Vysoká škola ekonomická v Praze
Fakulta informatiky a statistiky
Katedra informačních technologií

Governance a management služeb cloud computingu z pohledu spotřebitele

DOKTORSKÁ DISERTAČNÍ PRÁCE

Doktorand:	Ing. et Ing. Soňa Karkošková
Školitel:	doc. Jiří Feuerlicht, Ph.D.
Obor:	Aplikovaná informatika

Praha, 2017

Prohlášení

Prohlašuji, že doktorskou práci na téma „Governance a management služeb cloud computingu z pohledu spotřebitele“ jsem vypracovala samostatně. Použitou literaturu a podkladové materiály uvádím v přiloženém seznamu literatury.

V Praze dne 19.6. 2017 .....

Ing. et Ing. Soňa Karkošková

Poděkování

V úvodu mé doktorské disertační práce bych ráda poděkovala doc. Jiřímu Feuerlichtovi, Ph.D. za vedení této doktorské disertační práce, za odborné rady a připomínky a za podporu během celého mého doktorského studia.

Abstrakt

Využívání služeb cloud computingu přináší kromě široce uznávaných benefitů také nové výzvy a rizika vyplývající zejména z faktu, že poskytovatel služeb cloud computingu je externí třetí stranou, která poskytuje službu v modelu veřejného cloud computingu velkému množství spotřebitelů. V současnosti žádný z široce přijímaných IT governance a IT management rámců plně nezohledňuje specifika využívání služeb cloud computingu a žádný z nich není primárně určen pro governance a management služeb cloud computingu z pohledu spotřebitele. Z tohoto důvodu se doktorská disertační práce zaměřuje na specifické aspekty governance a managementu služeb cloud computingu z pohledu spotřebitele služeb.

Cílem doktorské disertační práce je návrh metodického rámce pro governance a management využívání služeb cloud computingu (metodický rámec Cloud computing governance a management) z pohledu spotřebitele služeb cloud computingu. Jako spotřebitel služeb cloud computingu je pro potřeby této doktorské disertační práce považován středně velký až velký podnik, který využívá služby v modelu veřejného cloud computingu, které jsou dodávané poskytovatelem služeb cloud computingu.

Teoretická část doktorské disertační práce identifikuje základní teoretická východiska IT governance, IT managementu a cloud computingu (kapitola 2). Navazující analytická část doktorské disertační práce popisuje výstupy z rešerše dostupné literatury, která se zabývá specifiky využívání služeb cloud computingu a jejich vlivem na IT governance a IT management, cloud computing governance a cloud computing managementem (kapitola 3). Dále jsou analyzovány současné široce uznávané metodické rámce IT governance a IT managementu (SOA Governance, COBIT, ITIL a MBI) z hlediska jejich podpory governance a managementu využívání služeb cloud computingu z pohledu spotřebitele (kaptiola 4).

Vědecký výzkum, který se váže k této doktorské disertační práci, je považován za výzkum typu návrh (Design Science Research), neboť výstupem této doktorské disertační práce je artefakt metodický rámec. V hlavní části této doktorské disertační práce je navržen metodický rámec Cloud computing governance a management, který je postaven na metodických rámcích SOA Governance, COBIT 5 a ITIL 2011 (kapitola 5, 6 a 7). Pro ověření navrženého metodického rámce Cloud computing governance a management byla využita metoda případové studie (kapitola 8). Cílem případové studie bylo vyhodnotit a ověřit navržený metodický rámec Cloud computing governance a management v reálném byznys prostředí.

Důležitým přínosem této doktorské disertační práce je kromě využití stávajících znalostí, přístupů a metodik IT governance a IT managementu při návrhu metodického rámce Cloud computing governance a management také rozšíření modelu Management podnikové informatiky (MBI) o nové úlohy obsahující postupy a doporučení související s adopcí a vyžíváním služeb cloud computingu.

Klíčová slova

Cloud computing governance, Cloud computing management, spotřebitel služby cloud computingu, veřejný cloud computing, governance procesy, management procesy, metodický rámec.

Abstract

Cloud computing brings widely recognized benefits as well as new challenges and risks resulting mainly from the fact that cloud service provider is an external third party that provides public cloud services in multi-tenancy model. At present, widely accepted IT governance frameworks lack focus on cloud computing governance and do not fully address the requirements of cloud computing from cloud consumer viewpoint. Given the absence of any comprehensive cloud computing governance and management framework, this doctoral dissertation thesis focuses on specific aspects of cloud service governance and management from consumer perspective.

The main aim of doctoral dissertation thesis is the design of methodological framework for cloud service governance and management (Cloud computing governance and management) from consumer point of view. Cloud consumer is considered as a medium or large-sized enterprise that uses services in public cloud computing model, which are offered and delivered by cloud service provider.

Theoretical part of this doctoral dissertation thesis identifies the main theoretical concepts of IT governance, IT management and cloud computing (chapter 2). Analytical part of this doctoral dissertation thesis reviews the literature dealing with specifics of cloud services utilization and their impact on IT governance and IT management, cloud computing governance and cloud computing management (chapter 3). Further, existing IT governance and IT management frameworks (SOA Governance, COBIT, ITIL and MBI) were analysed and evaluated in terms of the use of cloud services from cloud consumer perspective (chapter 4).

Scientific research was based on Design Science Research Methodology with intention to design and evaluate artifact methodological framework. The main part of this doctoral dissertation thesis proposes methodical framework Cloud computing governance and management based on SOA Governance, COBIT 5 and ITIL 2011 (chapter 5, 6 and 7). Verification of proposed methodical framework Cloud computing governance and management from cloud consumer perspective was based on scientific method of case study (chapter 8). The main objective of the case study was to evaluate and verify proposed methodical framework Cloud computing governance and management in a real business environment.

The main contribution of this doctoral dissertation thesis is both the use of existing knowledge, approaches and methodologies in area of IT governance and IT management to design methodical framework Cloud computing governance and management and the extension of Management of Business Informatics (MBI) framework by a set of new tasks containing procedures and recommendations relating to adoption and utilization of cloud computing services.

Keywords

Cloud computing governance, cloud computing management, cloud service consumer, public cloud computing, governance process, management process, methodical framework.

Obsah

1 Úvod k práci

Tato doktorská disertační práce se věnuje governance[1] a managementu[2] služeb cloud computingu z pohledu spotřebitele. Pro pojmy governance a management lze použít české významy vládnutí a řízení. Pojem vládnutí se však v podnikové praxi běžně nepoužívá a jeho obvyklou formou je anglický ekvivalent governance, který jednoznačně a srozumitelně vyjadřuje podstatu tohoto pojmu a bývá oproti pojmu vládnutí všeobecně správně interpretován. Jelikož lze anglický pojem governance považovat za jazykový úzus, bude výhradně používán v rámci celé této doktorské disertační práce. Aby v disertační práci byly použity jednotné pojmy a bylo zabráněno chybné interpretaci obou jmenovaných pojmů, bude i pro pojem řízení používán odpovídající anglický ekvivalent management.

Cílem této doktorské disertační práce je vytvoření návrhu metodického rámce pro governance a management využívání služeb cloud computingu (metodický rámec Cloud computing governance a management) z pohledu spotřebitele služeb, který vychází z široce akceptovaných rámců pro IT governance a IT management a informačních zdrojů zabývajících se aplikací principů IT governance a IT managementu do prostředí cloud computingu.

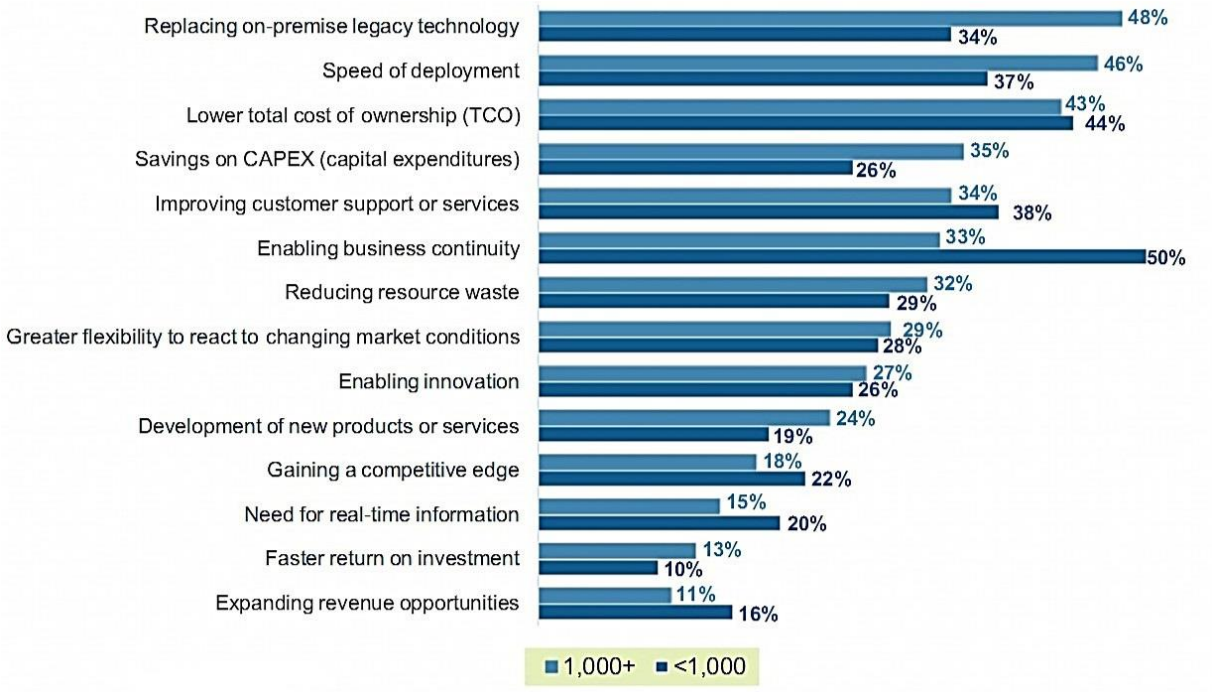
1.1 Vymezení tématu doktorské disertační práce

Současné vysoce konkurenční obchodní prostředí se vyznačuje vysokou mírou komplexnosti a značným tlakem na organizace, aby byly schopné rychle a pružně reagovat na měnící se byznys podmínky a požadavky na trzích. Pro udržení agility a konkurenceschopného postavení by organizace měly implementovat takové politiky, postupy, procesy a metody, které umožní flexibilně realizovat podporu měnících se byznys procesů s ohledem na zabezpečení efektivního dosažení podnikových cílů a potřeb zainteresovaných stran. Podpora byznys procesů by byla prakticky neudržitelná bez přímé podpory informačních technologií, které se během svého vývoje staly integrální součástí podniku. Při současném trendu globalizace se informační technologie (IT) stávají více než zdrojem konkurenční výhody (Selčan, 2012). Tato skutečnost vede k růstu potřeby ovládat a řídit podnikové informační technologie (Svatá, 2011). Tradiční IT architektura je ve velkých podnicích obvykle velmi rozsáhlá, časově náročná na plánování, testování, nasazení a na integraci a finančně nákladná (Gála, a další, 2012). S rozvojem organizace rostou závislosti mezi systémy a jejich komplexnost, s tím rostou náklady a klesá konkurenceschopnost organizace, což může mít negativní vliv na její fungování a prosperitu. V posledních letech spolu se vzrůstající potřebou řídit komplexitu informačních systémů nabývá na důležitosti tlak na snižování nákladů, důraz na byznys agilitu a udržení si či proaktivní budování konkurenční pozice (Lewis, et al., 2010; MacLennan, et al., 2014). To vede k vyhledávání méně náročných a méně nákladných IT řešení a k orientaci na koncept informačních systémů založených na principu servisní orientace, kam se řadí také cloud computing.

[1] Governance se překládá jako vládnutí, vláda nebo správa, sloveso to govern je vnímáno ve významu vládnout, ovládat, určovat.

[2] Management bývá označován pojmem řízení. Cílem řízení je zabezpečit, aby struktura, chování organizace a alokace podnikových zdrojů byly v souladu s cíli organizace (Gála, a další, 2012). Charakteristickým znakem řízení je existence dvou systémů označených jako systém řízení a řízený systém (Gála, a další, 2012). Gála (2012) dále uvádí, že *„mezi řízeným a řídicím systémem existuje zpětná vazba, která umožňuje řídicímu systému vyhodnocovat (kontrolovat) dosažené cílové chování řízeného systému“*. Funkce řízení je obvykle realizována manažerskými procesy plánování, organizování, vedení a kontrola (Gála, a další, 2012).

Cloud computing, jakožto forma poskytování sdílených, škálovatelných a flexibilních IT zdrojů ve formě služeb, zjednodušuje a urychluje realizaci informačních systému, snižuje náklady spojené s IT, zvyšuje efektivitu a byznys agilitu, a tím umožňuje organizacím, aby pružně reagovaly potřebám rychle se měnícího obchodního prostředí (Buyya, a další, 2011). Ačkoliv je cloud computing relativně novým přístupem, dle průzkumu realizovaného společností International Data Corporation (IDC), trend přijetí služeb veřejného cloud computingu v organizacích neustále roste. Více než 43 % dotázaných organizací očekává, že do roku 2019 budou využívat více než 78 % IT zdrojů ve formě služeb cloud computingu (Mahowald, a další, 2016). Do roku 2018 IDC předpovídá, že minimálně polovina výdajů na IT bude vynakládána na služby cloud computingu (Mahowald, a další, 2016). V České republice celkové výdaje na služby cloud computingu v roce 2014 dosáhly 71 miliónů amerických dolarů, přičemž meziročně se zvýšily o 17,5 % (IDG Czech Republic, 2015). Nejpodstatnější složkou z toho byly výdaje na aplikační služby veřejného cloud computingu, které dosáhly 48 miliónů amerických dolarů (IDG Czech Republic, 2015). V období mezi lety 2014–2019 se v České republice očekává roční míra růstu výdajů na služby veřejného cloud computingu 19,3 % (IDG Czech Republic, 2015). Nejdůležitější hnací síly, které umocňují růst investic vynakládaných organizacemi do využití služeb cloud computingu znázorňuje Obrázek 1.



Obrázek 1: Nejčastější důvody pro využití služeb cloud computingu, zdroj: (IDG Enterprise, 2015)

V prostředí cloud computingu dochází k jasnému odlišení mezi spotřebitelem a poskytovatelem služeb cloud computingu (NIST, 2013). Spotřebitel služby cloud computingu je oddělen od odpovědnosti za rizika spojená s vývojem, poskytováním a údržbou služeb. Tyto odpovědnosti jsou přesunuty na externího poskytovatele, který musí zajistit, aby poskytované služby splňovaly nároky a uspokojovaly potřeby spotřebitelů. Ačkoliv jsou benefity z využívání služeb cloud computingu z pohledu spotřebitele služeb známé a široce akceptované (Barde, 2013), využívání služeb cloud computingu vede z hlediska governance a managementu podnikového IT k problémovým situacím. Tyto situace vyplývají z nedostatečně přizpůsobené organizační struktury, z konfliktů mezi byznys procesy podporovanými službami cloud computingu a mezi byznys procesy podporovanými tradičními IT službami a z nedostatečně přizpůsobených IT procesů, které nejsou schopné zabezpečit efektivní využívání služeb cloud computingu. Navíc z pohledu spotřebitele služeb cloud computingu přestávají

být procesy návrhu a vývoje nové služby cloud computingu relevantní a na významu nabývají zejména procesy týkající se plánování výběru služby a řízení produktivního provozu služby cloud computingu. Za této situace je řízení tradičního životního cyklu IT služeb v prostředí cloud computingu nevyhovující (Tran, a další, 2015). Tyto skutečnosti však současné široce přijímané IT governance a IT management rámce plně nezohledňují a žádný z nich není primárně určen pro governance a management služeb cloud computingu z pohledu spotřebitele (Feuerlicht, a další, 2012). Organizace jakožto spotřebitelé služeb cloud computingu se mohou spoléhat jen na tradiční postupy a nejlepší zkušenosti z praxe IT governance a IT managementu a snažit se je přizpůsobit na základě svých zkušeností tak, aby vyhovovaly specifickým charakteristikám vyplývajících z využívání služeb cloud computingu. Specifika governance a managementu služeb cloud computingu z pohledu spotřebitele služeb cloud computingu se mohou odlišovat v závislosti na modelu nasazení, a proto se tato doktorská disertační práce zaměřuje pouze na model veřejného cloud computingu, kdy jsou služby cloud computingu poskytovány širokému počtu spotřebitelů externím poskytovatelem služeb cloud computingu.

Existující metodiky pro governance a management podnikové informatiky se liší zejména komplexností a zaměřením na oblast řízení IT jako celku nebo na určitou funkční oblast IT. Rozsáhlé metodické rámce, jakými jsou například COBIT nebo ITIL, nejsou zejména z důvodů jejich přílišné složitosti a potenciálně vysokých nákladů spojených s jejich implementací a provozem přijatelné pro malé podniky (Voříšek, a další, 2015). V případě malých podniků se takto komplexní metody řízení nevyužívají, neboť by pro ně byly neefektivní a náklady na jejich zavedení by byly neúměrně vysoké. Jelikož návrh metodického rámce pro governance a management služeb cloud computingu z pohledu spotřebitele vychází z rozsáhlých metodických rámců SOA Governance, COBIT a ITIL, je tato doktorská disertační práce zaměřena na governance a management středních a velkých podniků[3] vystupujících v roli spotřebitele služeb veřejného cloud computingu.

1.2 Stručný přehled současného stavu výzkumu v dané oblasti

Aby informační technologie poskytovaly požadovanou hodnotu nejen organizaci samotné, ale i jejím zákazníkům a dalším zainteresovaným stranám, musí být vyvažován finanční i nefinanční přínos IT s riziky, které s ním souvisí (Brandis, a další, 2013). S rozvojem governance a managementu podnikového IT vznikala řada rámců a doporučení v oblasti IT governance a IT managementu, jako je Control Objectives for Information and Related Technology (COBIT), Information Technology Infrastructure Library (ITIL), ISO 38500 Podniková governance informačních technologií a řada dalších (Buchalcevova, a další, 2015; Jäntti, a další, 2015). IT governance a IT management se soustředí zejména na oblast řízení výkonnosti informačních technologií a snaží se zajistit, aby IT produkovalo očekávanou byznys hodnotu při optimalizaci zdrojů, nákladů a rizik (Orozco, a další, 2015). Vzhledem k rostoucí závislosti úspěšnosti podnikání na informačních technologiích poskytovaných interními či externími dodavateli a nárůstu objemu informací generovaných podnikem nutných pro podporu podnikání, je zavedení některého z rámců pro IT governance a IT management nezbytným krokem (Buchalcevova, a další, 2015).

[3] Nejčastějšími kritérii rozdělení podniků podle velikosti je počet zaměstnanců nebo velikost obratu, velikost kapitálu, případně velikost zisku (Synek, a další, 2010). Podle Doporučení Komise ze dne 6. května 2003 týkající se definice mikropodniků, malých a středních podniků je střední podnik klasifikován jako podnik do 250 zaměstnanců s ročním obratem do 50 milionů EUR nebo pokud bilanční suma rozvahy dosahuje maximálně 43 milionů EUR. Ostatní podniky převyšující hodnoty těchto ukazatelů jsou považovány za velké podniky.

Jednou z nových a stále se rozvíjejících oblastí informačních technologií je poskytování IT zdrojů ve formě služeb (Wattal, a další, 2014). Služby, jakožto základní jednotky servisně orientovaného logického řešení, jsou skládány do kompozitních řešení, které poskytují funkcionalitu požadovanou k automatizaci určitého byznys procesu (Erl, Thomas, 2007a). Jedním z častých důvodů, který mluví pro servisní orientaci, jsou zejména nákladové důvody. Vzhledem k omezeným finančním zdrojům a k rostoucím tlakům na snižování nákladů nabývá hledání cesty k jejich snižování či optimalizaci stále větší význam (Sultan, 2011). Spolu s tím roste také význam systémů založených na službách. Na principu servisní orientace je postavená servisně orientovaná architektura (SOA), kdy volně spojené a znovupoužitelné služby realizují a automatizují specifické byznys procesy, což poskytuje rychlé, flexibilní a nákladově efektivní řešení (Unnamalai, a další, 2014). Na obdobných přístupech je postaven také cloud computing, který stejně jako SOA hraje důležitou funkci v poskytování sdílených IT zdrojů ve formě služeb dostupných přes veřejně dostupnou síť. Řada autorů zabývajících se servisně orientovanou architekturou a cloud computingem hledá vzájemnou synergii mezi těmito přístupy (Hui-min, a další, 2013; Sutherland, 2013; Yang, a další, 2012). Jak SOA, tak i cloud computing sdílí koncept servisní orientace. Oba přístupy mohou být realizovány nezávisle na sobě anebo současně, kdy zejména infrastrukturní a platformní služby cloud computingu mohou poskytnout přidanou hodnotu při budování SOA (Yang, a další, 2012). Cloud computing nenahrazuje SOA (Nabeeh, a další, 2015), ale soustředí se na služby, které mohou být nakoupeny a využívány dle specifické potřeby spotřebitele od externích poskytovatelů služeb cloud computingu. Rajmohan (2014) se domnívá, že servisně orientovaná architektura vytváří stabilní základnu, která usnadňuje celopodnikové přijetí služeb cloud computingu a umožňuje realizaci benefitů spojených s využíváním služeb cloud computingu (Rajmohan, a další, 2014). Principy servisně orientované architektury přináší podnikovému IT vyšší agilitu (Voříšek, a další, 2010), avšak se ve svém důsledku omezují spíše na on-premise řešení, kdy zdroje jsou sdíleny v rámci jediné organizace, což je finančně přijatelné pouze pro velké organizace (Yang, a další, 2012). Podniky hnané potřebou redukce nákladů (Gála, a další, 2012) hledají alternativu k investičně náročným on-premise řešením, což ústí v orientaci směrem ke cloud computingu (Feuerlicht, 2010). Trend směřující směrem k SOA a cloud computingu je bezesporu hnán stejnými silami s cílem rychlé reakce organizace na tržní příležitosti a poptávku zákazníků, získat rychlý přístup k potřebným IT zdrojům, flexibilitu a přizpůsobivost, která je potřeba pro zabezpečení konkurenceschopnosti a minimalizovat náklady na IT (Carroll, a další, 2014; Luthria, a další, 2015). Někteří autoři tvrdí (Wang, a další, 2012), že přijetí služeb cloud computingu je zjednodušeno přijetím servisně orientované architektury, a to z důvodu, že SOA poskytuje vhodný metodický rámec jak pro interně, tak i externě dodávané služby, který zohledňuje také potřebu governance a managementu těchto služeb (Feuerlicht, a další, 2011). Důležitost návrhu rámce pro governance a management služeb vyzdvihuje také Laird (2011), který určuje jako důležitý nástroj pro řízení služeb servisně orientované architektury SOA Governance (Laird, 2011). SOA Governance je nedílnou součástí servisně orientované architektury a její úloha spočívá zejména v definici a implementaci praktik a procesů pro řízení životního cyklu služeb SOA (Rajmohan, a další, 2014). SOA Governance definuje procesy a aktivity zahrnující fáze životního cyklu služby od plánování až po produktivní provoz služby (Hauptvogel, 2013) a to tak, aby služba byla ve shodě s politikami podniku a potřebami obchodních procesů. Stejně jako servisně orientovaná architektura, tak i cloud computing vyžaduje implementaci vhodného IT governance a IT management modelu pro zajištění bezpečného IT prostředí v souladu s regulatorními a legislativními aspekty, s dohodami o využívání služeb cloud computingu a s příslušnými interními standardy a politikami (Brandis, a další, 2013). Existují autoři, kteří se zabývají přizpůsobením různých oblastí tradičních IT governance a IT management rámců jako jsou COBIT nebo ITIL pro prostředí cloud computingu (Bailey, a další, 2014; Feuerlicht, 2010; Stanley, 2014) nebo mapováním specifik cloud computingu na SOA governance. Aplikace principů IT governance a IT managementu je zásadní, jak pro přijetí

služeb cloud computingu, tak pro řízení životního cyklu služeb cloud computingu (Bailey, a další, 2014). Principy obsažené v rámcích pro IT governance a IT management je však nutné přizpůsobit podmínkám prostředí cloud computingu (Van Grembergen, a další, 2009). IT governance by se v prostředí využívání služeb cloud computingu měla soustředit na tvorbu, komunikování a vyžadování politik (Munteanu, a další, 2013), definici organizačních rolí a odpovědností, definici omezení (Bounagui, a další, 2014) a definici procesů (Saidah, a další, 2014) s cílem podpořit výkonnost podnikání a měla by zabezpečovat realizaci byznys hodnoty ze služeb cloud computingu prostřednictvím vytváření rovnováhy mezi benefity, náklady a rizikem (ISACA, 2014b) vyplývajícím z využívání služeb cloud computingu. IT management by se v prostředí řízení služeb cloud computingu měl soustředit na realizaci činností souvisejících s řízením životního cyklu služby cloud computingu v souladu s IT governance (ISACA, 2014b).

Pro prostředí cloud computingu není dostupný žádný všeobecně přijímaný rámec, který by komplexně pokrýval governance a management služeb cloud computingu (Feuerlicht, a další, 2012) jako je tomu například v případě tradičních IT služeb a výše uvedených rámců ITIL, COBIT a ISO 38500 nebo jako v případě servisně orientované architektury (Fortis, a další, 2014), kdy rámec SOA Governance prošel ratifikací a byl uznán jako mezinárodní standard ISO (Kreger, et al., 2012) pro governance servisně orientované architektury. Snahy o standardizaci praktik governance a managementu služeb cloud computingu jsou stále předmětem výzkumu (Gao, a další, 2012). S rostoucím využitím služeb cloud computingu však roste potřeba po efektivním modelu governance a managementu služeb cloud computingu (Bounagui, a další, 2014), který napomůže při naplnění IT cílů v souvislosti s využitím služeb cloud computingu (Hsu, 2012). Stejně jako IT governance a IT management, tak i governance a management v prostředí cloud computingu vyžaduje definování cílů, politik, rolí, odpovědností a procesů v závislosti na zralosti a komplexitě organizace, neboť využití služeb cloud computingu ovlivňuje byznys procesy kritické pro dosažení podnikových cílů (Bailey, a další, 2014). Ačkoliv žádný z rámců pro IT governance a IT management v zásadě není určen pro prostředí cloud computingu (Bounagui, a další, 2014), principy, praktiky a procesy v nich obsažené lze rozšířit a přizpůsobit pro governance a management služeb cloud computingu tak, aby reflektovaly zásadní charakteristiky cloud computingu (Ahmad, a další, 2011). Žádná z dostupných prací však neposkytuje přehled o tom, které procesy dostupných IT governance a IT management rámců jsou nejvíce ovlivněny cloud computingem a jakým způsobem tyto rámce pro prostředí cloud computingu přizpůsobit. Navíc s ohledem na to, že cloud computing je z pohledu zákazníka jedním z nových modelů sourcingu informačních technologií, musí se governance a management v prostředí cloud computingu zabývat nejen stranou poskytovatele služeb computingu, ale také zejména potřebami a požadavky spotřebitelů služeb cloud computingu, a to jak na strategické, tak i na taktické a operativní úrovni tak, aby spotřebitel mohl plně využít potenciál služeb cloud computingu a jejich prostřednictvím realizovat očekávanou byznys hodnotu (Heilig, a další, 2016). Metodický rámec pro cloud computing governance a management by měl obsahovat procesy a postupy, které umožní implementaci systému cloud computing governance a managementu uvnitř organizace a zajistí jeho snadné fungování a kontinuální zlepšování (Saidah, a další, 2014). Problémem je, že ačkoliv Saidah (2014) vyzdvihuje nutnost metodického rámce založeného na procesech, sám ve své práci procesy detailně nespecifikuje (Cook, a další, 2012; Saidah, a další, 2014).

1.2.1 Mezera v poznání v oblasti cloud computing governance a managementu

Autorka této doktorské disertační práce provedla analýzu aktuálního stavu poznání v oblasti IT governance a IT managementu v prostředí využívání služeb cloud computingu, jejímž cílem bylo zjistit mezeru v tomto poznání a zároveň výstupy z této analýzy sloužily jako podklad pro formulaci cílů této doktorské disertační práce a pro stanovení výzkumných otázek. Pro zjištění aktuálního stavu

poznání byla autorkou provedena rešerše dokumentů identifikovaných v databázích Scopus a Web of Science s využitím kombinace klíčových slov „cloud, computing, service, služba, governance, management, framework, proces a proces“. Ačkoliv je cloud computing governance a management aktuálním předmětem výzkumu, velká část nalezených dokumentů se zaměřuje na perspektivu poskytovatele služeb cloud computingu a pouze omezený počet vědeckých publikací je orientován na aspekty governance a managementu služeb cloud computingu z pohledu spotřebitele a to často pouze na specificky úzkou výseč dané problematiky. Z rešerše byly autorkou této doktorské disertační práce záměrně vyřazeny dokumenty, které se týkají pohledu poskytovatele na governance a management služeb cloud computingu. Ty totiž přesně neodrážejí specifika významná z pohledu spotřebitele. Dalším problémem je, že řada autorů zaměňuje pojem IT governance a IT management a pod pojem IT governance zařazuje i aktivity realizované v rámci IT managementu. Ačkoliv je cloud computing governance a management z pohledu spotřebitele stále otevřeným výzkumným problémem, bylo autorkou této doktorské disertační práce celkem nalzeno a analyzováno pouze osm relevantních zdrojů. Z toho se pouze jeden dokument věnuje čistě problematice governance a ostatních sedm dokumentů je zaměřeno na management služeb cloud computingu.

Níže uvedená Tabulka 1 představuje vyhodnocení identifikovaných zdrojů z hlediska jejich obsahového zaměření. Hodnocenými kritérii z hlediska obsahového zaměření identifikovaných zdrojů jsou:

- *databáze* – identifikovaný dokument je uložen v databázi Scopus anebo Web of Science,
- *předmět* – předmět popisuje obsahové zaměření identifikovaného dokumentu. A to jmenovitě, zda dokument popisuje specifické oblasti cloud computing governance (CC governance) anebo cloud computing managementu (CC management),
- *role a odpovědnosti* – role představují vykonávání odpovědností nad činnostmi v rámci pracovního zaměření jednotlivých rolí. Role jsou typicky zařazeny do organizační struktury pro potřeby governance nebo managementu služeb cloud computingu,
- *definice požadavků na budoucí stav, studie proveditelnosti, návrh strategie* – definice požadavků na budoucí stav, studie proveditelnosti, návrh strategie jakožto součást strategického řízení má za cíl identifikace a stanovení budoucího směru a rozvoje podnikové informatiky prostřednictvím využívání služeb cloud computingu. Studie proveditelnosti slouží k posouzení technické a finanční proveditelnosti využívání služeb cloud computingu. Strategické záměry rozvoje podnikové informatiky do prostředí cloud computingu jsou obvykle formulovány v cloud computing strategii. Cloud computing strategie je koncipována tak, aby sloužila jako základní nástroj pro zajištění řízení a správného provádění činností při migraci do prostředí cloud computing a při využívání služeb cloud computingu,
- *řízení rizik* – řízení rizik je zaměřeno na pochopení vystavení se rizikům z využití služeb cloud computingu, na plánování, identifikaci a hodnocení rizik souvisejících s využíváním služeb cloud computingu s cílem minimalizace jejich dopadu na byznys,
- *řízení souladu* – řízení souladu ve smyslu compliance spočívá v identifikaci postupů k zajištění využívání služeb cloud computingu s ohledem na omezení vyplývající z regulativních externích standardů, norem, zákonů a jurisdikce,
- *řízení exit strategie* – řízení exit strategie je zaměřeno na stanovení požadavků a plánů pro ukončení využívání služby cloud computingu u aktuálního poskytovatele služby a přechod k jinému poskytovateli služby nebo k přechodu k on-premise řešení. Ukončení využívání služby vychází zejména z ujednání a podmínek smluv o poskytování služby cloud computingu, a to zejména s ohledem na aktiva spotřebitele,
- *řízení portfolia poskytovatelů* – řízení portfolia poskytovatelů se zaměřuje na hodnocení externích poskytovatelů služeb cloud computingu z různých hledisek. Sleduje se zejména

spolehlivost poskytovatele, zajištění bezpečnosti a ochrany soukromí poskytovatelem, kvalita poskytovaných služeb ve smyslu smluvené úrovně služeb a způsob financování poskytovaných služeb a finanční náročnost vzhledem k rozsahu a úrovni služeb,

- *řízení smluv, SLA* – řízení smluv, SLA se zaměřuje na jasnou definici poskytované služby cloud computingu a zároveň hraje důležitou roli při vytváření a udržování stabilního, spolehlivého a měřitelného smluvního vztahu mezi spotřebitelem a poskytovatelem služeb cloud computingu,
- *řízení výběru služby* – řízení výběru služby se zaměřuje na hodnocení služby cloud computingu z různých hledisek. Zahrnuje zejména stanovení požadavků na službu cloud computingu a identifikaci kritérií hodnocení vzhledem k byznys případu. Provádí zejména hodnocení kvalitativních charakteristik poskytovaných služeb. Vstupem je katalog služeb cloud computingu od různých poskytovatelů,
- *plánování přechodu* – plánování přechodu zahrnuje vytváření plánů pro nasazení a integraci služby cloud computingu do provozního IT prostředí spotřebitele včetně plánování příslušných testů,
- *testování* – testování zahrnuje aktivity související s návrhem a provedením testů přechodu služby cloud computingu do produktivního provozu,
- *řízení přístupu* – jelikož uživatelé přistupují ke službě cloud computingu typicky přes webový prohlížeč, je kritérium řízení přístupu podstatné pro spotřebitele služby cloud computingu zejména z hlediska odpovědnosti za řízení identit, proces autentizace uživatele a stanovení politik přístupové bezpečnosti vzhledem ke službám cloud computingu,
- *monitorování* – monitorování provozu služby zahrnuje aktivity realizující sběr dat o provozu služby cloud computingu včetně hodnocení těchto dat vzhledem k metrikám odsouhlasených ve smlouvách o poskytování služby cloud computingu a eskalace zjištěných odchylek skutečně naměřených hodnot metrik od smluvně stanovených hodnot metrik,
- *řízení událostí, incidentů a problémů* – řízení událostí, incidentů a problémů se zaměřuje na vyhodnocení a nalezení optimálního řešení v případě výskytu odchylky skutečně naměřených hodnot metrik od očekávaných hodnot metrik služby cloud computingu,
- *řízení změn* – řízení změn zajišťuje provedení standardních změn služby cloud computingu, které umožní přizpůsobení služby do žádoucího budoucího stavu. Všechny změny musí být schváleny jak spotřebitelem, tak i poskytovatelem služeb cloud computingu,
- *řízení nepřetržitého zdokonalování* – řízení nepřetržitého zdokonalování stanovuje hodnotící metriky služeb cloud computingu a posuzuje využívané služby z hlediska jejich optimální vhodnosti vzhledem k byznys potřebám,
- *identifikace procesů* – dokument definuje nutnost návrhu procesně orientovaného cloud computing governance anebo cloud computing management,
- *definice procesů* – dokument definuje procesy cloud computing governance anebo cloud computing managementu.

Skutečnost, že v rámci provedené analýzy byly autorkou této disertační práce identifikovány vědecké práce zabývající se problematikou IT governance a IT managementu v prostředí využívání služeb cloud computingu vede k závěru, že existuje teorie cloud computing governance a managementu, kdy na cloud computing governance a management je nahlíženo jako na specializaci metodik IT governance a IT managementu (Fortis, a další, 2014). Cloud computing governance a management by měl obsahovat definici procesů, které umožní spravovat a řídit využívání služeb cloud computingu (Saidah, a další, 2014). Bohužel ve vědecké komunitě neexistuje jednotná definice cloud computing governance a managementu (Saidah, a další, 2014) a není dostupný žádný komplexní metodický rámec pro cloud computing governance a management (Feuerlicht, a další, 2012). Protože se však

jedná o IT službu, nabízí se přizpůsobení procesně orientovaných standardů zaměřených na governance a management servisně orientovaného prostředí, kdy na poskytovanou službu cloud computingu je nahlíženo jako na specifickou IT službu v prostředí veřejného cloud computingu, která je provozována a dodávána poskytovatelem služeb cloud computingu na bázi řešení dostupného velkému množství spotřebitelů na požádání, a která je poptávána a využívána spotřebitelem služeb cloud computingu k informatické podpoře byznys procesů. Služba cloud computingu může být kompozicí dílčích služeb, avšak spotřebitel ji vnímá jako službu komplexní. Při hodnocení stavu poznání není důležitým faktorem hodnocení struktury identifikovaných dokumentů, nýbrž jejich obsahové pokrytí problematiky governance a managementu využívání služeb cloud computingu.

V prvním analyzovaném dokumentu jeho autor Bounagui (2014) identifikuje potřebu cloud computing governance a vymezuje vztah cloud computing governance k podnikové a IT governance. Využití služeb cloud computingu má dopad na oblasti IT governance a IT managementu, a to zejména na aspekty bezpečnosti a soukromí, na dohody o úrovni služby cloud computingu SLA (Service Level Agreement), na řízení rizik, souladu a auditu, na politiky řízení služeb cloud computingu a na interoperabilitu a portabilitu.

V dalším výzkumu se Bounagui (2015) zabývá identifikací a analýzou požadavků na cloud computing governance a analýzou metodik z hlediska naplnění cílů cloud computing governance. V tomto případě však zaměňuje pojmy governance a management a zahrnuje pod pojem cloud computing governance také aktivity spojené s řízením (managementem). Nefunkční požadavky na cloud computing governance stanovuje Bounagui (2015) jako naplnění potřeb zainteresovaných stran, pokrytí všech aspektů cloud computingu, pokrytí celého životního cyklu cloud computing governance, který zahrnuje návrh, implementaci, řízení, monitorování a neustálé zlepšování služeb cloud computingu, dále využití jednotného integrovaného rámce pro řízení IT služeb a cloud computing služeb, procesně orientovaný přístup, udržování úrovně kvality služby a využití metrik pro měření výkonnosti. Funkční požadavky jsou kategorizovány do tří hierarchických úrovní domén, kontrol a aktivit. Doménami jsou cloud migrace, informační bezpečnost, řízení rizik a dohody o úrovni služby cloud computingu (SLA). Doména cloud migrace zahrnuje aktivity související s plánováním, realizací a hodnocením úspěšnosti migrace dat a aplikací mezi poskytovateli služeb. Doména informační bezpečnost zahrnuje řízení informační bezpečnosti v prostředí cloud computingu založené na rodině norem ISO 27000. Doména řízení rizik se zaměřuje na vytvoření systému řízení rizik v prostředí cloud computingu. Doména SLA se zaměřuje na řízení dohod o úrovni služby jakožto základním nástroji pro vytvoření a udržování spolehlivého a měřitelného obchodního vztahu mezi poskytovatelem a spotřebitelem.

Bailey (2014) diskutuje aplikovatelnost IT governance rámců COBIT, Cloud Cube Model, COSO ERM framework, ENISA, ITIL a ISO 2700 pro prostředí cloud computingu a rozšiřitelnost tradičního IT governance pro řízení služeb cloud computingu. A to zejména z hlediska řízení rizik, interních hrozeb, auditu, výkonnostních metrik, bezpečnosti a zodpovědnosti. Dále jako výsledek dekompozičního procesu s cílem rozšířit podnikový IT governance rámec do prostředí cloud computingu identifikuje nejvýznamnější domény k řešení jako byznys procesy, modely služeb cloud computingu, modely nasazení služeb cloud computingu, způsob implementace služeb cloud computingu, řízení rizik a metody řízení služeb cloud computingu specifické pro vybrané řešení.

Ahmad (2011) se zaměřuje na specifickou oblast řízení služeb cloud computingu, kterou je ochrana uživatelských dat a navrhuje governance a management rámec pro řízení adopce a využívání služeb cloud computingu založený na standardech ISO27001/2, COBIT, PCI-DSS, NIST 800-53 rev3 a HIPAA a na legislativních principech. Diskuze o otázkách governance a managementu služeb v prostředí cloud computingu je rozdělena do oblastí v závislosti na modelu služeb, kdy je oddělena

a přehledně definována odpovědnost v oblastech governance a managementu na straně spotřebitele a poskytovatele služeb cloud computingu. Ahmad (2011) zdůrazňuje nutnost souladu využívání služeb cloud computingu s národní legislativou a jurisdikcí a zahrnuje oblast compliance mezi základní oblasti navrhovaného rámce. Z pohledu spotřebitele vidí jako nejdůležitější oblasti podnikový management, řízení rizik, řízení aktiv, výběr modelu služeb cloud computingu a governance organizační strukturu skládající se z vrcholového vedení.

Saidah (2014) definuje cloud computing governance jako management rámec pokrývající relevantní zainteresované strany a byznys procesy a zabezepčující, že služby cloud computingu budou podporovat realizaci byznys strategie a dosažení podnikových cílů. Saidah (2014) navrhuje nový procesně orientovaný cloud governance model, který se zaměřuje na perspektivu tvorby a prosazování politik, na provozní perspektivu a na perspektivu řízení. V rámci každé perspektivy je definován soubor procesů. Bohužel však dokument neobsahuje definici těchto procesů, ale pouze jeji názvy. Navržený cloud governance model je možno implementovat prostřednictvím kroků, které zahrnují vznik události iniciující potřebu využití služby cloud computingu, plánování adopce služby cloud computingu v souladu s potřebami byznysu, návrh a realizace cloud prostředí, provozování služby cloud computingu, dodávka a monitorování služby a hodnocení provozu služby cloud computingu.

Rehman (2015) se zabývá řízením služeb cloud computingu z perspektivy spotřebitele. Podle něj se management služeb cloud computingu skládá ze dvou fází, a to z před-interakční fáze a z interakční fáze. Před-interakční fáze obsahuje aktivity související s výběrem služby cloud computingu od vhodného poskytovatele. Interakční fáze zahrnuje aktivity související s využíváním služby cloud computingu, monitorování výkonnosti provozu vybrané služby, hodnocení alternativních služeb cloud computingu aktuálně dostupných na trhu a zahájení výběru a přechodu na alternativní službu v případě, že aktuálně využívaná služba nesplňuje kvalitativní požadavky či dosahuje stejné úrovně kvalitativních požadavků jako alternativní služba, avšak při vyšších nákladech.

Schneider (2015) definuje životní cyklus služby cloud computingu se zaměřením na získávání a využívání služeb cloud computingu. Proces získávání a využívání služeb cloud computingu a integrace externích IT zdrojů do běžných byznys operací je komplexní aktivitou, kdy organizace čelí novým rizikům vyplývajících z obavy ochrany dat při zpracování a uchovávání dat externím poskytovatelem, z rostoucí závislosti na externím poskytovateli nebo z nejistoty při dodržování legislativních požadavků. Proces řízení životního cyklu služby cloud computingu se skládá z kroků identifikace požadavků na služby cloud computingu, identifikace kritérií pro výběr služby, specifikace systémů nebo částí systémů, které budou přeneseny do prostředí cloud computingu, hodnocení dostupných poskytovatelů na trhu služeb cloud computingu a jimi poskytovaných služeb vzhledem k byznys případu, výběr poskytovatele a vyjednávání smluvních podmínek, finální hodnocení a rozhodnutí o výběru poskytovatele a služby cloud computingu, integrace služby cloud computingu do provozního prostředí, konfigurace služby, testování služby, využívání služby cloud computingu v produktivním provozu, monitorování provozu služby, řízení vztahů s poskytovatelem a ukončení využívání služby cloud computingu.

Prasad (2014) se ve své práci zabývá definicí organizační struktury z hlediska IT governance v prostředí využívání služeb cloud computingu a hodnotí vliv přizpůsobení organizační struktury pro toto prostředí z hlediska efektivnosti a z hlediska vztahu organizační struktury k byznys cílům a finančním cílům v oblasti využívání služeb cloud computingu a k dosažení zvýšení celkové byznys agility.

Tabulka 1 znázorňuje vyhodnocení výše popsaných zdrojů vzhledem ke kritéiím hodnotícím obsah těchto zdrojů.

Tabulka 1: Vyhodnocení identifikovaných zdrojů vůči kritériím z hlediska jejich obsahového zaměření, zdroj: (autor)

Zdroj / Obsahové zaměření	(Bounagui, a další, 2014)	(Bounagui, a další, 2015)	(Bailey, a další, 2014)	(Ahmad, a další, 2011)	(Saidah, a další, 2014)	(Rehman, a další, 2015)	(Schneider, a další, 2015)	(Prasad, a další, 2014)
Databáze	WoS	Scopus	Scopus	Scopus	Scopus	WoS Scopus	WoS, Scopus	Scopus WoS
Předmět	CC management	CC management	CC management	CC management	CC management	CC management	CC management	CC governance
Role a odpovědnosti	+	—	+	+	+	—	—	++
Definice požadavků na budoucí stav, studie proveditelnosti, návrh strategie	—	+	—	—	—	—	+	—
Řízení rizik	+	+	+	+	+	—	—	—
Řízení souladu	+	—	—	+	+	—	—	—
Řízení exit strategie	—	—	—	—	+	—	+	—
Řízení portfolia poskytovatelů	—	+	—	—	—	+	+	—
Řízení smluv, SLA	+	+	—	—	+	—	+	—
Řízení výběru služby	—	+	—	—	—	+	+	—
Plánování přechodu	—	+	—	—	—	—	+	—
Testování	—	+	—	+	—	—	+	—
Řízení přístupu	—	—	—	+	+	—	—	—

Zdroj / Obsahové zaměření	(Bounagui, a další, 2014)	(Bounagui, a další, 2015)	(Bailey, a další, 2014)	(Ahmad, a další, 2011)	(Saidah, a další, 2014)	(Rehman, a další, 2015)	(Schneider, a další, 2015)	(Prasad, a další, 2014)
Monitorování provozu služby	—	—	—	+	+	+	+	—
Řízení událostí, incidentů a problémů	—	—	—	—	+	—	—	—
Řízení změn	—	—	—	—	+	—	—	—
Řízení nepřetržitého zdokonalování	—	+	—	—	+	+	—	—
Identifikace procesů	Ne	Ano	Ne	Ne	Ano	Ne	Ne	Ne
Definice procesů	Ne	Ne	Ne	Ne	Ne	Ne	Ne	Ne

Legenda	
Aspekt není řešen	—
Aspekt je řešen	+
Aspekt je detailně řešen	++

Jak vyplývá z analýzy výše uvedených dokumentů (Tabulka 1), ani jeden dokument nenabízí kompletní rámec pro cloud computing governance a management a chybí identifikace a definice procesů governance a managementu služeb cloud computingu z pohledu spotřebitele. Z rešerše provedené autorkou této doktorské disertační práce dále vyplynulo, že existuje odlišení mezi cloud computing governance a cloud computing managementem (Copie, a další, 2013). Zatímco výzkumu v oblasti cloud computing managementu je věnována pozornost, ačkoliv perspektiva spotřebitele byla relativně do nedávna opomíjena (Rehman, a další, 2015), jak vyplývá z poznatků získaných během procesu rešerše, výzkum v oblasti cloud computing governance stojí více méně stranou (Copie, a další, 2013) nebo je problematika governance v prostředí využívání služeb cloud computingu často zaměňována s problematikou cloud computing managementu a není brán zřetel na skutečnost, že cloud computing governance se sestává z vedení, organizačních struktur a procesů (Brandis, a další, 2013), které zajišťují pouze to, že informační technologie efektivně podporují realizaci byznys strategie a zajištění cílů organizace, a že cloud computing governance je prakticky pouze v odpovědnosti vrcholového vedení organizace. V souvislosti s cloud computing managementem a s řízením životního cyklu služby cloud computingu jsou různými autory často adresovány pouze specifické otázky a problémy cloud computing managementu (Fortis, a další, 2014) jako je například řízení rizik cloud computingu (Harlili, 2014) nebo aspekty řízení SLA (Aljoumah, a další, 2015; Comuzzi, a další, 2013). Návrh komplexnějšího metodického rámce pro cloud computing governance a management obsahujícího navíc detailní specifikaci procesů zatím ve vědecké komunitě chybí. Existuje řada platforem pro cloud computing management nabízených jako služba, které jsou specificky navržené s cílem poskytnout nástroje pro řízení prostředí využívání služeb v modelu veřejného cloud computingu, a které poskytují kromě samoobslužného rozhraní, portálu pro měření úrovně využití a účtování služeb a katalogu služeb také nabídku integrace s externími systémy podnikového managementu. Nicméně, žádný z nich není navržen z pohledu spotřebitele služeb cloud computingu. To potvrzuje skutečnost, že perspektiva řízení služeb cloud computingu z pohledu spotřebitele služeb cloud computingu začala v rámci vědeckého výzkumu nabírat na důležitosti teprve relativně nedávno (Rehman, a další, 2015). Pro spotřebitele není navržen metodický rámec, který by komplexně pokrýval aspekty governance a managementu služeb cloud computingu (Bounagui, a další, 2015; Feuerlicht, a další, 2012), jakými jsou zejména aplikace jednotného přístupu cloud computing governance a managementu, uspokojení potřeb zainteresovaných stran, pokrytí specifik využití služeb cloud computingu, pokrytí životního cyklu cloud computing governance, pokrytí cloud computing managementu, udržování požadované úrovně kvality služby cloud computingu hodnocené pomocí výkonnostních metrik a procesní orientace (Bounagui, a další, 2015). Je proto nutné zajistit návrh komplexního governance a managementu služeb cloud computingu s cílem podpory byznys cílů, zajištění realizace byznys hodnoty z využití služeb cloud computingu a vytvoření vhodného rozhodovacího procesu ve vztahu ke službám cloud computingu (Bounagui, a další, 2015). Metodický rámec pro governance a management služeb cloud computingu by měl obsahovat procesy, s jejichž pomocí bude vytvořen specifický model cloud computing governance a management v organizaci, a dále role odpovědné za tyto procesy, které současně zajistí podporu při implementaci a prosazování tohoto modelu v organizaci (Saidah, a další, 2014). Takovýto komplexní a procesně orientovaný metodický rámec pro governance a management služeb cloud computingu z pohledu spotřebitele však žádný z analyzovaných dokumentů nenavrhuje.

1.3 Cíle doktorské disertační práce

Hlavním cílem této doktorské disertační práce je ***návrh metodického rámce pro governance a management využívání služeb cloud computingu (metodický rámec Cloud computing governance a management) z pohledu spotřebitele služeb cloud computingu***. Navržený metodický rámec Cloud computing governance a management se skládá z modelu cloud computing governance a z modelu cloud computing management.

Hlavní cíl doktorské disertační práce vychází ze stavu poznání současného reálného prostředí. K dosažení hlavního cíle byly autorkou této doktorské disertační práce definovány následující dílčí cíle, které umožňují splnit hlavní cíl práce:

- DC1: Analýza stávajících metodických rámců IT governance a IT managementu z hlediska prostředí cloud computingu z pohledu spotřebitele služeb.
- DC2: Vymezení a sjednocení pojmů governance služeb cloud computingu (cloud computing governance) a management služeb cloud computingu (cloud computing management).
- DC3: Přizpůsobení a rozšíření metod metodických rámců SOA Governance a COBIT 5 se zohledněním specifik vyplývajících z prostředí využívání služeb cloud computingu z pohledu spotřebitele služeb pro návrh modelu pro governance využívání služeb cloud computingu (Cloud computing governance).
- DC4: Přizpůsobení a rozšíření metod metodických rámců ITIL 2011 a COBIT 5 se zohledněním specifik vyplývajících z prostředí využívání služeb cloud computingu z pohledu spotřebitele služeb pro návrh modelu řízení životního cyklu služeb cloud computingu (Cloud computing management).
- DC5: Ověření navrženého metodického rámce pro governance a management využívání služeb cloud computingu (Cloud computing governance a management) z pohledu spotřebitele služeb cloud computingu na případové studii.

1.4 Výzkumné otázky

Jedním z východisek pro návrh metodického rámce pro governance a management využívání služeb cloud computingu (Cloud computing governance a management) z pohledu spotřebitele služeb cloud computingu je formulace výzkumných otázek, které napomáhají identifikovat aktuální stav reálného prostředí tak, aby na základě nalezení jejich odpovědí byly naplněny výše definované cíle této doktorské disertační práce. Výzkumné otázky vychází z rešerše literatury a ze současného stavu výzkumu v dané oblasti.

Pro naplnění cílů doktorské disertační práce jsou stanoveny následující výzkumné otázky:

- ***VO1: Jak je ve stávajících metodických rámcích IT governance a IT managementu podporována governance a management služeb cloud computingu z hlediska spotřebitele služeb?***

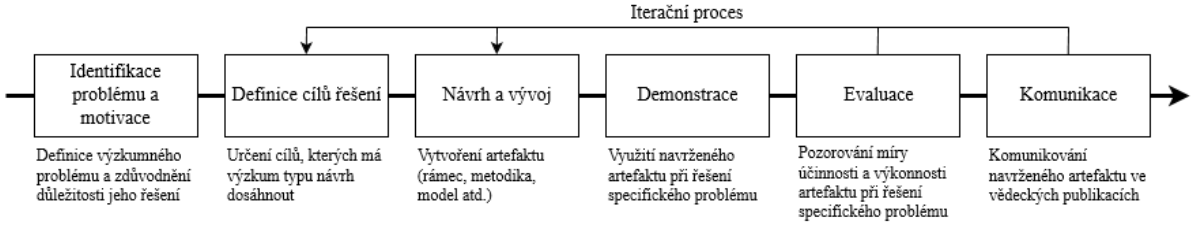
Tato výzkumná otázka zkoumá, zda vůbec a na jaké úrovni stávající metodické rámce pro IT governance a IT management podporují oblast governance a managementu využívání služeb cloud computingu z hlediska spotřebitele. Dále výzkumná otázka zkoumá, zda případná existující podpora je nebo není na dostatečné úrovni.

- ***VO2: V jakých oblastech, do jaké míry a jakým způsobem je možné přizpůsobit metodické rámce IT governance a IT managementu pro governance a management služeb cloud computingu z hlediska spotřebitele služeb?***

Tato výzkumná otázka zkoumá možnosti přizpůsobení metodických rámců pro IT governance a IT management pro prostředí cloud computingu z hlediska spotřebitele služeb a v jakých oblastech je možné toto přizpůsobení realizovat. Zároveň tato výzkumná otázka je zaměřená na úroveň přizpůsobitelnosti IT governance a IT management procesů pro prostředí cloud computingu.

1.5 Vědecké metody dosažení cílů práce

Pro dosažení cílů této disertační práce byla autorkou této disertační práce použita vědecká metoda Design Science Research Methodology (Peffers, a další, 2008). Výstupem této vědecké metody je artefakt metodický rámec, který musí být ověřen při řešení konkrétního problému a komunikován prostřednictvím vědeckých publikací. Vědecká metoda Design Science Research Methodology se skládá ze šesti sekvenčně posloupných kroků znázorněných na Obrázku 2. Tato metoda umožňuje provádění kroků v iteracích, kdy jednotlivá opakování mění kontext, ve kterém probíhá další krok.



Obrázek 2: Design Science Research Methodology, zdroj: (Peffers, a další, 2008)

Nejprve byla autorkou této doktorské disertační práce provedena rešerše a kritická analýza dostupných vědeckých publikací a charakteristika aktuálního stavu reálného prostředí governance a managementu využívání služeb cloud computingu. Z této analýzy poznatků získaných z dostupné a relevantní vědecké literatury vyplynulo, že neexistuje komplexní metodika pro governance a management služeb cloud computingu z pohledu spotřebitele. Základním východiskem této doktorské disertační práce je stanovení výzkumných otázek (kapitola 1.4), kdy nalezení odpovědí na tyto otázky umožní naplnění cílů této doktorské disertační práce (kapitola 1.3). Za účelem nalezení předpokládaných odpovědí na výzkumné otázky (Molnár, a další, 2012), byl realizován exploratorní výzkum, který umožnil autorce této doktorské disertační práce získat povědomí o aktuálním stavu zkoumané oblasti. Základem je deskripce zkoumané oblasti a rozbor existujících systémů, který je popsán v kapitole Teoretická východiska a koncepty (kapitola 2), IT governance a IT management v prostředí cloud computingu (kapitola 3) a aplikovatelnost metodických rámců IT governance a IT managementu pro prostředí využívání služeb cloud computingu (kapitola 4). Pomocí metody abstrakce byly autorkou vydělené pouze poznatky podstatné z hlediska vymezení cílů této doktorské disertační práce.

Při návrhu a vytvoření artefaktu metodický rámec cloud computingu governance a management z pohledu spotřebitele služeb cloud computingu byl autorkou této doktorské disertační práce využit normativní přístup k vědeckému zkoumání systému. Během tohoto kroku autorka vycházela z detailní analýzy metodických rámců pro IT governance a IT managment a odborné literatury. Metoda analýzy byla autorkou této doktorské disertační práce doplněna o další logické metody indukce a dedukce, které spolu úzce souvisejí a vzájemně se doplňují (Molnár, a další, 2012) a v této doktorské disertační práci jsou navzájem kombinovány. Pomocí dedukce bylo autorkou z obecně platných závěrů a teoretických poznatků získaných z provedené analýzy usuzováno na specifické případy governance

a managementu služeb cloud computingu z pohledu spotřebitele. Oproti tomu pomocí indukce byly autorkou vyvozeny obecné závěry na základě jedinečných poznatků o teoretickém a praktickém fungování systémů IT governance a IT managementu využitých v navrženém metodickém rámci. Syntézou získaných poznatků z provedené analýzy a rozvojem obecně platných závěrů s využitím metod indukce a dedukce byl autorkou této doktorské disertační práce vytvořen výsledný artefakt metodický rámec (kapitola 5, kapitola 6, kapitola 7).

Pro demonstraci a evaluaci navrženého artefaktu Metodický rámec cloud computing governance a management z pohledu spotřebitele služeb cloud computingu byla autorkou této doktorské disertační práce využita empirická metoda případová studie (Molnár, a další, 2012), pomocí které byl navržený metodický rámec ověřen v praxi (kapitola 8). Případová studie byla realizovaná v souladu s metodologií pro návrh a realizaci případové studie pro vědecké účely definované v publikaci Case Study Research: Design and Methods (Yin, 2009), která definuje jednotlivé kroky plánování a realizace případové studie jako plánování, návrh a příprava případové studie, sběr podkladů a dat a jejich interpretace a vyhodnocení případové studie. Pro sběr podkladů a dat byly autorkou navíc využity metody pozorování, strukturovaný rozhovor, dotazníkové šetření a analýza dostupných dokumentů z reálného byznys prostředí při řešení specifického problému.

Části této doktorské disertační práce byly publikovány ve formě příspěvku na konferencích a v recenzovaných časopisech.

1.6 Typy výstupů a očekávané přínosy doktorské disertační práce

Vědecký výzkum, který se váže k této doktorské disertační práci, je považován za výzkum typu návrh (Design Science Research), neboť výstupem je artefakt metodický rámec (Gregor, a další, 2013). Jak již autorka této disertační práce objasnila v kapitole 1.3, hlavním cílem doktorské disertační práce je návrh metodického rámce Cloud computing governance a management z pohledu spotřebitele služeb.

Předpokládané přínosy doktorské disertační práce jsou:

- analýza aplikovatelnosti principů IT governance a IT managementu v prostředí governance a managementu využívání služeb cloud computingu z pohledu spotřebitele služeb,
- sjednocení pojmů v oblasti governance a managementu služeb cloud computingu z pohledu spotřebitele služeb,
- návrh metodického rámce Cloud computing governance a management z pohledu spotřebitele služeb cloud computingu,
- návrh modelu governance využívání služeb cloud computingu a modelu řízení životního cyklu služby cloud computingu z pohledu spotřebitele služeb.

Pro praktické využití doktorská disertační práce poskytne:

- návrh procesů vhodných pro realizaci modelu Cloud computing governance z pohledu spotřebitele služeb,
- návrh rolí specifických pro Cloud computing governance z pohledu spotřebitele služeb,
- vymezení postupu implementace modelu Cloud computing governance z pohledu spotřebitele služeb,
- návrh procesů vhodných pro realizaci modelu Cloud computing management z pohledu spotřebitele služeb a jejich logické seskupení do fází životního cyklu služby cloud computingu z hlediska spotřebitele služeb,
- návrh rolí specifických pro Cloud computing management z pohledu spotřebitele služeb,

- rozšíření vybraných objektů a definice nových objektů modelu Management Byznys Informatiky (MBI) na podkladu navrženého metodického rámce Cloud computing governance a management z pohledu spotřebitele služeb cloud computingu.

1.7 Věcná návaznost jednotlivých kapitol práce

Věcná návaznost kapitol doktorské disertační práce je výsledkem logického postupu jejího zpracování pro dosažení cílů práce. Doktorská disertační práce je rozdělena do jednotlivých logických celků, které pokrývají úvodní vymezení, teoretickou část práce, praktickou část práce a její verifikaci.

Úvodní vymezení doktorské disertační práce (kapitola 1) se zabývá určením tématu doktorské disertační práce, jehož východiska jsou podložená stručným přehledem současného stavu výzkumu v dané oblasti, identifikací mezery v poznání v oblasti cloud computing governance a managementu, definicí cílů doktorské disertační práce, určením typů výstupů a očekávaných přínosů, vymezením výzkumných otázek a popsáním vědeckých metod zkoumání pro dosažení cíle této doktorské disertační práce.

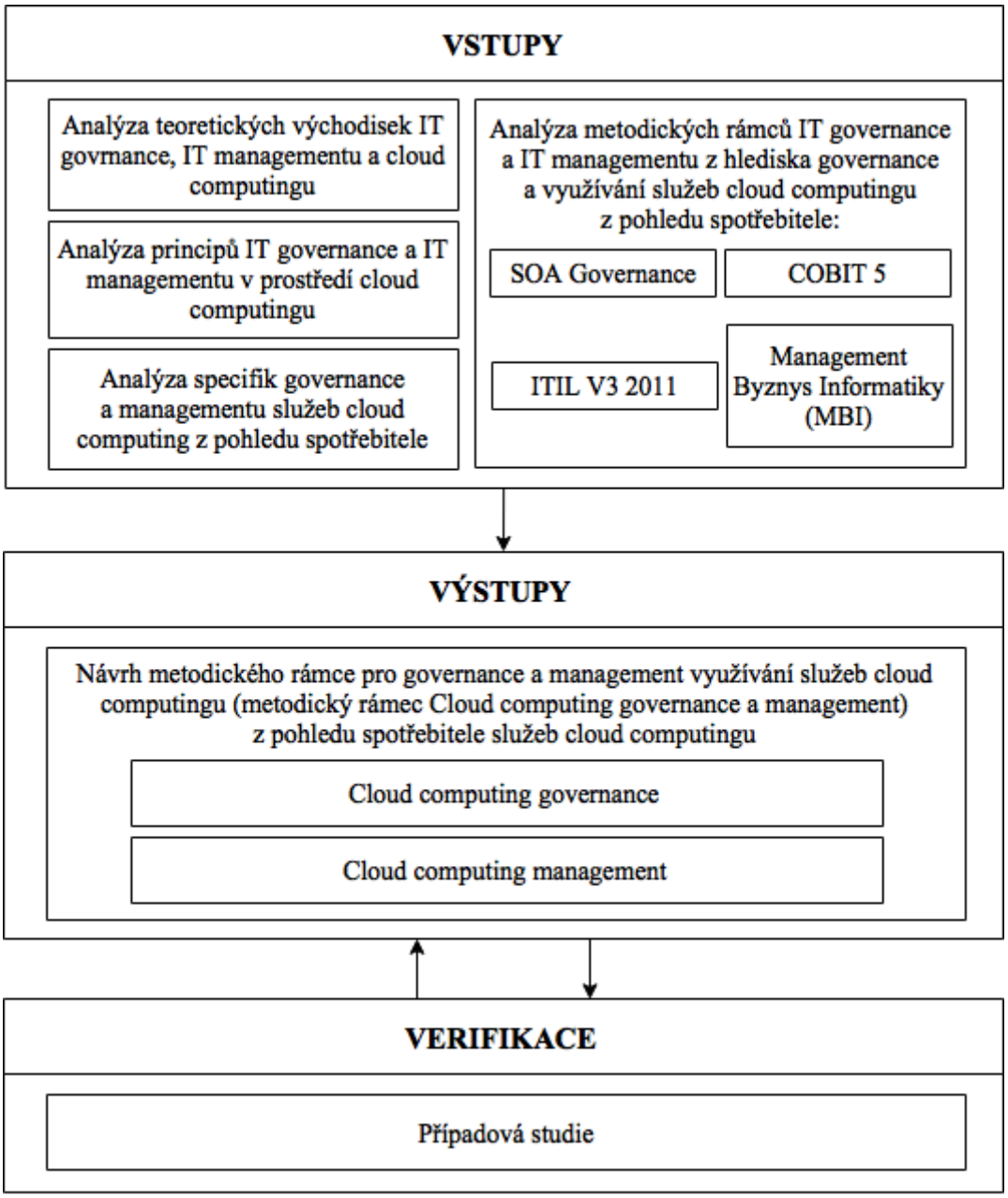
Teoretická část doktorské disertační práce (kapitola 2, 3, 4) vymezuje hlavní teoretická východiska a koncepty této práce. Zabývá se analýzou základních teoretických východisek IT governance, IT management a cloud computing (kapitola 2), principů governance a managementu služeb cloud computingu z pohledu spotřebitele (kapitola 3) a metodických rámců vztahujících se k oblasti IT governance a IT managementu se zohledněním specifik využívání služeb cloud computingu (kapitola 4).

Praktická část doktorské disertační práce (kapitola 5, kapitola 6, kapitola 7) se na základě analýzy současného stavu výzkumu v oblasti aplikace praktik IT governance a IT managementu do prostředí využívání služeb cloud computingu zabývá návrhem metodického rámce Cloud computing governance a management z pohledu spotřebitele služeb cloud computingu. Stanovuje východiska navrženého metodického rámce, cíle, rozsah a definuje strukturu a komponenty metodického rámce Cloud computing governance a management, který se skládá z částí Cloud computing governance a Cloud computing management.

Verifikace doktorské disertační práce (kapitola 8) realizuje prostřednictvím případové studie praktické ověření navrženého metodického rámce Cloud computing governance a management z pohledu spotřebitele služeb cloud computingu.

Závěry doktorské disertační práce (kapitola 9) popisuje zhodnocení úrovně naplnění cílů této doktorské disertační práce, odpovědí na výzkumné otázky, teoretické a praktické přínosy práce, srovnání navrženého artefaktu metodický rámec s aktuálním mezinárodním výzkumem v dané oblasti, zhodnocení dosažených výsledků z hlediska jejich využitelnosti v reálném byznys prostředí nebo pro další vědecký výzkum a náměty pro další vědecký výzkum.

Výše uvedená struktura doktorské disertační práce odráží aktivity, které vedou k naplnění definovaných cílů této doktorské disertační práce (kapitola 1.3). Teoretická (kapitola 2) a analytická část práce (kapitola 3 a 4) obsahuje vstupy pro řešení cílů této doktorské disertační práce. Praktická část definuje navržený metodický rámec (kapitola 5, kapitola 6, kapitola 7) jakožto výstup řešení cílů této doktorské disertační práce, který je ověřen na případové studii (kapitola 8). Struktura řešení této doktorské disertační práce je přehledně znázorněna na Obrázku 3.



Obrázek 3: Postup řešení dosažení cílů odrážející se ve struktuře doktorské disertační práce, zdroj: (autor)

2 Teoretická východiska doktorské disertační práce

Cílem této kapitoly je definovat základní teoretická východiska doktorské disertační práce. Jednotlivé podkapitoly popisují výstupy z rešerše dokumentů provedené autorkou této doktorské disertační práce, které se zabývají IT governance, IT managementem a cloud computingem. Kapitola vymezuje definice IT governance, IT managementu a cloud computingu.

Organizace jsou natolik závislé na informačních technologiích (IT), že úspěšnost realizace klíčových činností a efektivní podpory byznys procesů je přímo ovlivněna výkonností podnikového IT. Spolu s výkonností podnikového IT rostou také náklady na pořízení a rozvoj podnikového IT. Informační technologie však nejsou pouze faktorem úspěšnosti dosažení byznys cílů a dlouhodobé prosperity podnikání, ale přináší příležitost odlišovat se a dosáhnout konkurenční výhody. Z tohoto důvodu je kritické implementovat efektivní systém IT governance a IT management v souladu s potřebami byznysu. Efektivní systém IT governance a IT management zajistí naplnění požadavků byznysu a zainteresovaných stran na využití IT při minimalizaci nákladů a rizik spojených s využitím IT. Jak IT governance, tak i IT management slouží k různým účelům a jsou realizovány odlišnými typy aktivit a na různých organizačních úrovních s rozdílnými odpovědnostmi. IT governance je kritickým faktorem, který umožňuje generovat požadovanou byznys hodnotu z využití IT a zajišťuje, že rozvoj IT bude v souladu se strategickými potřebami byznysu. Zároveň IT governance definuje pravidla a omezení a dohlíží jejich dodržování. IT management je kritickým faktorem pro efektivní provoz IT operací v souladu s požadavky IT governance. S růstem důležitosti IT governance a IT managementu vznikaly návody, jak efektivně a účinně dosáhnout strategických cílů s využitím informačních technologií. Tyto návody souhrnně nazývané metodiky (Svatá, 2011) jsou postavené nejčastěji na doporučeních založených na zkušenostech z praxe a obsahují řadu procesů, praktik a postupů. Principy IT governance, IT managementu, governance a managementu využívání služeb cloud computingu a analýza stávajících metodik IT governance a IT managementu z hlediska prostředí cloud computingu z pohledu spotřebitele služeb jsou diskutovány v následujících podkapitolách.

2.1 IT governance

Governance ve svém nejužším pojetí představuje postupy a procesy pro správu, regulaci a kontrolu organizace reprezentující zájmy zainteresovaných stran (OECD, 2015). Governance je realizována pomocí souboru politik, pravidel, omezení, procesů, kontrolních mechanismů a nastavení odpovědností tak, aby organizace prováděla činnosti efektivně, transparentně a odpovědně (OECD, 2015). Principy governance se přenesly z governance obchodních společností do specifických systémů podnikové (enterprise) governance, governance podnikové architektury či governance informačních technologií (Gála, a další, 2015). Erl (2011) formuloval společné charakteristiky systémů governance následovně:

- reprezentace společných pravidel nebo zájmů,
- stanovení pravidel, omezení a parametrů, které řídí, vedou a ovlivňují rozhodování,
- měření a regulace výkonnosti procesů, minimalizace spotřeby nákladů, času a zdrojů při realizaci procesů při zachování požadované kvality výstupu,
- určení odpovědností a pravomocí pro rozhodování,
- vytvoření mechanismu pro interakci, kooperaci a sdílení znalostí,

- kontrolování dodržování souladu s platnými pravidly a politikami governance, legislativními a regulatorními požadavky.

Governance je postavena na čtyřech základních složkách (Ondruška, 2011; Selig, 2015), kterými jsou politiky, procesy, technologie a lidé. Lidé zahrnují organizační struktury, role, odpovědnosti a rozhodovací procesy, na kterých se podílí. Role a jim přiřazené odpovědnosti musí být definované v souladu se strukturou governance, jejích politik, definovaných pravidel a omezení, procesů a souvisejících aktivit jako je řízení a přezkoumání realizovaných činností a komponent governance (Selig, 2015). Lidé jsou základním prostředkem, pomocí kterého je možno dosáhnout byznys cílů. Aby lidé věděli, co jsou cíle podniku a byli srozuměni s tím, jak těchto cílů dosáhnout, definuje governance politiky, které navádí lidi zaměstnané v organizaci požadovaným směrem. Na vrcholu hierarchie stojí vedoucí manažeři, kteří iniciují politiky a jejich prosazování. Politiky fungují jako určitá příručka, která reguluje činnost lidí v podniku. Procesy pak zajišťují, že politiky definované v podniku budou komunikovány a realizovány všemi lidmi na všech pozicích podle byznys potřeb daného podniku a bude pochopena důležitost a význam governance. Podle Ondruška (2011) musí být v kontextu governance rozlišení mezi řídícími (governing) a řízenými (governed) procesy. Řídící procesy neustále probíhají v organizaci a zabezpečují, že řízené procesy budou ve shodě s politikami, pravidly a omezeními governance. Řízené procesy realizují a prosazují governance v konkrétní organizaci. Je zřejmé, že nelze v praxi definovat politiky a procesy tak, aby byly ve všech podnicích stejné. Vedení každého podniku tak má za úkol definovat politiky a procesy na míru potřebám obchodních zájmů svého podniku. Návrh, implementace a realizace governance je typicky podporována různými technologiemi a nástroji. Zejména nástroji pro řízení provozu governance, pro podporu governance procesů, pro podporu monitorování a pro správu artefaktů.

Čtyři základní složky governance se promítají také ve struktuře IT governance. Podle Van Grembergen (2012) se IT governance se skládá z:

- IT governance struktur,
- IT governance procesů,
- IT governance relačních mechanismů.

IT governance struktury jsou organizační jednotky, útvary nebo role, které mají přidělené odpovědnosti a kompetence vztahující se k procesu rozhodování o IT aktivech a IT operacích. Důležitou součástí IT governance struktury je řídící výbor tzv. steering committee složený ze zástupců byznysu a IT na vrcholové úrovni, který připravuje a realizuje rozhodnutí v oblasti IT v souladu s potřebami organizace jako celku s cílem realizovat byznys hodnotu z IT investic (Schlosser, a další, 2011). Řídící výbor by se měl zabývat společnou koordinací a plánováním byznys cílů, IT cílů, byznys plánů, IT plánů a investic. Řídící výbor, tzn. všichni členové řídícího výboru by měli společně převzít zodpovědnost za realizovaná rozhodnutí, aktivity a související rizika. IT governance procesy zajišťují, že plánování a provoz IT je v souladu s IT politikami a legislativními a regulatorními požadavky (Van Grembergen, a další, 2012). IT governance relační mechanismy se vztahují k aktivní spolupráci vrcholných představitelů byznysu a IT, které umožňují zabezpečit dosažení souladu mezi byznysem a IT. Součástí by mělo být vytvoření prostředí umožňující sdílení a výměnu potřebných znalostí a informací souvisejících s byznysem a IT (Schlosser, a další, 2011). Výstupem IT governance by měl podle Novotny (2012) být soulad mezi byznysem a IT a dodání očekávané hodnoty byznysu prostřednictvím využívání podnikového IT. Soulad mezi byznysem a IT podle Gála (2015) znamená dosažení strategických byznys cílů prostřednictvím efektivní podpory informačních technologií. Soulad byznysu a IT by měl pokrývat soulad byznys strategie s IT strategií a soulad organizační infrastruktury a byznys procesů a organizačních zdrojů, které mohou přispívat k tvorbě hodnoty, s IT infrastrukturou, IT procesy a IT zdroji (Henderson, a další, 1993). IT governance

prostřednictvím politik, procesů a struktur umožňuje interakci vedoucích zástupců byznysu a IT, což podporuje soulad mezi byznysem a IT a vede k tvorbě byznys hodnoty z IT (Van Grembergen, a další, 2012).

Definice IT governance a její vymezení se v praxi i ve vědecké komunitě často překrývá s definicí IT managementu. V současnosti existuje celá řada definic IT governance, neboť IT governance je stále jednou z centrálních oblastí výzkumu, a to zejména z následujících důvodů (Mangalaraj, a další, 2014):

- výkonnost IT prostřednictvím podpory byznys procesů významně ovlivňuje výkonnost byznysu,
- existence hrozeb a rizik souvisejících s využitím IT, které negativně ovlivňují kontinuitu podnikání a mohou způsobit vysoké náklady či ukončení činnosti organizace,
- náklady na budování a provoz podnikového IT představují významný podíl na celkových nákladech organizace,
- potřeba plnění regulativních a legislativních požadavků.

Některé z vybraných definic IT governance jsou shrnuty v Tabulce 2.

Tabulka 2: Identifikované definice pojmu IT governance, zdroj: (autor)

Autor	Definice IT governance
(Erl, a další, 2011)	IT governance poskytuje pokyny, návody, organizaci a směr pro rozvoj IT aktiv a IT zdrojů.
(Mangalaraj, a další, 2014)	IT governance je odvozena od základních cílů podnikové governance a je postaveno na sladění IT strategie s celopodnikovou strategií. Na IT governance může být nahlíženo jako na rámec pro audit a ujištění, na rámec pro zabezpečení rozhodovacího procesu vrcholového managementu v souvislosti s IT. IT governance je považována za specifickou oblast podnikové governance.
(Jamsa, 2012)	IT governance je podmnožinou podnikového governance a zahrnuje politiky, postupy a kontroly, které se vztahují k využívání podnikového IT, k řízení výkonnosti IT, návratnosti investic vložených do IT a snižování souvisejících rizik a snaží se zajistit, aby IT produkovalo očekávanou byznys hodnotu.
(Carstensen, a další, 2012)	IT governance zaručuje, že IT aktiva jsou spravována na odpovídající úrovni, monitorována a kontrolována ve vztahu k úrovni, v jaké ovlivňují dosažení mise nebo strategických cílů organizace. IT governance se typicky soustředí na soulad IT s byznysem v oblasti souladu politik, cílů a strategií s důrazem na vytvoření IT architektury, která bude realizovat konzistentní byznys hodnotu.
(Selig, 2015)	IT governance je soubor politik, praktik a procesů a kontrolních aktivit včetně souvisejících rozhodovacích práv. Stanovuje kontrolní mechanismy, soubor kompetencí a systémy pro řízení výkonnosti IT, rizik, investic a zdrojů. Zabezpečuje dodržování organizačních politik a regulatorních požadavků.
(Van Grembergen, 2004)	Snahou IT governance je umožnit organizaci plně využít potenciál podnikového IT pro podporu byznys procesů a dosažení podnikových cílů. IT governance se soustředí na výkonné fungování a transformaci IT s cílem uspokojit měnící se potřeby byznysu a dalších zainteresovaných stran.
(Dohnal, 2012)	IT governance se skládá z mechanizmu rozhodování o IT, procesů IT governance a manažerských rolí CIO při prosazování pravidel IT governance.
(ISO/IEC	IT governance neexistuje jako samostatná oblast, neboť IT je integrální součást organizace,

Autor	Definice IT governance
38500, 2015)	a tudíž musí být spravováno v rámci podnikové governance. IT governance musí být v souladu s politiky a pravidly organizace. IT governance je záležitostí vrcholového vedení IT (CIO).
(ISACA, 2012c)	IT governance zabezpečuje neustálé vyhodnocování obchodních podmínek a potřeb zainteresovaných stran, na jejichž základě stanovuje požadovanou úroveň byznys cílů, stanovuje způsob dosažení těchto cílů, určuje směr prostřednictvím stanovení priorit a rozhodování, a sleduje výkon a dodržování shody reálně dosažených cílů s plánovanými byznys cíli.
(The Cabinet Office, 2011)	IT governance zastřešuje propojení vazeb mezi IT a byznysem. Určuje směr a definuje pravidla a omezení, role a odpovědnosti, kontrolování shody a realizaci nápravných opatření v případě detekované neshody. Zajišťuje provádění politik a pravidel a zabezpečuje, že procesy jsou ve shodě s těmito politikami a pravidly. Politiky stanovují pravidla a omezení a definují způsob rozhodování a strukturu oprávnění.

Ačkoliv se definice v některých aspektech liší, tak IT governance lze primárně považovat za soubor politik, pravidel, omezení, procesů a odpovědností definovaných a prováděných vrcholovým managementem, které se soustředí zejména na zabezpečení strategického souladu mezi byznysem a IT, na efektivní využití podnikového IT při optimalizaci zdrojů a na minimalizaci nákladů a rizik tak, aby IT produkovalo očekávanou byznys hodnotu z investic do IT v souladu s potřebami zainteresovaných stran a legislativními a regulatorními požadavky. Byznys hodnota z využití a z investic do IT je v případě IT governance považována za úroveň naplnění byznys cílů a potřeb zainteresovaných stran prostřednictvím IT. Tvorba hodnoty z IT je považována za realizaci benefitů z využití IT při optimálních nákladech na IT zdroje a při optimalizaci rizik IT (ISACA, 2012c). Mezi hlavní úlohy IT governance se podle Selig (2015) řadí:

- zajištění souladu mezi byznysem a IT, zejména ve smyslu souladu strategií a cílů,
- efektivní podpora byznys cílů a zabezpečení potřeb zainteresovaných stran využitím IT, dodání byznys hodnoty z IT,
- vytvoření IT governance struktury, zajištění interakce vrcholových byznys manažerů s vrcholovými IT manažery,
- ustanovení rolí, odpovědností a definice rozhodovacích práv,
- komunikování politik a praktik IT governance,
- realizace nezávislých ujištění o souladu IT s legislativou, politikami a standardy,
- zajištění systému řízení IT služeb a potřebné infrastruktury,
- zajištění systému řízení nákladů, rozpočtů, investic a zdrojů,
- zajištění systému řízení rizik, bezpečnosti a shody,
- zajištění systému řízení lidí, schopností a znalostí,
- zajištění systému pro řízení vztahu s poskytovateli a dodavateli,
- zajištění systému řízení výkonnosti IT a zabezpečení kontrolních mechanismů.

