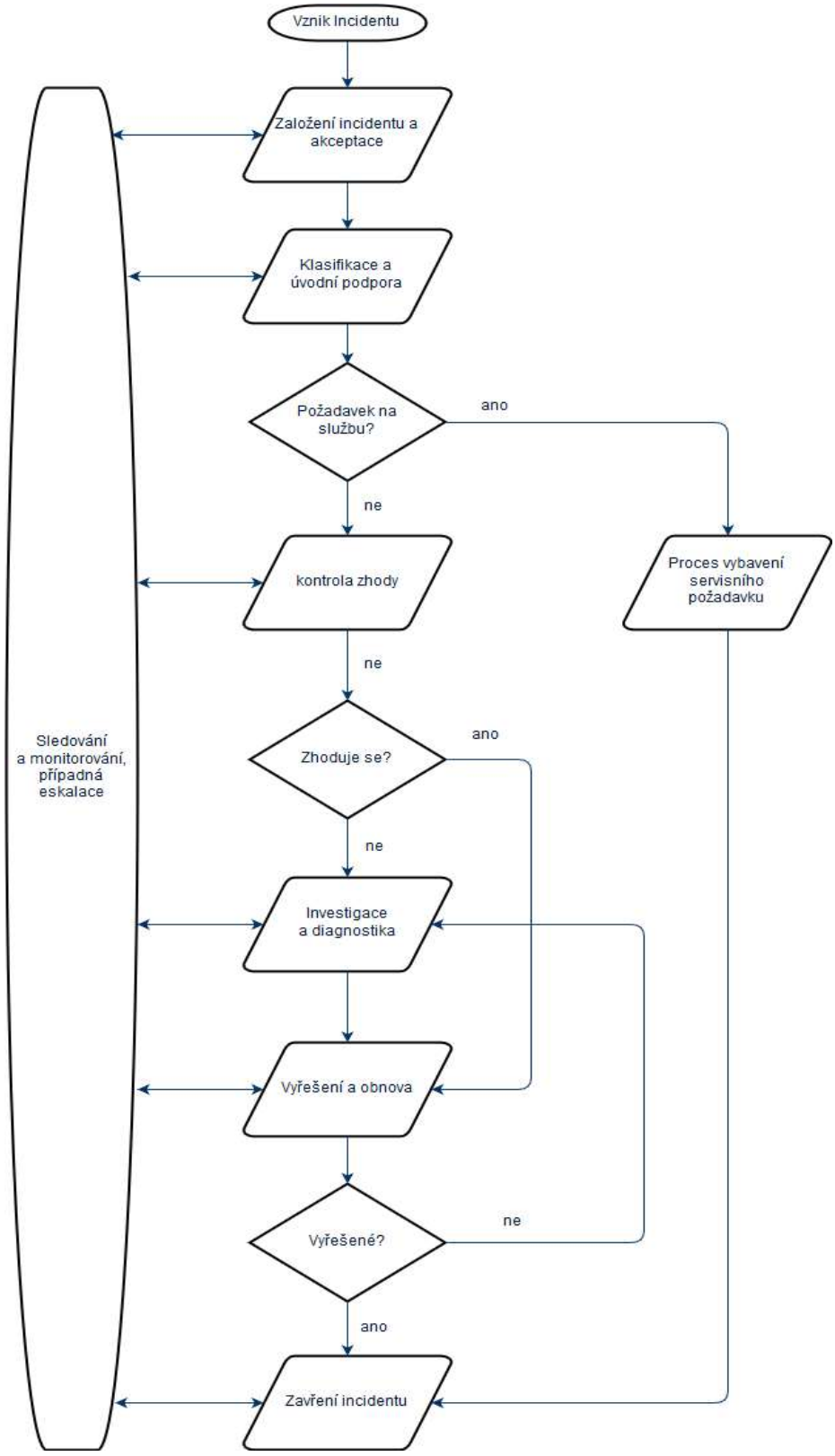
Jan van Bon definoval „incident“ v jeho knize jako [5]:

„Jakákoliv událost, která není části standardního provozu služeb a která způsobuje, nebo může způsobit přerušení anebo omezení kvality služby.“

Na základě definice incidentu, cílem Incident Managementu se chápe obnovení provozu do normálního stavu tak rychle jak je to jenom možné za minimální náklady a v co nejmenším dopadu na byznys, v návaznosti na spokojenost zákazníka a v rámci navzájem akceptované SLA (Service Level Agreement) [6].

Další aktivity, jako je eskalace (která z principu fungování vyžaduje klasifikaci incidentů) nebo parametry pro přirazení, jako jsou priorita, urgentnost nebo dopad, by měly být zohledněné v Incident Management workflow a jelikož pro každou implementaci může být takový postup jiný, obecně lze proces toku akcí každého incidentu zakreslit do názorného diagramu (Obrázek 3). [5,7,8]

- Založení incidentu a akceptace – v této fázi je záznam o incidentu vytvořen na základě telefonátu, emailu, nebo jakékoliv jiné cesty;
- Klasifikace a úvodní podpora – typ, dopad, priorita a urgentnost incidentu jsou zmíněné v reportu, v případě nejasností je zakladatel incidentu dotazován a reálnost incidentu je potvrzovaná;
- Požadavek na službu – pokud zakladatel incidentu požádá o službu, je spuštěn separátní proces pro vyhovění;
- Kontrola shody – hledání identického nebo podobného incidentu v znalostní databázi;
- Vyřešení a obnova – řešení incidentu až po nalezení opravy a návratu do funkčního stavu;
- Zavření incidentu – potvrzení možnosti uzavření incidentu jeho vlastníkem (zpravidla zakladatelem incidentu).



Obrázek 3: Rámcový model životního cyklu incidentu (zdroj: [18])

3.4.5 **Podrobné rozdělení životního cyklu incidentu**

Identifikace – v rámci ITILu lze definovat několik fází existence incidentu. Tou první je samotná identifikace, která je zahájením procesu pro samotné zpracování požadavku. Pokud se možný incident podaří odhalit ještě před jeho dopadem na službu, může být proces řešení jednodušší a méně náročný na výslednou cenu za samotné řešení. Včasné odhalení incidentu lze provést pomocí monitorování klíčových součástí řešení a souvisejících procesů správy událostí. Identifikace může být učiněna zákazníkem, zaměstnancem, automatickým systémem apod. [16].

Zaznamenání – Oznámit incident lze akcí, která končí vytvořením záznamu. Tím je spuštěné jakési workflow, které incident provází celým životním cyklem. Stejně tak lze kontaktovat uživatelskou linku osobně, telefonicky nebo emailem a ta tiket vytvoří. Tato fáze se nazývá zaznamenání. Nezávisle na tom, jakým způsobem je incident nahlášen, by měly být při vytvoření dodržené podmínky, které tento incident jasně definují. Obecně by záznam měl obsahovat co nejvíce informací. Zákaznická linka také zkontroluje, zda je popis dostatečný a dopad splňuje podmínky pro vytvoření incidentu. Pokud to tak není, je potřeba vytvořit odpovídající typ záznamu a stávajícím zaznamenáváním se dál nezabývat [16].

Kategorizace – V procesu definování záznamu o události je nutné vložit tento záznam do odpovídající kategorie. Může se jednat o kategorizaci podle geolokace, priority, postižené služby, systému a aplikace. Protože lze definovat odlišné eskalační postupy pro každou kategorii incidentů, je nutné počítat se zaznamenáváním odpovědnosti, součinnosti, preventivních opatření, limitů pro časové délky splnění a způsobu zaznamenávání činností. Další využití je při vyhodnocování metrik, jakou jsou frekvence výskytů jednotlivých kategorií, trend zvyšování, nebo snižování apod. Tyto informace pak lze zohlednit při implementaci konkrétního řešení a zvolení správné metodiky, kterou je událost řešená [16].

Prioritizace – Na základě naléhavosti a objemu dopadu je stanovena výše priority pro definici snahy k vyřešení události nebo přímo incidentu. Definice toho, jakým způsobem a v jakém nejzazším časovém úseku bude incident vyřešený, lze definovat v servisních smlouvách. Stanovené priority jsou pak závazné pro všechny úrovně a skupiny řešící daný incident nebo událost. V některých případech může být priorita změněna v průběhu řešení z praktických, organizačních nebo jiných důvodů, jedná se ale o neprocesní řešení motivované subjektivním hodnocením situace a domluvou s dotčenými stranami [16].

Prvotní zkoumání – Po vytvoření tiketu je nutnost upřesnit symptomy incidentu za pomocí dotazování a ověřování. Pokud existuje aktivní kontakt s ohlašovatelem události, je vhodné držet ho ve spojení a snažit se získat co nejvíc informací i přímým ověřováním funkčnosti a dalším okamžitým dotazováním. Výstupem by měla být kromě popisu nežádoucího stavu i specifikace, co je cílový a požadovaný, a funkční stav. Následně se stav porovnává s existujícími záznamy o pravdivosti tvrzení. Nejdříve je to porovnání s podobnými nebo identickými incidenty, a to je z důvodu, aby nedocházelo k násobnému řešení duplicitních incidentů. Je-li identifikován takový ticket, je potřeba jej jen připojit k takovému, který byl vytvořen jako první záznam. Dále musí být ověřeny znalostní báze, kde se podobný výskyt už může objevit jako jeden z řešených problémů, který prokazuje stejné příznaky. Jestli lze k danému záznamu najít náhradní, nebo dočasné řešení (anglicky workaround), tak v případě použitelnosti jej operátor může navrhnout jako další krok a případně zjistit možnou aplikovatelnost takového řešení na aktuální situaci. Pak přichází na řadu fáze „Vyřešení a obnova“, či rovnou uzavření incidentu, pokud jsou splněny náležité podmínky [16].

Eskalace – ta může probíhat současně s dalšími fázemi. Eskalace představuje způsob, jak získat dodatečné zdroje a informace nutné pro samotné vyřešení anebo jenom urychlení řešení incidentu. Lze definovat dva typy eskalace – první je funkční eskalace sloužící k předání řešení incidentu z nižší úrovně podpory, na úroveň vyšší. Je to z důvodu toho, že nižší úroveň nemá dostatečné znalosti nebo vyčerpala všechen dohodnutý čas k vyřešení. Pro tyto účely musí existovat dohoda pro způsob eskalace, upravující eskalační časy, posloupnosti, rychlost reakce a dodání. Hierarchická eskalace je druhým typem eskalace a dohlíží na to, aby byly zúčastněné strany řádně informovány. Prostřednictvím ní se také řeší nesrovnalosti ohledně odpovědností a priorit. I tyto zásady je potřeba definovat v procesech, které popisují eskalaci jako takovou [16].

Zkoumání a diagnóza – Cílem důkladněji osvětlit co je požadováno opravit, jaký byl průběh incidentu a identifikovat možné příčiny a potenciální řešení. Rovněž je důležité zjistit celkový dopad události. Je-li zjištěno, že udávané dopady nejsou popsané korektně a neodrážejí skutečný stav, je možné jich změnit, rovněž i přehodnotit prioritu události nebo incidentu. Aktivity, které jsou zmiňovány musí být zdokumentovány, ideálně právě k samotnému ticketu, který vytvořil zákazník anebo help desk [16].

Řešení a obnova – Tato fáze řeší implementaci nalezeného řešení, čím se produkt anebo řešení vrací do původního, nebo normálního stavu. Pokud se opravou zabývá vícero

zúčastněných stran, je úkolem toho, kdo je za událost anebo incident odpovědný, koordinovat aktivity pro vyřešení a aktivně komunikovat pro nejrychlejší a jednodušší spolupráci [16].

Uzavření – Závěrečná fáze má za úkol ověření toho, že je náprava kompletně hotová, je korektně zaznamenaná, zkategorizovaná a jednoduše zpracovaná v systému procesem na to určeným. Zákazník by v rámci této fázi měl potvrdit spokojenost s řešením a vyjádřit souhlas s uzavřením události nebo incidentu. V případě, že není jasná příčina této události anebo incidentu, měl by být vytvořen nový ticket kategorizovaný jako „problém“ který je přímým pokračovatelem k nalezení důvodu výpadku [16].

3.5 Proces

„Proces je organizovaná skupina vzájemně souvisejících činností a/nebo subprocesů, které procházejí jedním nebo více organizačními útvary či jednou (podnikový proces) nebo více spolupracujícími organizacemi (mezipodnikový proces), které spotřebovávají materiální, lidské, finanční a informační vstupy a jejichž výstupem je produkt, který má hodnotu pro externího nebo interního zákazníka.“ [29]

Zjednodušeně tedy můžeme proces definovat jako soubor činností transformujících vstupy na výstupy, které se stávají přínosem a/nebo hodnotu. K tomu, aby mohlo dojít k popisované transformaci, musí ještě existovat dostatek energie, podpůrné hmoty (tzn. např. stroje, zařízení, nástroje apod.) a znalostí, a to všechno musí být vzájemně propojené v důsledku činností lidí, strojů, nástrojů, technik a materiálů. [30]

Podnikové procesy jsou součástí všech organizací. V podnicích jsou nejčastěji využívané tzv. klíčové, řídící a podpůrné procesy. Hlavní procesy jsou ty procesy, které vytvářejí přidanou hodnotu směrem k okolí a jejich prostřednictvím se realizují zásadní podnikové aktivity, které souvisí s uspokojováním potřeb zákazníků, nebo i jenom vnitřních potřeb. Prostřednictvím fungujících a dobře řízených procesů může organizace pracovat efektivněji. Řídící procesy slouží k rozvoji a řízení výkonu společnosti. Zabezpečují fungování ostatních procesů tím, že zajišťují integritu a fungování organizace. Do této skupiny spadají procesy manažerské, tedy takové, které zabezpečují, že poslání je naplňováno kvalitně a v souladu s regulátory řízení. Podpůrné procesy zajišťují fungování ostatních procesů, kterým dodávají produkty (hmotné / nehmotné), ale přitom nejsou součástí hlavních procesů. Zabezpečují tedy chod samotné organizace. [29]

3.5.1 Účastníci procesu

Pro každý definovaný proces platí několik jasně definovaných omezení a hodnot. Jednou z takových jsou samotní účastníci procesu, kteří v stupují do případných fází přímo anebo i nepřímo, jako pozorovatelé, nebo ti, kteří na proces jenom dohlíží. Bližší pohled a definice jednotlivých rolí lze rozdělit na několik skupin. [30]

3.5.2 Vlastník procesu

Vlastník procesu má nejen odpovědnost, ale také disponuje dostatečnou pravomocí, je to zároveň osoba, která je odpovědná za dosahování cílů procesu a jeho dlouhodobou efektivnost, monitorování procesu, systematické zlepšování, řešení problémů v průběhu procesu a správu procesu. Jeho náplní práce je například řízení motivace a odměňování pracovníků, spolupráce s finančním oddělením, koordinace činností v rámci procesu, analýza a včasná reakce na měřítka procesu apod. [29].