Jelikož je IT governance považována za podmnožinu podnikového governance (ISO/IEC 38500, 2015), řada autorů se soustředí spíše na podnikovou governance informačních technologií (IT) než na samotnou IT governance. Protože informační technologie významně ovlivňují dosažení strategických cílů a jsou pro řadu společností kritickým vstupem, který je zohledňován při strategickém plánování, neměla by IT governance stát odděleně od podnikové governance, ale měla by být vytvořena harmonická governance struktura pokrývající celopodnikovou úroveň (Van Grembergen, a další, 2009). Tím by měl být eliminován vznik duplicitních governance struktur. Podniková governance IT

definuje struktury a odpovědnosti, politiky a procesy na úrovni organizace, které podporují soulad mezi byznysem a IT a umožnují, aby zástupci byznysu a IT vytvořili prostředí pro tvorbu hodnoty z IT (Van Grembergen, a další, 2009). Jedná se tedy o podnikovou governance, která zahrnuje IT governance, čímž podporuje efektivní a účinné využití IT za účelem zvýšení výkonnosti organizace při minimálních nákladech a spotřebě zdrojů a minimalizaci rizik. Podniková governance IT je v odpovědnosti výkonného managementu organizace a řízení provozu IT nejčastěji v podobě ředitele IT oddělení tzv. Chief Information Officer (CIO). Podniková governance IT zahrnuje aktivity související s využíváním informačních technologií jakožto podnikových aktiv včetně souvisejících rozhodovacích procesů s cílem nákladově efektivní tvorby byznys hodnoty z IT (Selig, 2015). Podniková governance IT je dle ISO 38500 postavena na 6 principech, které zahrnují (ISO/IEC 38500, 2015):

- *Odpovědnost* – Všichni zaměstnanci musí znát a rozumět přiděleným odpovědnostem. Musí si být vědomi kompetencí v rámci jejich pracovního zařazení a musí být zodpovědní za výstupy jimi realizovaných aktivit.
- *Strategie* – Při tvorbě byznys strategie by měly být brány v úvahu všechny funkční oblasti podniku včetně řízení a rozvoje IT. IT by mělo pružně podporovat potřeby byznysu v závislosti na změnách okolí, a tudíž musí být strategické plány IT plně provázané s byznys strategií.
- *Akvizice* – Investice do IT musí být spojeny s přínosem k novému nebo vylepšenému byznys řešení, který musí být neustále sledován a vyhodnocován. Pro řízení investic do IT je nutné vytvoření transparentního modelu včetně jasné definice odpovědností, pravomocí a kompetencí pro rozhodování o investicích do IT. Investiční portfolia by měla být vyvážená z hlediska jejich finančního a nefinančního přínosu k souvisejícím nákladům a rizikům v průběhu celého ekonomického životního cyklu IT.
- *Výkonnost* – Výkonnost IT je hodnocena z hlediska schopnosti dosáhnout požadované podpory byznys cílů. IT služby by měly být poskytovány na takové úrovni a v takové kvalitě, která je potřebná k uspokojení současných i budoucích potřeb byznysu.
- *Shoda* – Politiky a praktiky IT governance musí být v organizaci jasně definovány, implementovány a prosazovány ve shodě s legislativními, regulatorními a dalšími externími požadavky. Ty musí být pravidelně přezkoumávány a na jejich základě musí být politiky a praktiky správy v IT upravovány tak, aby vždy splňovaly tyto požadavky.
- *Lidské chování* – Lidé jsou jednou ze základních složek governance a jejich chování a jednání musí být respektováno při tvorbě IT politik, praktik a při definici odpovědností a v rámci rozhodovacího procesu. Lidé by měly být školení s cílem zajistit potřebnou podnikovou kulturu a chování a měli by být schopni porozumět a plně podporovat IT prostředí na všech potřebných úrovních.

2.2 IT management

Management ve smyslu řízení definuje Veber (Veber, a další, 2011) jako "*souhrn všech činností, které je třeba udělat, aby byl zabezpečen chod organizace*". V prostředí řízení se lze často setkat s anglickým termínem control, který vyjadřuje nižší stupeň řídících činností a užívá se v souvislosti v oblasti výrobních a technických systémů (Gála, a další, 2015). Management (řízení) je všeobecně soubor aktivit, doporučení, praktik, přístupů a metod, které jsou využívány k zabezpečení specifických činností za účelem dosažení cílů organizace s ohledem na regulativní a podnikové normy. Management by měl zabezpečit koordinaci a integraci činností probíhajících v organizaci tak, aby byly realizovány efektivně a účinně (Robbins, a další, 2012). To znamená, že by měly být realizovány

pouze takové činnosti, které napomáhají dosažení cílů organizace, a výstup jednotlivých činností by měl být vytvořen s daným rozsahem zdrojů při minimalizaci nákladů. Některé definice managementu zahrnují také výčet funkcí procesu řízení. Mezi klasické funkce procesu řízení patří (Veber, a další, 2011):

- *plánování*, tj. stanovení cílů řízení a činností zabezpečujících dosažení stanovených cílů včetně určení potřebných zdrojů,
- *rozhodování*, tj. plánování a koordinace průběhu činností a prostředků dosahování plánovaných cílů řízení,
- *organizování*, tj. uspořádání systému složeného z lidí, procesů a technologií s ohledem na dosažení cílů řízení,
- *vedení*, tj. ovlivňování a usměrňování lidí tak, aby byly splněny plánované cíle řízení,
- *kontrola*, tj. zhodnocení odchylek reality od plánovaných cílů řízení a určení, zda bylo dosaženo shody ve vývoji reality vzhledem k cílům řízení.

Existují různé oblasti managementu, které vymezují dílčí či specifické přístupy řízení lišící se zejména rozdílnými vstupy a výstupy, uplatňovanými metodami a procesy. Ačkoliv se jednotlivé oblasti managementu v různých prostředích liší, společnými rysy jsou podřízenost činností dosažení plánovaného cíle, určení výstupů a hodnot z daných činností, flexibilita činností, zabezpečení finančních, lidských a technologických zdrojů, řízení průběhu činností a respektování rizika.

S rozvojem informačních technologií se objevil přístup nazývaný IT management spojený s provozem a rozvojem podnikového IT. Cílem IT managementu je zabezpečit organizaci dostatečnou úroveň flexibility, výkonnosti a agility prostřednictvím podnikového IT (Svatá, 2011). Aby bylo zajištěno dosažení cílů IT managementu včetně tvorby požadované hodnoty pro zainteresované strany, měl by být IT management prováděn efektivně a účinně a v souladu s IT governance. IT managementem se rozumí procesy a činnosti spojené s určováním základní koncepce, IT strategie, s plánováním rozvojových úloh, s poskytováním IT služeb uživatelům, se zajišťováním potřebných finančních, personálních, technických a dalších zdrojů (Gála, a další, 2015). IT management obsahuje aktivity, které se soustředí na plánování, tvorbu, provozování a monitorování činností ve shodě s požadavky IT governance za účelem dosažení byznys cílů (ISACA, 2012c). IT management je realizován na třech úrovních – strategická, taktická a operativní (Svatá, 2007). Na každé úrovni jsou uplatňovány odlišné metody a jednotlivé IT management procesy mají různé vstupy a výstupy (Gála, a další, 2012). Na strategické úrovni jsou realizovány dlouhodobé záměry v horizontu několika let vycházející z byznys strategie a celkových byznys cílů. Taktická úroveň se detailně zabývá aktivitami sloužícími pro realizaci dlouhodobých strategických plánů, nejčastěji v horizontu jednoho až tří let. IT management na operativní úrovni realizuje aktivity na každodenní bázi v souladu s taktickými plány a změnami okolního prostředí.

IT management se soustředí primárně na řízení IT operací a pokrývá následující oblasti (ISACA, 2012b; Selig, 2015; Voříšek, a další, 2012):

- *IT strategie a IT cíle* – IT strategie a IT cíle by měly podporovat byznys strategii a zabezpečit dosažení byznys cílů. IT strategie poskytuje směr pro rozvoj a řízení podnikového IT v souladu s potřebami zainteresovaných stran a umožňuje prioritizovat IT programy a projekty a investice do IT.
- *Řízení sourcingu IT* – Řízení sourcingu IT řeší způsob dodání a provozování IT, kdy se může jednat o dodání IT vlastními nebo cizími silami nebo dodání a provozování IT na bázi on-premise či on-demand řešení. Zajištění IT zdrojů nutných pro obnovu a rozvoj IT musí vycházet z IT strategie.

- *Realizace IT operací* – IT operace jsou realizovány IT procesy, kterými jsou například změnové řízení, řízení úrovně služby, řízení dostupnosti, řízení kapacit, řízení incidentů, řízení konfigurací, atd. Význam kvality IT procesů roste zejména s významem byznys procesu, který IT proces prostřednictvím IT služby podporuje, s nárokem na kvalitu IT služby, s počtem uživatelů IT služby a s rozsahem IT zdrojů, které jsou potřeba pro zajištění IT procesu (Voříšek, a další, 2011).
- *Řízení výkonnosti a rizik IT* – Řízení, monitorování a hodnocení výkonnosti provozovaných IT procesů a IT služeb oproti jejich plánované výkonnosti a identifikování oblastí pro zlepšení ve významu příspěvku IT v dosahování byznys cílů (ISACA, 2012b). Řízení rizik vyplývajících z využití IT zahrnuje neustálou identifikaci rizik, jejich analýzu a vyhodnocení a přijetí opatření ke zmírnění rizik (Doucek, a další, 2008).
- *Řízení dodavatelů* – Jedná se zejména o výběr dodavatelů, řízení vztahů s dodavateli, řízení smluv, hodnocení dodavatelů, monitorování výkonnosti dodavatelů a prověřování dodržování souladu s byznys a regulatorními požadavky.
- *Řízení lidských zdrojů* – Pro zabezpečení výkonnosti IT je kritické vytvoření optimálních IT řídících struktur, definování rolí a odpovědností, ustanovení rozhodovacího procesu, rozvoj a motivování lidských zdrojů a řízení znalostí.
- *Řízení rozpočtů a nákladů* – Aby IT přinášelo očekávané efekty při optimálních nákladech, je nutné řídit finanční plánování IT, tvorbu rozpočtů a sledovat a analyzovat náklady související s využitím IT.
- *Řízení IT služeb* – Řízením IT služeb je myšlena jejich optimalizace z hlediska disponibility, struktury a kvality a musí být zajištěn soulad IT služeb s regulatorními požadavky. Funkcionalita IT služeb musí podporovat byznys procesy a být v souladu s potřebami podniku. Životní cyklus řízení IT služeb obecně obsahuje realizaci katalogu IT služeb, návrh, implementace, testování, produktivní provoz, monitorování a vyřazení IT služby.

Specifickou oblastí IT managementu je management IT služeb (IT service management). IT službou se podle Voříška (2010) rozumí „*koherentní aktivity a/nebo informace dodávané poskytovatelem IT služby příjemci služby. IT služba je vytvářena IT procesy, které při svém průběhu konzumují IT zdroje (hardware, software, data, lidé atd.). Služba se realizuje na základě dohodnutých obchodních a technických podmínek*“ (Voříšek, a další, 2010). IT služby představují rozhraní mezi byznysem a IT, které popisuje, jak jednotlivé IT služby podporují byznys procesy (Voříšek, a další, 2011). Na IT služby může být nahlíženo také jako na komunikační nástroj mezi byznysem a IT, kdy byznys uživatelé jsou odstíněni od implementačních detailů IT služeb a tyto specifikace jsou v kompetenci poskytovatele IT služby (Voříšek, a další, 2011). Podstatou managementu IT služeb je řízení životního cyklu IT služeb ve smyslu řízení kvality IT služeb s cílem podporovat dosažení potřeb podniku prostřednictvím řízení životního cyklu služeb a souvisejících IT schopností, kapacit a zdrojů podle specifických požadavků podniku (The Cabinet Office, 2011). Management IT služeb je realizován souborem procesů a procedur ovlivňovaných politikami IT governance, které zajišťují plánování, návrh, realizaci, testování, produktivní nasazení, monitorování a podporu provozu IT služeb, které budou v souladu s principy IT governance a servisními dohodami poskytovat funkcionalitu očekávanou pro podporu příslušného obchodního procesu a budou dostatečně spolehlivé a výkonné. Předpokladem efektivního managementu IT služeb je existence katalogu IT služeb, dohoda o úrovni IT služby a vhodná architektura IT služeb (Jelínek, a další, 2007). Na management IT služeb může být nahlíženo jak z pohledu poskytovatele IT služeb, tak i z pohledu spotřebitele IT služeb. Fáze řízení životního cyklu IT služby z pohledu poskytovatele IT služeb jsou podle Schneider (2015) totožné s fázemi životního cyklu IT služby dle ITIL:

- strategie služby (service strategy),
- návrh služby (service design),
- přechod služby do produktivního provozu (service transition),
- produktivní provoz služby (service organization),
- neustálé zlepšování služby (continual service improvement).

Naopak na fáze řízení životního cyklu IT služby z pohledu spotřebitele IT služeb pohlíží Schneider (2015) jako na jednotlivé dimenze management procesů definovaných v COBIT 5:

- soulad, plánování a organizování (APO - Align, Plan, Organise),
- vybudování, osvojení a implementace (BAI - Build, Acquire, Implement),
- dodávka, servis a podpora (DSS - Deliver, Service, Support),
- monitorování, hodnocení a posouzení (MEA - Monitor, Evaluate, Assess).

S růstem důležitosti řízení IT vznikaly návody, jak efektivně a účinně dosáhnout cíle řízení. Tyto návody, postavené nejčastěji na doporučeních založených na zkušenostech z praxe, obsahují řadu procesů, praktik a postupů a souhrnně se nazývají metodikami řízení IT (Svatá, 2011).

2.3 Cloud computing

Cloud computing se objevil jako nové paradigma, které mění tradiční pohled na způsob, jakým jsou informační technologie poskytovány, využívány a účtovány (Bounagui, a další, 2014). Služby cloud computingu jsou dynamicky škálovatelné IT služby dodávané poskytovatelem služeb cloud computingu přes internet spotřebitelům na základě poptávky spotřebitelů po těchto službách, a to nezávisle na použité výpočetní technice a na lokalizaci spotřebitele, kdy spotřebitel přistupuje ke službám cloud computingu a administruje tyto služby samoobslužně bez nutnosti přímé interakce s poskytovatelem služeb cloud computingu a je mu umožněno automaticky a dynamicky měnit využití služby cloud computingu dle aktuální potřeby (Liu, a další, 2016; Prasad, a další, 2015). Cloud computing poskytuje spotřebiteli standardizovaný a snadný přístup ke sdílenému hardware a software, což zjednodušuje získání moderních informačních technologií bez nutnosti vysokých investic do vlastní infrastruktury (Rajmohan, a další, 2014). Kapitálové a provozní náklady spojené s tradičním on-premise řešením jsou v mnoha případech příliš vysoké, nepředvídatelné a obtížně kontrolovatelné (Suicimezov, a další, 2014) a velký podíl fixních nákladů při dynamicky se měnícím se využití informačního systému zatěžuje podnik, a to i při plném nevyužití kapacit výpočetních zdrojů. Výpočetní prostředky jsou v prostředí cloud computingu spotřebiteli alokovány na základě dohody o úrovni služby cloud computingu uzavřené mezi poskytovatelem této služby a spotřebitelem (Gutierrez, a další, 2015) a spotřebitel platí pouze za objem skutečně využitých služeb. Služby cloud computingu tak lze považovat jako specifické IT služby poskytované v prostředí cloud computingu. Cloud computing se vyznačuje rysy jako je všudypřítomný přístup přes internet, škálovatelnost, elasticita, sdílení IT zdrojů, koncentrace dat v datových centrech poskytovatele a platební model pay-per-use (Liu, a další, 2016). Řada podniků se snaží o optimalizaci využití IT zdrojů. Prostředí cloud computingu je využití pouze aktuálně potřebného množství zdrojů spojeno s novým modelem financování pay-per-use, který se odvíjí od míry objemu využití služeb cloud computingu. Tento model umožňuje přechod z kapitálových nákladů (CAPEX) na provozní náklady (OPEX) závislé na míře využití obousměrně škálovatelných zdrojů. National Institute of Standards and Technology (NIST) definuje zásadní charakteristiky cloud computingu, modely služeb cloud computingu a modely nasazení (NIST, 2013). Definice NIST je všeobecně považována za de-facto standard a je přijímána organizacemi i různými autory celosvětově (Žamberský, 2013). Zásadní charakteristiky jsou

specificky unikátní pro cloud computing a umožňují jej odlišit od jiných technologických řešení. Zásadními charakteristikami jsou (NIST, 2013):

- samoobslužná a automatická administrace služeb cloud computingu na základě poptávky,
- všeobecný síťový přístup,
- sdílení zdrojů,
- rapidní elasticita, měřitelnost služeb cloud computingu.

IT zdroje jako jsou například datová úložiště, paměť atd. mohou být v prostředí cloud computingu virtuálně a dynamicky přiděleny spotřebiteli na základě individuální aktuální potřeby těchto zdrojů. Spotřebitelé administrují alokaci potřebných zdrojů služby cloud computingu samostatně bez přímé účasti poskytovatele. Spotřebitelé všeobecně nemají kontrolu nebo znalost týkající se lokalizace těchto zdrojů, avšak samoobslužná a automatická administrace umožňuje jednodušší a rychlejší přístup k potřebným zdrojům a díky škálovatelnosti služeb jak směrem nahoru, tak i směrem dolu, mohou spotřebitelé využívat pouze takové množství zdrojů, které skutečně potřebují a optimalizovat tak náklady na využití infrastrukturních zdrojů. Optimalizace nákladů je realizovaná prostřednictvím modelu pay-per-use a garantované míry dostupnosti, bezpečnosti a dalších parametrů služeb odsouhlasených v SLA.

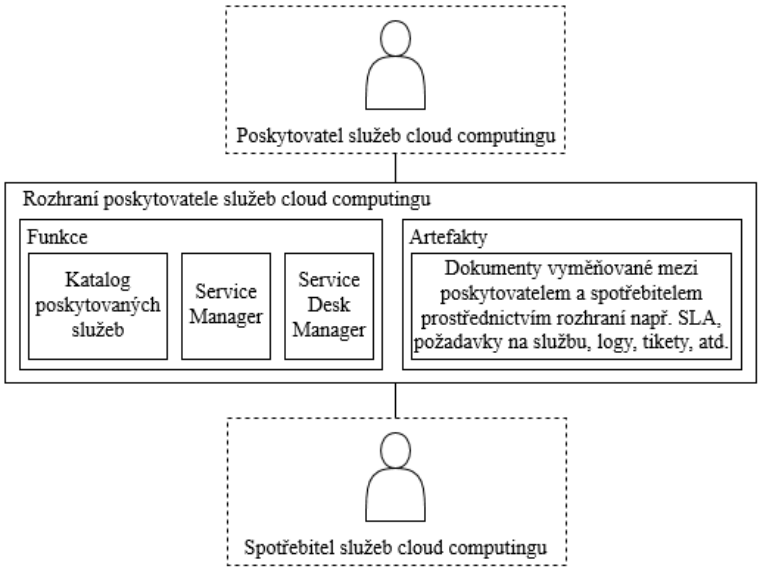
Modely služeb cloud computingu odráží vrstvy tradiční architektury budování informačních systémů přizpůsobené pro podmínky prostředí cloud computingu. Modely služeb cloud computingu jsou (NIST, 2013):

- *Infrastruktura jako služba (IaaS)* – IaaS zahrnuje služby, které poskytují infrastrukturní zdroje, jako výpočetní výkon, datové úložiště, sítě a další fundamentální výpočetní zdroje. Zákazník má možnost na těchto zdrojích nasadit a provozovat libovolný software, který může zahrnovat operační systémy a aplikace.
- *Platforma jako služba (PaaS)* – PaaS zahrnuje služby, které poskytují běhové prostředí pro podporu realizace a provozu aplikací napsaných v některém programovacím jazyce.
- *Software jako služba (SaaS)* – SaaS poskytuje aplikační služby pro koncové zákazníky, které běží na cloud infrastruktuře. Aplikace jsou přístupné prostřednictvím rozhraní, jako je například webový prohlížeč. Poskytovatel je zodpovědný za správu, upgrade a aktualizaci aplikací.

Modely nasazení poskytují pohled na způsob implementace služeb cloud computingu. V praxi jsou definovány čtyři modely nasazení, které jsou kvantifikované jako (NIST, 2013):

- *Veřejný cloud computing* – služby v modelu veřejného cloud computingu jsou poskytovány širokému počtu spotřebitelů. Poskytovatel je obvykle externí společnost, což znamená, že služby cloud computingu jsou dodávány prostřednictvím třetí strany.
- *Soukromý cloud computing* – v modelu soukromého cloud computingu jsou zdroje vlastněny a poskytovány pouze pro účely dané organizace nebo jejích dceřiných společností a autorizované obchodní partnery. Struktura a řízení služeb jsou pod kontrolou dané společnosti, díky čemuž mohou být služby plně přizpůsobeny byznys procesům organizace.
- *Komunitní cloud computing* – infrastruktura komunitního cloud computingu je sdílena mezi více organizacemi, které reprezentují specifickou komunitu obhajující podobné nebo stejné zájmy.
- *Hybridní cloud computing* – hybridní cloud computing vzniká spojením dvou a více modelů cloud computingu, které si zachovávají svoje vlastnosti, ale jsou propojené standardizovanou nebo proprietární technologií, která umožňuje datovou a aplikační přenositelnost. Jedná se zejména o kombinaci interně a externě poskytovaných a řízených služeb.

V modelu služeb veřejného cloud computingu jsou základními dvěma komponentami účastníci (spotřebitel služeb cloud computingu, poskytovatel služeb cloud computingu) a rozhraní poskytovatele pro přístup ke službě. Konceptuální model veřejného cloud computingu je znázorněn na Obrázku 4. Dle NIST (2013) je *„spotřebitel služeb cloud computingu jedinec nebo organizace, která získává a využívá služby cloud computingu, které jsou dodávané poskytovatelem služeb cloud computingu. Spotřebitel služeb cloud computingu službu vybírá z katalogu služeb poskytovatele, žádá příslušnou službu, vyjednává a podepisuje smlouvu o poskytování služby a o úrovni služby s poskytovatelem služeb cloud computingu a užívá danou službu a platí poskytovateli služeb cloud computingu v závislosti na objemu využití této služby. Poskytovatel služeb cloud computingu je jedinec nebo organizace zodpovědná za zabezpečení dostupnosti služeb pro spotřebitele služeb cloud computingu. Poskytovatel služeb cloud computingu vytváří služby cloud computingu, řídí technickou infrastrukturu potřebnou pro poskytování služeb, poskytuje služby dle dohodnuté úrovně služeb a chrání bezpečnost a soukromí služeb.“* Pro účely této doktorské disertační práce je často místo termínu „spotřebitel služeb cloud computingu“ používán termín „spotřebitel“, „spotřebitel služby“ anebo „spotřebitel služeb“.



Obrázek 4: Konceptuální model veřejného cloud computingu, zdroj: (DMTF, 2010)

Další pohled na prostředí cloud computingu definuje Cloud Security Alliance, která rozlišuje sedm vrstev v závislosti na tom, zda je vrstva kontrolována poskytovatelem nebo spotřebitelem služby cloud computingu. Jedná se o vrstvu fyzické infrastruktury, síťové infrastruktury, hardware, operační systémy, middleware, aplikace a uživatelské rozhraní a aplikace (Aceto, a další, 2012).

V kapitole 2.1 a 2.2. byly autorkou definovány pojmy IT governance a IT management, které představují základní teoretická východiska této doktorské disertační práce. Ačkoliv se výzkum na oblast IT governance a IT managementu soustředí již mnoho let, definice IT governance a IT managementu nejsou jednotné a liší se v závislosti na jednotlivých autorech. Navíc velké množství autorů explicitně nerozlišuje mezi oběma pojmy a do problematiky IT governance zařazuje také problematiku IT managementu. Z tohoto důvodu bylo nutné analyzovat a vymezit definici IT governance a IT managementu.

V kapitole 2.3. autorka této doktorské disertační práce vymezila definici pojmu cloud computing.

3 IT governance a IT management v prostředí cloud computingu

Cílem této kapitoly je analyzovat současný stav výzkumu v oblasti aplikace praktik IT governance a IT managementu do prostředí cloud computingu. Kapitola vymezuje přístupy světových a českých autorů ke cloud computing governance a cloud computing managementu získaných na základě rešerše odborné literatury provedené autorkou této doktorské disertační práce.

Rozhodnutí podniku, že bude využívat služby cloud computingu, kterými nahradí některé nebo všechny IT služby, má vždy vliv na s těmito službami spojené byznys procesy. Adopce služeb cloud computingu napomáhá zvýšit agilitu organizace tak, aby organizace byla schopna rychleji reagovat na změny vnějšího i vnitřního prostředí (Iyer, a další, 2010). Přestože důvody pro zavedení služeb cloud computingu jsou zřejmé a široce uznávané (Barde, 2013), má adopce služeb cloud computingu obvykle za následek vznik konfliktních situací uvnitř organizace. Dochází k narušení stávající podnikové kultury, kdy zaměstnanci společnosti ještě nejsou dostatečně vyškoleni v oblasti cloudových řešení. Dále může docházet ke konfliktům mezi byznys procesy podporovanými službami cloud computingu a stávajícími byznys procesy a ani organizační struktura ještě není schopná dostáhnout maximálních efektivnosti z využití služeb cloud computingu. Současně se zaváděním služeb cloud computingu nebo s přechodem na služby cloud computingu je potřeba systematicky vyhodnocovat připravenost podniku na adopci prostředí cloud computingu. Cílem je odstranění konfliktních oblastí a přesnější ohodnocení nákladů a rizik spojených s přechodem na služby cloud computingu. Zejména v případě, že služby cloud computingu jsou externí třetí stranou poskytovány v modelu veřejného cloud computingu přes internet, vyvstávají na důležitosti otázky týkající se soukromí a ochrany osobních údajů, bezpečnosti a důvěry v poskytovatele (Adjei, 2015). Přechod na služby cloud computingu se musí odrazit v potřebě doplnění stávajících procesů governance a managementu podnikového IT tak, aby byly schopny efektivně působit i v podmínkách prostředí cloud computingu (Saidah, a další, 2014). IT governance a IT management v prostředí využívání služeb cloud computingu musí být přizpůsobeny novým podmínkám tak, aby po přechodu na služby cloud computingu byla zajištěna kontinuita výkonnosti podnikání a bylo zabezpečeno dosahování cílů vycházejících z potřeb zainteresovaných stran. To se týká zejména potřeby reakce na zvýšené riziko v prostředí využívání služeb cloud computingu zahrnující otázky bezpečnosti, shody s platnou legislativou, ochrany soukromí a dále projektových a provozních činností (Brandis, a další, 2013). Dále je zapotřebí zajistit kontinuitu kritických obchodních procesů, jejichž data se v prostředí cloud computingu mohou rozšířit za hranice stávajícího datového centra. Je zapotřebí modifikovat procesy související se změnovým řízením, neboť flexibilita a škálovatelnost prostředí cloud computingu vyžaduje nové přístupy k této problematice. Cíle a zaměření IT governance a IT managementu uvedené v podkapitolách 2.1 a 2.2 se však nemění a jejich hlavním záměrem i v prostředí využívání služeb cloud computingu zůstává zvyšování efektivnosti podnikání, realizace benefitů prostřednictvím zvýšení automatizace a efektivní podpory byznys procesů, snižování nákladů a řízení rizik (Bounagui, a další, 2014). Tradiční přístupy IT governance a IT managementu rozšířené o specifika využívání služeb cloud computingu zmírňují potenciální rizika spojená s adopcí služeb a umožnují zajistit bezpečný a efektivní provoz služeb cloud computingu (Owuonda, a další, 2016). IT governance a IT management jsou v prostředí cloud computingu ovlivněny zejména následujícími skutečnostmi:

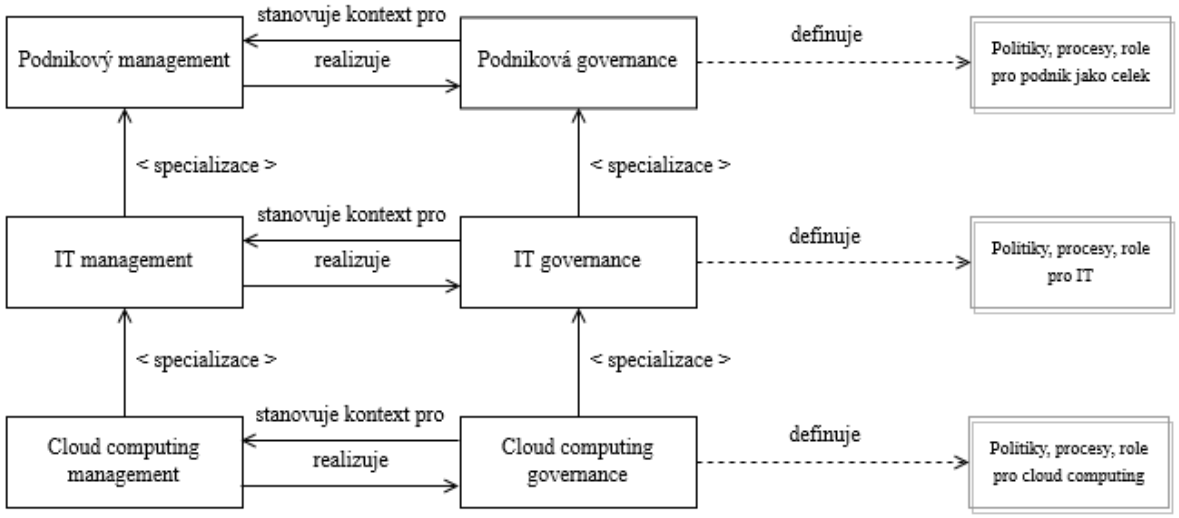
- *Oddělení spotřebitele od poskytovatele* – spotřebitel služby je oddělen od odpovědnosti za rizika spojená s poskytováním, údržbou a řízením cloudové infrastruktury a tyto odpovědnosti

jsou přesunuty na externího poskytovatele, který musí zajistit, aby infrastruktura splňovala nároky potřeb spotřebitele (Schneider, a další, 2015).

- *Měření služeb a benchmarking* – pro každou službu jsou definovány její cíle včetně parametrů umožňujících měření úrovně dosahování těchto cílů vůči jejich dohodnuté úrovni v dohodě o úrovni služeb (SLA) (Rehman, a další, 2012). Důležité je transparentní měření a vykazování dosažených výkonů služeb v reálném čase, ideálně pomocí technik integrovaných do stávajících systémů řízení poskytovatele i spotřebitele.
- *Operační transparentnost* – transparentní poskytování služeb umožňuje efektivně provádět diagnostiku provozu služeb včetně identifikace potencionálních dopadů vlivu nedostupnosti služeb na byznys procesy (Bond, 2015).
- *Exponování podnikových aktiv externímu prostředí* – podniková aktiva zejména ve smyslu podnikových dat by měla být kategorizována a hodnocena podle jejich kritičnosti a vhodnosti pro prostředí cloud computingu (Maghrabi, a další, 2015).
- *Síťový přístup k podnikovým aktivům* – k podnikovým aktivům ve smyslu dat je přistupováno prostřednictvím sítě, v prostředí veřejného cloud computingu se typicky jedná o Internet. Přístup ke službám vyžaduje v čase a v místě dostupnou síť s vysokou rychlostí vyhovující potřebám služby cloud computingu.
- *Shoda s legislativními požadavky* – v prostředí cloud computingu musí být zajištěna dostupnost metod, které zohledňují legislativní požadavky související s využíváním služeb cloud computingu jako je ochrana citlivých dat nebo geografické uložení dat.
- *Nové typy rizik a bezpečnostních výzev* – v prostředí cloud computingu dochází ke sdílení odpovědnosti za bezpečnostní rizika mezi poskytovatelem a spotřebitelem, který musí čelit novým typům rizik vyplývajících zejména ze skutečnosti, že je služba využívaná velkým množstvím spotřebitelů a jejich data jsou ukládána na stejné servery a z možné závislosti na poskytovateli. Dále s využíváním služeb cloud computingu souvisí celá řada legislativních a operativních rizik, která musí být řízena (Bounagui, a další, 2014).
- *Přechod z kapitálových nákladů na provozní náklady* – kapitálové náklady jsou považovány za investiční náklady na pořízení nových aktiv a na obnovu stávajících aktiv. Investice je typicky spojená s vyššími finančními požadavky a v dlouhodobém charakteru ovlivňuje hospodářské výsledky organizace a její prosperitu a je proto často realizována formou projektu. Kapitálové náklady jsou často označovány zkratkou CAPEX z anglického Capital Expenditure. V prostředí cloud computingu je kalkulováno s provozními nebo také operačními náklady, tzv. OPEX – Operating Expenditures. OPEX jsou variabilní neinvestiční náklady, které se odvíjí od výše spotřebovávané služby cloud computingu.
- *Těsnější smluvní vztah s poskytovateli* – v modelu veřejného cloud computingu jsou služby poskytovány velkému množství spotřebitelů externí třetí stranou vystupující v roli poskytovatele služeb cloud computingu, který je odpovědný za návrh, provoz a řízení jím poskytovaných služeb. Spotřebitel vytváří s poskytovatelem smluvní vztah na základě dohod o poskytování služby cloud computingu. Tyto dohody jsou základem k ustanovení, udržování a ukončení vztahu s poskytovatelem služeb cloud computingu prostřednictvím smluvních pravidel a podmínek a také nástrojem pro zajištění kvality služeb cloud computingu.

Rozšíření IT governance a IT managementu o specifika využívání služeb cloud computingu umožnuje získat hodnotu z adopce služeb cloud computingu prostřednictvím realizace přínosů z využití služeb cloud computingu definovaných a odsouhlasených před započetím migrace do prostředí cloud computingu, řízením rizik během využívání služeb cloud computingu a zabezpečením optimálního využití a řízení zdrojů, a to jak interních, tak i outsourcovaných od externích poskytovatelů (Hsu, 2012). IT governance a management je širší pojem než cloud computing governance a management.

IT governance a IT management se zabývají aspekty, které se týkají specificky oblastí informačních technologií a způsobu jakým informační technologie podporují cíle podniku. Činnostmi IT governance se zabývají zejména členové správní rady, řídícího výboru nebo výkonného managementu zastupující zájmy byznysu a IT (Bounagui, a další, 2014). Činnostmi IT managementu se zabývají zejména zástupci IT na vrcholové úrovni a IT personál. Definice cloud computing governance a cloud computing managementu nebyla doposud jasně identifikovaná. Cloud computing governance a management identifikuje s ohledem na využívání služeb cloud computingu změny v IT governance a managementu s cílem zajistit, že principy a služby cloud computingu budou spravovány a řízeny efektivním způsobem a že využitím vhodného souboru služeb cloud computingu bude zabezpečeno dosažení byznys cílů. Cloud computing governance a management lze považovat za specializaci IT governance a IT managementu (viz Obrázek 6), přičemž existuje jasné odlišení mezi cloud computing governance a cloud computing managementem (Copie, a další, 2013). Implementovaný model IT governance a IT managementu zjednodušuje vytvoření efektivního modelu pro cloud computing governance a management jakožto souboru politik, pravidel, omezení, procesů, struktur a odpovědností specializovaných pro prostředí cloud computingu. Ale i v případě chybějícího nebo neúplného modelu IT governance a IT managementu, by měl cloud computing governance a management poskytovat příležitost k odstranění nedostatků v oblasti IT governance a IT managementu a k vytvoření celkového modelu IT governance a IT managementu včetně governance a managementu specifických aspektů cloud computingu. Obrázek 5 znázorňuje vztah specializace cloud computing governance a cloud computing managementu v rámci hierarchické struktury governance a managementu a je z něj patrné jaké místo v organizačním systému governance a managementu zaujímá cloud computing governance a management.



Obrázek 5: Vztah specializace mezi podnikovou governance, IT governance a cloud computing governance, zdroj: (autor), podle: (Bounagui, a další, 2014; Ondruška, 2010)

3.1 Cloud computing governance

Neexistuje jednotně přijatá definice cloud computing governance a samotné pojetí významu cloud computing governance se neustále vyvíjí (Saidah, a další, 2014). Někteří autoři považují cloud computing governance za součást IT governance (Owuonda, a další, 2016), jiní na cloud computing governance pohlížejí jako na rozšíření tradičních principů IT governance o specifika vyplývající z využívání služeb cloud computingu (Brandis, a další, 2013). Stejně jako IT governance musí být i cloud computing governance v souladu s podnikovou governance. To znamená, že využití služeb cloud computingu musí podporovat IT cíle definované v IT strategii a jejich prostřednictvím musí

napomáhat k dosažení celopodnikových byznys cílů (Saidah, a další, 2014). Podle Gai (2012) se proces vytváření modelu governance v organizaci skládá z definování, tvorby a provádění politik. Na to navazuje Munteanu (2013), který shodně identifikuje hlavní úlohy cloud computing governance jako tvorbu, komunikování a prosazování politik (Munteanu, a další, 2013). Cloud computing governance je soubor procesů, odpovědností a praktik využívaných k vládnutí, správě a kontrole přijetí a provozování služeb cloud computingu v souladu s politikami, postupy a zásadami governance (Bounagui, a další, 2015). Cloud computing governance by měla napomáhat tvorbě byznys hodnoty nalezením optimální rovnováhy mezi dosažením benefitů z využití služeb cloud computingu, optimalizací finančních investic do využívání služeb cloud computingu a minimalizací rizik, které plynou z využití služeb cloud computingu (ISACA, 2014a; Saidah, a další, 2014). Toho je dosaženo správným nastavením governance procesů a neustálou kontrolou a realizací ujištění z hlediska prověřování shody governance procesů s politikami, legislativními a regulativními opatřeními (Saidah, a další, 2014). Efektivní cloud computing governance vede stejně jako IT governance ke zlepšení byznys agility, ke zvýšení výkonnosti podniku a ke zlepšení celkové konkurenceschopnosti podniku (Peiris, a další, 2010). Dle Suicimezova (2014) cloud computing governance souvisí stejně jako IT governance s rozhodovacím procesem. Cloud computing governance stanovuje pravidla a omezení, které ovlivňují rozhodování o službách cloud computingu, usnadňuje a zprůhledňuje komunikaci mezi poskytovatelem služeb cloud computingu a spotřebitelem. To zlepšuje kontrolu a dohled nad kvalitativními parametry služeb cloud computingu jako je výkonnost nebo bezpečnost, jejichž důležitost roste zejména v prostředí, kdy poskytovatelem je externí třetí strana (Linthicum, 2009). Stejně tak musí být zabezpečena neustálá analýza a hodnocení rizik, neboť riziko je v modelu veřejného cloud computingu značně vysoké a bez vhodných governance procesů může vést k poklesu flexibility byznys procesů a tím i k redukci celkové výkonnosti a agility organizace a k významným finančním ztrátám (Ritchey, 2009).

Existují dva pohledy na cloud computing governance. Jeden nahlíží na governance spotřebitele služeb cloud computingu a druhý na governance poskytovatele služeb cloud computingu. Poskytovatel by měl mít implementované takové IT governance zásady a praktiky, které zajistí, že jím nabízené služby cloud computingu fungují účinně a efektivně a dosahují potřebné úrovně zabezpečení a ochrany osobních údajů. Spotřebitel může od poskytovatele vyžadovat poskytnutí záruk týkající se opatření a postupů bezpečnosti informací a interních kontrolních mechanismů dle standardů jako je standard ISO/IEC 27001 pro systémy managementu bezpečnosti informací, standard ISAE 3402 zaměřený na organizace poskytující služby nebo dohoda Safe Harbour mezi EU a USA, která je v souladu se Směrnicí Evropského parlamentu a Rady 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Cloud computing governance z pohledu spotřebitele zabezpečuje governance využívání služeb cloud computingu v souladu s potřebami podniku, organizačními politikami a regulatorními požadavky tak, aby tyto služby napomohly realizovat očekávanou byznys hodnotu (Bounagui, a další, 2014). Byznys hodnota z využití služeb cloud computingu může být dosažena prostřednictvím redukce nákladů na pořízení, provoz a údržbu IT, převedením kapitálových nákladů na provozní výdaje s využitím modelu pay-as-you-go, snadnou využitelností a dostupností služeb, zkrácením doby implementace, automatizovaným způsobem poskytování a provozní efektivností spolehlivých a bezpečných služeb cloud computingu v souladu s regulatorními a legislativními požadavky (Odell, a další, 2015). Realizace očekávané byznys hodnoty je dosaženo prostřednictvím přímé podpory byznys procesů službami cloud computingu, čímž služby napomáhají dosažení byznys cílů (Prasad, a další, 2014). Realizace očekávané byznys hodnoty může být dosažena ve třech krocích, kterými jsou identifikace příležitostí pro podporu byznys procesu, transformace příležitostí do prostředí informačních technologií vhodných pro podporu byznys procesu a využití informačních technologií pro podporu byznys procesu vedoucí k tvorbě očekávané byznys

hodnoty (Smith, a další, 2003). Chou (2015) navrhuje model realizace očekávané byznys hodnoty z využití služeb cloud computingu, který se skládá ze čtyř kroků (Chou, 2015). Prvním krokem je uvědomění si potřeby, pochopení cloud computingu a nákladová analýza. V druhém kroku jsou objasněny základní determinanty byznys hodnoty a je provedena identifikace rizik, nutná úroveň bezpečnosti a ochrany dat a je řešena problematika uzavírání smluv a řízení vztahů s poskytovateli. Třetím krokem v modelu je plné porozumění všem charakteristikám cloud computingu včetně legislativních požadavků a musí být vytvořen systém pro monitorování provozu služeb a pro sdílení informací a znalostí. Jako metoda posouzení je realizován audit. Kombinací tří předchozích fází je dosažena poslední čtvrtá fáze realizace očekávané byznys hodnoty z využití služeb cloud computingu.

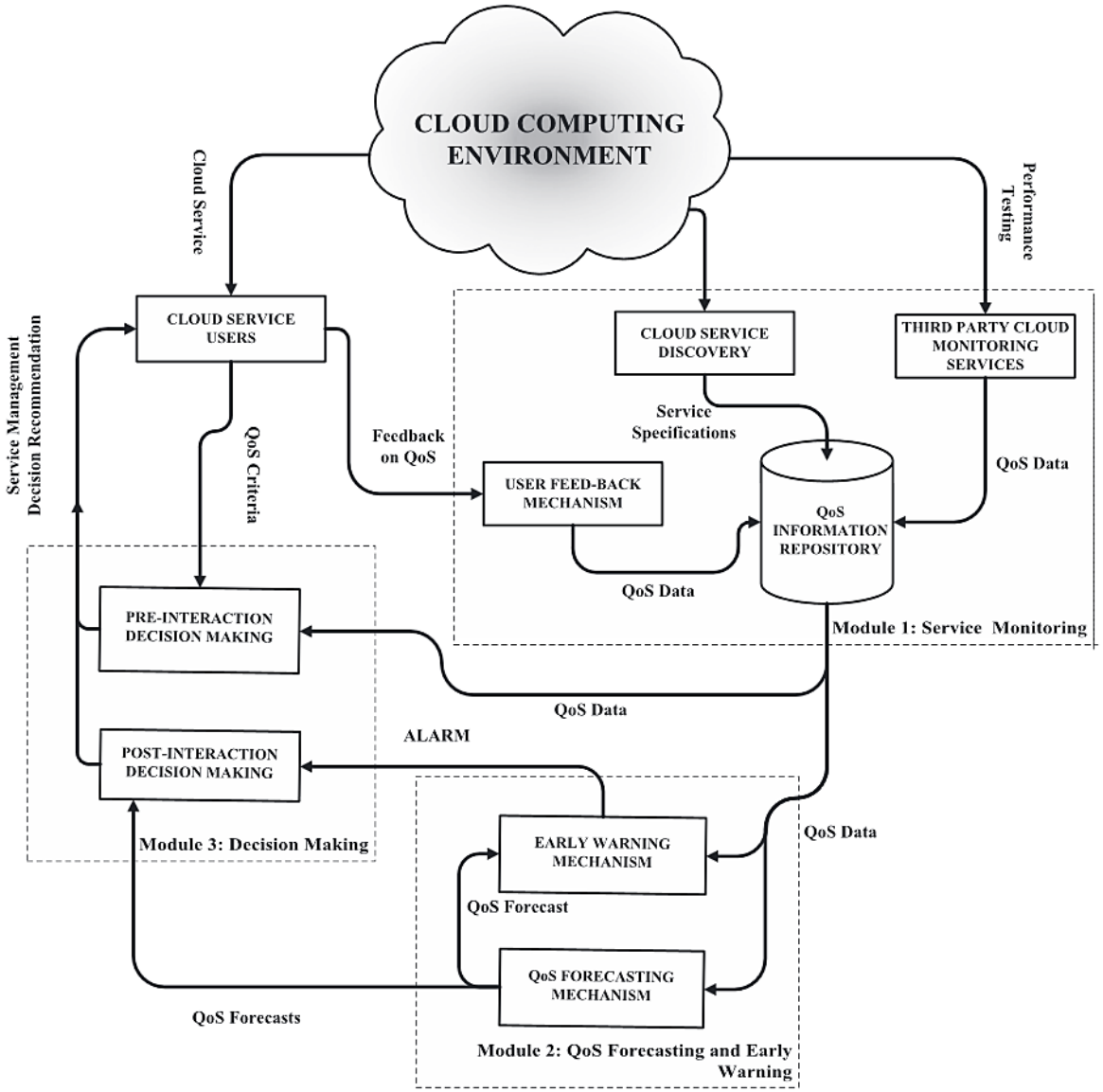
Cloud computing governance musí reflektovat také změny v oblasti lidských zdrojů, na které má využívání služeb cloud computingu významný vliv (Ross, a další, 2013). Využívání služeb cloud computingu by mělo být podpořeno změnou organizační struktury, musí být přijaty nové role a odpovědnosti stávajících rolí musí být rozšířeny tak, aby vyhovovaly novému prostředí s cílem zajistit efektivnější podporu pro governance a management služeb cloud computingu (Prasad, a další, 2014). Organizační struktura IT, která reflektuje specifika prostředí cloud computingu je flexibilnější a efektivnější při rozhodování, koordinování, ovlivňování a řízení využívání služeb cloud computingu a tyto služby tak mohou efektivněji přímo přispívat k dosažení byznys cílů. Prasad (2014) na základě průzkumu identifikuje hlavní součásti cloud computing governance organizační struktury jako Chief Cloud Officer, Cloud Management Committee, Cloud Service Facilitation pro řízení provozu služeb cloud computingu a Cloud Relationship Centre pro řízení vztahů s poskytovateli a vztahů mezi IT oddělením a byznys jednotkami (Prasad, a další, 2014). Chief Cloud Officer zodpovídá za plánování, rozhodování, schvalování a koordinaci činností v souvislosti s adopcí a využíváním služeb cloud computingu v souladu s byznys strategií. Zaměřuje se jak na technickou oblast využívání služeb cloud computingu, tak na jejich finanční řízení a na řízení informačních aktiv. Cloud Management Committee je řídící výbor, který realizuje společné plánování a rozhodování o adopci služeb cloud computingu v souladu s potřebami podniku s cílem realizovat byznys hodnotu z finančních prostředků vložených do využití služeb cloud computingu. Aby i zaměstnanci fyzicky využívající služby cloud computingu mohli svoji činnost úspěšně provádět, musí být vyškoleni s důrazem na specifika prostředí cloud computingu, a to nejen z technologického hlediska, ale i důrazem na hledisko organizační. Tito zaměstnanci musí být dopodrobna seznámeni s tím, jak fungují organizačně procesy zavádění a změn služeb, jak fungují firemní nástroje pro podporu těchto procesů, jaké je postavení a jaké jsou úkoly jejich oddělení a stejně tak musí být seznámeni s postavením a úkoly všech ostatních pracovišť, a to nejen IT. Dále musí zaměstnanci znát principy a procesy používané v oblasti cloud computing governance a managementu a musí plně rozumět důvodům, proč jsou tyto procesy v podniku zavedeny.

3.2 Cloud computing management

Stejně jako v případě cloud computing governance, ani v případě cloud computing managementu neexistuje jednomyslný konsenzus při stanovení jeho definice. Podle Amanatullah (2013) je cloud computing management soubor procesů, aktivit a metod, které zabezpečují nezbytné funkce pro řízení a provozování služeb cloud computingu (Amanatullah, a další, 2013). S tím souhlasí i Rehman (2015), který cloud computing management definuje taktéž jako proces, který napomáhá spotřebiteli služeb cloud computingu řídit výkonnost služeb cloud computingu, a to ve fázi rozhodování o výběru služby, kdy jsou identifikovány kvalitativní požadavky byznysu na službu, dále ve fázi výběru služby tak, aby služba byla schopná naplnit požadavky a potřeby byznysu a ve fázi provozu a využívání služby, kdy služba je řízena tak, aby dosahovala požadovaných výstupů. Podstata cloud computing managementu

z pohledu spotřebitele spočívá v řízení výběru optimální služby vzhledem k byznys požadavkům, sledování výkonnosti služby a posouzení, zda je služba poskytovaná v rámci kvalitativních úrovní hodnot parametrů služby smluvně odsouhlasenými mezi poskytovatelem a spotřebitelem služby cloud computingu a zda i během svého provozu služba splňuje požadavky byznysu (Rehman, a další, 2015). Jelikož spotřebitelé nemají přístup k virtuálním zdrojům a nedisponují kontrolou nad základní cloudovou infrastrukturou, nemohou ovlivňovat řízení skutečných hardwarových a softwarových prostředků zajišťujících provoz služby. Cloud computing management z pohledu spotřebitele se tak omezuje pouze na strategická rozhodnutí výběru služby cloud computingu, řízení využívání této služby a na hodnocení její výkonnosti vzhledem k byznys požadavkům a smluvním podmínkám.

Rehman (2015) navrhuje rámec pro cloud computing management z pohledu spotřebitele, jehož struktura včetně toku informací mezi jednotlivými komponentami je znázorněna na Obrázku 6.



Obrázek 6: Cloud computing management z pohledu spotřebitele, zdroj: (Rehman, a další, 2015)

Tento rámec se skládá ze tří hlavních modulů – rozhodování, monitorování, predikce a včasné varování. První modul zabezpečuje monitorování kvalitativních výkonnostních charakteristik služeb a obsahuje úložiště uchovávající informace o službách cloud computingu dostupných pro využití nebo budoucí potenciální využití spotřebitelem a evidující kvalitativní charakteristiky aktuálních

a historických monitorovaných dat z interních a externích monitorovacích systémů. Druhý modul zabezpečuje realizaci predikcí o vývoji kvalitativních charakteristik poskytované služby a generování včasných varování před hrozícím zhoršením hodnot parametrů kvalitativních charakteristik nebo před úplným selháním služby. Tyto prognózy stejně jako informace z prvního modulu využívá třetí modul, který zabezpečuje realizaci procesu rozhodování jako informační bázi při řízení služeb cloud computingu. Rozhodování se týká buď výběru nové služby cloud computingu nebo ukončení využívání stávající služby cloud computingu a migrace na potenciální dostupnou službu cloud computingu ze souboru identifikovaných služeb. Výběr služby je realizován s využitím informací z úložiště, kdy tyto informace jsou vyhodnocovány vzhledem k preferencím spotřebitele. Hodnocení využívané služby cloud computingu jak vzhledem k SLA, tak k byznys požadavkům na službu je taktéž postaveno na využití informací z úložiště a z analýz předpovědí o chování služby.

3.2.1 Životní cyklus služby cloud computingu

Schneider (2015) pohlíží na cloud computing management jako na řízení životního cyklu služby cloud computingu. Společné rysy služeb cloud computingu s tradičními IT službami a službami SOA a sdílení stejných zásad, které ve všech třech případech vychází z orientace na služby (Hui-min, a další, 2013) vedou k předpokladu, že životní cyklus těchto služeb bude podobný. Ačkoliv je řízení životního cyklu tradičních IT služeb předmětem mnohaletého výzkumu (Selčan, 2011; Susanti, a další, 2011; Voříšek, a další, 2010; Voříšek, a další, 2011), životní cyklus služeb v souvislosti s cloud computingem z perspektivy spotřebitele služeb cloud computingu není stále jasně definovaný (Schneider, a další, 2015). Tradiční životní cyklus IT služeb vychází z předpokladu, že IT služby jsou navržené, vyvinuté, poskytované a kontinuálně zlepšované ve stejné organizaci, která využívá tyto IT služby pro podporu byznys procesů (Feuerlicht, a další, 2015). Životní cyklus služby cloud computingu je ovlivněn skutečností, že služba cloud computingu je poskytovatelem poskytována velkému množství spotřebitelů. To způsobuje odlišení mezi životním cyklem služby cloud computingu z pohledu poskytovatele a z pohledu spotřebitele. Joshi (2011) definuje pět fází životního cyklu služby cloud computingu z pohledu spotřebitele, kterými jsou definice funkčních a technických požadavků na službu, nalezení požadované služby nabízené různými poskytovateli při očekávané úrovni nákladů a kvalitativních charakteristik služby, vyjednávání podmínek poskytování služby včetně smluvních podmínek, využívání služby a monitorování provozu a míry využití služby (Joshi, 2011). Schneider (2015) navrhuje taktéž pět fází životního cyklu služeb cloud computing z pohledu spotřebitele, kterými jsou stanovení požadavků, získání služby, integrace, plnění smluvních dohod a ukončení produktivního provozu služby cloud computingu (Schneider, a další, 2015). Fáze stanovení požadavků zahrnuje proces tvorby požadavků na poskytovatele a na službu cloud computingu a stanovení kritérií pro výběr poskytovatele a služby, specifikaci části systému, která bude migrována do prostředí cloud computingu a výběr vhodného modelu služeb a modelu nasazení. Fáze získávání zahrnuje hodnocení poskytovatele a služby cloud computingu, hodnocení příležitostí a rizik, porovnávání jednotlivých variant hodnocení, finanční hodnocení a vyjednávání smluv o poskytování služby cloud computingu. Fáze integrace zahrnuje konfiguraci služeb cloud computingu, jejich integraci do stávajícího IT prostředí spotřebitele a testování a implementaci do produktivního provozu. Fáze plnění smluvních dohod zahrnuje monitorování úrovně atributů služeb cloud computingu a hodnocení plnění smluvních požadavků, fakturování dle míry využití služeb cloud computingu a řízení vztahů s poskytovateli. Fáze ukončení produktivního provozu pokrývá aktivity realizované v případě ukončení využívání dané služby cloud computingu, v případě přechodu k jinému poskytovateli či v případě návratu k on-premise řešení. Obdobnou náplň životního cyklu služby cloud computingu definuje také Feuerlicht (2015),s jehož navržené fáze se liší zejména v použitém formalismu a výrazových prostředcích, avšak implementace životního cyklu je v podstatě totožná. Jednotlivé fáze jsou

prováděny sekvenčně počínaje specifikací požadavků, dále následuje identifikace služby, integrace služby, monitoring a optimalizace služby cloud computingu (Feuerlicht, a další, 2015). Na rozdíl od životního cyklu, který navrhl Joshi (2011), fáze vyjednávání není v ostatních modelech uvedena jako samostatná fáze, ale její obsah je začleněn do jiné stávající fáze (do fáze získání služby (Schneider, a další, 2015) nebo identifikace služby (Feuerlicht, a další, 2015)). A to z důvodu, že v modelu veřejného cloud computingu není poskytovatel schopen brát v úvahu individuální požadavky spotřebitelů na službu cloud computingu a všem spotřebitelům nabízí standardní smluvní podmínky. Pouze v určitých případech v závislosti na typu a objemu služby je spotřebiteli umožněno vyjednávat smluvní podmínky poskytování služby cloud computingu. Odlišné pojetí životního cyklu služby cloud computingu, které naopak integruje specifické fáze relevantní jak pro spotřebitele, tak i pro poskytovatele, navrhuje Fortis (2014). Fortis (2014) se domnívá, že životní cyklus služby cloud computingu by neměl být oddělený, neboť aktivity specifické pro spotřebitele a poskytovatele se mohou v jednotlivých fázích navzájem ovlivňovat. Integrovaný životní cyklus služby cloud computingu začíná inicializací životního cyklu a dále se sestává z kroků, které zajišťují definici služby, nabízení služby poskytovatelem, uzavření smluvního vztahu mezi poskytovatelem a spotřebitelem, nasazení služby u spotřebitele a její uvedení do produktivního provozu, produktivní provoz služby, údržba a řízení provozu služby, verzování, aktualizace, ukončení provozu služby, ukončení poskytování služby, ukončení smluvního vztahu, dealokace výpočetních zdrojů, archivace dat a ukončení životního cyklu služby (Fortis, a další, 2014).

ETSI (2016) shrnuje komplexně fáze životního cyklu do tří základních kroků, kterými jsou adopce služby cloud computingu, provoz služby cloud computingu a ukončení využívání služby cloud computingu. Každá z těchto fází je rozdělena do jednotlivých dílčích oblastí. ETSI (2016) provedla analýzu stávajících standardů a norem aplikovatelných specificky nebo po přizpůsobení do prostředí cloud computingu, které byly dostupné mezi lety 2013 a 2016 a to jak z hlediska spotřebitele služeb cloud computingu, tak i z hlediska poskytovatele, a navíc i z hlediska státních institucí, které vystupují jako regulátoři prostředí cloud computingu. Mezi oblasti fáze adopce služby cloud computingu, které nejsou pokryty žádným standardem ani normou patří (ETSI, 2016):

- specifikace požadavků na službu cloud computingu,
- vyjednávání s více poskytovateli různých služeb cloud computingu,
- integrace služeb cloud computingu se stávajícími systémy,
- strategie,
- hodnocení rizik.

Mezi oblasti fáze provoz služby cloud computingu, které nejsou pokryty žádným standardem ani normou patří (ETSI, 2016):

- reakce na porušení SLA,
- preventivní reakce na porušení SLA,
- řešení sporů týkajících se porušení SLA,
- správa uživatelů, identit a oprávnění,
- monitorování dostupnosti služby cloud computingu,
- monitorování incidentů,
- monitorování výkonnostních parametrů služby cloud computingu.

Mezi oblasti fáze ukončení využívání služby cloud computingu, které nejsou pokryty žádným standardem ani normou patří (ETSI, 2016):

- iniciace procesu ukončení využívání služby cloud computingu,
- tvorba reportu hodnotícího proces ukončení využívání služby cloud computingu,

- řešení sporů,
- uchovávání transakčních záznamů o ukončení využívání služby cloud computingu.

Důležitým nástrojem pro řízení životního cyklu služby cloud computingu je specializovaný registr služeb v podobě katalogu služeb cloud computingu (Fortis, a další, 2014). Katalog služeb cloud computingu by měl zejména obsahovat soubor deskriptorů obsahujících obecné informace o aktuálně využívaných službách, sémantickou definici služeb, soubor obsahující data o provozu instance služby včetně dat pro finanční účetnictví, soubor spravující informace o předem schválených službách, které jsou aktuálně dostupné na trhu služeb cloud computingu a odkaz na soubory uchovávající platné smlouvy o poskytování služby cloud computingu (Copie, a další, 2012). Typy a formáty smluv o poskytování služby cloud computingu se liší v závislosti na poskytovateli a mohou nabývat typicky podobu rámcové smlouvy o službě cloud computingu nebo dohody o službách cloud computingu obsahující zásady, podmínky, záruky a odpovědnosti vztahující se k využívání a ukončení využívání služeb cloud computingu, anebo dohody o úrovni služby cloud computingu (CSCC, 2015).

3.2.2 Finanční aspekty využívání služby cloud computingu

Rozhodování o využití služby cloud computingu podstatně ovlivňují zejména finanční aspekty využívání služby cloud computingu. Pro prostředí cloud computingu je charakteristické převedení kapitálových nákladů na IT (CAPEX) na variabilní provozní náklady na IT závislé na míře využití služby cloud computingu (OPEX), čímž dochází ke snížení rozsáhlých počátečních investic do IT. Poplatky za využití instance služby cloud computingu jsou ve srovnání s tradičními investicemi do IT jasně definovány. V případě tradičních investic do IT jsou celkové náklady na vlastnictví mnohdy velmi neprůhledné a jejich rozpad na jednotlivé nákladové jednotky je obtížný. Také realizace benefitů z využití služby cloud computingu může být dosaženo v kratším časovém horizontu oproti době návratnosti investice do IT, která může být realizována až po několika letech provozu IT. Kvantifikace benefitů z využití služby cloud computingu je postavena na stanovení změny přímo a nepřímo měřitelných finančních ukazatelů, které jsou ovlivněny využitím služby cloud computingu a náklady na tyto služby vynaloženými. Pro hodnocení přímých finančně vyjádřitelných benefitů je vhodné provést kvantifikaci fixních a variabilních nákladů a vyhodnotit návratnost vynaložených nákladů s využitím ukazatelů rentability vložených peněžních prostředků, a to zejména pomocí metody návratnosti investice a metody návratnosti investice do bezpečnosti (Lamberth, a další, 2010), které je nutné upravit tak, aby byly aplikovatelné i v prostředí cloud computingu. Pro hodnocení nepřímých finančně vyjádřitelných benefitů je nutné určit stínové hodnoty, které kvantifikují změnu finančních ukazatelů ve vztahu ke změně provozní flexibility, flexibility lidských zdrojů, efektivnosti byznys procesů a efektivnosti podnikového IT, které jsou vyvolané využíváním služby cloud computingu (Lamberth, a další, 2010). Posledním typem benefitů jsou nehmotné kvalitativní benefity z využití služeb cloud computingu, které je obtížné měřitelně kvantifikovat, ale které ovlivňují výkonnost, flexibilitu a prosperitu celého podniku (Lamberth, a další, 2010). Pro vyčíslení celkových nákladů vynaložených na využití služby cloud computingu je vhodné aplikovat metodu celkových nákladů na vlastnictví (Total Cost of Ownership – TCO). TCO lze vyjádřit jako součet všech veškerých nákladů souvisejících s výběrem, využíváním a ukončením využívání služby cloud computingu (Williams, 2012). Martens (2012) identifikoval typy nákladů v závislosti na životním cyklu služby cloud computingu. Jedná se zejména o přímo kvantifikovatelné náklady související se strategickým rozhodováním o využívání služby cloud computingu, výběrem služby, hodnocením a výběrem poskytovatele, účtováním za službu v závislosti na modelu služby, implementací, konfigurací, integrací, migrací, podporou, školením personálu, řešením změn a chyb vzniklých během provozu služby a ukončením využívání služby (Martens, a další, 2012). Lamberth (2010) porovnává náklady vznikající v prostředí cloud computingu s náklady na tradiční IT. Tyto náklady dělí na přímé

a nepřímé (Lamberth, a další, 2010). Přímé náklady jsou náklady vyplývající z provozu služby cloud computingu, z míry jejího využití a náklady na zabezpečení provozního prostředí. Nepřímé náklady jsou náklady vznikající z nevyužití nebo z nesprávného využití služeb cloud computingu a náklady vznikající z nedostupnosti služby cloud computingu. Dostupnost služby cloud computingu je významným aspektem pro efektivní realizaci byznys procesů. Pokud služba očekávaným způsobem podporuje realizaci kriticky důležitých byznys procesů, snížená dostupnost nebo úplná nedostupnost vede ke vzniku dodatečných nákladů, které mohou mít dopad na prosperitu celého podniku (Williams, 2012).

Využívání služeb cloud computingu je stejně jako jiná IT řešení spojené s nutností vynaložit peněžní prostředky související se strategickým rozhodováním o využití služby cloud computingu, výběrem vhodné služby a poskytovatele, přípravou prostředí na využívání služby, nasazením a operativním provozem služby, ukončením provozu služby a přechodem k jinému IT řešení. Ačkoliv toto vynaložení peněžních prostředků není v prostředí cloud computingu investicí v pravém slova smyslu, přesto jsou náklady na využití služby cloud computingu realizovány s cílem získání budoucích benefitů peněžního i nepeněžního charakteru prostřednictvím využívání služby cloud computingu. Kromě přímých provozních nákladů závislých na míře využití služby cloud computingu je nutné zohlednit také přidružené finanční investice do potřebných infrastrukturních zdrojů, organizační připravenosti a nákladů ušlé příležitosti (ISACA, 2012a). Proto i v prostředí cloud computingu lze po přizpůsobení aplikovat metody hodnocení investic jakými jsou metoda návratnosti investice ROI, metoda návratnosti investice do bezpečnosti ROSI, metoda čisté současné hodnoty NPV nebo metoda vnitřního výnosového procenta IRR (ENISA, 2012; ISACA, 2012a; Lamberth, a další, 2010; Tsalis, a další, 2013).

3.2.3 Řízení rizik v prostředí cloud computingu z pohledu spotřebitele

Přijetí služeb cloud computingu s sebou nese značný počet výhod vedoucích ke zvýšení byznys agility, ale i výzev a rizik, které mají významný dopad na úspěšnost dosahování cílů organizace (Stieninger, a další, 2014). Prostředí cloud computingu přináší do podnikových procesů nová rizika (Martens, a další, 2011), u nichž musí podnik provádět analýzy, zda příslušné riziko je vždy v akceptovatelných hranicích. Vystavení organizace novým typům rizik vede k podstatné změně rizikového profilu organizace (Prasad, a další, 2015). To vyžaduje komplexní zvážení portfolia podnikových procesů a identifikaci nejkritičtějších procesů a dat, technologií a lidí, kteří budou potenciálně ovlivněni využíváním služeb cloud computingu (Low, a další, 2011). Organizace využívající služby veřejného cloud computingu jsou vystaveny mnohem vyššímu bezpečnostnímu riziku určitých typů kybernetických útoků, neoprávněnému přístupu k datům (Haimes, a další, 2015) a řadě dalších organizačních, provozních (Bounagui, a další, 2014) a legislativních rizik (Martens, a další, 2011) než v případě tradičních on-premise řešení. Někteří autoři se domnívají, že ve specifických případech by riziko z využívání služeb cloud computingu mělo být transferováno na poskytovatele služeb cloud computingu nebo důvěryhodnou třetí stranu (Saripalli, a další, 2010; Tanimoto, a další, 2011). Na druhou stranu je však pro spotřebitele obtížné kontrolovat poskytovatele služeb cloud computingu z hlediska implementovaných bezepečnostních politik, praktik ochrany dat a bezpečnostních postupů pro přenášení, zpracování a uchovávání citlivých dat spotřebitele ve shodě s legislativními požadavky (ENISA, 2009). Proto je z pohledu spotřebitele služeb cloud computingu důležité zahrnout do procesu řízení rizik také aspekt poskytovatele služeb cloud computingu, neboť poskytovatel vlastní, provozuje a řídí cloud infrastrukturu a uchovává, zpracovává a v některých případech se stává i vlastníkem dat spotřebitele (Alosaimi, a další, 2016). Rizika spojená s využíváním služeb cloud computingu bez governance a management procesů mohou být značně vysoká a je potřeba je cíleně řídit, jinak by ve své podstatě mohly vést k poklesu flexibility byznys procesů a tím

ke snížení byznys agility (ISACA, 2014b). V průběhu několika posledních let vzniklo množství dokumentů zaměřujících se na analýzu a hodnocení rizik souvisejících s cloud computingem či kontrolní seznamy obsahující body, které mají být zváženy před migrací do prostředí cloud computingu (Vohradsky, 2012). Nejznámější je kontrolní seznam Cloud Controls Matrix v3.0.1 publikovaný společností Cloud Security Alliance (CSA) obsahující sadu kritérií, které spotřebiteli napomáhají při hodnocení bezpečnostních rizik během procesu výběru poskytovatele služeb cloud computingu (Cloud Security Alliance (CSA), 2016a). Dále Cloud Security Alliance (2016b) definuje dvanáct nejvážnějších bezpečnostních hrozeb cloud computingu, kterými jsou bezpečnostní incidenty, nedostatečné postupy řízení identit a řízení přístupu, krádež účtu, nedostatečně zabezpečená uživatelská rozhraní a aplikační programovací rozhraní API, zranitelnost informačních systémů, vnitřní útočník, útoky typu odepření služby, pokročilé techniky útoků (APT)[4], ztráta dat, nedostatečná due dilligence poskytovatele, zneužití a nekalé využívání služeb cloud computingu a zranitelnost vyplývající ze sdílené technologie (Cloud Security Alliance (CSA), 2016b). Doporučení pro aplikaci bezpečnostních kontrol z pohledu spotřebitele služeb cloud computingu dává také norma ISO/IEC 27017:2015 – Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací pro cloud služby založených na ISO/IEC 27002. Norma ISO/IEC 27017:2015 se zabývá konkrétními aspekty bezpečnosti informací v prostředí cloud computingu a to jak z pohledu poskytovatele, tak i z pohledu spotřebitele. Poskytuje soubor nejlepších praktik a doporučení pro realizaci bezpečnostních opatření specifických pro prostředí cloud computingu, tedy nad rámec těch, které jsou uvedeny v normách řady ISO/IEC 27000. Dalšími častými bezpečnostními hrozbami jsou smíšení dat, kdy více spotřebitelů sdílí využití stejné služby, nakládání s daty, nedostatečné zajištění integrity dat, nedostatečné postupy řízení bezpečnosti na straně poskytovatele služeb cloud computingu včetně zálohování a havarijní obnovy dat spotřebitele, závislost na proprietárním API poskytovatele (vendor lock-in) či nedostupnost dat a záznamů poskytovatele služeb cloud computingu pro třetí strany (Bounagui, a další, 2014). Vláda australského spolkového státu Queensland (2016) doporučuje zaměřit se zejména na problematiku spojenou se smlouvami o poskytování služeb cloud computingu, ochranou a bezpečností dat, fyzickým uložením dat a se zajištěním shody s legislativními a regulatorními požadavky (The State of Queensland, 2016). Fortinová (2013) identifikuje jako tři základní rizikové oblasti z pohledu spotřebitele jako nedostupnost dat, neoprávněný přístup k datům ve smyslu poškození, úprav či vyzrazení dat a diskontinuitu poskytování služby cloud computingu (Fortinová, 2013). Evropská agentura pro bezpečnost sítí a informací (ENISA) identifikuje nejdůležitější rizika specifická pro cloud computing, definuje 24 typů organizačních, technických a legislativních rizik souvisejících s cloud computingem a 11 typů rizik nespecifických pro cloud computing. Pro každé riziko uvádí pravděpodobnost výskytu rizika, míru dopadu na byznys, typy zranitelnosti, exponovaná aktiva a stanovení výše rizika ve stupnici nízké, střední, vysoké (ENISA, 2009). ENISA (2009) považuje za nejdůležitější rizika ztrátu governance, závislost na poskytovateli služeb cloud computingu, smíšení dat, nedodržování legislativy, regulatorních, smluvních a dalších předpisů, nedostatečně zabezpečené přístupové rozhraní, nedostatečnou ochrana dat, nesmazání dat spotřebitele po ukončení využívání služby cloud computingu poskytovatelem a výskyt škodlivého narušitele (ENISA, 2009). Dutta (2013) na základě posouzení literatury navrhuje ontologický model rizik cloud computingu, ve kterém navíc kromě organizační, technické a legislativní kategorie rizik, definuje kategorii provozních rizik, které mají vliv na každodenní byznys a IT operace (Dutta, a další, 2013). Provozní rizika zahrnují rizika vyplývající z netransparentních a špatně definovaných dohod o úrovni služby cloud computingu SLA, kdy poskytovatel není schopen poskytnout nasmlouvané

[4] Advanced Persistent Threat (APT) je souhrnné označení pro soubor pokročilých technik útoků zaměřených na konkrétní osobu nebo organizaci.

parametry služeb z technologických důvodů na straně poskytovatele vedoucích až k nedostupnosti služby, z finančních rizik jako jsou skryté náklady nebo špatně sestavený rozpočet provozních výdajů na služby cloud computingu, z obtížné přenositelnosti dat a z nedostatečně vyškoleného personálu z hlediska pochopení důvodů adopce služeb cloud computingu a z hlediska správného využití služeb cloud computingu při výkonu práce (Dutta, a další, 2013). Medhioub (2017) navrhuje model řízení rizik v prostředí cloud computingu, které se skládají z kontextové analýzy hrozeb, adaptivního nakládání s riziky a monitorování a přezkoumávání rizik. Kontextová analýza hrozeb má za cíl shromažďovat informace o prostředí cloud computingu v kontextu konkrétního byznys případu, odhad rizika a provedení rozhodnutí o tom, která bezpečnostní opatření a mechanismy jsou v daných souvislostech nejvhodnější. Adaptivní nakládání s riziky hledá kompromis mezi bezpečností a dopadem na výkonnostní charakteristiky služby cloud computingu. Monitorování a přezkoumávání spočívá v monitorování rizik a přezkoumávání přijatých opatření a rizikových scénářů. Informace získané z monitorování mohou umožnit lepší pochopení vznikající rizikové situace, čímž bude dosaženo rychlejší a pružnější reakce na měnící se rizikové prostředí s cílem zajistit efektivitu využívání služby cloud computingu. Proces řízení rizik v prostředí cloud computingu odráží tradiční fáze řízení rizik, avšak tyto fáze vyžadují detailní zvážení specifických aktiv, identifikaci zranitelnosti těchto aktiv a identifikaci nových typů rizik a hrozeb vyplývajících z využívání služeb cloud computingu a aktivity jednotlivých fází je nutné přizpůsobit dynamickému prostředí cloud computingu (Zhang, a další, 2010).

3.2.4 Legislativní aspekty využívání služeb cloud computingu

Pro využívání služeb cloud computingu je specifická migrace dat z interního prostředí organizace spotřebitele do externího prostředí poskytovatele služeb cloud computingu, který má typicky svá datová centra rozmístěná po celém světě a přesouvá data mezi jednotlivými datovými centry. Data jsou tak ovlivněna legislativou různých států v závislosti na jejich aktuálním fyzickém uložení a dle typu dat ve smyslu úrovně citlivosti a důvěrnosti dat. Spolu s tím vyvstává nutnost vyřešení požadavků na dostupnost metod zabezpečujících legislativní ochranu soukromí a zejména ochranu citlivých dat, jakými jsou osobní údaje, údaje z platebních médií, finanční reporty nebo respektování geografického uložení dat. Spotřebitel služeb cloud computingu musí dodržovat legislativní a regulatorní požadavky dané státem, ze kterého pochází. Spotřebitel služeb cloud computingu má povinnost zohlednit při výběru pouze takové poskytovatele služeb cloud computingu, kteří jsou schopni zaručit soulad jimi poskytovaných služeb s legislativou země původu spotřebitele (Pavlát, 2013). Spotřebitel je v tomto případě považován za správce osobních údajů, neboť definuje účel, prostředky a způsob zpracování osobních údajů a rozhoduje o výběru externího poskytovatele, který bude osobní údaje zpracovávat, přičemž poskytovatel vystupuje v roli zpracovatele osobních údajů pro správce (WP 196, 2012). Působí-li spotřebitel v některé ze zemí EU, přejímá odpovědnost za dodržování předpisů na ochranu osobních údajů včetně právních závazků stanovených ve Směrnici Evropského parlamentu a Rady 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (WP 196, 2012). Směrnice 95/46/ES stanovuje pravidla pro předávání osobních údajů ze členských zemí EU do třetích zemí. Tato směrnice ve článku 25 specifikuje, že je možné předávat osobní údaje z EU ke zpracování do třetích zemí, pouze pokud třetí země zajišťuje odpovídající úroveň ochrany osobních údajů a pokud to nevylučuje dodržování vnitrostátních předpisů přijatých na základě ostatních ustanovení této Směrnice. Odpovídající úroveň ochrany se odvíjí od povahy osobních údajů, účelu a doby trvání zpracování osobních údajů, zemi původu a zemi konečného určení, legislativě a regulativům třetí země. Na základě článku 25 odstavce 6 Směrnice Evropského parlamentu a Rady 95/46/ES přijala Komise Rozhodnutí 2000/520/ES o odpovídající ochraně poskytované podle zásad bezpečného přístavu a s tím souvisejících "často kladených otázek"

vydaných Ministerstvem obchodu Spojených států. Toto Rozhodnutí upravuje zásady předávání osobních údajů z EU do USA a jeho záměrem je zaručit bezproblémové a rychlé splnění podmínek vyžadovaných přísnější evropskou legislativou. V případě, že zpracovatel osobních údajů v USA oznámí Ministerstvu obchodu Spojených států, že se zavazuje dodržovat zásady bezpečného přístavu tzv. Safe Harbour, je Evropskou unií považován za organizaci zajišťující dostatečnou úroveň ochrany osobních údajů požadovanou Směrnicí Evropského parlamentu a Rady 95/46/ES. V posledních letech začaly být USA Evropskou unií vnímány spíše jako stát řadící se ke třetím zemím, které neposkytují adekvátní úroveň zabezpečení osobních údajů, a to z důvodu, že americké státní orgány mají pravomoc sledovat a získávat informace z datových center poskytovatelů služeb cloud computingu bez vědomí spotřebitele a evropských autorit ochrany osobních údajů. Tato skutečnost negativně ovlivnila důvěru EU ve způsob zpracování a ochrany osobních údajů v USA (Pavlát, 2015). Ve Sdělení Komise Evropskému parlamentu a Radě – Obnovení důvěry v toky údajů mezi EU a USA, COM(2013) 846 final a ve Sdělení Komise Evropskému parlamentu a Radě o fungování bezpečného přístavu z pohledu občanů EU a společností usazených v EU, COM(2013) 847 final Evropská komise uvedla, že zásady bezpečného přístavu je třeba přezkoumat vzhledem k rapidnímu nárůstu toku osobních údajů významných pro transatlantickou ekonomiku, k rychlému nárůstu organizací v USA, které přijaly zásady bezpečného přístavu, a k vyvstání nových informací o rozsahu některých amerických zpravodajských programů vedoucích k otázkám týkajících se toho, jakou míru úrovně ochrany může bezpečný přístav zaručit. Dále je zapotřebí posílit hmotněprávní zásady ochrany soukromí, transparentnost politik ochrany soukromí amerických autocertifikovaných společností, zlepšit dohled, monitorování a vymáhání zásad bezpečného přístavu americkými státními orgány a zajistit dostupnost finančně přijatelných mechanismů řešení sporů (Rozhodnutí 2016/1250, 2016). Na základě toho Evropská komise schválila Prováděcí rozhodnutí Komise (EU) 2016/1250 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající úrovni ochrany poskytované štítem EU-USA na ochranu soukromí pro předávání dat z EU do USA, dále uváděným pod názvem „štít EU-USA“, jehož cílem je zabezpečit lepší ochranu transferu osobních dat mezi EU a USA a zavést jasnější a vymahatelnější legislativní prostředí pro organizace, které se na toku dat podílejí (Pavlát, 2016). Štít EU-USA zavádí opatření na ochranu proti přístupu orgánů veřejné moci USA k osobním údajům a zjednodušuje možnosti nápravy, které mohou fyzické osoby využít v případě stížnosti (European Commission, 2016). Štít EU-USA reflektuje požadavky vyjádřené v rozhodnutí Soudního dvora ve věci C-362/14, Maximillian Schrems proti Data Protection Commissioner ze dne 6. října 2015, kterým byla prohlášena za neplatnou dohoda bezpečný přístav tzv. Safe Harbour (European Commission, 2016) a to zejména z důvodu, že ze zajištění odpovídající úrovně ochrany osobních údajů v USA nevyplývá rovnocenné zajištění ochrany osobních údajů zaručené v rámci EU Směrnicí 95/46/ES (Rozhodnutí 2016/1250, 2016). Štít EU-USA je postaven na následujících zásadách (European Commission, 2016):

- Ministerstvo obchodu Spojených států bude pravidelně aktualizovat seznam organizací, které se zavázaly dodržovat pravidla a zásady Štítu EU-USA a kontrolovat tyto organizace z hlediska pravidel a zásad Štítu EU-USA. V případě jejich nedodržení budou organizace postiženy odstraněním ze seznamu.
- Zpřísnění podmínek pro další předávání údajů třetím stranám, které zaručí, že stejná úroveň ochrany bude platit i pro osobní údaje, které organizace participující na Štítu EU-USA předá třetím stranám.
- Zpřesnit ochranná opatření spotřebitelů a povinnosti týkající se přístupu amerických státních orgánů k osobním údajům spotřebitele služeb cloud computingu za účelem vymáhání americké národní legislativy, zajištění americké národní bezpečnosti bude ve vztahu k osobním údajům probíhat v souladu s jasnými omezeními, ochrannými opatřeními

a mechanismy dohledu definovanými EU a jakákoliv osoba v EU bude mít oprávnění v této oblasti využít těchto nápravných mechanismů.

- Účinná ochrana práv fyzických osob EU a dostupnost finančně přístupných mechanismů v případě řešení sporů, možnost fyzických osob EU obrátit se na národní orgán pro ochranu osobních údajů, který ve spolupráci s americkou Federální obchodní komisí dohlédne na prošetření a řešení stížností, využití rozhodčího řízení při řešení sporů.
- Společný roční přezkum fungování Štítu EU-USA Evropskou komisí a Ministerstvem obchodu Spojených států za účasti národních zpravodajských odborníků z USA a z evropských orgánů pro ochranu osobních údajů.

Komplexní reforma Evropské komise týkající se pravidel ochrany osobních údajů s sebou kromě Štítu EU-USA přináší aktualizované právní akty evropské unie upravující ochranu osobních údajů v souladu s rozvojem moderních informačních technologií a s cílem poskytnout občanům EU řádnou kontrolou nad osobními údaji a zlepšit transparentnost legislativního prostředí. V Úředním věstníku EU bylo nově publikované Nařízení Evropského parlamentu a Rady 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), které vstoupilo v platnost v květnu 2016 a použije se od 25. května 2018 (Nařízení 2016/679, 2016). Hlavními cíli Nařízení 2016/679 je sjednotit dosavadní roztříštěnost v provádění ochrany osobních údajů v členských státech EU, která vznikla zejména z důvodu rozdílů v provádění a uplatňování Směrnice 95/46/ES a odstranění rozdílů v úrovni ochrany práv a svobod fyzických osob a zejména ochrany osobních údajů, které mají potenciál bránit volnému toku osobních údajů v rámci EU tak, aby tato úroveň byla ve všech státech EU rovnocenná (Nařízení 2016/679, 2016). Dalším nově publikovaným legislativním aktem v Úředním věstníku EU je Směrnice Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV, která vstoupila v platnost v květnu 2016 a členské státy EU ji musí implementovat do národních právních řádů do 6. května 2018 (Směrnice 2016/680, 2016). Směrnice 2016/680 se zaměřuje zejména na ochranu osobních údajů a volný pohyb osobních údajů v oblastech justiční spolupráce v trestních věcech a policejní spolupráce a stanovuje *„pravidla zpracování osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení“* (Směrnice 2016/680, 2016). Jsou-li osobní údaje zpracovány pro jiné účely, použije se nařízení o ochraně osobních údajů dle Směrnice 95/46/ES popř. od roku 2018 Nařízení Evropského parlamentu a Rady 2016/679.