3.5.3 Příjemce procesu

Subjektem, kterému jsou výsledku procesu určeny se nazývá příjemce procesu. Může to být organizace, člověk anebo i věc ve formě navazujícího procesu. Příjemci se v běžné praxi dělí na interní a externí. Interní příjemci (můžeme označovat i jako zákazníky) jsou zpravidla kolegové, nebo jednotlivá oddělení, externí příjemci už můžou být nezávislé entity vystupující jako společnosti, jednotlivci a další. [29]

3.5.4 Šampión procesu

Je ním osoba, nebo spíš subjekt, která se procesu dlouhodobé účastní a svým chováním a vystupováním podporuje zlepšování procesů. Šampión má znalost toho, jak potřeby samotného procesu, tak i všechny vnitřní závislosti nebo náležitosti procesu a všech souvisejících jednotlivých elementů. Své znalosti a zkušenosti předává dalším osobám například formou dokumentace, nebo školením. [29]

3.5.5 Vedlejší procesní osoby a zdroje

Existuje vícero definicí, jak proces obhospodařovat a které role jsou odpovědné za různé vstupy a činnosti. Jedna z takových definicí určuje několik zařazení, do kterých lze pracovníky a účastníky kategorizovat. Jsou to [30]:

- Dodavatel – subjekt, který zajišťuje vstupy;

- Sponzor – zástupce provozovatele procesu, který má zájem o bezproblémové fungování procesu;
- Manažer – osoba, která se přímo účastní řízení procesu;
- Operátor – osoba, která se procesu přímo účastní. Ovlivňuje pouze výkonnost nebo kvalitu dílčí činnosti, na které se svou prací podílí.

3.5.6 **Produkt procesu**

Produkt procesu je hmotný nebo nehmotný výstup, který slouží k uspokojení potřeb nebo přání zákazníka procesu. Posláním každé organizace je svým zákazníkům buď prodávat nebo jinak poskytovat svoje výrobky, nebo i službu. V tomto smyslu jsou produkty výsledkem činnosti organizací. Produkt ovšem může být označení také pro výsledek činnosti jednotlivce, skupiny lidí, nebo samotného procesu. [29]

3.5.7 **Riziko procesu**

Riziko je nahodilá událost vedoucí ke vzniku škody v nebo z podnikání společnosti. Riziko procesu je určitá událost, jednání nebo stav s následnými nežádoucími dopady na zajištění výsledku procesu a dosažení cíle procesu. [29]

3.5.8 **Hranice procesu**

Určuje se rozmezí pravomocí mezi dodavatelem, vlastníkem procesu a zákazníkem. Hranice procesu jsou součástí zadání zlepšovatelského projektu. Účelem je vymezení oblasti působení konkrétní iniciativy a zefektivňování komunikace mezi členy týmu a ostatními zájmovými skupinami projektu. [30]

3.6 **Procesní řízení**

Procesní řízení neboli Business Process Management (BPM) je soubor činností, které se týkají plánování a sledování výkonnosti zejména realizačních firemních procesů. Velmi často využívá znalostí, zkušeností, dovedností, nástrojů, technik a systémů k měření, kontrole, informování, definování, vizualizaci a zlepšování procesů, aby mohly být úspěšně a důkladně splněny požadavky zákazníků za současné optimální rentability svých aktivit. Další aspekty, které jsou zohledněné v rámci transformace procesů, jsou v rámci ITILu definované následujícím způsobem, vyjádřeným jako procesní řízení.

3.6.1 **Řízení cílů**

Cíle procesu by měly být ve shodě se strategií organizace. Podobný účel má proces správy úrovní služeb knihovny ITIL. Stanoveny by měly být tak, aby byly SMART (specifické, měřitelné, akceptovatelné, realizovatelné a časově omezené). Spolu s definicí cíle, by měla být stanovena kritéria pro hodnocení úrovně dosažení cíle [19].

3.6.2 **Řízení výkonu**

Výkonnost procesu je standardně ve společnosti posuzována podle ukazatele výkonnosti. KPI (Key Performance Indicators) jsou indikátory, ukazatele či metriky výkonnosti přiřazené procesu, službě, organizačnímu útvaru, nebo celé organizaci a které vyjadřují požadovanou výkonnost (kvalitu, efektivnost nebo hospodárnost). KPI může být vypočítán jako úroveň dosažení cílů procesu s ohledem na náklady, kvalitu nebo rychlost. Výkon každého procesu by měl být řízen s využitím zpětné vazby [20]:

- Proces a jeho plnění je pravidelně vyhodnocované;
- Pokud není plnění v rámci dohodnutých mezí, jsou učiněny nápravné kroky.

Jedním z nápravních aktivit může být například identifikace úzkých míst dle teorie omezení a korektní upravení zdroje, kroků a všeho, co s tím souvisí. Tento postup úprav má název „Průběžné zlepšování procesu“ (anglicky Business Process Improvement, dále BPI). Pokud ale nelze nápravu vykonat jednoduše zvýšením anebo jakoukoliv jednoduchou změnou výkonu, je nutné aplikovat takzvaný reengineering[6] procesu (anglicky Business Process Reengineering, dále BPR), který má za následek kompletní změnu procesu a nastavení KPI [19].

Správný popis procesu je základ, bez kterého nelze aplikovat korektní řízení. Stejně tak musí být známe všechny skutečnosti, které tento proces ovlivňují. Procesy dodržují a aplikují pracovníci, kteří tím dosahují výsledků a od procesu samotného záleží i to, jak velké úsilí je nutné aplikovat k splnění požadovaného cíle. Proces by měl poskytovat jednoznačný návod k tomu, jak lze dosahovat dostatečné kvality práce a výstupů nezávisle na individuálních znalostech.

Použitím BPR je možné dosáhnout kvality jen pokud lze korektně definovat postup, jak přesně žádaných výstupů dosáhnout. Nežádoucí je však velké riziko selhání, pokud je záběr

[6] Reengineering – přeplánování, přepracování technického návrhu

BPR příliš široký a není správně aplikovaný. Tyto rizika lze eliminovat korektním návrhem a řízením kvalifikovanými prostředky a pracovníky [19].

3.6.3 Řízení zdrojů

Požadovaný výkonu procesu nelze zabezpečit bez korektního a kvalifikovaného řízení zdrojů. Nalezení optimálních procesů je tím složitější, čím je složitější organizační struktura. Pracovní zatížení pracovníků je nutné optimalizovat v nejvyšší možné míře. Samotný proces není jediným požadavkem na práci a pracovníci mají i další povinnosti, které se jakýchkoliv procesů vůbec netýkají. Tento prostor je možné vytvořit například změnou organizační struktury, nebo vytvořením nové pracovní pozice či jiným zásahem do samotných procesu [19].

3.6.4 Řízení návazností

Zajištění kompatibility mezi vstupy a výstupy jednotlivých činností a procesů je jednoznačně úloha kompetentní osoby, která má na starost řízení návazností. To lze dosáhnout návrhem procesů a souvisejících workflow, které s různými návaznostmi počítají [19].

3.7 Bezpečnost dat a informací

Společnost by měla mít zavedenou bezpečnostní politiku ve vztahu k informacím, která musí být, pokud je to vhodné, komunikovaná všem příslušným zaměstnancům a zákazníkům. Na bezpečnost informačních služeb a informací se vztahuje rodina norem ISO 27000, jejímž cílem je zavedení jednotného systému řízení pro všechny oblasti a v návaznosti na tuto normu taky umožnění budování integrovaného systému řízení. Jedná se o normy:

- ISO 27000, která uvádí definice pojmů a terminologický slovník pro všechny ostatní normy z této série;
- ISO 27001, která je hlavní normou pro systém řízení bezpečnosti informací (ISMS), dříve to byla norma BS 7799 část 2, podle které byly ISMS certifikovány. Norma ISO 27001 byla publikována koncem října 2005;
- ISO 27002 (dříve normy ISO/IEC 17799 a BS7799-1), která je aktuální verzí normy, která byla vydána v červnu 2005 jako ISO/IEC 17799:2005 a označena ISO 27002:2005 v roce 2007;
- ISO 27003, která je návodem k implementaci ostatních norem;

- ISO 27004, která bude vydána pod názvem "Information Security Management Metrics and Measurement", (Metriky a měření);
- ISO 27005 (dříve BS 7799-3), vydaná pod názvem "Information Security Management Systems – Guidelines for Information Security Risk Management" a nahrazuje BS 7799 část 3. (Informační technologie – bezpečnostní techniky – mezinárodní uznávaná směrnice pro uznání osob pro řízení certifikace / registrace zabezpečení systémů řízení informací);
- ISO 27006, která je vydaná pod názvem "Information technology – Security techniques – International accreditation guidelines for the accreditation of bodies operating certification / Registration of information security management systems", (Informační technologie – bezpečnostní techniky – Návody pro mezinárodní akreditování v oblasti certifikace a registrace řídících systémů);
- ISO 27007, která uvádí doporučení pro auditování ISMS;
- ISO/IEC TR 27008, vydaná pod názvem „Guidance for auditors on ISMS controls", zaměřená na provozování auditu kontrolu informační bezpečnosti
- ISO/IEC 27009, vydaná pod názvem „Essentially an internal document for the committee developing sector/industry-specific variants or implementation guidelines for the ISO27K standards", obsahuje základní specifikaci normy pro specifiká odvětví v rámci IT;
- ISO/IEC 27010, vydaná pod názvem „Information security management for inter-sector and inter-organizational communications", (Management bezpečnosti informačních technologií v oblasti mezisektrorní a meziorganizační komunikace);
- ISO/IEC 27011, vydaná po názvem „Information security management guidelines for telecommunications organizations based on ISO/IEC 27002", (Návod pro management bezpečnosti informačních technologií v oblasti telekomunikací);
- ISO/IEC 27013, vydaná pod názvem „Guideline on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1", (Návod pro ingrovanou implementaci norem);
- ISO/IEC 27014, vydaná pod názvem „Information security governance", (Řízení zabezpečení informačních technologií);

- ISO/IEC TR 27015, vydaná pod názvem „Information security management guidelines for financial services“, (Bezpečnost nformačních technologií v oblasti financí);
- ISO/IEC TR 27016, vydaná pod názvem „Information security economics“, (Ekonomika v bezpečnosti informačních technologií);
- ISO/IEC 27017, vydaná pod názvem „Code of practice for information security controls based on ISO/IEC 27002 for cloud services“, (Příručka použitelnosti informačních technologií v cloudu);
- ISO/IEC 27018, vydaná pod názvem „Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors“, (Příručka použitelnosti v oblasti identifikačních údajů);
- ISO/IEC TR 27019, vydaná pod názvem „Information security for process control in the energy industry“, (Informační bezpečnost v oblasti energetiky);
- ISO/IEC 27031, vydaná pod názvem „Guidelines for information and communication technology readiness for business continuity“, (Příručka použití informačních technologií zaměřené pro udržitelnost obchodu);
- ISO/IEC 27032 – Doporučené postupy v oblasti „Cybersecurity“
- ISO/IEC 27033 – Síťová bezpečnost
- ISO/IEC 27034 – Aplikační bezpečnost
- ISO/IEC 27035 – Bezpečnost informačních technologii v Incident Managementu
- ISO/IEC 27036 – Bezpečnost informačních technologii v komunikaci s dodavateli
- ISO/IEC 27037 – Vydaná pod názvem „Guidelines for identification, collection, acquisition and preservation of digital evidence“, (Návod pro obsluhu digitální evidence);
- ISO/IEC 27038 – Specifikace digitální redakce digitálního obsahu a dokumentů
- ISO/IEC 27039 – Prevence proti neoprávněnému přístupu
- ISO/IEC 27040 – Zabezpečení digitálního úložiště
- ISO/IEC 27041 – Zprocesování investigativy
- ISO/IEC 27042 – Analýza digitálních záznamů/důkazů
- ISO/IEC 27043 – Vyšetřování Incidentů
- ISO/IEC 27050 – Vyhledávaní elektronických zařízení

- ISO 27799 – Vydaná pod názvem „Information security management in health using ISO/IEC 27002 - guides health industry organizations on how to protect personal health information using ISO/IEC 27002“, (Použití norem zabezpečení informačních technologií v zdravotnictví);

Z palety norem, které se bezpečností věnují nebo ji přímo určují, lze definovat různé aspekty procesů a celkově i práci s daty (uložení, archivaci, strukturu atp.). Bezpečnostní opatření ale musí být použitá k:

- Implementaci požadavků bezpečnostní politiky;
- Řízení rizik spojených s přístupem ke službám nebo systémům.

Veškerá bezpečnostní opatření musí být zdokumentovaná. Dokumentace musí popisovat rizika, ke kterým se opatření vztahuje, a způsob provozování a udržování tohoto opatření. Vliv změn na opatření musí být ohodnocen před tím, než jsou změny implementovány.

Uspořádání, které zahrnuje přístup třetích stran k informačním systémům a službám, musí být založeno na formální smlouvě, která stanovuje všechny nezbytné požadavky na bezpečnost.

Bezpečnostní incident musí být oznámen a zaznamenán v souladu s postupem pro management incidentů hned, jak je možné. Musí existovat postupy, které zajistí, že všechny bezpečnostní incidenty jsou prošetřeny a že jsou přijata opatření v oblasti kontroly. Musí existovat mechanismy, které zajistí, že typy, objemy a vlivy bezpečnostních incidentů a selhání jsou kvantifikovány a monitorovány, a poskytují vstupy do plánů zlepšování služeb [21].

3.8 Ochrana osobních údajů

Procesní uchopení problematiky řešení incidentů je ve své podstatě nakládání s informacemi. Tyto informace můžou být i osobního charakteru a je to i z toho důvodu, že automatizace aktivit kolem hledání řešení nejsou z velké části technologicky možné (rok 2019, pozn. autora), a je nutné do procesů zapojit primárně lidský faktor. Neméně důležité je i to, co bude předmětem problému a s jakými údaji tento lidský faktor bude ve spojení. Typickým příkladem může být podpora databáze oddělení lidských zdrojů, systému zdravotnického zařízení s informacemi o pacientech, nebo i sázkové společnosti s miliony verifikovaných údajů o stávkujících. Z toho důvodu je nevyhnutelné při výběru nástroje pro incident management řešit variantu nutnosti ochrany osobních údajů.

3.8.1 **Osobní údaj**

Dle § 4 písm. a) zákona č. 101/2000 Sb. se „*osobním údajem rozumí jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, pokud lze subjekt údajů přímo nebo nepřímo identifikovat na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu*“. [4, § 4 písm. a)] [34]

Subjektem údajů je ale myšlena pouze fyzická osoba. Z předešlé definice je patrné, že osobním údajem může být jakákoli informace. Zákon č. 101/2000 Sb. o ochraně osobních údajů (dále jen ZoOÚ) informace nijak neomezuje, znamená to, že mohou být i nepravdivé a k tomu dává ZoOÚ nástroje, jak se s takovou situací vyrovnat [35].

Jedná se o informace vypovídající o soukromí každého z nás. Tyto informace se týkají osob, zálib, zvyklostí, vlastností nebo názorů a majetkových poměrů. Mimo jiné mohou vypovídat o tom, jaké jsou vztahy jednoho člověka k ostatním, o jeho zdravotním stavu a stylu života. Osobním údajem tedy rozumíme jakýkoliv údaj týkající se naší osoby [22].

Osobní údaje můžou být i informace, které přímo nebo nepřímo identifikují jednotlivce a obsahují konkrétní on-line identifikátory, typicky IP adresy, email, soubory cookies, digitální otisky prstů a údaje, které by mohly identifikovat jednotlivce [23].

3.8.2 **Informace**

Za informaci jsou považována přesná a včasná data, jež mají určitou specifikaci a jsou organizována za účelem prezentace v kontextu dávajícím smysl a význam. Cílem informací je zvýšit porozumění a zároveň snížit nejistotu. Každá informace má svoji důležitost, protože je schopná ovlivnit chování, rozhodování a v neposlední řadě i výsledky [24].

3.8.3 **Data**

Obecně jsou data výrazem pro údaje, jež se používají pro popis jevu nebo vlastnosti pozorovaného objektu. Jedná se například o číselné hodnoty z tabulky. Data jsou přitom podmnožinou informace, dokonce tvoří jakousi vstupní surovinu pro vytvoření plnohodnotné informace [24].

3.8.4 **Právní zakotvení ochrany osobních údajů**

Základním právním předpisem, jenž upravuje ochranu osobních údajů v České republice, je zákon č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů s je doplněný tzv.

Obecným ustanovením „GDPR – General Data Protection Regulation“. V zákoně č. 101/2000 Sb. je určeno a zakotveno vymezení jeho působnosti a pojmů týkajících se dané problematiky, práva a povinnosti související se zpracováním osobních údajů, likvidace osobních údajů, ochrany práv subjektu údajů, nápravy nemajetkové újmy či škody a také předávání osobních údajů do dalších států. V rámci tohoto zákona jsou jednak definovány základní pojmy jako osobní údaj, citlivý a anonymní údaj, jejichž definice už v rámci této práce zmíněná je. Tyto pojmy můžeme považovat za základní stavební kameny ochrany osobních údajů, i když nejsou revoluční, ve své podstatě existovali již v původní právní úpravě zákonu č. 101/2000 Sb. Novinkou je jejich jasné vyjmenování, stanovení odpovědnosti a povinnosti dokládání souladu. Z nařízení vyplívají ještě další zásady:

Dále jsou zde definovány tyto pojmy [26]:

- **subjekt údajů**, jímž je fyzická osoba, k níž se osobní údaje přímo vztahují;
- **zpracování osobních údajů**, kdy se jedná o operaci či soustavu operací prováděných správcem nebo zpracovatelem, ať už automatizovaně, či jinými prostředky;
- **shromažďování osobních údajů**, což je systematický postup či soubor postupů, kdy cílem je získat osobní údaje za účelem jejich dalšího uložení pro jejich další zpracování;
- **uchovávání osobních údajů**, jedná se o udržování údajů v takové podobě, aby mohly být dále zpracovávány;
- **blokování**, tedy operace nebo soustava operací, prostřednictvím kterých dojde k omezení způsobu či prostředků ke zpracování osobních údajů, a to po předem stanovenou dobu;
- **likvidace osobních údajů**, čímž se rozumí fyzické zničení nosiče osobních údajů, fyzické vymazání, popřípadě přerušení jakéhokoliv dalšího zpracování;
- **správce**, má odpovědnost za zákonné korektní zpracování osobních údajů. Osoba správce určuje činnosti, které jsou spojené se zpracováním;
- **zpracovatelé**, jsou osoby, které mají přístup k osobním údajům, které shromáždil správce nebo je zpracovávají. Zpracovatelem může být i společnost, která osobní údaje nijak nezpracovává, ale jsou uloženy na jejích serverech;
- **zveřejněný osobní údaj**, kdy se jedná o takový údaj, jenž byl zpřístupněn prostřednictvím hromadných sdělovacích prostředků či jiným veřejným sdělením;
- **evidence nebo datový soubor osobních údajů**, tedy jakýkoliv soubor osobních údajů, jenž je uspořádán či zpřístupněn na základě společných, popřípadě zvláštních podmínek;

- **souhlas subjektu údajů**, kdy subjekt údajů projeví svobodně a vědomě vůli, že souhlasí se zpracováním svých osobních údajů;
- **příjemce**, přičemž jím je každý ze subjektů, jimž jsou osobní údaje zpřístupněny.

3.8.5 Působnost zákona

Zákon o ochraně osobních údajů se vztahuje na ty osobní údaje, které jsou zpracovávány státními orgány, dále orgány územní samosprávy, jiné orgány veřejné moci a fyzické či právnické osoby. Spadá pod něj i veškeré zpracování osobních údajů, jak automatizované zpracování, tak prostřednictvím jiných prostředků [26].

Další vyjmenované pole působnosti v zákonu se týkají zpracování fyzickými osobami pro jejich vlastní potřeby, shromažďování dat, které nejsou dále zpracovávané anebo podnět pro zpracování přichází z vnějšku. Statistické zpracování má na to určený vlastní zákon (101/2000 Sb), vliv při implementaci řešení pro incident management je spíše teoretický. Stejně tak se je incident management mimo působnost vědeckého využití, a tudíž je krytí zákonem pro potřeby implementace řešení irelevantní [26].

3.8.6 Povinnosti při/během zpracování osobních údajů

Nejdůležitější zásada je „Zásada zákonnosti“ protože říká, že správce může osobní údaje zpracovávat či je mít pouze má-li k tomu alespoň jeden právní důvod. Pokud žádný právní důvod nemá, nebo zanikne a zároveň neuplatní jiný právní důvod, má povinnost osobní údaje zlikvidovat. Pokud uplatní jiný právní důvod pouze na část údajů, musí údaje jejichž zpracování není pokryto tímto právním důvodem zlikvidovat.

Následující zásady můžeme považovat za důležitou součást ochrany osobních údajů. Tyto zásady jsou obsažené i v původní právní úpravě zákonu č. 101/2000 Sb., změnou prošlo jejich jasné vyjmenování, stanovení odpovědnosti a povinnosti dokládání souladu a z kterého vyplývají i jiné zásady:

- Bezpečnost dat;
- Odpovědnost správce;
- Povinnost prokazování;
- Mezinárodní transfery.

Povinnosti týkající se zpracování osobních údajů se týkají správce a zpracovatele, ale také jejich zaměstnanců a jiných osob, které osobní údaje zpracovávají na základě smluvního vztahu se správcem nebo zpracovatelem.

3.8.7 **GDPR**

Obecně vzato, je GDPR rozšířením a zpřesněním popisu a výkladu klíčových instrumentů pro ochranu osobních údajů už existujícího zákona. Definice, kterých se to týká, a které byly detailněji rozpracovány a zpřesněny jsou například:

- nutnost disponovat pro zpracování právním důvodem;
- nebo zabezpečení osobních údajů;
- transparentnost vůči subjektu údajů;
- a mnoho dalších.

Obecné nařízení přináší nástavbu, která spočívá v nových povinnostech, které budou pro české správce nové. Jedná se zejména o tyto povinnosti [27]:

- povinnost vést záznamy o činnostech zpracování;
- posouzení vlivu na ochranu osobních údajů;
- předchozí konzultace;
- ohlašování případu porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů;
- oznamování případu porušení zabezpečení osobních údajů subjektu údajů;
- ustavení pověřence pro ochranu osobních údajů.

Autor Bolognini se ve svém článku zaobírá použitím anonymizace. Cílem této metody je nezvratně zabránit jakékoliv identifikaci subjektu. Jedná se o proces, který však musí respektovat podmínky stanovené Obecným nařízením, které říká, že konkrétní účely, pro něž jsou zpracovávány osobní údaje, musí být legitimní a určené v době sběru osobních údajů. Techniky anonymizace se používají pro ukládání dat, pro možnost jejich případného zveřejnění či sdělení třetím osobám, dále pro statistické, historické a vědecké účely [28].

4 Analytická část

Zdokumentováním existujících procesů při řešení incidentů je prvním krokem k dosažení cíle, kterým je návrh na změnu směrem k Incident managementu dle rámce ITSM. To nelze jiným způsobem, než je aktivní zkoumání existujících záznamů, dokumentace a aktivním diskutováním o konkrétních situacích s jednotlivými řešiteli různých událostí v rámci společnosti. Jednoduchým dotazováním dotčených osob, které chyby nahlašují lze dosáhnout informace jak o spokojenosti, tak i o reálné délce trvání jednotlivých problémů.

4.1 Incident Management v Nejmenované společnosti

Pokud se společnost rozhodne pro změnu, je nutná především vnitřní motivace. Snaha o potřebnou transformaci je na základě této motivace vyšší. Ke zdárnému výsledku se ale nemusí společnost dopracovat ani přes veškerou snahu, pokud není jasně definovaný cíl. Jediným měřidlem případného úspěchu je viditelný soubor klíčových hodnot výkonnosti procesů nebo pravomocí. Tento může být aplikován v jakékoliv společnosti. Neexistuje však žádné konkrétní doporučení, které by bylo možné využít k dosažení procesů za všech situací a ve všech společnostech [31].

Pisatel pracuje pro společnost, která operuje v segmentu loterií, stávek a hazardních her. Hlavním oborem podnikání jsou online služby a hry. Pravé jméno společnosti není zveřejněné z důvodu bezpečnosti a nesouhlasu managementu. Proto je zvolený fiktivní název Nejmenovaná stávková společnost a.s. (dále jenom Nejmenovaná). Společnost se radí do segmentu středně velkých společností, jelikož zaměstnává přibližně 400 zaměstnanců s mezinárodní působností.

V Nejmenované stávkové společnosti je snaha o zefektivnění procesů a výkonu práce v oblasti IT. Byla proto zvolená cesta implementace ITSM podle ITIL, která má za úkol napravit a vyladit stávající procesy Incident managementu. Management společnosti nelimitoval implementaci žádným omezením a je nakloněný každé odůvodněné změně, jak personální, tak i organizační a technologické. Z toho důvodu byla vypracovaná pilotní analýza aktuálního stavu. Pisatel vykonal analyzování stavu řešení požadavků na opravu a jednotlivých servisních zásahů.

4.1.1 **Analýza aktuálního stavu**

Zavedení jakékoliv změny musí předcházet analýza Ta by měla být dostatečně podrobná a měla by mapovat aktuální stav procesů, který ve společnosti existuje. Analýza by měla být především nestranná.

Přechod ITSM na procesy, které zmiňuje ITIL, je záležitost, která se dotýká jak organizační struktury, tak přidělování rolí. Je nutné zmínit i možnou změnu v procesech jako takových a zaměřit se na potřeby, které jsou obecně k fungování ITILu nevyhnutelné. Příkladem je neúplná, nebo zcela chybějící CMDB[7].

Analýza musí být dostatečně důkladní. Proto postup, který má být zvolený je takzvaně zdola nahoru, který umožní vymodelování existujících procesů ve společnosti. Iterativním prováděním různých pracovních schůzek a konzultací, a doplňováním nových informací do pracovní databázi znalostí, můžou pak být vytvořené a graficky zobrazené modely procesů, které jsou analyzované.

4.1.2 **Organizační struktura**

Bez jasně definované organizační struktury nelze jednoznačně vyhodnocovat efektivitu a motivovat jednotlivé oddělení k požadovaným výkonům Jelikož z analýzy je využitá část s definováním stavu kolem Incident managementu, je vhodné zaměřit se na to, jaké skupiny v Nejmenované společnosti reálně pracují s incidenty.

Skupiny (nebo přímo oddělení), byly nejdříve identifikované zkoumáním organizační struktury. Následně byly někteří pracovníci slovně dotázaní na způsob práce, aby potvrdili, nebo vyvrátili reálnou činnost na incidentech. Dotčené skupiny, které jsou pro Incident Management relevantní, mají přímo v popisu práce následující činnosti:

- Analytici
- Administrátoři
- Vývojáři
- Testeři
- Projektoví manažeři
- Pracovníci helpdesku

[7] Configuration Management Database – místo pro uchovávání informací pro jednotlivé položky ve správě ITSM, častokrát spjatá s pojmem CI – Configuration Item

Tyto skupiny mají v organizační struktuře jasně definované vedoucí týmů a zároveň i přímo odpovědné vedení.

4.1.3 Životní cyklus incidentů v Nejmenované společnosti

Nejmenovaná společnost působí na trhu už několik let a za tu dobu, už má zavedený alespoň částečný způsob pro řešení incidentů. Nároky na kvalitu a rychlost řešení incidentu jsou však oproti skutečnému stavu neporovnatelně vyšší a proces, který společnost využívá nemá ideální podobu. Z analýzy vyplynulo, že společnost nevyužívá hierarchickou strukturu podpory na bázi tří hladin. Znamená to, že v případě jakékoliv chyby může řešit incidenty primárně vývojář od jeho vzniku až po jeho konec. Jelikož je práce vývojáře hodnocena v jiné cenové hladině, je tak jeho zatěžování i incidenty týkajícími se pouze provozu vysoce ztrátové a neefektivní.

Řešení incidentů se taky potýká s nekorektním, neúplným anebo variabilním workflow. To v Nejmenované společnosti nemá pevně dané stavy a ani zodpovědného vlastníka. Stává se, že v případě, že ten není jasně definovaný, dochází k různým nežádoucím situacím, jako jsou prodlevy při zpracování a řešení.

Proces řešení incidentů zároveň probíhá paralelně s procesem řízení změn, a to není optimální, protože opravenou chybu tak znovu zanáší do sytému změna, kterou řeší jiný vývojář, pracující na stejném produktu.

4.1.4 Způsob sledování incidentů

Ve společnosti není ujednocený systém pro sledování veškerých incidentů. Vývojové oddělení, které zaštiťuje analytiky, vývojáře, testery a projektové manažery využívá pro práci nástroj Jira od společnosti Atlassian, určené primárně pro agilní programování. Nástroj umožňuje sledovat různé typy úloh, jednou z nich je i takzvaný „Bug“.