V českém právním řádu je veřejnoprávní úprava zpracování a ochrany osobních údajů upravena zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (Pavlát, 2013). Podle § 6 zákona č. 101/2000 Sb. *„musí správce se zpracovatelem uzavřít smlouvu o zpracování osobních údajů. Smlouva musí mít písemnou formu. Musí v ní být zejména výslovně uvedeno, v jakém rozsahu, za jakým účelem a na jakou dobu se uzavírá a musí obsahovat záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů.“* Zákon č. 101/2000 Sb. upravuje práva a povinnosti při zpracování osobních údajů a předávání osobních údajů do jiných států. Předávání osobních údajů do zemí EU je upraveno v § 27 odst. 1 zákona č. 101/2000 Sb., který uvádí, že *„volný pohyb osobních údajů nemůže být omezován, pokud jsou údaje předány do členského státu Evropské unie.“* Předávání osobních údajů do třetích zemí mimo EU/EHP se řídí zákonem č. 101/2000 Sb. a pravidly na základě specifických právních instrumentů, jako jsou mezinárodní smlouvy anebo dodatečné zvláštní záruky ochrany osobních údajů ve formě standardních smluvních doložek mezi správcem a zpracovatelem nebo závazných podnikových pravidel (Pavlát, 2013). Standardní smluvní

doložky tvoří vzorový text smlouvy mezi správcem osobních údajů se sídlem v EU a zpracovatelem osobních údajů se sídlem ve třetí zemi, kdy správce přijímá odpovědnost za zajištění bezpečnosti předávaných osobních údajů (Rozhodnutí 2010/87, 2010). Pokud správce osobních údajů uzavře se zpracovatelem osobních údajů ve třetí zemi smlouvu o zpracování osobních údajů, jejíž součástí jsou standardní smluvní doložky v souladu s Rozhodnutím 2010/87, neuplatní se § 27 odst. 4 zákona č. 101/2000 Sb., tzn. správce není povinen požádat Úřad pro ochranu osobních údajů o povolení k předání osobních údajů zpracovateli a předání osobních údajů se řídí podle § 27 odst. 2 zákona č. 101/2000 Sb., tzn. osobní údaje jsou do třetích zemí předány na základě rozhodnutí orgánu Evropské unie (ÚOOÚ, 2013). Závazná podniková pravidla jsou určena zejména pro organizace, jejichž organizační složky jsou umístěné jak v zemích EU, tak i ve třetích zemích. Závazná podniková pravidla jsou tvořena schváleným souhrnem zásad zpracování a ochrany osobních údajů splňující požadavky evropské legislativní úpravy ochrany osobních údajů, který je právně závazný pro celou organizaci.

3.2.5 Výběr služby cloud computingu a poskytovatele služeb cloud computingu

Důvodem využívání služeb cloud computingu od různých poskytovatelů je to, že různé služby různým způsobem vyhovují specifickým byznys potřebám a požadavkům a zároveň klesá riziko závislosti na jednom poskytovateli (Heilig, a další, 2016). V řadě případů je však obtížné nalézt vhodnou kombinaci služeb, které by naplňovaly funkční a technologické požadavky, rozpočtová omezení a zároveň maximalizovaly očekávanou hodnotu z hlediska jejich nákladů, výkonnosti a úrovně kvality. Vzhledem k rapidně rostoucímu počtu poskytovatelů, kteří nabízejí různé služby na různé úrovni kvality za různé ceny s různými platebními modely, se výběr služby cloud computingu stává stále složitější (Rehman, a další, 2015). Různorodost nabídky služeb cloud computingu vede k potřebě zajistit soubor takových služeb cloud computingu poskytovaných takovými poskytovateli, kteří mohou uspokojit funkční a nefunkční požadavky byznysu na služby. Cloud Service Measurement Index Consortium (CSMIC, 2014) identifikovalo metriky pro hodnocení a porovnání služeb cloud computingu formulované do podoby Indexu měření služeb. Index měření služeb je hierarchicky uspořádaný model, který rozděluje metriky do sedmi kategorií, kterými jsou (CSMIC, 2014):

- odpovědnost poskytovatele služeb cloud computingu,
- agilita spotřebitele služeb cloud computingu,
- ujištění o požadované dostupnosti služby cloud computingu,
- finanční aspekty využívání služby cloud computingu,
- výkonnostní a funkční charakteristiky služby cloud computingu,
- bezpečnost a soukromí,
- snadnost použití služby cloud computingu.

Karim (2013) navrhuje výběr na základě kvalitativních charakteristik služeb, které dělí na výkonnostní charakteristiky, individuální charakteristiky spotřebitele a na charakteristiky vztahující se k elasticitě a kapacitě prostředí cloud computingu. Společnými charakteristikami navrhovaných modelů výběru služby cloud computingu jsou všeobecně požadavky na výkonnostní charakteristiky služby, technologické požadavky a rozpočtové omezení spotřebitele. Dále existují různé matematické multikriteriální a optimalizační modely a algoritmy, které optimalizují výběr vhodné služby cloud computingu, kdy míra vlivu každého jednotlivého parametru charakteristiky služby na proces výběru služby je dána jeho relativní vahou vzhledem k ostatním parametrům (Coutinho, a další, 2013; Heilig, a další, 2016). Mezi multikriteriální metody výběru se řadí zejména analytický hierarchický proces, analytický síťový proces, metoda nadřazování anebo teorie multiatributové využitelnosti (Sun, a další, 2014). Optimalizační modely aplikovatelné do prostředí cloud computingu jsou zejména dynamické

programování, celočíselné programování anebo hladový algoritmus (Sun, a další, 2014). Tyto modely a algoritmy jsou však náročné na znalosti a schopnosti zaměstnanců, kteří se podílejí na procesu hodnocení a výběru služby cloud computingu anebo kladou vysoké nároky na dostupnost vhodných softwarových nástrojů. Jiné modely se zabývají výběrem poskytovatelů služeb cloud computingu, a to zejména z hlediska hodnocení míry důvěryhodnosti poskytovatele a míry důvěry v poskytovatele (Adjei, 2015; Wu, 2015). Důvěryhodnost poskytovatele může být posílena například tak, že poskytovatel spotřebiteli předá určité informace týkající se implementovaných bezpečnostních mechanismů jako je například autentizace, verifikace anebo identifikace uživatele. Schopnost poskytovatelů služeb neustále udržovat a zlepšovat výkonnost služeb přispívá k budování důvěryhodných dlouhodobých obchodních vztahů mezi spotřebitelem a poskytovatelem. Proto by měly být při výběru služby vzaty v úvahu také aspekty týkající se potenciálních poskytovatelů služeb cloud computingu, jako jsou důvěryhodnost, finanční stabilita, právní předpisy, strategie dlouhodobého rozvoje atd. Poskytovatel by měl vytvořit prostředí, které poskytuje spotřebitelům jistotu, že bude schopen kontinuální dodávky služeb a jejich podpory, bude schopen zabezpečit ochranu dat a bude realizovat své aktivity v zájmu spotřebitelů (Adjei, 2015). Často řešeným aspektem při výběru optimálního poskytovatele služeb cloud computingu je tzv. vendor lock-in neboli závislost spotřebitele na proprietárních API poskytovatele, která omezuje interoperabilitu služby a portabilitu dat a tím ztěžují změnu poskytovatele, integraci mezi různými IT službami a interními systémy spotřebitele, zvyšují náklady s tím spojené a snižují agilitu organizace (Opara-Martins, a další, 2016). Vendor lock-in vede ke zranitelnosti spotřebitele vzhledem ke změnám realizovaných na straně poskytovatele služeb cloud computingu. Dalším způsobem, jak může poskytovatel zvýšit závislost spotřebitele na jím poskytovaných službách je licencování softwaru při odsouhlasení specifických podmínek a budování systému, který je vysoce nekompatibilní se systémy jiných poskytovatelů cloud či IT služeb (Opara-Martins, a další, 2014). Riziko závislosti na jediném poskytovateli služeb cloud computingu umožňuje snížit jasně definovaná exit strategie (Opara-Martins, a další, 2016).

Politika výběru a využívání služeb cloud computingu by neměla být stacionární, ale měla by být dynamickým procesem, v němž mohou být vybrané služby změněny v reálném čase podle nových požadavků byznysu na službu cloud computingu anebo na poskytovatele cloud computingu. Problémem udržování souboru optimálních služeb cloud computingu nabízených souborem optimálních poskytovatelů těchto služeb vzhledem k požadavkům byznysu je zejména chybějící jednotné prostředí sloužící jako tržiště pro obchodování se službami cloud computingu, chybějící systém pro automatickou identifikaci a vyhledávání optimálních služeb cloud computingu, nejednotná technická a obchodní definice služeb cloud computingu, obtížný přístup k informacím o kvalitativních charakteristikách služeb a získání zpětné vazby o poskytovateli od ostatních spotřebitelů (Sun, a další, 2014).

3.2.1 Metody zajištění důvěry v poskytovatele služeb cloud computingu

Rostoucí využití služeb cloud computingu vyžaduje potřebu realizovatelnosti auditu, to znamená mít k dispozici data pro provedení auditu pro prevenci a sledování podvodných činností, nesrovnalostí, mezer v kontrolách atd. (Bailey, a další, 2014). Poskytovatel služeb cloud computingu by tudíž měl provádět bezpečnostní logování aktivit spotřebitele v prostředí cloud computingu, které musí být dostupné spotřebiteli pro potřeby auditu. Zároveň musí být dostupná data a záznamy pro potřeby forenzního auditu. Data spotřebitele jsou obecně uložena na konkrétním serveru společně s daty jiných spotřebitelů a migrována mezi různými servery často velmi geograficky vzdálenými. Může tedy nastat situace, že pro konkrétní časový interval data pro audit nebudou k dispozici. Může se případně i stát, že místní úřad zabaví server za účelem soudního zajištění dat některého ze spotřebitelů i s daty všech ostatních spotřebitelů, kteří sdílí stejný server. Z tohoto důvodu je vhodné posoudit účinnost vnitřních

systémů a opatření poskytovatele, který by měl poskytovat potřebnou míru otevřenosti k průběžnému posouzení a hodnocení spotřebitelem, již před zahájením migrace během fáze vyjednávání smluvních podmínek. Jednou z forem ujištění pro spotřebitele, že poskytovatel plní zákonné požadavky a průmyslové standardy je certifikace (Bailey, a další, 2014). Certifikace poskytuje nezávislé ověření třetím důvěryhodným a akreditovaným subjektem (Svatá, 2011), tzv. certifikační autoritou a zvyšuje důvěryhodnost v poskytovatele služeb cloud computingu. Některé certifikační organizace se zaměřují specificky na region, například StarAudit, ENISA nebo EuroCloud Europe působí v Evropě, zatímco jiné certifikační organizace operují globálně, např. Cloud Security Alliance (Polash, a další, 2015). Cloud Security Alliance poskytuje dva programy certifikace poskytovatelům služeb cloud computingu v oblasti zajištění bezpečnosti provozu a poskytování služeb cloud computingu, které jsou schopny dokumentovat shodu s nejlepšími praktikami CSA. Těmito programy jsou CSA Star a certifikace Cloud Security Knowledge. CSA Star je program pro zajištění bezpečnosti v prostředí cloud computingu založený na seznamu kontrolních cílů podle Cloud Controls Matrix a na souboru otázek pro spotřebitele služeb cloud computingu, na které by se mohl ptát auditor poskytovatele služeb cloud computingu s cílem zjistit úroveň souladu poskytovatele s kontrolními cíli Cloud Controls Matrix a s CSA nejlepšími praktikami minimálního zajištění bezpečnosti (Cloud Security Alliance (CSA), 2016c). Některé organizace a zejména orgány veřejné správy při vyjednávání o využívání služeb cloud computingu vyžadují od poskytovatele specifické certifikáty, které indikují, že poskytovatel naplňuje specifické požadavky organizace. Příkladem může být požadavek Federální vlády USA směřovaný poskytovatelům služeb cloud computingu na certifikaci FedRAMP (Polash, a další, 2015).

3.2.2 Řízení úrovně služby cloud computingu a SLA

Služby v prostředí cloud computingu jsou poskytovány na různých úrovních kvalitativních parametrů. Správnou a úplnou specifikaci těchto parametrů včetně limitních hodnot metrik pro měření aktuální úrovně poskytované služby cloud computingu zajišťuje dohoda o úrovni služby (SLA). SLA je kontrakt uzavřený mezi poskytovatelem služby a spotřebitelem služby, který specifikuje zejména (Aljoumah, a další, 2015; Badidi, 2016; Šubrta, 2015):

- popis sjednané služby,
- strany uzavírající dohodu,
- kategorie uživatelů služby,
- platnost SLA,
- rozsah SLA,
- kvalitativní parametry úrovně služeb,
- konkrétní hodnoty metrik pro měření úrovně služeb ve vztahu k času (SLO),
- bezpečnostní pravidla a mechanismy,
- monitorování a reportování dat týkajících se dodávané služby,
- administrace služby,
- záruky týkající se kvality služby,
- omezení a další smluvní ustanovení,
- opatření pro případy porušení smluvních ustanovení a výši sankcí z nich vyplývající,
- cenu služby a platební metody,
- související smlouvy a práva.

Vzhledem k tomu, že pro každou využívanou službu cloud computingu je uzavřena separátní SLA, je nutné všechny aktivní SLA spravovat a řídit, a to vše při potenciálně měnících se požadavcích na kvalitativní parametry služeb. To je hlavní úlohou SLA managementu. SLA management pokrývá

kroky životního cyklu SLA zahrnující vytvoření návrhu SLA, vyjednávání podmínek uzavření SLA, uzavření SLA, poskytování služby, podpora a údržba služby, monitorování využití provozované služby z hlediska souladu s SLA, řešení problémů provozu služby a přijímání nápravných opatření při porušení SLA a ukončení využívání služby a uzavření SLA (Aljoumah, a další, 2015). K porušení SLA mohou vést zejména faktory vyplývající z nedodržení požadovaných kvalitativních parametrů služby, bezpečnostních standardů, legislativních požadavků, časové dostupnosti, špatně řízené infrastruktury, chybného odhadu při plánování škálovatelnosti služeb atd. Způsob výpočtu a výše sankcí by měla být definována v SLA. Sankce se může například odvíjet od doby, po kterou dohodnutá úroveň služby nebyla pro spotřebitele dostupná nebo od doby nutné pro nápravu nesouladu. Ne všechny kroky životního cyklu SLA se nutně aplikují při řízení SLA spotřebitelem. Problémem standardních SLA v prostředí veřejného cloud computingu je zejména nízký stupeň customizace SLA, tzn. s poskytovatelem není možné vyjednávat specifické podmínky poskytování služby cloud computingu a změny obchodních a technických podmínek poskytované služby závisí na poskytovateli služby (Comuzzi, a další, 2013). Možnost vyjednávání podmínek poskytování služby cloud computingu, a tedy vyšší stupeň customizovatelnosti SLA a tím i jasnější definování vztahu mezi poskytovatelem a spotřebitelem a vyšší stupeň transparentnosti poskytování služby je typický spíše u poskytovatelů, kteří nabízejí své služby velkým organizacím nebo v modelu privátního cloud computingu. Definice a struktura vysoce customizovatelných SLA se ve své podstatě blíží definici a struktuře SLA využívané při tradičním IT outsourcingu (Comuzzi, a další, 2013). Obsah SLA a zejména kvalitativní charakteristiky úrovně služby se v prostředí cloud computingu liší v závislosti na modelu nasazení (Aljoumah, a další, 2015). Zároveň je nutné rozlišovat mezi testovacím prostředím a produkčním prostředím, které vyžaduje přísnější hodnoty parametrů SLO.

SLA management je důležitým faktorem také při budování a udržování obchodních vztahů mezi spotřebitelem a poskytovateli služeb cloud computingu. SLA management napomáhá zajistit, že vztahy s poskytovateli budou stabilní a spolehlivé a že řízení těchto vztahů bude postavené na měřitelných ukazatelích vycházejících zejména z požadavků byznysu.

3.2.1 Řízení provozu služby cloud computingu

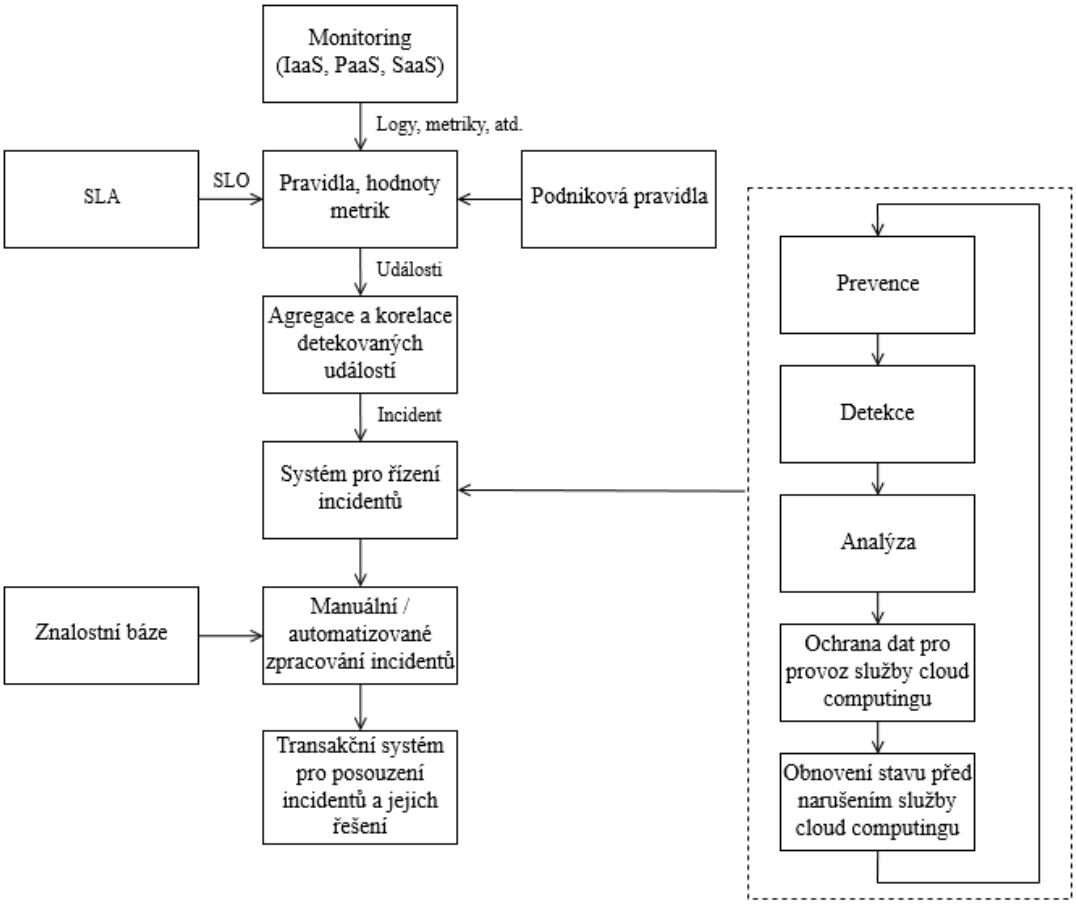
Služby cloud computingu vyžadují vyšší stupeň řízení jejich využití ve fázi jejich produktivního provozu v organizaci, neboť musí být koordinovány jak interní, tak i externí aspekty provozu služeb cloud computingu. Koordinace externích aspektů by navíc měla probíhat v součinnosti s poskytovatelem těchto služeb. Řízení provozu služeb cloud computingu by mělo poskytnout základní metodu řešení neočekávaných událostí v souvislosti s produktivním provozem a využíváním služeb cloud computingu. A to zejména prostřednictvím sledování, analýzy a vyhodnocování událostí, které mohou způsobit narušení provozu služby anebo porušení smluv o poskytování služby cloud computingu (Munteanu, a další, 2014). Řízení provozu služby cloud computingu je ovlivněno faktem, že kvantita a kvalita služeb cloud computingu je závislá na smluvních podmínkách sjednaných v SLA. V prostředí využívání služeb cloud computingu je důležitou aktivitou monitorování výkonnostních parametrů služeb cloud computingu a vyhodnocování jejich souladu s SLA (Aceto, a další, 2012). Spotřebitel by měl stanovit monitorovací metriky a realizovat monitorování v oblasti výkonnostních charakteristik služby a interakce mezi jednotlivými službami cloud computingu od různých poskytovatelů včetně hodnocení výkonnosti služby a efektivnosti jejího využití v organizaci a reportování odchylek od SLA, chyb a problémů spojených s provozem služby cloud computingu (CSCC, 2015). Specifikace monitorování a monitorovacích metod by měla být společným parametrem všech typů služeb cloud computingu (Aljoumah, a další, 2015). Parametry úrovně služby cloud computingu odsouhlasené v SLA jsou základem pro monitorování provozu služby. Odchylky skutečně naměřených hodnot těchto parametrů od hodnot parametrů definovaných v SLA mohou sloužit jako

spouštěcí událost pro rekonfiguraci parametrů poskytované služby (Venticinque, a další, 2010). Monitorování je významným prostředkem ujištění o přesnosti účtování míry využití služby cloud computingu nezávisle na různých způsobech účtování různých poskytovatelů. Monitorování dále umožňuje předvídat chování služby cloud computingu (Minor, a další, 2014), na jehož základě je možné zahájit proces zlepšování služby cloud computingu. Monitorování musí v prostředí cloud computingu shromáždit a analyzovat velké množství dat za určitý čas, přičemž by se v optimálním případě mělo jednat o automatizovaný proces s minimální manuální editací. Monitorování by mělo být spojené s procesem eskalace výskytu jakýchkoliv pro provoz netypických událostí a s analýzou monitorovacích dat (Ward, a další, 2015).

Pro prostředí využívání služeb cloud computingu je monitorování zásadním nástrojem pro identifikaci problémů vzniklých v souvislosti s provozem služby. Data nasbíraná během monitorování mohou sloužit pro analýzu prvotní příčiny problému, ale i jako podklad pro vyžadování plnění smluvních podmínek, účtování za využití služeb a pro ujištění o poskytování spolehlivých a efektivních služeb cloud computingu (Aceto, a další, 2012). Data získaná z monitoringu umožní odhalit chyby služeb a problémy při provozu a využívání služeb cloud computingu, odchylky parametrů poskytovaných služeb od parametrů definovaných v SLA a významné trendy provozu služeb (Ward, a další, 2015). Sledování trendů ve vývoji dat o provozu služby cloud computingu může navíc napomoct přecházet problémům před jejich vznikem. Předcházení problémům je méně nákladnější a účinnější než realizace nápravných opatření po výskytu problému (Cichonski, a další, 2012).

Jelikož definice parametrů služeb v SLA je realizována obvykle poskytovatelem a spotřebitel pouze vyjednává hodnoty těchto parametrů, může být pro spotřebitele obtížné navrhnout adekvátní monitorovací systém pro monitorování SLA (Emeakarohaa, a další, 2012). Důležité je stanovení vhodných metrik a učení monitorovacích intervalů s ohledem na možné porušování SLA a z toho plynoucích nákladů a dopadů na byznys procesy. Služby cloud computingu poskytované třetí stranou se během svého provozu mohou dynamicky měnit v závislosti na rozhodnutí poskytovatele, který je odpovědný za tvorbu a provoz jím poskytovaných služeb. Poskytovatel služeb cloud computingu může iniciovat změnu služeb, změnu charakteristik služeb, změnu platebních modelů anebo procedur a mechanismů řízení služeb. Zároveň ale musí zajistit dodání očekávané úrovně kvality služby cloud computingu spotřebiteli v souladu se smlouvami o poskytnutí služby cloud computingu, kdy její porušení ze strany poskytovatele je postihováno smluvními sankcemi. Vzhledem k vysoké dynamičnosti změn v prostředí cloud computingu, je nezbytné i ze strany spotřebitele implementovat procesy, procedury, mechanismy a nástroje pro zabezpečení automatizovaného monitorování a přezkoumávání požadovaného stavu, charakteristik a chování služeb cloud computingu. Tyto nástroje by měly být schopny monitorovat, jak menší počet metrik, tak i zároveň zahrnout všechny metriky, které ovlivňují úroveň kvality služby cloud computingu a naplnění byznys požadavků na tuto službu (Aceto, a další, 2012). Jelikož prostředí cloud computingu je velice dynamické, měly by se monitorovací systémy vyrovnat změnám monitorovaných služeb bez dodatečného zatížení systému. Může se jednat o změny v nákladech způsobené změnami potřebného výkonu služby, změnami objemu využitých infrastrukturních zdrojů anebo softwarové služby nebo změnami cen za využití služby ze strany poskytovatele, a dále o změny kvality služby, o změny konfigurace služby, o chybové stavy služby, o změny legislativních nebo regulatorních požadavků anebo neplnění požadavků na službu poskytovatelem (Copil, a další, 2015). Proto by se monitorovací systém v prostředí cloud computingu měl umět vyrovnat s velkými změnami objemu dat, s různými mírami zatížení výpočetních zdrojů a sítě, s měnícím se rozsahem monitorovacích entit, měl by automaticky reagovat na nepředvídatelné změny a zavčas upozorňovat na zjištěné odchylky od běžného stavu a měl by podporovat monitorování různých typů služeb cloud computingu od různých poskytovatelů a provádět sběr různých druhů monitorovacích dat (Aceto, a další, 2012). Prostředí služeb veřejného cloud

computingu je svým charakterem prostředí, které je mnohem více než tradiční IT prostředí díky své komplexnosti vystavené velkému množství útoků a různých forem incidentů. Řízení incidentů v prostředí cloud computingu se soustředí zejména na incidenty vedoucí k porušení SLA nebo narušení očekávaného využití služby cloud computingu (Munteanu, a další, 2014). Proces řízení incidentů analyzuje informace z dostupných logů a vytváří vhodné nápravné opatření pro co nejrychlejší znovuobnovení normálního stavu služby cloud computingu. Bohužel však řízení incidentů v prostředí cloud computingu není stále i přes nabídku specializovaných automatizovaných nástrojů poskytovateli služeb cloud computingu na dostatečné úrovni, což se odráží i v řadě problémů vyplývající z integrace služeb cloud computingu do prostředí organizace a z interakce s ostatními službami (Munteanu, a další, 2014). Základem každého procesu řízení incidentů je správná identifikace událostí, které způsobují incident, jejich spojování a nalezení vzájemného vztahu mezi těmito událostmi a určení míry jejich dopadu na byznys. Obtížným úkolem může být analýza těchto událostí zejména v prostředí, kdy jsou využívány služby cloud computingu od většího množství různých poskytovatelů. Nejčastějšími incidenty v prostředí cloud computingu jsou zejména incidenty související s výpadkem služby, útoky na zranitelná místa, selháním automatické aktualizace, ztrátou dat a hackerstvím jako jsou například DDoS útoky, flooding nebo cross-site scripting (Chang, a další, 2015). Bezpečnostní incidenty jsou proto zejména v prostředí cloud computingu velice diskutovaným tématem (Doelitzscher, a další, 2012). Bezpečnostní incidenty týkající se služeb cloud computingu se typicky vyskytují na straně poskytovatele, který by měl okamžitě zahájit proces řešení incidentů s cílem minimalizovat dopad incidentu, implementovat potřebné řešení a vrátit se do běžného stavu. Bohužel však velký počet poskytovatelů nedisponuje systémem, který by v reálném čase, informoval spotřebitele v případě útoku na infrastrukturu potřebnou pro provoz konkrétní služby. Zároveň často se měnící infrastruktura komplikuje definici toho, jak by měl vypadat běžný stav a je tudíž složitější odhalovat abnormální chování. Je tedy pouze na poskytovateli, aby zabezpečil kontinuitu služby cloud computingu, tím dodržel smluvní podmínky, které tuto problematiku typicky upravují, a nenarušil kontinuitu podnikání spotřebitelů. Detekce a eskalace incidentů v prostředí cloud computingu je významnou aktivitou zejména vzhledem k vlastnostem služeb veřejného cloud computingu. Spotřebitel často využívá pro podporu svých byznys procesů hybridní prostředí tvořené jak tradičními IT službami, tak službami cloud computingu. Z tohoto důvodu je důležité mít potřebný počet kontrolních bodů pro zjištění stavu monitorovaných entit. Tyto kontrolní body detekují v systému se vyskytující události, které mají potenciál narušit normální stav (Doelitzscher, a další, 2012). Systém pro detekci událostí a incidentů včetně definice monitorovacích entit by měl být navržen dostatečně flexibilně se schopností získávat monitorovaná data paralelně a nezávisle, aby při změně instance služby cloud computingu nebylo nutné provést rekonfiguraci celého systému. Takovýto systém u spotřebitele by měl monitorovat a sledovat jednotlivé služby cloud computingu a dynamicky načíst moduly umožňující použít rozhraní pro přístup k dalším monitorovacím nástrojům případně k monitorovacím nástrojům poskytovatele. Munteanu (2014) navrhuje architekturu monitorovacího systému pro prostředí cloud computingu včetně životního cyklu řízení incidentů, která je zobrazena na Obrázku 7.



Obrázek 7: Architektura systému monitorování v prostředí cloud computingu včetně životního cyklu řízení incidentů, zdroj: (Munteanu, a další, 2014)

Podle Cao (2011) by měl proces řízení incidentů v prostředí cloud computingu zahrnovat mechanismus predikce incidentu. Předpovídání neočekávané odchylky od normálního stavu by mělo vycházet z dostupných údajů shromážděných během monitorování provozu služby (Rehman, a další, 2015) a z analýzy rizik vyplývajících z využití této služby. Ve vysoce dynamickém prostředí, jakým je využívání služeb cloud computingu, je klíčovým prvkem pro zajištění kontinuální efektivnosti v případě nasazení nové služby či změny stávající služby automaticky konfigurovatelný systém pro monitorování a pro řízení incidentů nové anebo změněné služby (Gupta, a další, 2009). To vyžaduje zvážení aspektů týkajících se řízení problémů a incidentů v každé fázi životního cyklu služby cloud computingu. Monitorování závisí na modelu služby (IaaS, PaaS, SaaS), zamýšleném typu monitorovaných dat a účelu jejich využití a na zdroji monitorování, kdy se může jednat jak o fyzické zdroje, tak i o virtuální zdroje poskytované spotřebiteli s cílem dohlížet na plnění požadavků vyplývajících z SLA (Montes, a další, 2013). Fyzické zdroje jsou obvykle představovány datovými centry složenými ze souboru výpočetních klastrů a mohou být monitorovány s využitím tradičních monitorovacích technik určených pro distribuované systémy. V tomto případě je monitorování typicky realizováno poskytovatelem služeb cloud computingu. Pro monitorování virtuálních zdrojů je nutné využít pokročilé techniky monitorování. Monitorování virtuálních zdrojů, poskytovaných spotřebiteli ve formě infrastrukturní, platformní či aplikační služby je realizováno jak poskytovatelem, tak i spotřebitelem služby cloud computingu. Jasná specifikace sledovaných informací o virtuálních zdrojích je umožněna díky abstraktnímu popisu služby cloud computingu, který je formálně vyjádřen pomocí kvalitativních parametrů služeb ve smlouvách SLA zakládajících vztah mezi poskytovatelem a spotřebitelem služby cloud computingu. Takto získaná informace z monitoringu napomáhá spotřebiteli sledovat plnění smluvních podmínek a optimalizovat využití služby cloud computingu

z hlediska objemu spotřebovaných zdrojů, doby využití služby a nákladů na službu. V případě IaaS může spotřebitel monitorovat stav jemu přidělených instancí virtuálního stroje s cílem získat informace o zatížení systému, využití paměti a výkonu (Montes, a další, 2013). V případě PaaS se monitoruje míra využití platformních zdrojů a v případě SaaS se měří stav a míra využití aplikační služby a souvisejících zdrojů (Montes, a další, 2013).

3.2.2 Zlepšování služby cloud computingu

Obecně platí, že služba lze zlepšovat na úrovni její kvality, výkonnosti, efektivity, dostupnosti, hodnoty pro spotřebitele a spokojenosti spotřebitele využívajícího tuto službu (Boyne, 2003). Pokud úroveň kvalitativních parametrů služby nedosahuje očekávání spotřebitele anebo míra nákladů na službu převyšuje užitek z této služby plynoucí, spotřebitel odmítne přijmout službu, pokračovat ve využívání služby anebo bude požadovat změnu poskytovatele služby, jehož služba bude lépe splňovat požadavky na ni kladené (Hobfeld, a další, 2012). Vzhledem k dynamickému charakteru prostředí cloud computingu je nutné neustále měřit a hodnotit skutečně dosaženou úroveň kvality služby cloud computingu vzhledem k požadované úrovni kvality služby (Aceto, a další, 2012). Pokud je služba cloud computingu neuspokojivá, nákladově neefektivní, přesahuje tolerovanou úroveň rizika či neefektivně podporuje byznys procesy anebo pokud poskytovatel neplní smluvní závazky, je nutné zahájit proces zlepšování služby. Proces zlepšování služby definuje ITIL jako sedmi krokový proces nepřetržitého zdokonalování IT služby. Zlepšování služby cloud computingu z pohledu spotřebitele si klade za cíl zajistit dodávání takové služby cloud computingu, která poskytuje požadovanou funkcionalitu, její vlastnosti naplňují požadavky byznysu, je dodávaná na požadované úrovni kvality služby a umožnuje realizovat očekávanou byznys hodnotu (Wang, a další, 2014). Zlepšování služby cloud computingu z pohledu spotřebitele služeb cloud computingu představuje změny v kvalitativních parametrech služby, ve funkcionalitě služby, změnu služby anebo změnu poskytovatele služeb cloud computingu. Plánování činností souvisejících s ukončením využívání sužby cloud computingu nebo s ukončením smluvního vztahu s poskytovatelem služeb cloud computingu by mělo být provedeno před zahájením procesu přechodu na využívání služby cloud computingu. Podrobná specifikace těchto činností by měla být součástí tzv. exit strategie.

Exit strategie napomáhá organizacím vytvořit jasný plán pro nákladově efektivní a účinný odchod od poskytovatele, pro přechod k jinému poskytovateli anebo návrat k on-premise řešení (Bisong, a další, 2011). Definice takového plánu před zahájením migrace do prostředí cloud computingu umožňuje v budoucnu překonat nejen problémy závislosti na daném poskytovateli služeb cloud computingu ale i problémy související se zpětným získáváním dat od poskytovatele (Comuzzi, a další, 2013). Tvorba exit strategie je náročný proces, který vyžaduje individuální přístup spolu se součinností poskytovatele služeb cloud computingu. Exit strategie by měla obsahovat specifikaci dat, která budou získána zpět od poskytovatele včetně metod jejich získání, popisu způsobu jejich transferu, high level definici konverzní platformy a dále seznam potenciálních poskytovatelů a služeb (Wilson, 2011). Pro transfer dat od poskytovatele služby cloud computingu je nutné identifikovat důsledky vyplývající z právních předpisů a norem. To je zejména důležité při transferu dat mezi různými geografickými oblastmi specificky mezi členkami státy Evropské unie a ostatními státy světa. Základním předpokladem je splnění požadavku na přenositelnost dat a přiměřená interoperabilita mezi systémy různých poskytovatelů. Důležitým faktorem při tvorbě exit strategie je tedy zejména znalost rozdílů mezi různou syntaxí a sémantikou přenášených dat, technologiemi rozhraní nabízených různými poskytovateli a používanými standardy a protokoly (Opara-Martins, a další, 2016). Transfer dat mezi různými poskytovateli může usnadnit přijetí stejných standardů jako např. REST (REpresentational State Transfer) API. Aspekty přenositelnosti dat a interoperability v prostředí cloud computingu budou podrobně popsány v připravované normě ISO/IEC 19941 Information technology – Cloud computing

– Interoperability and portability. Jelikož proces získávání dat je časově i finančně náročná aktivita, je nutné zahrnout metody ukončení smluvního vztahu s poskytovatelem služeb cloud computingu a další relevantní požadavky vyplývající z exit strategie přímo do smluv o poskytování služby cloud computingu (Chou, 2015). Ve smlouvách by mělo být mimo jiné definováno vlastnictví dat, klasifikace dat, integrita dat, zajištění bezpečnosti a ochrany dat, a to jak během provozu služby cloud computingu, tak i během přenosu dat. Pro případ neplnění smluvních závazků ze strany poskytovatele je nutné ve smlouvách o poskytování služby definovat vyplývající právní postihy. Exit strategie by pro tento případ měla obsahovat pohotovostní plán pro případ nouze, který zahrnuje činnosti, které by měly být provedeny v případě neplánované nedostupnosti služby cloud computingu, která má vysoký dopad na kritické byznys procesy spotřebitele.

V kapitole 3. autorka této doktorské disertační práce vymezila základní specifika vyplývající z prostředí cloud computingu, která mají podstatní vliv na IT governance a IT management a odvodila základní vztah mezi governance a managment systémy v podniku.

Pro zjištění aktuálního stavu poznání cloud computing governance a cloud computing managementu byla autorkou této doktorské disertační práce provedena rešerše dostupných dokumentů zabývajících se specificky problematikou cloud computing governance a cloud computing managementu z pohledu spotřebitele. Výsledky analýzy těchto dokumentů jsou popsány v kapitolách 3.1 a 3.2. Navzdory množství a kvalitě analyzovaných dokumentů žádný z nich neposkytuje jednotný a komplexní přístup ke governance a managementu služeb cloud computingu, ve kterých by byly zastoupeny specifické oblasti využívání služeb cloud computingu z pohledu spotřebitele služeb cloud computingu, a žádný z nich neposkytuje komplexní metodický rámec pro cloud computing governance a cloud computing management.

Všeobecným problémem dostupných dokumentů zabývajících se praktikami governance a managementu služeb cloud computingu z pohledu spotřebitele je:

- *nejasné odlišení governance a managementu služeb cloud computingu, zaměňování těchto pojmů anebo případné zastřešení obou oblastí pod pojem governance,*
- *zaměření se často v omezeném rozsahu pouze na jednu specifickou oblast governance a managementu služeb cloud computingu,*
- *neakceptování dostupných dokumentů jako standard pro oblast governance a managementu služeb cloud computingu žádnou z uznávaných organizací,*
- *chybějící definice procesů governance a managementu služeb cloud computingu.*

4 Aplikovatelnost metodických rámců IT governance a IT managementu pro prostředí využívání služeb cloud computingu

Cílem této kapitoly je analyzovat současné široce uznávané metodické rámce IT governance a IT managementu z hlediska jejich podpory pro governance a management využívání služeb cloud computingu z pohledu spotřebitele.

Autorka této disertační práce se zaměřila specifiky na analýzu metodických rámců SOA Governance, ITIL 2011, COBIT 5 a modelu MBI.

V souladu s rozvojem informačních technologií dochází také k rozvoji správy a řízení IT. Spolu s tím vznikají nové a mění se stávající metodiky IT governance a IT managementu. Pro oblast IT governance a IT managementu existuje řada dostupných metodik postavených zejména na procesech řízení a na doporučeních z nejlepší zkušenosti z praxe pro řešení jednotlivých problémů governance a managementu podnikové informatiky (Gála, a další, 2015). Důležitost těchto modelů se soustředí zejména na oblast řízení výkonnosti informačních technologií a snaží se zajistit, aby informační technologie produkovaly očekávanou hodnotu z vložených investic při minimalizaci nákladů a rizik (Orozco, et al., 2015). Metodiky IT governance a IT managementu se v mnoha oblastech překrývají, ale nelze je považovat za absolutně shodné. Každá z nich poskytuje návod na vybudování podnikového systému IT governance anebo IT managementu, avšak různým organizacím přináší různou hodnotu, neboť se liší svojí komplexností, zaměřením na oblast řízení IT, metodami a procesy.

Akceptovanými metodickými rámci pro governance a management podnikového IT jsou (Bailey, a další, 2014; Jäntti, a další, 2015; Voříšek, a další, 2015):

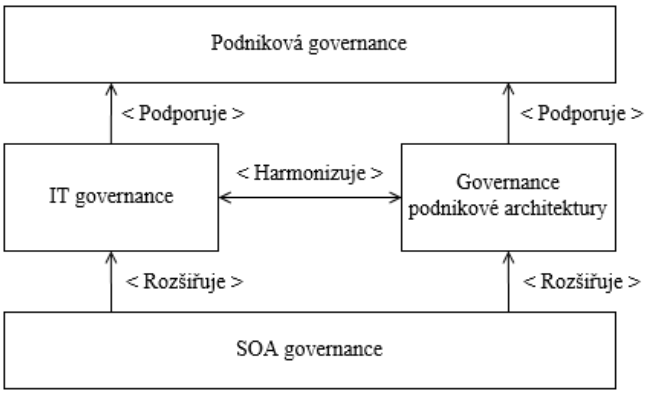
- Control Objectives for Information and Related Technology (COBIT),
- Information Technology Infrastructure Library (ITIL),
- SOA Governance Framework,
- Capability Maturity Model (CMM),
- ISO/IEC 38500 Corporate governance of information technology,
- ISO/IEC 20000 Information technology – Service management,
- Management Byznys Informatiky (MBI).

Tyto metodické rámce jsou často určeny organizacím, které vlastní aktiva nutná k provozování a využívání informačních technologií pro podporu byznys procesů a dosažení podnikových cílů. Obecně se proto tyto rámce zaměřují na governance a management podnikových aktiv ve smyslu lidí, dat, procesů a technologií ať už softwarových nebo hardwarových. V prostředí cloud computingu tato odpovědnost za aktiva nabývá novou perspektivu, neboť úroveň vlastnictví aktiv a kontroly nad těmito aktivy se liší v závislosti na modelu služeb a přesouvá se od poskytovatele ke spotřebiteli při používání služeb v modelu SaaS, PaaS a IaaS (Ahmad, a další, 2011). Navzdory širokému zaměření a vysoké kvalitě těchto metodických rámců, aspekty využívání služeb cloud computingu z pohledu spotřebitele nejsou v těchto metodikách komplexně řešeny, neboť žádný z nich není speciálně navržen pro prostředí cloud computingu (Bounagui, a další, 2015). Další podkapitoly se zabývají specificky metodickými rámci SOA governance, ITIL 2011 a COBIT 5 a specifikují konkrétní domény

governance a managementu služeb cloud computingu na které je možno tyto metodiky samostatně aplikovat či aplikovat po jejich přizpůsobení.

4.1 SOA governance

Servisně orientovaná architektura (SOA) je koncept realizace aplikační a technologické architektury informačních systémů, jejichž funkcionalita je reprezentována službami (Selčan, 2011). Služby v prostředí SOA mají specifické vlastnosti, které jim umožňují být součástí servisně orientovaného řešení. Služby představují autonomní jednotky, kdy programovací logika je ostatním službám skryta, což zabezpečuje nezávislost na použité implementační technologii. Významnou charakteristikou je znovupoužitelnost služby (Nourbakhsh, a další, 2015). Služby je možné skládat do kompozitních řešení, kdy každá služba realizuje určitou byznys funkci a může být opětovně použita jako součást jiné kompozice. Benefity plynoucí z vlastností služeb umožňují dosažení vyšší byznys agility, protože SOA poskytuje podniku schopnost změny nebo přizpůsobení služeb tak, aby vyhovovaly měnícím se potřebám s minimálními náklady (Rajmohan, a další, 2014) a zároveň usnadňuje automatizaci byznys procesů. Řada organizací využívá SOA jako efektivní nástroj k dosažení souladu byznysu s IT (Javeri, a další, 2013). Protože implementace SOA je náročnou činností vzhledem ke zdrojům a času, která může skončit neúspěchem a nedosažením benefitů ze SOA, je vhodné využít některou z dostupných metodik, které reflektují specifika SOA a obsahují zejména principy, praktiky a procesy pro správu a řízení služeb SOA nazývanou SOA governance (Joukhadar, a další, 2015a). SOA governance se zejména soustředí na governance a management služeb a poskytuje základní rámec pro dosažení benefitů a hodnoty SOA vyplývající z úspěšné implementace SOA, ze správného fungování SOA, které je plně v souladu s potřebami byznys procesů podniku a ze schopnosti rychle a pružně reagovat na změny byznys procesů, což přispívá výkonnosti organizace (Dehghani, a další, 2015). SOA governance by neměla stát izolovaně, ale měla by být součástí ostatních governance struktur. SOA governance rozšiřuje IT governance a governance podnikové architektury a musí být v souladu s pravidly a omezeními podnikové governance (The Open Group, 2009). SOA governance v hierarchii governance struktur zobrazuje Obrázek 8.



Obrázek 8: Vztah SOA governance vzhledem k ostatním governance strukturám, zdroj: (autor), podle: (The Open Group, 2009)

Existuje několik rámců nebo modelů pro governance a management služeb SOA vytvořené velkými organizacemi jako je IBM, Oracle, Software AG nebo Open Group (Joukhadar, a další, 2013). Pro řadu organizací definice SOA governance znamenala spíše doplněk k jejich vyvíjeným a poskytovaným SOA byznys řešením a governance a managementem služeb SOA se zabývají pouze z pohledu jejich produktů. Spolu s tím jak servisní orientace nabývala na významu, autoři odborné literatury publikovali vlastní návrhy rámců a modelů pro governance a management SOA (Joukhadar, a další, 2013; Niemann, a další, 2008) často zaměřené pouze na určité aspekty jako je například řízení

životního cyklu SOA governance (Schepers, a další, 2008), řízení životního cyklu služeb (Joukhadar, a další, 2013), zlepšování zralosti SOA prostřednictvím SOA governance (Joukhadar, a další, 2015a), návrh referenčního modelu SOA governance (Ott, a další, 2010), návrh modelu nasazení SOA governance (Javeri, a další, 2013) nebo návrh rámce pro hodnocení SOA governance s využitím COBIT (Dehghani, a další, 2015). Je patrné, že existuje velké množství přístupů SOA governance, které se liší svým zaměřením a úrovní detailu řešení problémů budování SOA. Přesto řada organizací při budování SOA čelí problémům vznikajícím během integrace systémů postavených na službách SOA se stávajícími systémy či obtížím vyvstávajících při návrhu efektivní rozhodovací struktury, při implementaci governance a managementu služeb SOA v konkrétních podmínkách, z nedostatku konzistentních governance procesů nebo hodnocení zralosti SOA a SOA governance (Joukhadar, a další, 2015a). Přijetí vhodného rámce SOA governance může pomoci překlenout obtíže s governance a managementem služeb SOA. Bohužel však řada rámců nedisponuje návodem pro jejich implementaci a není dostupný žádný empirický důkaz o úspěšné adopci dostupných rámců SOA governance (Joukhadar, a další, 2015a). Důvody pro implementaci rámce SOA governance lze shrnout následovně (Ramakrishnan, a další, 2013):

- zabezpečení souladu mezi byznysem a IT,
- propojení byznys a IT a SOA strategie,
- governance a management služeb SOA na celopodnikové úrovni,
- tvorba hodnoty ze SOA,
- zvýšení pravděpodobnosti úspěšné implementace SOA,
- řízení SOA investic a hodnocení jejich návratnosti,
- zefektivnění procesu rozhodování,
- efektivní řízení změn.

Porovnání mezi třemi rámci SOA governance publikovaných organizacemi IBM, Open Group a Oracle a třemi modely SOA governance publikovaných v odborných článcích včetně vybraných aspektů SOA governance, které slouží jako kritéria pro porovnání těchto rámců a modelů, znázorňuje Tabulka 3.

Tabulka 3: Porovnání aspektů SOA governance rámců, zdroj: (autor), na základě: (IBM, 2009; Javeri, a další, 2013; Joukhadar, a další, 2013; Dehghani, a další, 2015; Niemann, a další, 2008; Oracle, 2013; Ott, a další, 2010; The Open Group, 2009)

Aspekty SOA governance	IBM (2009)	Open Group (2009)	Oracle (2013)	Ott (2010)	Niemann (2008)	Javeri (2013)
Řízení životního cyklu SOA governance	++	++	++	—	++	++
Řízení životního cyklu portfolia SOA řešení	—	++	—	—	—	+
Řízení životního cyklu SOA řešení	—	++	—	—	—	+
Řízení životního cyklu portfolia SOA služeb	+	++	+	++	+	+
Řízení životního cyklu SOA služeb	++	++	+	++	+	+
SOA governance řídící	—	++	—	—	—	+

Aspekty SOA governance	IBM (2009)	Open Group (2009)	Oracle (2013)	Ott (2010)	Niemann (2008)	Javeri (2013)
principy						
Aspekty SOA, které potřebují být spravované	—	—	++	—	—	—
SOA politiky	++	—	+	—	+	+
SOA governance procesy	++	++	+	—	—	+
SOA governance organizační struktury, role, odpovědnosti	—	++	+	++	+	+
SOA governance artefakty	—	++	+	—	—	+
SOA governance technologie	+	++	++	—	+	+
SOA governance metriky	—	+	—	—	+	+
Zralost SOA	++	++	++	—	+	+
Zralost SOA governance	—	—	—	—	—	+

Legenda	
Aspekt není řešen	—
Aspekt je řešen	+
Aspekt je detailně řešen	++

Jak je vidět z Tabulky 3 rámec SOA Governance Framework vytvořený společností Open Group (The Open Group, 2009) řeší nejpodrobněji většinu z vybraných kritérií pro porovnání SOA governance rámců a modelů. SOA Governance Framework v roce 2012 prošel ratifikací a byla uznán Mezinárodní organizací pro normalizaci ISO jako mezinárodní standard (Kreger, et al., 2012) ISO/IEC 17998:2012 Information technology – SOA Governance Framework (ISO/IEC 17998, 2012). Norma ISO/IEC 17998 popisuje rámec pro governance servisně orientované architektury včetně metody pro jeho implementaci a neustálé přizpůsobování modelu SOA governance konkrétním potřebám podniku (ISO/IEC 17998, 2012). SOA governance jako podmnožina IT Governance (Gála, 2010) definuje politiky a procesy, které mají zajistit, že servisně orientovaná architektura bude fungovat správně, dle očekávání a plně v souladu s potřebami byznys procesů podniku a bude se agilně přizpůsobovat jejich změnám. SOA governance mění tradiční IT governance přístupy tak, aby bylo zajištěno, že servisně orientovaná architektura je řízena v souladu s potřebami realizace byznys procesů, funguje správně a dle očekávání a služby jsou navrhovány s důrazem na agilitu ve vztahu ke změnám v byznys prostředí (Owuonda, a další, 2016).

4.1.1 SOA Governance Framework

SOA Governance Framework je realizován pomocí dvou prostředků, kterými jsou SOA Governance referenční model a SOA Governance vitální metoda. SOA Governance referenční model popisuje a definuje podnikovou SOA architekturu a zahrnuje obvykle následující oblasti (The Open Group, 2009):

- řídící principy SOA Governance,

- řídící procesy SOA Governance,
- řízené procesy SOA Governance,
- SOA Governance artefakty,
- SOA Governance role a odpovědnosti,
- SOA Governance technologie.

SOA Governance vitální metoda je proces, který používá SOA Governance referenční model jako výchozí základ pro zdokonalování SOA architektury podniku pomocí cyklu plánování, definování, implementace a monitorování. Jedná se o nepřetržitý proces, který na základě postupných iterací zvyšuje nepřetržitě v cyklech efektivnost SOA Governance procesů v podniku.

Při porovnání SOA a cloud computingu je u obou přístupů patrná orientace na služby a tím i sdílení některých základních zásad (Hui-min, a další, 2013). V servisně orientovaném prostředí systémy a aplikace jsou poskytovány jako služby. Služby mohou být sdíleny více aplikacemi či uživateli současně, čímž lze optimalizovat využití IT zdrojů a zvýšit škálovatelnost, přičemž je abstrahována znalost implementačních detailů. Wang (2014) uvádí, že jedním ze základů cloud computingu je SOA, neboť služba v prostředí SOA může být představována jak za softwarovou službou, tak i platformní nebo infrastrukturní službou (Wang, a další, 2014), což podporuje fakt, že koncepce SOA a cloud computingu jsou příbuzné a navzájem se podporují, ale na druhou stranu nejde SOA a cloud computing považovat za identické koncepce (Tsai, a další, 2010; Yang, a další, 2012; Zhao, a další, 2015). SOA a cloud computing mohou vedle sebe existovat, doplňovat se a podporovat navzájem (Nourbakhsh, a další, 2015; Tsai, a další, 2010). Jak SOA, tak i cloud computingu přispívají k vyšší flexibilitě organizace. Laird (2011) předpokládá, že existuje pozitivní korelace mezi adopcí SOA v organizaci a schopností maximalizovat benefity z využití služeb cloud computingu (Laird, 2011). SOA může pro služby cloud computingu vytvořit provozní prostředí tak, aby jednotlivá funkcionalita tradičních podnikových informačních systémů mohla být představována souborem služeb cloud computingu poskytovaných externím poskytovatelem podle aktuální potřeby organizace. Stejně tak může servisně orientované řešení běžet na kompletním vývojovém, ladícím a aplikačním prostředí nebo na infrastruktuře dodávané jako služba cloud computingu. Vztah mezi SOA a cloud computingem je dále patrný v oblasti governance. Protože cloud computing je reprezentován službami, což je pro SOA governance optimální prostředí, principy a procesy SOA governance mohou být, po jejich přizpůsobení typickým aspektům cloud computingu, aplikovatelné při budování governance služeb cloud computingu (Laird, 2011; Rajmohan, a další, 2014). Stejně tak přístup ke správě životního cyklu služeb cloud computingu je podobný jako přístup definovaný SOA governance, ale jeho odlišnosti vyplývají ze specifik prostředí služeb veřejného cloud computingu (Copie, a další, 2012). Jak governance a management v prostředí SOA tak i v prostředí cloud computingu jsou založené na podpoře strategických (Copie, a další, 2012) byznys cílů, ze kterých jsou odvozovány cíle SOA a cíle cloud computingu (Owuonda, a další, 2016). Na cloud computing governance lze pohlížet jako na rozšíření SOA governance (Fortis, a další, 2014). Ačkoliv jak je patrné i z výše uvedené Tabulky 3, existuje řada přístupů k SOA governance, ale komplexní řešení cloud computing governance stále chybí (Fortis, a další, 2012).

Řada autorů tvrdí, že SOA governance je ideálním předpokladem pro cloud computing governance (Linthicum, 2009). Přesto však tradiční SOA governance předpokládá, že tradiční životní cyklus služeb je kontrolován interně, a tedy že služby jsou navržené, vyvinuté, provozované a poskytované IT oddělením ve stejné organizaci, která využívá služby pro podporu svých byznys procesů. Ačkoliv ke službám SOA může být přistupováno přes internet s využitím protokolů SOAP nebo REST, jejich hlavním cílem zůstává podpora on-premise aplikačních služeb (Feuerlicht, a další, 2015). Specifika SOA governance v prostředí cloud computingu určuje fakt, že množství poskytovaných služeb je

v prostředí cloud computingu obvykle mnohem vyšší než v klasickém IT prostředí a že spotřebitel služeb cloud computingu je oddělen od jejich poskytovatele. SOA governance a management procesy jsou typicky zaměřené na služby poskytované interním poskytovatelem, kdy spotřebitel je nejčastěji odlišnou organizační jednotkou ve stejné organizaci, dceřiná společnost či společnost vlastnící majoritní podíl v organizaci poskytovatele. Tudíž procesy SOA governance se aspektům cloud computingu, kdy je poskytovatel externí třetí strana, věnují pouze v omezené míře nebo vůbec (Schneider, a další, 2015). Problémem je tedy, že procesy SOA governance nezohledňují specifika využití služeb cloud computingu, ale jsou zaměřeny specificky na poskytovatele služeb SOA. SOA governance neposkytuje přístup, který by zahrnoval interakce mezi poskytovatelem a spotřebitelem během celého životního cyklu služby (Schneider, a další, 2015). Nezbytnost governance a managementu v prostředí cloud computingu je zvýrazněna zvláště pro procesy provozování služeb (run-time fáze). Služby v prostředí cloud computingu jsou dodávány v různých úrovních s různými parametry a atributy. Governance a management procesy musí plně pokrýt tuto oblast a být schopny řídit nastavení a údržbu úrovní služeb. Tím na vyšší váze nabývá řízení smluv o poskytování služeb. SOA governance vidí taktéž dohody o úrovni služeb SLA jako jeden z nástrojů zásadních pro řízení provozu služeb, kdy musí být provoz služeb monitorován z hlediska souladu s SLA a odchylky o porušení reportovány příslušným pracovníkům. Podle řídícího principu musí být správné dodání služby o požadovaném objemu a úrovni parametrů služby zajištěno smlouvou uzavřenou mezi poskytovatelem služby a spotřebiteli. Důležitým požadavkem na obsah smluv je zajištění požadované úrovně bezpečnosti služby a specifikace měřitelných cílů úrovně bezpečnosti. Z hlediska využívání služeb cloud computingu se typicky jedná o požadavky na spolehlivost služby, autentizaci a autorizaci uživatelů, řízení bezpečnostních incidentů, zajištění obnovy po havárii nebo logování dat provozu služby. Detailněji se však SOA Governance problematice smluv o poskytování služby nevěnuje. I přesto se SOA Governance se zabývá správou řady artefaktů souvisejících s řízením životního cyklu služeb. Některé artefakty jsou ve formě nestrukturovaných dat. V tomto případě se zejména jedná dokumenty popisující službu, řízení služby SOA anebo projektové dokumentace ve vztahu k SOA Governance rámci. Většina dat týkajících se služeb SOA a řízení jejich životního cyklu by měla být udržována v centrálním úložišti pro snadné sdílení informací o službách a pro automatizaci aktivit řízení životního cyklu služby jako je například monitorování služby (Königsberger, a další, 2014). Monitorování služeb nabývá na důležitosti zejména v prostředí cloud computingu. A to zejména z hlediska využití služeb spotřebitelem a jeho porovnání s kontraktně dohodnutými úrovněmi služeb. SOA Governance vyžaduje implementaci monitorovacího mechanismu pro sledování stavu služeb během jejich provozu a reportování odchylek vyskytujících se u jednotlivých služeb od normálního stavu služby. Tyto mechanismy pomáhají také sledovat využití služby spotřebitelem a objem využití služby. Od objemu využití služby cloud computingu se odvíjí celkové provozní náklady na službu, neboť účtování jejího využití je typicky založeno na principu pay per use. SOA i cloud computing vyžadují nový model finančního řízení služeb v rámci organizace (Owuonda, a další, 2016), kdy nový model financování služby musí odrážet relativně neomezené využití služby a výrazné změny objemu využité služby. Avšak tématu finančního řízení se SOA Governance Framework vůbec nevěnuje. Problémem SOA Governance je, že náklady na vývoj služby jsou účtovány typicky jednomu oddělení či jedné zainteresované straně.

Základními procesy metodického rámce SOA Governance jsou řídící procesy a řízené SOA procesy. Řídící procesy jsou specifické procesy, které governance model používá pro řízení jednotlivých řízených procesů. Úkolem řízených SOA procesů je zabezpečit dodání řešení požadovaného byznysem. Governance těchto procesů se soustředí na aktivity související s životním cyklem SOA služby, respektive SOA řešení.

SOA Governance definuje tři řídící procesy řízení shody, řízení výjimek a řízení komunikace. Proces řízení shody poskytuje mechanismus, který umožňuje objektivně vyhodnotit, zda je daný SOA governance proces ve shodě se SOA politikami, pravidly a standardy. SOA Governance Framework doporučuje v rámci SOA governance procesů definovat jednotlivé kontrolní body, ve kterých je realizováno hodnocení shody na základě předdefinovaných kritérií. V prostředí využívání služeb cloud computingu tento soubor kritérií vychází nejenom z interních politik a pravidel a legislativy a dalších externích norem, ale zejména ze smluv o poskytování služeb cloud computingu, specificky z SLA. Spouštěcí událostí jsou v případě tohoto procesu jakékoliv odchylky od parametrů úrovně služeb definovaných v SLA. Proces může být redefinován buď jako governance proces pro hodnocení realizované hodnoty z využití služeb cloud computingu, který se specificky zaměřuje pouze na řízené procesy nebo jako management proces úzce spjatý s procesem monitorování. Pokud proces řízení shody detekuje výjimku, která není ve shodě, je iniciován proces řízení výjimek. Proces řízení výjimek identifikuje výjimku, v případě jejího akceptování provede hodnocení výjimky, realizuje činnosti pro odstranění důvodu neshody a výjimku uzavře. V prostředí využívání služeb cloud computingu se může jednat o výjimky, kdy neshoda vznikla buď na straně poskytovatele služeb cloud computingu nebo na straně spotřebitele. Proces řízení výjimek musí být přizpůsoben pro skutečnost, kdy je informace o neshodě eskalována poskytovateli služeb a jakým způsobem bude daná neshoda řešena na straně spotřebitele služeb. Mechanismy eskalace a komunikace zainteresovaných stran jsou součástí procesu řízení komunikace. Proces řízení komunikace realizuje aktivity dané komunikační strategií a plánem a zabezpečuje, že relevantní informace týkající se sytému governance budou komunikovány s relevantními zainteresovanými stranami. V prostředí cloud computingu to znamená zejména zajistit komunikační kanály a definovat komunikační praktiky s poskytovatelem služeb cloud computingu.

Řízené procesy slouží k realizaci fází plánování, návrhu a operativního provozu SOA. SOA Governance definuje čtyři řízené SOA procesy:

- řízení portfolia řešení,
- řízení portfolia služeb,
- životní cyklus služby,
- životní cyklus řešení.

Jelikož úkolem SOA governance je nejen zabezpečit aktivity související s řízením životního cyklu SOA služeb, ale také zajistit efektivní dodávku SOA řešení vzhledem k byznys potřebám organizace a potřebám byznys procesů, je tok požadavků byznysu řízen ze směru počínaje plánováním a prioritizací individuálních SOA řešení. Tato SOA řešení jsou kompozicemi znovupoužitelných služeb SOA z portfolia existujících služeb. V případě, že v portfoliu služeb není dostupná vhodná služba SOA, je znovu zahájen životní cyklus služby s cílem navrhnout, vytvořit a nasadit do produktivního provozu službu novou. Stejně jako služba SOA, tak i SOA řešení podléhá životnímu cyklu skládajícího se z fází vývoje, nasazení a řízení SOA řešení. Z pohledu spotřebitele služeb je nutné nejprve na základě analýzy byznys požadavků a vytvoření byznys případu analyzovat dostupná cloudová řešení a služby na trhu služeb cloud computingu a poskytovatele těchto služeb. Poté by mělo být vytvořeno portfolio služeb cloud computingu poskytovaných souborem schválených poskytovatelů. Toto portfolio by mělo zajistit, že spotřebitel bude mít k dispozici služby, které jsou optimální z hlediska byznys požadavků, přijatelné míry rizika, nákladově efektivní a jsou schopny optimálně podporovat byznys procesy. *Řízení portfolia služeb* SOA přebírá zodpovědnost za plánování služby a změn této služby v souladu s byznys a SOA strategií. Řízení portfolia služeb SOA je realizováno aktivitami plánování portfolia, identifikace služby v souladu s byznys potřebami, vlastnictví služby, financování služby a změnové řízení služby. Analýza rizik nemá při řízení portfolia

služeb SOA takovou důležitost jako je tomu v případě služeb cloud computingu, a tudíž není součástí výše jmenovaných aktivit. Řízení rizik se však v prostředí využívání služeb cloud computingu stává jedním z nejdůležitějších faktorů a vyžaduje nutnost zavedení mechanismů pro realizaci řízení rizik souvisejících s přechodem a využíváním služeb cloud computingu (Bailey, a další, 2014). Na řízení rizik by měly podílet jak spotřebitel, tak i poskytovatel služeb computingu. Spotřebitel musí brát v úvahu nová rizika vyplývající z prostředí, kdy vlastník poskytovaných služeb je externí třetí stranou a tato rizika musí být řízena tak, aby byla na akceptovatelné úrovni. Poskytovatel vlastní a řídí cloud infrastrukturu, služby cloud computingu a vlastní či spravuje data spotřebitele. Vlastnictví služby cloud computingu poskytovatelem je chráněno autorským právem a k jejímu užívání musí spotřebitel odsouhlasit licenční podmínky uváděné obvykle jako nedílná součást smlouvy o poskytování služby cloud computingu. Ve smlouvě je také typicky ukotvena klauzule týkající se způsobů účtování využití služby, a to buď formou předplatného nebo dle aktuálního objemu spotřebované služby. Řízení změn služby cloud computingu je realizovatelné buď změnou parametrů služby nebo změnou smlouvy. Problémem modelu služeb veřejného cloud computingu je, že spotřebitel často nemá možnost jakkoliv změnit obsah smlouvy. Důležitým nástrojem pro řízení portfolia služeb cloud computingu je katalog služeb cloud computingu. SOA Governance definuje vytvoření a správu katalogu služeb SOA v rámci aktivity plánování portfolia služeb SOA. Správa portfolia služeb SOA má vliv i na řízení průběhu životního cyklu služby SOA a to tím, že definuje kontrolní body k zajištění shody v procesech životního cyklu služby. *Řízení životního cyklu služby* SOA je jednou z nejdůležitějších aktivit SOA governance (Königsberger, a další, 2014). Hlavním rozdílem životního cyklu služby SOA a služby veřejného cloud computingu je fakt, že v případě SOA služby je služba navržena, vyvinuta a testována interně, zatímco v případě služby veřejného cloud computingu jsou tyto činnosti plně pod kontrolou poskytovatele a z pohledu spotřebitele se tedy jedná pouze o aktivity hodnocení a výběru služeb od externího poskytovatele. Aktivity řízení životního cyklu SOA služeb se v prostředí využívání služby cloud computingu omezí pouze na získání služby, testování, nasazení do produktivního provozu, produktivní provoz služby, monitorování služby a podpora provozu služby. To však nepokrývá celý životní cyklus služby cloud computingu z pohledu spotřebitele a je nutné je doplnit o další fáze specifické pro využívání služeb cloud computingu. Po přizpůsobení je však možné aplikovat ty aktivity, které se zaměřují zejména na dokumentaci služby z hlediska požadavků na funkcionalitu služby nebo změň těchto požadavků včetně změn vyplývajících se smluv, vytvoření a schválení podkladů pro vyjednávání smluvních podmínek, testování služby s cílem zajistit, že služby splňuje požadavky na očekávanou funkcionalitu, bezpečnost a výkonnost, produktivní nasazení služby, monitorování služby a detekce událostí generovaných chybnou funkcionalitou, nedostatečnou výkonností nebo bezpečnostními problémy služby a řešení hlášení uživatelů služby o problémech spojených s provozem služby.

Řízení portfolia řešení je proces, který zajišťuje, že organizace má k dispozici soubor SOA řešení, které efektivně podporují potřeby byznys procesů a disponuje takovými IT schopnostmi, kapacitami a zdroji, které jí umožnují tento soubor SOA řešení úspěšně implementovat a že náklady na zvolené SOA řešení jsou optimální a že existuje plán financování rozvoje daného SOA řešení. Řízení portfolia řešení je proces, který se typicky realizuje na straně poskytovatele, který sestaví kompozitní řešení z jím poskytovaných služeb, které realizuje podporu konkrétnímu byznys problému spotřebitele. V prostředí spotřebitele služeb cloud computingu se jedná spíše o integraci služeb od různých poskytovatelů se stávajícími podnikovými informačními systémy. Každá služba v katalogu služeb cloud computingu je propojena s odpovídajícím rozhraním, které jí umožňuje komunikaci s ostatními službami a systémy. Toto rozhraní zajišťuje volání služby, udržuje informaci o službě a realizuje transformaci požadavku dané služby cloud computingu na takový požadavek, který bude srozumitelný pro ostatní služby a systémy. Aktivity procesu řízení portfolia řešení se v prostředí řízení využívání

služby cloud computingu prakticky neuplatní. Z tohoto důvodu je i *životní cyklus řešení* z pohledu spotřebitele služby nerelevantní.

Implementace SOA je časově i finančně náročnou aktivitou vyžadující dostupnost technických a lidských zdrojů, kdy nedostupnost a neefektivní koordinace zdrojů může skončit neúspěchem celého projektu a nedosažením očekávaných benefitů ze SOA (Joukhadar, a další, 2015b). SOA Governance Framework na rozdíl od ostatních SOA governance rámců (Joukhadar, a další, 2015b) poskytuje návod pro realizaci SOA governance v organizaci (Dehghani & Emadi, 2015). SOA Governance vitální metoda poskytuje návod pro implementaci modelu SOA governance, který je možno přizpůsobit v souladu se specifickými potřebami organizace (The Open Group, 2009). SOA Governance vitální metoda realizuje SOA Governance referenční model v krocích, které tvoří cyklus skládající se z fází plánování, definování, implementace a monitorování. Fáze *plánování* vychází z potřeb zainteresovaných stran a byznys strategie. Základem této fáze je pochopení současných governance modelů a struktur v organizaci, zhodnocení zralosti organizace z hlediska SOA, návrh vizi, strategie a rozsahu SOA governance, přizpůsobení řídících principů SOA Governance a definice plánu postupu realizace SOA governance v organizaci. Z hlediska spotřebitele služeb cloud computingu je jedná o podobné kroky, které však vyžadují posun od governance SOA k řešení governance služeb cloud computingu. Z byznys strategie by měla vyplynout potřeba podpory byznys procesů službami cloud computingu a výsledná cloud computing strategie by měla definovat jakým způsobem, při jak potřebném objemu jakých zdrojů a v jakém časovém horizontu lze naplnit cíle byznys strategie. Analýza stávajících governance modelů implementovaných v organizaci by měla sloužit přípravná fáze pro návrh a zlepšování modelu cloud computing governance jako součást IT governance případně SOA governance. Pro zjištění aktuální úrovně zralosti cloud computing governance v organizaci je nutné provést hodnocení, které poskytne zpětnou vazbu vrcholovému vedení a napomáhá definovat budoucí rozvoj cloud computing governance. Cloud computing governance by se měla rozvíjet v souladu s řídícími principy. SOA Governance Framework definuje soubor řídících principů určených specificky pro SOA a SOA governance, ty však jsou jenom částečně aplikovatelné pro cloud computing governance a aby poskytovaly optimální referenci a podporu při návrhu a realizaci cloud computing governance modelu je nutné je upravit a doplnit o nové specifické řídící principy. Fáze *definování* se skládá z definice SOA Governance procesů, definice organizační struktury, rolí a jejich odpovědností, definice dokumentů, definice SOA governance prostředí a z vytvoření plánů realizace SOA governance modelu. Je nutné stanovit procesy přizpůsobené pro prostředí využívání cloud computingu a takové, které budou odpovídat governance procesům. Problém rámce SOA Governance Framework je, že kombinuje governance přístup s managementem a nerozlišuje jasně mezi governance procesy a management procesy, přičemž některé procesy překrývají obě oblasti. Z tohoto důvodu je nutné upravit také navrženou organizační strukturu a klíčové role, tak abych reflektovaly pouze governance strukturu a zaměřovaly se na plánování a řízení cloud computing governance. Stejně tak budou odlišnosti i v definici dokumentů, které budou popisovat model cloud computing governance a jednotlivé jeho komponenty nebo budou relevantní z hlediska modelu cloud computing governance. Tomu se musí přizpůsobit i plány realizace cloud computingu governance modelu, které budou jinak specifické pro každou organizaci. Dle plánů přechodu bude realizovaná fáze *implementace*. Fáze *monitorování* cloud computing governance se bude lišit od fáze monitorování SOA governance zejména z hlediska monitorovacích objektů a metrik.

4.2 COBIT

COBIT (The Control Objectives for Information and Related Technology) je soubor dobrých praktik pro oblast governance a managementu informačních technologií (ISACA, 2012c). COBIT napomáhá organizacím naplňovat požadavky v oblasti legislativních předpisů, řízení rizik a celkového sladění IT strategie s cíli organizace (Youssfi, a další, 2014). Aktuální verze COBIT 5 z roku 2012 je integrací rámců vytvořených mezinárodní asociací Information Systems Audit and Control Association (ISACA) jako jsou Val IT 2.0, Risk IT, IT Assurance Framework (ITAF) a Business Model for Information Security (BMIS) s verzí COBIT 4.1 (ISACA, 2012c). Verze COBIT 5 je vyvinuta s ohledem na široce akceptované standardy a rámce, které se vztahují na oblast IT Govenace jako je Information Technology Infrastructure Library (ITIL), International Organization for Standardization (ISO), PRINCE2, Capability Maturity Model Integration (CMMI) a The Open Group Architecture Framework (TOGAF) (ISACA, 2012c). COBIT 5 poskytuje ucelený rámec pro governance a management podnikového IT a pomáhá vytvořit přidanou hodnotu z IT prostřednictvím vytvoření rovnováhy mezi přínosy z využití IT a optimalizací jejich rizika. COBIT 5 napomáhá (ISACA, 2014a):

- zabezpečení informací v kvalitě potřebné pro podporu obchodních rozhodnutí,
- dosažení strategických cílů efektivním a inovativním využitím IT,
- dosažení operační excelence nasazením spolehlivých a účinných technologií,
- řízení IT rizik na akceptovatelné úrovni,
- optimalizace nákladů na IT služby a technologie,
- dosahování shody s platnou legislativou, smlouvami a politikami.

COBIT 5 je založen na pěti klíčových principech (ISACA, 2012c):

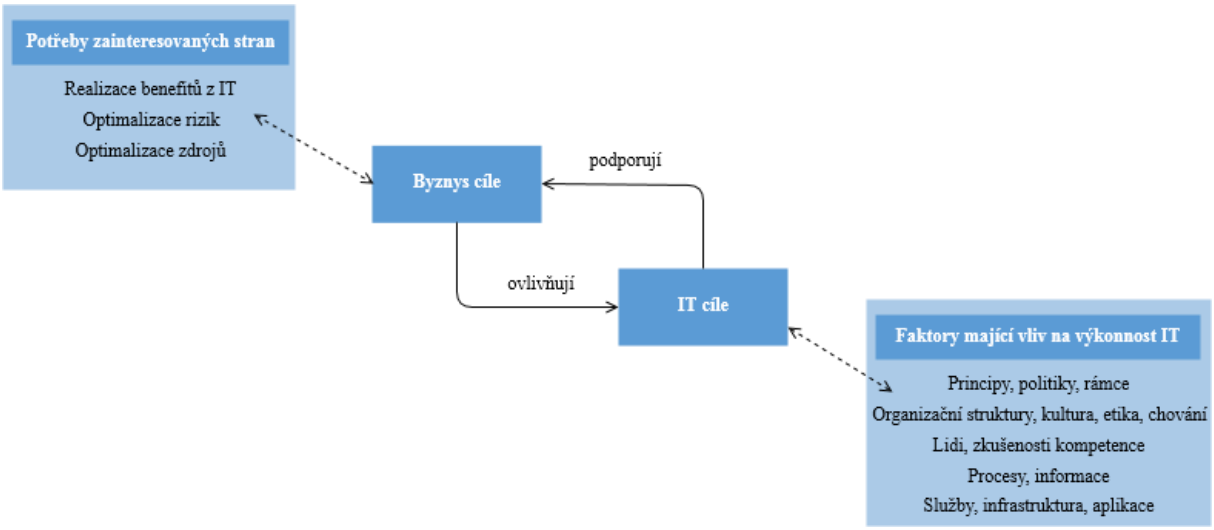
1. *Uspokojení potřeb a tvorba přidané hodnoty zainteresovaným stranám* – Potřeby zainteresovaných stran by měly být transformovány do specifických, přizpůsobitelných a realizovatelných podnikových cílů. Tyto cíle jsou následně mapovány do IT cílů, které reversně podporují podnikové cíle a požadavky zainteresovaných stran. Tvorba hodnoty finančního i nefinančního rázu odpovídající požadavkům zainteresovaných stran, optimalizace rizik a optimalizace zdrojů jsou základní governance cíle.
2. *Zabezpečení komplexního celopodnikového governance a managementu* – COBIT 5 integruje IT Governance do celopodnikového governance a pokrývá funkce, procesy a služby potřebné pro governance a management podnikové informatiky.
3. *Použití jednotného integrovaného rámce* – COBIT 5 díky integraci s ostatními ISACA standardy vytváří jednotný integrovaný rámec IT governance a IT managementu.
4. *Aplikace holistického přístupu* – COBIT 5 poskytuje holistický a systematický pohled na governance a management podnikové informatiky postavený na správě a řízení souboru faktorů tzv. enablerů, které pokrývají podnik jako celek. Jsou to faktory, které ovlivňují governance a management podnikového IT a jsou řízeny kaskádou cílů. Jedná se o principy, politiky a rámce aplikující principy IT governance a IT managementu do operativního řízení, procesy, organizační struktury, kulturu, etiku a chování, informace, služby, infrastrukturu a aplikace a lidé, znalosti a kompetence. Každý z faktorů má 4 dimenze, kterými jsou zainteresované strany, cíle, životní cyklus a dobré praktiky.
5. *Oddělení governance od managementu* – Governance a management slouží k různým účelům a jsou realizovány odlišnými typy aktivit, a proto vyžadují i různou organizační strukturu s rozdílnými odpovědnostmi. Governance zabezpečuje neustálé vyhodnocování obchodních podmínek a potřeb zainteresovaných stran, na jejichž základě stanovuje požadovanou úroveň

podnikových cílů, stanovuje způsob dosažení těchto cílů a sleduje výkon a dodržování shody reálně dosažených cílů s plánovanými podnikovými cíli. Management plánuje, vytváří, provozuje a monitoruje činnosti ve shodě s požadavky governance za účelem dosažení podnikových cílů.

Ačkoliv COBIT 5 v zásadě není určen pro cloud computing, praktiky, principy a procesy v něm obsažené lze přizpůsobit také pro řízení služeb cloud computingu (Kratzke, 2012). Mezinárodní asociace Information Systems Audit and Control Association (ISACA) vydala příručku Controls and Assurance in the Cloud: Using COBIT 5 obsahující praktické kroky k realizaci auditu, kontroly a řízení rizik a zajištění informační bezpečnosti v prostředí cloud computingu postavené na využití COBIT 5 (ISACA, 2014b). Příručka poskytuje následující oblasti pro efektivní governance a management nejdůležitějších oblastí v prostředí cloud computingu (ISACA, 2014b):

- otázky bezpečnosti a ujištění,
- posuzování způsobilosti procesů,
- scénáře rizik cloud computingu a kontrolní seznam pro řízení rizik v prostředí cloud computingu,
- praktický přístup k měření ROI v prostředí cloud computingu.

COBIT 5 se soustředí na zajištění souladu byznysu a IT s cílem zabezpečit potřeby zainteresovaných stran ve smyslu realizace benefitů z IT, optimalizace rizik a zdrojů. Toho dosahuje COBIT 5 prostřednictvím kaskády cílů. Byznys cíle přímo souvisí se zabezpečením potřeb zainteresovaných stran, které jsou ovlivňovány změnou externího prostředí (ISACA, 2012b). Byznys cíle jsou určující pro definování IT cílů, které zpětně podporují dosažení byznys cílů, viz Obrázek 9. Realizace IT cílů je ovlivněna řadou faktorů, které jsou důležitými komponentami IT prostředí a významně ovlivňují provádění IT operací a výkonnost IT. COBIT 5 definuje sedm faktorů ovlivňujících governance a management podnikového IT a umožňující realizovat dané IT cíle.



Obrázek 9: Kaskáda cílů zabezpečující soulad byznysu a IT, zdroj: (autor), podle (ISACA, 2012b; Van Grembergen, a další, 2009)

Z hlediska faktorů definovaných v COBIT 5 je zapotřebí se v prostředí cloud computingu věnovat řešení následujících otázek a úkolů (ISACA, 2014b):

- Faktor principů, politik a rámců
  - Oblast bezpečnostní politiky a její transparentnosti. Zde je nutno společně s poskytovatelem služeb cloud computingu dojít k dohodě obsahující záruky, že

poskytovatel aplikuje bezpečnostní mechanismy na takové úrovni, které jsou vyžadovány spotřebitelem. Tyto bezpečnostní mechanismy a jejich úrovně musí být definovány v SLA.

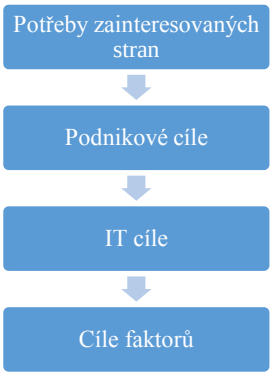
- Oblast shody s legislativními požadavky. Patří sem nutnost vyřešení požadavků na dostupnost metod zabezpečujících legislativní ochranu citlivých dat, jako jsou osobní údaje, údaje z platebních médií, finanční reporty nebo geografické uložení dat. Současně je potřeba mít k dispozici data pro provedení auditu.

- Faktor procesů
  - Oblast řízení bezpečnosti. Je zapotřebí prověřit, zda poskytovatel má implementovány procesy pro detekci bezpečnostních narušení jako je například detekce vniknutí neautorizovaného uživatele do systému. Poskytovatel musí provádět bezpečnostní logování aktivit, které musí být dostupné spotřebiteli pro potřeby auditu.
- Faktor organizačních struktur
  - Oblast opatrnosti a pečlivosti s jakou vlastník serveru přistupuje k ochraně dat spotřebitele. Jedná se zejména o model veřejného cloud computingu a uložení citlivých dat v prostředí cloud computingu. Zde je nutno získat od poskytovatele informace o všech s ním spolupracujících externích firmách, které by se potenciálně při své činnosti u poskytovatele mohly dostat do kontaktu s těmito citlivými daty spotřebitele. Spotřebitel musí mít možnost se rozhodnout, zda bude těmto externím firmám důvěřovat. Spotřebitel musí mít v tomto případě mít k dispozici informace, kde jsou jeho citlivá data fyzicky uložena.
- Faktor kultury, etiky a chování
  - Oblast životaschopnosti poskytovatele. Je nutno zvážit rizika spojená s možným ukončením činnosti poskytovatele. Je nutno provést analýzu rizik a rozhodnout se, zda a která data mohou být u daného poskytovatele uložena a jaké náklady budou spojené s případným nouzovým transferem dat a zda bude takový transfer realizovatelný.
  - Oblast prověřování ostatních spotřebitelů. Je vhodné mít údaje o tom, kteří další spotřebitelé služeb cloud computingu sdílejí stejné cloudové servery nebo datová úložiště. Spotřebitel by měl prověřit reputaci těchto spotřebitelů.
- Faktor informací
  - Oblast vlastnictví dat. V některých smlouvách o využití služeb cloud computingu může být dohodnuto, že vlastníkem dat uložených v prostředí cloud computingu je poskytovatel služeb. Poskytovatel může v těchto případech ve smlouvě vyžadovat definovat poplatek za převedení dat zpět ke spotřebiteli v případě ukončení využívání služby.
  - Oblast ochrany záznamů pro forenzní audity. Spotřebitel musí zvážit dostupnost dat a záznamů, tak aby byly případně k dispozici pro forenzní audit. Data spotřebitele jsou obecně uložená na konkrétním serveru společně s daty jiných spotřebitelů a migrována mezi různými servery často velmi geograficky vzdálenými. Může tedy nastat situace, že pro konkrétní časový interval data pro audit nebudou k dispozici. Může se případně i stát, že místní úřad zabaví server za účelem soudního zajištění dat některého ze spotřebitelů i s daty všech ostatních spotřebitelů, kteří sdílí stejný server.
  - Oblast nakládání s daty. Jedním z důsledků dynamické škálovatelnosti, kdy aplikace a datové soubory jsou přeneseny z jednoho serveru na druhý, může být to, že původní aplikace a jejich data zůstanou na originálním datovém serveru a nesmí být ihned vymazána. Například bezpečnostní logy, které jsou spojeny s danou aplikací a daným serverem mohou být vymazány až po jejich uložení do zálohovacího systému pro účely budoucího bezpečnostního auditu. Nicméně aplikace a data spotřebitele musí

být po provedené záloze a v časovém intervalu daném v SLA spolehlivě vymazána. To dává spotřebiteli jistotu, že jeho citlivá data se nedostanou k nepovolaným osobám. Stejně tak musí být ve smlouvě jasně definováno, že po ukončení smluvního vztahu s poskytovatelem budou data spotřebitele okamžitě zničena.