Funkce helpdesku se omezuje na jednoduché řešení hardwarových problémů, na přidělování oprávnění a správu uživatelů v podnikovém Active Directory[8]. Helpdesk v případě požadavku na opravu, kterou nemá v kompetenci, předává na jiné oddělení (HR, vývoj) emailem, pro zakládání „bugů“ vývojářům helpdesk nemá oprávnění. Veškerá evidence záznamů o požadavcích je ve skupinovém emailu a v malém množství v různých excelovských tabulkách na sdílených discích.

[8] Systém pro správu uživatelů, jejich oprávnění a dalších informací jako jsou telefonní číslo, email, adresa apod.

4.1.5 **Analýza nástroje pro správu incidentů**

Obecně platí při jakékoliv analýze, že pokud existuje nástroj, který je z hlediska funkčnosti primárně určený na použití v Incident Managementu, je nutné analyzovat jeho schopnosti a možnosti další konfigurace a rozšíření. Manažerská analýza existujícího nástroje je vítaná, avšak není nevyhnutná. Na konečné posouzení a odporučení analýzy však manažér může mít vplyv.

Zaměření na funkcionalitu a vlastnosti by se mělo týkat především:

- Možností kategorizace incidentů, změnových požadavků apod.
- Plnění požadavků v rámci GDPR
- Nutnost možnosti formovat workflow
- Efektivita komunikace mezi společností a zákazníkem
- Celkovou robustnost a napojení na vnitřní systémy společnosti (například AD, emailový systém, CMDB apod.)
- Případně i na potřeby zabezpečení a splňování norem ze skupiny ISO 27000

Situace ohledně nástroje v Nejmenované společnosti vyplývá z analýzy, která definuje tyto primární nedostatky:

- Ve společnosti nepanuje stejné názvosloví, požadavek na změnu se častokrát zaměňuje s požadavkem na opravu
- Není určený hlavní nástroj pro sledování incidentů a změnových požadavků a z toho vyplývá množství větvících se nedostatků – nemožnost sledování času, ztrácející se informace apod.
- Workflov pro zpracování požadavku existuje, avšak není striktně dané a bývá častokrát porušované
- Zabezpečení proti neoprávněnému přístupu k informacím je minimální
- A další.

4.2 Tvorba procesů pro Incident Management

Podklady pro procesů pro Incident management v rámci společnosti jsou dané analýzou. Zavádění ITILu a přizpůsobování stávajících požadavků lze provést postupným porovnáváním současného stavu a iterovaným zaváděním nových prvků do existujícího procesu. Iterace se bude týkat následujících konkrétních bodů:

- Zaznamenání incidentu

- Určení priority
- Určení kategorie
- Aktualizace záznamů
- Eskalace
- Vyřešení
- Uzavření

Potřeby na propojení procesu v rámci Incident managementu s ostatními procesy lze zobrazit pomocí diagramu:

Obrázek 4: Vstupy a propojení Incident Managementu (zdroj: [16])

Tento diagram nemusí být úplný, jelikož ve společnosti může existovat množství dalších vstupů, jako například správa přístupu, nebo správa financí. Pokud mají tyto vstupy vplyv na formování procesů, musí být zahrnuté do iterace při hledání výsledného řešení.

4.2.1 Postup pro navržení procesů a nástroje

Způsobů pro nalezení řešení a dopracování se k cíli, čímž jsou jasně stanovené procesy a nástroj pro Incident Management, může být několik. Každý má určitou postoupnost a trvání, záleží však na společnosti a integrátorovi změn, kterou variantu zvolí [32]:

a) Důkladné zkoumání a kategorizace znalostí získaných analýzou
b) Definování stěžejních bodů podle ITIL
c) Vytvoření modelu
d) Posouzení managementem
e) Provedení simulace
f) Akceptace výsledků a kontrola proveditelnosti

g) Pilotní implementace, školení osob a ladění chodu
h) Ukotvení v provozu

Kroky a) až c) je vhodné zopakovat i několikrát s tím, že se snižuje riziko zavedení chyby nebo nepochopení aktuálního stavu a potřeb společnosti.

Důležitým bodem je i rozhodnutí o způsobu zavádění požadovaných změn do praxe. Způsobů, jakým lze tuto aktivitu realizovat je několik, pro Nejmenovanou společnost se nabízí realizace několika způsoby:

- Pilotní projekt pro malou část společnosti
  - Výhody – možnost ověření nového řešení na ještě nezavedeném odvětví
  - Nevýhody – malý vzorek problémů, nutnost mít „nové“ oddělení apod.
- Paralelní běh zavádění změn v rámce celé společnosti
  - Výhody – existující situace můžou být překlopené do řešení původním způsobem
  - Nevýhody – extrémně složité udržování kontinuity a přehledu práce
- Přechod po částech
  - Výhody – možnost postupného a pečlivého zavádění změn v společnosti a to je menší riziko zanesení chyby
  - Nevýhody – přechod je dlouhotrvající a nemusí se vůbec povést
- Velký třesk
  - Výhody – rychlá a jasná změna, někdy jediná možná
  - Nevýhody – množství „porodních“ bolestí, které se okamžitě projevují v chodu společností, náročnost na přípravu a realizaci

Způsob, který bude zvolený záleží především na schopnostech a potřebách společnosti. Výhody i nevýhody jsou u každého ze způsobu enormní, je proto nevyhnutné pečlivě zvážit všechny varianty a zvolit optimální.

4.2.2 **Definice procesu správy incidentů**

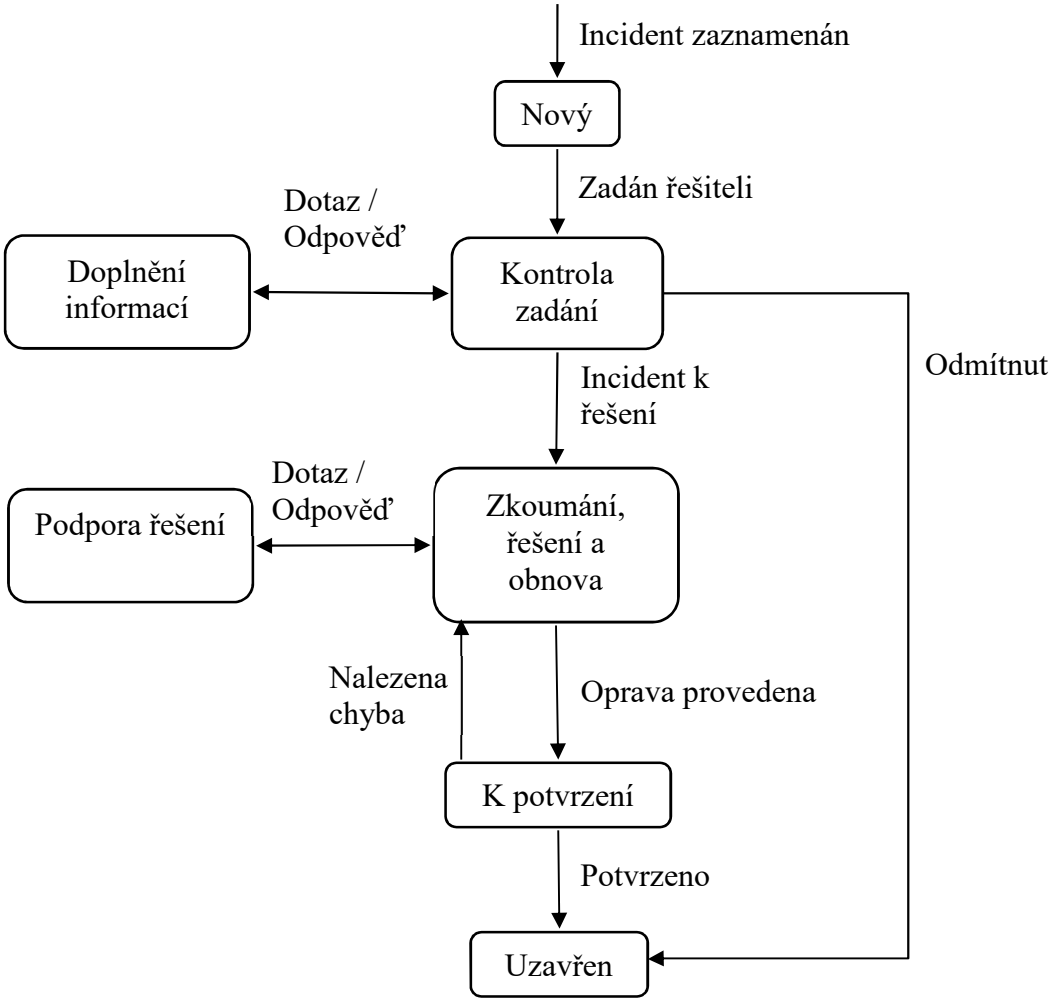
Důležitý je subproces při vytváření, kterým vzniká incident jako takový. Incident může být vytvořený i automatickým systémem, v praxi (rok 2019) je jednodušší k situaci přistupovat za použití lidského faktoru. Ten může probíhat následovně:

a) Identifikace chyby
   a. Přímé vytvoření Incidentů Oznamovatelem

b. Oznámení o chybě helpdesku

b) Vytvoření Incidentu Helpdeskem

Dalším krokem je pak samotný proces řešení Incidentu. Za plnění je odpovědný Helpdesk, který má práci s incidenty i v popisu práce jako standardní činnost. Každý takový incident prochází workflow. Za každý stav je odpovědná skupina, nebo přímo konkrétní vlastník. Workflow lze zobrazit následovně:



Obrázek 5: Teoretické workflow průběhu řešení incidentu (zdroj: [16])

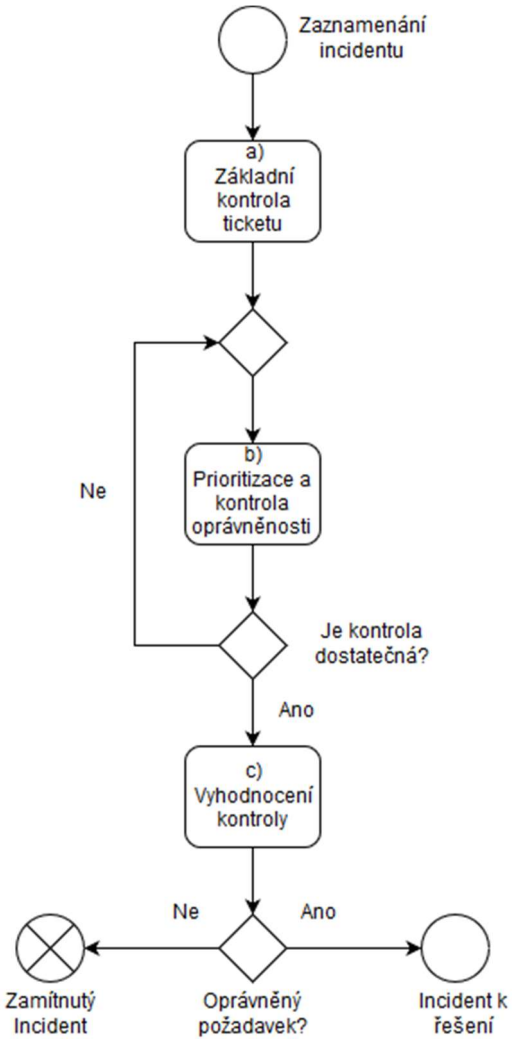
4.2.3 **Zprocesování a validace incidentu**

Nástroj pro správu požadavků by měl umožňovat automatické stanovení kategorie a priority na základě zadaných vstupů. Pomůckou při kategorizaci je jednoznačně databáze použitých produktů a prvků v rámci infrastruktury, na základě které je pak zřejmé, zda může být daný incident nebo požadavek zadán nebo nahlášen zrovna s konkrétní požadovanou prioritou. Prostřednictvím této databáze lze vyloučit i případné neautorizované založení incidentu. To

probíhá ruční kontrolou. ITIL definuje to, že by ji měl zajistit Helpdesk, pokud má dostatečné oprávnění a přístup k datem a umí využít dodatečné prostředky k adekvátní kontrole. U větších společností jsou pro validaci určené specializované skupiny, častokrát s přímým kontaktem na zákazníka. V několika případech, ale lze přistoupit i na takzvanou eskalaci, kdy prvotní oznámení není validované Helpdeskem. ITIL tuto praktiku nijak nevylučuje.

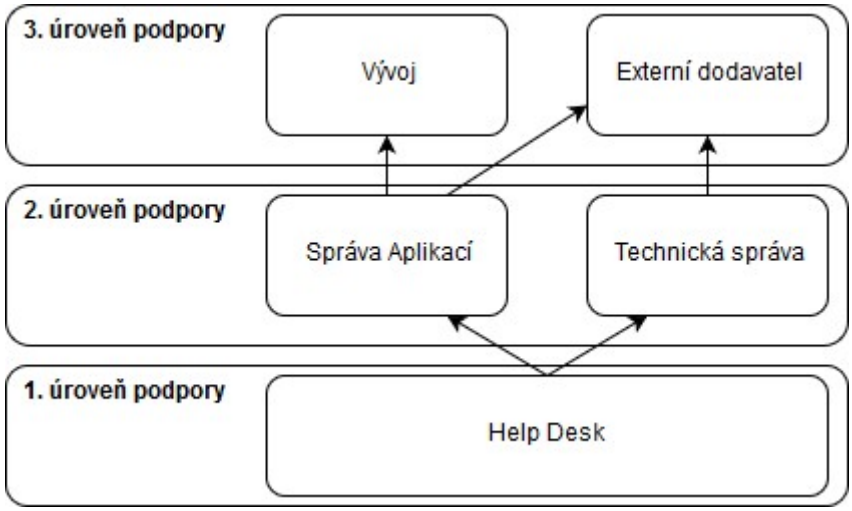
Celkový postup při validaci incidentu lze provést ve čtyřech krocích, kterými jsou:

- Základní kontrola ticketu
- Prioritizace a kontrola oprávněnosti
- Vyhodnocení kontroly
- Zamítnutí nebo potvrzení incidentu



Obrázek 6: Sled kroků validace incidentů (zdroj: [16])