- Faktor služeb, infrastruktury a aplikací
    - Oblast fyzického uložení dat. Z technologického hlediska, data mohou být fyzicky uložena na kterémkoliv serveru poskytovatele. Toto uložení se může dynamicky měnit. Mohou však existovat legislativní nebo data governance požadavky vyžadující, aby určitá data spotřebitele byla uložena v dané geografické lokalitě. Tato lokalita může být definována jako země nebo určitá oblast území, jako datové centrum nebo dokonce jako server.
    - Oblast smíšení dat. Pokud více spotřebitelů sdílí stejnou aplikaci na stejném serveru, pak jednotlivé datové soubory této aplikace mohou obecně obsahovat data více než jednoho spotřebitele. V případě, že spotřebitel vyžaduje v SLA, že jeho data nesmí být smíšená s daty jiných spotřebitelů, musí poskytovatel pomocí vhodné technologie zabezpečit, že jednotlivé datové soubory obsahují data pouze daného spotřebitele. V některých případech může být tato separace provedena tak, že data spotřebitelů jsou kódována a každý se spotřebitelů používá jiný kód.
    - Oblast řízení identit a přístupu. Při jakékoliv manipulaci s daty spotřebitele pomocí některé z aplikací musí být vždy zřejmé, který fyzický uživatel s těmito daty manipuloval. A to ať ve smyslu vytvoření změny nebo výmazu dat či pouhého prohlížení dat. To znamená, že každý uživatel musí být jednoznačně identifikován a na základě této identifikace mu pro dané aplikace musí být přiřazena role, která umožní tomuto uživateli pouze takové datové manipulace vyplývající z jeho pracovního zařazení ve společnosti spotřebitele nebo některé jeho partnerské společnosti.
    - Oblast disaster recovery. Scénáře zálohování a havarijní obnovy dat spotřebitele jsou v prostředí cloud poskytovány jako služby. Poskytovatel služby však nemusí být tím, kdo tyto služby skutečně realizuje, neboť tyto služby mohou být outsourcovány na třetí strany. V některých případech mohou tyto třetí strany fyzické provádění dat znovu outsourcovat. V prostředí veřejného cloud computingu je zapotřebí, aby ve smlouvě byly otázky testování, obnovitelnosti dat nebo požadavky na časové lhůty obnovení dat detailně definovány.
- Faktor lidí, zkušeností a kompetencí
    - Oblast závislosti na proprietárním API poskytovatele. Pokud spotřebitel využívá takové služby, ke kterým je přístup možný pouze proprietárního API poskytovatele, je zapotřebí zvážit riziko v případě nutnosti změny poskytovatele. Náklady na převod dat z aplikace s proprietárním API jsou obvykle mnohem vyšší než převod dat z prostředí standardních neproprietárních API.

V prostředí COBIT 5 vychází cloud computing governance a management z definované kaskády cílů, na jejímž vrcholu stojí potřeby zainteresovaných stran mapující se do třinácti podnikových cílů, které jsou následně mapovány do třinácti IT cílů. Ty se následně mapují do cílů faktorů, jak je patrné z Obrázku 10. Potřeby zainteresovaných stran jsou ovlivněny například změnami obchodního prostředí, legislativními požadavky či novými technologiemi. Podnikové a IT cíle jsou rozčleněny do čtyř oblastí finanční dimenze, dimenze zákazníků, interní dimenze a dimenze učení se a růst, které reflektují dimenze dle balanced scorecard.



Obrázek 10: Kaskáda cílů COBIT 5, zdroj: (ISACA, 2012c)

NIST pro prostředí cloud computingu definuje pět zainteresovaných stran, které se účastní na transakcích, realizaci procesů či plní související úkoly a identifikuje jejich vzájemné působení (NIST, 2013). Těmito zainteresovanými stranami jsou cloud spotřebitel, cloud poskytovatel, cloud auditor, cloud broker a cloud zprostředkovatel. V prostředí COBIT 5 je cloud computing považován jako rozšíření IT aktiv, a tudíž musí být identifikovány všechny relevantní zainteresované strany, jichž se přijetí služeb cloud computingu dotýká. Pro detailní analýzu a identifikaci potřeb zainteresovaných stran v prostředí cloud computingu jsou zásadní následující COBIT 5 procesy a k nim vztahující se procesní praktiky (ISACA, 2014b; Harlili, 2014):

- EDM02 Zajištění realizace přínosů
  - EDM02.02 – Řízení optimalizace hodnoty – řízení principů a praktik s cílem realizovat optimální hodnotu z investic do IT v průběhu celého jejich životního cyklu
- EDM03 Zajištění optimalizace rizika – zajišťuje, že míra tolerance k riziku je definovaná a komunikovaná, že riziko nepřekročí podnikovou toleranci k riziku, a že optimalizace rizika je součástí stávajících governance politik, které prosazují vytvoření efektivního systému pro řízení IT rizik
- APO02 Řízení strategie – poskytuje komplexní pohled na aktuální byznys a IT prostředí, stanovuje a jasně sděluje IT cíle v souladu s byznys cíli, určuje kroky a plány pro jejich dosažení
  - APO02.02 Hodnocení současného prostředí a jeho výkonnosti – porozumění podnikové architektuře v souvislosti s podnikovými informačními technologiemi, posouzení výkonnosti interního IT prostředí, tzv. IT schopností, kapacit a zdrojů a externích IT služeb a zhodnocení poskytovatelů služeb včetně finančního dopadu, potenciálních nákladů a přínosů využívání externích služeb
  - APO02.03 Definice cílového stavu IT prostředí – definování požadovaných IT schopností, kapacit a zdrojů a IT služeb na základě zhodnocení současného IT prostředí a moderních informačních technologií v souladu s podnikovou architekturou
  - APO02.04 Provedení diferenční analýzy – identifikace rozdílů mezi aktuálním a požadovaným stavem IT schopností, kapacit a zdrojů a IT služeb, zvážení kritických faktorů úspěchu provádění strategie a upřesnění definice požadovaných IT schopností, kapacit a zdrojů a IT služeb včetně formulace potenciálně dosažitelné hodnoty a benefitů z využití podnikového IT
  - APO02.05 Definice strategického plánu a plánu projektu – vytvoření strategického plánu pro dosažení požadovaných IT schopností, kapacit a zdrojů a IT služeb obsahující definici IT cílů, formulace investičních programů do IT včetně způsobu získávání zdrojů, financování, identifikace souvisejících rizik, nákladů, organizačních

změn a regulatorních požadavků, vytvoření projektového plánu a převedení cílů do měřitelných ukazatelů

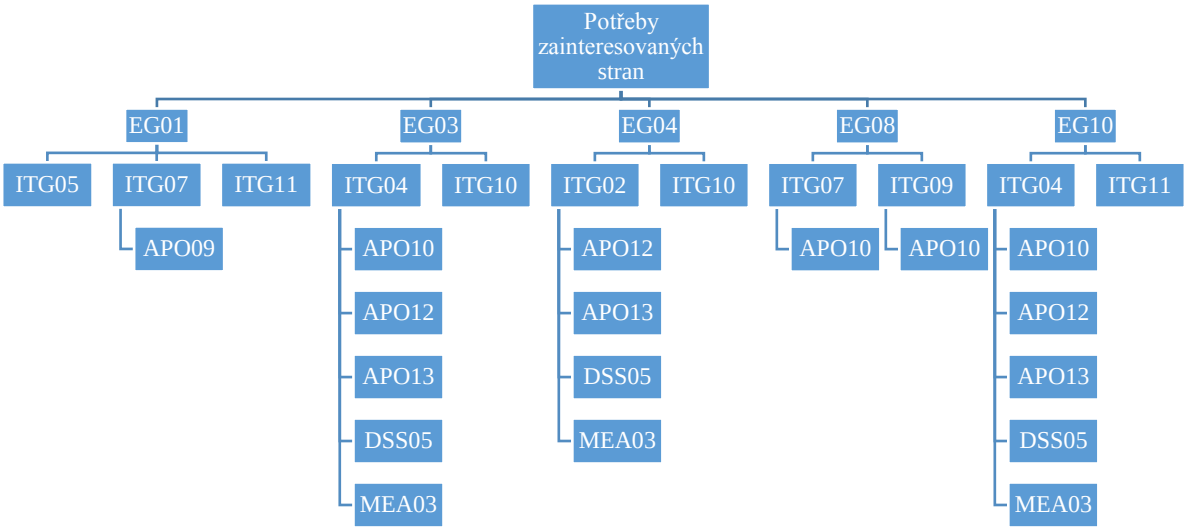
- APO05 Řízení portfolia
  - APO05.01 Vytvoření cílového investičního mixu – identifikace nákladů, finančních a nefinančních přínosů investic do IT, očekávané návratnosti investic v průběhu celého ekonomického životního cyklu podnikového IT
  - APO05.03 Hodnocení a výběr investičních programů – hodnocení a prioritizace investičních programů, vyčlenění finančních prostředků a iniciace zvolených programů
- APO06 Řízení rozpočtů a nákladů
  - APO06.01 Řízení finanční a účetnictví – zavedení jednotných finančních a účetních standardů
  - APO06.02 Prioritizace alokace zdrojů – implementace rozhodovacího procesu prioritizace IT zdrojů a pravidel rozhodování o způsobu alokace finančních prostředků
  - APO06.03 Tvorba a řízení rozpočtů – vytvoření rozpočtů obsahujících očekávané náklady na IT v závislosti na portfoliu investičních programů do IT
  - APO06.04 Modelování a alokace nákladů – kategorizace nákladů na IT, identifikace platebních modelů služeb a vytvoření transparentního modelu nákladů na IT umožňujícího identifikovat skutečné využití služeb a s nimi spojených poplatků a předpovídat náklady na IT
  - APO06.05 Řízení nákladů – řízení nákladů na IT, jejich monitorování, identifikace odchylek a jejich dopadů na obchodní procesy
- APO12 Řízení rizik – identifikace rizik a analýza rizik, stanovení odpovědi na riziko a monitorování rizika
  - APO12.03 Udržování profilu rizika – správa registru rizik obsahujícího popis jednotlivých rizik, očekávané frekvence výskytu hrozeb, potenciální dopad hrozeb na aktiva, reakce na riziko, identifikace IT zdrojů a IT služeb nezbytných pro zajištění požadované realizace obchodních procesů a jejich omezení
- BAI01 Řízení programů a projektů
  - BAI01.02 Zahájení programu – zahájení programu cílem potvrdit očekávané přínosy přijetí IT služeb
  - BAI01.03 Řízení zapojení zainteresovaných stran – identifikace, analýza, zapojení a řízení zainteresovaných stran, analýza zájmů a požadavků zainteresovaných stran, zabezpečení aktivní výměny přesných a konzistentních informací mezi zainteresovanými stranami ve správný čas
  - BAI01.04 Vytvoření a udržování programů – definice a zdokumentování všech projektů z hlediska jejich rozsahu, vstupů, výstupů, dosažení cílů a hodnoty IT investic pro zainteresované strany, zajištění souladu se strategickými byznys cíli
- BAI03 Řízení identifikace a budování řešení
  - BAI03.01 Návrh vysoce kvalitních řešení – navržení IT řešení, které budou schopny na vysoké úrovni zabezpečit podporu obchodních procesů a dosažení podnikových cílů v souladu s podnikovou architekturou, IT strategií, byznys strategií a regulatorními požadavky
- MEA03 Monitorování, hodnocení a posouzení shody s externími požadavky
  - MEA03.01 Identifikace externích požadavků na shodu – identifikace a monitorování změn legislativních, regulatorních a dalších externích požadavků ve shodě s provozem IT

- MEA03.02 Optimalizace reakce na externí požadavky – pravidelná revize politik, principů a procedur z hlediska shody s legislativními, regulatorními a dalšími externími požadavky, proškolení relevantních zaměstnanců
- MEA03.03 Potvrzení shody s externími požadavky – potvrzení shody politik, principů a procedur s legislativními, regulatorními a dalšími externími požadavky
- MEA03.04 Získání ujištění o souladu s externími požadavky – realizace pravidelných přezkoumání o souladu politik, principů a procedur s externími požadavky a posouzení míry shody, prohlášení poskytovatelů IT služeb třetích stran o úrovni jejich souladu s platnými zákony a předpisy

Mezi podnikové cíle a s nimi související IT cíle obzvláště důležité pro prostředí cloud computingu patří (ISACA, 2014b):

- EG01 Hodnota byznys investic pro zainteresované strany
  - ITG05 Realizace benefitů z investic do IT a do portfolia služeb
  - ITG07 Dodání IT služeb v souladu s byznys požadavky
  - ITG11 Optimalizace IT aktiv, IT zdrojů a IT schopností a kapacit
- EG03 Řízení rizik byznysu
  - ITG04 Řízení rizik vyplývající z využití IT
  - ITG10 Bezpečnost informací a bezpečnost provozu infrastruktury a aplikací
  - EG04 Shoda s legislativními předpisy a oborovými standardy
  - ITG02 Shoda IT s externími právními předpisy a regulacemi a podpora IT pro zajištění shody byznysu s externími právními předpisy
  - ITG10 Bezpečnost informací a bezpečnost provozu infrastruktury a aplikací
- EG08 Byznys agilita
  - ITG07 Dodání IT služeb v souladu s byznys požadavky
  - ITG09 IT agilita
- EG10 Optimalizace nákladů na dodání IT služeb
  - ITG04 Řízení rizik vyplývající z využití IT
  - ITG11 Optimalizace IT aktiv, IT zdrojů a IT schopností a kapacit

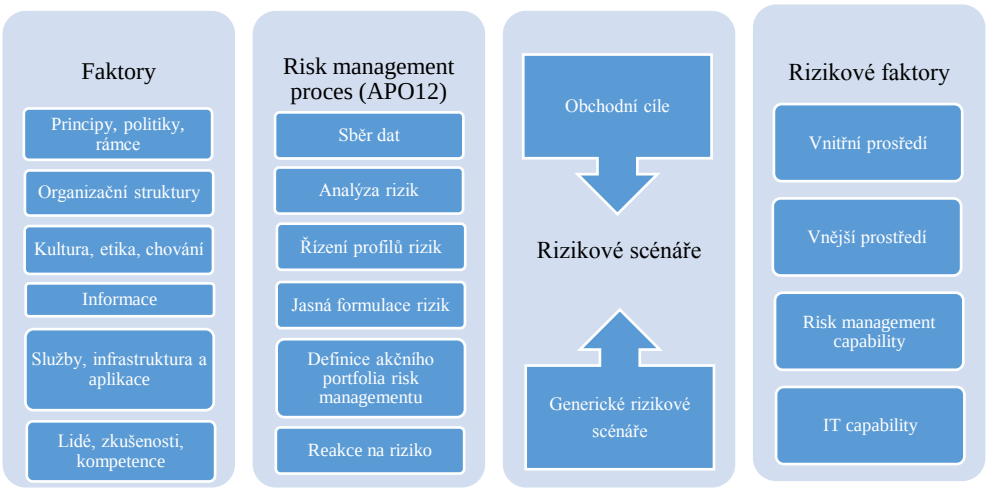
Pro prostředí cloud computingu se k výše uvedeným IT cílům vztahují procesy znázorněné na Obrázku 11 (ISACA, 2014b):



Obrázek 11: COBIT 5 procesy vztahující se k IT cílům v prostředí cloud computingu, zdroj: (ISACA, 2014b)

Proces APO09 Řízení dohod o službách zabezpečuje efektivní využití IT služeb definovaných v katalogu služeb, jejich identifikaci, specifikaci, návrh, publikování a monitorování úrovně služeb a ukazatele výkonnosti. Na základě informací obsažených v katalogu služeb napomáhá definovat a připravit dohody o poskytování služeb, provádět pravidelné přezkoumávání dohod o službách a jejich revizi v případě potřeby. Proces APO10 Řízení dodavatelů zabezpečuje, aby služby od všech dodavatelů splňovaly požadavky podniku, výběr dodavatelů, řízení vztahů s dodavateli včetně řízení rizik, řízení smluv, monitorování výkonu dodavatele a dodržování poskytování dohodnuté úrovně služeb. Cílem procesu APO12 Řízení rizik je průběžně identifikovat, posoudit a snížit rizika související s IT v rámci úrovní tolerance stanovených výkonným vedením společnosti. Cílem procesu APO13 Řízení bezpečnosti je definovat, provozovat a monitorovat systém pro řízení bezpečnosti informací. Proces DSS05 Řízení bezpečnosti služeb obsahuje praktiky vztahující se k zajištění síťové a komunikační bezpečnosti, řízení a správě uživatelských identit a přístupových oprávnění a to tak, aby bezpečnostní riziko bylo pro podnik přijatelné a v souladu s bezpečnostní politikou. Proces MEA03 Monitorování, hodnocení a posouzení shody s externími požadavky zabezpečuje, aby legislativní, regulatorní a další externí požadavky byly ve shodě s IT a umožňuje realizovat pravidelné přezkoumání interních politik, principů, standardů, procedur a metodik a posouzení míry jejich shody s legislativními požadavky.

V případě zvážení obecných problémů a výzev vztahujících se ke cloud computingu, jako je bezpečnost, umístění dat, vlastnictví dat, zabezpečení dat pro audit, správa identit a řízení přístupu, shoda s předpisy atd., se z hlediska metodiky COBIT 5 v prostředí cloud computingu jeví jako jedna z důležitých oblastí aplikace procesu řízení rizik (APO12) (ISACA, 2014b). Následující Obrázek 12 ukazuje vzájemné propojení faktorů, risk management procesů, rizikových scénářů a rizikových faktorů metodiky COBIT 5 v prostředí cloud computingu.



Obrázek 12: Propojení faktorů majících vliv na výkonnost IT, risk management procesů, rizikových scénářů a rizikových faktorů COBIT 5 v prostředí cloud computingu, zdroj: (ISACA, 2014)

Dále se jako důležité procesy relevantní z pohledu spotřebitele služeb cloud computingu, které lze přizpůsobit pro prostředí governance a managementu využívání služeb cloud computingu poskytovaných externím poskytovatelem těchto služeb, jeví následující governance a management procesy (ISACA, 2014b; Harlili, 2014):

- EDM01 Zajištění vytvoření a udržování rámce governance – analýza a formulace požadavků na IT governance, zavedení a udržování struktur, principů, procesů a praktik a stanovení jasně vymezených odpovědností s cílem podpořit naplnění podnikové mise a cílů

- EDM05 Zajištění transparence pro zainteresované strany – zajišťuje transparentní, komplexní, včasné a přesné monitorování a reporting výkonnosti a souladu podnikového IT, efektivní a včasné informování zainteresovaných stran a definování schvalovacích procedur pro stanovení výkonnostních cílů, metrik a potřebných nápravných opatření příslušnými zainteresovanými stranami
- APO01 Řízení rámce pro IT management – poskytuje konzistentní přístup k naplnění požadavků, mise a vize IT governance prostřednictvím souboru procesů, organizačních struktur, rolí, odpovědností, aktivit, zkušeností a kompetencí
- APO07 Řízení lidských zdrojů – zajištění optimální organizační struktury, vytvoření rolí, přidělení pravomocí a rozhodovacích práv, rozvoj znalostí a motivování lidí k naplňování byznys cílů. Důležitou procesní praktikou je APO07.06 Řízení zaměstnanců, v jejichž odpovědnosti je řízení dohod o službách
- APO08 Řízení vztahů – formalizované a transparentní zajištění dosažení společných cílů při omezeném rozpočtu, stanovené hranici tolerance rizika, daném čase a vysokém stupni důvěry. Procesními praktikami jsou porozumění byznys požadavků, identifikace příležitostí, rizik a omezení, řízení vztahů, koordinace a komunikování a poskytnutí dat pro kontinuální zlepšování služeb
- APO11 Řízení kvality – definování a komunikování kvalitativních požadavků, kontrol, metrik a monitorování těchto metrik s cílem zajistit, že dodávané služby jsou v souladu s kvalitativními požadavky byznysu a uspokojují potřeby zainteresovaných stran
- BAI02 Řízení definice požadavků – analýza byznys funkčních a technických požadavků na IT řešení s cílem zajistit, že IT řešení je v souladu s byznys strategií, porovnání variant hodnocení IT řešení ve vztahu k nákladům, přínosům, rizikům a výběr optimální varianty odpovídající potřebám byznysu

4.3 ITIL

Information Technology Infrastructure Library (ITIL) je standardizovaná metodologie nejlepších zkušeností z praxe pro řízení IT služeb. ITIL je vytvořen formou souboru nezávazných doporučení vycházejících z nejlepších zkušeností z praxe IT, kdy si každý podnik při implementaci ITIL může podle svých individuálních potřeb zvolit k realizaci pouze ta doporučení, která jsou pro něj optimální. ITIL poskytuje praktiky, na jejichž základě je možno vytvořit a realizovat IT Service Management (ITSM) pro řízení životního cyklu IT služeb (The Cabinet Office, 2011). Cílem implementace ITSM je dosažení průběžně se opakujícího cyklu zkvalitnění IT služeb při minimálních nákladech a realizace přínosů z jejich využití. ITSM je postaven na procesně orientovaném přístupu. Nejnovější verze ITIL publikovaná v roce 2011 se sestává z pěti publikací, které odrážejí jednotlivé fáze životního cyklu IT služby a obsahují klíčové principy, procesy a aktivity, role, technologie a s nimi spojené výzvy a rizika. Těmito publikacemi jsou (The Cabinet Office, 2011):

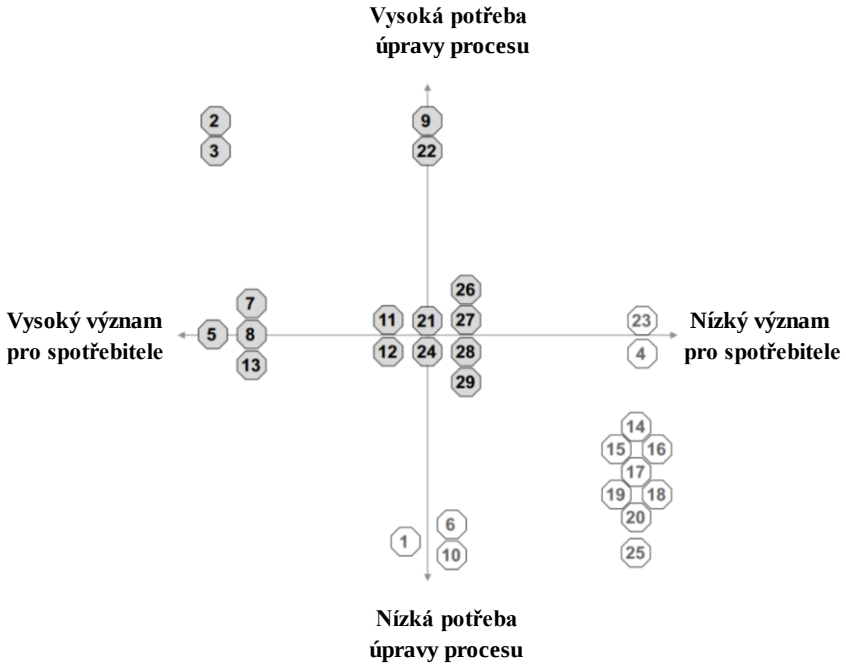
- Service Strategy,
- Service Design,
- Service Transition,
- Service Operation,
- Continual Service Improvement.

ITIL je považován jako de-facto standard pro řízení IT služeb. Nezabývá se však specifiky a způsoby využívání konkrétních služeb od konkrétních poskytovatelů a ani technickými detaily služeb, ale zaměřuje se na poskytnutí rámce, který strukturuje aktivity související s řízením IT služeb do

jednotlivých procesů (Sun, a další, 2010). Podobné vlastnosti IT služeb a služeb cloud computingu a téměř shodný životní cyklus předurčují ITIL jako vhodný nástroj pro podporu rozhodnutí nezbytných pro přijetí a využívání služeb cloud computingu. Ale stávající procesy ITIL plně nepodporují prostředí využívání služeb cloud computingu a neumožnují plně realizovat očekávané benefity (Mourad, a další, 2014). ITIL není explicitně adresován pro řízení služeb cloud computingu z pohledu spotřebitele, spotřebitel může procesy ITSM přizpůsobit prostředí cloud computingu tak, aby byl optimálně připraven na celý životní cyklus služby cloud computingu od rozhodnutí o jejím přijetí, přes využívání této služby až po ukončení smluvního vztahu s poskytovatelem služby cloud computingu (Robrecht, a další, 2014). Ačkoliv je cloud computing v posledních letech široce přijatým trendem v poskytování a využívání IT zdrojů, aktuální přepracované vydání ITIL z roku 2011 neobsahuje jasné zaměření a zpřesnění problematiky řízení služeb cloud computingu a omezuje se pouze na dílčí aspekty prostředí cloud computingu, a to i přes identifikaci potřeby o jeho přepracování z hlediska řízení služeb cloud computingu řadou vědeckých publikací (Heininger, a další, 2012). Nejpodstatnější obsah související s cloud computingem lze nalézt v publikaci Service Strategy, která navíc v dodatku C pojednává o charakteristikách služeb cloud computingu, modelech služeb, modelech nasazení a komponentách architektury služeb cloud computingu, kterými jsou katalog služeb a portál pro přístup ke službám, governance služeb cloud computingu, management dodávky služeb cloud computingu a infrastruktura pro provoz a poskytování služeb cloud computingu. Na tyto komponenty stejně jako na ostatní obsah je však nahlíženo z pohledu poskytovatele služeb cloud computingu.

ITIL se primárně zaměřuje na způsob, jak by procesy a procedury měly být navržené a soustředí se na způsob, jak plánovat, navrhovat a implementovat efektivní procesy řízení IT služeb tak, aby IT služby plně podporovaly byznys procesy v souladu s potřebami byznysu a aby se podnikové IT stalo strategickou výhodou organizace. ITIL je orientovaný zejména na IT organizace či IT oddělení, jejichž hlavní činností je poskytovat IT služby pro podporu byznysu, a které tedy vystupují v roli tvůrce, vlastníka a poskytovatele IT služeb. To se odráží i v životním cyklu IT služeb, kdy ITIL explicitně nerozlišuje poskytovatele a spotřebitele služby a předpokládá, že IT služby jsou navržené, vyvinuté, poskytované a optimalizované stejnou organizací, která využívá služby pro provoz on-premise podnikových informačních systémů a aplikací, a proto je často v procesech zohledňována perspektiva poskytovatele služeb. Tím, že ITIL není primárně určený pro prostředí cloud computingu a ani pro řízení služeb cloud computingu spotřebitelem, je nutné ITIL přizpůsobit nebo rozšířit tak aby reflektoval specifika prostředí využívání služeb cloud computingu. Řízení služeb cloud computingu z pohledu spotřebitele vyžaduje přizpůsobení nebo rozšíření procesů ITIL v závislosti na modelu nasazení služeb cloud computingu a na rozsahu jejich využití (Pröhl, a další, 2012). Z pohledu spotřebitele služeb cloud computingu ustupují do pozadí procesy související s návrhem služby a zvýrazňují se zejména procesy související se strategickým rozhodováním o využívání služby a procesy související s využíváním a provozováním služby. Problémem je, že většina vědeckých publikací se nezabývá řízením služeb cloud computingu jako celkem, ale zabývá se pouze individuálními aspekty řízení služeb cloud computingu na různých úrovních detailu, které nejčastěji souvisí s návrhem služeb (např. řízení informační bezpečnosti) (Heininger, a další, 2012), se strategickými aspekty (Pröhl, a další, 2012) jako je řízení rizik, finanční řízení nebo optimalizace výběru poskytovatele a jen některé vědecké publikace se zabývají provozními aspekty jako je monitorování služeb cloud computingu nebo incident management. Nebyla nalezena žádná vědecká publikace, která by se zabývala neustálým zlepšování služeb cloud computingu, a to i přes to, že Pröhl (2012) označuje tuto fázi za vysoce důležitou v kontextu spotřebitele služeb cloud computingu. Pröhl (2012) identifikoval procesy definované v ITIL z hlediska jejich významu pro spotřebitele

služeb cloud computingu a z hlediska potenciální nutnosti upravit proces tak, aby lépe vyhovoval prostředí cloud computingu. Tyto procesy jsou zvýrazněné na následujícím Obrázku 13.



Service Strategy	
1	Strategy Management
2	Service Portfolio Management
3	Financial Management
4	Demand Management
5	Business Relationship Management

Service Design	
6	Design Coordination
7	Service Catalogue Management
8	Service Level Management
9	Capacity Management
10	Availability Management
11	IT-Service Continuity Management
12	Information Security Management
13	Supplier Management

Service Transition	
14	Change Management
15	Change Evaluation
16	Transition Planning & Support
17	Release & Deployment Management
18	Service Validation & Testing
19	Service Asset & Configuration Mgmt.
20	Knowledge Management

Service Operation	
21	Event Management
22	Incident Management
23	Request Fulfilment
24	Access Management
25	Problem Management

CSI	
26	Service Review
27	Process Evaluation
28	Definition of CSI Initiatives
29	Monitoring of CSI Initiatives

Obrázek 13: Portfolio ITIL procesů z hlediska významu pro cloud computing management, zdroj: (Pröhl, a další, 2012)

Robrecht (2014) na základě analýzy literatury stanovil kroky životního cyklu služby cloud computingu z pohledu spotřebitele, které namapoval na procesy ITIL (viz Tabulka 4) (Robrecht, a další, 2014).

Tabulka 4: Kroky životního cyklu služby cloud computingu z pohledu spotřebitele mapované na procesy ITIL, zdroj: (Robrecht, a další, 2014)

	Service Strategy					Service Design								Service Transition							Service Operation					CSI
R - responsible C - consulted	Strategy Management	Service Portfolio Management	Financial Management	Demand Management	Business Relationship Management	Design Coordination	Service Catalogue Management	Service Level Management	Availability Management	Capacity Management	IT-Service Continuity Management	Information Security Management	Supplier Management	Transition Planning & Support	Change Management	Service Asset & Configuration Mgmt.	Release & Deployment Management	Service Validation & Testing	Change Evaluation	Knowledge Management	Event Management	Incident Management	Request Fulfilment	Problem Management	Access Management	7-Step Improvement Process
Rozhodnutí o adopci služby cloud computingu	R		C	R	C																					R
Navržení portfolia služeb cloud computingu	C	R	C	C	C	C	C	C	C	C	C	C	C			C										
Výběr poskytovatele a služby veřejného cloud computingu	C	R	C			C	C	C	C	C	C	C	C		C	C										
Návrh a uzavření smluv o využívání služby cloud computingu			C			C	C	R	C	C	C	C	R													
Zavedení služby cloud computingu do produktivního provozu							C				C	C		C	R	C	C	C	C	C						
Hodnocení produktivního provozu služby cloud computingu			C		C			C	C	C	C	C	R								C	C	C	C	C	R
Řešení požadavků a incidentů v souvislosti s provozem služby cloud computingu															R							R	C	C	C	
Řešení závažných incidentů v souvislosti se službou cloud computingu											R	C	C		C						C	C				
Změna posyktovatele / návrat k on-premise řešení	C	R	C			C	C	C	C	C	C	C	R		C	C										R

4.3.1 Strategie služeb

Rozhodnutí o využívání jedné nebo více služeb cloud computingu musí vyplývat z byznys strategie, musí být podloženo finančními a nefinančními benefity, které má využití služeb cloud computingu přinést. Rizika by neměla převážit tyto benefity. Strategická rozhodnutí týkající se IT služeb, a tedy využívání služeb cloud computingu vyplývají z fáze Strategie služeb (Service Strategy). Strategie služeb je v ITIL pojímána jako centrální fáze. Procesy této fáze se zabývají strategickými rozhodnutími týkající se návrhu a provozování IT služeb v souladu s potřebami spotřebitelů při minimalizaci nákladů na provoz služeb. Proces *Strategické řízení IT služeb* definuje a spravuje strategické plány vzhledem potřebám a požadavkům organizace týkajících se IT služeb a zajišťuje naplnění strategie IT služeb. Ačkoliv se celá publikace zaměřuje na poskytovatele služeb, lze proces modifikovat tak, aby byl aplikovatelný z hlediska spotřebitele do prostředí využívání služeb cloud computingu. Jelikož IT strategie je podmnožinou celkové byznys strategie, lze z této skutečnosti odvodit, že cloud computing strategie bude podmnožinou IT strategie a bude v souladu s podnikovou strategií. Rozsah cloud computing strategie bude vycházet z rozsahu IT strategie dle ITIL, ale bude přizpůsoben potřebám spotřebitele. Cílem procesu je jasné vymezení způsobu, jakým poskytovatel služeb umožní organizaci dosáhnout očekávaných výstupů, což lze aplikovat i do prostředí využívání

služeb cloud computingu, kdy spotřebitel vyžaduje skrz využití služeb cloud computingu poskytovaných externím poskytovatelem dosažení očekávaných benefitů vyplývajících z požadavků zainteresovaných stran a potřeb byznys procesů. Proces Strategické řízení IT služeb napomáhá stanovit kritéria a mechanismy, které podporují rozhodování o výběru služeb z hlediska jejich vhodnosti, efektivnosti a účinnosti. V tomto případě se jedná o rozhodování o využití IT služeb v modelu veřejného cloud computingu, o vyčlenění byznys procesu vhodného z hlediska podpory službou cloud computingu a o hodnocení dat, se kterými tento proces pracuje z hlediska jejich významnosti pro organizaci. Součástí je posouzení interních schopností a kapacit pro přijetí služeb cloud computingu a provedení externí analýzy, kdy v případě služeb veřejného cloud computingu vystupuje do popředí analýza legislativního prostředí. Jakmile je strategie pro využívání služeb cloud computingu definovaná, proces Strategické řízení IT služeb je dále zodpovědný za zajištění provádění strategie. Jednotlivé procesní aktivity vychází ze zásad strategického řízení a z tvorby podnikové strategie a i přesto, že procesní aktivity definované v ITIL nejsou určeny pro spotřebitele služeb cloud computingu, lze je využít právě i v případě, že organizace spotřebitele zvolí cloud computing jako jeden z modelů sourcingu IT služeb. Účelem procesu *Řízení portfolia služeb* je dle ITIL zajistit, že poskytovatel služeb má v souladu s IT strategií správný soubor služeb, kdy investice do těchto IT služeb nepřevýší byznys hodnotu, kterou jsou tyto služby schopné vygenerovat. Portfolio služeb popisuje služby nově navržené a připravené na vývoj, služby ve vývoji a služby připravené pro nasazení do produktivního provozu obsažené ve frontě služeb v tzv. service pipeline, služby v produktivním provozu obsažené v katalogu služeb a také služby vyřazené z produktivního provozu a jinak nevhodné služby pro produktivní provoz. V případě spotřebitele služeb cloud computingu by portfolio služeb mělo obsahovat soubor všech potenciálně přípustných služeb pro budoucí využití poskytovaných schváleným portfoliem poskytovatelů a aktuálně využívaných služeb, které jsou schopné přispět k tvorbě byznys hodnoty, a dále služby které byly z využívání vyřazeny včetně důvodu jejich vyřazení. Portfolio služeb napomáhá řídit životní cyklus služeb. Jako hlavní nástroj pro řízení životního cyklu služby se používá katalog služeb, který ITIL definuje ve fázi návrhu služby. Proces Řízení portfolia služeb se skládá z procesní aktivity, která prochází několika fázemi. Nejprve musí být zdokumentován byznys případ pro každou existující nebo novou službu, musí být definováno s jakými daty služba pracuje, jaká aktiva služba pro svůj provoz vyžaduje a jaká je potřebná výše investice do vytvoření a provozu služby. Následně je provedena analýza služeb v portfoliu z hlediska optimalizace hodnoty a každá služba musí být schválena a musí být zajištěny dostatečné zdroje pro zabezpečení očekávané úrovně služeb požadované zákazníky. V poslední fázi je odsouhlasena zakládající listina projektu vytvoření nové služby nebo změny stávající služby relevantními zainteresovanými stranami. V případě spotřebitele služby cloud computingu nelze tuto procesní aktivitu plně realizovat. Nejprve musí být pro různé scénáře přijetí a využívání služby cloud computingu taktéž vytvořen byznys případ, který se však bude lišit na základě účelu, za jakým je vypracováván. Byznys případ musí poskytnout objektivní zdůvodnění pro přijetí služby cloud computingu. Dále musí obsahovat způsobu řešení konkrétního problému přijetím této služby včetně porovnání alternativního řešení ve smyslu jiné služby či on-premise řešení. Byznys případ musí vycházet z požadavků cloud computing strategie a musí specifikovat, jak budou tyto požadavky naplněny prostřednictvím služby cloud computingu. Každá služba cloud computingu v portfoliu služeb musí být zdokumentovaná a schválená, musí být propojena s příslušnými smlouvami o poskytování služeb a musí být alokované potřebné množství infrastrukturních zdrojů. Finančními zdroji ve vztahu k řízení IT služeb a zajištěním rovnováhy mezi cenou a kvalitou služeb se zabývá proces *Finanční řízení pro IT služby*. Základní principy procesu finanční řízení pro IT služby se v případě spotřebitele služeb cloud computingu nemění, mění se však účel a rozsah procesu, a to zejména díky odlišnému životnímu cyklu služby cloud computingu z pohledu spotřebitele a IT služby dle ITIL a faktu, že účtování služeb je založeno na objemu aktuální spotřeby služby cloud computingu

postavené na modelu pay-as-you-go. Na rozdíl od ITILu není v prostředí využívání služeb cloud computingu účelem zajistit odpovídající úroveň financování při návrhu, vývoji a dodávce služeb, které splňují potřeby strategie organizace, ale zajistit odpovídající úroveň financování při výběru, získání, nasazení, využívání a při ukončení využívání služby cloud computingu a při migraci k jinému poskytovateli či k jinému řešení. Další odlišnost je v základních procesech finančního řízení. ITIL je definuje jako rozpočtování, účetnictví a účtování. Z pohledu spotřebitele se však v případě procesu účtování nejedná o účtování za poskytované služby ale o fakturaci využívaných služeb v závislosti na modelu účtování poskytovatele formou předplatného dle objemu spotřeby služby cloud computingu. Procesy rozpočtování a účetnictví zůstávají platné, avšak jednotlivé aktivity a výpočty ukazatelů je nutné přizpůsobit tak, aby odrážely specifika finančního řízení služeb cloud computingu. Proces Finanční řízení pro IT služby musí poskytovat nezbytné informace pro rozhodování využívání služeb cloud computingu z hlediska jejich nákladové efektivnosti včetně jejich porovnání s alternativními službami cloud computingu anebo s tradičním řešením IT. Proces *Řízení poptávky* se v prostředí řízení služeb cloud computingu z pohledu spotřebitele neaplikuje, neboť cílem tohoto procesu je pochopit, předvídat a ovlivňovat poptávku po nabízených službách a z pohledu poskytovatele zajistit potřebné kapacity pro dodání požadovaného objemu služeb. Poslední proces fáze strategie služeb *Řízení obchodních vztahů* se zaměřuje z pohledu poskytovatele IT služeb na vytvoření a udržování obchodních vztahů se spotřebitelem IT služeb založených na porozumění byznys potřeb spotřebitelů a na uspokojení jejich požadavků dodáním optimálního souboru služeb na předem dohodnuté úrovni těchto služeb. Z pohledu spotřebitele služeb cloud computingu by se naopak jednalo o řízení vztahů mezi ním a poskytovatelem služeb cloud computingu, o neustálé vyhodnocování poskytovatele a jeho schopnosti uspokojit požadavky spotřebitele dodávkou služeb cloud computingu v souladu s dohodami o službách cloud computingu. Proces Řízení obchodních vztahů se podílí na definici a vyjasnění požadavků na poskytovatele a na služby cloud computingu, které vychází z požadavků byznysu, z definice cloud computing strategie a jednotlivých strategických plánů. To zahrnuje identifikaci byznys potřeby týkající se využití služby cloud computingu a příležitostí k efektivnější podpoře byznys procesů a definování byznys případu ve spolupráci s procesem Řízení portfolia služeb. Z pohledu spotřebitele služeb cloud computingu by měl proces Řízení obchodních vztahů zajistit, že vybraní poskytovatelé a jimi poskytované služby cloud computingu v optimální míře splňují požadavky byznysu a cloud computing strategie. Dále by měl identifikovat změny byznys potřeb, které by mohly mít potenciálně dopad na rozsah využívání služeb cloud computingu, na typ služby či na úroveň poskytované služby cloud computingu a formulovat požadavky na změnu služby nebo na změnu kvalitativních parametrů služby cloud computingu.

4.3.2 Návrh služby

Fáze Návrh služby (Service Design) se zaměřuje na návrh a vývoj IT služeb tak, aby v souladu s IT strategií poskytovatele uspokojovaly byznys požadavky spotřebitelů, byla zajištěna optimální úroveň kvality těchto služeb a provoz služeb byl nákladově efektivní. Většina procesů této fáze je plně v kompetenci poskytovatele služeb a z pohledu spotřebitele se při řízení služeb cloud computingu neaplikují. Podstatným procesem z hlediska spotřebitele služeb cloud computingu je proces *Řízení katalogu služeb*, který má za cíl zajistit, že v podniku existuje a je průběžně udržován katalog služeb a že katalog služeb obsahuje přesné a aktuální informace o všech aktuálně využívaných službách a o alternativních službách od předem schválených poskytovatelů. Katalog služeb definovaný v ITIL se dělí na dvě části, a to katalog byznys/zákaznických služeb a katalog technických/podpůrných služeb. Katalog byznys/zákaznických služeb obsahuje detailní dokumentaci služby z pohledu uživatele a ve vztahu k příslušným obchodním procesům. Katalog technických/podpůrných služeb obsahuje detailní dokumentaci služby ve vztahu k podpůrným službám, sdíleným službám, hardwarovým nebo

softwarovým komponentům potřebných pro produktivní provoz služby. Katalog služeb v prostředí cloud computingu může být realizován jako statický katalog služeb založený na souboru dokumentů nebo jako interaktivní internetová aplikace vybavená na pozadí vysokým stupněm automatizace. Z hlediska spotřebitele by měl takto automatizovaný katalog služeb poskytovat informace o všech službách, které poskytovatel služeb poskytuje spotřebitelům k realizaci jejich byznys procesů včetně poskytovaných úrovní služeb a parametrů a atributů služeb. Katalog služeb v tomto případě slouží jako závazný standard. To znamená, že jak samotné služby uvedené v katalogu služeb, tak jejich definice a popis v katalogu služeb musí zcela závazně odpovídat skutečnosti. Dalším důležitým faktorem vysoce automatizovaného katalogu služeb je to, že každý uživatel pracující se katalogem služeb je plně identifikován svými přihlašovacími údaji a na základě smlouvy mezi poskytovatelem a spotřebitelem má definovanou oblast oprávnění určující, které údaje z katalogu služeb má mít k dispozici a jaké činnosti s nimi může provádět. Například jaký pohled na data v katalogu služeb má uživatel k dispozici nebo o jaký druh služeb, respektive jaké úrovně služeb může daný uživatel přímo interaktivně definovat k aktivaci. K tomu má spotřebitel obvykle i možnost, aby v návaznosti na potřebu změny byznys procesů vytvořil pomocí funkce katalogu služeb žádost o rozšíření nebo změnu některé služby. Druhým významným procesem fáze návrhu služby je *Řízení úrovně služeb*, který je zodpovědný za definice a popis hodnot úrovně kvality, které mají služby minimálně dosáhnout a za zajištění, že dodávané služby budou dosahovat dohodnuté úrovně. Proces zahrnuje určení, vyjednávání, dokumentování a odsouhlasení požadavků na nastavení úrovně nové nebo změněné služby. Zároveň tento proces definuje monitorování hodnot úrovně služeb, sleduje skutečně dosažené hodnoty úrovně služby a tyto hodnoty porovnává s příslušnými dohodami za účelem zjištění, zda služba splňuje nebo nesplňuje příslušnou dohodu. Dohody o úrovni služeb SLA slouží jako nástroj garance úrovně poskytované služby a zajišťují úplnou specifikaci hodnot úrovní služeb. V prostředí využití služeb cloud computingu se tento proces omezuje pouze na několik dílčích aktivit. Spotřebitel v modelu veřejného cloud computingu nemá možnost navrhovat kvalitativní parametry úrovně služby, může pouze s poskytovatelem vyjednávat hodnoty cílové úrovně dodávané služby, jejichž odsouhlasení obě strany stvrdí v dohodě SLA. V určitých případech, zejména při silné vyjednávací pozici může spotřebitel svojí poptávkou ovlivnit poskytovatele při návrhu nové nebo změněné služby. V ostatních případech však musí spotřebitel vybrat alternativní službu, která lépe splňuje jeho požadavky. Řízení úrovně služeb z pohledu spotřebitele služeb cloud computingu pokrývá kroky životního cyklu SLA, které se skládají z vyjednávaní podmínek uzavření, dokumentování a odsouhlasení SLA, monitorování výkonnosti poskytované služby z hlediska souladu s SLA, reportování o výkonnosti poskytované služby, řešení problémů provozu služby a přijímání nápravných opatření, ukončení využívání služby a hodnocení SLA.

Proces *Řízení bezpečnosti informací* realizuje činnosti související se řízením a správou informačních aktiv a zajišťuje, že rizika bezpečnosti informací jsou vhodně a nákladově efektivně řízena. Proces zabezpečuje vytvoření, udržování, komunikování a prosazování politiky bezpečnosti informací, která pokrývá všechny IT systémy a IT služby. V širším kontextu to znamená, že by politika bezpečnosti informací měla pokrývat také využívání služeb cloud computingu. Řízení bezpečnosti informací vyžaduje pochopení bezpečnostních požadavků na zabezpečení realizace byznys procesů, legislativních a regulativních požadavků a bezpečnostních požadavků vyplývajících z SLA. Tedy oblasti vysoce důležité i v prostředí cloud computingu, kdy efektivní řízení bezpečnosti informací je navíc podmíněno bezpečností politikou poskytovatele. Proces řízení bezpečnosti informací realizuje implementaci souboru bezpečnostních kontrol, které podporují prosazování politiky bezpečnosti informací a řídí rizika spojená s prací s IT službami, IT systémy a s informacemi, které zpracovávají. ITIL se zaměřuje na definici politiky bezpečnosti informací pro tradiční IT služby a IT systémy, a tudíž nezohledňuje specifika vyplývající z prostředí cloud computingu, o které je potřeba politiku

bezpečnosti informací rozšířit. Avšak v posledních letech vznikla řada publikací zaměřených na řízení bezpečnosti informací z hlediska spotřebitele (Ahmad, a další, 2011) a všeobecně akceptovaných norem jako je Cloud Controls Matrix (CCM) publikovaný společností The Cloud Security Alliance (CSA), který poskytuje kontrolní rámec pokrývající bezpečností domény prostředí cloud computingu, anebo norma ISO/IEC 27017:2015, která je zaměřená na řízení bezpečnosti informací v prostředí cloud computingu. Obě normy zohledňují aplikace bezpečnostních kontrol z pohledu spotřebitele služeb cloud computingu. ITIL pro dosažení cílů řízení bezpečnosti informací vyžaduje implementaci metod řízení rizik tak, aby riziko související se zpracováním informací a s bezpečností informací bylo na přijatelné úrovni. Způsob řízení rizik v prostředí cloud computingu ITIL nespecifikuje.

4.3.3 Přechod služby do produktivního provozu

V porovnání s tradičními IT službami je přechod na využívání služeb cloud computingu méně komplexní a časově náročný, což se odráží ve zkrácení doby životního cyklu služeb cloud computingu. Důležitým faktorem přechodu však nadále zůstává zvládnutí všech integračních úloh, nastavení nových rozhraní, upravení byznys procesů, modifikace organizačních rolí, testování a nasazení do produktivního provozu. To vyžaduje sdílenou odpovědnost mezi spotřebitelem a poskytovatelem služeb cloud computingu včetně určení odpovědností. Fáze přechodu by také měla zahrnovat přechod k jinému poskytovateli služeb včetně migrace dat mezi poskytovateli. Během počáteční adopce bude nutné držet se tradičních metod projektového řízení a efektivně plánovat a koordinovat zdroje potřebné pro přechod na vyžívání služby cloud computingu. ITIL ve fázi Přechod služby do produktivního provozu (Service Transition) pro tento účel definuje proces *Plánování a podpora přechodu*. Procesní aktivity je možné po jejich přizpůsobení plně aplikovat do prostředí cloud computingu, avšak fáze přechodu se v při řízení služeb cloud computingu liší od fází přechodu pro IT služby ve skutečnosti, že služby cloud computingu jsou plně ve vlastnictví a odpovědnosti poskytovatele, který se stará o jejich vytvoření, testování a zajištění potřebných zdrojů pro jejich provoz a poskytování a na spotřebiteli leží odpovědnost za připravení vlastního provozního prostředí, dat určených pro migraci, testování, nasazení do produktivního provozu a zabezpečení provozu služby cloud computingu v rané fázi. Na proces Plánování a podpora přechodu v prostředí využívání služeb cloud computingu navazuje proces *Validace a testování služeb*. Tento proces má za úkol naplánovat a realizovat validační a testovací procedury, které umožní prokázat, že nová nebo změněná IT služba je v souladu s IT strategií, podporuje byznys potřeby spotřebitelů a funguje spolehlivě a bez chyb v její funkcionalitě. Pro spotřebitele služeb cloud computingu to navíc znamená, že služba je dodávaná a využívaná s ohledem na příslušná ustanovení v platných dohodách či v SLA. Během testování jsou identifikovány všechny chyby, nedostatky nebo rizikové situace spojené s novou službou a všechny relevantní informace jsou komunikovány příslušným zainteresovaným stranám. Plánování a řízení jednotlivých verzí, sestavení IT služeb, testování a nasazení uvolnění do produktivního provozu realizuje proces *Řízení verzí a nasazení do produktivního provozu*. Tento proces odpovídá za dodávku služeb požadovaných spotřebitelem a má zajistit integritu jednotlivých komponent jak verzí, tak výsledných služeb v produktivním nasazení. Takto definovaný proces odpovídá perspektivě poskytovatele. V prostředí řízení využívání služeb cloud computingu je však vyžadován výrazný posun ve vnímání aktivit souvisejících s nasazení služby do produktivního provozu. Na straně poskytovatele je služba již ve fázi produktivního provozu, je poskytována a dodávána velkému množství spotřebitelů, je monitorována, vyhodnocována a řízena z hlediska její výkonnosti. Z pohledu spotřebitele služby nasazení do produktivního provozu znamená provedení importu dat do produktivního prostředí poskytovatele služby, vytvoření účtů a oprávnění pro přístup ke službě, integrace služby do provozního prostředí spotřebitele, akceptační testování, zahájení dodávky a využívání služby a aktivace procesů řízení

provozu služby dle plánů realizace přechodu služby cloud computingu do produktivního provozu. Procesní aktivity se tedy omezí pouze na vytvoření plánů, testování a nasazení služby do produktivního provozu a hodnocení úspěšnosti nasazení služby. Postupy vyřazení služby z provozu by měly být součástí exit strategie, a to včetně identifikace dat, licencí a jiných aktiv, které ukončení využívání služby ovlivní. Je velice důležité specifikovat jednotlivé kroky v součinnosti s poskytovatelem služby cloud computingu o způsobu, technické a časové realizovatelnosti exportu dat a o maximálním časovém horizontu, do kdy budou zálohy dat k dispozici u poskytovatele před jejich úplným vymazáním a odstraněním veškerých souvisejících dat ze systémů poskytovatele. Podmínky ukončení využívání služby cloud computingu podléhají smluvním ustanovením v dohodách uzavřených mezi poskytovatelem a spotřebitelem. Ostatní procesy fáze přechodu služby do produktivního provozu definované v ITIL, kterými jsou *Řízení změn*, *Řízení aktiv a konfigurace služeb* a *Hodnocení změn*, jsou určeny specificky pro poskytovatele IT služeb. Řízení znalostí v organizaci spotřebitele vychází z procesu *Řízení znalostí* dle ITIL, řízení znalostí mezi spotřebitelem a poskytovatelem se řídí příslušnými dohodami a předem definovanými komunikačními rozhraními.

4.3.4 Provoz služby

Fáze Provoz služby (Service Operation) zabezpečuje optimalizaci produktivního provozu služby z hlediska její funkcionality, výkonnosti a potřebných kapacit pro efektivní provoz v souladu s IT strategií a potřebami byznysu. Data o provozu služby získané ve fázi produktivního provozu služby slouží jako základ pro objektivní hodnocení provozované služby a jako impuls pro zahájení procesu zlepšování kvality služby. Účelem fáze produktivního provozu služby v prostředí cloud computingu je koordinovat a provádět aktivity potřebné k bezproblémovému využívání služeb oprávněnými osobami v rámci dohodnutých úrovní kvality služeb. Tyto aktivity zabezpečují sledování výkonnosti služeb, hodnotí metriky a shromažďují data o provozu služeb, což umožnuje detekovat hrozby ovlivňující kvalitu služeb a minimalizovat dopad na byznys v případě nedodání smluvně dohodnuté úrovně služby. Všechny události, které se vyskytnou při provozu služby, jsou řízeny procesem *Řízení událostí*. Cílem tohoto procesu je monitorovat události způsobující odchylku od normálního stavu nebo od SLA, které mají význam pro řízení IT služeb, pro detekované události určit příslušné řídící akce a událost definovaným způsobem eskalovat. Data shromážděná procesem jsou důležitým základem pro hodnocení služby v rámci procesu nepřetržitého zdokonalování služby. Důležitou vlastností procesu řízení událostí je i eskalace toho, že služba s detekovanou výjimkou se navrátila ke své normálně očekávané funkcionalitě. V souvislosti s řízením využívání služby cloud computingu je cílem procesu mít vždy aktuální informace o stavu dodávky služby identifikací a vyhodnocením událostí vznikajících během produktivního provozu služby cloud computingu v podniku spotřebitele. Procesní aktivity definované v ITILu je nutné přizpůsobit o zohlednění událostí, které se týkají poskytovatele služby cloud computingu. Eskalace detekovaných událostí se následně bude řídit smluvními podmínkami. Řešení odchylek od požadovaného stavu hodnot parametrů služby cloud computingu, od hodnot parametrů definovaných v SLA a odchylek od normálního stavu služby musí i v případě procesu *Řízení incidentů* odrážet nutné aktivity řešení incidentů vzniklých jak na straně spotřebitele služby cloud computingu, tak i incidentů vzniklých na straně poskytovatele služby cloud computingu. Incident je považován za událost, která není součást standardního provozu a využívání služeb cloud computingu a narušuje nebo snižuje kvalitu služby. Cílem procesu Řízení incidentů je obnovit normální provoz po narušení co nejrychleji, s co nejmenším možným dopadem na byznys a při co nejnižších nákladech. Základem je stejně jako v ITILu identifikace incidentu a vytvoření záznamu o incidentu identifikovaného prostřednictvím různých kanálů, kategorizace incidentu a prvotní analýza příčin vzniku incidentu, která určí, zda příčina narušení očekávaného stavu služby je na straně poskytovatele služby cloud computingu nebo na straně

spotřebitele. V případě, že servis desk spotřebitele není schopen nebo oprávněn vyřešit incident, musí být incident eskalován na odborné pracoviště poskytovatele dle sjednané dohody. Řešení incidentů je realizováno pouze v případě, že příčina narušení provozu služby cloud computingu je na straně spotřebitele. V případě, že příčina narušení leží na straně poskytovatele, je incident předán na servis desk poskytovatele nebo na jiný dohodnutý jednotný kontaktní bod. Informace o řešení incidentu musí být následně vrácena zpět na servis desk spotřebitele, který vytvořil tiket k příslušnému incidentu, a ten incident uzavře. Pravidla eskalace, komunikace a řešení incidentů musí probíhat vždy podle smluvních podmínek uzavřených v dohodách o poskytování služeb cloud computingu. Proces vytváří podklady pro řízení problémů. Proces *Řízení problémů* se aplikuje pouze v případě, že příčina výskytu incidentu je na straně spotřebitele. Poté se uplatní všechny procesní aktivity přizpůsobené pro dané provozní prostředí spotřebitele služeb cloud computingu, a to od detekce problému, analýzy důvodu jeho vzniku, odstranění příčiny vzniku problému na základě již dříve provedené podrobné analýzy, nalezení řešení dosud neznámého problému, jeho dokumentace a uzavření problému. Proces *Plnění požadavků* zajišťuje realizaci požadavků uživatelů na funkčnost služby v podobě malých nevýznamných a často standardizovaných provozních změn s nízkou mírou rizika jak pro provoz služby, tak pro organizaci, jejichž provedení je časově nenáročné a je realizovatelné s nízkými náklady. V prostředí využívání služeb cloud computingu se tento proces aplikuje s přihlédnutím na specifika prostředí, kdy služby cloud computingu jsou plně pod kontrolou poskytovatele a uživatel často nemá na tyto změny oprávnění, což vychází nejen z politik organizace spotřebitele ale i z pravomocí, ke kterým opravňuje poskytovatel služby cloud computingu spotřebitele. V tomto případě je realizace jednotlivých procesních aktivit podřízena smluvně dohodnutým podmínkám mezi poskytovatelem a spotřebitelem služby cloud computingu. Požadavky na změnu na rozsah služeb či na změnu parametrů služeb cloud computingu jsou často adresovány přes servis desk nebo přes servisní portál oprávněnou osobou spotřebitele, kterou si může spotřebitel sám definovat v rámci nastavení na servisním portálu. Na jednotný servisní portál poskytovatele je pohlíženo jako na nástroj pro automatizaci rutinních činností při řízení služeb cloud computingu, který umožnuje měnit nastavení služby a rychle ji tak přizpůsobit aktuálním potřebám. Přidělováním oprávnění uživatelům přistupovat ke službě a řízením identit se zabývá proces *Řízení přístupu*. Proces zajišťuje, aby oprávnění uživatelé měli přidělena přístupová práva k provádění určitých operací se službami a mohli tak ke službě přistupovat a se službou pracovat a zároveň, aby byl odepřen přístup ke službě všem subjektům, kteří nemají oprávnění ke službě přistupovat a vykonávat požadovanou operaci. Spotřebitel služeb cloud computingu vyjednává požadavky na přístup ke službě cloud computingu v součinnosti s poskytovatelem. Pro spotřebitele je pro danou službu typicky vytvořena role administrátora. Ze strany poskytovatele jsou v mnoha případech dostupné odpovídající nástroje pro řízení identit a přístupu ke službě cloud computingu, kde administrátor spotřebitele má možnost nastavit role a přístupová oprávnění jednotlivým uživatelům organizace, avšak nemá právo, jakkoliv technicky zasahovat do poskytované služby. V tomto případě je možné aplikovat procesní aktivity dle ITIL tak, aby proces řízení přístupu v prostředí využívání služeb cloud computingu primárně zajistil, aby uživatel spotřebitele měl přístup ke službě cloud computingu, měl oprávnění pouze k vykonávání určitých operací související s jeho pracovním zařazením a aby k požadovaným funkcionalitám služby cloud computingu mohli přistupovat také externí koncoví uživatelé přistupující často prostřednictvím vnějšího webového rozhraní.

4.3.5 Neustálé zlepšování služby

Poslední publikace ITIL dokumentuje fázi Neustálé zlepšování služby (Continual service improvement) jako sedmi krokový proces nepřetržitého zdokonalování služby, který se skládá z identifikace strategie pro zdokonalování služby, definice cílů monitorování, sběru dat

z monitorování, zpracování dat z monitorování, analýzy zpracovaných dat, prezentace a užití výsledků analýzy a implementace korekce pro zlepšení služby. Proces nepřetržitého zdokonalování služby je postaven na monitorování, analýze monitorovaných dat v příslušných fázích životního cyklu služby a na implementaci poznatků získaných z analyzovaných dat. Obecné dimenze zdokonalování služby jsou kvalita, výkonnost, efektivita, nákladová efektivita, hodnota služby a uspokojení spotřebitele (Boyne, 2003). ITIL na nepřetržité zdokonalování služby nahlíží ve smyslu poskytování IT služby efektivnějším způsobem při dosahování nákladové efektivity provozu služby s cílem optimálně podporovat naplnění byznys požadavků. Zdokonalování služby cloud computingu z pohledu spotřebitele sleduje zejména dostupnost souboru služeb cloud computingu poskytující potřebnou funkcionalitu při požadované úrovni kvality služeb (Wang, a další, 2014), při optimálních nákladech a přijatelné míře rizika tak, aby každá služba optimálním způsobem podporovala byznys potřeby spotřebitele. Hodnoty parametrů úrovní aktuálně využívaných služeb cloud computingu by se po dobu svého produktivního provozu měly pohybovat v rozpětí předem dohodnutých limitních hodnot definovaných v SLA. Ustanovení v SLA jsou základem pro realizaci aktivit nepřetržitého zdokonalování služby cloud computingu spotřebitelem služby a limitní hodnoty parametrů úrovní služeb jsou tak nezbytným podkladem pro definici cílů monitorování. Monitorování je nezbytným prostředkem pro měření výkonnosti služby, pro zjišťování odchylek hodnot kvalitativních parametrů služby od hodnot definovaných v SLA a pro sledování dlouhodobých trendů provozu služby cloud computingu z hlediska plnění byznys požadavků. Pokud služba cloud computingu nesplňuje byznys požadavky nebo vykazuje trend, že tyto požadavky přestanou být plněny, je nutné komunikovat požadavek za změnu parametrů služby nebo na změnu služby poskytovateli anebo využívání služby cloud computingu ukončit a přejít k výběru alternativní služby cloud computingu dostupné na trhu a zahájit tak nový cyklus řízení služby cloud computingu.

4.3.6 Hodnocení procesů ITIL 2011 z pohledu spotřebitele služeb cloud computingu

Na základě provedené analýzy procesů ITIL 2011 je možné obdobně jako Pröhl (2012) vyhodnotit procesy definované v ITIL 2011 na základě jejich důležitosti pro spotřebitele služeb cloud computingu. Důležitými pro cloud computing management z pohledu spotřebitele služeb cloud computingu jsou zejména publikace Service strategy, Service transition, Service operation a Continual service improvement. Publikace Service design je určena zejména pro management IT služeb z pohledu spotřebitele. Hodnocení procesů definovaných v ITIL 2011 z hlediska významu pro cloud computing management z pohledu spotřebitele je specifikováno v následující Tabulce 5.

Tabulka 5: Hodnocení ITIL procesů z hlediska významu pro cloud computing management z pohledu spotřebitele, zdroj: (autor)

Service strategy – strategie služeb	
Strategické řízení IT služeb	Velmi důležitý
Řízení portfolia služeb	Velmi důležitý
Finanční řízení pro IT služby	Velmi důležitý
Řízení poptávky	Nedůležitý
Řízení obchodních vztahů	Velmi důležitý
Service Design – návrh služeb	
Koordinace návrhu	Nedůležitý
Řízení katalogu služeb	Velmi důležitý

Řízení úrovně služeb	Velmi důležitý
Řízení dostupnosti	Nedůležitý
Řízení kapacit	Nedůležitý
Řízeni kontinuity IT služeb	Nedůležitý
Řízení informační bezpečnosti	Velmi důležitý
Řízení dodavatelů	Nedůležitý
Service Transition – přechod na produktivní provoz služby	
Plánování a podpora přechodu	Velmi důležitý
Řízení změn	Nedůležitý
Řízení aktiv a konfigurace služeb	Nedůležitý
Řízení verzí a nasazení do produktivního provozu	Nedůležitý
Validace a testování služeb	Velmi důležitý
Hodnocení změn	Nedůležitý
Řízení znalostí	Nedůležitý
Service Operation – produktivní provoz služby	
Řízení událostí	Velmi důležitý
Řízení incidentů	Velmi důležitý
Plnění požadavků	Velmi důležitý
Řízení problémů	Velmi důležitý
Řízení přístupu	Velmi důležitý
Continual service improvement – nepřetržité zdokonalování služby	
Sedmi krokový proces zdokonalování služby	Velmi důležitý

4.4 MBI

Management podnikové informatiky (MBI) je konzistentní a flexibilní metodický rámec řízení podnikové informatiky a nejlepších praktik v oboru (Voříšek, a další, 2012), která je vyvíjena na katedře informačních technologií VŠE v kooperaci s katedrou softwarového inženýrství ČVUT (Dohnal, a další, 2013). Základním cílem modelu je prostřednictvím efektivního využití IT dosáhnout zvýšení celkové efektivity podniku (Voříšek, a další, 2012). Model vedoucím IT pracovníkům napomáhá zaznamenat a dokumentovat stávající systém řízení podnikové informatiky, případně navrhnout a implementovat nový efektivnější systém řízení podnikové informatiky s využitím osvědčených praktik a doporučení, kdy jednotlivé prvky modelu jsou mapovány na široce uznávané metodiky a standardy řízení podnikového IT (Voříšek, a další, 2015). Model MBI je zaměřen řízení specifických podmínek IT podniku s primární orientací na malé a střední podniky (Voříšek, a další, 2012). Malé a střední podniky se vyznačují zejména nedostatkem potřebných zdrojů pro efektivní fungování a podporu IT, které se projevují i v oblasti lidských zdrojů. Smyslem modelu MBI je sdílet a využívat znalosti a doporučení vyplývající z praxe podnikového IT a z dalších informačních zdrojů.

Model MBI je na konceptuální úrovni popsán na metamodelem, který definuje objekty, ze kterých se model skládá, a vazby mezi nimi. Centrálním objektem modelu řízení podnikové informatiky je Úloha. Úloha popisuje praktiky a doporučení pro řešení problémů a úkolů v různých oblastech provozu IT. Základní organizace modelu MBI dělí Úlohy do tří hlavních úrovní (strategické, taktické a operativní řízení) a osmi domén (strategické řízení podnikové informatiky, řízení IT služeb, řízení IT zdrojů, řízení ekonomiky podnikové informatiky, řízení rozvoje podnikové informatiky, řízení provozu podnikové informatiky, IT v řízení podniku a řízení IT a podniku podle odvětvových řešení). V rámci domén jsou definovány Skupiny úloh a Úlohy. Dalšími objekty MBI jsou (Voříšek, a další, 2015):

- *Dokument/data.* Dokumenty mohou sloužit jako vstupy nebo výstupy jednotlivých úloh nebo poskytovat návod na řešení problémů spjatých s provozem podnikového IT. Vlastnosti objektů jsou popsány souborem datových záznamů.
- *Role.* Role vyjadřují přidělení odpovědností jednotlivým pracovním pozicím ve vztahu k úkolům a jejich výstupům na základě kvalifikačních požadavků pomocí RACI matice.
- *Aplikace.* Aplikace reprezentuje funkcionalitu aplikačního software, se kterým pracuje daná úloha.
- *Metriky.* Metriky vyjadřují klíčové ukazatele výkonnosti realizace úloh, jako jsou klíčové identifikátory výkonnosti (KPI) a klíčové identifikátory cílů (KGI).
- *Metody.* Metody představují doporučené postupy pro řízení konkrétních úloh.
- *Scénáře.* Scénáře popisují modelové příklady potenciálních problémů spjatých s provozem podnikového IT.
- *Faktory.* Faktory ovlivňují použité metody k řešení konkrétních úloh.

MBI používá metody, které jsou popsány v jednotlivých objektech MBI formou prezentace nejlepších nebo dobrých zkušeností z praxe z provozu IT. MBI považuje cloud computing jako jeden z Faktorů ovlivňující řešení specifického problému řízení podnikového IT, především vzhledem k plánování a řízení rozvoje IT služeb podniku, tj. vzhledem k plánovaným IT projektům. Smyslem Faktorů je definovat existující prostředí pro řízení podniku, a proto Faktor F100 Cloud computing pokrývá pouze základní vymezení a definici cloud computingu a analýzu modelů a služeb poskytovaných v prostředí cloud computingu. Některé Úlohy se odkazují na služby cloud computingu spíše jako na jednu z forem IT outsourcingu než na přístup k budování podnikové informatiky. Pouze tři Úlohy jsou specificky zaměřeny na governance a management služeb cloud computingu, avšak komplexně nepokrývají specifické problémy, které jsou vymezené v jejich názvu. Těmito Úlohami jsou:

- Cloud Governance
- Řízení efektů cloud computingu
- Řízení rizik cloud computingu

Faktory skupiny Cloud computing a jeho služby (infrastrukturní, platformní a aplikační) se na strategické úrovni řízení IT promítají do výše jmenovaných Úloh Cloud Governance, Řízení efektů cloud computingu a Řízení rizik cloud computingu. Využití možností, které přináší cloud computing se promítá také do Skupin úloh Plán transformace IT podniku do cílového stavu, Řízení portfolia projektů a Řešení aplikačního projektu a jeho jednotlivých typů.

Výhodou modelu MBI je, že je navržen s ohledem na jeho neustálý rozvoj a může být rozšířen o nové objekty anebo existující objekty mohou být modifikovány se zohledněním působení různých faktorů.

4.5 Porovnání analyzovaných metodických rámců IT governance a IT managementu vzhledem ke governance a managementu využívání služeb cloud computingu

Existují různé důvody, které vedou podniky k tomu, aby přistoupily k implementaci metodických rámců pro IT governance a IT management. Tabulka 6 zobrazuje porovnání metodických rámců SOA Governance, ITIL 201, COBIT 5 a MBI z hlediska specifik governance a managementu služeb cloud computingu z pohledu spotřebitele. Z Tabulky 6 vyplývá, že ač je předmět zaměření metodických rámců odlišný, lze je po určité míře přizpůsobení aplikovat i v prostředí cloud computingu. Ačkoliv metodiky používají odlišné výrazové prostředky, jejich cíle jsou v podstatě totožné. Ve všech případech se jedná zejména o efektivní a účinné využití IT služeb pro generování zisku, přidané hodnoty, pro nákladově optimalizovanou a výkonnou výrobu produktů nebo poskytovaných služeb, pro udržení konkurenceschopnosti na trhu, případně i pro dosažení konkurenční výhody využíváním pokročilých IT technologií. Porovnávané metodiky jsou procesně orientované.

Tabulka 6: Porovnání metodických rámců SOA Governance, ITIL 2011, COBIT 5 a MBI z hlediska prostředí cloud computingu, zdroj: (autor)

	SOA Governance	ITIL V3 2011	COBIT 5	MBI
Předmět	SOA služby	IT služby	Podnikové IT	Podnikové IT
Oblast řízení	Governance SOA	IT governance je řešena částečně v publikaci Service Strategy	IT governance	IT governance
	Management SOA	Management IT služeb	IT management	IT management
Cílová organizace	Poskytovatel SOA služeb	Poskytovatel IT služeb	Organizace budující podnikové IT, může vystupovat v roli poskytovatele i zákazníka podnikového IT	Organizace budující podnikové IT, může vystupovat v roli poskytovatele i zákazníka podnikového IT
Cíle	Tvorba byznys hodnoty ze SOA	Dosažení přínosů	Tvorba hodnoty pro zainteresované strany	Zvýšení výkonnosti primárně malých a středních podniků
	Realizace benefitů prostřednictvím investic do SOA skrz kombinaci lidí, procesů a technologií	Návratnost investice (ROI)	Realizace benefitů prostřednictvím investic do IT a nákladová efektivnost	Optimalizace investic do podnikového IT
	Zabezpečení souladu mezi byznysem a IT	Dlouhodobě udržitelný úspěch	Zvýšení výkonnosti	Zvýšení výkonnosti
Zaměření na služby cloud computingu	Ne	Ne, služby cloud computingu jsou diskutovány	Ne, služby cloud computingu jsou brány jen jako jedna	Minoritně

	SOA Governance	ITIL V3 2011	COBIT 5	MBI
		minoritně ve vztahu k poskytovateli IT služeb	z forem externího poskytování IT služeb	
Zohlednění spotřebitele služeb cloud computingu	Ne	Ne	Minoritně	Minoritně
Aplikovatelnost do prostředí spotřebitele služeb cloud computingu	Částečná po přizpůsobení	Částečná po přizpůsobení	Částečná po přizpůsobení	Po přizpůsobení
Oblast řízení aplikovatelná do prostředí spotřebitele služeb cloud computingu	Governance	Management	Governance	Governance
	Metoda implementace governance modelu		Management	Management

V kapitole 4. autorka této doktorské disertační práce analyzovala metodické rámce SOA Governance, ITIL 2011, COBIT 5 a modelu MBI z hlediska jejich podpory pro governance a management využívání služeb cloud computingu z pohledu spotřebitele. Žádný z analyzovaných metodických rámců není specificky navržen jako standard pro governance a management využívání služeb cloud computingu z pohledu spotřebitele a není ani původně vytvořen s cílem reagovat na aspekty a rizika vyplývající z využívání služeb cloud computingu. Využití služeb cloud computingu nemění účel těchto metodických rámců, je však nutné je upravit takovým způsobem, aby zohledňovaly specifika vyplývající ze skutečnosti, že vlastníkem a poskytovatelem služeb cloud computingu je externí třetí strana odlišná od spotřebitele, která služby v modelu veřejného cloud computingu nabízí současně neomezenému počtu spotřebitelů.

SOA Governance jasně definuje oblast governance a managementu služeb SOA. Procesy SOA Governance nezohledňují specifika využívání služeb cloud computingu, ale jsou zaměřeny na služby SOA, a to z pohledu poskytovatele. Z analýzy metodického rámce SOA Governance vyplývá, že vybrané principy a procesy SOA Governance mohou být, po jejich přizpůsobení specifikům využívání služeb cloud computingu, aplikovatelné při návrhu modelu cloud computing governance a při budování governance služeb cloud computingu v podniku. Samotná modifikace principů a procesů SOA governance však není dostačující a je nutné cloud computing governance rozšířit o procesy nové, které v metodickém rámci SOA Governance obsaženy nejsou, a to zejména z důvodu, že SOA Governance nezohledňuje externí vlastnictví služeb cloud computingu a interakci mezi poskytovatelem a spotřebitelem během celého životního cyklu služby cloud computingu.

Metodický rámec COBIT 5 v zásadě není určen pro prostředí cloud computingu, avšak praktiky, principy a procesy v něm obsažené lze přizpůsobit také pro governance a management služeb cloud computingu. Governance a management procesy COBIT 5 mohou být po jejich přizpůsobení specifikům využívání služeb cloud computingu,

aplikovatelné při návrhu modelu cloud computing governance a modelu cloud computing management.

Metodický rámec ITIL 2011 je považován jako de-facto standard pro management IT služeb. Vzhledem k podobným vlastnostem IT služeb a služeb cloud computingu a podobnému životnímu cyklu služeb lze ITIL považovat jako metodický rámec, který je možné po svém přizpůsobení aplikovat do prostředí managementu služeb cloud computingu z pohledu spotřebitele. Protože ITIL není explicitně určen pro řízení služeb cloud computingu z pohledu spotřebitele, procesy definované pro jednotlivé fáze řízení životního cyklu IT služby je nutné modifikovat a doplnit o takové procesy, které budou vhodné pro spotřebitele služeb cloud computingu tak, aby byl spotřebitel optimálně připraven na řízení celého životního cyklu služby cloud computingu od rozhodnutí o jejím přijetí, přes využívání této služby až po ukončení smluvního vztahu s poskytovatelem služby cloud computingu a přechodem na jiné řešení.

Model MBI pohlíží na cloud computing pouze jako na jeden z faktorů, který ovlivňuje řešení specifického problému (tzv. Úlohy) řízení podnikového IT, avšak jeho otevřenost směrem k neustálému rozvoji umožňuje jeho přizpůsobení prostřednictvím definice nových Úloh pro governance a management využívání služeb cloud computingu z pohledu spotřebitele.

5 Návrh metodického rámce CCGM

Cílem této kapitoly je popsat autorkou této doktorské disertační práce navržený metodický rámec Cloud computing governance a management (CCGM).

Metodický rámec Cloud computing governance a management (CCGM) se skládá se ze dvou částí, kterými jsou Cloud computing governance a Cloud computing management.

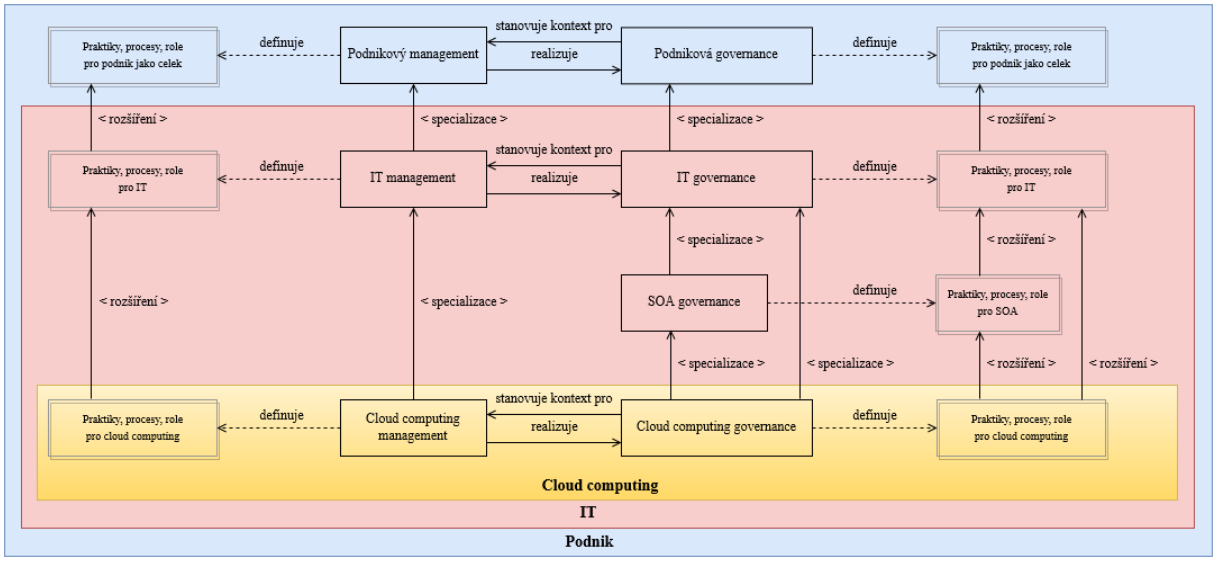
Metodický rámec Cloud computing governance a management pro governance a management služeb cloud computingu z pohledu spotřebitele služeb cloud computingu je autorkou této doktorské disertační práce nazvaný zkratkou jako „CCGM“ nebo také jako „metodický rámec CCGM“.

Návrh metodického rámce CCGM pro governance a management služeb cloud computingu z pohledu spotřebitele služeb vychází z široce akceptovaných rámců pro IT governance a IT management, a to konkrétně ze SOA Governance, ITIL 2011 a COBIT 5. Autorkou této disertační práce navržený metodický rámec CCGM je vytvořený přizpůsobením těchto rámců pro prostředí cloud computingu z pohledu spotřebitele služeb cloud computingu, přičemž zohledňuje jejich strukturu, principy, praktiky a procesy. Účelem navrženého metodického rámce CCGM pro governance a management služeb cloud computingu z pohledu spotřebitele služeb cloud computingu je poskytnout organizacím návod na vytvoření a implementaci jejich vlastního a podle jejich potřeb přizpůsobitelného a jednotného modelu cloud computing governance a cloud computing management. Metodický rámec CCGM umožňuje organizacím pochopit principy governance a managementu využívání služeb v prostředí cloud computingu a poskytuje praktiky, které napomáhají zabezpečit optimalizovat využití služeb cloud computingu a maximalizaci hodnoty z těchto služeb pro byznys plynoucí.

Metodický rámec CCGM se zaměřuje na specifickou oblast governance a managementu podnikového IT, kdy IT zdroje jsou poskytovány ve formě služeb veřejného cloud computingu vlastněných třetí stranou a poskytovaných velkému množství spotřebitelů služeb cloud computingu. Druhým specifikem je zaměření na spotřebitele služeb cloud computingu. Spotřebitel služeb cloud computingu využívá za úplatu služby cloud computingu, které jsou vytvářené a dodávané poskytovatelem veřejných služeb cloud computingu na dohodnuté úrovni služby. Spotřebitel má k dispozici informace o účelu a vlastnostech služeb, ale jejich vnitřní logika a algoritmus řešení není pro něj relevantní. Governance a management se v prostředí cloud computingu z pohledu spotřebitele služeb zaměřuje zejména na ovlivňování využívání služeb cloud computingu a na plánování, výběr a produktivní provoz služeb cloud computingu v podniku spotřebitele. Fáze návrhu služeb cloud computingu a řízení základní infrastruktury nutné pro realizaci a provoz těchto služeb není pro spotřebitele relevantní. Tyto skutečnosti nejsou ve stávajících metodikách IT governance a IT managementu plně pokryty a je nutné metody, principy a procesy obsažené v těchto rámcích upravit či doplnit o nové, které budou plně reflektovat aspekty vyplývající ze zásadních charakteristik cloud computingu z pohledu spotřebitele a které umožní dosažení očekávané byznys hodnoty z využití služeb cloud computingu.

Navržený metodický rámec CCGM plně respektuje již existující struktury governance a managementu, které specializuje tak, aby byly vyhovující pro prostředí cloud computingu. Specializace stávajících modelů governance a managementu eliminuje riziko, že organizace vytvoří několik oddělených systémů governance a managementu podniku a podnikového IT, které budou nekonzistentní a budou duplicitně pokrývat shodné oblasti jejich zaměření. Navržený metodický rámec CCGM pro governance a management služeb cloud computingu z pohledu spotřebitele služeb cloud computingu je proto podmnožinou IT governance a IT managementu a rozšiřuje jejich praktiky, procesy a role o specifika vyplývající z využití služeb cloud computingu spotřebitelem (viz

Obrázek 14). Obrázek 14 znázorňuje vztah specializace modelu Cloud computing governance a modelu Cloud computing managementu v rámci struktury governance a managementu vzhledem k IT governance a IT managementu a jejich prostřednictvím i vzhledem k podnikové governance a podnikovému managementu. Cloud computing governance a Cloud computing management definují soubor praktik, procesů a rolí. Tyto praktiky, procesy a role jsou rozšířením praktik, procesů a rolí podnikové governance, podnikového managementu, IT governance a IT managementu o specifika využívání služeb cloud computingu z pohledu spotřebitele služeb cloud computingu.



Obrázek 14: Vztah specializace mezi podnikovou governance a managementem, IT governance a managementem, SOA governance a cloud computing governance a managementem a vztah rozšíření jejich praktik, procesů a rolí, zdroj: (autor)

Aby bylo možno dosáhnout přínosy z využití služeb cloud computingu, pokrývá metodický rámec CCGM aspekty využívání služeb cloud computingu na strategické, taktické i operativní úrovni, neboť využití služeb cloud computingu ovlivňuje byznys procesy kritické pro dosažení byznys cílů.

5.1 Východiska navrženého metodického rámce CCGM

Ačkoliv je cloud computing rozšířeným přístupem, kdy investice do adopce a využívání služeb neustále rostou, existují problémy, které brání plně realizovat benefity ze služeb cloud computingu a které vyplývají z neúčinných nebo chybějících metod governance a managementu. Mezi tyto problémy patří:

- nesoulad mezi byznysem a IT,
- odolnost organizace vůči změnám a inovativním technologiím,
- nedostatečné informace pro realizaci strategických rozhodnutí v oblasti služeb cloud computingu,
- nejasná orientace mezi velkým množstvím poskytovatelů na trhu služeb cloud computingu poskytujících služby v různé kvalitě,
- nesoulad mezi byznys požadavky a využíváním služeb cloud computingu,
- ohrožení bezpečnosti dat a ztráta kontroly nad daty,
- nedostupnost metod pro měření přínosů a návratnosti investice do služeb cloud computingu,
- nejasná aplikovatelnost a vynutitelnost dodržování legislativy, standardů a norem,
- neefektivní provozní procesy,
- nedostatečná transparentnost operací poskytovatele služeb cloud computingu.

Prostředí cloud computingu je svým principem prostředí, ve kterém poskytovatelé služeb cloud computingu poskytují služby spotřebitelům služeb cloud computingu. Spotřebitel služby může tedy při řízení adopce a využití služeb cloud computingu využívat principy a metody rámců zaměřených jak na governance a management IT služeb, tak na governance a management služeb servisně orientované architektury. Pokud jsou již v organizaci implementovány modely IT governance a managementu nebo SOA governance a managementu, pak lze na ně navázat a rozšířit je o specifika vyplývající ze skutečnosti, že poskytovatelem služeb cloud computingu je externí společnost. Pokud IT nebo SOA governance a management v organizaci před adopcí služeb cloud computingu zaveden není, je jeho implementace vhodným výchozím krokem.

Pokud se organizace rozhodne, že k naplnění svých byznys cílů bude používat pro některé nebo případně všechny byznys procesy služby cloud computingu poskytované externím poskytovatelem služeb cloud computingu, je z hlediska rámců pro governance a management IT nebo SOA postaven před následující otázky a úkoly:

- Umožňuje stávající model IT nebo SOA governance a managementu plně podporu adopce a využívání služeb cloud computingu?
- Jakým způsobem je potřeba upravit nebo rozšířit stávající model IT nebo SOA governance a managementu tak, aby služby cloud computingu podporovaly byznys procesy v souladu s podnikovou governance?
- Jaké úpravy stávajících IT nebo SOA governance a management procesů jsou potřebné pro adopci a využívání služeb cloud computingu?
- Jaké nové governance a management procesy jsou potřebné pro adopci a využívání služeb cloud computingu?

Iniciální adopce služeb cloud computingu znamená zcela zásadní změnu statutu a postavení podnikového IT (Cisco, 2015). Dosavadní status výhradního poskytovatele IT služeb se změní na status prostředníka IT služeb, které dodává třetí strana. Pokud by se jednalo o klasický outsourcing, bylo by evidentně možné využít stávající IT nebo SOA governance a management model. V prostředí klasického outsourcingu je možné na základě smluvních ujednání s dodavatelem outsourcingu realizovat stávající governance a management procesy i na straně dodavatele. V prostředí modelu veřejného cloud computingu existuje řada omezení, která limitují využití a aplikovatelnost stávajících governance a management metod na straně poskytovatele služeb cloud computingu.

5.2 Cíle navrženého metodického rámce CCGM

Navržený metodický rámec CCGM napomáhá organizaci jakožto spotřebiteli služeb cloud computingu navrhnout a realizovat systém governance a managementu služeb cloud computingu, který umožňuje zabezpečit dosažení přínosů z využití služeb cloud computingu, zvýšit výkonnost IT a prostřednictvím efektivní podpory byznys procesů službami cloud computingu a zvýšit celopodnikovou výkonnost spotřebitele služeb cloud computingu. Metodický rámec CCGM respektuje široce akceptované rámce pro IT governance a IT management a v nich obsažené osvědčené postupy, praktiky a principy (viz kapitola 4).

Hlavní cíle navrženého metodického rámce CCGM pro governance a management využívání služeb cloud computingu z pohledu spotřebitele služeb jsou:

- C1: Poskytnutí jednotného metodického rámce pro governance a management využívání služeb cloud computingu, který odděluje cloud computing governance od cloud computing managementu, přičemž jejich rozhraní je jasně definováno.

- C2: Poskytnutí konzistentního, flexibilního, jednoduchého a srozumitelného a snadno implementovatelného procesně orientovaného metodického rámce pro governance a management využívání služeb cloud computingu.
- C3: Přizpůsobení metodického rámce pro governance a management využívání služeb cloud computingu specifickým podmínkám podniku a vytvoření systému governance a managementu využívání služeb cloud computingu konkrétního podniku.
- C4: Vytvoření rozhodovacího procesu a pravidel a omezení souvisejících s adopcí a využíváním služeb cloud computingu vzhledem k IT anebo cloud computing strategii s cílem dosažení potřeb byznysu.
- C5: Realizace benefitů z využití služby cloud computingu optimalizací nákladů a rizik při využívání služeb cloud computingu.
- C6: Zabezpečení efektivní adopce a efektivního a výkonného využívání služby cloud computingu v souladu s potřebami byznysu a zainteresovaných stran v rámci celého životního cyklu služby cloud computingu.

5.3 Vymezení rozsahu navrženého metodického rámce CCGM

Metodický rámec CCGM je určen spotřebitelům služeb cloud computingu, kteří využívají služby cloud computingu v modelu veřejného cloud computingu. Nezávisle na jejich velikosti a na struktuře jejich organizace jim poskytuje metodiky pro vybudování modelu governance a managementu jimi využívaných služeb cloud computingu. V modelu veřejného cloud computingu se jedná o IT služby, které organizaci dodává třetí strana, nikoliv jejich vlastní IT oddělení. Spotřebitel služeb cloud computingu je v metodickém rámci CCGM charakterizován jako organizace, která za úplatu využívá služby veřejného cloud computingu poskytované poskytovatelem služeb cloud computingu. Oproti tomu uživatel služby cloud computingu je koncový uživatel dané služby cloud computingu. Metodický rámec CCGM předpokládá, že spotřebitel služby cloud computingu má vytvořen model governance a managementu podnikového IT na základě některého z široce využívaného rámce. Tyto široce využívané rámce neobsahují metodiky governance a managementu využívání služeb cloud computingu v modelu veřejného cloud computingu. Metodický rámec CCGM rozšiřuje stávající modely IT governance a IT managementu o metodiku správy a řízení specifickou právě pro oblast využívání služeb cloud computing v modelu veřejného cloud computingu. Metodický rámec CCGM je specializací nebo také podmnožinou existujících IT governance a management rámců. Navržené procesy governance a managementu služeb cloud computingu navazují na stávající IT governance a management procesy a rozšiřují je s cílem vytvořit jednotný celek governance a managementu, který umožňuje efektivně zabezpečit dosažení benefitů z využití služeb cloud computingu. Metodický rámec CCGM nemění metodiku governance a managementu podnikového IT, která zůstává zachována, je však rozšířena o specializaci využívání služeb cloud computingu v modelu veřejného cloud computingu. Metodický rámec CCGM tak umožňuje organizaci, aby adopce využívání služeb cloud computingu byla plně v souladu s potřebami zainteresovaných stran a se strategickými byznys cíli organizace. Metodický rámec CCGM tedy neslouží jako rámec pro vytvoření modelu governance a managementu celopodnikového IT, věnuje se pouze specifickým rozšířením využívání služeb cloud computingu.

Navržený metodický rámec CCGM se zaměřuje specificky na:

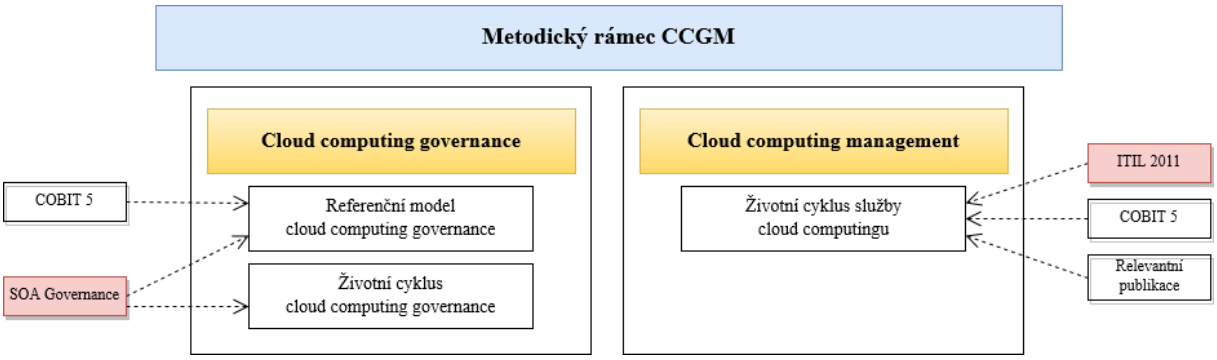
- obchodní společnosti vystupující v roli spotřebitele služeb cloud computingu,
- střední a velké podniky využívající služby cloud computingu bez specifického odvětvového zaměření,
- služby cloud computingu v modelu veřejného cloud computingu (public cloud computing),

- modely služeb cloud computingu infrastruktura jako služba (IaaS), platforma jako služba (PaaS), software jako služba (SaaS).

5.4 Struktura navrženého metodického rámce CCGM

Navržený metodický rámec CCGM odlišuje governance služeb cloud computingu z pohledu spotřebitele služeb od managementu služeb cloud computingu z pohledu spotřebitele služeb. Tuto separaci reflektuje struktura metodického rámce, která se skládá se ze dvou částí znázorněných na Obrázku 15. Těmito částmi jsou:

- Cloud computing governance
- Cloud computing management



Obrázek 15: Struktura navrženého metodického rámce CCGM, zdroj: (autor)

Cloud computing governance (kapitola 6) definuje Referenční model cloud computing governance poskytující základní komponenty pro návrh modelu Cloud computing governance customizovatelného pro potřeby organizace vystupující v roli spotřebitele služeb cloud computingu. Dále poskytuje postup ve formě Životního cyklu cloud computing governance pro praktickou implementaci navrženého modelu Cloud computing governance v organizaci. Cloud computing governance vychází z rámce SOA Governance a z governance procesů COBIT 5. Cloud computing governance plně respektuje strukturu SOA Governance, na jejímž základě definuje následující komponenty:

- Referenční model cloud computing governance
- Životní cyklus cloud computing governance

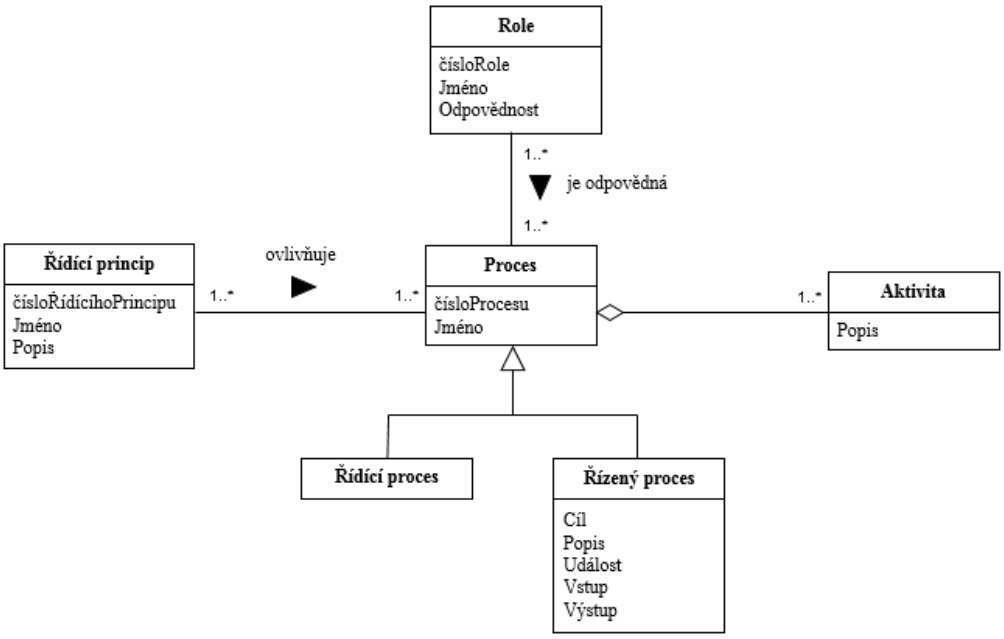
Referenční model cloud computing governance (kapitola 6.1) definuje principy, procesy a role, které slouží jako reference pro návrh vlastního a pro konkrétní potřeby spotřebitele přizpůsobeného modelu Cloud computing governance. Životní cyklus cloud computing governance (kapitola 6.2) definuje činnosti prováděné v rámci cyklu sestávajícího se z fází plánování, definování, implementace a monitorování s cílem implementovat a neustále zlepšovat úroveň navrženého modelu Cloud computing governance.

Cloud computing management (kapitola 7) definuje model umožňující řízení životního cyklu služby cloud computingu z pohledu spotřebitele v souladu s principy a praktikami cloud computing governance. Cloud computing management vychází z životního cyklu řízení IT služeb dle ITIL 2011, z management procesů rámce COBIT 5 a dalších relevantních publikací včetně dobrých praktik z praxe. Cloud computing management respektuje strukturu rámce ITIL 2011, na jehož základě definuje fáze životního cyklu služeb cloud computingu a příslušné procesy pro řízení využití služeb cloud computingu (kapitola 7.3, kapitola 7.4 a kapitola 7.5, kapitola 7.6 a kapitola 7.7)

5.5 Konceptuální model metodického rámce CCGM

V rámci vymezení použité terminologie je pojem metodický rámec jako skupina metodik obsahující souhrn doporučených praktik a postupů pro řešení specifického úkolu (Svatá, 2011). Metodika formalizuje postupy pro řešení specifického úkolu a definuje odpovědnosti ve vztahu k těmto činnostem (Buchalcevová, 2005). Metodika se skládá z různých metodických prvků, mezi které lze zařadit fáze, dimenze, role, principy, praktiky, procesy, činnosti, nástroje, vzory, standardy, produkty a metriky (Buchalcevová, 2003), přičemž struktura metodiky by měla odrážet řešení specifického úkolu, problému či situace, pro které je metodika určena. Metodický rámec CCGM je navržen tak, aby umožnil spotřebiteli služeb řešit problémy spojené s využíváním služeb cloud computingu. Konceptuální model navrženého metodického rámce CCGM pro governance a management služeb cloud computingu z pohledu spotřebitele služeb popisuje prvky metodického rámce CCGM, navržené atributy těchto metodických prvků a vztahy mezi těmito prvky. Pro účely standardizovaného vyjádření je konceptuální model cloud computing governance a konceptuální model cloud computing managementu metodického rámce CCGM znázorněný na Obrázcích 16 a 17 vytvořen pomocí Diagramu tříd jazyka UML. Pro realizaci efektivního modelu cloud computing governance a cloud computing managementu musí existovat určitá míra závazku dodržovat soulad mezi těmito dvěma doménami řízení. Každá doména obsahuje soubor specifických procesů, řídících principů a rolí.

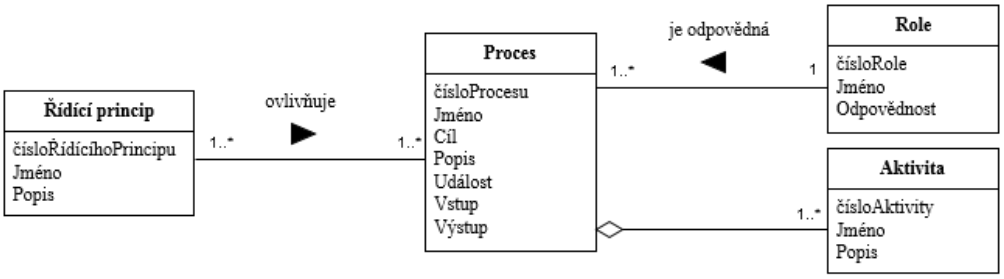
Centrální třídou konceptuálního modelu cloud computing governance metodického rámce CCGM (viz Obrázek 16) je proces, který je generalizací řídících procesů a řízených procesů. To vyjadřuje skutečnost, že model cloud computing governance je realizován dvěma typy procesů, a to řídícími procesy a řízenými procesy. Řídící procesy jsou určeny pro řízení řízených procesů, pro jejich monitorování a komunikování. Řízené procesy realizují návrh a uplatňování cloud computing governance. Definice procesů je ovlivněna řídícími principy, které definují pravidla umožňující zabezpečit jednotný a konzistentní přístup pro návrh modelu governance služeb cloud computingu. Každý proces se skládá z procesních aktivit. Na návrhu a realizaci procesů se podílí řada pracovníků, kteří v rámci jim vymezených rolí mají přidělené odpovědnosti za daný proces.



Obrázek 16: Konceptuální model cloud computing governance metodického rámce CCGM, zdroj: (autor)

Centrální třídou konceptuálního modelu cloud computing managementu metodického rámce CCGM (viz Obrázek 17) je proces. Popis každého procesu se skládá z identifikačního čísla procesu, jména

procesu, cíle procesu, popisu procesu, události vedoucí ke spuštění procesu a základních vstupů a výstupů procesu. Proces se skládá ze skupiny procesních aktivit, které transformují vstupy na výstupy. Návrh a definice procesů je ovlivněna řídícími principy. Za návrh a definici procesu odpovídá vždy jedna příslušná role. Role je dána souhrnem odpovědností za realizaci procesu.



Obrázek 17: Konceptuální model cloud computing managementu metodického rámce CCGM, zdroj: (autor)

5.6 Přínosy metodického rámce CCGM

Metodický rámec CCGM poskytuje spotřebiteli služeb cloud computingu zejména následující přínosy:

- použití jednotného metodického rámce pro governance a management služeb cloud computingu, který umožňuje oddělení governance od managementu,
- dosažení vyšší úrovně souladu mezi byznysem a IT,
- dosažení strategických cílů efektivním využitím služeb cloud computingu,
- zlepšení schopnosti organizace rychle a efektivně reagovat na změny v byznys prostředí,
- zachování konkurenceschopnosti organizace,
- dosažení vyšší výkonnosti definováním jednotlivých fází řízení životního cyklu služby cloud computingu, procesů v rámci těchto fází a procesních aktivit,
- řízení celého životního cyklu služby cloud computingu od výběru až po ukončení využívání služby cloud computingu,
- dosažení operační excelence optimálním výběrem spolehlivých a důvěryhodných poskytovatelů služeb cloud computingu a nasazením výkonných a účinných služeb cloud computingu,
- snížení rizik vyplývající z využívání služeb cloud computingu na akceptovatelné úrovni,
- efektivnější řízení nákladů na služby cloud computingu na optimální úrovni,
- dosahování shody s platnou legislativou, standardy a normami,
- vytvoření jasného komunikačního standardu pro zainteresované strany,
- řízení interakce s poskytovateli služeb cloud computingu,
- efektivnější sledování využití služby ve vztahu ke smlouvám o poskytování služby cloud computingu,
- vymezení rolí a odpovědností Cloud computing governance a managementu.

V kapitole 5 autorka této doktorské disertační práce popisuje navržený metodický rámec CCGM (Cloud computing governance a managment) z hlediska jeho cílů, rozsahu, struktury, komponent a přínosů. Metodický rámec CCGM se skládá ze dvou částí, kterými jsou:

- *Cloud computing governance*
- *Cloud computing management*

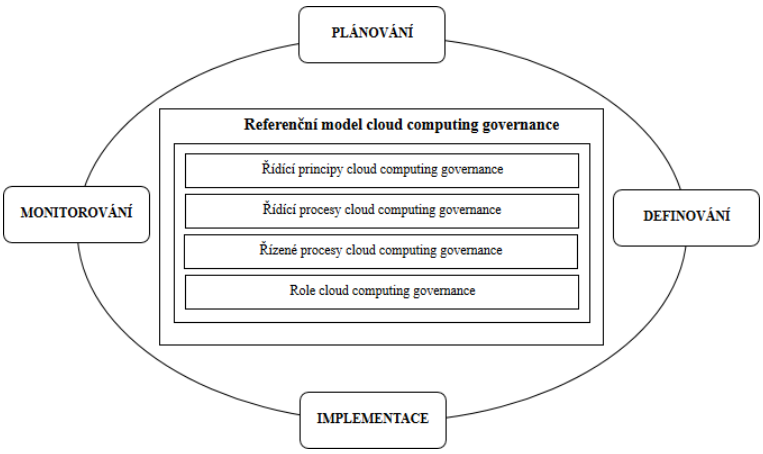
6 Cloud computing governance

Cílem kapitoly je popsat autorkou této doktorské disertační práce navržený model Cloud computing governance metodického rámce Cloud computing governance a management (CCGM). Cloud computing governance je vytvořený modifikací metodického rámce SOA Governance a governance procesů COBIT 5. Cloud computing governance se skládá z Referenčního modelu cloud computing governance a Životního cyklu cloud computing governance.

Pro potřeby této doktorské disertační práce autorka formulovala definici cloud computing governance, která je odvozena od definice IT governance (2.1), kdy principy IT governance jsou přizpůsobeny specifickému prostředí cloud computingu, avšak komponenty governance modelu se neliší. Odlišuje se jejich obsah, který musí reflektovat skutečnost, že služby cloud computingu jsou poskytovány externím poskytovatelem služeb cloud computingu, který je zodpovědný za jejich návrh, poskytování, údržbu a za řízení infrastruktury potřebné pro provoz služeb. Definice cloud computing governance zní následovně:

Cloud computing governance je soubor politik, pravidel, omezení, organizačních struktur, rolí a odpovědností uzpůsobených pro prostředí cloud computingu z pohledu spotřebitele služeb, které se soustředí na zabezpečení efektivního využívání služeb cloud computingu při minimalizaci souvisejících nákladů a rizik tak, aby služby cloud computingu přispívaly k tvorbě očekávané byznys hodnoty v souladu s potřebami podniku a zainteresovaných stran. Cloud computing governance jako součást governance struktur v podniku podporuje soulad mezi byznysem a IT, který naplňuje prostřednictvím politik, procesů, nastavením rolí a odpovědností a součinností vrcholových byznys manažerů s IT manažery.

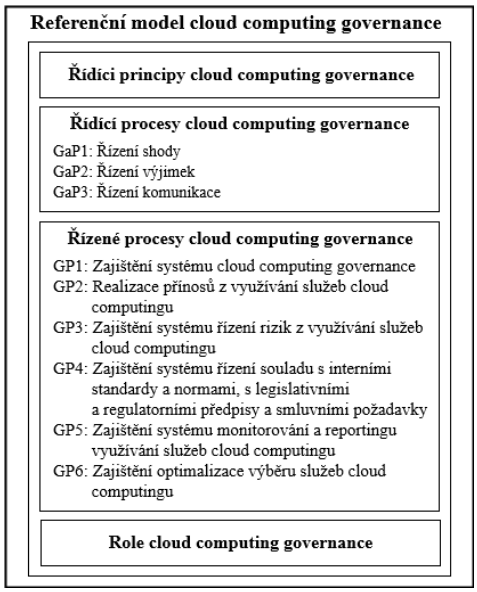
Cloud computing governance je vytvořený modifikací rámce SOA Governance a governance procesů COBIT 5 pro prostředí cloud computingu z pohledu spotřebitele služeb. Struktura modelu Cloud computing governance zohledňuje strukturu rámce SOA Governance a stejně jako SOA Governance se skládá z referenčního modelu a životního cyklu pro návrh, realizaci a řízení referenčního modelu tak, aby referenční model mohl být plně přizpůsoben konkrétním podmínkám organizace. Cloud computing governance se skládá z Referenčního modelu cloud computing governance a z Životního cyklu cloud computing governance, jejichž strukturu znázorňuje Obrázek 18.



Obrázek 18: Struktura Cloud computing governance, zdroj: (autor)

6.1 Referenční model cloud computing governance

Referenční model cloud computing governance je customizovatelný model, který poskytuje referenci pro definici, návrh a implementaci pro konkrétní potřeby přizpůsobeného modelu cloud computing governance. Referenční model cloud computing governance pokrývá strategickou úroveň správy služeb cloud computingu a poskytuje rámec pro governance služeb cloud computingu ve shodě se strategickými byznys cíli. Referenční model cloud computing governance obsahuje principy a procesy, které na strategické úrovni spravují využívání služeb cloud computingu s cílem dosažení strategických cílů v souladu s potřebami zainteresovaných stran a zajišťují realizaci účinného nástroje pro zabezpečení potřebné úrovně výkonnosti a kvality využívaných služeb, které jsou v souladu s regulatorními opatřeními. Referenční model cloud computing governance definuje a popisuje komponenty pro realizaci modelu governance služeb cloud computingu z pohledu spotřebitele. Obrázek 19 znázorňuje komponenty Referenčního modelu cloud computing governance, kdy klíčovými komponentami jsou zejména procesy Cloud computing governance.



Obrázek 19: Struktura Referenčního modelu cloud computing governance, zdroj: (autor)

6.1.1 Řídící principy cloud computing governance

Řídící principy cloud computing governance definují společná pravidla a doporučení pro efektivní propojení byznysu, IT a služeb cloud computingu, což umožňuje aplikovat konzistentní řízený přístup využití služeb cloud computingu na všech úrovních organizace. Řídící principy cloud computing governance zabezpečují podporu rozhodování při návrhu, nasazení a provozování Referenčního modelu cloud computing governance. Umožňují podpořit a lépe pochopit využití služeb cloud computingu v souladu s potřebami zainteresovaných stran, slouží jako podpora při návrhu politik a stanovují hranici operací cloud computing governance. Řídící principy cloud computing governance jsou následující:

ŘPG1: Cloud computing strategie musí být v souladu s byznys strategií a musí být podporována výkonným vedením. Soulad strategií, ve smyslu souladu byznys strategie, IT strategie a cloud computing strategie, zabezpečuje, že iniciativy v oblasti cloud computingu jsou v souladu s celopodnikovými cíli. Iniciativy v oblasti cloud computingu musí být podporovány vrcholovým managementem a vycházet z potřeb podniku a zainteresovaných stran. Pro zabezpečení správné

realizace strategií musí být identifikovány příslušné zainteresované strany, které přijmou odpovědnost za realizaci procesů provádění strategií.

ŘPG2: Cloud computing governance musí být v souladu s podnikovou governance a IT governance a musí být podporována výkonným vedením. Soulad modelů governance v organizaci, ve smyslu souladu podnikového governance, IT governance a cloud computing governance zabezpečuje, že governance služeb cloud computingu vychází z IT governance a rozšiřuje jej o specifika využívání služeb cloud computingu. Tento princip zabraňuje vytváření paralelních governance struktur v organizaci. Potřeba a důležitost cloud computing governance jako součást řízení podniku musí být podporována vrcholovým managementem a vycházet z potřeb podniku a zainteresovaných stran. Pro zajištění realizace, prosazování a souladu governance musí být identifikovány příslušné zainteresované strany, které přijmou odpovědnost za realizaci procesů provádění governance.

ŘPG3: Využití služeb cloud computingu musí přinášet hodnotu zainteresovaným stranám. Hodnota z využití služby cloud computingu vyjadřuje úroveň naplnění potřeb zainteresovaných stran. Hodnota, kterou má přinést využití služeb cloud computingu musí být jasně definovaná, akceptovaná a měřitelná. To napomáhá určit priority týkající se využití služeb cloud computingu a stanovit metriky pro měření odchylek skutečně dosažené hodnoty od plánované hodnoty.

ŘPG4: Rizika související s využíváním služeb cloud computingu musí být kontinuálně optimalizovaná. Existence systému řízení rizik cloud computingu zajišťuje optimalizaci úrovně rizik souvisejících s využíváním služeb cloud computingu tak, aby úroveň rizik spojených s využíváním služeb cloud computingu byla pro organizaci přijatelná z hlediska její úrovně tolerance rizika.

ŘPG5: Využívání služeb cloud computingu musí být v souladu s legislativními, regulatorními a dalšími oborovými požadavky. Tento princip znamená, že jsou využívány pouze takové služby cloud computingu a jsou využívány takovým způsobem, že jejich využívání je v souladu s platnou legislativou.

ŘPG6: Náklady na využívání služeb cloud computingu musí být kontinuálně optimalizované. Tento princip znamená, že využívání služeb cloud computing je řízeno tak, aby jejich provoz byl nákladově efektivní a byly maximalizovány benefity z využívání služeb cloud computingu.

ŘPG7: Politiky cloud computing governance při využívání služeb v prostředí cloud computingu musí být komunikovány a musí být dostupné příslušným zainteresovaným stranám. V organizaci musí být definovány politiky cloud computing governance, které stanovují pravidla a omezení v souvislosti s využíváním služeb cloud computingu a definují způsob rozhodování v organizaci a strukturu oprávnění v souladu s potřebami cloud computing strategie. Iniciace těchto politik a jejich prosazování musí být realizováno vrcholovým vedením IT. Definované politiky cloud computing governance musí být komunikovány a dostupné všem příslušným zainteresovaným stranám, tzn. všem příslušným lidem na všech pozicích.

ŘPG8: Účinnost, výkonnost implementovaného cloud computing governance modelu musí být monitorována a musí být vyhodnocována shoda s definovanými governance principy. Monitorování shody implementovaného systému využívání služeb cloud computingu zajišťuje, že řízené procesy realizované při využívání služeb cloud computingu jsou v souladu s definovanými governance principy a že případné odchylky od shody jsou detekovány a definovaným způsobem řešeny tak, aby opět nastala shoda.

ŘPG9: Pro efektivní podporu implementace a provozu cloud computing governance musí být dostupné potřebné umožňující schopnosti a prostředí. Organizace musí mít k dispozici potřebné

technologie pro implementaci a provoz systému cloud computing governance. To znamená infrastrukturní zdroje, aplikace a nástroje pro realizaci cloud computing governance.

6.1.2 Řídící procesy cloud computing governance

Řídící procesy cloud computing governance jsou takové procesy, které Referenční model cloud computing governance používá pro řízení jednotlivých řízených procesů. Tyto procesy neustále probíhají v organizaci. Řídící procesy cloud computing governance plně respektují řídící principy SOA Governance, avšak jejich obsah reflektuje specifika cloud computingu. Řídící procesy cloud computing governance:

- GaP1: Řízení shody,
- GaP2: Řízení výjimek,
- GaP3: Řízení komunikace.

GaP1: Řízení shody

Proces řízení shody zabezpečuje, že řízený proces je ve shodě s politikami a pravidly cloud computing governance. Proces řízení shody umožňuje prokázat, zda řízený proces je nebo není ve shodě s kritérii definovanými v rámci cloud computing governance. V případě, že není dosaženo shody, musí proces řízení shody vygenerovat výjimku. Obvyklá metoda realizace tohoto principu řízení je definování kontrolních bodů v řízených procesech, ve kterých se kontrola shody provádí. Tyto kontrolní body jsou vyhodnocovány odpovědnými pracovníky nebo automatizovaně. Každá výjimka generovaná procesem řízení shody musí být analyzována s primárním cílem odstranění příčiny neshody. Pokud se z nějakého důvodu nedaří obnovit shodu nebo se z některého důvodu jeví jako výhodné nebo potřebné tuto výjimku akceptovat, pak se jako následný krok uplatní proces řízení výjimek.

GaP2: Řízení výjimek

Proces řízení výjimek umožňuje zpracovat detekovanou výjimku a stanovit, zda tato výjimka může být za definovaných podmínek a na omezenou dobu akceptována či naopak zamítnuta s tím, že důvod neshody musí být odstraněn. V řadě případů detekovaná výjimka slouží jako signál, že poskytovatel služeb cloud computingu provedl v poskytované službě změnu bez předchozí konzultace se spotřebitelem služeb cloud computingu. Výjimka může signalizovat i nedostatek nebo chybu v některé politice nebo pravidlu. Proces řízení výjimek musí být schopen správně vyhodnotit, zda se jedná o výjimky, které porušují pravidla shody a jejichž důvody vzniku musí být opraveny tak, aby byla opět nastolena shoda, o výjimky, které jsou akceptovány za definovaných podmínek a na omezenou dobu nebo o výjimky, které detekují nutnost změny např. některé z politik nebo pravidel. Pokud výjimka nebyla akceptována a zároveň zúčastněné strany nedošly ke konsenzu na způsob řešení výjimky, eskaluje se výjimka k vyššímu stupni řízení v podniku. Pokud je výjimka vyhodnocená tak, že nastala na straně poskytovatele služeb, musí eskalační manažer nahlásit výjimku poskytovateli služeb a na základě komunikace o výjimce s poskytovatelem služeb stanoví, jakým způsobem bude daná výjimka zprocesována na straně spotřebitele služeb. To znamená, že dle ohodnocení vlivu výjimky na realizaci byznys procesů spotřebitele služeb, bude probíhat komunikace mezi eskalačním manažerem spotřebitele a pracovištěm podpory poskytovatele nebo eskalačním manažerem poskytovatele. V případě výjimek způsobených například změnou softwaru po provedení jeho upgrade nebo update na straně poskytovatele mohou být do jednání zapojeni i příslušní pracovníci byznys oddělení.

GaP3: Řízení komunikace

Proces řízení komunikace zabezpečuje, aby byly potřebné a relevantní informace vztahující se k systému cloud computing governance komunikovány s relevantními zainteresovanými stranami. Proces řízení komunikace musí zajistit pochopení systému cloud computing governance a to včetně:

- důležitosti a významu cloud computing governance,
- politik, standardů a principů cloud computing governance při využívání služeb v prostředí cloud computingu,
- procesů řízení shody a řízení výjimek v prostředí cloud computing governance, a to včetně eskalačních mechanismů,
- organizační struktury, rolí a odpovědností cloud computing governance pro využívání služeb cloud computingu,
- technologií cloud computing governance,
- řízených cloud computing governance procesů v prostředí využívání služeb cloud computingu.

6.1.3 Řízené procesy cloud computing governance

Úkolem řízených procesů je zabezpečit prosazování Cloud computing governance a dodržování souladu s politikami a pravidly governance na celopodnikové úrovni. Řízenými procesy jsou:

- GP1: Zajištění systému cloud computing governance,
- GP2: Realizace přínosů z využívání služeb cloud computingu,
- GP3: Zajištění systému řízení rizik z využívání služeb cloud computingu,
- GP4: Zajištění systému řízení souladu s interními standardy a normami, s legislativními a regulatorními předpisy a smluvními požadavky,
- GP5: Zajištění systému monitorování a reportingu využívání služeb cloud computingu,
- GP6: Zajištění optimalizace výběru služeb cloud computingu.

Definice řízených procesů cloud computing governance obsahují následující tabulky Tabulka 7, Tabulka 8, Tabulka 9, Tabulka 10, Tabulka 11 a Tabulka 12.

Tabulka 7: Proces GP1 Zajištění systému cloud computing governance, zdroj: (autor)

Číslo procesu	**GP1**
Jméno procesu	**Zajištění systému cloud computing governance**
Cíl procesu	Vytvoření, udržování a prosazování systému cloud computing governance v souladu podnikovými cíli a potřebami zainteresovaných stran.
Popis procesu	Proces dodává konzistentní přístup, který v souladu s podnikovou governance poskytuje mechanismy a principy pro vytvoření a udržování cloud computing governance ve vztahu k vytvoření a údržbě organizační struktury, rolí, odpovědností, pravomocí, principů, politik a procesů. Proces zabezpečuje, že rozhodnutí týkající se využívání služeb cloud computingu jsou prováděna v souladu s IT strategií a že související procesy pro využívání služeb cloud computingu jsou efektivní, transparentní a v souladu se standardy a legislativními a regulatorními požadavky.
Událost	Strategické rozhodnutí o využívání služeb cloud computingu, změna v byznys strategii.
Vstup	Byznys strategie, cloud computing strategie, standardy a normy.
Výstup	Cloud computing governance mechanismy a principy.

Procesní aktivity	Vytvoření, údržba, prosazování, monitorování a vyhodnocování cloud computing governance.

Tabulka 8: Proces GP2 Realizace přínosů z využití služeb cloud computingu, zdroj: (autor)

Číslo procesu	**GP2**
Jméno procesu	**Realizace přínosů z využívání služeb cloud computingu**
Cíl procesu	Optimalizace přínosů z využívání služeb cloud computingu ke tvorbě byznys hodnoty při minimalizaci nákladů vynaložených na tyto služby.
Popis procesu	Proces poskytuje mechanismy a principy pro stanovení a hodnocení přínosů z využití služeb cloud computingu pro potřeby byznysu. Proces zabezpečuje, že pro každou službu cloud computingu je provedena optimalizace nákladů, stanovení předpokládaných přínosů z využití služby cloud computingu a určení pravděpodobnosti, s jakou služba dosáhne očekávaných přínosů.
Událost	Strategické rozhodnutí o využívání služeb cloud computingu, změna v byznys strategii**.**
Vstup	Byznys strategie, cloud computing strategie.
Výstup	Mechanismy a principy zabezpečující realizaci optimálních přínosů z využití služeb cloud computingu.
Procesní aktivity	Vytvoření, údržba, prosazování, monitorování a vyhodnocování systému pro realizaci optimálních přínosů z využívání služeb cloud computingu.

Tabulka 9: Proces GP3 Zajištění systému řízení rizik z využívání služeb cloud computingu, zdroj: (autor)

Číslo procesu	**GP3**
Jméno procesu	**Zajištění systému řízení rizik z využívání služeb cloud computingu**
Cíl procesu	Zajištění řízení systému řízení rizik tak, aby rizika využívání služeb cloud computingu byla analyzována, identifikována, vyhodnocována, monitorována a byla realizována opatření pro optimalizaci úrovně rizik tak, aby úroveň rizik spojených s využíváním služeb cloud computingu byla pro organizaci přijatelná
Popis procesu	Proces zajišťuje, že realizaci účinného a efektivního systému řízení rizik z využívání služeb cloud computingu. Umožňuje, aby rizika služeb cloud computingu byla identifikována a řízena tak, aby úroveň rizika pro hodnotu byznysu byla na optimální a akceptovatelné úrovni. Proces zabezpečuje, že změny v prostředí jsou neustále sledovány a je na ně reagováno se zohledněním míry přijatelného rizika z využívání služeb cloud computingu, kterou je podnik ochoten přijmout a úrovní tolerance rizika v závislosti na požadavcích zainteresovaných stran. Proces stanovuje postupy řízení rizik z využívání služeb cloud computingu tak, aby riziko nepřekračovalo míru přijatelného rizika, postupy kontinuálního sledování a vyhodnocování míry přijatelného rizika a postupy identifikace, hlášení a realizace opatření ke snižování rizik z využívání služeb cloud computingu a postupy pro vymezení rolí a odpovědností při řízení rizik z využívání služeb cloud computingu.
Událost	Strategické rozhodnutí o využívání služeb cloud computingu, změna v byznys strategii**.**
Vstup	Byznys strategie, cloud computing strategie.

Výstup	Mechanismy a principy zabezpečující optimalizaci rizik z využívání služeb cloud computingu.
Procesní aktivity	Vytvoření, údržba, prosazování, monitorování a vyhodnocování systému řízení rizik z využívání služeb cloud computingu.

Tabulka 10: Proces GP4 Zajištění systému řízení souladu s interními standardy a normami, s legislativními a regulatorními předpisy a smluvními požadavky, zdroj: (autor)

Číslo procesu	**GP4**
Jméno procesu	**Zajištění systému řízení souladu s interními standardy a normami, s legislativními a regulatorními předpisy a smluvními požadavky**
Cíl procesu	Zajištění systému řízení souladu s interními standardy a normami, s legislativními a regulatorními předpisy a smluvními požadavky tak, aby byl zajištěno, že služby cloud computingu jsou provozovány v souladu s požadavky vyplývajícími z interních standardů a norem a z legislativních a regulatorních předpisů a ze smluvních požadavků, a že jsou definovány procedury pro analýzu a hodnocení souladu služeb cloud computingu, a že jsou realizována opatření pro odstranění nesouladu služeb cloud computingu s požadavky vyplývajícími z interních standardů a norem, z legislativních a regulatorních předpisů a ze smluvních požadavků.
Popis procesu	Proces zajišťuje vytvoření systému řízení souladu s interními standardy a normami, s legislativními a regulatorními předpisy a smluvními požadavky. Proces zabezpečuje, že relevantní požadavky související s využíváním služeb cloud computingu jsou identifikovány, je vyhodnocena jejich důležitost pro organizaci, jsou komunikovány příslušným zainteresovaným stranám, jsou vytvořeny procedury pro jejich aplikaci a procedury pro monitorování souladu služeb cloud computingu s těmito požadavky.
Událost	Strategické rozhodnutí o využívání služeb cloud computingu, změna v byznys strategii**.**
Vstup	Byznys strategie, cloud computing strategie.
Výstup	Mechanismy a principy zabezpečující řízení souladu provozovaných služeb cloud computingu s interními standardy a normami, s legislativními a regulatorními předpisy a smluvními požadavky.
Procesní aktivity	Vytvoření, údržba, prosazování, monitorování a vyhodnocování systému řízení souladu s interními standardy a normami, s legislativními a regulatorními předpisy a smluvními požadavky.

Tabulka 11: Proces GP5 Zajištění systému monitorování a reportingu využívání služeb cloud computingu, zdroj: (autor)

Číslo procesu	**GP5**
Jméno procesu	**Zajištění systému monitorování a reportingu využívání služeb cloud computingu**
Cíl procesu	Zajištění řízení systému monitorování parametrů a metrik využívaných služeb cloud computingu a vytváření reportů pro potřeby vrcholového managementu.
Popis procesu	Proces zajišťuje realizaci systému monitorování služeb cloud computingu a reportingu, který bude poskytovat data o výkonnosti využívaných služeb cloud

	computingu z hlediska jejich přínosu pro tvorbu byznys hodnoty a z hlediska jejich souladu s byznys strategií a cloud computing strategií.
Událost	Strategické rozhodnutí o využívání služeb cloud computingu, změna v byznys strategii.
Vstup	Byznys strategie, cloud computing strategie.
Výstup	Mechanismy a principy zabezpečující monitorování a reporting využívání služeb cloud computingu z hlediska jejich přínosu pro tvorbu byznys hodnoty.
Procesní aktivity	Vytvoření, údržba, prosazování, monitorování a vyhodnocování systému monitorování a reportingu využívání služeb cloud computingu.

Tabulka 12: Proces GP6 Zajištění optimalizace výběru služeb cloud computingu, zdroj: (autor)

Číslo procesu	**GP6**
Jméno procesu	**Zajištění optimalizace výběru služeb cloud computingu**
Cíl procesu	Zajištění, že výběr služeb cloud computingu je prováděn takovým způsobem, aby využívané portfolio služeb cloud computingu bylo optimalizováno z hlediska výkonnosti služeb cloud computingu a z hlediska nákladů na provoz služeb cloud computingu.
Popis procesu	Proces zajišťuje, že správa portfolia služeb cloud computingu bude prováděna takovým způsobem, že organizace využívá služby cloud computingu právě v takovém rozsahu, který je pro realizaci byznys procesu optimální. Proces zároveň zajišťuje, že náklady na provoz služeb cloud computing jsou řízeny tak, aby byly maximalizovány benefity z využívání služeb cloud computingu.
Událost	Strategické rozhodnutí o využívání služeb cloud computingu, změna v byznys strategii.
Vstup	Byznys strategie, cloud computing strategie.
Výstup	Mechanismy a principy zabezpečující optimalizaci výběru služeb cloud computingu.
Procesní aktivity	Vytvoření, údržba, prosazování, monitorování a vyhodnocování systému optimalizace výběru služeb cloud computingu.

6.1.4 Role cloud computing governance

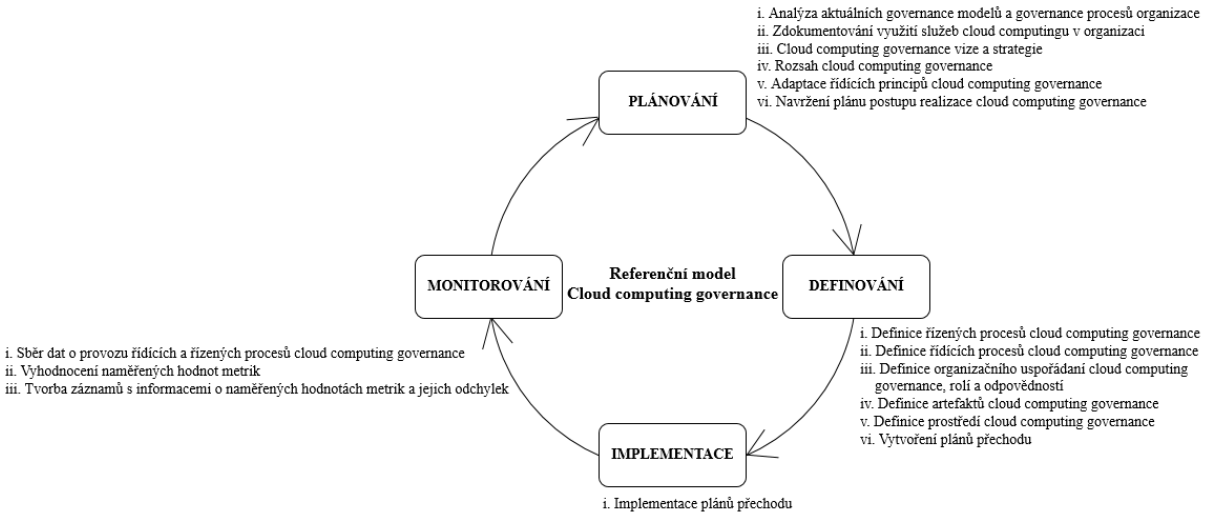
Na návrhu a realizaci modelu cloud computing governance se podílí řada pracovníků, kteří v rámci jejich vymezených rolí provádí akce odpovídající zaměření těchto rolí. Role mohou být nově definovány na základě potřeb governance služeb cloud computingu nebo mohou být stávající byznys manažerské a IT role rozšířeny s ohledem na potřeby zajištění systému cloud computing governance. Souhrnně definované role v rámci governance struktur pro realizaci Cloud computing governance definovaného metodickým rámcem CCGM jsou uvedené v Tabulce 13.

Tabulka 13: Role cloud computing governance, zdroj: (autor)

Struktura	Role	Odpovědnost
Byznys/IT Řídící Výbor	Chief Information Officer (CIO)	Koordinace a plánování byznys cílů a cloud computing cílů Koordinace a plánování byznys strategie a cloud computing strategie Rozhodování o akceptovatelnosti služeb cloud computingu Rozhodování, které klíčové byznys procesy mohou být podporovány formou veřejných služeb cloud computingu Rozhodování, které klíčové byznys procesy nesmí být podporovány formou veřejných služeb cloud computingu Plánování a schvalování investic do využití služeb cloud computingu
Cloud Computing Governance Řídící Skupina	Cloud Computing Governance Chief Cloud Computing Architekt Cloud Computing Compliance Chief	Definice cloud computing cílů Definice cloud computing strategie Definice cloud computing governance vize a strategie Definice rozsahu cloud computing governance Přijetí rámce cloud computing governance a přizpůsobení governance procesů a rolí a odpovědností pro potřeby organizace Definice cloud computing governance politik Definice cloud computing governance technologií Definice cloud computing governance procesů Definice plánu postupu realizace cloud computing governance Posuzování a schvalování požadavku na změnu
Cloud Computing Governance Vývojový Tým	Cloud Computing Governance Analytik Cloud Computing Governance Projektový Manažer Cloud Computing Governance Vývojář	Analýza governance modelů a governance procesů v organizaci Návrh na změnu modelu cloud computing governance Vytvoření plánů přechodu Implementace plánů přechodu
Provoz Cloud Computing Governance	Cloud Computing Governance Operační Administrátor	Administrace provozu cloud computing governance Sběr a vyhodnocování výstupů z monitorování řídících procesů cloud computing governance a eskalace detekovaných odchylek

6.2 Životní cyklus cloud computing governance

Životní cyklus cloud computing governance je proces, na jehož základě může být Referenční model cloud computing governance individuálně upraven pro potřeby konkrétní organizace. Model cloud computing governance může být v organizaci s využitím životního cyklu cloud computing governance implementován iterativním a inkrementálním způsobem. Životní cyklus cloud computing governance je realizovaný řadou aktivit prováděných v cyklu, který se skládá z fází plánování, definování, implementace a monitorování (viz Obrázek 20). Cílem tohoto cyklu je implementovat Referenční model cloud computing governance a v jednotlivých iteracích kontinuálně zlepšovat úroveň implementovaného modelu.



Obrázek 20: Životní cyklus cloud computing governance, zdroj: (autor)

Plánování

Plánování zahrnuje identifikaci jednotlivých procesů cloud computing governance, u nichž by bylo vhodné provést určitou korekci na základě analýzy monitorování efektivity procesů a na základě výsledků z předchozích cyklů. Plánovací fáze musí reagovat na potřeby a změny potřeb byznys procesů podniku a porovnat je s aktuálním stavem cloud computing governance procesů. Výsledky této analýzy jsou zdokumentovány jako postup změny daného cloud computing governance procesu. Východiskem fáze plánování je zdokumentování potřeb zainteresovaných stran a z nich vyplývajících byznys cílů a dokumentace způsobu, kterým organizace tyto potřeby a cíle naplňuje.

Fáze plánování se skládá z následujících aktivit:

i. Analýza aktuálních governance modelů a governance procesů organizace

Analýza aktuálních governance modelů a governance procesů existujících v organizaci na úrovni byznysu, podnikové nebo IT architektury zkoumá aktuálně implementované modely podnikové governance, governance podnikové architektury, IT governance nebo SOA governance. Cílem této aktivity je najít výchozí body pro vytvoření, respektive udržování modelu cloud computing governance.

Hodnocení zralosti modelu cloud computing governance umožní pochopení aktuální úrovně vyspělosti modelu cloud computing governance implementovaného v organizaci a zda je cloud computing governance definována na úrovni odpovídající potřebám organizace. Hodnocení zralosti poskytuje

zpětnou vazbu vrcholovému vedení a napomáhá při definici cloud computing governance strategie. Úrovně zralosti cloud computing governance zobrazuje Tabulka 14.

Tabulka 14: Úrovně zralosti cloud computing governance, zdroj: (autor), podle: (Svatá, 2011)

Úroveň 0: Neexistující cloud computing governance
Cloud computing governance není implementovaná. Procesy cloud computing governance nejsou definovány ani prováděny. Není rozpoznána potřeba cloud computing governance.
Úroveň 1: Počáteční/ad hoc cloud computing governance
Chybějící nebo neadekvátně definované praktiky a procesy cloud computing governance, které jsou prováděné ad hoc, nekonzistentně a závisí na zkušenostech pracovníků IT oddělení. Vedoucí IT oddělení rozpoznal potřebu cloud computing governance.
Úroveň 2: Opakovaná cloud computing governance
Praktiky, politiky a procesy cloud computing governance jsou definované a implementované. Vrcholové vedení dohlíží nad definicí a rozvojem modelu cloud computing governance. Je plánováno vytvoření Byznys/IT Řídícího Výboru v rámci governance struktury. Role a odpovědnosti nejsou explicitně definovaná. Politiky nejsou řádně komunikované relevantním zainteresovaným stranám.
Úroveň 3: Definovaná cloud computing governance
Cloud computing governance politiky a řízené procesy jsou standardizovaný, implementovaný, dokumentovaný a komunikovaný zainteresovaným stranám a zaměstnancům prostřednictvím formálního školení. Role a jim přiřazené odpovědnosti jsou jasně pochopeny a praktikovány. Řídící procesy nejsou plně implementované, a tudíž odchylky provádění řízených procesů nejsou detekovány. Byznys/IT Řídící Výbor spolupracuje s byznysem při rozhodování o strategických byznys a cloud computing cílech.
Úroveň 4: Řízená a měřitelná cloud computing governance
Soubor ukazatelů výkonnosti a metrik pro měření shody s politikami cloud computing governance je definován. Cloud computing governance procesy jsou monitorovány a hodnoceny v závislosti na statistických a kvalitativních technikách. Výstupy cloud computing governance procesů jsou v rámci nastavených limitů. Zlepšování cloud computing governance je založeno na kvantitativních metrikách. Cíle cloud computingu jsou v souladu s byznys cíli a cloud computing governance zajišťuje efektivní podporu tvorby byznys hodnoty prostřednictvím realizace benefitů z využití služeb cloud computingu.
Úroveň 5: Optimalizovaná cloud computing governance
Cloud computing governance je součást podnikové governance. Cloud computing governance je přizpůsobená konkrétnímu byznys prostředí, je optimalizovaná a neustále zlepšovaná. Byznys/IT Řídící Výbor se plně podílí na koordinaci a plánování byznys cílů, cílů v oblasti využívání služeb cloud computingu, byznys strategie, cloud computing strategie a v součinnosti s byznysem rozhoduje o investicích do služeb cloud computingu.

ii. Zdokumentování využití služeb cloud computingu v organizaci

Tato aktivita se skládá ze dvou základních částí. Obsahem první části je dokumentace stávajícího stavu využití služeb cloud computingu v organizaci. Druhá část představuje dokumentaci cílového stavu využití služeb cloud computingu v organizaci, kterého chce organizace v budoucnu dosáhnout. Jedná se tedy o provedení gap analýzy, jejíž výsledky následně slouží k formování plánu postupu realizace cloud computing governance.

iii. Cloud computing governance vize a strategie

Cílem této aktivity je vytvořit dlouhodobou vizi pro cloud computing governance a strategii pro realizaci této vize v organizaci. Při realizaci cloud computing governance vize se vychází z řídících

principů cloud computing governance a z byznys strategie organizace. Součástí strategie pro realizaci cloud computing governance vize by měla být definice návratnosti investice cloud computing governance aktivit, metrik pro měření hodnoty z cloud computing governance aktivit a prioritizace aktivit v rámci strategie cloud computing governance.

iv. Rozsah cloud computing governance

Definice rozsahu cloud computing governance zahrnuje identifikaci zájmů zainteresovaných stran, identifikaci potřebných procesů cloud computing governance a identifikaci potřebné úrovně řízení s cílem omezit se pouze na takové objekty cloud computing governance tak, aby cloud computing governance pokrývala pouze relevantní a skutečně potřebné objekty a byla realizovatelná s akceptovatelnými náklady a v akceptovatelném čase.

v. Adaptace řídících principů cloud computing governance

Účelem této aktivity je přizpůsobení a rozšíření řídících principů cloud computing governance pro konkrétní organizaci v souladu s podnikovými a IT principy a cloud computing strategií podniku, aktuální úrovní využívání služeb cloud computingu a požadavky zainteresovaných stran.

vi. Navržení plánu postupu realizace cloud computing governance

Plán postupu realizace cloud computing governance definuje počet iterací životního cyklu cloud computing governance. Během realizace prvního cyklu se provádí iniciální nasazení cloud computing governance. Během dalších iterací může být postupně realizována celá cloud computing governance vize. V případě, že během provádění jednotlivých cyklů dojde ke změně ve využívání služeb cloud computingu, je zapotřebí, aby se tato změna projevila i v plánu postupu realizace cloud computing governance.

Definování

Definování zahrnuje definici kroků nutných k realizaci cílů z fáze plánování. Výstupem fáze definování jsou plány postupů, pomocí nichž dojde k iniciálnímu nasazení cloud computing governance nebo k plánovaným změnám v jednotlivých oblastech cloud computing governance.

Fáze definování se skládá z následujících aktivit:

i. Definice řízených procesů cloud computing governance

Účelem této aktivity je identifikovat procesy cloud computingu, jejichž nastavení nebo způsob aplikování v praxi podniku neodpovídá požadavkům na jejich řízení z hlediska cloud computing governance. Zároveň je zde definováno, jak má být identifikovaný cloud computing proces upraven, aby splňovat požadavky na jeho cloud computing governance z hlediska cloud computing governance rozsahu, vize a strategie.

ii. Definice řídících procesů cloud computing governance

Účelem této aktivity je nastavení řídících procesů cloud computing governance tak, aby vyhovovaly potřebám podniku.

- Proces řízení shody – je zde definována metoda, která bude v podniku použita pro tvorbu cloud computing směrnic a podnikových cloud computing norem. Směrnice a normy pro cloud computing musí obsahovat prvky, které umožní aplikovatelnost procesu řízení shody. Obecně je zde nutno definovat všechny aspekty potřebné pro jeho provoz včetně potřebných technologií.

- Proces řízení výjimek – je zde definováno, za jakých podmínek a jakým způsobem bude při zjištěné odchylce detekované procesem řízení shody spuštěn mechanismus procesu řízení výjimek. Jsou zde definována kritéria pro ohodnocení druhu a závažnosti výjimky a jsou zde stanovena pravidla eskalačního postupu pro dodání informací o zjištěné odchylce příslušným rolím.
- Proces řízení komunikace – je zde definováno, jaké metody budou v podniku použity pro tvorbu komunikačních procesů cloud computingu, aby bylo zajištěno, že cloud computing governance politiky budou v těchto procesech plně realizovatelné. S tím opět souvisí potřeba definovat technologie pro provoz procesu řízení komunikace.

iii. Definice organizačního uspořádaní cloud computing governance, rolí a odpovědností

Účelem této aktivity je definice organizačního uspořádání cloud computing governance a souvisejících rolí a odpovědností. Výchozím bodem je obecný Referenční model cloud computing governance, který je upraven tak, aby vyhovoval specifickým potřebám podniku jak z hlediska organizačního uspořádání cloud computing governance, tak z hlediska v podniku definovaných cloud computing governance rolí a zodpovědností. Může se stát, že pro realizování byznys cílů podniku je vhodné vytvořit role nebo odpovědnosti, které v obecném Referenčním modelu cloud computing governance nejsou uvedeny. Taková situace může být např. spojena s velmi specifickou nebo úplně novou oblastí byznysu.

iv. Definice artefaktů cloud computing governance

V průběhu životního cyklu cloud computing governance dochází ke tvorbě a modifikaci artefaktů, které definují jednotlivé komponenty Cloud computing governance. Tyto artefakty se skládají z dokumentů ustanovujících Referenční model cloud computing governance, definujících politiky, procesy, role a odpovědnosti a z dalších dokumentů souvisejících s plánováním, implementací a s řízením provozu Cloud computing governance (viz Tabulka 15). Účelem této aktivity je identifikovat artefakty jak řídících, tak řízených procesů cloud computing governance, které je zapotřebí upravit, nově vytvořit, nahradit novými nebo zrušit. Důležité je se věnovat nejen existenci nebo absenci artefaktů, ale i jejich obsahu a věcné správnosti.

Tabulka 15: Cloud computing governance artefakty, zdroj: (autor)

Cloud computing governance artefakty	Typy Cloud computing governance artefaktů
Artefakty strategického řízení Cloud computing governance	Prohlášení o akceptaci cloud computingu organizací Dokument definující cloud computing cíle Cloud computing strategie Cloud computing governance vize a strategie Cloud computing governance rozsah Cloud computing governance příručka Komunikační plán
Artefakty ustanovení Cloud computing governance	Cloud computing governance řídící principy Cloud computing governance politiky Cloud computing governance procesy Seznam metrik cloud computing governance procesů a jejich hodnot Organizační struktura cloud computing governance Seznam rolí a odpovědností cloud computing governance

Cloud computing governance artefakty	Typy Cloud computing governance artefaktů
	Cloud computing governance technologie
Artefakty životního cyklu cloud computing governance	Plán postupu realizace cloud computing governance Plány přechodu Hodnocení governance modelů a governance procesů v organizaci Záznamy o schválených výjimkách governance procesů Záznamy o obnovení shody governance procesů Změnové dokumenty

v. Definice prostředí cloud computing governance

Cloud computing governance technologie jsou určeny pro realizaci a podporu řídících procesů cloud computing governance. Mohou být ve formě od jednoduchých nástrojů pro manuální realizaci řídících procesů cloud computing governance až po plně sofistikovaný software umožňující automatizaci řídících procesů cloud computing governance. Cloud computing governance technologie by se měly skládat z následujících částí:

- systém pro ukládání a správu artefaktů – účelem systému je ukládat a spravovat cloud computing governance artefakty a uživatelům umožnit přístup k těmto artefaktům v závislosti na jejich oprávněních. Oprávnění uživatele mohou artefakty číst nebo modifikovat případně vytvářet nové artefakty nebo zastaralé artefakty ze systému mazat. Důležitou funkcionalitou systému pro ukládání a správu artefaktů je schopnost správy verzí artefaktů.
- systém pro monitorování a detekci odchylek cloud computing governance politik – jedná se o monitorovací technologie umožňující detekovat odchylky politik aktuálně provozované cloud computing governance od definovaných cloud computing 0governance politik. Tyto technologie mohou být opět realizovány jako manuální periodická činnost, avšak optimální bude využít automatizované monitorovací systémy, které provádějí vyhledávání odchylek automaticky a po detekci odchylky vytvoří automaticky hlášení o výjimce a v souladu se stanoveným eskalačním procesem je odešle příslušným rolím.
- systém pro monitorování úrovně cloud computing governance – jedná se o monitorovací technologie, které měří stanovené metriky cloud computing governance procesů a stanovené metriky poskytovaných cloud computing služeb. Analýza naměřených hodnot metrik a jejich odchylek od požadovaných hodnot slouží k ohodnocení aktuální úrovně cloud computing governance, aktuální úrovně aplikace cloud computing governance politik a k ohodnocení správnosti a přiměřenosti implementovaného cloud computing governance systému. Výstupy z tohoto monitorování nejsou spojeny s eskalačním procesem. Jsou k dispozici rolím, které je využijí v rámci svých řídících odpovědností nebo rolím, které mají oprávněný zájem být o výstupech z monitorování úrovně cloud computing governance informovány.
- systém pro řízení provozu cloud computing governance – jedná se o nástroje např. typu ITSM podle ITIL. Jde o to, aby organizace měla k dispozici jedno centrální místo nebo centrální aplikaci, kde jsou k dispozici uživatelům nebo rolím podklady a dokumenty pro řízení životního cyklu cloud computing governance. Mohou to být artefakty, incidenty, změnové požadavky atd. Optimální je mít možnost využít při implementaci nebo následné údržbě cloud computing governance systému automatizované funkcionality pro podporu procesování řídících podkladů a dokumentů.

Účelem této aktivity je definovat, jaké technologie a nástroje nebo aplikace jsou zapotřebí pro realizaci cloud computing governance v podniku. Provádí se analýza, zda v podniku existující technologie je možno využít pro realizaci cloud computing governance a zda mají dostatek zdrojů. Provádí se analýza technologií dostupných na trhu včetně jejich nákladové náročnosti. Na základě porovnání výsledků těchto analýz se definují požadavky na rozšíření stávající technologie nebo požadavky na pořízení technologií nových. Podobně se provádí analýza již existujících nástrojů a aplikací, vyhodnocuje se jejich funkcionalita a výkonnost. Porovnávají se s dalšími aplikacemi existujícími na trhu. Důležité je vzít v potaz, do jaké míry nástroje a aplikace reprezentují obecně uznávané standardy, jak jsou schopny podporovat realizaci podnikové vize, strategie a rozsahu cloud computing governance a jaké jsou jejich schopnosti automatizovat procesy cloud computing governance. Na základě výsledků těchto analýz se definují změny nebo úpravy stávajících nástrojů a aplikací, aktivace jejich dosud nevyužívaných funkcionalit nebo přechod na nový nástroj nebo aplikaci.

vi. Vytvoření plánů přechodu

Účelem této aktivity je vytvořit plány přechodu, definující postupy, jakými chce podnik dosáhnout realizace přechodu z aktuálního do definovaného cílového stavu cloud computing governance. Protože cloud computing governance je rozšířením IT governance a SOA governance, musí být plány přechodu cloud computing governance buď součástí plánů přechodu IT, IT governance a SOA governance nebo musí být s nimi plně sladěny. Stejně jako plány přechodu IT, IT governance a SOA governance jsou i plány přechodu cloud computing governance vytvářeny pro tři oblasti, kterými jsou:

- organizační uspořádání, role a odpovědnosti,
- procesy,
- technologie.

V plánech přechodu všech těchto tří oblastí jsou zahrnuty i plány přechodu pro příslušné artefakty. Plány přechodů podrobně definují postup, který bude použit v následné fázi implementace. Jedná se o posloupnost činností definovaných a popsaných v takovém stupni podrobností, který definuje projektovým, akvizičním, školícím, vývojovým, testovacím a implementačním týmům obsah jejich činností a zároveň umožňuje transparentním způsobem řídit a vyhodnocovat průběh implementace. V řadě případů popis kroku v rámci některého plánu přechodu nepostačuje pro plné definování činností některého týmu. Zde je pak nutno vytvořit příručku, ve které je činnost jednoho nebo více zúčastněných týmů popsána v potřebném detailu. Typickým příkladem je změna v aplikaci, kdy je potřeba definovat jaká funkcionalita má být změněna, jaká má být cílová funkcionalita, jakými testy má testovací tým prověřit cílovou funkcionalitu atd. Jinými slovy, musí zde být v rámci jednoho kroku plánu přechodu cloud computing governance definován např. celý cyklus změny služby. Plány přechodu musí být komunikovány s příslušnými rolemi IT, rolemi byznysu a zainteresovanými stranami s cílem dosáhnout souhlas všech odpovědných v podniku se všemi aspekty plánovaných a definovaných změn včetně způsobů a termínů jejich realizace. Finální verze plánů přechodu tak obsahuje i časový harmonogram realizace fáze implementace.

Implementace

Ve fázi implementace jsou realizovány plány přechodu vytvořené ve fázi definování. Postupuje se podle kroků definovaných v těchto plánech. Na konci fáze implementace je cloud computing governance na úrovni naplánované ve fázi plánování. Stejně tak řešení využívání služeb cloud computingu v podniku je řiditelné a spravovatelné na úrovni naplánované ve fázi plánování.

Monitorování

Monitorování cloud computing governance:

- realizuje sběr dat o provozu řídících a řízených procesů cloud computing governance,
- poskytuje informace o provozu organizačního uspořádání, rolí a odpovědností cloud computing governance,
- vyhodnocuje naměřené hodnoty metrik, porovnává je s definovanými hodnotami,
- generuje výstupy s informacemi o naměřených hodnotách metrik a jejich odchylek

Monitorování shromažďuje informace o úrovni a efektivnosti řídících a řízených procesů cloud computing governance. Umožňuje tím posoudit, zda procesy cloud computing governance jsou provozovány způsobem splňujícím projektované cíle cloud computing governance. Vyhodnocení naměřených hodnot metrik umožňuje určit, v jaké kvalitě jsou tyto cíle plněny. Důležitým aspektem monitorování je tedy jeho schopnost naměřená data vyhodnocovat a porovnávat je s nastavenými hodnotami metrik a poskytovat tak podklady pro rozhodnutí, zda aktuální cloud computing governance optimálně podporuje byznys cíle realizované pomocí služeb cloud computingu, anebo zda je zapotřebí některý prvek cloud computing governance revidovat. Potřebu změny prvku cloud computing governance může evokovat i změna nastavení metriky. Důležitou schopností monitorovacího systému je sledování a vyhodnocování četností změn, neboť příliš vysoká frekvence změn některého prvku cloud computingu může signalizovat nevhodně nebo chybně nastavený prvek cloud computing governance. Zvláštní pozornost je třeba věnovat detekci četnosti akceptace výjimky v procesu řízení shody nebo v procesu řízení výjimek. Vysoká frekvence akceptace výjimky může signalizovat nefunkčnost nebo nedostatečně nízkou úroveň cloud computing governance. K rozhodnutí revidovat některý prvek cloud computing governance může dojít nejen na základě monitorování uvnitř cloud computing governance prostředí, avšak velmi často i z externích příčin. Ke správnému vyhodnocení stavu a úrovně cloud computing governance je proto zapotřebí monitorovat události vyvolané např. změnou v podnikové byznys strategii, změnou v podnikové cloud computing strategii, změnou v organizačním uspořádání podniku nebo změnou v legislativě. Aby monitorování poskytovalo aktuální a správně vypovídající informace, musí monitorování probíhat nepřetržitě. Vyhodnocování naměřených dat se provádí v závislosti na jejich povaze a důležitosti buď také nepřetržitě, nebo v pravidelných časových intervalech podle potřeb podniku.

V kapitole 6 je popsán autorkou této doktorské disertační práce navržený model Cloud computing governance metodického rámce Cloud computing governance a management (CCGM). Cloud computing governance se skládá z Referenčního modelu cloud computing governance a z Životního cyklu cloud computing governance.

V kapitole 6.1 autorka této doktorské disertační práce definovala Referenční model cloud computing governance z hlediska jeho základních komponent. Těmi jsou:

- *Řídící principy cloud computing governance*
- *Řídící procesy cloud computing governance*
- *Řízené procesy cloud computing governance*
- *Role cloud computing governance.*

Řídící principy cloud computing governance (kapitola 6.1.1.) navrhla autorka této doktorské disertační práce prostřednicím návrhu nových a modifikací stávajících Řídících principů SOA Governance vzhledem ke specifikům potřeb governance využívání služeb cloud

computingu. Řídící principy cloud computing governance představují společná pravidla a doporučení pro návrh, nasazení a provozování Referenčního modelu cloud computing governance.

Řídící procesy cloud computing governance (kapitola 6.1.2.) navrhla autorka této doktorské disertační práce prostřednicím modifikace stávajících Řídících procesů SOA Governance vzhledem ke specifikům potřeb governance využívání služeb cloud computingu. Řídící procesy cloud computing governance využívá Referenční model cloud computing governance pro řízení jednotlivých řízených procesů.

Řízené procesy cloud computing governance (kapitola 6.1.3.) navrhla autorka této doktorské disertační práce prostřednicím návrhu nových a modifikací stávajících governance procesů COBIT 5 a Řízených procesů SOA Governance vzhledem ke specifikům potřeb governance využívání služeb cloud computingu. Řízené procesy cloud computing governance slouží k vybudování a prosazování modelu Cloud computing governance v organizaci. Navrženými Řízenými procesy jsou:

- *GP1: Zajištění systému cloud computing governance*
- *GP2: Realizace přínosů z využívání služeb cloud computingu*
- *GP3: Zajištění systému řízení rizik z využívání služeb cloud computingu*
- *GP4: Zajištění systému řízení souladu s interními standardy a normami, s legislativními a regulatorními předpisy a smluvními požadavky*
- *GP5: Zajištění systému monitorování a reportingu využívání služeb cloud computingu*
- *GP6: Zajištění optimalizace výběru služeb cloud computingu*

Role cloud computing governance (kapitola 6.1.4.) navrhla autorka této doktorské disertační práce na základě metodického rámce SOA Governance a zkušeností z praxe pro potřeby Referenčního modelu cloud computing governance.

V kapitole 6.2 autorka této doktorské disertační práce definovala Životní cyklus cloud computing governance. Životní cyklus cloud computing governance navrhla autorka této doktorské disertační práce prostřednicím modifikace SOA Governance Vitální metody a v rámci fáze Plánování navrhla model pro hodnocení Úrovně zralosti cloud computing governance.

7 Cloud computing management

Cílem kapitoly je popsat autorkou této doktorské disertační práce navržený model Cloud computing management metodického rámce Cloud computing governance a management (CCGM). Cloud computing management je vytvořený modifikací metodického rámce ITIL 2011. Cloud computing management se skládá z Řídících principů cloud computing managementu, Rolí cloud computing managementu a fází životního cyklu služby cloud computingu z pohledu spotřebitele.

Pro potřeby této doktorské disertační práce autorka formulovala definici cloud computing managementu, která je odvozena od definice IT managementu (kapitola 2.2), kdy principy IT managementu jsou přizpůsobeny specifikám využívání služeb cloud computingu z pohledu spotřebitele, avšak komponenty management modelu se neliší. Odlišuje se jejich obsah, který musí reflektovat skutečnost, že služby cloud computingu jsou poskytovány externím poskytovatelem služeb cloud computingu, který je zodpovědný za jejich návrh, poskytování, údržbu a za řízení infrastruktury potřebné pro provoz služeb. Definice cloud computing management je formulována následovně:

Cloud computing management je výkonný řídicí systém, který zabezpečuje efektivní využívání služeb cloud computingu a zajišťuje, že cíle stanovené cloud computing governance budou dosaženy prostřednictvím souboru aktivit, které realizují plánování, výběr, osvojení, nasazení, provoz, monitorování a ukončení využívání služeb cloud computingu poskytovaných externím poskytovatelem služeb cloud computingu.

Cloud computing management definuje model řízení životního cyklu služeb cloud computingu z pohledu spotřebitele, který vychází z životního cyklu řízení IT služeb dle ITIL a respektuje management procesy rámce COBIT. Zaměřuje se na strategickou, taktickou a operativní úroveň řízení služeb cloud computingu od plánování až po vyřazení služby cloud computingu z produktivního provozu a to tak, aby služba byla ve shodě s politikami cloud computing governance a potřebami byznys procesů. Cloud computing management z pohledu spotřebitele řídí:

- plánování využívání služby cloud computingu,
- výběr služby cloud computingu,
- osvojení služby cloud computingu,
- instalaci a integraci služby cloud computingu,
- provoz služby cloud computingu,
- monitorování a hodnocení služby cloud computingu,
- ukončení provozu služby cloud computingu.

Životní cyklus služby cloud computingu z pohledu spotřebitele služby cloud computingu se skládá z fází, v rámci, kterých jsou seskupeny procesy pro řízení životního cyklu služby cloud computingu. Tyto fáze odráží logickou návaznost jednotlivých procesů či skupin procesů při přízemí životního cyklu služby cloud computingu. Fáze řízení životního cyklu služby cloud computingu z pohledu spotřebitele jsou:

- (CM1) Strategie využití služeb cloud computingu
- (CM2) Výběr služby cloud computingu
- (CM3) Přechod na využívání služby cloud computingu

- (CM4) Provoz služby cloud computingu
- (CM5) Nepřetržité zdokonalování služby cloud computingu

Navržené fáze životního cyklu služby cloud computingu z pohledu spotřebitele služeb cloud computingu vychází z fází životního cyklus IT služby dle ITIL 2011. Tabulka 16 uvádí porovnání fází životního cyklu řízení cloud computing služby a IT služby.

Tabulka 16: Vazba životního cyklu služby cloud computingu na životní cyklus IT služby dle ITIL 2011, zdroj: (autor)

Fáze životního cyklu služby cloud computingu metodického rámce CCGM	Fáze životního cyklu IT služby dle ITIL 2011 (The Cabinet Office, 2011)
(CM1) Strategie využití služeb cloud computingu	Strategie služby (Service Strategy)
(CM2) Výběr služby cloud computingu	Návrh služby (Service Design)
(CM3) Přechod na využívání služby cloud computingu	Přechod služby do produktivního provozu (Service Transition)
(CM4) Provoz služby cloud computingu	Provoz služby (Service Operation)
(CM5) Nepřetržité zdokonalování služby cloud computingu	Nepřetržité zdokonalování služby (Continual Service Improvement)

Každá fáze životního cyklu služby cloud computingu obsahuje soubor procesů s jasně vymezeným rozsahem, který je daný souborem procesních aktivit. Fáze životního cyklu na sebe logicky navazují a zároveň jsou navzájem propojené s cílem zajistit realizaci byznys hodnoty z využívání služby cloud computingu. Toto propojení fází je realizovatelné prostřednictvím zabezpečení integrace procesů, kdy spolu procesy spolupracují a vzájemně si předávají informace potřebné pro realizaci procesních aktivit. Procesy definované v jednotlivých fázích životního cyklu řízení služby cloud computingu zobrazuje následující Tabulka 17.

Tabulka 17: Seznam procesů v rámci jednotlivých fází životního cyklu služby cloud computingu metodického rámce CCGM, zdroj: (autor)

Fáze životního cyklu služby cloud computingu metodického rámce CCGM	Management procesy metodického rámce CCGM
(CM1) Strategie využití služeb cloud computingu	CMS1: Řízení rizik z využití služby cloud computingu CMS2: Finanční řízení služby cloud computingu CMS3: Řízení souladu s interními standardy a normami, s legislativními a regulatorními předpisy a smluvními požadavky CMS4: Řízení exit strategie CMS5: Řízení portfolia poskytovatelů služeb cloud computingu CMS6: Řízení portfolia služeb cloud computingu CMS7: Řízení smluv o poskytování služby cloud computingu
(CM2) Výběr služby cloud computingu	CMD1: Řízení výběru služby cloud computingu
(CM3) Přechod na využívání služby cloud computingu	CMT1: Plánování přechodu na využívání služby cloud computingu CMT2: Testování a validace služby cloud computingu CMT3: Řízení přístupu uživatele ke službě cloud computingu CMT4: Řízení nasazení služby cloud computingu do produktivního provozu

Fáze životního cyklu služby cloud computingu metodického rámce CCGM	Management procesy metodického rámce CCGM
(CM4) Provoz služby cloud computingu	CMO1: Řízení událostí CMO2: Řízení incidentů CMO3: Řízení problémů CMO4: Řízení požadavků na službu cloud computingu CMO5: Řízení požadavků na přístup ke službě cloud computingu CMO6: Monitorování provozu služby cloud computingu
(CM5) Nepřetržité zdokonalování služby cloud computingu	CMI1: Řízení nepřetržitého zdokonalování služby cloud computingu

7.1 Řídící principy cloud computing managementu

Řídící principy cloud computing managementu definují společná pravidla a doporučení pro návrh, nasazení a provozování modelu Cloud computing management v organizaci. Umožňují podpořit a efektivněji využívat služby cloud computingu v souladu s byznys požadavky a s Cloud computing governance, slouží jako podpora při návrhu politik provozu IT a stanovují hranici operací managementu služeb cloud computingu. Řídící principy cloud computing governance jsou následující:

ŘPM1: Cloud computing management musí být v souladu s podnikovým managementem a IT managementem a musí být podporována výkonným vedením. Soulad modelů managementu v organizaci, ve smyslu souladu podnikového managementu, IT managementu a cloud computing managementu umožňuje vytvoření jednotného modelu, který zabezpečuje, že management služeb cloud computingu vychází z IT managementu a rozšiřuje jej o specifika využívání služeb cloud computingu. Tento princip zabraňuje vytváření paralelních management struktur v organizaci. Potřeba a důležitost cloud computing managementu jako součást řízení IT musí být podporována vrcholovým managementem a musí vycházet z potřeb podniku a zainteresovaných stran.

ŘPM2: Vytvoření, rozvoj a ukončení vztahu mezi poskytovatelem a spotřebitelem musí být založeno na smluvní dohodě vymahatelné zákonem. Poskytovatel služeb cloud computingu přebírá zodpovědnost za návrh, poskytování, údržbu a řízení služeb. Mezi poskytovatelem a spotřebitelem musí existovat smluvní dohoda o poskytování služby a dohoda o úrovni služby, která zabezpečuje, že poskytovaná služba splňuje dohodnuté parametry uspokojující potřeby spotřebitele.

ŘPM3: Data o dodávaných službách cloud computingu musí být udržovaná v systému metadat služeb cloud computingu. Systém metadat služeb cloud computingu zabezpečuje centrální řízení dat vztahujících se ke službám cloud computingu jako je popis služby, vztahy mezi službami, smluvní dohody a dohody o úrovni služeb a se službami související dokumenty. Systém metadat služeb cloud computingu umožňuje, aby relevantní zainteresované strany měly dosažitelné a transparentní informace o účelu služby a jejím postavení v kontextu ostatních služeb.

ŘPM4: Data o poskytovatelích služeb cloud computingu musí být udržovaná v systému metadat o poskytovatelích služeb cloud computingu. Systém metadat o poskytovatelích služeb cloud computingu poskytuje informace vztahující se k poskytovatelům služeb, k jejich výběru, řízení vztahu a k ukončení vztahu. Metadata obsahují informace nutné pro zabezpečení požadavku organizace na bezpečnost a důvěrnost implementovanou ve službách a na ohodnocení důvěryhodnosti poskytovatele.

ŘPM5: Rizika související s využíváním služeb cloud computingu musí být efektivně řízená. Pro řízení rizik souvisejících s využíváním služeb cloud computingu je nutné zajistit vybudování potřebné infrastruktury a systematického přístupu zjišťování rizik, hodnocení jejich nebezpečnosti a nežádoucích důsledků, zvládání rizik a monitorování rizik tak, že tato rizika budou eliminována, minimalizována, včas předvídána, bude snížen jejich dopad a to způsobem, který dovolí minimalizovat ztráty a maximalizovat zisky.