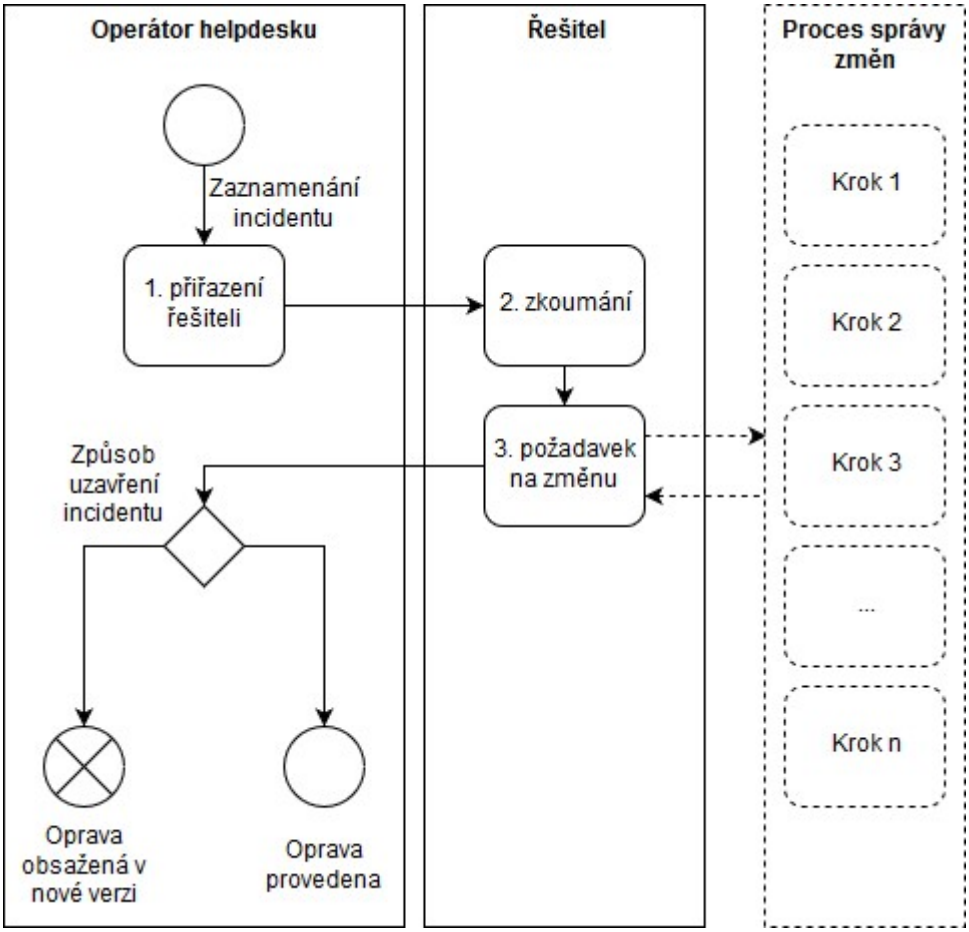
V případě, že je zřejmé, že incident nemůže být vyřešen pracovníky Helpdesku, dochází k funkční eskalaci. To znamená, že incident je předán na řešitele druhé úrovně (zvláštní tým dle oblasti, které se incident týká – vývojáři, administrátoři...). Podobně může být řešení Incidentu eskalováno na třetí úroveň podpory, kterým může být i samotný dodavatel externí služby (hardware, různé aplikace). K hierarchické eskalaci dochází, pokud je zřejmé, že incident nebyl/nebude vyřešen včas a je třeba přidělit dodatečné zdroje na řešení daného incidentu, nebo naplánovat mimořádné kroky. V rámci hierarchické eskalace jsou informováni příslušní IT manažeři. Eskalační matice lze zakreslit způsobem ve třech vrstvách. Jinak dimenzovaná eskalační matice je znázorněná hierarchicky, podle rozložení firemní struktury.



Obrázek 7: Eskalační matice při řešení incidentů (zdroj: [16])

4.2.4 Investigace incidentu a náprava

ITIL stanovuje to, že každá změna musí být evidovaná. Vzhledem k vysokému provázání správy incidentů s procesem správy změn je vhodné navrhnout workflow způsobem, aby byly navzájem ovlivněné a závislé co nejméně. Někdy je možné řešení incidentu přesunout, nebo spíš navázat na zaváděnou změnu. Následnou komunikaci operátora helpdesku, řešitele a spolu s procesem správy změn lze znázornit, tak jak je to na následujícím obrázku (Obrázek č.8).



Obrázek 8: Proces řešení incidentu s ohledem na změnové požadavky (zdroj: [16])

Proces správy změn lze v určitých případech eliminovat úplně. Zejména v prostředí, které není dynamicky se rozvíjející, nebo jde o nekritické a neproduktivní prostředí.

4.2.5 Eskalace a management incidentu

Subproces pro eskalaci umožňuje service desku vykonávat všechny činnosti potřebné k vyřízení incidentu i když pro jejich samostatné vykonávání nemá vytvořeny dostatečné možnosti a schopnosti. Tyto můžou být doplněné dodatečně přímým zásahem vyššího stupně podpory. Neméně důležitou funkcí je zajišťování kontaktu se zákazníkem, když řešitelé potřebují získat informace a zajistit spolupráci s oznamovatelem incidentu. Informace o aktuálním stavu zvyšuje spokojenost zákazníka, který vyžaduje informace o aktuálním dění a řešení kolem incidentů.

4.3 Definice požadavků na produkty

Za zdárné zavedení Incident managementu lze považovat takové, které splňuje veškeré požadavky na funkčnost, které šetří čas a peníze, a konkurenceschopnost společnosti. Pro společnosti, které zpracovávají desítky až stovky různých požadavků denně, je vhodné zavést systém na to speciálně určený. Řešení, které poskytují dostatečnou rychlost, spolehlivost, jsou robustní a splňují požadavky na funkčnost, je na světovém trhu několik. Výběr toho správného může ovlivnit běh a zisk společnosti na další roky fungování, proto je důležité věnovat tomuto kroku dostatečnou vážnost a pečlivost. Způsobů, jakým lze jednotlivé produkty ohodnotit a nakonec zvolit, je rovněž několik. Jednou z možností jsou metody vícekriteriální analýzy variant, které nejsou složité a lze je aplikovat na různé situace v rámci podnikání.

Požadavky, které jsou definované pro jednotlivé podniky se budou lišit případ od případu. Vzorový výčet toho, co produkt pro Incident management musí splňovat jsou shrnuté v několika bodech.

4.3.1 Vytváření a úprava workflow

Možnost vytvářet a upravovat workflow slouží jako důsledný proces schvalování jednotlivých kroků a činností, spolu s nastavením různých oprávnění zabraňuje nevyžádané aktivitě pracovníků společnosti. Zároveň slouží i jako částečná automatizace pro doplňkové úkony (spouštěč počítání SLA a OLA).

Potřeba jednoduché změny funkcionality je na místě v případě, že se společnost rozvíjí, nebo jinak mění v krátkém časovém období. Funkcionalita je pro hladkou implementaci změn zásadní, jelikož umožňuje přizpůsobení procesů v krátkém čase a s vlastními prostředky. Příkladem budiž případ v Nejmenované společnosti, kterou přinutily legislativní změny a rozhodnutí soudu k monitorování požadavků uživatelů. Workflow mohlo být v krátkém a čase obohaceno o krok kontroly různých typů incidentů právním oddělením.

4.3.2 Uživatelský portál

Slouží pro zakládání incidentů a požadavků na službu a pro komunikaci zákazníků s pracovníky společností. Tato funkcionalita může být zastoupena i jinými komunikačními kanály, portál jako takový je univerzální a praxí ověřený způsob výměny informací.

Uživatelský portál může umožňovat snadné zobrazení seznamu aktuálně otevřených i uzavřených incidentů, jejich stav řešení, nebo interaktivní možnost ovládání jednotlivých incidentů – uzavírání, komentování, doplňování apod.

4.3.3 **Koncepce oprávnění a restrikcí**

Celkový koncept oprávnění a restrikcí musí být komplexní s vícevrstvou možností nastavení. Je to jednak z důvodu GDPR, ze kterého vychází požadavek na omezení přístupu k informacím mimo dotčený subjekt a jednak je to z důvodu konkurenční výhody pomocí nastavení restrikcí pro zobrazení informací nežádoucím subjektům a osobám. Tento požadavek v praxi může být aplikovaný pro následující situace:

- Možnost zobrazení jednotlivých incidentů pouze osobě, která incidenty zakládala
- Možnost skupinových oprávnění a omezení (zobrazení anebo i editace)
- Možnost zobrazení a práce s incidenty pouze pracovníky, které mají k typu incidentu povolený přístup
- Rozdělení typu zobrazení a povolených činností na externí (zákazníci) a interní (pracovníci) skupiny
- Omezení možnosti měnit jednotlivé stavy workflow různými skupinami

4.3.4 **Zabezpečení**

Celkové zabezpečení dat, přístupů, případná potřeba pseudonymizace z důvodu požadavků GDPR. Zabezpečení se týká i způsobu přihlašování k portálu – vícefázové ověřování, nebo ověřování odesílatele emailu. Zabezpečení se týká i samotné komunikace, která může mít různou formu – pomocí šifrovaných správ, korektně šifrovaná http komunikace z portálu apod. Celková bezpečnost přístupu je široké téma, které zahrnuje různé oblasti, od chybného kódu, přes různé silové útoky pro zamezení funkčnosti služby po omezenou dobu, nebo i trvale.

4.3.5 **Měření výkonnosti a dostupnosti**

Vyhodnocování plnění služeb (KPI) a dostupnosti v podobě SLA a OLA, je nevyhnutnou součástí většiny kontraktů mezi společností a zákazníky (interními i externími), moderní nástroj musí splňovat i tento požadavek. Přidanou hodnotu tvoří funkcionalita samotného vyhodnocování a zobrazení, které je přehledné a dostatečně detailní. Příkladem jsou grafy,

nebo statistiky, kolik času bylo stráveno jednotlivými pracovníky při řešení, nebo čas strávený v jednotlivých stavech workflow incidentu.

4.3.6 **Uživatelský komfort**

V dynamickém prostředí a v moderních společnostech je možnost jednoduchého obsluhování nástrojů základem. Nástroj musí splňovat požadavek na jednoduchou dostupnost, moderní intuitivní prostředí s responzivním dizajnem a rychlost odezvy na interakci uživatelem. Řešení může obsahovat nespočet vylepšení jmenovitě například – využití standardu html5, Drag & Drop[9] funkcionalita, prostředí nenáročné na výkon, vlastní aplikace pro přístup, modularita a mnoho dalších.

4.3.7 **Cena**

Hraje velmi důležitou roli při pořizování a správě systému, stejně tak i pro výsledek konkurenceschopnosti společnosti. Cena se odvíjí od faktorů, kterými jsou:

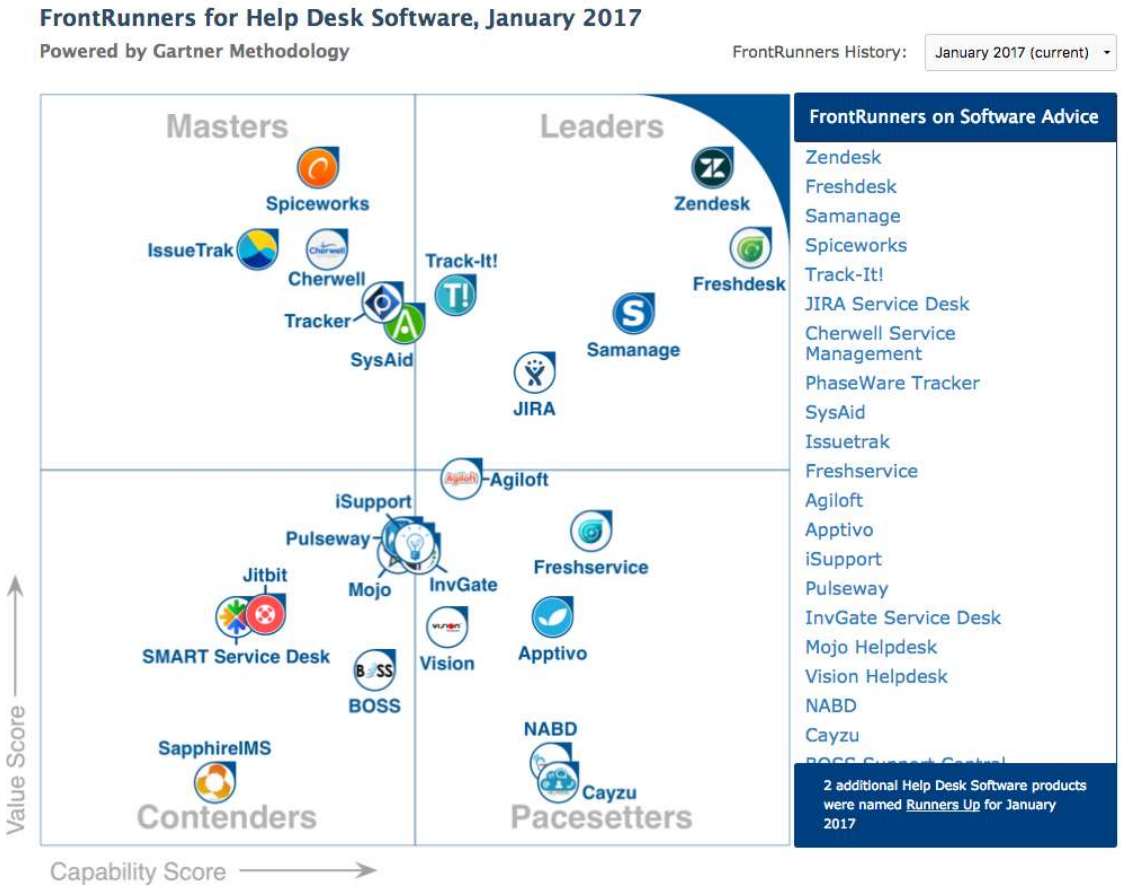
- Licence vázaná počtem uživatelů (externích, interních)
- Funkcionalita a přídavné moduly
- Řešení v cloudu nebo on-premise
- Cena za správu a údržbu
- Cena za případnou úpravu na míru

4.4 **Představení vzorových produktů**

Produktů, které můžou být implementované nebo nakonfigurované takovým způsobem, aby splňovaly výše popsané požadavky, je několik. Proto je důležité zvolit ten správný, který pro danou situaci splňuje co nejdokonaleji zadané požadavky. Dle společnosti Gartner, která se zabývá krom jiného i statistickým šetřením, jsou lídři na trhu za rok 2017 v oblasti poskytování vhodného software pro Helpdesk společnosti s produkty:

- Zendesk
- Freshdesk
- Samanage
- Jira
- Track-It!

[9] „Chyť a vlož“ – funkcionalita umožňující práci s objekty prostým přetažením pomocí myši



Obrázek 9: Matice lídrů na trhu software pro Helpdesk (zdroj: [34])

Na základě informace z této statistiky, jsou proto vybrané jako vzorové řešení pro vyhodnocení nejlepšího řešení pouze produkty Atlassian Jira Service Desk, Fresh Desk, Samanage, Track-It! a Zendesk.