ŘPM6: Náklady na provoz služeb cloud computingu musí být efektivně řízené. Identifikace nákladů na přijetí a využívání služby cloud computingu a jejich pravidelné vyhodnocování s využitím správných a včasných relevantních informací umožní dosahovat redukce a optimalizace nákladů při zabezpečení všech provozních charakteristik služby cloud computingu. Zároveň zhodnocení nákladů oproti očekávaným benefitům umožní efektivně racionalizovat využití služby cloud computingu.

ŘPM7: Výkonnost služeb cloud computingu musí být efektivně řízená. Výkonnostní parametry služby cloud computingu musí jasně vyplývat z byznys požadavků na využití služby cloud computingu. Tyto požadavky musí být převedeny na konkrétní kvalitativní ukazatele, které budou obsažené ve smlouvách o poskytování služby cloud computingu, specificky v SLA. Tyto smlouvy musí být uzavřeny mezi poskytovatelem služby cloud computingu a spotřebitelem služby cloud computingu. K zabezpečení prosazování SLA musí být realizovány aktivity pro ujištění o dodání služby cloud computingu na úrovni výkonnostních parametrů služby definovaných v SLA. Služba cloud computingu musí být monitorována a na základě monitorovacích dat ověřována její úroveň výkonnosti pomocí porovnání skutečně naměřených hodnot s hodnotami definovanými v SLA a musí být iniciována realizace příslušných opatření v případě odchylek hodnot těchto parametrů a nedodržení smluvních podmínek.

ŘPM8: Provoz služeb cloud computingu musí být kontinuálně řízen tak, aby využívané služby cloud computingu nepřetržitě splňovaly kritéria obsažená v SLA a požadavky byznysu a aby odchylky od těchto kritérií byly detekovány a eliminovány. Stanovení jasných postupů a procedur operativního využití služby cloud computingu umožní dosažení účinnosti a efektivity při provozu služby cloud computingu s cílem podpory souvisejících byznys procesů a dosažení hodnoty pro byznys.

ŘPM9: Pro efektivní podporu modelu cloud computing management musí být dostupné potřebné umožňující schopnosti a prostředí. Organizace musí mít k dispozici potřebné nástroje a technologie pro podporu všech fází životního cyklu služby cloud computingu.

7.2 Role cloud computing managementu

Na řízení životního cyklu služby cloud computingu se podílí řada osob v různých rolích. Tyto role mohou být zcela nově definovány na základě potřeb řízení využívání služby cloud computingu nebo se může jednat o stávající IT role, jejichž odpovědnosti ve vztahu k realizaci procesu jsou rozšířené s ohledem na prostředí využívání služeb cloud computingu v modelu veřejného cloud computingu. Souhrnně definované role pro jednotlivé fáze životního cyklu služby cloud computingu metodického rámce CCGM jsou uvedené v Tabulce 18. Vymezení základních odpovědností jednotlivých rolí je definováno v příloze A.

Tabulka 18: Cloud computing management role, zdroj: (autor)

Fáze životního cyklu služby cloud computingu	Proces	Role
(CM1) Strategie využití služeb cloud computingu		Chief Information Officer
		Cloud computing analytik
	CMS1: Řízení rizik z využití služby cloud computingu	Manažer řízení rizik cloud computingu
	CMS2: Finanční řízení služeb cloud computingu	Finanční manažer služeb cloud computingu
	CMS3: Řízení souladu s interními standardy a normami, s legislativními a regulatorními předpisy a smluvními požadavky	Manažer pro řízení souladu služeb cloud computingu s legislativou
	CMS4: Řízení exit strategie	Manažer cloud exit strategie
	CMS5: Řízení portfolia poskytovatelů služeb cloud computingu	Manažer portfolia poskytovatelů a řízení vztahu s poskytovateli
	CMS6: Řízení portfolia služeb cloud computingu	Manažer katalogu služeb cloud computingu
	CMS7: Řízení smluv o poskytování služby cloud computingu	Cloud SLA manažer
(CM2) Výběr služby cloud computingu	CMD1: Řízení výběru služby cloud computingu	Manažer služeb cloud computingu
(CM3) Přechod na využívání služby cloud computingu	CMT1: Plánování přechodu na využívání služby cloud computingu	Manažer přechodu na využití služby cloud computingu
	CMT2: Testování a validace služby cloud computingu	Cloud test manažer
	CMT3: Řízení přístupu uživatele ke službě cloud computingu	Manažer pro řízení přístupu ke službě
	CMT4: Řízení nasazení služby cloud computingu do produktivního provozu	Manažer nasazení služeb cloud computingu
(CM4) Provoz služby cloud computingu		Cloud servis desk manažer
		Cloud eskalační manažer
	CMO1: Řízení událostí	Manažer provozu služeb cloud computingu
	CMO2: Řízení incidentů	Cloud incident manažer
	CMO3: Řízení problémů	Cloud problém manažer
	CMO4: Řízení požadavků na službu cloud computingu	Manažer řízení požadavků na službu cloud computingu
	CMO5: Řízení požadavků na přístup ke službě cloud computingu	Manažer řízení požadavků na přístup ke službě cloud computingu

Fáze životního cyklu služby cloud computingu	Proces	Role
	CMO6: Monitorování provozu služby cloud computingu	Cloud monitoring manažer
(CM5) Nepřetržité zdokonalování služby cloud computingu	CMI1: Řízení nepřetržitého zdokonalování služby cloud computingu	Manažer nepřetržitého zdokonalování služby cloud computingu

7.3 Strategie využití služeb cloud computingu

Strategická úroveň řízení služeb cloud computingu napomáhá pochopení realizace byznys cílů a naplnění potřeb zainteresovaných stran prostřednictvím využívání služeb cloud computingu. Procesy realizované v rámci fáze strategie využití služeb cloud computingu pomáhají organizaci dosáhnout požadované úrovně byznys hodnoty z využívání služeb cloud computingu. Byznys hodnota, kterou má přinést využití služeb cloud computingu odráží míru, v jaké služba splňuje požadavky zainteresovaných stran a umožňuje dosažení byznys cílů. Hodnota z využití služeb by měla být jasně definovaná, akceptovaná a měřitelná, aby bylo možné určit priority využití služeb cloud computingu a stanovit metriky pro měření odchylek skutečně dosažené hodnoty od plánované hodnoty z využití služeb cloud computingu. Tvorba hodnoty z využití služeb cloud computingu musí vycházet z porozumění potřeb zainteresovaných stran, které by měly být transformovány do specifických, přizpůsobitelných a realizovatelných byznys cílů a odráží míru vhodnosti služby cloud computingu pro podporu daného byznys procesu.

Strategie využití služeb cloud computingu definuje prostřednictvím plánu cloud computing strategie způsob, jakým bude organizace realizovat naplnění strategických byznys cílů prostřednictvím využívání služeb cloud computingu. Plán cloud computing strategie obsahuje aktivity, které zabezpečí naplnění strategických byznys cílů a které řídí změny cloud computing strategie v souladu se změnami vnitřního anebo vnějšího prostředí organizace z hlediska využívání služeb cloud computingu. Vytvoření plánu cloud computing strategie je realizováno následujícími aktivitami:

- analýza a hodnocení současného stavu prostředí organizace z hlediska využívání služeb cloud computingu,
- analýza a hodnocení připravenosti organizace pro přijetí služeb cloud computingu,
- analýza aktuálního stavu využívání služeb cloud computingu v organizaci,
- analýza externího prostředí organizace z hlediska využívání služeb cloud computingu,
- definice budoucího stavu využívání služeb cloud computingu v organizaci,
- plánování transformace z aktuálního stavu využívání služeb cloud computingu na budoucí stav využívání služeb cloud computingu.

Analýzu a hodnocení současného stavu prostředí organizace z hlediska využívání služeb cloud computingu zajišťuje posouzení organizace na základě následujících hledisek:

- úroveň souladu byznys cílů, IT cílů a cloud computing cílů,
- míra podpory adopce služeb veřejného cloud computingu ze strany vedení společnosti,
- aktuální management modely a procesy v organizaci,
- aktuálně realizované byznys procesy v organizaci,
- úroveň podnikové kultury z hlediska schopnosti zabezpečit prostředí podporující změnu a přechod na nová podniková IT řešení a úspěšnou adopci těchto řešení,

- organizační struktura, role a odpovědnosti z hlediska vhodnosti pro prostředí veřejného cloud computingu,
- úroveň znalostí a zkušeností IT pracovníků v oblasti využívání služeb cloud computingu,
- úroveň stávající technologické infrastruktury, aplikací a dat z hlediska jejich vhodnosti pro prostředí veřejného cloud computingu,
- nákladová efektivnost stávajících IT služeb.

Důležitou součástí posouzení současného stavu organizace z hlediska cloud computingu je analýza a hodnocení stávajících byznys procesů z hlediska jejich vhodnosti pro realizaci prostřednictvím služeb cloud computingu a definice kritérií a metrik pro rozhodnutí, zda daný byznys proces je z hlediska strategických a taktických záměrů organizace vhodný pro realizaci prostřednictvím služeb cloud computingu. To znamená, že organizace by měla porozumět stávajícímu portfoliu byznys procesů, aby přechod na využívání služeb cloud computingu vedl ke zvýšení efektivnosti a účinnosti byznys procesů místo k poklesu jejich flexibility a tím i poklesu byznys agility. Součástí může být i stanovení zákazu realizace byznys procesu prostřednictvím služeb cloud computingu. Analýza a hodnocení byznys procesů z hlediska využívání služeb cloud computingu by měla obsahovat jak provedení komplexní byznys portfolio analýzy, tak i definici typů dat zpracovávaných těmito byznys procesy. Klasifikace typů dat vyžaduje porozumění předmětu činnosti organizace a potřebám organizace, aby bylo možné určit hodnotu těchto dat pro organizaci. Nezávisle na tom, zda se jedná o strukturovaná nebo nestrukturovaná data, je nutné provést analýzu stupně citlivosti a důvěrnosti dat, analýzu vlivu zneužití dat třetí stranou na konkurenceschopnost podniku a analýzu aplikovatelnosti regulatorních předpisů a norem v případě uložení, zpracování a přenosu dat v prostředí služeb veřejného cloud computingu. Cloud Controls Matrix v3.0.1 společnosti Cloud Security Alliance (CSA) v rámci kontroly DSI-01 definuje možné klasifikace dat a to podle (Cloud Security Alliance (CSA), 2016a):

- typu dat,
- hodnoty dat pro organizaci,
- stupně citlivosti dat,
- stupně kritičnosti dat pro organizaci.

Data je možné klasifikovat jako data s vysokou, střední a nízkou citlivostí a jako data důvěrná, data soukromá určená pouze pro interní užití a data veřejně dostupná (Simorjay, 2014). Vysoce citlivá a důvěrná data jsou data s vysokou kritičností pro realizaci byznys procesů organizace, kdy neautorizovaný přístup k datům, neoprávněné pozměnění nebo zničení dat vede k fatálnímu dopadu na fungování a prosperitu organizace. Tato data mohou zahrnovat data chráněná legislativními předpisy na ochranu osobních údajů, data, která jsou předmětem ochrany duševního vlastnictví, data podléhající smlouvě o ochraně důvěrných informací nebo data týkající se finančních záznamů. Středně citlivá a soukromá data určená pouze pro interní užití jsou data se střední kritičností pro realizaci byznys procesů organizace. Neautorizovaný přístup k datům, neoprávněné pozměnění nebo zničení těchto dat nebude mít vážný dopad na fungování a prosperitu organizace. Jedná se o data, která nejsou klasifikovaná jako data důvěrná nebo veřejně přístupná. Data s nízkou citlivostí, která jsou veřejně dostupná, jsou data s minimální nebo nulovou kritičností pro realizaci byznys procesů organizace.

Současně se zaváděním služeb cloud computingu je potřeba realizovat analýzu a hodnocení připravenosti organizace pro přijetí služeb cloud computingu. Cílem je přesnější posouzení potřeb spojených s přechodem na využívání služeb cloud computingu. Míru zralosti neboli schopnosti organizace přijmout služby cloud computingu umožňuje objektivně hodnotit Cloud computing maturity model. Cloud computing maturity model organizaci poskytuje údaje o jejím aktuálním stavu prostředí z hlediska využívání služeb cloud computingu, o úrovni její vyspělosti pro adopci služeb

cloud computingu, a jakým způsobem, a ve které oblasti může být úroveň schopnosti přijmout a efektivně využívat služby cloud computingu zvýšena. K tomu, aby mohla být dosažena některá z vyšších úrovní zralosti organizace pro přijetí služeb cloud computingu, musí být zároveň splněny všechny podmínky všech nižších úrovní. Úrovně zralosti dovolují porovnání změny vyspělosti ve schopnosti přijetí a efektivního využívání služeb cloud computingu, kdy na nejnižší úrovni organizace nevyužívá nebo není připravena využívat služby cloud computingu. Jednotlivé úrovně zralosti Cloud computing maturity modelu jsou hodnoceny z následujících hledisek:

- procesy,
- governance,
- management,
- podniková kultura a lidé,
- technologická infrastruktura.

Tabulka 19 definuje úrovně zralosti Cloud computing maturity modelu napříč pěti výše identifikovanými hledisky.

Tabulka 19: Cloud computing maturity model, zdroj: (autor), podle: (ISACA, 2012c; Open Data Center Alliance, 2013; Svatá, 2011; Weiss, a další, 2013)

	Governance	Management	Procesy	Podniková kultura a lidé	Technologická infrastruktura
Úroveň 1: Počáteční/Ad hoc	Chybějící nebo nedostatečné praktiky a procesy cloud computing governance, které jsou nahodilé, nekonzistentní a závisí na znalostech a zkušenostech vedoucího IT útvaru, který rozpoznal nutnost cloud computing governance.	Chybějící nebo nedostatečné procesy cloud computing managementu, které jsou realizovány nahodile, nekonzistentně a závisí na znalostech a zkušenostech IT pracovníků.	Neexistující nebo nedostatečné procesy vhodné pro governance a management využívání služeb cloud computingu. Procesy jsou realizovány ad hoc některými IT pracovníky. Výkonnost procesu je nepředvídatelná.	Omezená podpora prostředí cloud computingu, nepochopení přínosu z využití služeb cloud computingu, nedostatek znalostí a nevyškolení zaměstnanci pro práci v prostředí cloud computingu, malá ochota přijímat cloud computing řešení	Je využívána technologická infrastruktura tradičního IT prostředí, která je nedostatečná pro potřeby využívání služeb cloud computingu, omezená integrovatelnost služeb cloud computingu
Úroveň 2: Opakovaná	Praktiky a procesy cloud computing governance jsou definované a prováděné IT manažery s účastí a dohledem vrcholového vedení. Začíná se formovat Byznys/IT Řídící Výbor. Role a odpovědnosti nejsou explicitně definovány. Politiky cloud computing governance nejsou řádně komunikovány a vyžadovány.	Hodnocení a výběr služeb cloud computingu je realizováno na základě analýzy nákladů a přínosů, hodnocení a výběr poskytovatelů závisí na preferencích vedoucího IT oddělení, monitorování výkonnosti služby a bezpečnost využívání služeb cloud computingu je realizována na straně poskytovatele.	Redefinice a definice nových procesů schopných přijmout nové aktivity spojené s využíváním služeb cloud computingu. Proces je realizován pomocí procesních aktivit, které lze opakovat, má k dispozici dostatečné zdroje a je plánován v souladu s definovanými politikami.	Podpora využívaní služeb cloud computingu ze strany IT oddělení, školení týkající se aktuálně využívaných služeb cloud computingu, vznik nových rolí	Vedoucí IT oddělení rozhoduje o výběru a pořízení technologické infrastruktury vhodné pro cloud computing. Přizpůsobení stávající technologické infrastruktury pro potřeby využívání služeb cloud computingu. Pořízení základní technologické infrastruktury pro cloud computing. Katalog služeb cloud computingu je statický, údaje jsou aktualizovány manuálně.

	Governance	Management	Procesy	Podniková kultura a lidé	Technologická infrastruktura
Úroveň 3: Definovaná	Praktiky a řízené procesy cloud computing governance jsou standardizovány, realizovány, zdokumentovány a komunikovány prostřednictvím formálního školení pracovníků. Role a odpovědnosti jsou jasně chápány. Řídící procesy nejsou plně implementovány a neumožňují detekci odchylek řízených procesů od požadovaného stavu. Členové Byznys/IT Řídícího Výboru součinně rozhodují o stanovení byznys a cloud computing cílů.	Veškeré činnosti jsou v souladu s cloud computing strategií. Hodnocení a výběr poskytovatelů je realizován na základě kvalitativních kritérií. Monitorování výkonnosti služby cloud computingu je součást monitorovacího systému spotřebitele, řízení bezpečnosti využívání služeb cloud computingu je součást systému řízení rizik spotřebitele. Jsou definovány základní metriky pro monitorování a hodnocení bezpečnosti služeb cloud computingu. Zajištění bezpečnosti poskytovatelem je analyzováno a dokumentováno. Odpovědnosti jsou definovány na základě smluv o poskytování služeb cloud computingu. Formování multi-vendor strategie.	Procesy jsou definované, standardizované a dokumentované. Proces je prováděn pomocí definovaného postupu a je schopen dosahovat očekávaných výstupů.	Definování a přijetí kultury podporující prostředí cloud computingu na úrovni podniku, definování rolí a odpovědností	Dostupná technologická infrastruktura pro podporu využívání služeb cloud computingu, která je snadno rozšiřitelná pro potřeby cloud computing cílů, Technologická infrastruktura umožnuje integraci stávajících IT služeb se službami cloud computingu, automatizované workflow a komunikaci mezi nástroji spotřebitele a poskytovatele.
Úroveň 4: Řízená a měřitelná	Je definovaná sada kvantitativních metrik pro měření shody modelu cloud computing governance. Procesy cloud computing governance jsou monitorovány, jejich průběh je vyhodnocován	Cloud computing strategie je plně v souladu s IT strategií a byznys strategií. Je realizovaná multi-vendor strategie. Je definovaná sada kvantitativních metrik pro hodnocení výkonnosti,	Procesy jsou cíleně řízeny a monitorovány na základě kvantitativních metrik. Proces funguje v rámci definovaných limitů a dosahuje	Pravidelná školení IT personálu včetně relevantních zaměstnanců z byznys části podniku a vrcholového vedení	Řízení technologické infrastruktury na celopodnikové úrovni.

	Governance	Management	Procesy	Podniková kultura a lidé	Technologická infrastruktura
	s využitím statistických a kvantitativních metod. Cloud computing cíle jsou v souladu s byznys cíli, cloud computing governance podporuje dosažení tvorby byznys hodnoty realizací výhod z využívání služeb cloud computingu.	bezpečnosti a kvality služeb cloud computingu. Jsou vyjednány specifické podmínky smluv o poskytování služeb cloud computingu a je realizována a vyhodnocována compliance poskytovatele.	očekávané výstupy.		
Úroveň 5: Optimalizovaná	Cloud computing governance je součástí enterprise governance, je optimalizovaná, její úroveň neustále zlepšovaná a flexibilně se přizpůsobuje konkrétnímu prostředí. Byznys/IT Řídící Výbor koordinuje a plánuje byznys cíle a cloud computing cíle, byznys strategii a cloud computing strategii a společně rozhoduje o investicích. Služby cloud computingu realizují byznys hodnotu.	Řízení výkonnosti služeb cloud computingu je plně realizováno, je zajištěna plná interoperabilita a přenositelnost služeb, je realizované hodnocení poskytovatelů a služeb cloud computingu v souladu s potřebami byznysu, jsou realizovány bezpečnostní audity u poskytovatele, proaktivní řízení bezpečnosti služeb cloud computingu.	Proces je neustále zlepšován za účelem plnění cloud computing cílů v souladu s byznys cíli.	Organizační struktura podporující prostředí cloud computingu, vyškolení zaměstnanci na všech úrovních, vyhodnocování dopadu cloud computingu na role a odpovědnosti	Technologická infrastruktura řízená v souladu s požadavky obchodních procesů.

Analýza aktuálního stavu využívání služeb cloud computingu v organizaci dokumentuje stávající stav využívání služeb cloud computingu v organizaci, realizuje jejich hodnocení z hlediska hodnoty, kterou jejich využití přináší a posuzuje efektivitu a výkonnost z hlediska jejich podpory byznys procesů.

Analýza externího prostředí organizace z hlediska využívání služeb cloud computingu hodnotí externí faktory ovlivňující využití služeb cloud computingu. Externí analýza se zaměřuje na analýzu příležitostí a hrozeb a na jejich budoucí vývoj. Analýza externího prostředí zahrnuje následující hlediska:

- poskytovatelé služeb cloud computingu z hlediska jejich vhodnosti pro organizaci,
- nabízené služby na trhu služeb cloud computingu,
- kooperace s obchodními partnery organizace,
- legislativní a regulatorní předpisy aplikovatelné v prostředí veřejného cloud computingu,
- trendy v oblasti informačních technologií, rozvoj trhu
- technologické prostředí z hlediska využívání služeb cloud computingu a úroveň podpory jeho rozvoje na nadnárodní úrovni,
- úroveň využívání služeb cloud computingu konkurenčními organizacemi z pohledu kvality a výkonnosti IT.

Definice budoucího stavu využívání služeb cloud computingu v organizaci vyplývá z výsledků výše uvedených strategických analýz hodnocení současného stavu prostředí organizace, připravenosti organizace pro přijetí služeb cloud computingu, aktuálního stavu využívání služeb cloud computingu v organizaci a hodnocení externího prostředí organizace, které napomáhají identifikovat cíle využívání služeb cloud computingu. Stručný popis požadovaného budoucího stavu, kterého chce podnik prostřednictvím využívání služeb cloud computingu dosáhnout je formulován prostřednictvím vize cloud computingu. Vize cloud computingu popisuje očekávanou konkurenční výhodu, byznys hodnotu, zlepšení výkonnosti a změny, ke kterým by v podniku mělo dojít využitím služeb cloud computingu. Vize by měla podporovat inovační prostředí potřebné k transformaci podniku a k dosažení cílového budoucího stavu. Stanovení vize cloud computingu musí reflektovat celopodnikovou vizi. Vize cloud computingu by měla být promítnuta do definice cílů využívání služeb cloud computingu, které mohou být rozlišeny na základě dimenzí metody Balanced Scorecard (BSC[5]). Definice budoucího stavu využívání služeb cloud computingu se promítne také do architektury cloud computing služeb, v rámci, které musí být specifikován seznam všech cloud computing služeb, jejich vzájemných vazeb a vazeb na stávající IT služby. Poté co byly definovány cloud computing cíle, je nutné definovat plán postupu realizace cloud computing cílů, který zabezpečí dosažení budoucího stavu využívání služeb cloud computingu. Součástí této transformace ze stávajícího stavu do cílového stavu je reinženýring existujících byznys procesů podporovaných tradičními IT službami tak, aby tyto procesy byly schopny akceptovat nové aktivity spojené s využíváním služeb veřejného cloud computingu, transformace organizační struktury tak, aby podporovala nové prostředí veřejného cloud computingu včetně redefinice příslušných rolí a odpovědností, či definice nových rolí a odpovědností a dále vytvoření povědomí a porozumění prostředí využívání služeb cloud computingu a strategickým cloud computing cílům prostřednictvím jejich komunikace příslušným zainteresovaným stranám.

Mezi hlavní úkoly strategie využití služeb cloud computingu patří:

- rozhodnutí, zda mohou být v organizaci využívány služby cloud computingu a rozhodnutí, zda stávající byznys a IT infrastruktura podporuje využití služeb cloud computingu,

[5] Balanced Scorecard (BSC) je metoda měření výkonnosti podniku využívající finanční a nefinanční ukazatele. Podnikové činnosti jsou rozděleny dimenzí: finance, zákazníci, interní procesy a učení se a růst (Nekvasil, 2008).

- určení specifických změn v organizaci souvisejících s využíváním služeb cloud computingu,
- identifikace kroků dosažení cloud computing cílů,
- určení nejvhodnějších služeb cloud computingu a jejich poskytovatelů,
- identifikace benefitů a nákladů z využití služeb cloud computingu,
- identifikace a hodnocení rizik souvisejících s využíváním služeb cloud computingu,
- vytvoření smluvního vztahu s poskytovatelem služeb cloud computingu,
- vytvoření jednotného nástroje pro řízení portfolia služeb cloud computingu,
- zabezpečení potřebné míry souladu využívání služby cloud s legislativními a regulatorními předpisy,
- identifikace aktivit a zdrojů potřebných pro ukončení využívání služby cloud computingu.

Procesy fáze strategie využití služeb cloud computingu jsou:

- CMS1: Řízení rizik z využití služby cloud computingu,
- CMS2: Finanční řízení služeb cloud computingu,
- CMS3: Řízení souladu s interními standardy a normami, s legislativními a regulatorními předpisy a smluvními požadavky,
- CMS4: Řízení exit strategie,
- CMS5: Řízení portfolia poskytovatelů služeb cloud computingu,
- CMS6: Řízení portfolia služeb cloud computingu,
- CMS7: Řízení smluv o poskytování služby cloud computingu.

7.3.1 Řízení rizik z využití služby cloud computingu

Číslo procesu	**CMS1**
Jméno procesu	**Řízení rizik z využití služby cloud computingu**
Cíl procesu	Analýza, hodnocení a zvládání rizika vyplývajícího z využití služby cloud computingu.
Popis procesu	Proces realizuje analýzu potenciálních rizik z využití služeb cloud computingu a hodnocení jejich dopadu na aktiva organizace. Proces provádí hodnocení významnosti rizika na základě určení pravděpodobnosti výskytu rizika a míry dopadu rizika. Proces definuje opatření ke zvládání rizik. Analýza a hodnocení rizik z využití služby cloud computingu musí být realizována průběžně v rámci celého životního cyklu řízení služby cloud computingu. Frekvence analýzy a hodnocení rizik z využití služby cloud computingu závisí na účelu a rozsahu prováděné analýzy a hodnocení rizik. Monitorování rizik vyplývajících z využití služby cloud computingu sbírá data o existujících rizicích s cílem identifikovat odchylky od očekávané úrovně přijatelného rizika, výskyt nových rizikových faktorů a změn podmínek prostředí cloud computingu. Nasbíraná data z monitorování jsou vstupem pro jednolitvé procesní aktivity.
Událost	Změna byznys prostředí, změna podnikových governance směrnic, změna bezpečnostní politiky, rozhodnutí o využívání nové služby cloud computingu, změna ve službě cloud computingu, periodické přezkoumání.
Vstup	Seznam rizik z využití služeb cloud computingu, seznam aktiv spotřebitele služeb cloud computingu, kritéria pro hodnocení rizik z využití služeb cloud computingu, úroveň tolerance rizika, akceptovatelná míra rizika, informace získané z procesu řízení incidentů.

Výstup	Seznam ohodnocených rizik služby cloud computingu, seznam ohodnocených aktiv spotřebitele služeb cloud computingu, seznam opatření ke snížení rizika z využití služeb cloud computingu, seznam akceptovaných reziduálních rizik z využití služeb cloud computingu.
Procesní aktivity	CMS1.1: Analýza rizik vyplývajících z využití služby cloud computingu CMS1.2: Hodnocení rizik vyplývajících z využití služby cloud computingu CMS1.3: Zvládání rizik vyplývajících z využití služby cloud computingu CMS1.4: Monitorování rizik vyplývajících z využití služby cloud computingu

Procesní aktivity:

❖ **Analýza rizik vyplývajících z využití služby cloud computingu**

Součástí analýzy rizik služeb cloud computingu je identifikace rizik vyplývajících z využití služeb cloud computingu, které mají potenciál ohrozit organizaci prostřednictvím narušení provozních operací a fungování organizace nebo prostřednictvím hrozeb namířených na aktiva organizace. Rizika z využití služby cloud computingu mohou být kategorizována na základě následujících hledisek:

- organizační riziko cloud computingu,
- provozní riziko cloud computingu,
- bezpečnostní riziko cloud computingu.

Mezi organizační rizika cloud computingu patří rizika, která mohou v organizaci ohrozit realizaci governance a kontroly v prostředí cloud computingu, poškodit pověst organizace, narušit kontinuitu podnikání nebo mohou vést k nesouladu organizace s legislativou, normami a standardy. Seznam organizačních rizik cloud computingu je definován v Tabulce 20.

Tabulka 20: Organizační rizika cloud computingu, zdroj: (autor)

Kategorie organizačních rizik	Seznam organizačních rizik
Ztráta governance a kontroly v cloud computingu	Ztráta schopnosti operativního řízení dosahování cílů Ztráta vlivu na definování a výkon rolí a odpovědností Nejasné rozdělení zodpovědností mezi poskytovatele a spotřebitele Ztráta schopnosti zajistit plnění bezpečnostních požadavků Ztráta kontroly nad integritou, dostupností a důvěrností dat Nejasné vlastnictví aktiv Snížení transparentnosti provádění auditu Snížení transparentnosti aplikačního a bezpečnostního reportingu Ztráta schopnosti aktivně předcházet omezení výkonnosti provozu služby cloud computingu Vznik závislosti spotřebitele služby na poskytovateli služby
Pověst organizace	Nevhodně vybraný poskytovatel služeb cloud computingu Nevhodně vybraná služba cloud computingu Nedostatečná izolace spotřebitelů služeb a smíšení dat Úmyslný útok ze strany spotřebitele sdílejícího zdroje cloud computingu Následky škodlivých praktik spotřebitele sdílejícího zdroje cloud

Kategorie organizačních rizik	Seznam organizačních rizik
	computingu
Kontinuita podnikání	Neočekávané ukončení činnosti poskytovatele služeb cloud computingu Neočekávané přerušení dodávky služby cloud computingu Akvizice poskytovatele služeb cloud computingu Chyby v dodávaných službách a výpadky služeb Poškození nebo ztráta dat Zcizení a zneužití důvěrných dat Zcizení šifrovacích klíčů Nedostatečná obnova provozu služby po havárii Závislost na interních plánech poskytovatele pro havarijní obnovu a zabezpečení dat proti ztrátě nebo poškození Nedostatečně definovaná nebo obtížně realizovatelná exit strategie Dodatečné náklady na realizaci exit strategie
Soulad s legislativou, normami a standardy	Ztráta nezávislosti při plnění požadavků daných legislativou, normami a standardy a vznik závislosti na plnění těchto požadavků poskytovatelem Ztráta schopnosti kompletně a transparentně doložit plnění požadavků daných legislativou, normami a standardy Ztráta schopnosti obhájit získané certifikáty Poskytovatel nebude schopen splnit legislativní požadavky Aplikovatelnost různých legislativních požadavků lišících se dle místa vzniku dat a dle místa fyzického uložení dat

Mezi provozní rizika cloud computingu patří rizika, která mohou ohrozit dodávku služeb cloud computingu definovanou na základě dohody o úrovni služeb, narušit provozní výkonnost a generovat vysoké provozní náklady. Seznam provozních rizik cloud computingu je definován v Tabulce 21.

Tabulka 21: Provozní rizika cloud computingu, zdroj: (autor)

Kategorie provozních rizik	Seznam provozních rizik
Dohoda o úrovni služby	Netransparentní dohoda o úrovni služby cloud computingu Nejasně a neúplně definovaná pravidla a podmínky dohody o úrovni služby cloud computingu Nejasně a neúplně definované cíle úrovně služby cloud computingu Nejasná definice odpovědností Neschopnost poskytovatele plnit podmínky definované v dohodě o úrovni služby
Provozní výkonnost	Nedostupnost a výpadky služby cloud computingu Nedostatečná výkonnost služby cloud computingu Nespolehlivost služby cloud computingu Špatná konfigurace služby cloud computingu Nedostatečné zálohování Nedostatečné havarijní plány

Kategorie provozních rizik	Seznam provozních rizik
	Útok na službu cloud computingu Odepření služby Nedostatečné řízení výkonnosti služeb poskytovatelem Nedodržení dohody o úrovni služby Nedostatečná kapacita a přetížení sítě Narušení bezpečnosti sítě Nedostatečné bezpečnostní mechanismy Nedostatečné vyškolení zaměstnanců spotřebitele Nepřenositelnost dat Selhání hardwaru
Provozní náklady	Nepředvídané navýšení nákladů na provoz služby Nedostupnost průběžných informací o rozsahu aktuálně využívaných zdrojů cloud computingu Nevhodný způsob propojení služeb cloud computingu s lokálními systémy spotřebitele Nedostatečné vyškolení zaměstnanců spotřebitele Chybný odhad objemu zpracovávaných dat službou cloud computingu Chybný odhad objemu dat přenášených mezi poskytovatelem a spotřebitelem služby Navýšení nákladů z důvodu nemožnosti řídit plnění licenčních smluv

Mezi bezpečnostní rizika cloud computingu patří rizika, která mohou ohrozit bezpečnost dat organizace. Seznam bezpečnostních rizik cloud computingu je definován v Tabulce 22.

Tabulka 22: Bezpečnostní rizika cloud computingu, zdroj: (autor)

Kategorie bezpečnostních rizik	Seznam bezpečnostních rizik
Bezpečnost dat	Narušení bezpečnosti osobních údajů Krádež účtu Ztráta dat Zneužití dat Neautorizovaný přístup k datům Neautorizovaný přístup k zálohovaným datům Neautorizovaný přístup k archivovaným datům Nedostatečné bezpečnostní mechanismy na straně poskytovatele služeb cloud computingu pro rozpoznání útoku z vnějšku a pro minimalizaci dopadů vnějších útoků Nedostatečně zabezpečené API Obtížná realizace bezpečnostních kontrol dat Neoprávněné uchovávání dat spotřebitele služeb poskytovatelem služeb cloud computingu Kontrola nad daty, smíšení dat různých spotřebitelů služeb cloud computingu

Kategorie bezpečnostních rizik	Seznam bezpečnostních rizik
	Nevhodně zvolená lokalita pro uložení dat poskytovatelem služeb cloud computingu

Pro určení dopadu rizik z využití služeb cloud computingu musí být identifikována aktiva spotřebitele služeb cloud computingu včetně jejich hodnoty pro organizaci na takové úrovni detailu, která je nutná z hlediska potřeb organizace pro hodnocení rizik. Hodnota aktiv pro organizaci vyplývá z jejich důležitosti jejich podpory realizace byznys procesů. Spolu s identifikací aktiv je vhodné definovat také vlastníka aktiva, který je za dané aktivum zodpovědný. Vlastník aktiva je zodpovědný za životní cyklus aktiva, správnou klasifikaci aktiva a za naplňování legislativních požadavků a smluvních závazků vztahující se k aktivu. Seznam aktiv spotřebitele služeb cloud computingu je definován v Tabulce 23.

Tabulka 23: Aktiva spotřebitele služeb cloud computingu, zdroj: (autor)

Kategorie aktiv	Aktiva spotřebitele služeb cloud computingu
Strategická aktiva	Pověst společnosti Značka Důvěra partnerů Důvěra zákazníků Data (důvěrná data, citlivá data)
Lidé	Loajalita zaměstnanců Zkušenosti zaměstnanců
Organizační aktiva	Dokumentace vedení klasifikované jako interní anebo důvěrné Data obsahující osobní data Interní organizační data Finanční data Operativní data Zálohovaná data Archivovaná data Informační bezpečnost Provozní dokumentace

Všechna aktiva musí být klasifikována. Aktiva jsou typicky klasifikována na základě toho, jaký typ datových aktiv zpracovávají, podporují anebo využívají. Při klasifikaci datových aktiv musí být zvažován finanční a nefinanční dopad, a to zejména reputační riziko a požadavky vyplývající z legislativních a regulatorních předpisů a ze smluvních ujednání. Při určení správné úrovně klasifikace datových aktiv a vyhodnocení, zda se jedná o data citlivá, důvěrná anebo soukromá určená pro interní účely lze vycházet z úrovně rizika, finančního dopadu, dopadu na pověst, dopadu na důvěru a motivaci zaměstnanců a dopadu vyplývajícího z regulativních požadavků.

- **Hodnocení rizik vyplývajících z využití služby cloud computingu**

Procesní aktivita provádí hodnocení významnosti rizika na základě určení pravděpodobnosti výskytu rizika a míry dopadu rizika. Pravděpodobnost výskytu rizika odráží pravděpodobnost výskytu hrozby,

která je schopna využít slabé místo zranitelnosti aktiv a způsobit škodu. Míra dopadu rizika je chápána jako rozsah škod způsobených hrozbou. Míra dopadu rizika závisí na zranitelnosti aktiv a na účinnosti bezpečnostních opatření. Výsledkem hodnocení rizik je určení významnosti rizika, což je typicky funkce pravděpodobnosti výskytu rizika a míry dopadu rizika. Posouzení rizik může být realizováno různými kvalitativními či kvantitativními přístupy.

❖ **Zvládání rizik vyplývajících z využití služby cloud computingu**

Procesní aktivita realizuje návrh opatření ke snížení významnosti rizika z využití služeb cloud computingu. Cílem je definovat taková opatření, která umožní eliminovat či zmírnit riziko na úroveň rizika, která je pro organizaci akceptovatelná, vzhledem k jejich nákladové efektivnosti. Kroky, které realizuje procesní aktivita, jsou:

- návrh alternativních opatření ke snížení významnosti rizika,
- hodnocení alternativních opatření ke snížení významnosti rizika,
- výběr opatření ke snížení rizika vzhledem k podnikové úrovni tolerance rizika a jejich nákladové efektivnosti.

Opatření ke snížení významnosti rizika mohou být formulována v dokumentu Strategie snížení významnosti rizika. Strategie snížení významnosti rizika závisí na povaze rizika. Strategie definuje kroky a zavádí bezpečností mechanismy s cílem minimalizace pravděpodobnosti výskytu a dopadu rizika. V modelu veřejného cloud computingu se může jednat o:

- ad-hoc opatření,
- prevenci rizik vyplývajících z využití služby cloud computingu,
- redukci rizik vyplývajících z využití služby cloud computingu,
- transfer rizik vyplývajících z využití služby cloud computingu.

Transfer rizik vyplývajících z využití služby cloud computingu je vhodnou metodou snížení významnosti rizika převedením rizika na třetí stranu. Požadavky vyplývající ze strategie snížení významnosti rizika mohou být realizována prostřednictvím dohody o poskytování služeb cloud computingu a dohody o úrovni služby cloud computingu (SLA). Například v tomto případě může zákazník prostřednictvím smlouvy sdílet své riziko při ukládání dat s poskytovatele služeb cloud computingu.

7.3.2 Finanční řízení služby cloud computingu

Číslo procesu	**CMS2**
Jméno procesu	**Finanční řízení služby cloud computingu**
Cíl procesu	Analýza nákladů a přínosů z využívání služeb do cloud computingu a hodnocení efektivnosti vynaložených nákladů na využívání služby cloud computingu.
Popis procesu	Proces zabezpečuje řízení finančních aktivit souvisejících s využíváním služeb cloud computingu, které zahrnuje řízení nákladů a přínosů z využívání služeb cloud computingu a řízení vynaložených nákladů na využívání služby cloud computingu. Proces realizuje analýzu nákladů a přínosů pro finanční hodnocení vynaložených nákladů na využívání služby cloud computingu, jejíž součástí je analýza nákladů na využívání služby cloud computingu a analýza přínosů z využívání služby cloud computingu vyjádřená pomocí měřitelných indikátorů.
Událost	Cyklus finančního účetnictví, cyklus tvorby rozpočtů, rozhodnutí o využívání nové

	služby cloud computingu, změna ve využívání služby cloud computingu, realizace finančního auditu.
Vstup	Účetní standardy, legislativa, účetní praktiky, finanční údaje týkající se služby cloud computingu.
Výstup	Náklady na využívání služeb cloud computingu, rozpočet pro zavedení služby cloud computingu, rozpočet pro provoz služby cloud computingu, rozpočet pro ukončení využívání služby cloud computingu, přínosy z využívání služby cloud computingu, hodnocení efektivnosti vynaložených nákladů na využívání služby cloud computingu, hodnocení čisté současné hodnoty investice do využívání služby cloud computingu, hodnocení vnitřního výnosového procenta do využívání služby cloud computingu, hodnocení doby splácení nákladů vynaložených na využívání služby cloud computingu.
Procesní aktivity	CMS2.1: Analýza nákladů na využívání služby cloud computingu CMS2.2: Tvorba rozpočtů pro zavedení služby cloud computingu, pro provoz služby cloud computingu a pro ukončení využívání služby cloud computingu CMS2.3: Analýza přínosů z využívání služby cloud computingu CMS2.4: Hodnocení efektivnosti vynaložených nákladů na využívání služby cloud computingu

Procesní aktivity:

- **Analýza nákladů na využívání služby cloud computingu**

Analýza nákladů na využívání služby cloud computingu představuje součet všech nákladů souvisejících se získáním, nasazením, provozováním a ukončením využívání služby cloud computingu.

Ukazatele pro identifikaci celkových nákladů na využívání služeb cloud computingu jsou definované v Tabulce 24.

Tabulka 24: Náklady na využívání služby cloud computingu, zdroj: (autor)

Kategorie nákladů	Náklady
Počáteční náklady	Náklady na získání informací potřebných k rozhodování o využití služby cloud computingu Náklady spojené s hodnocením a výběrem služby cloud computingu Náklady spojené s hodnocením a výběrem poskytovatele služby cloud computingu Náklady na technologickou infrastrukturu Náklady na nasazení služby cloud computingu Náklady na integraci služby cloud computingu Náklady na customizaci Náklady na konfiguraci Náklady na testování Náklady na migraci dat Náklady na konzultační služby Náklady na školení

Kategorie nákladů	Náklady
	Náklady na organizační změnu
Provozní a opakující se náklady	Periodické předplatné služby cloud computingu Náklady na správu předplatného a na administraci služby cloud computingu Náklady na uživatele Náklady na spotřebu jednotky zdroje Náklady na výpočetní výkon Náklady na dobu provozuschopnosti vyšší než garantovanou Náklady na využití sítě a přenos dat Náklady na aktivitu (počet dotazů na API, počet incidentů, počet změn atd.) Náklady na instanci služby cloud computingu Náklady na změnu poskytované služby cloud computingu Náklady na určení geografické lokality fyzického uložení dat Náklady na zajištění bezpečnosti dat Náklady na zálohování dat a redundanci dat Náklady na zvýšení úrovně odpovědnosti za data poskytovatelem služby cloud computingu Náklady na zmírnění rizika Náklady na technickou podporu poskytovatelem služeb cloud computingu Náklady na podporu koncového uživatele služby computingu Náklady na softwarové licence Náklady na technické prostředky související s využíváním služby cloud computingu Náklady na ztrátu způsobenou selháním služby cloud computingu Náklady vznikající z nedodání očekávaných kvalitativních parametrů služby cloud computingu
Náklady na ukončení	Náklady na ukončení vztahu s poskytovatelem služby cloud computingu Náklady na změnu poskytovatele služby cloud computingu Náklady na návrat k on-premise řešení

- **Analýza přínosů z využívání služby cloud computingu**

Přínosy z využívání služeb cloud computingu odráží očekávané benefity ze změny výstupů všech byznys procesů, které služba cloud computingu za dané časové ovlivnila. Analýza přínosů z využívání služby cloud computingu představuje identifikaci celkové hodnoty všech finančních prostředků generovaných využíváním služby cloud computingu, a to prostřednictvím zvýšení výnosů nebo snížením nákladů.

Přínosy z využívání služby cloud computingu mohou být přímé a nepřímé. Přímé přínosy jsou měřitelné a snadno kvantifikovatelné pomocí finančních ukazatelů. Nepřímé přínosy jsou obtížně kvantifikovatelné a odhad jejich hodnoty převedený na finanční vyjádření může být realizován

některou z metod pro vyjádření očekávané hodnoty přínosu. Metody pro vyjádření očekávané hodnoty přínosu jsou postaveny zejména na:

- stanovení očekávané hodnoty přínosu pomocí nákladů obětované příležitosti,
- stanovení očekávané hodnoty přínosu jako ekvivalentu k nákladům, které by vznikly, pokud by hodnocená investice nebyla realizovaná,
- stanovení očekávané hodnoty pomocí stínových cen.

Přínosy, jejichž kvantifikace hodnoty je obtížná nebo nerealizovatelná do analýzy přínosů z využívání služeb cloud computingu zahrnuty nebudou.

Měřitelné veličiny pro identifikaci předpokládaných přímých přínosů z využívání služby cloud computingu jsou definovány v Tabulce 25:

Tabulka 25: Přímé přínosy z využívání služby cloud computingu, zdroj: (autor)

Kategorie přímých přínosů	Přímé přínosy
Zákazníci	Zkrácení průměrné doby splatnosti pohledávek
Výkonnost organizace	Zvýšení výnosů Zvýšení zisku Zvýšení produktivity Zkrácení doby k uvedení produktu na trh
Redukce IT nákladů	Snížení nákladů na technologickou infrastrukturu Snížení nákladů na licence Snížení nákladů na IT zaměstnance Snížení nákladů na změnové řízení Snížení nákladů na technickou podporu IT Snížení nákladů na údržbu IT Snížení nákladů na upgrade Snížení nákladů na inovace Snížená nákladů na testovací prostředí Snížení nákladů na IT bezpečnost Snížení nákladů na nadbytečné kapacity Optimalizace využití IT zdrojů Zkrácení doby implementace aplikace Zkrácení doby vývoje a testování Snížení nákladů na pronájem pracovních prostor

Ukazatele pro identifikaci předpokládaných nepřímých přínosů z využívání služby cloud computingu jsou definovány v Tabulce 26:

Tabulka 26: Nepřímé přínosy z využívání služby cloud computingu, zdroj: (autor)

Kategorie nepřímých přínosů	Nepřímé přínosy
Zákazníci	Zvýšení customer experience Zvýšení zákaznické spokojenosti Zvýšení hodnoty zákazníka

Kategorie nepřímých přínosů	Nepřímé přínosy
Výkonnost organizace	Zlepšení konkurenceschopnosti Zvýšení byznys agility Zlepšení podpory strategických byznys cílů Zlepšení spolupráce v reálném čase Vytvoření pevných vazeb k byznys partnerům Zefektivnění průběhu byznys procesů Zvýšení spokojenosti zaměstnanců
Výkonnost IT	Zvýšení uživatelské spokojenosti Zvýšení flexibility IT operací Zrychlení inovací a přístup k nejnovějším technologiím Transfer rizika na poskytovatele služeb cloud computingu Konzistentní kontrola a monitorování služeb cloud computingu poskytovatelem Alokace IT zdrojů na podporu klíčových obchodních funkcí Zlepšení mobility

❖ Hodnocení efektivnosti vynaložených nákladů na využívání služby cloud computingu

Pro hodnocení efektivnosti vynaložených nákladů na využívání služby cloud computingu lze využít metody hodnocení investic, které však musí být modifikovány tak, aby propočty těchto metod braly v úvahu faktory determinující využití služby cloud computingu, a to zejména faktor času, rizika a přechod z kapitálových nákladů, které jsou spojené s vynaložením vysoké počáteční finanční investice, na provozní náklady, jejichž výše je primárně spojená s objemem spotřebované služby cloud computingu. Pro zabezpečení konzistence hodnocení vynaložených nákladů na využívání služby cloud computingu, musí být přínosy i náklady realizované a vynaložené za určité budoucí časové období diskontovány na současnou hodnotu a sečteny. Těmito metodami jsou:

- návratnost investice (ROI[6]),
- čistá současná hodnota (NPV[7]),
- vnitřní výnosové procent (IRR[8]),
- doba splácení (PP[9]),
- návratnost investice do bezpečnosti (ROSI[10]).

[6] Návratnost investice – ROI (Return on Investment) je metoda, která se používá k hodnocení výnosnosti investice.

[7] Čistá současná hodnota – NPV (Net Present Value) vyjadřuje celkovou současnou diskontovanou hodnotu všech peněžních toků investice.

[8] Vnitřní výnosové procento – IRR (Internal Rate of Return) vyjadřuje výši úrokové míry, kdy se čistá současná hodnota očekávaných peněžních toků investice rovná 0.

[9] Doba splácení – PP (Payback Period) určuje, za jak dlouhou dobu peněžní toky plynoucí z investice přinesou hodnotu rovnající se investičním nákladům.

Hodnocení efektivnosti vynaložených nákladů na využívání služby cloud computingu pomocí metody návratnosti investice (ROI) vyhodnocuje ekonomickou výnosnost služby cloud computingu na základě vložených finančních prostředků na využívání služby cloud computingu. ROI neposkytuje informace o účinnosti a efektivitě nákladů vynaložených na využívání služby cloud computingu a nezohledňuje riziko nedosažení přínosu ze služby cloud computingu. ROI umožnuje zdůvodnit a prioritizovat budoucí vložení finančních prostředků do využívání služeb cloud computingu, hodnotit stávající náklady na využívání služby cloud computingu a posoudit návratnost vynaložených nákladů na využívání služby cloud computingu. Základem této metody je kvantifikace nákladů na investici do využívání služby cloud computingu a předpokládaných přínosů z finančních prostředků vložených do využívání služby cloud computingu. Výpočet ROI pro výpočet návratnosti vynaložených nákladů na využívání služby cloud computingu je poměrem rozdílu celkových přínosů z využívání služby cloud computingu a celkových nákladů na využívání služby cloud computingu k celkovým nákladům na využívání služby cloud computingu (viz rovnice (1.1)) (ISACA, 2012a). Pokud je výsledný podíl větší než 0, služba cloud computingu je výdělečná. V opačném případě je služba cloud computingu ztrátová. Pokud je výsledný podíl roven nule, návratnost nákladů na využívání služby cloud computingu se nachází na bodu zvratu a předpokládané přínosy z využívání služby cloud computingu se rovnají nákladům na využívání služby cloud computingu. Pro procentuální vyjádření čistého přínosu, které náklady na využívání služby cloud computingu v průměru ročně přinesou, je nutné poměr vynásobit hodnotou 100.

$$ROI = \frac{\frac{celkové\ přínosy\ z\ využívání\ služby\ cloud\ computingu - celkové\ náklady\ na\ využívání\ služby\ cloud\ computingu}{počet\ let\ životnosti\ investice\ t}}{celkové\ náklady\ na\ využívání\ služby\ cloud\ computingu} \quad (1.1)$$

Metoda ROI může být doplněna o ukazatel čisté současné hodnoty (NPV) vynaložených nákladů na využívání služby cloud computingu. NPV se vypočítá jako součet diskontovaných hodnot peněžních toků plynoucích z finančního obnosu vloženého do využívání služby cloud computingu (viz rovnice (1.2)) (ISACA, 2012a). Kladná hodnota NPV vyjadřuje současný zisk z vynaložených nákladů na využívání služby cloud computingu, záporná hodnota NPV vyjadřuje ztrátu plynoucí z enormních nákladů na využívání služby cloud computingu.

$$NPV = -počáteční\ náklady + \sum \frac{celkové\ přínosy - (provozní\ a\ opakující\ se\ náklady)_t}{(1 + úroková\ míra\ i)^t} \quad (1.2)$$

Na metodě NPV je založen ukazatel vnitřního výnosového procenta (IRR). Hodnota vnitřního výnosového procenta je rovna matematickému odhadu úrokové míry, při které se NPV = 0 (viz rovnice (1.3)) (ISACA, 2012a). Vynaložené náklady na využívání služby cloud computingu lze akceptovat, pokud bude vnitřní výnosové procento vyšší než zvažovaná diskontní míra s rizikovou prémií.

$$0 = -počáteční\ náklady + \sum \frac{celkové\ přínosy - (provozní\ a\ opakující\ se\ náklady)_t}{(1 + IRR)^t} \quad (1.3)$$

Doba, za kterou se čisté přínosy plynoucí z vynaložených nákladů na využívání služby cloud computingu vyrovnají celkovým nákladům na využívání služby cloud computingu se nazývá doba

[10] Návratnost investice do bezpečnosti – ROSI (Return On Security Investment) se používá k hodnocení investice na zajištění požadované úrovně IT bezpečnosti.

návratnosti investice. Doba návratnosti investice se vypočítá pomocí metody doby splácení (PP) jako podíl celkových nákladů na využívání služby cloud computingu a rozdílu mezi celkovými přínosy z vynaložených nákladů na využívání služby cloud computingu a provozními a opakujícími se náklady na využívání služby cloud computingu (viz vzorec (1.4)) (Hill, a další, 2013). Doba splácení musí být kratší než předpokládaná doba využívání služby cloud computingu.

$$PP = \frac{celkové\ náklady\ na\ využívání\ služby\ cloud\ computingu}{celkové\ přínosy - (provozní\ a\ opakující\ se\ náklady)} \quad (1.4)$$

Metoda hodnocení návratnosti vložených finančních prostředků do bezpečnosti (ROSI) je postavena na předpokladu, že cílem vynaložených nákladů na využívání služby cloud computingu není realizace finančních přínosů z využití služby cloud computingu, ale jedná se o vynaložení nákladů zabezpečujících snížení výše ztráty na znovuobnovení aktiv a na odstranění následků škod při dopadu hrozby. ROSI vyjadřuje poměr rozdílu předpokládané roční finanční ztráty způsobené výskytem hrozby a jeho dopadem na specifické aktivum při dané míře účinnosti opatření na snížení rizika a náklady na zajištění bezpečnosti aktiv ovlivněných využíváním služby cloud computingu k nákladům na zajištění bezpečnosti aktiv ovlivněných využíváním služby cloud computingu (viz vzorec (1.5)) (ENISA, 2012). Pokud je výsledný podíl větší než 0, vynaložené náklady na využívání služby cloud computingu jsou efektivní a je možné službu využívat. V opačném případě je využívání služby cloud computingu neefektivní. Pokud je výsledný podíl roven nule, návratnost vložených finančních prostředků do zajištění bezpečnosti využívání služby cloud computingu se nachází na bodu zvratu a předpokládané benefity z využívání služby cloud computingu se rovnají vynaloženým nákladům na využívání této služby.

$$ROSI = \frac{(PP\ výskytu\ hrozby \times rozsah\ škody) \times účinnost\ opatření\ ke\ snížení\ rizika - náklady\ na\ zajištění\ bezpečnosti}{náklady\ na\ zajištění\ bezpečnosti} \quad (1.5)$$

7.3.3 Řízení souladu s interními standardy a normami, s legislativními a regulatorními předpisy a smluvními požadavky

Číslo procesu	**CMS3**
Jméno procesu	**Řízení souladu s interními standardy a normami, s legislativními a regulatorními předpisy a smluvními požadavky**
Cíl procesu	Zajištění, že využívané služby cloud computingu jsou v souladu s interními standardy a normami, s legislativními a regulatorními předpisy a smluvními požadavky.
Popis procesu	Proces realizuje identifikaci relevantních požadavků interních standardů a norem, legislativních a regulatorních předpisů a smluvních požadavků souvisejících s využíváním služby cloud computingu. Proces vyhodnocuje důležitost těchto požadavků z hlediska fungování organizace a vytváří procedury a pravidla pro to, aby požadavky byly během provozu služby cloud computingu plněny v potřebné úrovni. Proces vytváří plány pro komunikaci těchto požadavků zainteresovaným stranám a pro pravidelné školení příslušných zainteresovaných stran o tom, co tyto požadavky znamenají pro provoz organizace. Proces vytváří procedury pro monitorování souladu, pro identifikaci odchylek, pro eskalaci odchylek a pro jejich řešení a znovuobnovení souladu služby cloud computingu s těmito požadavky. Proces zajišťuje, že smluvní ujednání s poskytovateli služby cloud computingu definují splnění potřebných požadavků na potřebné úrovni a umožní získání informací o stupni dosahovaného souladu poskytovatele služby cloud computingu.

	Proces zajišťuje, že v rámci SLA budou definovány příslušné metriky, jejich hodnoty a způsob jejich měření.
Událost	Změny v legislativním prostředí, detekce odchylky od souladu, rozhodnutí o využívání nové služby cloud computingu, změna využívání služby cloud computingu.
Vstup	Interní standardy a normy, legislativní a regulatorní předpisy, a smluvními požadavky, data z monitorování souladu, seznam požadavků na službu cloud computingu.
Výstup	Seznam požadavků na SLA a smluvní ujednání s poskytovatelem služby cloud computingu, pravidla pro plnění požadavků během provozu služby, dokumentace hodnocení souladu, plány pro komunikaci požadavků zainteresovaným stranám, plány školení příslušných zainteresovaných stran.
Procesní aktivity	CMS3.1: Identifikace relevantních požadavků interních standardů a norem, legislativních a regulatorních předpisů a smluvních požadavků souvisejících s využíváním služby cloud computingu CMS3.2: Hodnocení důležitosti relevantních požadavků interních standardů a norem, legislativních a regulatorních předpisů a smluvních požadavků z hlediska fungování organizace CMS3.3: Plánování plnění požadavků během provozu služby cloud computingu CMS3.4: Plánování školení zainteresovaných stran CMS3.5: Monitorování souladu CMS3.6: Hodnocení souladu a realizace nápravných opatření

7.3.4 Řízení exit strategie

Číslo procesu	**CMS4**
Jméno procesu	**Řízení exit strategie**
Cíl procesu	Vytvoření plánů pro ukončení využívání služby cloud computingu.
Popis procesu	Proces realizuje vytvoření plánů pro ukončení využívání služby cloud computingu u aktuálního poskytovatele služby a přechod k jinému poskytovateli služby nebo k přechodu k on-premise řešení. Tyto plány pokrývají dvě varianty důvodů ukončení využívání služby cloud computingu, a to ukončení využívání služby spotřebitelem nebo ukončení dodávky služby poskytovatelem.
Událost	Rozhodnutí o využívání služby cloud computingu.
Vstup	Artefakty definující využívání služby cloud computingu.
Výstup	Plány organizačních činností, plány technických činností, plány infrastrukturních zdrojů, plány lidských zdrojů, plány časového horizontu realizovatelnosti, plány financování ukončení služby, plány financování přechodu k jinému poskytovateli služeb nebo k on-premise řešení.
Procesní aktivity	CMS4.1: Vytváření plánů činností a zdrojů potřebných pro realizaci exit strategie.

Procesní aktivity:

- **Vytváření plánů činností a zdrojů potřebných pro realizaci exit strategie**

Procesní aktivita realizuje plánování činností a zdrojů potřebných pro ukončení využívání služby cloud computingu. Mezi hlavní činnosti patří:

- vytvoření definice datového modelu byznys procesu nebo jeho části, která je podporována službou cloud computingu,
- identifikace dat nutných pro realizaci ukončení využívání služby cloud computingu,
- definice metod získání dat pro realizaci ukončení využívání služby cloud computingu,
- definice infrastrukturních zdrojů pro přenos dat od poskytovatele služby a jejich uložení u spotřebitele služby,
- definice lidských zdrojů potřebných pro realizaci ukončení využívání služby cloud computingu,
- vytvoření harmonogramu časového horizontu realizovatelnosti ukončení využívání služby cloud computingu,
- financování nákladů na infrastrukturní a lidské zdroje udržované u spotřebitele služby pro případ ukončení využívání služby cloud computingu,
- financování nákladů na ukončení služby vyplývající ze smluvních ujednání s poskytovatelem služby,
- financování nákladů přechodu k jinému poskytovateli služeb nebo k on-premise řešení,
- definice požadavků na smluvní ujednání s poskytovatelem služby, které smluvně vytvoří podmínky pro realizovatelnost ukončení využívání služby cloud computingu.

7.3.5 Řízení portfolia poskytovatelů služeb cloud computingu

Číslo procesu	**CMS5**
Jméno procesu	**Řízení portfolia poskytovatelů služeb cloud computingu**
Cíl procesu	Identifikace a výběr poskytovatele služeb cloud computingu.
Popis procesu	Proces realizuje výběr a hodnocení poskytovatelů služeb cloud computingu dostupných na trhu služeb cloud computingu tak, aby vybraný poskytovatel v optimální míře splňoval požadavky cloud computing strategie s důrazem na kontinuální a bezproblémovou dodávku služeb cloud computingu. Proces zabezpečuje jasnou definici vztahu mezi poskytovatelem a spotřebitelem prostřednictvím dohody o službách cloud computingu. Proces zajišťuje vytvoření a udržování vztahu s poskytovateli služeb cloud computingu.
Událost	Změna byznys potřeb, změna byznys prostředí, nový poskytovatel na trhu, rozhodnutí o výběru nového poskytovatele služby cloud computingu, rozhodnutí o využívání nové služby cloud computingu, strategická změna na straně poskytovatele služby cloud computingu, neplnění podmínek dohody o úrovni služby cloud computingu, změna smluvních podmínek.
Vstup	Požadavky na poskytovatele služeb cloud computingu, informace o poskytovateli služeb cloud computingu.
Výstup	Seznam ohodnocených poskytovatelů služeb cloud computingu, seznam akceptovaných poskytovatelů služeb cloud computingu.

Procesní aktivity	CMS5.1: Hodnocení a výběr poskytovatele služby cloud computingu CMS5.2: Vytvoření a udržování vztahu s poskytovatelem služby cloud computingu

Procesní aktivity:

- **Hodnocení a výběr poskytovatele služeb cloud computingu**

Procesní aktivita realizuje identifikaci, hodnocení a výběr poskytovatele služeb cloud computingu, který vyhovuje stanoveným hodnotícím kritériím. Hodnotící kritéria slouží k hodnocení a výběru poskytovatele služeb cloud computingu a k pravidelnému přezkoumání již schválených poskytovatelů služeb cloud computingu. Hodnotící kritéria jsou stanovena na základě požadavků na poskytovatele a pokrývají ekonomické, technologické, legislativní i subjektivní aspekty hodnocení. Výběr poskytovatele je realizován na základě výsledků variant hodnocení poskytovatelů, závisí na preferencích spotřebitele služeb cloud computingu a na spotřebitelově rozpočtovém omezení.

Vhodný výběr poskytovatele služeb cloud computingu je jedním z aspektů, který ovlivňuje výkonnost organizace. Při hodnocení poskytovatele mohou být brána v úvahu hodnotící kritéria vycházející z požadavků definovaných v Tabulce 27.

Tabulka 27: Kritéria pro hodnocení poskytovatelů služeb cloud computingu, zdroj: (autor)

Soubor požadavků	Požadavky na poskytovatele služeb cloud computingu
Reputace	Vlastnická struktura poskytovatele služeb cloud computingu Pozice na trhu (příjmy, růst) Dobře definovaný byznys model Finanční stabilita poskytovatele služeb cloud computingu Životaschopnost poskytovatele služeb cloud computingu Etičnost poskytovatele služeb cloud computingu Pověst poskytovatele služeb cloud computingu Zpětná vazba od spotřebitelů služeb cloud computingu poskytovatele
Rozsah portfolia služeb	Model služeb Funkcionalita služby cloud computingu Přizpůsobitelnost služby cloud computingu Závislost na ostatních službách poskytovatele Elasticita služby cloud computingu Výkonnost služby cloud computingu Kapacitní omezení služby cloud computingu Dostupnost služby cloud computingu Testovatelnost služby cloud computingu Vhodnost služby cloud computingu
Flexibilita	Interoperabilita (API poskytovatele, standardy) Přenositelnost dat Škálovatelnost zdrojů Délka platnosti dohody o službách cloud computingu (krátkodobá, dlouhodobá)

Soubor požadavků	Požadavky na poskytovatele služeb cloud computingu
	Rozšiřitelnost dohody o službách cloud computingu Realizovatelnost exit strategie Omezení související s využitím služeb cloud computingu Doba potřebná pro zprovoznění služby cloud computingu Kapacita sítě a šířka pásma Automatická rezervace zdrojů
Spolehlivost a důvěryhodnost	Dodržování dohody o službách cloud computingu Odpovědnost a transparentnost poskytovatele služeb cloud computingu Zabezpečení kontinuity poskytování služeb cloud computingu Síťová redundance Poskytování častých a včasných informací o provozu služeb cloud computingu Certifikace poskytovatele služeb cloud computingu
Bezpečnost a ochrana dat	Bezpečnostní politika Dostupnost mechanismů pro zajištění bezpečnosti dat spotřebitele služeb cloud computingu (fyzická bezpečnost, komunikační bezpečnost, přístupová bezpečnost, informační bezpečnost) Odolnost služeb cloud computingu vůči chybám Zálohování a havarijní obnova Oddělení dat různých spotřebitelů služby cloud computingu Nakládání s daty po ukončení smluvního vztahu Vlastnictví dat Hodnocení bezpečnosti třetí stranou Certifikace
Řízení služeb	Kontrola a monitorování služeb cloud computingu Řízení incidentů Řízení detekce hrozeb a zranitelností služeb cloud computingu Řízení změn a aktualizace služeb cloud computingu Konfigurační řízení Podpora Úroveň zralosti procesů řízení služeb cloud computingu
Dodržování legislativy	Prokazatelnost dodržování národní nebo regionální jurisdikce Lokalizovatelnost dat Zálohování dat Realizovatelnost auditu
Náklady	Cenový model Cenová stabilita Platební metody Granularita plateb Doba splatnosti Transparentnost cen

Soubor požadavků	Požadavky na poskytovatele služeb cloud computingu
	Náklady na nasazení služeb cloud computingu Náklady na využívání služeb cloud computingu Náklady na změnu dodavatele cloud computingu
Uživatelská přívětivost	Využití služby cloud computingu v režimu Off-line Individualizace a přehlednost webového rozhraní Doplňkové služby (integrace, školení) k poskytovaným službám cloud computingu Snadná přístupnost ke službě cloud computingu

7.3.6 Řízení portfolia služeb cloud computingu

Číslo procesu	**CMS6**
Jméno procesu	**Řízení portfolia služeb cloud computingu**
Cíl procesu	Zajištění, že portfolio služeb cloud computingu v organizaci je tvořeno souborem služeb, které optimálně realizují podporu byznys procesů s ohledem na nabídku služeb cloud computingu schváleným portfoliem jejich poskytovatelů.
Popis procesu	Proces realizuje vytvoření a udržování portfolia služeb cloud computingu spotřebitelem služeb cloud computingu. Proces provádí dokumentaci služeb cloud computingu, dokumentuje propojení služby cloud computingu a byznys procesu, udržuje informace o parametrech služby cloud computingu a jejím modelu financování, propojuje službu cloud computingu s jejím poskytovatelem a příslušnou dohodou o úrovni služby SLA. Proces spravuje jak aktivně využívané služby cloud computingu, tak i takové, které by potencionálně mohly přicházet v úvahu pro využití v organizaci. Proces shromažďuje informace o ekvivalentních službách cloud computingu vybrané skupiny poskytovatelů s cílem umožnit porovnání kvality služeb jednotlivých dodavatelů a případně tak poskytnout podklady pro změnu služby nebo změnu poskytovatele. Proces dále udržuje informace o službách, které byly vyřazeny z provozu a o důvodech jejich vyřazení. Proces realizuje vytvoření a údržbu katalogu služeb spotřebitele. Katalog služeb spotřebitele je využíván jako centrální nástroj správy portfolia služeb, ve kterém jsou uloženy všechny relevantní a aktuální informace o všech službách portfolia služeb cloud computingu.
Událost	Změna byznys potřeb, změna byznys prostředí, nová služba na trhu, rozhodnutí o výběru nové služby cloud computingu, změna ve službě cloud computingu, neplnění podmínek dohody o úrovni služby cloud computingu, změna smluvních podmínek.
Vstup	Požadavky na službu cloud computingu, informace o službě cloud computingu, katalog služeb poskytovatele služeb cloud computingu.
Výstup	Katalog služeb spotřebitele služeb cloud computingu, dokumentace služby cloud computingu, informace o stavu služby cloud computingu, seznam dohod o službách cloud computingu.
Procesní aktivity	CSM6.1: Definice a zdokumentování služby cloud computingu CSM6.2: Analýza služeb v portfoliu služeb cloud computingu CSM6.3: Návrh a provoz katalogu služeb spotřebitele služeb cloud computingu

Procesní aktivity:

❖ **Návrh a provoz katalogu služeb spotřebitele služeb cloud computingu**

Hlavním nástrojem procesu řízení portfolia služeb je katalog služeb spotřebitele služeb cloud computingu. Katalog služeb cloud computingu je databázová aplikace obsahující informace o službách cloud computingu, které jsou poskytovány schválenými poskytovateli služeb cloud computingu. V katalogu služeb jsou tyto služby rozděleny do třech kategorií:

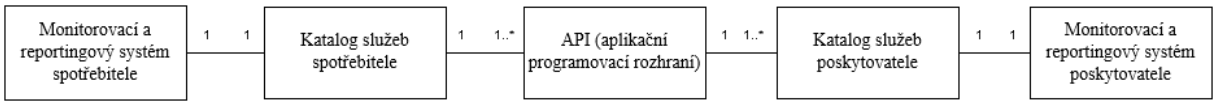
- aktuálně využívané služby cloud computingu,
- služby cloud computingu poskytované schváleným portfoliem poskytovatelů, avšak aktuálně nevyužívané,
- služby cloud computingu, které byly z využívání vyřazeny.

Katalog služeb cloud computingu slouží nejen k evidenci služeb využívaných v organizaci, ale i jako zdroj informací pro zařazení nových služeb do využívání nebo změny ve službách aktuálně využívaných.

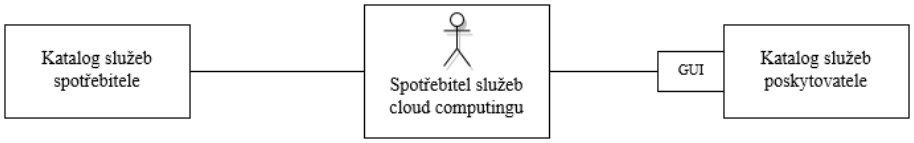
Mezi základní funkce katalogu služeb cloud computingu patří:

- katalogizace a centrální uložení informací o službách cloud computingu poskytovaných schváleným portfoliem poskytovatelů,
- identifikace vztahů mezi službami cloud computingu a byznys procesy spotřebitele,
- poskytování aktuálních informací o parametrech úrovně využívaných služeb cloud computingu,
- napojení na katalogy služeb schválených poskytovatelů a průběžná aktualizace informací o službách uložených v katalogu služeb spotřebitele,
- poskytování informací pro řízení životního cyklu služeb cloud computingu spotřebitele,
- zpřístupnění hodnot parametrů o úrovni využívaných služeb cloud computingu monitorovacímu systému spotřebitele,
- řízení přístupu k informacím a funkcím v katalogu služeb zaměstnanců spotřebitele na základě jejich identity.

Katalog služeb cloud computingu spotřebitele všeobecně může být realizován formou autonomní aplikace propojené s katalogem služeb poskytovatele pomocí API[11] (viz Obrázek 21) nebo formou subkatalogu katalogu služeb poskytovatele (viz Obrázek 22).



Obrázek 21: Propojení katalogu služeb spotřebitele prostřednictvím API s katalogem služeb poskytovatele, zdroj: (autor)

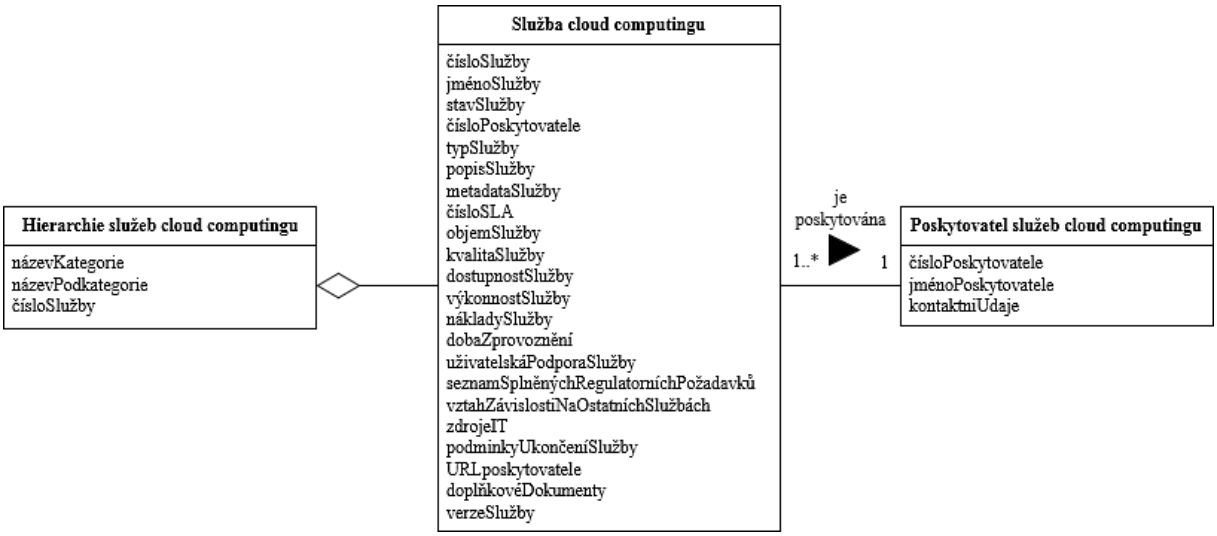


Obrázek 22: Katalog služeb spotřebitele je realizován ve formě subkatalogu katalogu služeb poskytovatele, ke kterému spotřebitel přistupuje přes webové rozhraní a data do svého centrálního katalogu služeb přenáší manuálně, zdroj: (autor)

[11] API (Application Programming Interface) je aplikační programovací rozhraní, které umožňuje vyvíjet aplikace, které zabezpečují komunikaci mezi různými systémy.

V prvním případě je možné řídit portfolio služeb všech schválených poskytovatelů, v druhém případě je řízení portfolia služeb cloud computingu omezeno na jednoho poskytovatele, případně přenos a aktualizace dat v centrálním katalogu služeb spotřebitele je prováděna manuálně. Na Obrázku 21 je znázorněn katalog služeb spotřebitele, který je prostřednictvím API propojen s katalogem služeb poskytovatele, do kterého se dotazuje. API je rozhraní, které umožňuje spotřebiteli služeb cloud computingu přistupovat ke katalogu poskytovatele služeb. Z katalogu služeb poskytovatele jsou přenášeny informace o jím poskytovaných službách a ty jsou ukládány do katalogu spotřebitele tak, že spotřebitel má k dispozici aktuální informace o poskytovaných službách včetně úrovně služeb a cenových charakteristik. Spotřebitel může svůj katalog služeb propojit pomocí různých API k pevnému počtu katalogů služeb předem schválených poskytovatelů. S těmito poskytovateli musí spotřebitel vyjednat technické a bezpečnostní požadavky propojení a komunikace katalogů a definici služeb zpřístupněných pro využití spotřebitelem. Podstatnou bezpečnostní charakteristikou musí být zabezpečení přístupu ke katalogu poskytovatele pouze pro autorizované uživatele spotřebitele služeb. K datům uloženým v katalogu služeb poskytovatele mohou přistupovat uživatelé spotřebitele vzhledem k rolím a oprávněním, ostatní data jsou jim skrytá. Katalog poskytovatele služeb je jedním ze zdrojů, které katalogu spotřebitele poskytují informace o aktuálně využívaných službách. Dalším zdrojem informací mohou být výstupy z monitorovacích a reportingových mechanismů poskytovatele služby cloud computingu.

Struktura katalogu služeb spotřebitele by měla být navržená tak, aby jednotlivé atributy popisu služeb zabezpečovaly konzistenci katalogu v případě, že katalog obsahuje informace o službách nabízených různými poskytovateli. Struktura katalogu služeb spotřebitele je znázorněná na Obrázku 23.



Obrázek 23: Struktura katalogu služeb spotřebitele, zdroj: (autor)

7.3.7 Řízení smluv o poskytování služby cloud computingu

Číslo procesu	**CMS7**
Jméno procesu	**Řízení smluv o poskytování služby cloud computingu**
Cíl procesu	Zajištění, že smlouvy o poskytování služby cloud computingu uzavřené mezi poskytovatelem a spotřebitelem budou obsahovat právně vymahatelné smluvní ustanovení, která zajistí tvorbu očekávané hodnoty z využití služby cloud computingu na základě dodání a poskytování služby očekávaným způsobem
Popis procesu	Řízení smluv o poskytování služby cloud computingu realizuje definování nebo

	zpřesnění podmínek dohody o službách cloud computingu, definování úrovně kvality služby cloud computingu potřebné pro zajištění byznys potřeb, vyjednávání podmínek dohody a zní vyplývajících povinností pro uzavírající strany, sledování výkonnosti dohody o úrovni sužby cloud computingu, vymáhání povinností a práv vyplývajících ze smlouvy a rozšíření nebo ukončení smlouvy. V rámci řízení smluv musí být specifikované způsoby formální komunikace s poskytovatelem služeb cloud computingu, postupy pro řešení sporů vztahujících se ke smlouvám a přidělené odpovědnosti za interakci s poskytovatelem služeb cloud computingu.
Událost	Rozhodnutí o využívání nové služby cloud computingu, rozhodnutí o změně poskytovatele, realizace exit strategie, ukončení poskytování služby původním poskytovatelem.
Vstup	Požadavky na službu cloud computingu, informace o službě cloud computingu z katalogu služeb poskytovatele služeb cloud computingu.
Výstup	Rámcová smlouva o službách cloud computingu, dohoda o službách cloud computingu, dohoda o úrovni služby cloud computingu (SLA).
Procesní aktivity	CMS7.1: Identifikace požadavků na smlouvy o poskytování služeb cloud computingu CMS7.2: Vyjednávání, odsouhlasení a uzavření smluv o poskytování služeb cloud computingu CMS7.3: Návrh změny a realizace změny ve smlouvách o poskytování služeb cloud computingu CMS7.4: Ukončení smluv o poskytování služeb cloud computingu

Smlouvy o poskytování služeb musí vyjadřovat požadavky spotřebitele na bezpečnost, ochranu citlivých dat, výkonnostní charakteristiky služby a požadavky vyplývající z legislativních a regulatorních předpisů. Povaha a rozsah smluv o poskytování služeb mezi spotřebitelem a poskytovatelem služeb cloud computingu se může lišit v závislosti na aktuálních faktorech vztahujících se k typu vztahu mezi spotřebitelem a poskytovatelem, na typu a objemu poskytovaných služeb cloud computingu, na objemu a typu zpracovávaných dat, na míře rizik vyplývajících z využívání služby cloud computingu a na související legislativě. Smlouvy o poskytování služeb cloud computingu by kromě základních pravidel a podmínek poskytování a využívání služby cloud computingu a povinností pro uzavírající strany měly obsahovat definice úrovně kvality služby cloud computingu potřebné pro zajištění byznys potřeb, příslušné sankce při nedodržení smluvních podmínek a podmínky obnovení anebo ukončení smlouvy.

Typy smluv o poskytování služeb cloud computingu jsou následující (CSCC, 2015):

- ***rámcová smlouva o službách cloud computingu*** – smlouva mezi poskytovatelem služeb cloud computingu a spotřebitelem služeb cloud computingu pokrývající základní pravidla, které budou určující pro uzavření budoucí dohody o službách cloud computingu a dohody o úrovni služeb cloud computingu. Uzavření těchto dohod probíhá na základě podmínek sjednaných v rámcové smlouvě a dohody ustanovují specifické podmínky poskytování služby cloud computingu. Rámcová smlouva dovoluje smluvním stranám rychle sjednat budoucí podmínky poskytování a využívání služby cloud computingu nebo rychle uzavřít budoucí dohodu o službách cloud computingu nebo SLA, protože tyto dohody jsou závislé na podmínkách stanovených v rámcové smlouvě a tyto podmínky nemusí být v budoucích dohodách opakovaně sjednávány a mohou obsahovat pouze budoucí specifické podmínky. Obsah rámcové smlouvy o službách cloud computingu se může lišit v závislosti na poskytovateli, ale všeobecně zahrnuje podmínky objednání služby, dodání služby, přístupu ke

službě, podmínky využívání služeb, ochranu dat, záruky poskytovatele, odpovědnosti spotřebitele, ustanovení týkající se práva duševního vlastnictví, metody fakturace a plateb, finanční nároky a spory, daně, specifikace technické podpory, pravidla úprav a změny ve smlouvě, ukončení smlouvy, prodloužení smlouvy, zřeknutí se práv, smluvní omezení odpovědnosti, mlčenlivost a ochrana obchodního tajemství, náhrada škody, jurisdikce, platné právní předpisy, geograficky specifická regulativa a salvátorská klauzule.

- ***dohoda o službách cloud computingu*** – smluvní dokument zakládající vztah mezi poskytovatelem služeb cloud computingu a spotřebitelem služeb cloud computingu, který obsahuje všeobecné informace o poskytovateli a spotřebiteli, pravidla poskytování služeb a technické a smluvní podmínky, které musí spotřebitel přijmout.
- ***dohoda o úrovni služby cloud computingu (SLA)*** – dohoda mezi poskytovatelem služeb cloud computingu a spotřebitelem služeb cloud computingu mající charakter závazného dokumentu, která obsahuje popis služby cloud computingu, definici cílů úrovně služby cloud computingu (SLO) a definici odpovědností poskytovatele a spotřebitele, akceptované využití služeb, omezení související se službami, výkonnostní parametry služeb a cenové podmínky využití služeb. V cloud SLA se poskytovatel služeb cloud computingu zavazuje zabezpečit plnění konkrétních výkonnostních cílů úrovně služeb jím poskytovaných služeb, realizovat nápravné prostředky v případě výpadku služby a přijmout sankci jako důsledek nesplnění uvedeného smluvního závazku. V dohodě o úrovni služeb cloud computingu jdou definovány obchodní a technické vlastnosti poskytované služby, zejména kvalita služeb, bezpečnost, výkonnost a nápravné prostředky pro obnovení chodu služby, tak aby byly splněny podmínky cloud SLA. Poskytovatel může v rámci cloud SLA také uvést řadu zásad, které nejsou výslovně určeny spotřebiteli, ale které bude muset spotřebitel akceptovat. Tyto mohou být v samostatném dokumentu podmínky užití služby cloud computingu. Dokument podmínky užití služby cloud computingu obsahuje řadu pravidel uplatňovaných poskytovatelem, které omezují způsoby, jimiž mohou být služby cloud computingu využity, neboť mohou být nevhodné či nezákonné a stanovují instrukce k jejich správnému využití. Struktura dohody o službách cloud computingu (SLA) je popsaná v Tabulce 28.