4.4.1 Atlassian Jira

Společnost Atlassian od svého založení v roce 2002 až do roku 2019 vyrostla na celosvětový formát s řešením, které využívá přes 175000 společností/zákazníků. Portfolio produktů a služeb pokrývá různé oblasti, které lze lehce aplikovat a upravovat pro potřeby bezpečnostních anebo procesních certifikací.

Z podmínek, které jsou definované pro zavedení Incident managementu jsou splněné všechny. Jiru lze provozovat jak v cloudu tak i v on-premise[10] řešení. Cena za užívání se liší podle počtu licencovaných uživatelů a modulů, které jsou na implementované. Jelikož Jira

[10] Řešení implementované na míru, spravované zpravidla vlastníkem licence a výpočetního výkonu, bez vnějších napojení a vlivů

jako celek se skládá z Jira Core, Jira Software a Jira Service Desk, je možné toto řešení různě škálovat a doplňovat moduly, které rozšiřují funkcionalitu v téměř neomezené míře. S rostoucí funkcionalitou roste i cena jak pro pořízení, tak i údržbu řešení.

Po zohlednění všech atributů, na základě případné analýzy a dodaných specifikací výrobcem, je zvolené bodové ohodnocení pro tento produkt následující:

Cena – Celková cena implementace a cena za licence jak v Cloudu, tak v on-premise řešení je ze zvolených produktů druhá nejvyšší. Bodové ohodnocení je proto nízké a to 2 pro metodu pořadí a 4 v bodovací metodě.

Funkcionalita – základní funkcionalita, která je v ceně, není komplexní, ale je důvodem vysokého výkonu a rychlé odezvy systému Výhodou je možnost postupného rozšíření, jenom na základě aktuálních potřeb. Ohodnocení je proto 2 pro metodu pořadí a 3 v stupnici bodovací metody.

Výkon – extrémně vyladěný systém dokáže dle specifikací zpracovávat obrovské množství dat a zároveň poskytovat dostatečně rychlou odezvu pro uživatele a napojené systémy. Ohodnocení v metodě pořadí je 4, v bodovací metodě 9 bodů.

Robustnost – Dílčí vlastnosti produktu jsou dotažené a provozované na širokém portfoliu použití, bodové ohodnocení produktu v metodě pořadí je zvolené 3,5 a v bodovací metodě 8 bodů.

4.4.2 **Freshdesk**

Společnost založená v roce 2010 s primárním záměrem vybudovat solidní systém pro uživatelskou podporu hmotného produktu. Působí celosvětově, s počtem zákazníků převyšujících číslo 20000. Společnost po letech vývoje nabízí i produkt zaměřený výhradně na podporu řešení v oblasti Incident Management. Vyznačuje se jednoduchým ale funkčním prostředím s požadovanou funkcionalitou a možnostmi. Řešení je postavené primárně na bázi cloudu.

Po zohlednění všech atributů, na základě případné analýzy a dodaných specifikací výrobcem, je zvolené bodové ohodnocení pro tento produkt následující:

Cena – Vyšší cena za užívaní licencovaného produktu pro počet uživatelů nad 200, je poměrně vysoká a s vyšším počtem uživatelů se cena za licenci nemění. Bodové ohodnocení je proto nízké a to 2 pro metodu pořadí a 4 v bodovací metodě.

Funkcionalita – jednoduchost řešení předurčuje vysoký výkon, který je daný i Cloudovou implementací, možnost rozšíření a přizpůsobení je však problematická. Ohodnocení je proto 1 pro metodu pořadí a 1 v stupnici bodovací metody.

Výkon – vzhledem na jednoduchost a strohou funkcionalitu je výkon a možnost zpracování velkého počtu dotazů obrovský. Ohodnocení v metodě pořadí je 4, v bodovací metodě 8 bodů.

Robustnost – Dílčí vlastnosti produktu jsou dotažené a provozované na širokém portfoliu použití, bodové ohodnocení produktu v metodě pořadí je zvolené 2 a v bodovací metodě 5 bodů.

4.4.3 Samanage

Moderní a flexibilní model Service Desku, který vytvořila a poskytuje společnost Samanage, dokáže uspokojit potřeby technologií, procesů a způsobů výkonu práce jako DevOps[11], nebo Agile[12]. Samanage vznikla v roku 2015, v roce 2018 překročila milník 1500 zákazníku z celého světa a snaží se dostat na první místo v poskytování řešení pro Incident Management v rámci definice ITILu. Zaměřuje se především více na sdílení znalostí, možnost přímé interakce pomocí cloudu, využívání metodiky SmartData[13]. Největší výhodou Samanage je snadná přizpůsobivost pro potřeby společnosti, ve které je Incident Management budován.

Produkt Helpdesku od Samanage splňuje veškeré požadavky pro funkčnost, bezpečnost, GDPR apod. Zároveň umožňuje i implementaci podpůrných řešení definovaných v rámci ITIL, jako jsou CMDB, Service Catalog, Release, Change a Problem management, a další.

Po zohlednění všech atributů, na základě případné analýzy a dodaných specifikací výrobcem, je zvolené bodové ohodnocení pro tento produkt následující:

Cena – produkt je k počtu uživatelů menšího než 500 nejdražším řešením. Bodové ohodnocení pro metodu pořadí je 1 a hodnota 2 v bodovací metodě.

Funkcionalita – Bez přídavných modulů je základní funkcionalita na vysoké úrovni. Zároveň se zde vybízí i možnost dalšího rozšíření pomocí programových úprav. Ohodnocení je proto 4 pro metodu pořadí a 10 v stupnici bodovací metody.

[11] Volně vysvětleno jako vývoj a správa systému v rámci jednoho týmu
[12] Agilní forma řešení úloh, využívajíc metodiky Kanban, Kaizen apod.
[13] Vychází z implementace BigData

Výkon – Možnost zpracovávat kvanta eventů a incidentů dle specifikace výrobce výrazně ovlivňují výkon, případně prodražují výsledné řešení. Ohodnocení v metodě pořadí je proto 3, v bodovací metodě 4 body.

Robustnost – Možnost okamžitého a automatického přizpůsobení řešení s ohledem k právním a technickým normám, řadí bodové ohodnocení produktu v metodě pořadí na hodnotu 3,5 a v bodovací metodě 7 bodů.

4.4.4 **Track-It!**

Software od společnosti BMC má za sebou mnohaletý vývoj a historii, navzdory tomu je to jednoduchý a přehledný nástroj určený pro Help Desk a Asset Management, který je spolehlivý a lehce použitelný. Lze jej využít pro měření SLA, správu licencí, podporu koncových uživatelů a další. Nevýhodou je nutnost on-premise instalace, která z pohledu GDPR vyžaduje vyšší nároky na provoz a zabezpečení.

Po zohlednění všech atributů, na základě případné analýzy a dodaných specifikací výrobcem, je zvolené bodové ohodnocení pro tento produkt následující:

Cena – možnost on-premise řešení řadí tento produkt mezi nejlevnější. Jednoduchá údržba a rozšíření řadí ohodnocení mezi vyšší, v metodě pořadí je hodnocení 3 a v bodovací metodě 9 bodů.

Funkcionalita – Funkcionalita je strohá a pro zavedení incident managementu je nejmenší ze všech představovaných produktů. Ohodnocení je proto 1 pro metodu pořadí a 2 v stupnici bodovací metody.

Výkon – Škálovatelnost výrazně zvyšuje možnosti výkonnosti řešení. Ohodnocení v metodě pořadí je proto 3, v bodovací metodě 7 bodů.

Robustnost – Možnost okamžitého a automatického přizpůsobení řešení s ohledem k právním a technickým normám, řadí bodové ohodnocení produktu v metodě pořadí na hodnotu 1,5 a v bodovací metodě 2 body.

4.4.5 **Zendesk**

Zendesk je společnost založená v roce 2007, poskytuje široké portfolio produktů, pro interakci společností a zákazníků. Jednou ze součástí je i produkt s názvem „Support“, která umožňuje sledování, prioritizací a záznam o řešení zákaznických požadavků. Prostředí a samotné řešení produktu umožňuje držet všechny validní informace na stejném místě, a to napomáhá ku komfortu správy incidentů. Výhodou je systém strojového učení, který dokáže

vykonávat určitou automatickou interakci se zákazníkem. Další z vlastností je možnost napojení na různé systémy dalších stran pro správu dokumentů, nebo napojení na marketingové nástroje jakými jsou třeba MailChimp, SurveyMonkey apod. Důležitou vlastností je možnost napojení na otevřený formát „Networked Help Desk“, který slouží jako univerzální nástroj pro komunikaci mezi různými řešeními sloužícími pro Incident Management.

Po zohlednění všech atributů, na základě případné analýzy a dodaných specifikací výrobcem, je zvolené bodové ohodnocení pro tento produkt následující:

Cena – Produkt se vyznačuje nízkou cenou za implementaci, licence a případnou údržbu. To řadí ohodnocení mezi vyšší, v metodě pořadí je počet bodů 4 a v bodovací metodě 10 bodů.

Funkcionalita – Produkt lze rozšiřovat pouze programovými úpravami. Ohodnocení je proto 3 pro metodu pořadí a 5 v stupnici bodovací metody.

Výkon – Možnosti škálovatelnosti jsou omezené. Rychlost odezvy Cloudového řešení jsou při vyšším počtu dat citelně nižší. Ohodnocení v metodě pořadí je proto 2, v bodovací metodě 3 body.

Robustnost – Požadavky na možnosti propojení a funkcionalitu jakou je zabezpečení, lze u toho produktu splnit jenom obtížně, případně jsou další možnosti rozšíření problematické. To řadí bodové ohodnocení produktu v metodě pořadí na hodnotu 1,5 a v bodovací metodě 3 body.

4.5 Kritéria a výběr požadovaného produktu

Definice hledaných vlastností vyplývají právě z doporučení a norem. Určité vlastnosti vyplývají i z obecného užití produktu a tím je cena anebo i výkon, či další možná funkcionalita a rozšíření.

4.5.1 Kritéria jednotlivých produktů

V definici toho, jaký produkt je hledaný, je jasně pojmenovaná stěžejní funkcionalita a požadované vlastnosti. Tu lze hodnotit separátně anebo je lze kategorizovat a pro zjednodušení zmenšit jejich celkový počet. Zároveň je lze doplnit i o funkcionality a vlastnosti, které jsou doplňkové, subjektivní, nebo mají významný dopad na implementaci a chod společnosti. Tyto definované funkcionality: *workflow, Uživatelský portál, Koncepce*

oprávnění a restrikcí, měření výkonnosti a dostupnosti; lze sloučit do jediného kritéria, kterým je celková robustnost, jelikož žádná z funkcionalit se neliší výrazným způsobem.
Dalším kritériem zvoleným pro hodnocení je *výkon*. Systém musí zvládat jak nápor dotazů pracovníků společnosti, tak i obrovské množství dat v podobě incidentů a dalších typů ticketů. Je nezanedbatelným prvkem, při hodnocení volby vhodného řešení.
Důležitým prvkem při hodnocení kritérií je *cena* řešení. Ta by měla obsahovat pořizovací náklady, náklady na implementaci a udržovací náklady v dlouhodobém horizontu.
Každý ze systémů má určitou specifickou *funkcionalitu*, která může hrát výraznou roli při vybírání navazujících produktů. Rovněž je v ní zahrnutý uživatelský komfort. Proto je jedním z hlavních kritérií, při hodnocení produktů pomocí vícekriteriální analýzy variant.

4.5.2 **Zhotovení tabulky vah**

Při použití metody pořadí je důležitost jednotlivých parametrů seřazená v pevně dané stupnici od 1 do 4 s tím, že nejlepší známku, kterou může jednotlivý produkt získat, je číslo 4. Sloupce jsou nositelem informací pro kritéria a jsou doplňovány jednotlivými vahami. Každý produkt má jeden řádek, na konci kterého je umístěný výsledek, který je vypočítaný zprůměrováním hodnot vah a ohodnocení. Řešení s nejvyšší hodnotou je to, které je dle metody pořadí to nejlepší. S rostoucím počtem kritérií se snižuje riziko nalezení produktů, se stejným oceněním. Problematické ale bude přesnost ohodnocení jednotlivých kritérií vahami, jelikož u některých kritérií se lze rozhodnout o pořadí nelze. Typicky při požadavku na podporu funkcionality, kde je odpověď jenom ve formátu ANO/NE. Při volení bodů jednotlivých kritérií lze využít rozhodnutí o jejich důležitosti v předešlém kroku a přiřadit odpovídající množství bodů. V tabulce pro výpočet jsou zvolené hodnoty pro cenu, funkcionalitu, výkon a robustnost tak, aby splňovaly požadavky Nejmenované společnosti pro nástroj incident managementu. Jelikož je cena obecně nízká v návaznosti na obrat a zisk společnosti, byla zvolená nejmenší důležitost a ohodnocená malým počtem bodů. Důležitější než je cena je funkcionalita, která může mít nepřímý vliv na spokojenost a výkonnost uživatelů. Výkon je základním stavebním kamenem, bez kterého nelze zvolit správný nástroj, zvolené body mají druhou nejvyšší hodnotu ze všech bodových ohodnocení. Posledním, nejdůležitějším kritériem je robustnost, která definuje například způsob napojení na jiné podnikové systémy. Z toho důvodu nepřímo ovlivňuje cenu a přímo rychlost a kvalitu práce v nástroji. V stupnici ohodnocení je zvolená nejvyšší hodnota.

Kritérium	Pořadí	Body	Váha
Cena	4	1	0,1
Funkcionalita	3	2	0,2
Výkon	2	3	0,3
Robustnost	1	4	0,4

Tabulka 1: Tabulka vah dle metody pořadí

Potvrzení správnosti lze vykonat další metodou, například bodovací metodou. Rozdíl oproti metodě pořadí je v použití ohodnocení jednotlivých parametrů stupnicí v přesně daném intervalu. Pro jednoduchost lze zvolit interval <1;10>. Nejvyšší hodnota znamená nejlepší ohodnocení, které lze přiřadit jednotlivým parametrům. Ty, podobně jako u metody pořadí představují jednotlivé sloupce a výsledek je součet násobků parametrů s jednotlivými vahami. Podobným způsobem, jako při hodnocení pomocí metody pořadí, lze ohodnotit kritéria: cena, funkcionalita, výkon a robustnost. Změna je v možnosti hodnocení, které je precizněji zvolené na základě skutečné důležitosti, proto je například rozdíl v hodnocení mezi výkonem a funkcionalitou menší, než mezi funkcionalitou a cenou. Váhy v tabulce jsou dopočteny na základě vzorce definovaného Bodovací metodou a to tak, že jednotlivé body jsou vydělené sumou všech bodů, výsledek určuje jednotlivé váhy kritérií.