Tabulka 28: Struktura dohody o úrovni služby cloud computingu, zdroj: (autor), podle: (CSCC, 2015; C-SIG SLA, 2014; MITRE, 2015)

Obsah SLA	Parametry SLA
Základní charakteristiky	Účel a rozsah SLA Informace o poskytovateli služeb cloud computingu Informace o spotřebiteli služeb cloud computingu Obsah služby cloud computingu Objem služby cloud computingu Rozsah služby cloud computingu Doba platnosti SLA Zainteresované strany
Definice služby cloud computingu	Cíle úrovně služby cloud computingu (Service Level Objectives) Vzájemné závislost služby cloud computingu na souvisejících službách Volitelná funkcionalita služby
Pravidla a podmínky	Začlenění klauzulí z rámcové smlouvy Odpovědnosti smluvních stran

Obsah SLA	Parametry SLA
	Komunikační a eskalační pravidla Podmínky změny SLA Porušení SLA (míra porušení úrovně služeb a pravidla pro výpočet sankce) Odškodnění a finanční sankce za nesplnění podmínek SLA Vlastnictví dat Omezení použití služby a povinnosti spotřebitele Omezení použitelnosti SLA Unikátní geograficky specifické a národní pravidla a podmínky, legislativní požadavky, jurisdikce Duševní vlastnictví, licenční ujednání Všeobecné podmínky
Technické specifikace a obchodní politiky	Řízení uživatelských účtů a identit (specifikace dostupných mechanismů autentizace, autorizace, federace identit, role pro definici přístupových oprávnění) Řízení přístupové a komunikační bezpečnosti (uživatelské profily, certifikační politika a správa klíčů, ochrana perimetru sítě) Formát přenositelnosti dat spotřebitele služeb cloud computingu Specifikace mechanismů a rozhraní (API) pro realizaci přenositelnosti dat spotřebitele služeb cloud computingu Politika narušení bezpečnostních opatření, řízení zranitelností (počet bezpečnostních opatření ke zmírnění zneužití zranitelnosti hrozbami, počet reportů poskytovatele spotřebiteli o zranitelnostech služby) Rozsah bezpečnostních kontrol poskytovatele služeb cloud computingu Uchovávání a využívání provozních a lokalizačních údajů Klasifikace dat, seznam specifických kategorií osobních dat Politiky pro předpokládané využití dat spotřebitele poskytovatelem a pro využití dat poskytovatelem odvozených z dat spotřebitele Seznam dokumentů, které poskytovatel služeb cloud computingu dává k dispozici za účelem provedení auditu, seznam certifikací poskytovatele Seznam geografických lokalit, kde mohou být data spotřebitele služeb cloud computingu ukládána a zpracovávána poskytovatelem služeb cloud computingu Definice výběru geografické polohy dat spotřebitelem služeb cloud computingu Podporovaná prostředí (vývoj a nasazení), podporované prohlížeče Specifikace požadavků změnového řízení Plánovaná údržba, aktualizace, upgrade, změnové řízení, informace o změnách, eskalační procedury Mechanismy pro zabezpečení nápravných opatření Způsoby formální komunikace Odpovědnost za dodržování legislativy Podmínky archivace dat Využití produktů a služeb třetích stran

Obsah SLA	Parametry SLA
Výkonnostní ukazatele	Dostupnost služby cloud computingu (doba provozuschopnosti služby, doba nedostupnosti služby, procento žádostí zpracovaných službou bez chyby, procento vyřízených žádostí o poskytnutí služby v rámci definovaného časového úseku, datová latence) Doba odezvy služby cloud computingu (maximální doba odezvy, průměrná doba odezvy) Kapacita služby cloud computingu (počet souběžných připojení ke službě v daném okamžiku, maximální počet uživatelů, kteří mohou využít službu v daném okamžiku, škálovatelnost – maximální kapacita zdrojů (velikost datového úložiště, velikost paměti, velikost databáze, doba odezvy databáze, počet operací, rychlost zpracování dat, počet jader procesoru, doba provozu serveru atd.) dostupná pro danou službu – doba potřebná na navýšení kapacity přidáním počtu zdrojů, doba potřebná na snížení kapacity odebráním počtu zdrojů, propustnost služby, vyrovnávání zátěže) Počet transakcí, počet žádostí na předdefinované funkce Konektivita služby cloud computingu k externím systémům a službám, typ API metod, počet žádostí na typ API operace Spolehlivost služby cloud computingu (úroveň schopnosti služby poskytovat funkci správně a bez poruchy v rámci definovaného časového úseku, úroveň schopnosti služby automaticky se přepnout na redundantní nebo záložní službu v případě výpadku)
Ukazatele bezpečnosti	Zabezpečení přístupu ke službě cloud computingu (úroveň zabezpečení poskytovaná mechanismem pro řízení přístupu ke službě, úroveň ochrany uživatelských identit, průměrná doba nutná ke zrušení přístupu uživatele ke službě, úroveň podpory autentizace třetí stranou) Kryptografická ochrana služby cloud computingu (typ protokolu, úroveň síly kryptografické ochrany na základě délky klíče, úroveň ochrany kryptografického klíče, úroveň ochrany šifrovacích operací s využitím kryptografického hardwaru) Bezpečnostní opatření (procento opravných opatření realizovaných poskytovatelem v rámci definovaného časového úseku, procento reportů o zranitelnosti služby dodaných spotřebiteli v rámci definovaného časového úseku)
Ukazatele provozu	Monitorování poskytovaných služeb cloud computingu a reporting (definice monitorovacích metrik, definice parametrů zachycených v logovacích souborech služeb, definice logovacích souborů, ke kterým má spotřebitel přístup, doba, po kterou jsou ukládány logovací soubory, doba provozu monitoringu a informace o výpadcích, definice upozornění na událost či na odchylku od stanovených metrik) Šířka pásma sítě (počet přenesených/přijatých bitů při určitém zatížení za jednu sekundu), propustnost sítě, přenosová výkonnost sítě, doba provozu sítě, latence sítě, odezva sítě, příchozí a odchozí síťový provoz, zpoždění paketů, rozptyl zpoždění paketů, počet ztracených paketů, směrovaní provozu na výstupní síťová zařízení vzhledem ke geografické zóně, počet veřejných IP adres, počet DNS zón, počet příchozích a odchozích emailů Řízení incidentů a reportingu (procento incidentů služby hlášených spotřebiteli v daném časovém intervalu po objevení incidentu, procento

Obsah SLA	Parametry SLA
	incidentů řešených v daném časovém intervalu po objevení) Zálohování dat spotřebitele cloud computingu (seznam metod pro zálohování dat, frekvence zálohování dat, čas potřebný pro zálohování, časový okamžik, od kterého bude služba restartovaná, definice plánu obnovy po havárii, RPO, RTO, doba reakce podpory na havarijní incidenty, čas potřebný pro obnovu dat, doba, po kterou jdou data dostupná pro obnovu, procento úspěšné obnovy dat) Úroveň podpory Service desku služby cloud computingu (typ podpory – telefonní/emailová/Self-Service Portal podpora, provozní doba Service desku poskytovatele služby v závislosti na dopadu nedostupnosti požadované služby na byznys – kritický/významný/nízký/minimální, doba odezvy Service desku, doba k vyřešení požadavku Service deskem)
Platební podmínky	Složky ceny ve vazbě na ukazatele (celkové náklady, fixní náklady, náklady na podporu uživatelů, variabilní FLOPS (Floating Point Operations per Second) náklady, náklady na jednotku výpočetního zdroje) Servisní zásahy Platební kalendář/splatnost Právo fakturovat Sankce za neplnění SLA (finanční sankce, kredit na využívání služeb)
Ukončení smlouvy	Pravidla ukončení smlouvy (asistence poskytovatele, poplatky) Definice exit strategie (doba pro získání dat zpět od poskytovatele, doba, po kterou poskytovatel uchovává kopie dat spotřebitele během procesu ukončení smlouvy, doba, po kterou poskytovatel uchovává data související se spotřebitelem po ukončení procesu ukončení smlouvy, kvalita odstranění dat spotřebitele a souvisejících metadat z úložišť poskytovatele, elektronický formát transferu dat, mechanismus pro transfer dat) Pravidla obnovení smlouvy (automatická obnova, kontinuální fakturace, povinná obnova)
Slovníček pojmů	Definice pojmů uvedených v SLA

7.4 Výběr služby cloud computingu

Fáze výběru služby cloud computingu obsahuje následující proces:

- CMD1: Řízení výběru služby cloud computingu.

7.4.1 Řízení výběru služby cloud computingu

Číslo procesu	**CMD1**
Jméno procesu	**Řízení výběru služby cloud computingu**
Cíl procesu	Výběr nové služby cloud computingu nebo přechod na ekvivalentní službu cloud computingu od jiného poskytovatele.
Popis procesu	Proces realizuje výběr nové služby cloud computingu nebo přechod na ekvivalentní službu cloud computingu od jiného poskytovatele na základě nabídky na trhu služeb cloud computingu tak, aby vybraná služba v optimální míře splňovala požadavky

	cloud computing strategie a příslušné byznys analýzy s důrazem na hodnotu služby cloud computingu pro byznys. Proces provádí analýzu aktuálního stavu nabídky na trhu služeb cloud computingu, hodnotí schopnost daného poskytovatele a jím poskytované služby splnit stanovené požadavky.
Událost	Rozhodnutí o využívání nové služby cloud computingu, rozhodnutí přejít na ekvivalentní službu cloud computingu, ukončení poskytování služby původním poskytovatelem, realizace exit strategie.
Vstup	Informace o službě cloud computingu, informace z portfolia služeb cloud computingu.
Výstup	Hodnocení služby cloud computingu, akceptace služby cloud computingu, zamítnutí služby cloud computingu, informace pro portfolio služeb cloud computingu.
Procesní aktivity	CMD1.1 Analýza stavu nabídky na trhu služeb cloud computingu CMD1.2 Hodnocení a výběr služby cloud computingu

Procesní aktivity:

- **Hodnocení a výběr služby cloud computingu**

Proces řízení výběru služby cloud computingu realizuje optimální výběr služby cloud computingu vedoucí k identifikaci nejvhodnější služby cloud computingu na základě souboru funkčních a nefunkčních požadavků, které musí služba cloud computingu splňovat (viz Tabulka 29). Funkční požadavky popisují, jakou funkcionalitu musí služba poskytovat včetně specifikace technických detailu rozhraní služby a potřebného provozního prostředí. Nefunkční požadavky zahrnují kvalitativní, bezpečnostní a cenové charakteristiky služby a mohou také obsahovat specifikaci provozně subjektivních požadavků na využití služby. Pro každý požadavek by měla být stanovena hodnotící kritéria umožňující porovnání služeb cloud computingu. Seznam kritérií pro hodnocení a výběr služby cloud computingu je definovaný v Tabulce 29.

Tabulka 29: Požadavky na službu cloud computingu, zdroj: (autor)

Soubor požadavků	Požadavky na službu cloud computingu
Kvalita služby	Spolehlivost Dostupnost Konzistentnost Stabilita Transparentnost provozu služby Údržba a spravování služby poskytovatelem
Bezpečnost a ochrana dat	Otevřenost a transparentnost Kontrolovatelnost Kontrola přístupu, nepopíratelnost transakcí Dostupnost, důvěrnost a integrita dat Ochrana osobních údajů Důvěryhodnost Fyzická bezpečnost Lokalizovatelnost dat Zálohování a havarijní obnova

Soubor požadavků	Požadavky na službu cloud computingu
	Vlastnictví dat
	Nakládání s daty po ukončení smluvního vztahu
	Realizovatelnost auditu
Provozní výkonnost služby	Flexibilita
	Funkcionalita
	Vhodnost pro využití
	Přesnost
	Škálovatelnost
	Přizpůsobitelnost
	Rozšiřitelnost
	Integrovatelnost
	Interoperabilita
	Přenositelnost
	Provozuschopnost
	Rychlost implementace a zprovoznění služby
	Kontinuita
	Obnovitelnost do normálního stavu po narušení provozu
	Odolnost proti výpadku
	Doba odezvy
	Objem transakcí
	Počet uživatelů
	Provozní prostředí
Náklady na službu	Cenový model
	Flexibilní licencování
	Náklady na nasazení
	Náklady na využívání
	Rentabilita
Snadnost využití služby	Přístupnost
	Mobilita
	Intuitivnost
	Pochopitelnost funkcionality služby
	Jednoduchost školení pro práci se službou
	Využití služby cloud computingu v režimu Off-line

Optimalizace výběru služeb může být řešena pomocí metod vícekriteriálního rozhodování. Metody vícekriteriálního rozhodování umožňují seřazení variant hodnocení služeb a stanovení optimální varianty výběru služby cloud computingu. Důležitost kritérií je možné vyjádřit stanovením vah.

7.5 Přechod na využívání služby cloud computingu

Přechod na využívání služby cloud computingu je v prostředí spotřebitele služeb cloud computingu je realizován procesy, mezi jejichž hlavní úkoly patří:

- plánování zdrojů potřebných pro nasazení služby cloud computingu do produktivního provozu,
- plánování a testování aktivit souvisejících s přechodem služby computingu do produktivního provozu,
- ověření realizovatelnosti přechodu na využívání služby cloud computingu,
- ověření úrovně kvality služby cloud computingu,
- instalace a služby cloud computingu do produktivního provozu,
- definice pravidel pro zabezpečení přístupu ke službě oprávněným uživatelům.

Procesy fáze přechod na využívání služby cloud computingu jsou:

- CMT1: Plánování přechodu na využívání služby cloud computingu,
- CMT2: Testování a validace služby cloud computingu,
- CMT3: Řízení přístupu uživatele ke službě cloud computingu,
- CMT4: Řízení nasazení služby cloud computingu do produktivního provozu.

7.5.1 Plánování přechodu na využívání služby cloud computingu

Číslo procesu	**CMT1**
Jméno procesu	**Plánování přechodu na využívání služby cloud computingu**
Cíl procesu	Vytvoření plánů aktivit realizace přechodu na využívání služby cloud computingu.
Popis procesu	Proces realizuje plánování a koordinování aktivit a zdrojů potřebných pro produktivní nasazení služby cloud computingu. Proces zajišťuje vytvoření jasných a komplexních plánů pro testování přechodu na využívání služby cloud computingu a pro přechod na využívání služby cloud computingu. Proces zabezpečuje plánování potřebných zdrojů, rozpočtu a harmonogramu.
Událost	Rozhodnutí o využívání nové služby cloud computingu.
Vstup	Artefakty definující využívání nové služby cloud computingu.
Výstup	Plány transformace dat, plány testů přechodu, plány testů služby cloud computingu, plány testů exit strategie, plány realizace přechodu služby cloud computingu do produktivního provozu.
Procesní aktivity	CMT1.1: Vytvoření plánů aktivit potřebných pro realizaci přechodu služby cloud computingu do produktivního provozu

Procesní aktivity:

- **Vytvoření plánů aktivit potřebných pro realizaci přechodu služby cloud computingu do produktivního provozu**

Procesní aktivita realizuje plánování aktivit a úkolů potřebných pro realizaci přechodu služby cloud computingu do produktivního provozu. Mezi hlavní aktivity přechodu na využívání služby cloud computingu patří:

- plánování vytvoření definice datového modelu byznys procesu nebo jeho části, která má být podporována službou cloud computingu,
- plánování identifikace dat nutných pro export z interního systému spotřebitele služby cloud computingu,
- plánování vytvoření definice procedur exportu dat,
- plánování vytvoření definice procedur transformace dat,
- plánování vytvoření definice procedur pro import dat do systému poskytovatele služby cloud computingu,
- plánování vytvoření definice kritérií pro vyhodnocení akceptovatelnosti technické a časové náročnosti procedury přechodu ve vztahu k odstávce produktivního provozu IT služby během realizace přechodu na využívání služby cloud computingu,
- plánování infrastrukturních zdrojů potřebných pro realizaci testů,
- plánování lidských zdrojů potřebných pro realizaci testů,
- plánování vytvoření prostředí pro realizaci testů přechodu,
- plánování časového harmonogramu testů přechodu,
- plánování časového harmonogramu a potřebných lidských zdrojů pro iniciální realizaci procesu řízení přístupu uživatele ke službě cloud computingu,
- plánování časového harmonogramu testů služby cloud computingu,
- plánování vytvoření prostředí pro realizace testů exit strategie,
- plánování časového harmonogramu testů exit strategie,
- plánování rozpočtu pro testování,
- plánování vytvoření definice testovacích případů a kritérií pro akceptaci testů,
- plánování infrastrukturních zdrojů potřebných pro realizaci přechodu služby cloud computingu do produktivního provozu,
- plánování lidských zdrojů potřebných pro realizaci přechodu služby cloud computingu do produktivního provozu,
- plánování harmonogramu realizace přechodu služby cloud computingu do produktivního provozu,
- plánování rozpočtu pro přechod služby cloud computingu do produktivního provozu,
- plánování vytvoření kritérií pro akceptaci služby cloud computingu do produktivního provozu a postupu pro návrat do původního stavu v případě zamítnutí zahájení využívání služby v produktivním provozu,
- plánování opatření pro zabezpečení provozu služby cloud computingu v rané fázi,
- plánování školení pracovníků IT,
- plánování školení uživatelů služby cloud computingu.

7.5.2 Testování a validace služby cloud computingu

Číslo procesu	**CMT2**
Jméno procesu	**Testování a validace služby cloud computingu**
Cíl procesu	Ověření, že přechod na využívání nové služby cloud computingu je realizovatelný technicky a v daném čase. Ověření, že nová služba cloud computingu je v souladu s požadavky na službu a podporuje potřeby byznys procesů očekávaným způsobem. Ověření, že služba cloud computingu splňuje požadavky na službu a podporuje potřeby byznysu očekávaným způsobem i po změně ve službě cloud computingu

	provedené poskytovatelem služby.
Popis procesu	Proces realizuje aktivity spojené s návrhem a provedením testů přechodu na využívání služeb, testů nové nebo změněné služby cloud computingu, testů exit strategie a integračních testů. Proces zabezpečuje objektivní ověření realizovatelnosti přechodu na využívání služby a zabezpečuje objektivní evidenci toho, že nová nebo změněná služba cloud computingu bude splňovat požadavky na službu cloud computingu a že bude schopna očekávaným způsobem podporovat požadované byznys procesy.
Událost	Naplánování testů přechodu, naplánování testů služby cloud computingu, naplánování testů exit strategie, naplánování integračního testu.
Vstup	Seznam požadavků na službu cloud computingu, seznam funkcionalit služby, plány transformace dat, plány testů přechodu, plány testů služby cloud computingu, plány testů exit strategie, definice exit strategie.
Výstup	Výsledky testů, validace výsledků testů.
Procesní aktivity	CMT2.1: Návrh a realizace testů přechodu. CMT2.2: Návrh a realizace testů služby cloud computingu. CMT2.3: Návrh a realizace testů exit strategie. CMT2.4: Provedení validace výsledků testování. CMT2.5: Návrh a realizace integračního testu. CMT2.6: Provedení validace výsledků integračního testu.

Procesní aktivity:

- **Návrh a realizace testů přechodu**

Procesní aktivita realizuje návrh testů přechodu a provedení testů přechodu dle vytvořeného návrhu. Návrh testů přechodu zahrnuje:

- definice hodnot testovaných parametrů, metodika měření hodnot testovaných parametrů, metodika vyhodnocení testů, definice akceptačních kritérií, definice dokumentování provedených testů,
- časový harmonogram pro export dat spotřebitele služby cloud computingu, časový harmonogram pro transformaci dat a časový harmonogram pro import dat do testovacího prostředí poskytovatele služby cloud computingu.

Provedení testů přechodu zahrnuje:

- provedení exportu dat spotřebitele služby, měření hodnot testovaných parametrů a jejich vyhodnocení dle návrhu,
- provedení transformace dat, měření hodnot testovaných parametrů a jejich vyhodnocení dle návrhu,
- import dat do testovacího prostředí poskytovatele služeb cloud computingu, měření hodnot testovaných parametrů a jejich vyhodnocení dle návrhu.

Během každého testu je provedeno zdokumentování výsledků testů, vyhodnocení výsledků testů, je rozhodnuto o akceptaci testů, způsobu řešení zjištěných chyb a je rozhodnuto, zda je možno pokračovat další fází testů.

❖ **Návrh a realizace testů služby cloud computingu**

Procesní aktivita realizuje návrh testů služby cloud computingu a provedení testů služby cloud computingu dle vytvořeného návrhu. Návrh testů služby cloud computingu zahrnuje:

- definice testovacích případů,
- příprava testovacích dat,
- metodika testování,
- metodika vyhodnocování testovacích případů,
- definice akceptačních kritérií,
- definice dokumentování provedených testů,
- časový harmonogram provedení testů služby cloud computingu.

Provedení testů služby cloud computingu zahrnuje:

- provedení testovacích případů dle návrhu,
- zdokumentování výsledků testů,
- vyhodnocení výsledků testů,
- rozhodnutí o akceptaci testů,
- rozhodnutí o způsobu řešení zjištěných chyb,
- rozhodnutí, zda je možno pokračovat další fází testů.

❖ **Návrh a realizace testů exit strategie**

Procesní aktivita realizuje návrh testů exit strategie služby cloud computingu a provedení testů exit strategie služby cloud computingu dle vytvořeného návrhu. Návrh testů exit strategie služby cloud computingu zahrnuje:

- definice testů činností potřebných pro realizaci exit strategie,
- definice hodnot testovaných parametrů,
- metodika měření hodnot testovaných parametrů,
- metodika vyhodnocení testů,
- definice akceptačních kritérií,
- definice dokumentování provedených testů,
- časový harmonogram provedení testů exit strategie.

Provedení testů exit strategie služby cloud computingu zahrnuje:

- provedení testů činností exit strategie dle návrhu,
- zdokumentování výsledků testů,
- vyhodnocení výsledků testů,
- rozhodnutí o akceptaci testů,
- rozhodnutí o způsobu řešení zjištěných chyb,
- rozhodnutí, zda je možno pokračovat další fází testů.

7.5.3 Řízení přístupu uživatele ke službě cloud computingu

Číslo procesu	**CMT3**
Jméno procesu	**Řízení přístupu uživatele ke službě cloud computingu**
Cíl procesu	Definice pravidel, kteří uživatelé nebo skupiny uživatelů mohou využívat službu cloud computingu a definovat soubory oprávnění, které mají být uživateli nebo skupině uživatelů přiřazeny.
Popis procesu	Proces realizuje vytvoření pravidel, kteří uživatelé nebo skupiny uživatelů mohou přistupovat ke službě cloud computingu a pro každého z těchto uživatelů definuje soubor oprávnění v rámci využívání této služby. Tato pravidla a soubory oprávnění jsou udržována pro jednotlivé uživatele, pro skupiny uživatelů v závislosti na jejich pracovní pozici v organizaci, pro uživatele nebo skupiny uživatelů partnerských organizací nebo pro registrované uživatele z řad veřejnosti či anonymní uživatele z řad veřejnosti.
Událost	Nová služba cloud computingu, potřeba byznysu provést změnu pravidel pro přístupu nebo oprávnění, výsledek bezpečnostního auditu.
Vstup	Bezpečnostní politika organizace pro přístup uživatelů ke službám cloud computingu, definice uživatelů nebo skupin uživatelů, dokumenty definující oprávnění potřebná pro přístup k dané funkcionalitě služby cloud computingu, doporučení bezpečnostního auditu.
Výstup	Definice seznamu uživatelů nebo skupin uživatelů, definice pravidel pro přístup uživatelů nebo skupin uživatelů ke službě cloud computingu, definice oprávnění přístupu uživatelů nebo skupin uživatelů ke službě cloud computingu, vytvořené profily oprávnění.
Procesní aktivity	Vytvoření seznamu uživatelů nebo skupin uživatelů s atributy, které identifikují, ke kterým službám cloud computingu mají mít tito uživatelé přístup a k jakým funkcionalitám nebo k jakým datům služby cloud computingu mají mít oprávnění přistupovat. Vytvoření pravidel pro každou položku seznamu uživatelů nebo skupin uživatelů definujících, ke kterým službám cloud computingu může být uživateli nebo skupině uživatelů umožněn přístup a jaká oprávnění mají být tomuto uživateli nebo skupině uživatelů přidělena. Vytvoření profilu oprávnění nebo rolí oprávnění tak, aby uživatel nebo skupina uživatelů mohla realizovat definované funkcionality služby cloud computingu nebo přistupovat k definovaným datům.

7.5.4 Řízení nasazení služby cloud computingu do produktivního provozu

Číslo procesu	**CMT4**
Jméno procesu	**Řízení nasazení služby cloud computingu do produktivního provozu**
Cíl procesu	Nasazení služby cloud computingu do produktivního provozu.
Popis procesu	Proces provádí realizaci plánů přechodu služby cloud computingu do produktivního provozu a aktivaci činností souvisejících s produktivním provozem služby.
Událost	Autorizovaný změnový požadavek na nasazení služby cloud computingu do

	produktivního provozu.
Vstup	Plán realizace přechodu služby cloud computingu do produktivního provozu.
Výstup	Služba cloud computingu v produktivním provozu
Procesní aktivity	CMT4.1: Realizace přechodu služby cloud computingu do produktivního provozu

Procesní aktivity:

- **Realizace přechodu služby cloud computingu do produktivního provozu**

Procesní aktivita provádí řízení realizace přechodu služby cloud computingu do produktivního provozu dle vytvořeného plánu přechodu. Realizace přechodu služby cloud computingu do produktivního provozu zahrnuje:

- provedení exportu dat z interního systému spotřebitele služby cloud computingu,
- provedení transformace dat,
- provedení importu dat do produktivního prostředí poskytovatele služeb cloud computingu,
- vytvoření administrátorských a uživatelských účtů,
- přiřazení profilů oprávnění k účtům,
- aktivace opatření pro řízení bezpečnosti produktivního provozu služby cloud computingu,
- provedení akceptačních testů funkčnosti služby cloud computingu po přechodu do produktivního provozu,
- zahrnutí služby cloud computingu do procesu řízení provozu služeb cloud computingu,
- nastavení metrik pro monitoring služby cloud computingu a zahájení monitorování provozu služby cloud computingu,
- aktivace činností řízení exit strategie definovaných v plánu exit strategie pro produktivní provoz služby cloud computingu

V průběhu realizace přechodu služby cloud computingu do produktivního provozu se provádí jednotlivé činnosti definované v plánu realizace přechodu služby cloud computingu do produktivního provozu. Po ukončení jednotlivých činností se provádí vyhodnocení úspěšnosti provedené činnosti a rozhoduje se o pokračování realizace přechodu nebo o aktivaci postupu pro návrat do původního stavu v případě výskytu kritické chyby.

7.6 Provoz služby cloud computingu

Provoz služby cloud computingu v prostředí spotřebitele služeb cloud computingu je realizován procesy, mezi jejichž hlavní úkoly patří:

- poskytování informací o stavu plnění SLA ze strany poskytovatele služeb cloud computingu,
- poskytování informací o stavu plnění SLA ze strany spotřebitele služeb cloud computingu,
- poskytování informací o stavu služby cloud computingu z hlediska optimalizace nastavení konfigurací služby, za které je odpovědný spotřebitel služby cloud computingu,
- poskytování informací o stavu shody úrovně služby cloud computingu s interními metrikami spotřebitele služby,
- identifikace odchylek od očekávaného stavu,
- řešení detekovaných odchylek,
- realizace požadavků byznysu souvisejících s běžným provozem služby cloud computingu,

- realizace požadavků na přístup ke službě cloud computingu.

Těmito procesy jsou:

- CMO1: Řízení událostí,
- CMO2: Řízení incidentů,
- CMO3: Řízení problémů,
- CMO4: Řízení požadavků na službu cloud computingu,
- CMO5: Řízení požadavků na přístup ke službě cloud computingu,
- CMO6: Monitorování provozu služby cloud computingu.

Procesy fáze provozu služeb cloud computingu jsou podporovány funkcemi:

- servis desk,
- technický management,
- IT operační management,
- aplikační management.

Funkce servis desku je v prostředí spotřebitele služeb cloud computingu rozšířena o propojení se servis deskem poskytovatele služby cloud computingu. Toto propojení zajišťuje, že procesy provozu služeb cloud computingu se realizují na obou stranách služby cloud computingu. Obvykle se jedná o manuální propojení, kdy příslušní pracovníci poskytovatele a spotřebitele služby cloud computingu mají přístup do obou servis desků. Na základě potřeby vyplývající z řízení provozu životního cyklu některého procesu v jednom servis desku vytvoří pracovník ve druhém servis desku incident, požadavek na službu nebo požadavek na přístup ke službě. Proces zdrojového servis desku pak čeká na výsledek příslušného procesu v partnerském servis desku.

Realizace funkcí technického managementu a aplikačního managementu závisí na typu služby cloud computingu služby a dohodnutých podmínkách dodávky služby cloud computingu služby. Rozsah technického, respektive aplikačního managementu se tak může pohybovat od stavu, kdy jeho existence na straně spotřebitele služby cloud computingu není vůbec realizovaná až po stav podobný dodávce služby vlastním IT.

Funkce IT operačního managementu je v prostředí spotřebitele služby cloud computingu služby modifikovaná. Oblast monitoringu je rozšířena o zaměření na parametry a metriky dodávané služby v závislosti na SLA, avšak tentokrát z pohledu spotřebitele služby. Podíl rozsahu monitoringu z pohledu dodavatele služby byznysu se může v závislosti na typu služby cloud computingu přiblížit až k nulové hodnotě. Oblast fyzické správy IT infrastruktury, která se fyzicky nachází u poskytovatele služby cloud computingu, je úplně eliminovaná.

7.6.1 Řízení událostí

Číslo procesu	**CMO1**
Jméno procesu	**Řízení událostí**
Cíl procesu	Dosažení kontinuální informovanosti o stavu provozování služby cloud computingu pomocí monitorování a vyhodnocování událostí vznikajících v souvislosti s provozem služby cloud computingu.
Popis procesu	Proces eviduje všechny události, které vznikají v souvislosti s provozem služby cloud computingu. Na základě vyhodnocení událostí proces určuje, zda provoz služby cloud computingu splňuje požadavky SLA nebo zda došlo k narušení služby cloud computingu. Dále proces pomocí vyhodnocení událostí identifikuje trendy změn

	hodnot parametrů nebo metrik služby.
Událost	Změna stavu některého monitorovaného parametru, metriky nebo funkcionality související s provozovanou službou cloud computingu.
Vstup	Parametry a metriky služby cloud computingu obsažené v SLA, interně definované hodnoty parametrů a metrik provozu služby spotřebitele služby cloud computingu, postupy a procedury smluvně dohodnuté mezi poskytovatelem a spotřebitelem služby cloud computingu pro zpracování událostí, jejich předávání druhé straně a vzájemné komunikaci o událostech, informace o stavu plnění parametrů poskytované služby cloud computingu ze strany poskytovatele služby, informace o stavu plnění parametrů poskytované služby, za něž nese odpovědnost spotřebitel služby cloud computingu, informace o stavu provozu podpůrných služeb souvisejících se službou cloud computingu.
Výstup	Seznam identifikovaných událostí, seznam eskalovaných událostí, dokumentace události, která indikuje incident, dokumentace události, která indikuje významné narušení metriky definované v SLA, seznam událostí souvisejících s nasazením služby anebo se zajištěním provozu služby cloud computingu.
Procesní aktivity	CMO1.1 Detekce a vyhodnocování událostí vznikajících v souvislosti s provozem služby cloud computingu CMO1.2 Zpracování události vzniklé v souvislosti s provozem služby cloud computingu CMO1.3 Uzavření zpracované události

Procesní aktivity:

- **Detekce a vyhodnocování událostí vznikajících v souvislosti s provozem služby cloud computingu**

Detekce a vyhodnocování událostí vznikajících v souvislosti s provozem služby cloud computingu poskytuje nepřetržité a aktuální informace o stavu provozování služby cloud computingu. Události jsou generovány na základě změny stavu některého monitorovaného parametru, metriky nebo funkcionality související s provozovanou službou cloud computingu. Události se mohou týkat jak samotné služby cloud computingu, tak i interních IT služeb, jejichž správná funkčnost podmiňuje správnou funkčnost služby cloud computingu. Vyhodnocení událostí určuje, zda příčina vzniku události je na straně poskytovatele nebo spotřebitele služby cloud computingu. Jsou definovány tři typy událostí:

- *Událost typu upozornění* – Událost typu upozornění poskytuje informaci o tom, že došlo ke změně hodnoty monitorovaného parametru nebo metriky, avšak ne tak významné, aby došlo k ohrožení dodávky služby cloud computingu. V závislosti na konkrétním parametru nebo metrice je zpracování události čistě v kompetenci operačního managementu nebo je obvykle automatizovaně nasměrováno na příslušné odborné pracoviště. Důležité je vyhodnocení trendu. Pokud jsou následující události generovány z důvodu dalšího pokračování ve změně hodnoty monitorovaného parametru nebo metriky nebo nestability jejich hodnot, je nutné aktivizovat eskalační proces a zahájit aktivity k znovuobnovení požadovaného stabilního stavu.
- *Událost typu výjimka* – Událost typu výjimka poskytuje informaci o tom, že došlo k významné změně hodnoty monitorovaného parametru nebo metriky, která znamená přímé ohrožení dodávky služby cloud computingu nebo dokonce její výpadek. Všechny události typu výjimka

jsou eskalovány na příslušné odborné pracoviště. Událost typu výjimka má za následek spuštění procesu řízení incidentu.

- *Událost typu informace* – Událost typu informace poskytuje všechny ostatní informace relevantní pro zajištění provozu služby cloud computingu.

Pokud se událost týká poskytovatele služby cloud computingu, může být na základě smluvních ujednání v dohodě o poskytování služby či v SLA předána informace na partnerský service desk poskytovatele služby cloud computingu. Výstupy z událostí typů upozornění nebo výjimka slouží nebo mohou sloužit jako iniciace řady následných procesů.

7.6.2 Řízení incidentů

Číslo procesu	**CMO2**
Jméno procesu	**Řízení incidentů**
Cíl procesu	Obnovení hodnot parametrů a metrik provozované služby cloud computingu po jejich narušení, a to tak, aby se minimalizoval vliv jejich narušení na provoz byznys procesů.
Popis procesu	Proces realizuje činnosti umožňující obnovu hodnot parametrů nebo metrik služby cloud computingu po jejich narušení. Provádí prvotní diagnózu příčin a realizuje dočasná řešení pro rychlé obnovení provozu služby. Identifikuje následky vzniku incidentu na byznys. Vytváří podklady pro řízení problému.
Událost	Událost typu upozornění nebo výjimka, která oznamuje, že došlo nebo by mohlo dojít k narušení provozu služby cloud computingu.
Vstup	Parametry a metriky služby cloud computingu obsažené v SLA, postupy a procedury smluvně dohodnuté mezi poskytovatelem a spotřebitelem služby cloud computingu, jejichž realizace je v odpovědnosti spotřebitele služby cloud computingu, smluvně dohodnuté procedury pro zpracování incidentů pro jejich předávání druhé straně a pro vzájemnou komunikaci o incidentech, interně definované hodnoty parametrů a metrik na straně spotřebitele služby, které souvisí s provozem služby cloud computingu, interní dokumentace eskalačních postupů incidentů souvisejících s provozem služby cloud computingu.
Výstup	Dokumentace incidentu, dokumentace prvotní analýzy příčin výskytu incidentu, dokumentace následků výskytu incidentu, dokumentace řešení incidentu, dokumentace eskalační komunikace s poskytovatelem služby, dokumentace reakce poskytovatele služby při řešení incidentu.
Procesní aktivity	CMO2.1: Identifikace incidentu vzniklého v souvislosti s provozem služby cloud computingu CMO2.2: Zdokumentování incidentu, kategorizace a prioritizace incidentu CMO2.3: Prvotní analýza příčin výskytu incidentu CMO2.4: Eskalace incidentu CMO2.5: Diagnóza incidentu CMO2.6: Stanovení řešení pro obnovení stavu před narušením služby cloud computingu CMO2.7: Realizace řešení a obnovení stavu před narušením služby cloud computingu CMO2.8: Uzavření incidentu

Procesní aktivity:

- **Prvotní analýza příčin výskytu incidentů vznikajících v souvislosti s provozem služby cloud computingu**

Prvotní analýza příčin výskytu incidentů vznikajících v souvislosti s provozem služby cloud computingu je prováděna s cílem v první řadě určit, zda příčina narušení služby je na straně poskytovatele služby cloud computingu nebo na straně spotřebitele služby. Pro tento případ se stranou spotřebitele služby rozumí i třetí strany, dodávající podpůrné služby, jako je např. internetové spojení. Dále se stranou spotřebitele rozumí i příčiny související s nevyhovujícími ustanoveními ve smlouvách s poskytovatelem služby.

V případě, že příčina narušení provozu služby cloud computingu leží na straně spotřebitele služby, pokračuje spotřebitel služby v prvotní analýze příčin výskytu incidentu, tentokrát s cílem identifikovat příslušné odborné pracoviště, na které je incident následně eskalován.

- **Eskalace incidentů vznikajících v souvislosti s provozem služby cloud computingu**

V případě, že příčina narušení provozu služby cloud computingu je na straně poskytovatele služby, eskaluje spotřebitel služby narušení provozu služby poskytovateli, a to smluvně dohodnutým způsobem. Incident na straně spotřebitele služby čeká, až poskytovatel služby narušení služby odstraní.

V případě, že příčina narušení provozu služby cloud computingu je na straně spotřebitele služby, je incident eskalován na odborné pracoviště spotřebitele identifikované prvotní analýzou incidentu.

- **Diagnóza incidentů vznikajících v souvislosti s provozem služby cloud computingu**

V případě, že příčina narušení provozu služby cloud computingu je na straně poskytovatele služby, není na straně spotřebitele služby diagnóza incidentu prováděna. Spotřebitel v incidentu zdokumentuje následky výskytu incidentu pro byznys.

Pokud je příčina narušení provozu služby cloud computingu na straně spotřebitele, provede spotřebitel diagnózu příčin výskytu incidentu s cílem rychlého obnovení provozu služby a zdokumentuje identifikované příčiny výskytu incidentu a následky výskytu incidentu pro byznys.

- **Stanovení řešení pro obnovení stavu před narušením služby cloud computingu**

V případě, že příčina narušení provozu služby cloud computingu je na straně poskytovatele služby, není na straně spotřebitele služby stanovení řešení pro obnovení stavu před narušením služby cloud computingu prováděno.

Pokud je příčina narušení provozu služby cloud computingu na straně spotřebitele, vyhledá spotřebitel podle výsledků diagnózy příslušný problém a incident k němu přiřadí. Činnosti při řešení incidentu pak vycházejí z dokumentace problému a v něm definovaného dočasného řešení. Není-li příslušný problém dosud k dispozici, pak je pro incident vytvořen nový problém. Na základě výsledků prvotní analýzy je stanoveno a v incidentu zdokumentováno řešení.

❖ **Realizace řešení a obnovení stavu před narušením služby cloud computingu**

V případě, že příčina narušení provozu služby cloud computingu leží na straně poskytovatele služby, není na straně spotřebitele služby realizace řešení pro obnovení stavu před narušením služby cloud computingu prováděna.

Pokud je příčina narušení provozu služby cloud computingu na straně spotřebitele a příslušný problém je již k dispozici, provede spotřebitel k realizaci řešení a obnovení stavu před narušením služby činnosti podle dokumentace dočasného řešení v problému. Pokud byl k incidentu vytvořen nový problém, realizuje spotřebitel řešení dle dokumentace v incidentu.

❖ **Uzavření incidentu**

Po obnovení služby do stavu před narušením je v incidentu finálně zdokumentován průběh jeho řešení.

V případě, že příčina narušení provozu služby cloud computingu leží na straně poskytovatele služby, zdokumentuje spotřebitel zejména údaje, související s odchylkami od SLA nebo jiných smluvních ujednání s poskytovatelem služby cloud computingu, jako je např. doba trvání narušení služby, průběh komunikace s poskytovatelem a případné informace k řešení incidentu získané od poskytovatele služby. Zároveň spotřebitel zdokumentuje následky výskytu incidentu na byznys.

Je-li příčina narušení provozu služby cloud computingu na straně spotřebitele, zdokumentuje spotřebitel služby v incidentu informace o příčině narušení, době trvání narušení služby, realizovaném řešení a důsledcích incidentu pro byznys.

Následně spotřebitel služby cloud computingu incident uzavře.

7.6.3 Řízení problémů

Číslo procesu	**CMO3**
Jméno procesu	**Řízení problémů**
Cíl procesu	Minimalizace výskytů incidentů souvisejících s provozovanými službami cloud computingu, jejichž příčina je na straně spotřebitele služby, eliminací důvodů vzniku těchto incidentů a minimalizace negativních vlivů incidentů souvisejících se službami cloud computingu na provoz byznys procesů.
Popis procesu	Proces analyzuje příčiny vzniku incidentů spojených s provozem služeb cloud computingu a realizuje eliminaci příčin těchto incidentů s využitím metod řešení příčin incidentů tak, aby byla maximalizována byznys hodnota provozovaných služeb cloud computingu. Proces pokrývá pouze incidenty, jejichž příčina výskytu je na straně spotřebitele služby cloud computingu.
Událost	Incident související s provozem služby cloud computingu, jehož příčina je na straně spotřebitele služby.
Vstup	Dokumentace prvotních analýz provedených v rámci procesu řízení incidentů, informace a obnovení provozu služby, informace o úrovni a stabilitě služby po obnovení provozu, informace o době trvání narušené dodávky služby, informace o významu narušení dodávky služby pro provoz byznys procesů, množství výskytu incidentů přiřazených k problému, rozložení výskytu incidentů a jejich významnosti v čase.
Výstup	Dokumentace analýzy dat o četnosti narušení dodávky služby cloud computingu, dokumentace analýzy dat o významnosti narušení dodávky služby cloud computingu,

	dokumentace analýzy dat o vlivu narušení dodávky služby cloud computingu na provoz byznys procesů, návrhy na změny v oblasti interně dodávaných služeb, které mají vliv na úroveň dodávaných služeb cloud computingu.
Procesní aktivity	CMO3.1: Identifikace problému vzniklého v souvislosti s provozem služby cloud computingu CMO3.2: Zdokumentování problému, kategorizace a prioritizace problému CMO3.3: Diagnóza příčin problému CMO3.4: Stanovení dočasného řešení CMO3.5: Analýza prvotních příčin problému CMO3.6: Odstranění příčiny a vyřešení problému CMO3.7: Uzavření problému

7.6.4 Řízení požadavků na službu cloud computingu

Číslo procesu	**CMO4**
Jméno procesu	**Řízení požadavků na službu cloud computingu**
Cíl procesu	Realizace požadavků ze strany uživatelů služby cloud computingu na provedení jednoduchých standardních a standardizovaných změn souvisejících s dodávanou službou cloud computingu.
Popis procesu	Proces realizuje provádění změn uvnitř služby cloud computingu, které uživatelé služby cloud computingu potřebují pro standardní provádění aktivit v rámci jejich byznys procesů. Jedná se o změny, které se vyznačují jednoduchostí a standardizací a tyto změny nijak nenarušují provoz služby cloud computingu. Současně uživatel nemá na provedení těchto změn oprávnění, např. proto, že se jedná o změny v gesci IT nebo změny související s bezpečnostní politikou organizace nebo provádění definovaných změn je ve výhradní pravomoci poskytovatele služby cloud computingu. Může se také jednat o změny, které sice splňují kritéria organizace pro požadavek na změnu, nicméně jejich realizace je podmíněna autorizací v procesu řízení změn. Podstatná jsou smluvní ujednání mezi poskytovatelem a spotřebitelem služby cloud computingu, definující obsah a rozsah změn, které je spotřebitel služby oprávněn provádět vlastními silami. Stejně tak tato smluvní ujednání definují obsah a rozsah změn, které na základě požadavků na službu provede pro spotřebitele poskytovatel služby.
Událost	Vytvoření požadavku na službu souvisejícího s dodávanou službou cloud computingu.
Vstup	Smluvní ujednání mezi poskytovatelem a spotřebitelem služby cloud computingu o obsahu, rozsahu a gesci provádění změn v rámci dodávané služby cloud computingu, interní předpisy o realizaci požadavků na služby týkajících se služby cloud computingu.
Výstup	Zpráva o provedení požadavku na službu cloud computingu, zpráva o zamítnutí požadavku na službu cloud computingu, neboť jeho realizace by byla v rozporu se smluvními ujednáními mezi poskytovatelem a spotřebitelem služby cloud computingu, zpráva o zamítnutí požadavku na službu cloud computingu z důvodů zamítnutí příslušného požadavku na změnu, zpráva o zamítnutí požadavku na službu cloud computingu ze strany poskytovatele služby cloud computingu.

Procesní aktivity	CMO4.1: Přijetí požadavku na službu cloud computingu CMO4.2: Zdokumentování a validace požadavku na službu cloud computingu CMO4.3: Kategorizace a prioritizace požadavku na službu cloud computingu CMO4.4: Autorizace požadavku na službu cloud computingu CMO4.5: Stanovení způsobu realizace požadavku na službu cloud computingu CMO4.6: Vytvoření a schválení požadavku na změnu v závislosti na kategorii požadavku CMO4.7: Provedení požadavku na službu cloud computingu CMO4.8: Uzavření požadavku na službu cloud computingu

7.6.5 Řízení požadavků na přístup ke službě cloud computingu

Číslo procesu	**CMO5**
Jméno procesu	**Řízení požadavků na přístup ke službě cloud computingu**
Cíl procesu	Zajištění, aby uživatel organizace spotřebitele služby cloud computingu, který má mít přístup ke službě cloud computingu, tento přístup měl. Zajištění, aby uživatel služby cloud computingu měl v rámci využívání služby cloud computingu právě a jen právě taková oprávnění, která jsou nutná pro výkon jeho činnosti. Zajištění, aby uživatelé organizace spotřebitele služby cloud computingu, kteří přístup ke službě cloud computingu ke své činnosti nepotřebují, k ní přístup neměli. Zajištění, aby k příslušným funkcionalitám služby cloud computingu měli přístup pracovníci partnerských organizací. Zajištění, aby k příslušným funkcionalitám služby cloud computingu měla přístup veřejnost.
Popis procesu	Proces realizuje informační bezpečnostní politiku spotřebitele v části, která se zaměřuje na oprávnění uživatelů přistupovat ke službě cloud computingu, jejich oprávnění ve vztahu k využívání jednotlivých funkcionalit služby cloud computingu a jejich oprávnění přistupovat k jednotlivým druhům dat služby.
Událost	Vytvoření požadavku na přístup k dodávané službě cloud computingu.
Vstup	Informační bezpečnostní politika spotřebitele, smluvní ujednání mezi poskytovatelem a spotřebitelem služby cloud computingu, obsah požadavku na přístup ke službě cloud computingu.
Výstup	Realizace požadavku na přístup ke službě cloud computingu, dokumentace realizace požadavku, zamítnutí požadavku s odůvodněním zamítnutí.
Procesní aktivity	CMO5.1: Přijetí požadavku na přístup ke službě cloud computingu CMO5.2: Verifikace požadavku na přístup ke službě cloud computingu CMO5.3: Validace požadavku na přístup ke službě cloud computingu CMO5.4: Vytvoření přístupu ke službě cloud computingu CMO5.5: Přiřazení nebo změna oprávnění CMO5.6: Dočasné zablokování přístupu ke službě cloud computingu nebo jeho opětovné uvolnění CMO5.7: Zrušení přístupu ke službě cloud computingu

	CMO5.8: Dokumentace realizace požadavku

Procesní aktivity:

- **Verifikace požadavků na přístup ke službě cloud computingu**

Procesní aktivita provádí v rámci řízení požadavků na přístup ke službě cloud computingu následující verifikace:

- verifikace, zda požadavek formálně odpovídá předpisům bezpečnostní politiky organizace,
- verifikace, zda požadavek formálně odpovídá předpisům bezpečnostní politiky organizace pro dodávanou službu cloud computingu,
- verifikace, zda požadavek autorizovali příslušní odpovědní pracovníci,
- verifikace autorizace požadavku jedná-li se o požadavek, jehož realizace je podmíněna autorizací v rámci procesu řízení změn,
- verifikace, zda realizace požadavku je v odpovědnosti poskytovatele nebo spotřebitele služby cloud computingu.

- **Validace požadavků na přístup ke službě cloud computingu.**

Procesní aktivita realizuje na základě výstupů z verifikace požadavků na přístup ke službě cloud computingu validaci požadavků jejímž výsledkem je:

- zamítnutí požadavku na přístup ke službě cloud computingu,
- realizace požadavku na přístup ke službě cloud computingu,
- předání požadavku na přístup ke službě cloud computingu na servis desk poskytovatele služby cloud computingu smluvně dohodnutým způsobem, pokud realizaci požadavku nebo jeho části je v odpovědnosti poskytovatele služby.

7.6.6 Monitorování provozu služby cloud computingu

Číslo procesu	**CMO6**
Jméno procesu	**Monitorování provozu služby cloud computingu**
Cíl procesu	Sběr dat o provozu služby cloud computingu, detekce odchylek od očekávané úrovně a eskalace detekovaných odchylek.
Popis procesu	Proces realizuje monitorování a reportování hodnot úrovně služby cloud computingu z hlediska souladu parametrů a hodnot metrik aktuálně provozované služby cloud computingu se smluvně dohodnutými parametry a hodnotami metrik v SLA. Proces zabezpečuje průběžný sběr dat o provozu služby cloud computingu, porovnání skutečně naměřené úrovně hodnot metrik s očekávanou úrovní hodnot metrik a v případě jejich odchylky od dohodnuté úrovně iniciuje generování reportů o zjištěných odchylkách a zajišťuje distribuci těchto reportů příslušným rolím na straně spotřebitele služby cloud computing a poskytovatele služby cloud computingu na základě smluvního ujednání.
Událost	Nasazení služby do produktivního provozu.
Vstup	Hodnoty metrik definovaných v SLA, definice eskalačních procedur.
Výstup	Soubory naměřených dat, reporty o odchylkách hodnot parametrů aktuálně

	dodávaných služeb od dohodnutých hodnot parametrů v dohodách o úrovni služeb SLA.
Procesní aktivity	CMO6.1: Sběr dat o provozu služby cloud computingu CMO6.2: Porovnání skutečně naměřené úrovně hodnot metrik s úrovní hodnot metrik definovaných v SLA CMO6.3: Generování odchylek CMO6.4: Eskalace detekovaných odchylek

7.7 Nepřetržité zdokonalování služby cloud computingu

Účelem fáze nepřetržitého zdokonalování služby cloud computingu je zabezpečení, že využívaná služba cloud computingu bude neustále a optimálním způsobem podporovat realizaci byznys procesů, a to jak z hlediska její účinnosti, tak i nákladové efektivity a přijatelné míry rizika. Využívaná služba cloud computingu by měla být schopna dosahovat očekávaných efektů s přijatelnými náklady na její využívání po celou dobu svého životního cyklu. Základem pro efektivní optimalizaci využívání služby cloud computingu jsou smluvní ustanovení ve smlouvě s poskytovatelem služby umožňující spotřebiteli služby realizovat aktivity potřebné pro podporu zdokonalování služby cloud computingu. Na tyto smluvní ustanovení navazuje SLA obsahující definice parametrů a metrik služby včetně jejich hodnot, které jsou pak použity pro měření výkonnosti služby cloud computingu. Prostředkem pro měření výkonnosti služby cloud computingu je monitorování a vyhodnocování naměřených hodnot parametrů a metrik služby. Pokud z porovnání naměřených hodnot parametrů a metrik a aktuálních požadavků byznysu vyplyne, že výkonnost služby již nesplňuje požadavky byznysu nebo vykazuje trend, že tyto požadavky přestanou být plněny, znamená to, že je potřeba vytvořit požadavek na změnu služby nebo úroveň poskytování služby. Realizace požadavku na změnu znamená zahájení komunikace s poskytovatelem služby. V případě potřeby změnit úroveň poskytované služby se bude jednat o úpravu SLA. V případě potřeby změny služby, což může být například změna některé funkcionality, se bude jednat o zahájení iterace životního cyklu služby cloud computingu. Oba typy změn mohou mít vliv jak na potřebu změny ve smluvních ujednáních s poskytovatelem služby, tak na potřebu spotřebitele aktualizovat plány řízení rizik, financování služby nebo revizi požadavků na službu cloud computingu. Není-li poskytovatel schopen akceptovat požadavek na změnu služby, mohou být zahájeny činnosti pro přechod k jinému poskytovateli.

Fáze nepřetržitého zdokonalování služby cloud computingu obsahuje následující proces:

- CMI1: Řízení nepřetržitého zdokonalování služby cloud computingu.

7.7.1 Řízení nepřetržitého zdokonalování služby cloud computingu

Číslo procesu	**CMI1**
Jméno procesu	**Řízení nepřetržitého zdokonalování služby cloud computingu**
Cíl procesu	Zajištění, že výkonnost služby cloud computingu odpovídá dynamicky se měnícím požadavkům byznysu a potřebám byznys procesů
Popis procesu	Proces realizuje aktivity zabezpečující zdokonalování dlouhodobé výkonnosti služby cloud computingu dle potřeb měnících se potřeb byznysu v závislosti na externím prostředí a v souladu s cloud computing strategií. Proces shromažďuje podklady umožňující identifikovat nutnost změny v dodávané službě a vytváří návrhy na změnu služby. Proces zajišťuje komunikaci návrhu se zainteresovanými stranami

	a realizaci schválených změn služby cloud computingu.
Událost	Periodický plán vyhodnocování výkonnosti služby cloud computingu
Vstup	Cloud computing strategie, data z monitorování provozu služby cloud computingu, požadavky byznysu, legislativní požadavky, informace z portfolia služeb cloud computingu, informace z portfolia poskytovatelů služeb cloud computingu, existující SLA.
Výstup	Strategie zdokonalování služby cloud computingu, plán monitorování provozu služby cloud computingu, sebraná data o provozu služby cloud computingu, datová analýza, reporty o výkonnosti služby cloud computingu, návrh na změnu v dodávané službě cloud computingu, verifikovaný návrh na změnu v dodávané službě zainteresovanými stranami, návrh nové SLA.
Procesní aktivity	CMI1.1: Definice strategie zdokonalování služby cloud computingu CMI1.2: Definice plánu monitorování provozu služby cloud computingu CMI1.3: Sběr dat o provozu služby cloud computingu CMI1.4: Zpracování dat o provozu služby cloud computingu CMI1.5: Analýza zpracovaných dat o provozu služby cloud computingu CMI1.6: Vytvoření reportů o výkonnosti služby cloud computingu CMI1.7: Návrh na změnu v dodávané službě cloud computingu CMI1.8: Verifikace návrhu zainteresovanými stranami CMI1.9: Realizace změny dodávané služby cloud computingu

Procesní aktivity:

- **Definice strategie zdokonalování služby cloud computingu**

Procesní aktivita na základě strategických požadavků na využívání služby cloud computingu definuje požadavky na možnost realizace zdokonalování služby cloud computingu formulované prostřednictvím strategie zdokonalování služby cloud computingu. Strategie zdokonalování služby cloud computingu by měla obsahovat:

- určení rozsahu zdokonalování služby cloud computingu,
- určení stupně spolupráce s poskytovatelem služby na zdokonalování služby cloud computingu,
- určení, zda jako alternativa k poskytované službě může být přechod k jinému poskytovateli,
- určení, zda jako alternativa k poskytované službě může být přechod k poskytování služby vlastním IT.

- **Definice plánu monitorování provozu služby cloud computingu**

Procesní aktivita realizuje plánování monitorování provozu služby cloud computingu za účelem získání podkladů pro zdokonalování služby cloud computingu. Těmito podklady jsou informace o požadavcích byznysu na úroveň dodávané služby a informace o aktuální úrovni dodávané služby cloud computingu. Jejich porovnáním jsou identifikovány potenciální oblasti dodávané služby cloud computingu pro realizaci změny služby. Pro definici plánu se využívá seznam parametrů a metrik definovaných v SLA, seznam monitorovacích aktivit monitorování provozu služby cloud computingu souvisejících se zdokonalováním služby cloud computingu, definice reportingu výstupů z řízení

incidentů a problémů a definice reportingu nedostatků ve výkonnosti služby identifikovaných byznysem.

❖ **Sběr dat o provozu služby cloud computingu**

Procesní aktivita realizuje periodické provádění plánu monitorování provozu služby cloud computingu a ukládání získaných dat v definovaných úložištích. Jedná se o data získaná automatizovaným způsobem z monitorovacích systémů a o data získaná manuální realizací plánu monitorování. Sběr dat za účelem zdokonalování služby cloud computingu je prováděn po dobu delšího časového intervalu, neboť cílem není určit pouze aktuální stav služby cloud computingu, ale dlouhodobější trendy ve změnách výkonnosti služby cloud computingu. Podobně monitorování požadavků byznysu na změny ve výkonnosti služby v závislosti na změnách byznys prostředí umožňuje detekovat skutečně relevantní důvody pro návrh na změnu služby nebo návrhy na optimalizaci SLA. Metrikami v tomto případě může být počet událostí a incidentů vztahujících se ke službě cloud computingu a eskalovaných poskytovateli, doba pro zajištění opatření k nápravě poskytovatelem, počet otevřených incidentů a míra jejich dopadu na byznys, počet incidentů vyřešených v daném čase, trend počtu reportovaných událostí a incidentů vztahujících se ke službě cloud computingu atd.

❖ **Návrh na změnu v dodávané službě cloud computingu**

Návrh na změnu v dodávané službě cloud computingu může být vytvořen ve dvou variantách:

- návrh na změnu v SLA,
- návrh na změnu funkcionality služby cloud computingu.

V obou případech je zapotřebí návrh připravit ve spolupráci s poskytovatelem služby. To umožní do návrhu zapracovat i sekundární efekty návrhu na změnu služby jako jsou změny ve finanční náročnosti provozu služby, změny v oblasti informační bezpečnosti nebo změny v oblastech týkajících se legislativních předpisů. Důležitá je také znalost nákladů na realizaci změny, která bude případně účtována spotřebiteli. Zároveň spotřebitel získá informaci, zda poskytovatel služby je schopen požadovanou změnu uskutečnit a v jakém časovém horizontu.

❖ **Realizace změny dodávané služby cloud computingu**

Procesní aktivita zabezpečuje realizaci změny dodávané služby cloud computingu na základě návrhu na změnu služby cloud computingu odsouhlaseného zainteresovanými stranami spotřebitele. Změna může být realizována ve třech úrovních:

- změna SLA,
- změna ve funkcionalitě služby cloud computingu,
- změna poskytovatele služeb cloud computingu.

V případě změny SLA se změna služby cloud computingu plně realizuje novou definicí SLA.

V případě změny ve funkcionalitě služby cloud computingu je spuštěna iterace životního cyklu služby. Poskytovatel dle návrhu spotřebitele provede v testovacím systému změnu funkcionality služby. Spotřebitel provede testy nové nebo změněné funkcionality a případně integrační testy. Poskytovatel provede opravu zjištěných chyb. Po úspěšně provedených testech a seznámení uživatelů s novou funkcionalitou je služba nasazena do produktivního provozu. Spotřebitel provede v produktivním systému potřebné doplňující činnosti, kterými mohou být například implementace nových profilů oprávnění uživatelů nebo úprava parametrů v monitorovacím systému.

Třetí úroveň změny dodávané služby computingu se realizuje v případě, že poskytovatel není schopen realizovat navržené změny a spotřebitel se rozhodne z tohoto důvodu přejít k jinému poskytovateli služby nebo realizovat dodávku služby interním IT oddělením. V tomto případě je nutno realizovat celý proces exit strategie a přechodu k novému poskytovateli služby.

V kapitole 7 je popsán autorkou této doktorské disertační práce navržený model Cloud computing management metodického rámce Cloud computing governance a management (CCGM). Cloud computing management se skládá z Řídících principů cloud computing managementu, Rolí cloud computing managementu a fází životního cyklu služby cloud computingu z pohledu spotřebitele. Těmito fázemi jsou:

- *(CM1) Strategie využití služeb cloud computingu*
- *(CM2) Výběr služby cloud computingu*
- *(CM3) Přechod na využívání služby cloud computingu*
- *(CM4) Provoz služby cloud computingu*
- *(CM5) Nepřetržité zdokonalování služby cloud computingu*

Autorkou této doktorské disertační práce navržené fáze životního cyklu služby cloud computingu z pohledu spotřebitele služeb vychází z fází životního cyklus IT služby dle ITIL 2011. Každá fáze životního cyklu služby cloud computingu obsahuje soubor procesů, které autorka této doktorské disertační práce navrhla na základě modifikace procesů ITIL 2011, management procesů COBIT 5 a dále na základě analýzy dostupných zdrojů a nejlepších zkušeností z praxe.

V kapitole 7.3 autorka této doktorské disertační práce definovala fázi (CM1) Strategie využití služeb cloud computingu, navrhla model pro hodnocení úrovně zralosti/připravenosti organizace pro přijetí služeb cloud computingu, který nazvala Cloud computing maturity model a navrhla a definovala soubor procesů, které realizují danou fázi životního cyklu služby cloud computingu z pohledu spotřebitele. Těmito procesy jsou:

- *CMS1: Řízení rizik z využití služby cloud computingu*
- *CMS2: Finanční řízení služby cloud computingu*
- *CMS3: Řízení souladu s interními standardy a normami, s legislativními a regulatorními předpisy a smluvními požadavky*
- *CMS4: Řízení exit strategie*
- *CMS5: Řízení portfolia poskytovatelů služeb cloud computingu*
- *CMS6: Řízení portfolia služeb cloud computingu*
- *CMS7: Řízení smluv o poskytování služby cloud computingu*

V kapitole 7.4 autorka této doktorské disertační práce definovala fázi (CM2) Výběr služby cloud computingu a navrhla a definovala proces, který realizuje danou fázi životního cyklu služby cloud computingu z pohledu spotřebitele. Tímto procesem je:

- *CMD1: Řízení výběru služby cloud computingu*

V kapitole 7.5 autorka této doktorské disertační práce definovala fázi (CM3) Přechod na využívání služby cloud computingu a navrhla a definovala soubor procesů, které realizují danou fázi životního cyklu služby cloud computingu z pohledu spotřebitele. Těmito procesy jsou:

- *CMT1: Plánování přechodu na využívání služby cloud computingu*

- *CMT2: Testování a validace služby cloud computingu*
- *CMT3: Řízení přístupu uživatele ke službě cloud computingu*
- *CMT4: Řízení nasazení služby cloud computingu do produktivního provozu*

V kapitole 7.6 autorka této doktorské disertační práce definovala fázi (CM4) Provoz služby cloud computingu a navrhla a definovala soubor procesů, které realizují danou fázi životního cyklu služby cloud computingu z pohledu spotřebitele. Těmito procesy jsou:

- *CMO1: Řízení událostí*
- *CMO2: Řízení incidentů*
- *CMO3: Řízení problémů*
- *CMO4: Řízení požadavků na službu cloud computingu*
- *CMO5: Řízení požadavků na přístup ke službě cloud computingu*
- *CMO6: Monitorování provozu služby cloud computingu*

V kapitole 7.7 autorka této doktorské disertační práce definovala fázi (CM5) Nepřetržité zdokonalování služby cloud computingu a navrhla a definovala proces, který realizuje danou fázi životního cyklu služby cloud computingu z pohledu spotřebitele. Tímto procesem je:

- *CMI1: Řízení nepřetržitého zdokonalování služby cloud computingu*

8 Ověření navrženého metodického rámce CCGM

Doktorská disertační práce si kladla za cíl navrhnout metodický rámec Cloud computing governance a management (CCGM) z pohledu spotřebitele služeb cloud computingu a ověřit jej na případové studii.

Cílem této kapitoly je dokumentovat provedenou případovou studii a na základě výsledků studie potvrdit validitu a správnost navrženého metodického rámce Cloud computing governance a management (CCGM) v kapitole 5, 6 a 7. V této kapitole a dílčích podkapitolách je popsána a vyhodnocena případová studie praktické aplikace a ověření metodického rámce Cloud computing governance a management (CCGM) ve velké IT organizaci.

Pro ověření validity, správnosti a praktické využitelnosti navrženého metodického rámce CCGM pro governance a management služeb cloud computingu z pohledu spotřebitele byla použita vědecká metoda případové studie. Případová studie byla realizována v souladu s metodikou pro návrh a realizaci případové studie pro vědecké účely definované v publikaci Case Study Research: Design and Methods (Yin, 2009). Postup případové studie pro ověření metodického rámce CCGM koresponduje s kroky procesu návrhu a realizace případové studie, kterou popisuje Yin (2009). Yin (2009) uvádí, že návrh a realizace případové studie je lineární iterativní proces sestávající se z fází plánování případové studie, návrh případové studie, příprava případové studie, sběr podkladů a dat, analýza podkladů a dat, jejich intepretace a vyhodnocení případové studie (Yin, 2009).

Případová studie byla realizována ve velké IT organizaci v období od ledna do října 2016.

8.1 Plánování případové studie

Výstupem této doktorské disertační práce je artefakt metodický rámec CCGM pro governance a management služeb cloud computingu z pohledu spotřebitele. Jednou z metod vědeckého výzkumu, která umožňuje studovat artefakty v reálném byznys prostředí je případová studie. Metoda případové studie byla vybrána s účelem:

- vyhodnocení platnosti, správnosti, úplnosti a srozumitelnosti navrženého metodického rámce CCGM,
- ověření praktické využitelnosti navrženého metodického rámce CCGM v prostředí spotřebitele služeb cloud computingu.

Realizace případové studie byla umožněna IT organizací, která poskytuje IT služby organizaci zabývající se maloobchodem na území EU podle klasifikace ekonomických činností CZ-NACE (Český statistický úřad, 2015) zařazené do tříd CZ-NACE 47.11 Maloobchod s převahou potravin, nápojů a tabákových výrobků v nespecializovaných prodejnách a CZ-NACE 47.19 Ostatní maloobchod v nespecializovaných prodejnách. IT organizace je považována za velký podnik. Podle Doporučení Komise ze dne 6. května 2003 týkající se definice mikropodniků, malých a středních podniků je střední podnik klasifikován jako podnik do 250 zaměstnanců s ročním obratem do 50 milionů EUR nebo bilanční suma rozvahy dosahuje maximálně 43 milionů EUR.

8.2 Návrh případové studie

Cílem případové studie bylo ověřit praktickou využitelnost navrženého metodického rámce CCGM v reálném byznys prostředí a vyhodnotit platnost a správnost navrženého metodického rámce CCGM

(kapitola 5, 6 a 7) formou pilotního projektu v IT organizaci, která se rozhodla využívat službu cloud computingu v modelu veřejného cloud computingu dodávanou poskytovatelem této služby.

Případová studie byla realizována v nadnárodní maloobchodní organizaci, v jejíž organizační struktuře je IT pracoviště realizováno jako samostatná právnická osoba poskytující informační služby samostatným právnickým osobám maloobchodní organizace. Toto IT pracoviště je pro potřeby případové studie označené jako IT organizace. V čele maloobchodní organizace je právnická osoba, jejímž úkolem je řízení všech právnických osob organizace. Všechny právnické osoby organizace jsou podřízeny této řídící právnické osobě. IT organizace je samostatná právnická osoba.

Organizační struktura IT organizace je kromě vedení IT organizace složena z oddělení IT Governance, IT architektury, IT servis portfolia managementu, IT bezpečnosti, IT compliance, IT office, řízení provozu IT, IT projekt managementu, řízení výkonnosti služeb, síťových služeb, serverových služeb, služeb úložišť dat, zálohovacích služeb a několik oddělení poskytování různých druhů platforem a aplikací. Hlavní činností IT organizace je budování, správa a řízení IT infrastruktury a poskytování služeb IT infrastruktury a IT platformy ostatním právnickým osobám maloobchodní organizace. Kromě toho IT organizace slouží i jako poskytovatel některých aplikací, jako jsou e-mailové nebo komunikační aplikace.

IT organizace zaměstnává přibližně 300 IT specialistů. Rozhodující část IT služeb v oblasti IT platformy tvoří databáze a prostředí pro aplikace dodávané společností SAP. V IT organizaci je spravováno zhruba 300 instalací systémů SAP a dalších zhruba 150 databází s non-SAP aplikacemi. IT organizace je významným zákazníkem firmy SAP a zároveň jejím partnerem ve vývoji nových byznys aplikací.

Pracoviště IT organizace bylo vybudováno jako servisně orientovaná IT infrastruktura na principu servisně orientované architektury. IT organizace je vnitřně rozdělena na oddělení a pracovní týmy, které jsou odpovědné za jednotlivé typy služeb IT infrastruktury. Jako základní nástroj řízení IT infrastruktury a komunikace s byznysem byl implementován systém ITSM dle ITIL, pomocí nějž jsou řízeny všechny fáze životního cyklu IT služeb.

Rozsah poskytovaných IT služeb pro byznys je velmi rozsáhlý. Vzhledem k rychle se měnícím potřebám byznysu se rychle mění i obsah poskytovaných IT služeb. Rozsah a dynamika potřebných změn je tak velká, že IT organizace musela ustoupit od plně formálního řízení provozu IT služeb na základě SLA, minimalizovat rozsah smluvních ustanovení v SLA a část metrik původně obsažených v SLA převést na dynamicky se měnící metriky definované v interním monitorovacím systému. Jako náhradu za metriky definované v SLA vytvořila IT organizace oddělení Řízení výkonnosti služeb, které komunikuje s byznysem jeho potřeby na výkonnost dodávaných IT služeb, a to ve všech fázích životního cyklu IT služby, a dynamicky mění jak příslušné metriky, tak vydává pokyny pro příslušné pracoviště IT organizace na realizaci změn nutných pro splnění nových hodnot metrik. To má za 7následek tak výrazný pokles uplatňování ustanovení SLA, že pracovníci IT organizace již většinou nemají o platných ustanoveních SLA žádné informace a SLA nehrají v jejich pracovní činnosti žádnou roli.

Souhrn specifik IT organizace podstatných z hlediska případové studie je následující:

- velká IT infrastruktura velké nadnárodní organizace,
- servisně orientovaná architektura IT infrastruktury,
- rozvinutá úroveň implementace SOA,
- rozvinutá implementace ITIL a ITSM,
- rozvinuté řízení portfolia služeb,
- rozvinuté řízení IT bezpečnosti,

- rozvinuté řízení přístupu uživatelů k IT službám,
- absence outsourcingu IT služeb,
- absence služeb cloud computingu,
- vymizelý význam SLA.

Podstatným faktorem pro realizaci případové studie v této IT organizaci bylo to, že maloobchodní organizace do této doby zabezpečovala všechny své potřeby na podporu byznys procesů IT službami realizovanými výhradně pomocí svých vnitřních zdrojů. Výjimkou je pouze servis hardwaru umístěného na pracovištích, který je prováděn pracovníky externích organizací. Organizace neprovozovala žádnou službu cloud computingu, a to ani interně.

Vedení organizace rozhodlo o změně procesu řízení přijímacího řízení nových zaměstnanců. Stávající proces, kdy uchazeči o zaměstnání kontaktovali jednotlivá lokální personální pracoviště pomocí e-mailu, byl nevyhovující. Požadavkem bylo zajištění jednoho centrálního kontaktního místa ve formě internetového portálu, na němž budou centrálně k dispozici jak všechny informace pro zájemce o zaměstnání bez omezení lokality, tak i informace pro kterékoliv personální pracoviště o tom, že žadatel má zájem o místo v jejich působnosti. Dále toto centrální kontaktní místo musí umožňovat komunikaci se žadatelem až do ukončení přijímacího řízení. Dalšími požadavky bylo splnění nároků na dostupnost služby, nároků legislativ zemí, kde má organizace zastoupení, realizace bezpečnostních požadavků organizace, realizace pravidel pro přístup uživatelů organizace ke službě a nákladová efektivnost. Vedení organizace odsouhlasilo ideu o výběru aplikační služby cloud computingu poskytující funkcionalitu pro nábor nových zaměstnanců.

8.3 Příprava případové studie

Sběr dat o využitelnosti metodického rámce CCGM v prostředí IT organizace byl umožněn na základě dokumentace generované při praktické aplikaci metod metodického rámce CCGM během plánování, výběru, implementace a provozu aplikační služby cloud computingu, z neformálních rozhovorů se zaměstnanci IT organizace, dotazníkového šetření a z výstupů ITSM aplikace o provozu aplikační služby cloud computingu.

Vzhledem k tomu, že se jednalo o první projekt, který měl za cíl zprovoznění služby cloud computingu poskytované externím poskytovatelem, byl projekt realizován formou pilotního projektu ověření realizovatelnosti adopce služby cloud computingu tzv. Proof-of-Concept. Kromě vlastní implementace zvolené služby cloud computingu a ověření realizovatelnosti adopce služby cloud computingu bylo cílem v rámci realizace tohoto projektu adaptovat stávající IT governance a IT management modely pro prostředí spotřebitele služby cloud computingu. Za tímto účelem byly vytvořeny dva dílčí projekty. První dílčí projekt se zabýval převedením stávající IT služby na službu cloud computingu. Druhý dílčí projekt byl vytvořen za účelem adaptace stávajících IT governance a IT management modelů.

Vstupem při přípravě případové studie byla první verze metodického rámce CCGM navržená na základě analýzy dostupných vědeckých publikací a dokumentů vztahujících se ke governance a managementu využívání služeb cloud computingu z hlediska spotřebitele a metodických rámců pro IT governance a IT managment. V rámci prvního dílčího projektu byl aplikován model cloud computing management metodického rámce CCGM. Vycházelo se z definice devíti řídících principů, které zabezpečují podporu rozhodování při návrhu, nasazení a provozování cloud computing managementu. V rámci jednotlivých kroků životního cyklu služby cloud computingu byly aplikovány procesy cloud computing managementu včetně cloud computing management rolí. Vyhodnocení těchto procesů a rolí je provedeno v následující kapitole 8.4. V rámci druhého dílčího projektu byla

provedena adaptace stávajícího modelu IT management na základě modelu Cloud computing management metodického rámce CCGM a stávajícího modelu IT governance na základě modelu Cloud computing governance metodického rámce CCGM. Implementační proces Cloud computing governance je popsán v kapitole 8.4.6. Adaptace stávajících IT governance a IT management modelů probíhala ve formě redefinice stávajících politik, procesů a rolí, definicí nových politik procesů a rolí adefinicí nových směrnic. Základní informace o governance a managementu služeb cloud computingu byla vložena do školícího systému organizace a přiřazena příslušným pracovníkům IT infrastruktury jako povinné školení. Školení k problematice governance a managementu služeb cloud computingu bylo prováděno v závislosti na pozici v průběhu realizace projektu.

8.4 Aplikace navrženého metodického rámce CCGM

V rámci prvního dílčího projektu převedení stávající IT služby na službu cloud computingu byla provedena praktická aplikace navrženého metodického rámce CCGM umožňující efektivní podporu při výběru, implementaci a v produktivním provozu služby. Během jednotlivých fází prvního dílčího projektu byla sbírána data vyplývající z praktického využití metodického rámce CCGM. Fáze projektu korespondují s fázemi životního cyklu služby cloud computingu, a proto byly během prvního dílčího procesu aplikovány nejprve cloud computing management procesy a byly rozšířeny odpovědnosti rolí existujících v IT organizaci v souladu s rolemi cloud computing managementu definovanými v kapitole 7.2. Jelikož IT organizace implementovala metodiky ITIL na rozvinuté úrovni a jedná se pouze o jedinou využívanou službu cloud computingu, většina rolí cloud computing managementu nebyla nově definovaná, ale jednalo se zejména o rozšíření odpovědností stávajících rolí zohledňující prostředí cloud computingu. Zcela novou rolí, kterou IT organizace na základě metodického rámce CCGM definovala je role manažer exit strategie.

Plánování modelu Cloud computing management vychází z řídících principů cloud computing managementu (kapitola 7.1), které byly plně převzaty. Tabulka 30 uvádí vyhodnocení řídících principů cloud computing management z hlediska jejich míry využití při realizaci případové studie.

Tabulka 30: Vyhodnocení řídících principů cloud computing management, zdroj: (autor)

Číslo	Název řídícího principu	Využití
ŘPM1	Cloud computing management musí být v souladu s podnikovým managementem a IT managementem a musí být podporována výkonným vedením.	Aplikován
ŘPM2	Vytvoření, rozvoj a ukončení vztahu mezi poskytovatelem a spotřebitelem musí být založeno na smluvní dohodě vymahatelné zákonem.	Aplikován
ŘPM3	Data o dodávaných službách cloud computingu musí být udržovaná v systému metadat služeb cloud computingu.	Aplikován
ŘPM4	Data o poskytovatelích služeb cloud computingu musí být udržovaná v systému metadat o poskytovatelích služeb cloud computingu.	Aplikován
ŘPM5	Rizika související s využíváním služeb cloud computingu musí být efektivně řízená.	Aplikován
ŘPM6	Náklady na provoz služeb cloud computingu musí být efektivně řízené.	Aplikován
ŘPM7	Výkonnost služeb cloud computingu musí být efektivně řízená.	Aplikován
ŘPM8	Provoz služeb cloud computingu musí být kontinuálně řízen tak, aby využívané služby cloud computingu nepřetržitě splňovaly kritéria obsažená v SLA a požadavky byznysu a aby odchylky od těchto kritérií byly detekovány a eliminovány.	Aplikován
ŘPM9	Pro efektivní podporu modelu cloud computing management musí být dostupné potřebné umožňující schopnosti a prostředí.	Aplikován

8.4.1 Strategie z využití služby cloud computingu

Tabulka 31 uvádí vyhodnocení procesů fáze (CM1) Strategie využití služeb cloud computingu z hlediska jejich míry využití při realizaci případové studie, resp. zda u každého procesu byly nebo nebyly aplikovány všechny procesní aktivity při převádění stávající IT služby na službu cloud computingu.

Tabulka 31: Vyhodnocení procesů fáze (CM1) Strategie z využití služby cloud computingu, zdroj: (autor)

Číslo	Proces	Využití procesu
CMS1	Proces řízení rizik z využití služby cloud computingu	Aplikován částečně
CMS2	Finanční řízení služeb cloud computingu	Aplikován částečně
CMS3	Řízení souladu s interními standardy a normami, s legislativními a regulatorními předpisy a smluvními požadavky	Aplikován částečně
CMS4	Řízení exit strategie	Aplikován
CMS5	Řízení portfolia poskytovatelů služeb cloud computingu	Aplikován částečně
CMS6	Řízení portfolia služeb cloud computingu	Aplikován částečně
CMS7	Řízení smluv o poskytování služby cloud computingu	Aplikován částečně

Tabulka 32 uvádí vyhodnocení rolí fáze (CM1) Strategie využití služeb cloud computingu ve vztahu k jednotlivým procesům. Popisuje úroveň využití role a tedy, zda byly role definované v kapitole 7.2 aplikovány, resp. nově vytvořeny anebo, zda byly na základě definovaných rolí v kapitole 7.2 existující role rozšířeny o příslušné odpovědnosti ve vztahu k těmto rolím.

Tabulka 32: Vyhodnocení rolí ve vztahu k procesům fáze (CM1) Strategie z využití služby cloud computingu, zdroj: (autor)

Číslo procesu	Role	Využití role
	Chief Information Officer	Rozšíření stávající role
	Cloud computing analytik	Rozšíření stávající role
CMS1	Manažer řízení rizik cloud computingu	Rozšíření stávajících rolí
CMS2	Finanční manažer služeb cloud computingu	Rozšíření stávajících rolí
CMS3	Manažer pro řízení souladu služeb cloud computingu s legislativou	Rozšíření stávajících rolí
CMS4	Manažer cloud exit strategie	Aplikována
CMS5	Manažer portfolia poskytovatelů a řízení vztahu s poskytovateli	Rozšíření stávajících rolí
CMS6	Manažer katalogu služeb cloud computingu	Rozšíření stávající role
CMS7	Cloud SLA manažer	Rozšíření stávající role

Proces ***CMS1: Řízení rizik z využití služby cloud computingu*** byl aplikován částečně. IT organizace implementovala na základě řady norem ISO/IEC 27000 systém ISMS. Analýza a hodnocení rizik zvolené služby cloud computingu byla provedena na základě dosavadních zkušeností pracovníků organizace ve spolupráci s vybraným poskytovatelem služby, s podrobnou dokumentací funkcionalit a vlastností služby dodanou poskytovatelem služby a s informacemi získanými od příslušných podpůrných a byznys oddělení. V rámci analýzy rizik byla nejprve identifikována relevantní rizika vztahující se k využití vybrané služby cloud computingu na základě seznamu rizik definovaných v Tabulkách 20, 21 a 22 (kapitola 7.3.1), byl aktualizován rizikový profil, IT registr rizik, limity a souhrn nejvýznamnějších rizik. Pro tato rizika bylo provedeno hodnocení významnosti rizika. Byla stanovena akceptační kritéria. Na závěr byla aktualizovaná bezpečností politika organizace zejména

z hlediska jednotného přístupu k hodnocení a řízení rizik z využití služby cloud computingu. Procesní aktivita CMS1.3: Zvládání rizik vyplývajících z využití služby cloud computingu nebyla provedena.

Odpovědnost za realizaci procesu byla přiřazena oddělení IT bezepečnosti. Stávající role byly rozšířené o specifické odpovědnosti role manažer řízení rizik cloud computingu definované v Tabulce 18 (kapitola 7.2).

Proces ***CMS2: Finanční řízení služeb cloud computingu*** byl aplikován částečně. Byla provedena analýza celkových nákladů na vlastnictví postavená na identifikaci celkových očekávaných nákladů na pořízení, provoz a ukončení provozu služby cloud computingu s využitím Tabulky 24 (kapitola 7.3.2). Ty byly porovnány s celkovými očekávanými náklady na realizaci služby interními zdroji ve formě IT služby. Dále byl připraven plánovaný rozpočet pro zavedení služby cloud computingu a pro první rok provozu služby cloud computingu a předpokládaná výše nákladů pro případ ukončení provozu služby a přechod na vlastní řešení. Procesní aktivity CMS2.3: Analýza přínosů z využívání služby cloud computingu a CMS2.4: Hodnocení efektivnosti investice do využívání služby cloud computingu nebyly provedeny.

Odpovědnost za realizaci procesu byla přiřazena oddělení IT office, který má na starosti řízení aktiv, správu a optimalizaci softwarových licencí, řízení portfolia dodavatelů, účtování SLA, analýzu nákladů, tvorbu rozpočtů a IT controlling. Stávající role byly rozšířené o specifické odpovědnosti role finanční manažer služeb cloud computingu definované v Tabulce 18 (kapitola 7.2).