Kritérium	Body	Váha
Cena	3	0.12
Funkcionalita	6	0.24
Výkon	7	0.28
Robustnost	9	0.36
Součet	25	

Tabulka 2: Tabulka vah bodovací metody

5 Zhodnocení výsledků a doporučení

Postupným přecházením doporučených postupů lze najít řešení, které nakonec přinese zlepšení. To však není finální fáze implementace. Po ukončení zavádění procesů a nástrojů musí pokračovat kontinuální zlepšování a udržování služeb. To znamená přizpůsobování procesů a workflow aktuálním trendům a požadavkům, přidávání funkcionality, nebo odstraňováním nepotřebných dat, nástrojů, přístupů apod.

5.1 Vyhodnocení požadavků společnosti

Jsou-li při analýze nalezeny nedostatky, které jeví známky nekompatibility s ITIL, GDPR, normou ISO 27000, případně neexistují procesy a řešení vůbec, lze využít všeobecné známé činitele, dle kterých lze definovat formování Incident Managementu. Tyto požadavky jsou definované následovně [19]:

- zvýšit standardizaci procesů správy incidentů a plnění požadavků;
- upravit workflow incidentu, aby vyhovoval ITIL a řešení incidentu do nalezení řešení;
- nastavit vyhovující workflow správy změn;
- stanovit proces správy vydání a nasazení;
- způsob přidělování řešiteli (eskalační rovina, přidělování podřízeným).

5.2 Zvolení vhodného produktu dle vícekriteriální analýzy variant

Na základě určených vah a kritérií lze jednoduše spočítat výsledné pořadí produktů dle ohodnocení. Podle metody pořadí je s nejvyšším počtem bodů nejvhodnější produkt Jira Servicedesk. Výsledky jsou těsné a je vhodné ověření za pomocí jiné metody.

Řešení	*Cena*	*Funkcionalita*	*Výkon*	*Robustnost*	*Výsledek*
Jira Servicedesk	2	2	4	3,5	**3,2**
Freshdesk	2	1	3	2	**2,1**
Samanage	1	4	1	3,5	**2,6**
Track-It!	3	1	3	1,5	**2**
Zendesk	4	3	2	1,5	**2,2**

Tabulka 3: Zhodnocení dle metody pořadí

Bodovací metoda potvrzuje pořadí s na prvním místě umístěným produktem Jira Servicedesk vzhledem na to, že ve výsledku obdržel nejvíc bodů. Výsledky jsou obdobné jako v případě metody pořadí, s přesnějším rozdělením pozic u produktů Track-It!, Freshdesk a Zendesk.

Řešení	*Cena*	*Funkcionalita*	*Výkon*	*Robustnost*	*Výsledek*
Jira Servicedesk	4	3	9	8	**6.6**
Freshdesk	4	1	8	5	**4.76**
Samanage	2	10	4	7	**6.28**
Track-It!	9	2	7	2	**4.24**
Zendesk	10	5	3	3	**4.32**
Váha	0.12	0.24	0.28	0.36	

Tabulka 4: Zhodnocení dle bodovací metody

5.3 Vyhodnocení a zvolení vzorového produktu

Pro zavedení Incident managementu je ze zvolených řešení a vah nejvhodnější použít Jira Servicedesk. Je to z toho důvodu, že toto řešení má nejvyšší skóre v rámci bodovací metody i metody pořadí. Tento nástroj je robustním řešením, které umožňuje jednoduché přepojení help desku s vývojovou větví sledování a zadávání úloh. Řešení nabízí obrovskou škálu rozšíření, kterým lze formovat jak procesy společnosti nejen v oblasti vývoje software a incident managementu, ale i z jiné sféry společnosti, jako jsou například oddělení marketingu a obchodu pro které lze definovat různé workflow pro schvalování fakturace, kampaní apod.

5.4 Procesy a prostředí v Jira Servicedesk

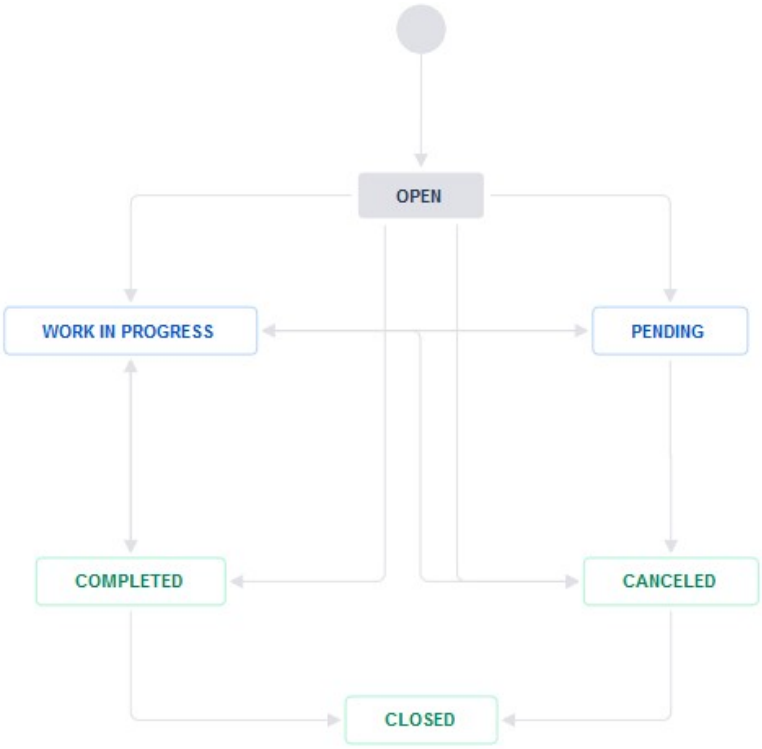
Produkt jako taký je komplexní nástroj a v případě využití Cloudové služby, přichází už s jednoduchým nastavením, které plně neodráží metodiku popsanou ITILem, je však dobře připravené z pohledu bezpečnosti, GDPR a uživatelského komfortu. Východiskové řešení to proto může být, ale i tak je ale nutná další konfigurace, která kopíruje především požadavky na funkcionalitu a potřeby společnosti.

5.4.1 Obecné workflow v Jira Servicedesk

Jako příklad pro implementaci je v nástroji hned po aktivaci uvedené workflow pro zpracování incidentu, které je rozšířením toho, které je analytické části tohoto dokumentu popsané v rámci základního doporučení ITIL. Jeho schéma společně s možnými kroky je popsaná v následujícím obrázku.

V Nejmenované společnosti je toto workflow přiřazené incidentům, které vznikají ve vztahu společnost a externí zákazník, který je především z řady franšízových provozoven. Jednotlivé incidenty můžou projít několika stavy, které lze popsat následujícím způsobem:

- **Open** (otevřen) – Ticket je po nahlášení incidentu okamžitě ve stavu „Otevřen“, může i nemusí mít přiřazeného uživatele, má založený jasný identifikátor a ticketu je monitorovaný aktuální čas řešení na základě definice SLA. Ze stavu „open“ lze ticket přesunout do všech ostatních stavů, kromě finálního zavření „closed“.
- **Work in progress** (probíhající práce) – je stav, který infikuje potvrzení incidentu a jsou zahájené práce na identifikaci a případné nápravě, nebo komunikace se zákazníkem. Z tohoto stavu, lze ticket převést do stavů „Pending“, „Completed“ a „Cancelled“. Podmínkou převedení do tohoto stavu je jasně přidělený identifikátor řešitele.
- **Pending** (čekání) – v případě nutnosti reakce zákazníka z důvodu ověření, nebo čekání na další spouštěč, týkající se incidentu (vydání záplaty, změna HW apod.), lze ticket převést do tohoto stavu. Ten nezahrnuje počítání SLA, obsahuje však čas, po který bude ticket v tomto stavu, než se vrátí do stavu „Work in progress“, nebo „Cancelled“.
- **Completed** (ukončený) – stav ticketu po vyřešení incidentu. Z tohoto stavu se lze vrátit do stavu „work in progress“ jestliže ukončení incidentu bylo neopodstatněné. Do stavu „closed“ se ticket dostane s časovou prodlevou a po kontrole splnění všech náležitostí na uzavření incidentů (například doplněný záznam stráveného času na řešení).
- **Canceled** (zrušený) – neopodstatněné incidenty mohou být převedeny do stavu (zrušený), rovněž i z důvodu vyžádání zákazníka. Stav „zrušený“ se využívá i pro duplicitní incidenty, nebo chyby, které byly vyřešené mimo tento workflow. Z „canceled“ stavu se lze dostat zpátky do „work in progress“ nebo ho úplně uzavřít stavem „closed“.
- **Closed** (uzavřený) – je poslední stav ticketu, ve kterém už nelze ticket nijak upravovat a pro případnou reklamaci zákazníkem je nutné vytvoření nového ticketu.



Obrázek 10: Obecné workflow pro řešení incidentů

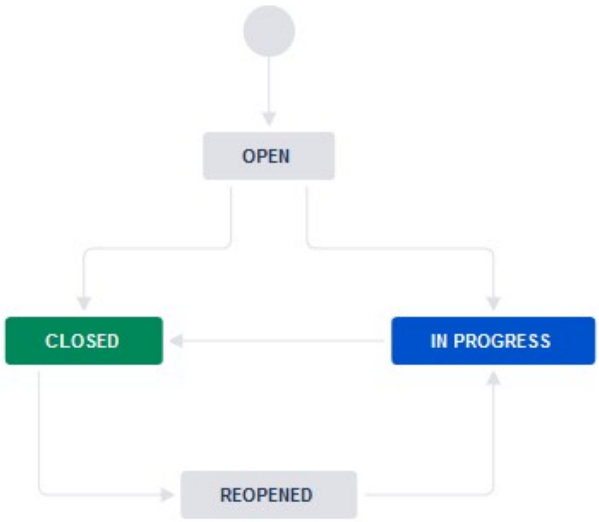
5.4.2 Zjednodušené workflow

Další variantou pro implementaci zpracování incidentů lze použít zjednodušené workflow, jen třech stavech a krocích. Toto workflow se využívá především pro sledování velkého množství incidentů stejného typu.

V Nejmenované společnosti je toto workflow určené pro incidenty hlášené na různých testovacích prostředích, kde není nutná extenzivní komunikace, ověřování stavu, měření SLA/OLA, nebo důkladné vyhodnocování. Typické úlohy pro řešení jsou restarty chybně běžících aplikací, čištění nepotřebných dat z důvodu zaplnění volného místa, nebo jiné aktivity spojené s testováním. Jednotlivé stavy jsou zdůvodněné následujícím způsobem:

- **Open** (otevřený) – založený incident s jasným identifikátorem. Možnost změny stavu do „In Progress“ a „Closed“.
- **Closed** (zavřený) – je stav ticketu po vyřešení nebo zamítnutí opravy. Z tohoto stavu se lze dostat do stavu „Reopened“.
- **In Progress** (v průběhu) – stav indikující zahájení prací na opravě, podmíněné definováním řešitele. Z tohoto stavu lze ticket pouze zavřít, to znamená přesunout ho do stavu „Closed“.

- **Reopened** (znovuotevřený) – stav je alternativou k „open“ a využívá se i pro zjednodušení administrativy v případě nedostatečně vyřešené chybě, nebo chybě opakující se.



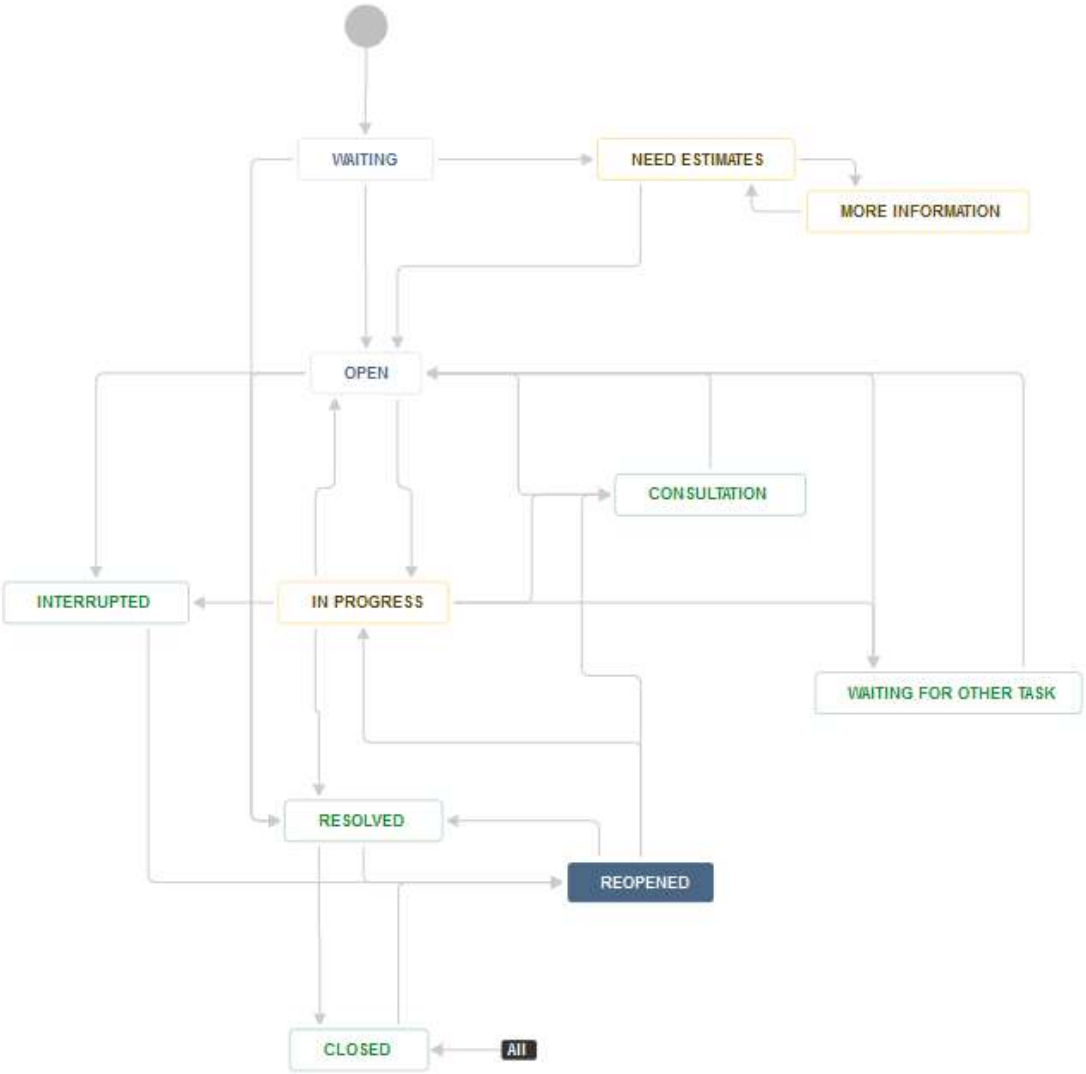
Obrázek 11: Zjednodušené workflow

5.4.3 Workflow se schvalovacím procesem

Pro zlepšení kontroly, zefektivnění prací je téměř u každé společnosti zavedené workflow, které je upravené přesně dle aktuálních potřeb, nebo přizpůsobené produktům a zákazníkům. Pro Nejmenovanou společnost bylo proto navržené workflow pro typ incidentů od specifického oddělení (zákazníka), které počítá i se schvalovacím procesem mezi založením a skutečným otevřením ticketu. To představují stavy „Need estimates“ a „More Information“. Zároveň bylo workflow rozšířené o jiné stavy, z důvodu dohledatelnosti a informovanosti zákazníka. Toto workflow umožňuje snáze rozlišovat jednotlivé fáze incidentu. Bližší informaci k jednotlivým krokům v rámci workflow jsou následující:

- **Waiting** (čekající) – stav po vytvoření ticketu a před zpracováním, kterému se přiřadí odhadce stráveného času, nebo se ticket přesune do stavu „open“.
- **Open** (otevřen) – Ticket je ve stavu „Otevřen“, musí mít přiřazeného řešitele, má založený jasný identifikátor a je mu odhadnutá délka řešení.
- **In Progress** (v průběhu) – je stav, který infikuje potvrzení incidentu a jsou zahájené práce na identifikaci a případné nápravě, nebo komunikace se zákazníkem.

- **Interrupted** (přerušený) – v případě nutnosti reakce zákazníka z důvodu ověření, nebo čekání na další spouštěč, týkající se incidentu (vydání záplaty, změna HW apod.), lze ticket převést do tohoto stavu. Obsahuje údaj o délce trvání, po který bude ticket v tomto stavu, než se přesune do jiného stavu v rámci tohoto workflow.
- **Resolved** (vyřešený) – stav ticketu po vyřešení incidentu. Z tohoto stavu se lze vrátit do stavu „Reopened" jestliže ukončení incidentu bylo neopodstatněné.
- **Reopened** (znovuotevřený) – stav je alternativou k „open" a využívá se pro případné nové odhadnutí stráveného času na řešení, jestliže byl ticket v předešlém kroku považovaný za vyřešený, nebo pro jeho řešení nebyl důvod.
- **Closed** (uzavřený) – je stav ticketu, který je uzavřený a na kterém neprobíhají žádné činnosti a ani jeho vyhodnocení.
- **Waiting For Other Task** (čekání na další úlohu) – stav, ve kterém se čeká na jinou, s incidentem nesouvisející úlohu, příkladem je periodické, hromadné nastavení přístupových práv, periodické záplatování komponenty nepřímo spojené s produktem (síťového prvku) apod.
- **Consultation** (konzultování) – stav ticketu, ve kterém je problematika a případný dopad řešení probíraná s architektem, projektovým manažerem, nebo jiným relevantním subjektem.
- **Need Estimates** (vyžádaný časový odhad) – krok workflow, který čeká na odhadce určujícího pravděpodobnou délku trvání. Tento odhad je důležitý pro plánování vytížení zdrojů.
- **More Information** (vyžádané další informace) – malé workflow v rámci odhadu času délky trvání prací na incidentu, ve kterém odhadce žádá zakladatele incidentu o doplňující informace k danému incidentu. Tyto informace pak slouží jak k odhadu času, tak i k urychlení prací při řešení incidentu.



Obrázek 12: Workflow se schvalovacím procesem

5.4.4 Zhodnocení procesů

Každá situace může vyžadovat různé nastavení procesní části. V Jira Servicedesk lze pro Incident Management používat i vícero procesů v závislosti na typu incidentu, nebo na větev komunikace, která může být definovaná pro interní potřeby nebo směrem k externímu zákazníkovi.

Workflow lze kombinovat i s různým oprávněním pro skupiny uživatelů. Právě v případě rozvětveného workflow se schvalovacím procesem jsou oprávnění stěžejní a určují odpovědné osoby z řad vedoucích týmů, nebo přímo manažerské role, které umožňují například zamítnutí incidentu, přiřazení incidentu konkrétnímu řešiteli, případně umožňují zastavit počítání času SLA/OLA, které je pro obchodní styk stěžejní.

6 Závěr

Implementace procesů v podobě Incident managementu není záležitost, kterou lze definovat jednoduchým a univerzálním způsobem. Vstupů, které ovlivňují výsledek snažení, je enormní množství. I zúžení množiny faktorů na několik jednotek vytváří mnoho možností pro posouzení a individuální rozhodování s tendencí rozhodovat subjektivně, na základě osobních preferencí. Prakticky ale lze najít postupným odbouráváním nejasných rozcestí tu správnou větev pro dosažení cíle v podobě funkčního Incident managementu.

Základem je důsledná analýza a pochopení toho, co lze od Incident Managementu očekávat, z důvodu toho, že to definovaná množina postupů pro řešení různých událostí není jasně stanovená. Tuto sféru zaštiťuje specificky zaměřená část ITILu, která i bez přesně stanovených kroků, určuje pevné obrysy konstrukce finálního řešení. V případě zavedení Incident managementu to bylo především rozdělení procesů, zavedení pojmů jako je incident, změnový požadavek nebo problém. Na základě dalších vstupů a požadavků a příkladem budiž nutnost počítat se správným zpracováním dat podle směrnice GDPR, je pak možné definovat produkt, který zjednoduší práci s procesy. Produkt lze jednoduše zvolit z několika možností na základě vícekriteriální analýzy variant, v závislosti určení vah na preferencích a požadavcích jednotlivé organizace.

Zásadním přínosem je prokázané splnění legislativních a bezpečnostních požadavků, které vyplývají ze zákona a které vyžadují všechny zúčastněné strany, jak zákazníci, tak i zaměstnanci společnosti. Obzvlášť důležitá je tato oblast při styku s veřejností, která klade extrémní požadavky právě na splnění všech podstatných náležitostí.

Na základě všech vstupů byla provedená analýza a jednoduchý výpočet, který přesně vydefinoval výsledný nástroj. Ten lze případným iterováním změn a požadavků konfigurovat i dodatečně až do výsledné podoby, která je specifická u každé společnosti, která patří do kategorie středně velkých společností.

7 Seznam použitých zdrojů

[1] **ŠUBRT, T.** a kolektiv. *Ekonomicko – matematické metody*. Vyd. 1. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2011, 351 s. ISBN 978-80-7380-345-2

[2] **BROŽOVÁ, H., ŠUBRT, T. a HOUŠKA, M.** *Modely pro vícekriteriální rozhodování*. Vyd. 1. Praha: Credit, 2003, 172 s. ISBN 978-80-213-1019-3

[3] **Paul Wilkinson, Jan Schilt,** *ABC of ICT An Introduction*. Vyd. 1. Amersfoort: Credit, 2008, 289 s. ISBN 978-90-875-3140-9

[4] **Randy A. Steinberg**. *ITIL Service Operation.* Vyd. 2. Londýn: The Stationery Office 2013, 384 s., ISBN**:** 978-0113313075

[5] **Van Bon**, *IT Service Management: An Introduction based on ITIL* (pp.11-70), 2004

[6] **Cartlidge, A., Hanna, A., Ruddit, C., & Manfarlane, I.,** *An introductory Overview of ITIL V3,* [Brochure], 2007, The UK chapter of itSMF

[7] **Claire Engle, Jackie Brewster, Gerard Blokdijk**, *How to Develop, Implement, and Enforce ITIL V3's best practices. (Vol. 3). Emereo Pty Ltd London, UK,* 2008, ISBN: 0980513669

[8] **Gilbert, P., Morse, R., & Lee, M.**, *Enhancing IT support with Knowledge Management.* (2007) [Brochure]. CA Technology

[9] **Xiaojun Tang, Yuki Todo,** *A Study of* Service Desk Setup in Implementing IT Service Management in Enterprises, doztupné z URL: http://dx.doi.org/10.4236/ti.2013.43022 2013

[10] **R. A. Steinberg,** *ITIL Service Operation, 2011 Edition*, 2011, The Stationery Office, London, ISBN: 978-0113313075

[11] **OMNICOM s.r.o.,** *Obsah a rozsah ITSM*, dostupné z URL: https://www.bestpractice.cz/cs/Best-practice/-ITSM-ITIL-/-Obsah-a-rozsah-ITSM.alej

[12] **AXELOS,** *Best Practice solutions,* dostupné z URL: https://www.axelos.com/best-practice-solutions/itil/what-is-itil

[13] **CABINET OFFICE**. *ITIL® Service Strategy: Best Management Practice*. Second edition. London: The Stationery Office, 2011. ISBN 9780113313044.

[14] **CABINET OFFICE**. *ITIL® Service Design: Best Management Practice*. Second edition. London: The Stationery Office, 2011. ISBN 9780113313051.

[15] **CABINET OFFICE**. *ITIL® Service Transition: Best Management Practice*. Second edition. London: The Stationery Office, 2011. ISBN 9780113313075

[16] **CABINET OFFICE**. *ITIL® Service Operation: Best Management Practice*. Second edition. London: The Stationery Office, 2011. ISBN 9780113313075

[17] **CABINET OFFICE**. *ITIL® Continual Service Improvement: Best Management Practice*. Second edition. London: The Stationery Office, 2011. ISBN 9780113313082.

[18] **Komentovaný výklad norem ISO 20000**, Masarykova universita 2008, dostupné z URL: https://is.muni.cz/el/1433/jaro2009/PA088/um/Vyklad_ISO20000.pdf

[19] **FIALA, Josef a Jan MINISTR**. Průvodce *analýzou a modelováním procesů*. Ostrava: VŠB – Technická univerzita Ostrava, 2003. ISBN 80-248-0500-6.

[20] **HAMMER, Michael**. *Reengineering – radikální proměna firmy: manifest revoluce v podnikání*. 3. vyd. Praha: Management Press, 2000. ISBN 80-7261-028-7

[21] **ISO/IEC 27000:2018** Information technology – Security techniques – Information security management systems – Overview and vocabulary, 2017. ISBN 978-0-580-94514-4

[22] **MATOUŠOVÁ, Miroslava a Ladislav HEJLÍK**, 2008. *Osobní údaje a jejich ochrana*. 2., dopl. a aktualiz. vyd. Praha: ASPI. ISBN 978-80-7357-322-5.

[23] **GODDARD, Michelle**, 2017. *The EU Data Protection Regulation (GDPR): European re-gulation that has a global impact*., Vol. 59, issue 6, s. 703-705 [cit. 2018-03-15]. ISSN: 1470-7853

[24] **BENEŠ, Pavel**, 2010. *Informace o informaci, aneb, Nový pohled na tento svět.* Praha: BEN – technická literatura. ISBN 978-80-7300-263-3

[25] **CALDER, Alan**, 2016. *EU GDPR: A Pocket Guide.* United Kingdom: IT Governance Publishing. ISBN 978-1-84928-833-0

[26] **BARTÍK, Václav a Eva JANEČKOVÁ**, 2013. *Ochrana osobních údajů v životě podnikate-le: 103 řešení modelových situací*. Olomouc: ANAG. ISBN 978-80-7263-811-6

[27] **NEZMAR, Luděk**, 2017. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing. ISBN 978-80-271-0668-4

[28] **BOLOGNINI, Luca**, **Camilla BISTOLFI**, 2017. *Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation. Computer Law & Security Review*, Vol. 33, issue 2, s. 171-181, ISSN: 0267-3649

[29] **Šmída, F**. 2007 *Zavádění a rozvoj procesního řízení ve firmě*. Praha: Grada Publishing. ISBN: 978-80-247-1679-4

[30] **Raturi, A., Evans, J**., *Principles of Operations Management. Mason: Thomson Corporation*, vyd. 2005, ISBN 0324008961

[31] **COLLISON, Chris a Geoff PARCELL,** *Knowledge management: praktický management znalostí z prostředí předních světových učících se organizací*., Brno: Computer Press, 2005, 236 s. ISBN 80-251-0760-4.

[32] **Adair, J. E**. *Efektivní inovace*, 1. vyd. Praha: Alfa Publishing, 2004. 233 s. ISBN 80-86854-04-4

[33] **ZENDESK,** *Helpdesk Magic Quadrant,* dostupné z URL: https://www.zendesk.com/resources/gartners-frontrunners-quadrant/

[34] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 6. října 2016. In: Úřad pro ochranu osobních údajů. 2000, ročník 2000, číslo 101. Dostupné také z: https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=21409

[35] **BARTÍK, Václav a Eva JANEČKOVÁ**. *Ochrana osobních údajů v životě podnikatele: 103 řešení modelových situací*, 1. vyd. Olomouc: ANAG, 2013, 199 s. ISBN 9788072638116

8 Přílohy

Tabulka pojmů:

Termín	Přípustné použití termínu	Ekvivalent v ITIL
Procesy zajišťující dodávku služeb	Service Delivery Processes	Service Delivery (název jednoho svazku z ITIL)
Management kapacit	Capacity Management	Capacity Management
Management kontinuity dodávky služeb Management dostupnosti	Service Continuity and Availability Management	IT Service Continuity Management Availability Management
Management úrovně služeb	Service Level Management	Service Level Management
Hlášení o úrovni služeb	Service Reporting	Není stanovován jako samostatný proces
Management informační bezpečnosti	Information Security Management	Security Management (název jednoho svazku z ITIL)
Rozpočtování a účtování IT služeb	Budgeting and Accounting for IT services	Financial Management for IT Services
Kontrolní procesy	Control Processes	Tato oblast je řešena v „Service Support" svazku
Management konfigurace	Configuration Management	Configuration Management
Management uvolňování jednotlivých verzí	Release Process	Release Management (součást Service Support)
Procesy řešení požadavků a problémů	Resolution Processes	Tato oblast je řešena v „Service Support" svazku
Management incidentů	Incident management	Incident management
Management problémů	Problem Management	Problem Management
Procesy řízení vztahů	Relationship Processes	Tato oblast je řešena v „Business Perspective: The IS View on Delivering Services to the Business"
Management vzájemných vztahů	Business Relationship Management	Business Perspective
Management vztahů s dodavateli	Supplier Management	Supplier Relationship Management