Proces ***CMS3: Řízení souladu s interními standardy a normami, s legislativními a regulatorními předpisy a smluvními požadavky*** byl aplikován částečně. Ve spolupráci s právním oddělením byly identifikovány relevantní zákony a regulatorní předpisy zemí EU, ve kterých bude služba provozovaná a využívaná, byl aktualizován seznam legislativních a regulatorních předpisů a byly doplněny příslušné předpisy a požadavky z nich vyplývajících z hlediska využití služby cloud computingu. Dále byly připraveny podklady pro vyjednávání smluv o poskytování služeb cloud computingu (SLA). Procesní aktivity CMS3.4: Plánování školení zainteresovaných stran, CMS3.5: Monitorování souladu a CMS3.6: Hodnocení souladu a realizace nápravných opatření nebyly provedeny.

Odpovědnost za realizaci procesu byla přiřazena oddělení IT compliance. Stávající role byly rozšířené o specifické odpovědnosti role manažer pro řízení souladu služeb cloud computingu s legislativou definované v Tabulce 18 (kapitola 7.2).

Proces ***CMS4: Řízení exit strategie*** byl aplikován. Vedení rozhodlo, že záložním scénářem pro případ nerealizovatelnosti využívání služby cloud computingu od firmy SAP, bude realizace služby interními zdroji ve formě non-cloudové služby. Exit strategie dokumentuje plány související s ukončením využívání aplikační služby cloud computingu. Byl definován datový model popisující byznys objekty související s procesem řízení přijímacího řízení nových zaměstnanců, jejich atributy včetně určení datového typu a vztahy mezi těmito objekty. Na jeho základě byla identifikována data, která bude IT organizace potřebovat pro ukončení využívání aplikační služby a přechod na její interní řešení při zachování kontinuity provozu. Byl vytvořen předpokládaný plán zdrojů potřebných pro realizaci ukončení využívání služby, časový harmonogram realizovatelnosti procesu přechodu na interní řešení a byla provedena analýza očekávaných nákladů na ukončení využívání služby a přechod internímu řešení. Pro SLA byly definovány podmínky ukončení využívání aplikační služby cloud computingu, kdy po jejím ukončení SAP provede export dat souvisejících se službou a předá je IT organizaci.

Pro proces CMS4: Řízení exit strategie byla definovaná nová role manažer cloud exit strategie definované v Tabulce 18 (kapitola 7.2). Roli manažer cloud exit strategie byly přiřazeny odpovědnosti za tvorbu plánů exit strategie služby cloud computingu, definici exit strategie služby cloud

computingu v SLA, koordinaci aktivit a zdrojů potřebných při plánování a realizaci exit strategie služby cloud computingu. Role manažer cloud exit strategie byla zařazena do oddělení IT office.

Proces ***CMS5: Řízení portfolia poskytovatelů*** služeb cloud computingu byl aplikován částečně. Výběr poskytovatele služby cloud computingu byl realizován na základě požadavků na spolehlivost a důvěryhodnost poskytovatele, na jeho reputaci, rozsah poskytované služby, bezpečnost a ochranu dat a na náklady na službu. Pro tyto skupiny požadavků byla definována minimální požadovaná kritéria, na základě, kterých byly do užšího výběru vybrány tři společnosti poskytující požadovanou službu cloud computingu, a to Oracle, IBM a SAP. Ve všech třech případech se jedná o velké a stabilní organizace působící v rámci EU. Hodnotící kritéria, na základě, kterých byli vybraní poskytovatele posuzováni, byla ohodnocena dle důležitosti a byly definovány minimálně očekávané hodnoty kritérií s ohledem na princip nákladové efektivnosti. Na základě výsledků hodnocení byla jako poskytovatel služby cloud computingu vybrána firma SAP. Procesní aktivita CMS5.2: Vytvoření a udržování vztahu s poskytovatelem služby cloud computingu nebyla provedena, jelikož se v případě SAPu již jedná o stávajícího a významného dodavatele IT řešení.

Odpovědnost za realizaci procesu byla přiřazena oddělení IT office, který má na starost řízení aktiv, správu a optimalizaci softwarových licencí, řízení portfolia dodavatelů, účtování SLA, analýzu nákladů, tvorbu rozpočtů a IT controlling. Stávající role byly rozšířené o specifické odpovědnosti role manažer portfolia poskytovatelů a řízení vztahu s poskytovateli definované v Tabulce 18 (kapitola 7.2).

Proces ***CMS6: Řízení portfolia služeb cloud computingu*** byl aplikován částečně. Údaje týkající se služby cloud computingu poskytnuté poskytovatelem služby cloud computingu a související dokumenty jsou udržovány jako soubor dokumentů ve speciálně vytvořeném adresáři. Katalog služeb cloud computingu spotřebitele nebyl vytvořen. Jelikož se jedná o jednu službu cloud computingu, byla tato služba zařazena do stávajícího katalogu IT služeb s příznakem identifikující její odlišnost od IT služeb. V současné době nebylo rozhodnuto, zda stávající software bude rozšířen tak, aby umožňoval automatizovanou správu služeb cloud computingu. Procesní aktivity CMS6.2: Analýza služeb v portfoliu služeb cloud computingu a CMS6.3: Návrh a provoz katalogu služeb spotřebitele služeb cloud computingu nebyly provedeny.

Odpovědnost za realizaci procesu byla přiřazena v rámci oddělení IT servis portfolia managementu týmu IT služby, který má na starost řízení IT služeb. Stávající role Service Catalogue Manager byla rozšířená o specifické odpovědnosti role manažer katalogu služeb cloud computingu definované v Tabulce 18 (kapitola 7.2). Jelikož však katalog služeb cloud computingu nebyl vytvořen, je role Service Catalogue Manager odpovědná zejména za udržování správného a aktuálního souboru dokumentů vztahujících se k aplikační službě cloud computingu ve speciálně vytvořeném adresáři, za periodické hodnocení aplikační služby cloud computingu z hlediska souladu s požadavky na službu cloud computingu, a za podporu týmu řízení IT rizik a podporu týmů zabezpečujících provoz aplikační služby cloud computingu.

Proces ***CMS7: Řízení smluv o poskytování služby cloud computingu*** byl aplikován částečně. Se společností SAP, jakožto nejen s poskytovatelem služby cloud computingu, ale také jako s dlouholetým poskytovatelem byznys aplikací, byla vyjednávána, odsouhlasena a uzavřena dohoda o službě a dohoda o úrovni služby (SLA). Dohoda o službě definuje základní specifikaci a omezení služby cloud computingu s ohledem na objem, obsah a cenu služby. V dohodě o službě se společnost SAP zavazuje poskytovat sjednanou službu po stanovené období při daném způsobu účtování služby. SLA stanovuje garantované výkonnostní parametry služby, cílové metriky služby a obsahuje definice eskalačního řízení. Konfigurace služby v závislosti na smlouvách o poskytování služby cloud computingu byla provedena v nástroji Solution Manager. Jedná se zejména o nastavení profilu služby,

profilu odezvy, definice procedur pro různé scénáře případů užití, customizaci transakčních typů, eskalační procedury, monitorování a reportování.

Odpovědnost za realizaci procesu byla přiřazena v rámci oddělení IT servis portfolia managementu týmu IT služby. Stávající role SLA manager byla rozšířená o specifické odpovědnosti role cloud SLA manažer definované v Tabulce 18 (kapitola 7.2).

8.4.2 Výběr služby cloud computingu

Tabulka 33 uvádí vyhodnocení procesu fáze (CM2) Výběr služby cloud computingu.

Tabulka 33: Vyhodnocení procesů fáze (CM2) Výběr služby cloud computingu, zdroj: (autor)

Číslo	Proces	Využití procesu
CMD1	Řízení výběru služby cloud computingu	Aplikován

Tabulka 34 uvádí vyhodnocení role fáze (CM2) Výběr služby cloud computingu ve vztahu k procesu.

Tabulka 34: Vyhodnocení role ve vztahu k procesu fáze (CM2) Výběr služby cloud computingu, zdroj: (autor)

Číslo procesu	Role	Využití role
CMS1	Manažer služeb cloud computingu	Rozšíření stávajících rolí

Proces ***CMD1 Řízení výběru služby cloud computingu byl aplikován***. Na základě analýzy trhu byly vybrány služby od třech poskytovatelů Oracle, IBM a SAP. Požadavky na službu cloud computingu byly definovány v součinnosti s příslušnými odděleními s využitím seznamu požadavků na službu cloud computingu definovaných v Tabulce 29 (kapitola 7.4.1). Požadavky byly vyhodnoceny dle preferencí na kvalitu poskytované služby cloud computingu, bezpečnost o ochranu dat, provozní výkonnost, snadnost využití a nákladovou efektivnost a byla vybrána aplikační služba společnosti SAP. Pro každý požadavek – kritérium byla expertním odhadem stanovena hodnota na bodové stupnici 1 až 10 (1 – nejhorší, 10 – nejlepší). Byla vybrána kritéria považovaná jako klíčová. Nesplnění těchto kritérií by bylo nepřijatelné, tato kritéria byla označena jako tzv. NoGo kritéria. Každému kritériu byla přidělena váha. Významná tzv. NoGo kritéria byla odhodnocena nejvyšší váhou (nejvyšší pořadové číslo). Pro každou hodnotu kritéria a váhu kritéria bylo provedeno normování. Celkové ohodnocení služeb bylo realizováno jako vážený součet variant služeb od poskytovatelů Oracle, IBM a SAP vzhledem k jednotlivým kritériím. Normované hodnocení jednotlivých variant byla násobeno s normovanými váhami, čímž bylo získáno výsledné pořadí, kdy v hodnocení dopadla nejlépe služba poskytovaná společností SAP.

Odpovědnost za realizaci procesu byla přiřazena týmu IT služby, který má na starost řízení IT služeb. Stávající role byly rozšířené o specifické odpovědnosti role manažer služeb cloud computingu definované v Tabulce 18 (kapitola 7.2).

8.4.3 Přechod na využívání služby cloud computingu

Tabulka 35 uvádí vyhodnocení procesů fáze (CM3) Přechod na využívání služby cloud computingu.

Tabulka 35: Vyhodnocení procesů fáze (CM3) Přechod na využívání služby cloud computingu, zdroj: (autor)

Číslo	Proces	Využití procesu
CMT1	Plánování přechodu na využívání služby cloud computingu	Aplikován
CMT2	Testování a validace služby cloud computingu	Aplikován částečně

Číslo	Proces	Využití procesu
CMT3	Řízení přístupu uživatele ke službě cloud computingu	Aplikován
CMT4	Řízení nasazení služby cloud computingu do produktivního provozu	Aplikován

Tabulka 36 uvádí vyhodnocení rolí fáze (CM3) Přechod na využívání služby cloud computingu ve vztahu k jednotlivým procesům.

Tabulka 36: Vyhodnocení rolí ve vztahu k procesům fáze (CM3) Přechod na využívání služby cloud computingu, zdroj: (autor)

Číslo procesu	Role	Využití role
CMT1	Manažer přechodu na využití služby cloud computingu	Rozšíření stávající role
CMT2	Cloud test manažer	Rozšíření stávající role
CMT3	Manažer pro řízení přístupu ke službě	Rozšíření stávající role
CMT4	Manažer nasazení služeb cloud computingu	Rozšíření stávajících rolí

Proces ***CMT1: Plánování přechodu na využívání služby cloud computingu*** byl aplikován. V rámci plánování přechodu byly vytvořené:

- plány aktivit a zdrojů potřebných pro realizaci přechodu aplikační služby do produktivního provozu,
- plán vytvoření datového modelu souvisejícího s byznys procesem, jehož podpora bude realizována aplikační službou cloud computingu, obsahující identifikaci dat, rozdělení dat podle typů, definici vazeb mezi datovými objekty a identifikaci kategorií uživatelů, kteří budou k datům přistupovat,
- plán exportu dat z interního systému a transformace dat,
- plán potřebných technických, lidských a finančních zdrojů, harmonogram aktivit pro realizaci testů přechodu a testů služby cloud computingu,
- plán definice testovacích případů a kritérií pro akceptaci testů,
- plán potřebných lidských zdrojů a harmonogram pro iniciální realizaci procesu řízení přístupu uživatele ke službě cloud computingu,
- plány technických, lidských a finančních zdrojů pro realizaci přechodu služby cloud computingu do produktivního provozu a časový harmonogram aktivit přechodu služby do produktivního provoz,
- plány pro vytvoření kritérií akceptace služby cloud computingu pro přechod do produktivního provozu,
- plány postupu pro návrat do původního stavu v případě zamítnutí zahájení využívání služby v produktivním provozu. Součástí bylo také naplánování školení IT pracovníků a uživatelů služby cloud computingu.

V rámci plánování přechodu na využívání služby cloud computingu byl sestaven tým pro řízení projektu přechodu na produktivní provoz služby. Jako členové týmu byli určeni techničtí pracovníci IT infrastruktury a zástupci byznys oddělení, které tuto službu bude využívat pro realizaci byznys procesu. Bylo stanoveno, že tento tým bude zabezpečovat provoz služby během prvních čtrnácti dnů produktivního provozu. Všechny vznikající požadavky, události a incidenty související s provozem nové služby byly po tuto dobu přesměrovány ihned přímo na tento tým, který je operativně vyhodnocoval na základě priorit. Tento tým v prvních čtrnácti dnech akceptoval požadavky, události a incidenty přijímané přímo telefonicky a e-mailem. Vedoucí týmu Transition Manager vedl evidenci o všech přímých přijatých požadavcích, událostech a incidentech v Excelu. Tento soubor byl dostupný

pro čtení ostatním členům týmu. Dále vedoucí týmu udržoval všechny další dokumenty související s přechodem a počátečním operativním provozem služby. Vedoucí týmu po dobu prvních čtrnácti dnů pracoval také jako eskalační manažer, kdy měl na starost komunikaci s poskytovatelem služby. Některé požadavky na službu byly vyhodnoceny jako události anebo incidenty, které je nutné řešit okamžitě. Tyto prioritní události byly vyřešeny během prvního týdne. Ostatní požadavky, které byly vyhodnoceny jako návrhy na změnu, se budou řešit klasickými procedurami životního cyklu služby po ukončení počáteční doby provozu služby. Během druhého týdne byla provozovaná služba v souladu s SLA a nevyskytly se žádné další události narušující efektivní provoz služby.

Odpovědnost za realizaci procesu byla přiřazena týmu IT projekt managementu, pod jehož kompetence spadá plánování a vedení projektů, koordinace projektů, technické vedení projektů, návrh architektury řešení a konzultační činnosti. Stávající role Transition Manager byla rozšířená o specifické odpovědnosti role manažer přechodu na využití služby cloud computingu definované v Tabulce 18 (kapitola 7.2).

Proces ***CMT2: Testování a validace služby cloud computingu*** byl aplikován částečně. Realizace testů přechodu a testů služby cloud computingu proběhla v plánovaném rozsahu v souladu s vytvořeným návrhem. Byl otestován přechod služby, bylo realizováno funkční testování služby prostřednictvím navržených testovacích případů pro určení, zda funkcionalita služby splňuje požadované očekávání a byly provedeny integrační testy pro otestování komunikace a spolupráce služby cloud computingu se stávajícími IT službami. Na základě vyhodnocení výsledků z provedených testů byla služba cloud computingu uvolněna pro nasazení do produktivního provozu. Procesní aktivita CMT2.3: Návrh a realizace testů exit strategie nebyla realizována, neboť exit strategie byla naplánovaná pouze pro případ smluvního ukončení využívání služby cloud computingu.

Odpovědnost za realizaci procesu byla přiřazena roli Test Manager v týmu interní IT testování, pod jehož kompetence spadá plánování a vedení testů, koordinace testů a realizace testů. Stávající role Test Manager byla rozšířená o specifické odpovědnosti role cloud test manažer definované v Tabulce 18 (kapitola 7.2).

Proces ***CMT3: Řízení přístupu uživatele ke službě cloud computingu*** byl aplikován. Protože tato aplikační služba realizuje aplikaci SAP, byla pro realizaci tohoto procesu použita stejná metodika jako pro ostatní aplikace SAP již existující v organizaci. Byly vytvořeny seznamy uživatelů rozdělených do tří skupin:

- skupina uživatelů technických administrátorů,
- skupina uživatelů aplikačních administrátorů,
- skupina uživatelů aplikace, která byla dále rozdělená do podskupin uživatelů podle pracovního zařazení.

Jako základ pro vytvoření tohoto seznamu byl použit seznam uživatelů v existující aplikaci SAP human capital management. Protože pro tuto službu již byly vytvořeny pravidla definující oprávnění pro přístup uživatelů a byly již vytvořeny role a oprávnění, byla tato pravidla a oprávnění převzata jako iniciální verze pro vytvoření cílové verze nové aplikační služby cloud computingu. Tato iniciální pravidla a oprávnění byla na základě aplikační dokumentace dodané poskytovatelem služby upravena pro potřeby využívání nové služby cloud computingu. Podle těchto upravených dokumentů byly v testovací verzi služby cloud computingu vytvořeni uživatelé. V průběhu realizace procesu testování a validace služby byly vyhodnoceny testy aplikace pravidel přístupu uživatele ke službě a oprávnění uživatele při využívání této služby. Na základě vyhodnocení těchto testů byly vytvořeny cílové verze pravidel pro přístup uživatelů ke službě cloud computingu a profilů oprávnění uživatelů z jednotlivých skupin uživatelů.

Vzhledem k tomu, že se jedná o aplikační službu od společnosti SAP, byla odpovědnost za realizaci procesu přiřazena týmu SAP access management. Stávající role byly rozšířené o specifické odpovědnosti role manažer pro řízení přístupu ke službě definované v Tabulce 18 (kapitola 7.2).

Proces ***CMT4: Řízení nasazení služby cloud computingu do produktivního provozu*** byl aplikován. Realizace přechodu aplikační služby cloud computingu do produktivního provozu byla provedena podle připraveného plánu přechodu. Protože v tomto případě se nejednalo o přechod na aplikaci s vysokou úrovní kritičnosti pro byznys, nebylo potřeba provést odstavení žádného produktivního systému. Na příslušných síťových prvcích organizace byly upraveny pravidla tak, aby umožňovala přístup k nové aplikační službě cloud computingu. Bylo provedeno propojení mezi exitující aplikací human capital management a novou aplikační službou cloud computingu. Toto propojení umožnilo online přenosy dat z human capital management aplikace do aplikační služby cloud computingu. V interní aplikaci identity managementu byla vytvořena definice nové aplikace SAP a uživatelé ze skupin definovaných procesem CMT3: Řízení přístupu uživatele ke službě cloud computingu byli k této nové aplikační službě přiřazeni. Data vygenerovaná identity managementem byla odeslána do systému centrální správy uživatelů SAP. V systému centrální správy uživatelů SAP byla vytvořena definice nové aplikační služby SAP. Na základě dat z identity managementu byly k nové aplikační službě SAP vytvořeny definice uživatelských účtů. Pro jednotlivé skupiny uživatelů nové aplikace byly vygenerovány profily oprávnění. Po propojení systému centrální správy uživatelů SAP s novou aplikační službou, byla do nové aplikační služby odeslána data pro vytvoření nových uživatelů a jejich profilu oprávnění. Na základě těchto dat byly v nové aplikační službě vytvořeny uživatelské účty a aktivovány jejich profily oprávnění. Samotné profily oprávnění byly do produktivní verze aplikační služby cloud computingu přeneseny z testovací verze služby. Uživatelé ze skupin technických administrátorů a aplikačních administrátorů provedli dle plánu akceptační testy funkčnosti služby. Po vyhodnocení akceptačních testů bylo rozhodnuto o zařazení nové služby cloud computingu do produktivního provozu. V prvních dnech provozu služby byly řešeny následující incidenty:

- služba je pro jednotlivé uživatele nebo skupinu uživatelů nedostupná,
- přístup ke službě je pro jednotlivé uživatele odepřen,
- uživatel nebo skupina uživatelů nemá přidělená požadovaná oprávnění,
- funkcionalita poskytovaná službou nefunguje očekávaným způsobem,
- nedostatečná kapacita služby vzhledem k paralelně přihlášeným uživatelům,
- nedostatečná výkonnost služby.

Monitorovací funkcionality realizované uvnitř nové aplikační služby cloud computingu byly poskytovatelem nastaveny dle ustanovení SLA. Současně byl poskytovatelem uvolněn přístup pro interní monitorovací systém organizace umožňující pravidelně se opakující načtení v SLA dohodnutých monitorovacích údajů do interního monitorovacího systému spotřebitele. Zároveň v interním monitorovacím systému byly nastaveny hodnoty metrik a parametrů dle SLA. Monitoring nové služby cloud computingu byl uveden do stavu produktivního provozu. Po prvních dvou týden provozu byla nová aplikační služba cloud computingu plně zahrnuta do systému řízení provozu IT služeb organizace jako produktivní služba. Žádné činnosti pro řízení exit strategie nebyly aktivovány, neboť plán řízení exit strategie této služby žádné činnosti během provozu služby neobsahuje.

Odpovědnost za realizaci procesu byla přiřazena oddělení IT projekt managementu, pod jehož kompetence spadá plánování a vedení projektů, koordinace projektů, technické vedení projektů, návrh architektury řešení a konzultační činnosti. Stávající role byly rozšířené o specifické odpovědnosti role manažer nasazení služeb cloud computingu definované v Tabulce 18 (kapitola 7.2).

8.4.4 Provoz služby cloud computingu

Tabulka 37 uvádí vyhodnocení procesů fáze (CM4) Provoz služeb cloud computingu.

Tabulka 37: Vyhodnocení procesů fáze (CM4) Provoz služeb cloud computingu, zdroj: (autor)

Číslo	Proces	Využití procesu
CMO1	Řízení událostí	Aplikován
CMO2	Řízení incidentů	Aplikován
CMO3	Řízení problémů	Aplikován
CMO4	Řízení požadavků na službu cloud computingu	Aplikován
CMO5	Řízení požadavků na přístup ke službě cloud computingu	Aplikován
CMO6	Monitorování provozu služby cloud computingu	Aplikován

Tabulka 38 uvádí vyhodnocení rolí fáze (CM4) Provoz služeb cloud computingu ve vztahu k jednotlivým procesům.

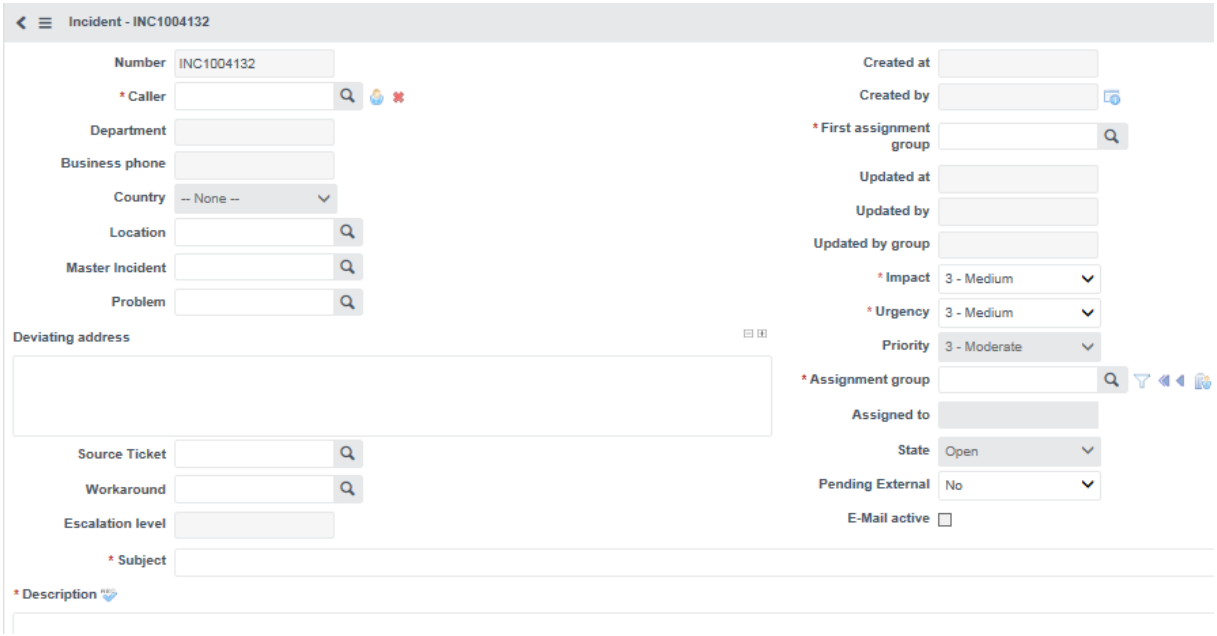
Tabulka 38: Vyhodnocení rolí ve vztahu k procesům fáze (CM4) Provoz služeb cloud computingu, zdroj: (autor)

Číslo procesu	Role	Využití role
	Cloud servis desk manažer	Rozšíření stávajících rolí
	Cloud eskalační manažer	Rozšíření stávající role
CMO1	Manažer provozu služeb cloud computingu	Rozšíření stávajících rolí
CMO2	Cloud incident manažer	Rozšíření stávající role
CMO3	Cloud problém manažer	Rozšíření stávající role
CMO4	Manažer řízení požadavků na službu cloud computingu	Rozšíření stávající role
CMO5	Manažer řízení požadavků na přístup ke službě cloud computingu	Rozšíření stávající role
CMO6	Cloud monitoring manažer	Rozšíření stávající role

Proces ***CMO1: Řízení událostí*** byl aplikován. Příručka organizace pro řízení událostí byla rozšířena o proceduru detekce a vyhodnocování událostí vznikajících v souvislosti s provozem služby cloud computingu. Toto rozšíření nebylo koncipováno pouze pro účely této nové aplikační služby cloud computingu, ale obecně pro novou třídu IT služeb. Definice procesu řízení událostí pro událost typu výjimka byla rozšířena o nové větvení postupu, kde podmínka vyhodnocuje, zda příčina vzniku události je na straně poskytovatele nebo spotřebitele. Nově byl do definice procesu doplněn postup pro řízení událostí v případě, že příčina vzniku události typu výjimka je na straně poskytovatele služby cloud computingu. Bylo definováno, že pracoviště, které provedlo vyhodnocení události, vytvoří v interním systému ITSM incident ke službě cloud computingu.

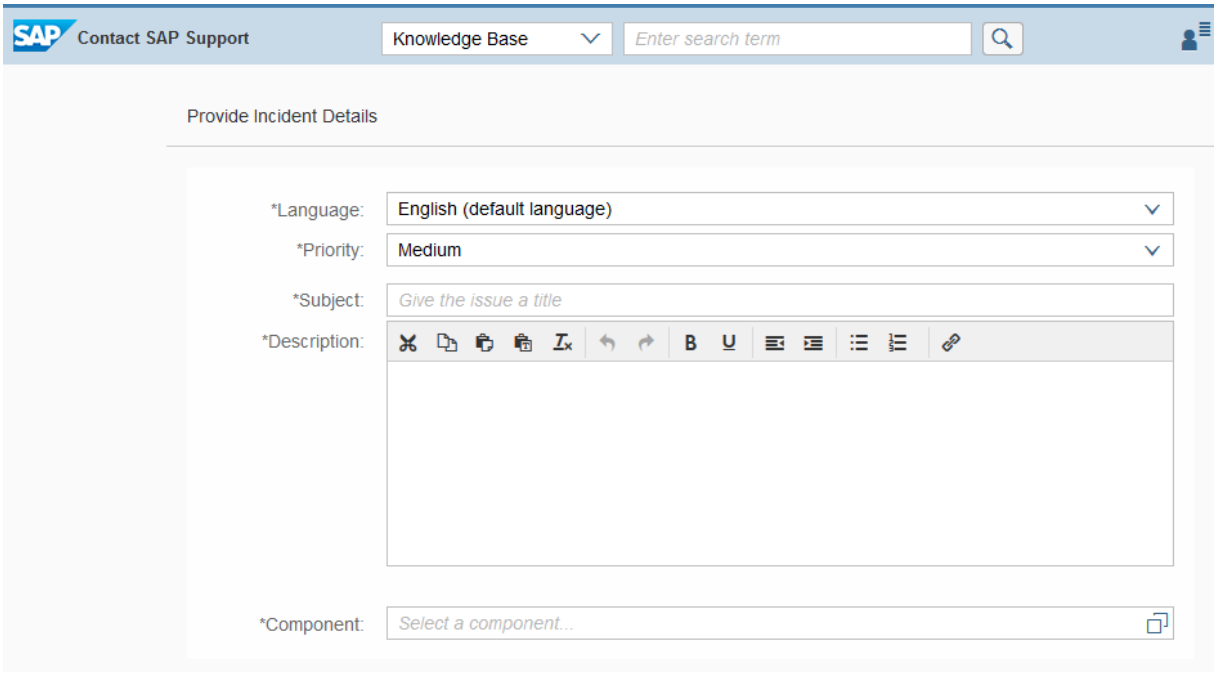
Odpovědnost za realizaci procesu byla přiřazena oddělení řízení provozu IT, pod jehož kompetence spadá kontrola a dohled nad provozem informačních systémů s využitím aktuálních výstupů z monitorování, řízení událostí a incidentů, změnové řízení, řízení přístupu a podpora eskalačního procesu a help desk IT infrastruktury. Stávající role IT Operation Manager byla rozšířená o specifické odpovědnosti role manažer provozu služeb cloud computingu definované v Tabulce 18 (kapitola 7.2).

Proces ***CMO2: Řízení incidentů*** byl aplikován. Příručka organizace pro řízení incidentů byla rozšířena o proceduru řízení životního cyklu incidentů služby cloud computingu. Pro incidenty ke službě cloud computingu vytvořené v interním systému ITSM (viz Obrázek 24) je realizována prvotní analýza příčin výskytu incidentů s cílem určit, zda příčina narušení služby cloud computingu je na straně spotřebitele nebo poskytovatele této služby.



Obrázek 24: Vytvoření nového incidentu v ITSM systému, zdroj: (interní ITSM systém IT organizace)

V případě, že příčina narušení služby cloud computingu je na straně poskytovatele, pracoviště, které realizovalo prvotní analýzu příčin výskytu incidentu, provede eskalaci na stranu poskytovatele služby cloud computingu. Eskalace je prováděna způsobem domluveným ve smlouvě s poskytovatelem služby. V tomto konkrétním případě, je vytvořen incident v systému řízení incidentů společnosti SAP určeném pro zákazníky využívající některou z poskytovaných služeb cloud computingu, ke kterému je přistupováno pomocí webového prohlížeče (viz Obrázek 25). Nejprve je nutné provést specifikaci systému, o který se jedná a následně je možné specifikovat incident včetně nastavení priority jako velmi vysoká, vysoká, střední, nízká.



Obrázek 25: Systém řízení incidentů společnosti SAP, zdroj: (interní systém SAP)

Incident ke službě cloud computingu vytvořený v interním systému ITSM je označen příznakem, že byla provedena jeho eskalace poskytovateli a čeká na informaci od poskytovatele o obnovení dodávky

služby ve stavu před jejím narušením. Informace o stavu incidentu je uložená v action logu. Po přijetí této informace je incident ke službě cloud computingu v interním systému ITSM doplněn o údaje dokumentující průběh řešení incidentu poskytovatelem služby a o údaje souvisejícími s odchylkami od SLA nebo jiných smluvních ujednání s poskytovatelem služby cloud computingu. Zároveň jsou zdokumentovány následky výskytu incidentu na byznys. Typy incidentů, které se vyskytly během produktivního provozu služby cloud computingu jsou:

- služba je nedostupná z důvodů na straně poskytovatele služeb cloud computingu,
- služba je nedostupná z důvodů na straně spotřebitele služeb cloud computingu,
- služba je pro jednotlivé uživatele nebo skupinu uživatelů nedostupná,
- přístup ke službě je pro jednotlivé uživatele odepřen,
- uživatel nebo skupina uživatelů nemá přidělená požadovaná oprávnění,
- funkcionalita poskytovaná službou nefunguje očekávaným způsobem,
- nedostatečná kapacita služby vzhledem k paralelně přihlášeným uživatelům,
- nedostatečná výkonnost služby.

Odpovědnost za realizaci procesu byla přiřazena oddělení řízení provozu IT, pod jehož kompetence spadá kontrola a dohled nad provozem informačních systémů s využitím aktuálních výstupů z monitorování, řízení událostí a incidentů, změnové řízení, řízení přístupu a podpora eskalačního procesu a help desk IT infrastruktury. Stávající role Incident Manager byla rozšířená o specifické odpovědnosti role cloud incident manažer definované v Tabulce 18 (kapitola 7.2).

Proces ***CMO3: Řízení problémů*** byl aplikován. Příručka organizace pro řízení problémů byla rozšířena o proceduru řízení životního cyklu problémů souvisejících se službou cloud computingu. Bylo definováno, že problémy jsou vytvářeny pro incidenty související se službou cloud computingu, je-li příčina vzniku incidentu na straně spotřebitele služby nebo funkcionalita poskytovaná službou nefunguje očekávaným způsobem nebo výkonnost služby není dostatečná. To znamená, že problémy související s využíváním služeb cloud computingu jsou řízeny stávajícím postupem.

Odpovědnost za realizaci procesu byla přiřazena oddělení řízení provozu IT, pod jehož kompetence spadá kontrola a dohled nad provozem informačních systémů s využitím aktuálních výstupů z monitorování, řízení událostí a incidentů, změnové řízení, řízení přístupu a podpora eskalačního procesu a help desk IT infrastruktury. Stávající role Problem Manager byla rozšířená o specifické odpovědnosti role cloud problém manažer definované v Tabulce 18 (kapitola 7.2).

Proces ***CMO4: Řízení požadavků na službu cloud computingu*** byl aplikován. Pro realizaci tohoto procesu bylo provedeno rozšíření seznamu standardních požadavků. K tomuto seznamu byl připojen seznam standardních požadavků pro novou aplikační službu cloud computingu. Toto rozšíření seznamu se týká pouze nové aplikační služby SAP. Pro definici položek seznamu byly využity smluvní ustanovení s poskytovatelem služby, které definují, jaké změny v nastavení parametrů služby může organizace realizovat vlastními silami. Konkrétně pro tuto novou aplikační službu byl seznam standardních požadavků definován pro transakce, které se týkají zejména nastavení aplikační služby pro realizaci komunikace mezi službou cloud computingu a interními systémy organizace. Seznam standardních požadavků popisuje Tabulka 39. Bylo rozhodnuto, že ke všem požadavkům na službu cloud computingu musí být vytvořen požadavek na změnu, který musí být před realizací schválen interním IT poradním výborem pro změny (IT Change Advisory Boad – CAB). Pokud přijatý požadavek na službu cloud computingu obsahuje požadavek jiný než ze seznamu standardních požadavků, je takovýto požadavek zamítnut.

Tabulka 39: Seznam standardních požadavků a kódy souvisejících transakcí SAP, zdroj: (autor), podle: (interní systém SAP)

Standardní požadavek	Název transakce SAP
Založení, úprava nebo vymazání definice logického systému	BD54
Založení, úprava nebo vymazání definice výstupního zařízení pro Application Linking and Embedding (ALE) komunikaci	SM59
Založení, úprava nebo vymazání portů Application Linking and Embedding (ALE) komunikace	WE21
Založení, úprava nebo vymazání partnerských dohod pro Application Linking and Embedding (ALE) komunikaci	WE20
Vytvoření a úprava distribučního modelu Application Linking and Embedding (ALE) komunikace	BD64
Údržba nastavení pro komunikaci email a SMS	SCOT
Údržba globálního nastavení modifikovatelnosti systému	SE06
Údržba nastavení modifikovatelnosti klienta	SCC4

Odpovědnost za realizaci procesu byla přiřazena oddělení řízení provozu IT, pod jehož kompetence spadá kontrola a dohled nad provozem informačních systémů s využitím aktuálních výstupů z monitorování, řízení událostí a incidentů, změnové řízení, řízení přístupu a podpora eskalačního procesu a help desk IT infrastruktury. Stávající role byly rozšířené o specifické odpovědnosti role manažer řízení požadavků na službu cloud computingu definované v Tabulce 18 (kapitola 7.2).

Proces ***CMO5: Řízení požadavků na přístup ke službě cloud computingu*** byl aplikován. Pro novou službu cloud computingu byl vypracován dodatek příručky pro řízení požadavků na přístup ke službě, která definuje skupiny uživatelů aplikační služby cloud computingu a profily oprávnění přiřazené ke každé z těchto skupin. Požadavek na přístup ke službě cloud computingu je validován z hlediska přiřazení uživatele ke správné skupině uživatelů. Pokud požadavek splňuje i ostatní formální kritéria, je realizován tím způsobem, že uživateli jsou přiřazena oprávnění definovaná pro danou skupinu uživatelů. V opačném případě je požadavek na přístup ke službě cloud computingu zamítnut.

Odpovědnost za realizaci procesu byla přiřazena oddělení řízení provozu IT, pod jehož kompetence spadá kontrola a dohled nad provozem informačních systémů s využitím aktuálních výstupů z monitorování, řízení událostí a incidentů, změnové řízení, řízení přístupu a podpora eskalačního procesu a help desk IT infrastruktury. Stávající role Access Manager byla rozšířená o specifické odpovědnosti role manažer řízení požadavků na přístup ke službě cloud computingu definované v Tabulce 18 (kapitola 7.2).

Proces ***CMO6: Monitorování provozu služby cloud computingu*** byl aplikován. Monitorování provozu nové služby cloud computingu bylo rozděleno na dvě části, automatizované monitorování provozu služby a ruční sběr dat o provozu služby. Příručka pro automatizované monitorování provozu IT služby byla rozšířena o monitorování hodnot metrik a parametrů nové služby cloud computingu dle ustanovení SLA, které umožňuje existující interní centrální monitorovací systém provádět automatizovaně. Dále byla příručka rozšířena o definici ručního sběru dat o provozu služby cloud computingu, která je prováděna jednou denně technickými administrátory. Hodnoty získané ručním sběrem jsou ukládány do pro tento účel definovaných souborů. Ručním způsobem je prováděn sběr dat zejména o výkonnosti služby cloud computingu.

Odpovědnost za realizaci procesu byla přiřazena týmu Monitoring, pod jehož kompetence spadá realizace sběru dat o provozu informačních systémů. Stávající role byly rozšířené o specifické odpovědnosti role cloud monitoring manažer definované v Tabulce 18 (kapitola 7.2).

8.4.5 Nepřetržité zdokonalování služby cloud computingu

Tabulka 40 uvádí vyhodnocení procesu fáze (CM5) Nepřetržité zdokonalování služby cloud computingu.

Tabulka 40: Vyhodnocení procesů fáze (CM5) Nepřetržité zdokonalování služby cloud computingu, zdroj: (autor)

Číslo	Proces	Využití procesu
CMI1	Řízení nepřetržitého zdokonalování služby cloud computingu	Aplikován částečně

Tabulka 41 uvádí vyhodnocení role fáze (CM5) Nepřetržité zdokonalování služby cloud computingu ve vztahu k procesu.

Tabulka 41: Vyhodnocení role ve vztahu k procesu fáze (CM5) Nepřetržité zdokonalování služby cloud computingu, zdroj: (autor)

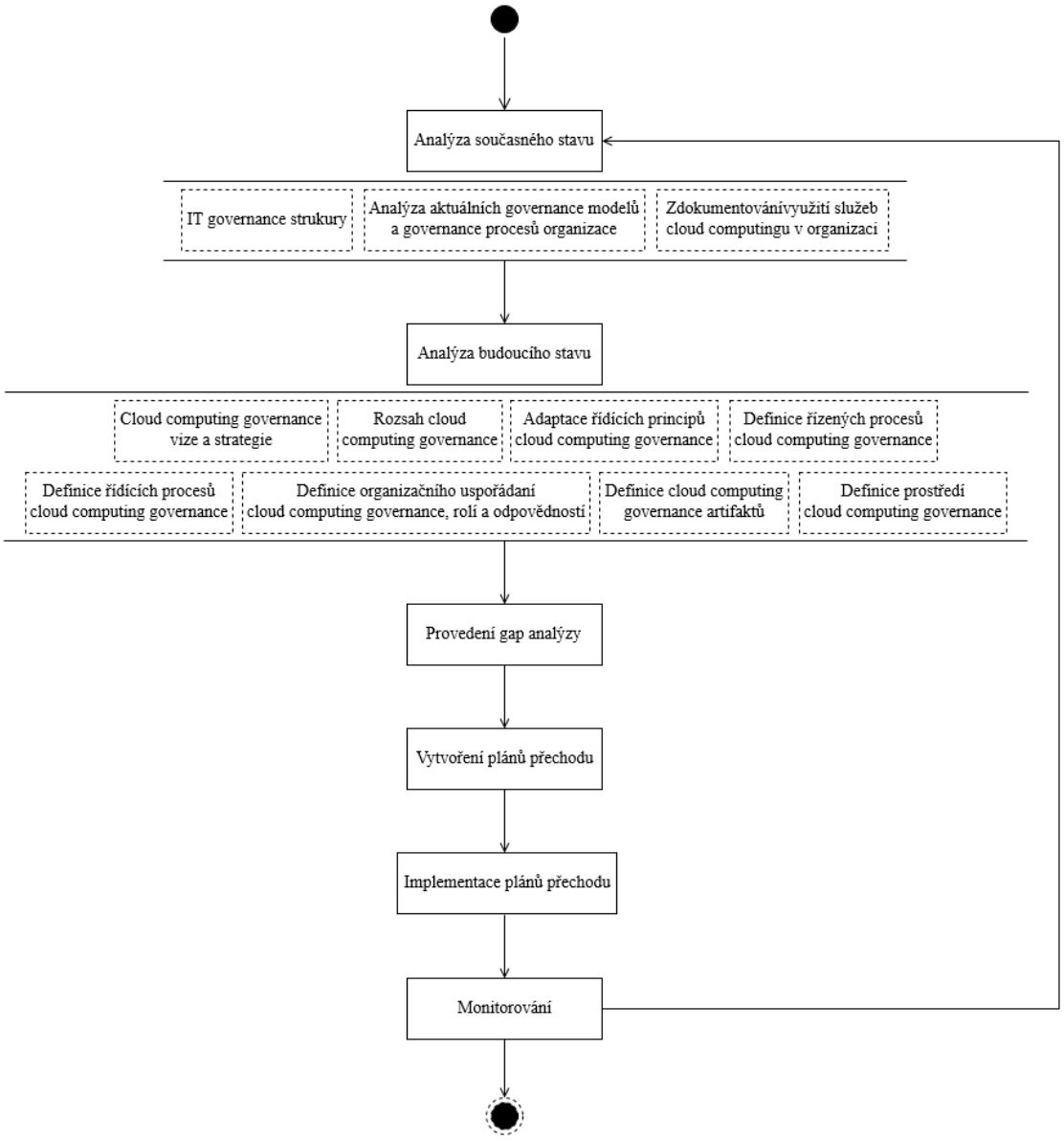
Číslo procesu	Role	Využití role
CMS1	Manažer nepřetržitého zdokonalování služby cloud computingu	Rozšíření stávajících rolí

Proces ***CMI1: Řízení nepřetržitého zdokonalování služby cloud computingu*** byl aplikován částečně. Ve smlouvě s poskytovatelem bylo dohodnuto, že poskytovatel bude provádět pravidelné aktualizace programového vybavení služby cloud computingu jako součást dodávky služby cloud computingu. O přechodu k jinému poskytovateli nebo o přechodu k poskytování služby vlastním IT se v době realizace této případové studie neuvažovalo. Sběr dat o provozu služby cloud computingu za účelem zdokonalování služby cloud computingu byl prováděn ručním způsobem. Z periodicky prováděných analýz dat ze sběru dat o provozu služby cloud computingu žádné požadavky na změny v dodávané službě cloud computingu nevyplynuly. Procesní aktivity CMI1.7: Návrh na změnu v dodávané službě cloud computingu, CMI1.8: Verifikace návrhu zainteresovanými stranami a CMI1.9: Realizace změny dodávané služby cloud computingu nebyly provedeny.

Odpovědnost za realizaci procesu byla přiřazena týmu IT služby, která má na starost řízení IT služeb. Stávající role IT Service Manager byla rozšířená o specifické odpovědnosti role manažer nepřetržitého zdokonalování služby cloud computingu definované v Tabulce 18 (kapitola 7.2).

8.4.6 Aplikace modelu cloud computing governance

Vzhledem k tomu, že životní cyklus cloud computing governance je iterativní proces a že do realizace této případové studie nebyla ve společnosti využívána žádná služba cloud computingu, byl navržen implementační proces modelu cloud computing governance znázorněný na Obrázku 26.



Obrázek 26: Implementační proces modelu cloud computing governance, zdroj: (autor)

Analýza současného stavu je zaměřena na analýzu stávajících IT governance struktur, analýzu aktuálních governance modelů a governance procesů organizace a na zdokumentování využití služeb cloud computingu v organizaci. V organizační struktuře IT organizace se nachází oddělení IT Governance, které má jednoho odpovědného vedoucího pracovníka. IT governance má na starosti definici, prosazování, řízení, optimalizaci a harmonizaci IT procesů, definici procesních metrik, koordinaci, komunikaci a školení IT personálu vzhledem k IT procesům, vedení a správu procesní dokumentace a udržování IT governance příručky. IT governance má jednoho vedoucího týmu a pět jemu podřízených pracovníků. Model IT governance je v IT organizaci vybudován na doporučeních metodiky ITIL, kdy implementace ITIL je na relativně rozvinuté úrovni. Cloud computing governance model nebyl do této doby implementován, z hlediska jeho zralosti se jedná o nultou úroveň, kdy procesy cloud computing governance nejsou definovány ani prováděny. V IT organizaci nebyly doposud využívané služby cloud computingu, tudíž ani nebyla rozpoznána potřeba cloud computing governance.

Analýza budoucího stavu je zaměřena na definici cloud computing governance vize a strategie, stanovení rozsahu cloud computing governance, adaptaci řídících principů cloud computing

governance, definici procesů, organizačního uspořádání, rolí a odpovědností, definici cloud computing governance artefaktů a definici umožňujícího prostředí cloud computing governance. Vizí IT organizace je plně implementovat model cloud computing governance a v případě úspěšnosti tohoto projektu, rozšířit v budoucnu portfolio služeb cloud computingu na služby Office 365, Sharepoint Online a další služby cloud computingu poskytované společností Microsoft. Rozsah cloud computing governance koresponduje s navrženým metodickým rámcem CCGM. Referenční model cloud computing governance byl implementovaný v celém svém rozsahu. Plánování modelu cloud computing governance vychází z řídících principů cloud computing governance, které byly plně převzaty. Tabulka 42 uvádí vyhodnocení řídících principů cloud computing governance z hlediska jejich míry využití při realizaci případové studie.

Tabulka 42: Vyhodnocení řídících principů cloud computing governance, zdroj: (autor)

Číslo	Název řídícího principu	Využití
ŘPG1	Cloud computing strategie musí být v souladu s byznys strategií a musí být podporována výkonným vedením.	Aplikován
ŘPG2	Cloud computing governance musí být v souladu s podnikovou governance a IT governance a musí být podporována výkonným vedením.	Aplikován
ŘPG3	Využití služeb cloud computingu musí přinášet hodnotu zainteresovaným stranám.	Aplikován
ŘPG4	Rizika související s využíváním služeb cloud computingu musí být kontinuálně optimalizovaná.	Aplikován
ŘPG5	Využívání služeb cloud computingu musí být v souladu s legislativními, regulatorními a dalšími oborovými požadavky.	Aplikován
ŘPG6	Náklady na využívání služeb cloud computingu musí být kontinuálně optimalizované.	Aplikován
ŘPG7	Politiky cloud computing governance při využívání služeb v prostředí cloud computingu musí být komunikovány a musí být dostupné příslušným zainteresovaným stranám.	Aplikován
ŘPG8	Účinnost, výkonnost implementovaného cloud computing governance modelu musí být monitorována a musí být vyhodnocována shoda s definovanými governance principy.	Aplikován
ŘPG9	Pro efektivní podporu implementace a provozu cloud computing governance musí být dostupné potřebné umožňující schopnosti a prostředí.	Aplikován

Tabulka 43 uvádí vyhodnocení řízených procesů cloud computing governance z hlediska jejich míry využití při realizaci případové studie.

Tabulka 43: Vyhodnocení řízených procesů cloud computing governance, zdroj: (autor)

Číslo	Proces	Využití procesu
GP1	Zajištění systému cloud computing governance	Aplikován
GP2	Realizace přínosů z využívání služeb cloud computingu	Aplikován
GP3	Zajištění systému řízení rizik z využívání služeb cloud computingu	Aplikován
GP4	Zajištění systému řízení souladu s interními standardy a normami, s legislativními a regulatorními předpisy a smluvními požadavky	Aplikován
GP5	Zajištění systému monitorování a reportingu využívání služeb cloud computingu	Aplikován
GP6	Zajištění optimalizace výběru služeb cloud computingu	Aplikován

Proces ***GP1: Zajištění systému cloud computing governance*** byl aplikován. Oddělení IT governance má na starosti definici politik, zásad a pravidel týkající se provozování a poskytování IT služeb v souladu s IT strategií vycházející z potřeb byznysu a zajišťuje, že potřebné IT procesy pro realizaci této strategie jsou implementovány a korektně dodržovány. Byly provedena analýza dopadu využívání služeb cloud computingu na byznys, v součinnosti s vedením IT organizace byla odsouhlasena

implementace modelu cloud computing governance včetně všech navržených procesů a rozšíření odpovědnosti a pravomocí pracovníků oddělení IT governance, byly aplikovány řídící principy při rozšíření stávajícího IT governance modelu o cloud computing governance, došlo k modifikaci vybraných stávajících politik a k formulaci nových politik, které byly komunikovány zainteresovaným stranám, stávajícím rolím byly modifikovány odpovědnosti a rozšířena jejich odpovědnost v rámci rozhodovacího procesu o službách cloud computingu, bylo realizováno školení pro IT personál s cílem pochopit využití služeb cloud computingu v IT organizaci a souvisejících pravidel a omezení. Oddělení IT governance rozšířilo svou odpovědnost o řízení cloud computing governance procesů, posuzování jejich účinnosti a identifikaci opatření při zjištění odchylek jejich průběhu.

Proces ***GP2: Realizace přínosů z využívání služeb cloud computingu*** byl aplikován. Oddělení IT governance v součinnosti s oddělením IT office definovalo mechanismy a principy pro stanovení a hodnocení přínosů z využití služeb cloud computingu v souladu s byznys strategií. Jedná se o subjektivně pozorovatelné přínosy z využívání služeb cloud computingu, přínosy vyplývající z pilotní implementace služby cloud computingu, přínosy měřené pomocí metrik KPI a KGI a přínosy měřené pomocí ukazatelů ekonomické efektivnosti využívání služeb cloud computingu. Oddělení IT office definovalo schéma pro hodnocení finančních přínosů z využívání služby cloud computingu, definovalo stínové ceny pro finanční vyjádření nepřímých přínosů, metody pro hodnocení nákladů a metody pro hodnocení efektivnosti vynaložených nákladů na využívání služby cloud computingu. Oddělení IT office rozšířilo svou odpovědnost o dohled nad stanovením a periodickým vyhodnocováním přínosů z využití služeb cloud computingu.

Proces ***GP3: Zajištění systému řízení rizik z využívání služeb cloud computingu*** byl aplikován. Vedoucí týmu řízení IT rizik, který je zodpovědný za dodržování strategie řízení IT rizik, jejíž součástí je definovaná politika řízení IT rizik odrážející rizikový profil organizace, se v součinnosti s vedením IT organizace podílel na formulaci míry přijatelného rizika z využívání služeb cloud computingu, kterou je podnik ochoten přijmout a aktualizoval politiku řízení IT rizik se zohledněním rizik vyplývajících z využívání služeb cloud computingu. Současně je vedoucí týmu odpovědný za aktualizaci stávajícího řízení IT rizik vzhledem k rizikům vyplývajících z využívání služeb cloud computingu, za realizaci procesu řízení rizik z využití služeb cloud computingu a za plnění jednotlivých funkcí v rámci tohoto procesu a soustřeďuje informace jak primárně z týmu řízení IT rizik, ale také z ostatních útvarů IT organizace, které mohou mít podstatný vliv na řízení rizik vyplývajících z využití služeb cloud computingu.

Proces ***GP4: Zajištění systému řízení souladu s interními standardy a normami, s legislativními a regulatorními předpisy a smluvními požadavky*** byl aplikován. Byl aktualizován Security & Compliance Framework (SCF) IT organizace, jehož rozvoj má na starosti oddělení IT compliance. Byla provedena analýza interních standardů a norem, legislativních, regulativních a smluvních požadavků ovlivňujících návrh a prosazování cloud computing governance. Bylo provedeno školení IT personálu tak, aby se zaměstnanci byli schopni řídit příslušnými pokyny a aby jim byly známy důsledky nesouladu s interními standardy a normami, s legislativními a regulatorními předpisy a smluvními požadavky. Tým IT compliance rozšířil svou odpovědnost o dohled nad dodržováním legislativních a smluvních povinností vyplývajících z využívání služeb cloud computingu.

Proces ***GP5: Zajištění systému monitorování a reportingu využívání služeb cloud computingu*** byl aplikován. Tým IT governance analyzoval interní standardy a normy, legislativní, regulativní a smluvní požadavky na monitorování a podávání zpráv týkajících se využívání služeb cloud computingu a určil rozsah rozšíření implementovaného systému monitorování a reportingu stávajících IT služeb. Byla aktualizována komunikační strategie obsahující politiku pro řízení komunikace

s interními a externími zainteresovanými stranami včetně definice komunikačních kanálů a komunikačních formátů.

Proces ***GP6: Zajištění optimalizace výběru služeb cloud computingu*** byl aplikován. Oddělení IT governance definovalo zásady výběru služeb cloud computingu, aby byly dostupné služby cloud computingu vzhledem k aktuálním a budoucím potřebám byznysu v souladu s rozpočtovým omezením definovaným oddělením IT office. Oddělení IT architektury definovalo zásady pro řízení a kontroly architektury služeb cloud computingu a aktualizovalo strategickou koncepci architektury IT služeb. Dále bylo realizováno technické posouzení využívání služeb cloud computingu.

Tabulka 44 uvádí vyhodnocení řídících procesů cloud computing governance z hlediska jejich míry využití při realizaci případové studie.

Tabulka 44: Vyhodnocení řídících procesů cloud computing governance, zdroj: (autor)

Číslo	Proces	Využití procesu
GaP1	Řízení shody	Aplikován
GaP2	Řízení výjimek	Aplikován
GaP3	Řízení komunikace	Aplikován

Za aplikaci řídících procesů cloud computing governance je odpovědné oddělení IT governance. Oddělení IT governance definovalo procesní metriky a kontrolní body pro hodnocení shody řízených procesů s politikami a pravidly cloud computing governance, byl definován postup řešení neshody, byla definována pravidla řízení výjimek a pravidla pro jejich eskalaci vedoucímu pracovníkovi oddělení IT Governance. Oddělení IT governance zabezpečilo realizaci školení IT pracovníků z hlediska pochopení významu cloud computing governance a definice souvisejících proces a školení týkající se změn governance politik ovlivňujících využívání služeb cloud computingu. Příslušným rolím byly komunikovány nové pravomoci a odpovědnosti vzhledem k systému cloud computing governance.

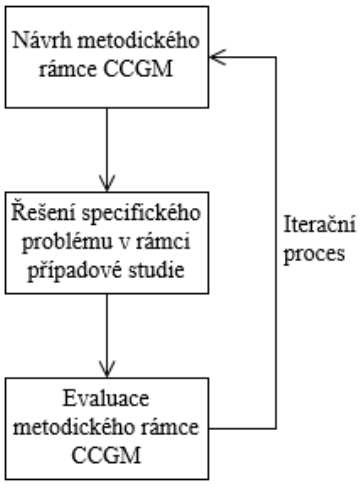
Vedení IT organizace rozšířilo svoje kompetence na oblast koordinace a plánování cloud computing cílů v souladu s byznys cíli a IT strategie zohledňující využívání služeb cloud computingu. Dále vedení rozhoduje o tom, pro které byznys procesy je akceptovatelná jejich podpora službou cloud computingu a schvaluje investice do využití služeb cloud computingu. IT pracovníkům z oddělení IT governance, IT architektury a IT compliance byly rozšířeny odpovědnosti definované v Tabulce 13 v kapitole 6.1.4 specifické pro strukturu Cloud Computing Governance Řídící Skupina. Odpovědnosti struktury Cloud Computing Governance Vývojový Tým a Provoz Cloud Computing Governance byly přidělené oddělení IT governance.

IT organizace využívá systém pro správu dokumentů (DMS), ve kterém byla vytvořena nová složka pro správu cloud computing governance artefaktů, která je sdílená mezi zaměstnanci IT organizace.

8.5 Závěry případové studie

Na základě průběhu a výsledků případové studie byla ověřena praktická využitelnost navrženého metodického rámce CCGM v reálném prostředí IT organizace, která aplikovala navržený metodický rámec CCGM v rámci pilotního projektu adopce služby cloud computingu. Pomocí aplikace navržených procesů pro řízení životního cyklu služby cloud computingu byl provedeno plánování výběru, hodnocení a výběr služby cloud computingu, plánování implementace a nasazení vybrané služby do provozního prostředí IT organizace a byl řízen její operativní provoz v souladu s potřebami byznys procesů a s požadavky vyplývajícími z SLA. Kromě adopce služby cloud computingu byl upraven stávající model ITSM pro řízení životního cyklu IT služeb pro prostředí využívání služeb cloud computingu na základě cloud computing managementu navrženého metodického rámce CCGM. Dále byla provedena adaptace modelu IT management a modelu IT governance v rámci implementačního procesu definovaného v kapitole 8.4.6. Pomocí governance a managementu služeb cloud computingu bylo dosažené optimální využití služby cloud computingu v souladu s byznys potřebami, potřebami podpory vybraného byznys procesu a potřebami spolehlivé a nákladově efektivní IT služby.

Jelikož byl artefakt metodický rámec CCGM vytvářen v souladu s vědeckou metodou Design Science Research Methodology (Peffers, a další, 2008), je návrh a tvorba tohoto artefaktu iterativním procesem, v rámci kterého využití navrženého metodického rámce CCGM v reálném prostředí v rámci této případové studie a jeho evaluace při řešení specifického problému podpory byznys procesu řízení přijímacího řízení nových zaměstnanců službou cloud computingu zpětně ovlivňuje návrh metodického rámce CCGM (viz Obrázek 27). Na základě zkušeností získaných při realizaci případové studie a doporučení vyplývajících z rozhovorů s odbornými IT pracovníky organizace byl v rámci jednotlivých iterací tvorby a návrhu artefaktu modifikován navržený metodický rámec CCGM do výsledné podoby popsané v kapitolách 5, 6 a 7.



Obrázek 27: Proces návrhu metodického rámce CCGM, zdroj: (autor)

V rámci prvního dílčího projektu adopce služby cloud computingu byl aplikován model cloud computing management metodického rámce CCGM. Vycházelo se z definice devíti řídících principů definovaných v kapitole 7.1, které zabezpečují podporu rozhodování při návrhu, nasazení a provozování cloud computing managementu. Tyto řídící principy zůstaly ve finální verzi oproti první verzi metodického rámce CCGM nezměněny. Seznam procesů a rolí cloud computing managementu finální verze navrženého metodického rámce CCGM koresponduje s první verzí návrhu. U vybraných procesů došlo k úpravě jejich obsahové náplně, tzn. k modifikaci popisu procesu a procesních aktivit z hlediska návrhu doporučení pro realizaci dané aktivity. U vybraných rolí byly

modifikovány základní odpovědnosti v souladu s potřebami identifikovanými během realizace případové studie. Seznam procesů a rolí cloud computing managementu finální verze navrženého metodického rámce CCGM a jejich stav oproti první verzi návrhu uvádí Tabulka 45.

Tabulka 45: Seznam stávajících a aktualizovaných procesů a rolí cloud computing managementu ve finální verzi navrženého metodického rámce CCGM, zdroj: (autor)

Fáze životního cyklu služby cloud computingu	Proces	Stav	Role	Stav
(CM1) Strategie využití služeb cloud computingu			Chief Information Officer	Nezměněn
			Cloud computing analytik	Nezměněn
	CMS1: Řízení rizik z využití služby cloud computingu	Změněn	Manažer řízení rizik cloud computingu	Změněn
	CMS2: Finanční řízení služeb cloud computingu	Změněn	Finanční manažer služeb cloud computingu	Změněn
	CMS3: Řízení souladu s interními standardy a normami, s legislativními a regulatorními předpisy a smluvními požadavky	Nezměněn	Manažer pro řízení souladu služeb cloud computingu s legislativou	Nezměněn
	CMS4: Řízení exit strategie	Nezměněn	Manažer cloud exit strategie	Nezměněn
	CMS5: Řízení portfolia poskytovatelů služeb cloud computingu	Změněn	Manažer portfolia poskytovatelů a řízení vztahu s poskytovateli	Nezměněn
	CMS6: Řízení portfolia služeb cloud computingu	Nezměněn	Manažer katalogu služeb cloud computingu	Nezměněn
	CMS7: Řízení smluv o poskytování služby cloud computingu	Změněn	Cloud SLA manažer	Nezměněn
(CM2) Výběr služby cloud computingu	CMD1: Řízení výběru služby cloud computingu	Nezměněn	Manažer služeb cloud computingu	Nezměněn
(CM3) Přechod na využívání služby cloud computingu	CMT1: Plánování přechodu na využívání služby cloud computingu	Změněn	Manažer přechodu na využití služby cloud computingu	Změněn
	CMT2: Testování a validace služby cloud computingu	Změněn	Cloud test manažer	Změněn
	CMT3: Řízení přístupu uživatele ke službě cloud computingu	Nezměněn	Manažer pro řízení přístupu ke službě	Nezměněn
	CMT4: Řízení nasazení služby cloud computingu do produktivního provozu	Změněn	Manažer nasazení služeb cloud computingu	Změněn
(CM4) Provoz			Cloud servis desk manažer	Nezměněn

Fáze životního cyklu služby cloud computingu	Proces	Stav	Role	Stav
služby cloud computingu			Cloud eskalační manažer	Změněn
	CMO1: Řízení událostí	Nezměněn	Manažer provozu služeb cloud computingu	Nezměněn
	CMO2: Řízení incidentů	Změněn	Cloud incident manažer	Nezměněn
	CMO3: Řízení problémů	Nezměněn	Cloud problém manažer	Nezměněn
	CMO4: Řízení požadavků na službu cloud computingu	Nezměněn	Manažer řízení požadavků na službu cloud computingu	Nezměněn
	CMO5: Řízení požadavků na přístup ke službě cloud computingu	Nezměněn	Manažer řízení požadavků na přístup ke službě cloud computingu	Nezměněn
	CMO6: Monitorování provozu služby cloud computingu	Nezměněn	Cloud monitoring manažer	Nezměněn
(CM5) Nepřetržité zdokonalování služby cloud computingu	CMI1: Řízení nepřetržitého zdokonalování služby cloud computingu	Nezměněn	Manažer nepřetržitého zdokonalování služby cloud computingu	Nezměněn

V rámci druhého dílčího projektu byla provedena aplikace modelu cloud computing management a modelu cloud computing governance metodického rámce CCGM. Aplikace modelu cloud computing governance byla provedena dle životního cyklu cloud computing governance definovaného v kapitole 6.2. V rámci procesu adaptace stávajícího modelu IT governance byl zjištěn nekorektní návrh řízených procesů cloud computing governance metodického rámce CCGM. Řízené procesy cloud computing governance navržené na základě analýzy dostupných a relevantních vědeckých publikací plně nekorespondovaly s reálnými potřebami z hlediska governance služeb cloud computingu z pohledu spotřebitele. Autorkou této doktorské disertační práce bylo vymazáno šest procesů, které řešily problémy specifické zejména pro management využívání služeb cloud computingu, byly definovány dva nové procesy pokrývající problematiku governance využívání služeb cloud computingu a ostatní řízené procesy cloud computing governance byly modifikovány s ohledem na průběh případové studie. Vyhodnocení a redefinice řízených procesů cloud computing governance realizovaná na základě případové studie je popsána v Tabulce 46. Řídící procesy cloud computing governance, řídící principy cloud computing governance a role cloud computing governance zůstaly nezměněné.

Tabulka 46: Změny řízených procesů při návrhu metodického rámce CCGM, zdroj: (autor)

Řízené procesy cloud computing governance první verze metodického rámce CCGM	Řízené procesy cloud computing governance finální verze metodického rámce CCGM
GP1: Zajištění systému cloud computing governance	Modifikace popisu procesu a procesních aktivit
GP2: Realizace přínosů z využívání služeb v prostředí cloud computingu	Modifikace popisu procesu a procesních aktivit
GP3: Řízení byznys procesů realizovaných	Proces vymazán

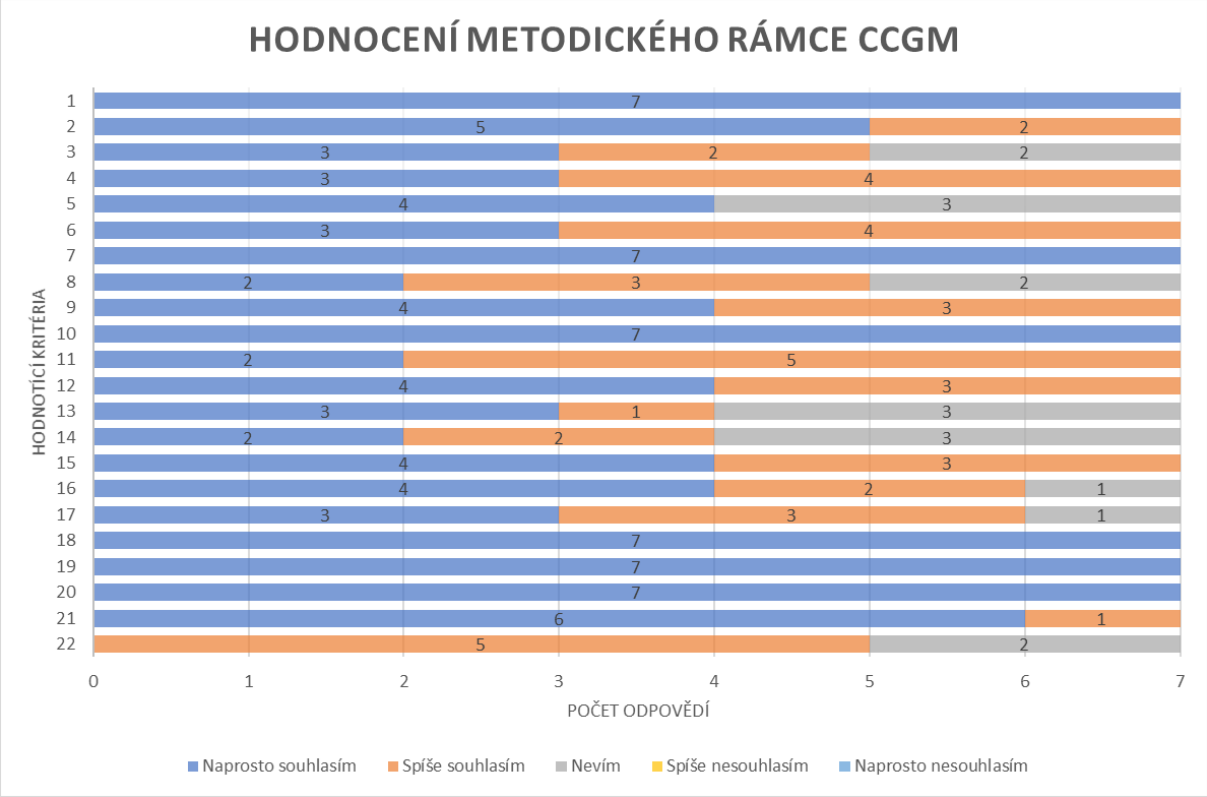
Řízené procesy cloud computing governance první verze metodického rámce CCGM	Řízené procesy cloud computing governance finální verze metodického rámce CCGM
prostřednictvím služeb cloud computingu	
GP4: Správa portfolia služeb cloud computingu	Proces vymazán
GP5: Řízení životního cyklu služeb cloud computingu	Proces vymazán
GP6: Správa portfolia cloud computing řešení	Proces vymazán
GP7: Řízení životního cyklu cloud computing řešení	Proces vymazán
GP8: Zajištění systému řízení rizik z využívání služeb v prostředí cloud computingu	Modifikace popisu procesu a procesních aktivit, nové označení procesu: GP3
GP9: Zajištění systému monitorování a reportingu využívání služeb v prostředí cloud computingu	Modifikace popisu procesu a procesních aktivit, nové označení procesu: GP4
GP10: Zajištění systému řízení poskytovatelů služeb cloud computingu	Proces vymazán
	Definice nového procesu: GP5: Zajištění systému řízení souladu s interními standardy a normami, s legislativními a regulatorními předpisy a smluvními požadavky
	Definice nového procesu: GP6: Zajištění optimalizace výběru služeb cloud computingu

Případová studie prokázala, že navržený metodický rámec CCGM umožnil netriviálním způsobem optimální výběr služby cloud computingu, služba byla otestovaná, byl naplánovaný její přechod na využívání, byla nasazena do produktivního provozu a je poskytovaná a využívaná v souladu s SLA. Pomocí rozhovorů se specializovanými IT pracovníky IT organizace byly posouzeny jednotlivé části navrženého metodického rámce CCGM a jeho praktická implementace. Cílem hodnocení metodického rámce CCGM odbornými IT pracovníky metodou rozhovorů bylo získat zpětnou vazbu k navrženému metodickému rámci CCGM a náměty na úpravu metodického rámce CCGM a ověřit správnost a úplnost koncepce metodik z hlediska metodických prvků (skupin principů, procesů a rolí). Po ukončení obou dílčích projektů byl vybraným odborným IT pracovníkům předložen dotazník. Jednalo se o sedm IT pracovníků zařazených na pracovní pozice Vedoucí oddělení IT governance, IT governance specialist, Procesní analytik, IT analytik, Vedoucí týmu IT služby, Vedoucí oddělení řízení provozu IT a Vedoucí týmu IT projekt management. Cílem dotazníku bylo zjistit správnost, úplnost a využitelnost navrženého metodického rámce CCGM. Odborným IT pracovníkům bylo prostřednictvím dotazníku předloženo 22 hodnotících kritérií. K měření postojů odborných IT pracovníků k hodnotícím kritériím byla využita pětistupňová Likertova škála, pomocí které odborný IT pracovník označil míra souhlasu s hodnotícím kritériem. Výsledky z dotazníkového šetření jsou uvedeny na Obrázku 28. Detailní výstupy z dotazníků jsou uvedeny v příloze B. Hodnotící kritéria jsou následující:

1. Metodický rámec CCGM je pochopitelný a implementovatelný.
2. Cíle, rozsah a struktura metodického rámce CCGM jsou jasně a srozumitelně definovány.
3. Metodické prvky (principy, procesy a role) metodického rámce CCGM jsou jasně, srozumitelně a korektně definovány.

4. Metodický rámec CCGM poskytuje potřebné metodiky umožňující zabezpečit efektivní adopci a využívání služby cloud computingu v souladu s byznys požadavky při minimalizaci nákladů a rizik.
5. Metodický rámec CCGM pokrývá aspekty governance služeb cloud computingu.
6. Metodický rámec CCGM pokrývá aspekty managementu služeb cloud computingu.
7. Metodický rámec CCGM poskytuje dostatečnou flexibilitu při návrhu governance a managementu služeb cloud computingu v organizaci.
8. Rozhraní mezi cloud computing governance a cloud computing management je jasně definováno.
9. Cloud computing governance napomáhá definovat rozhodovací proces, pravidla a omezení, které na strategické úrovni spravují a ovládají využívání služeb cloud computingu s cílem dosažení potřeb byznysu.
10. Cloud computing management pokrývá životní cyklus služby cloud computingu.
11. Cloud computing management umožňuje zabezpečit dodání požadovaného objemu služby při daných výkonnostních parametrech a při dané ceně v souladu se strategickými požadavky na službu.
12. Procesy metodického rámce CCGM umožňují řešení reálných problémů a umožňují dodání specifických výsledků řešení těchto problémů.
13. Procesy cloud computing governance jsou definovány korektně a na potřebné úrovni detailu.
14. Procesy cloud computing governance umožňují realizaci modelu governance služeb cloud computingu v konkrétním podniku a zahrnují praktiky a aktivity zaměřené na dosahování cílů IT governance, které určují směr využívání služeb cloud computingu, a umožňují monitorování výstupů.
15. Procesy cloud computing management jsou definovány korektně a na potřebné úrovni detailu.
16. Procesy fáze (CM1) Strategie využití služeb cloud computingu zabezpečují realizaci IT strategie prostřednictvím definice interních a externích požadavků, které musí služby cloud computingu splňovat při optimální úrovni nákladů a výši rizika, a dále zabezpečují vytvoření, udržování a ukončení smluvního vztahu s poskytovatelem služeb cloud computingu a vytvoření a udržování portfolia dostupných služeb cloud computingu splňujících potřeby byznysu a externích požadavků.
17. Proces fáze (CM2) Výběr služby cloud computingu zabezpečuje aktivity související s výběrem služby cloud computingu, která v optimální míře splňují požadavky vyplývající z předchozí fáze CM1 s důrazem na hodnotu pro byznys.
18. Procesy fáze (CM3) Přechod na využívání služby cloud computingu zabezpečují efektivní a účinné plánování nasazení služby cloud computingu o očekávané úrovni kvality do produktivního provozu při naplnění požadavků na službu vyplývajících z fází CM1 a CM2.
19. Procesy fáze (CM4) Provoz služby cloud computingu zabezpečují koordinaci a provádění aktivit potřebných pro sledování výkonnosti služeb cloud computingu, pro realizaci sběru provozních metrik používaných k hodnocení kvalitativní úrovně služeb a pro identifikaci odchylek hodnot metrik od požadovaného stavu, dále zabezpečují že přístup ke službám je umožněn pouze oprávněným uživatelům a že služba uspokojuje potřeby těchto uživatelů vzhledem k plnění jejich pracovního zařazení.
20. Proces fáze (CM5) Nepřetržité zdokonalování služby cloud computingu zabezpečuje, že využívaná služba cloud computingu bude neustále a optimálním způsobem podporovat realizaci byznys procesů, a to jak z hlediska její účinnosti, tak i nákladové efektivity a přijatelné míry rizika.
21. Metodický rámec CCGM jasně stanovuje role a odpovědnosti ve vztahu k procesům.

22. Metodický rámec CCGM umožňuje zúčastnění všech zainteresovaných stran v rámci životního cyklu služby cloud computingu.



Obrázek 28: Hodnocení navrženého metodického rámce CCGM odbornými IT pracovníky, zdroj: (autor)

Z realizovaného hodnocení metodického rámce CCGM formou dotazníků vyplývá, že metodický rámec CCGM je pochopitelný a lze jej implementovat v konkrétních podmínkách organizace. Komponenty metodického rámce CCGM jsou uspořádány v jasné a logicky definované struktuře, která zjednodušuje jeho praktické využití. Popis rámce je vymezen definicí jeho struktury a konceptuálním modelem. Aplikace metodického rámce CCGM vede k očekávaným výsledkům při řízení využívání služby cloud computingu. Jelikož je metodický rámec CCGM založen na rámcích SOA Governance, COBIT 5 a ITIL 2011, tak stejně jako tyto rámce, tak i metodický rámec CCGM je procesně orientovaný a jednotlivé procesy a procesní aktivity jsou organizovány v logické návaznosti a spolu s rolemi a odpovědnostmi jsou dostatečně dokumentované. Navržené procesy pokrývají všechny fáze životního cyklu služby cloud computingu z pohledu spotřebitele. Verifikace metodického rámce CCGM pomocí případové studie a odbornými IT pracovníky potvrzuje správné nastavení obou navržených modelů cloud computing governance a cloud computing management. Navržený metodický rámec CCGM byl úspěšně implementován pro governance a management služeb cloud computingu v IT organizaci a rozšířil stávající model IT governance a IT managementu.

Na základě výsledků dotazníku je v Tabulce 47 vyhodnocena míra naplnění cílů metodického rámce CCGM. Míra, ve které jednotlivé otázky přispívají k naplnění cílů metodického rámce CCGM byla určena jako procentuální podíl počtu odpovědí na Likertově škále hodnocených stupněm „Naprosto souhlasím“ a „Spíše souhlasím“ k celkovému počtu odpovědí na danou otázku. Míra naplnění cílů metodického rámce CCGM v procentuálním vyjádření byla určena jako vážený průměr míry naplnění cíle příslušnými otázkami. Vysoká míra naplnění cílů metodického rámce CCGM vypovídá

o schopnosti metodického rámce CCGM komplexně pokrýt potřeby IT organizace při řešení reálného problému governance a managementu služeb cloud computingu v rámci případové studie.

Tabulka 47: Vyhodnocení splnění cílů metodického rámce CCGM, zdroj: (autor)

ID cíle	Název cíle Míra naplnění cíle v %	Číslo otázky	Počet odpovědí Míra naplnění cíle danou otázkou v %
C1	Poskytnutí jednotného metodického rámce pro governance a management využívání služeb cloud computingu, který odděluje cloud computing governance od cloud computing managementu, přičemž jejich rozhraní je jasně definováno. **Míra naplnění cíle: 86 %**	5	Naprosto souhlasím: 4, Spíše souhlasím: 0, Nevím: 3 Procentuální vyjádření naplnění cíle: 57 %
		6	Naprosto souhlasím: 3, Spíše souhlasím: 4, Nevím: 0 Procentuální vyjádření naplnění cíle: 100 %
		8	Naprosto souhlasím: 2, Spíše souhlasím: 3, Nevím: 2 Procentuální vyjádření naplnění cíle: 71 %
		9	Naprosto souhlasím: 4, Spíše souhlasím: 3, Nevím: 0 Procentuální vyjádření naplnění cíle: 100 %
		10	Naprosto souhlasím: 7, Spíše souhlasím: 0, Nevím: 0 Procentuální vyjádření naplnění cíle: 100 %
C2	Poskytnutí konzistentního, flexibilního, jednoduchého a srozumitelného a snadno implementovatelného procesně orientovaného metodického rámce pro governance a management využívání služeb cloud computingu. **Míra naplnění cíle: 90 %**	1	Naprosto souhlasím: 7, Spíše souhlasím: 0, Nevím: 0 Procentuální vyjádření naplnění cíle: 100 %
		2	Naprosto souhlasím: 5, Spíše souhlasím: 2, Nevím: 0 Procentuální vyjádření naplnění cíle: 100 %
		3	Naprosto souhlasím: 3, Spíše souhlasím: 2, Nevím: 2 Procentuální vyjádření naplnění cíle: 71 %
		7	Naprosto souhlasím: 7, Spíše souhlasím: 0, Nevím: 0 Procentuální vyjádření naplnění cíle: 100 %
		13	Naprosto souhlasím: 3, Spíše souhlasím: 1, Nevím: 3 Procentuální vyjádření naplnění cíle: 57 %
		15	Naprosto souhlasím: 4, Spíše souhlasím: 3, Nevím: 0 Procentuální vyjádření naplnění cíle: 100 %
		21	Naprosto souhlasím: 6, Spíše souhlasím: 1, Nevím: 0 Procentuální vyjádření naplnění cíle: 100 %
C3	Přizpůsobení metodického rámce pro governance a management využívání služeb cloud computingu specifickým podmínkám podniku a vytvoření systému governance a managementu využívání služeb cloud computingu konkrétního podniku. **Míra naplnění cíle: 86 %**	7	Naprosto souhlasím: 7, Spíše souhlasím: 0, Nevím: 0 Procentuální vyjádření naplnění cíle: 100 %
		12	Naprosto souhlasím: 4, Spíše souhlasím: 3, Nevím: 0 Procentuální vyjádření naplnění cíle: 100 %
		14	Naprosto souhlasím: 2, Spíše souhlasím: 2, Nevím: 3 Procentuální vyjádření naplnění cíle: 57 %
C4	Vytvoření rozhodovacího	9	Naprosto souhlasím: 4, Spíše souhlasím: 3, Nevím: 0

ID cíle	Název cíle Míra naplnění cíle v %	Číslo otázky	Počet odpovědí Míra naplnění cíle danou otázkou v %
	procesu a pravidel a omezení souvisejících s adopcí a využíváním služeb cloud computingu vzhledem k IT anebo cloud computing strategii s cílem dosažení potřeb byznysu. **Míra naplnění cíle: 79 %**		Procentuální vyjádření naplnění cíle: 100 %
		14	Naprosto souhlasím: 2, Spíše souhlasím: 2, Nevím: 3 Procentuální vyjádření naplnění cíle: 57 %
C5	Realizace benefitů z využití služby cloud computingu optimalizací nákladů a rizik při využívání služeb cloud computingu. **Míra naplnění cíle: 100 %**	4	Naprosto souhlasím: 3, Spíše souhlasím: 4, Nevím: 0 Procentuální vyjádření naplnění cíle: 100 %
C6	Zabezpečení efektivní adopce a efektivního a výkonného využívání služby cloud computingu v souladu s potřebami byznysu a zainteresovaných v rámci celého životního cyklu služby cloud computingu. **Míra naplnění cíle: 92 %**	11	Naprosto souhlasím: 2, Spíše souhlasím: 5, Nevím: 0 Procentuální vyjádření naplnění cíle: 100 %
		16	Naprosto souhlasím: 4, Spíše souhlasím: 2, Nevím: 1 Procentuální vyjádření naplnění cíle: 86 %
		17	Naprosto souhlasím: 3, Spíše souhlasím: 3, Nevím: 1 Procentuální vyjádření naplnění cíle: 86 %
		18	Naprosto souhlasím: 7, Spíše souhlasím: 0, Nevím: 0 Procentuální vyjádření naplnění cíle: 100 %
		19	Naprosto souhlasím: 7, Spíše souhlasím: 0, Nevím: 0 Procentuální vyjádření naplnění cíle: 100 %
		20	Naprosto souhlasím: 7, Spíše souhlasím: 0, Nevím: 0 Procentuální vyjádření naplnění cíle: 100 %
		22	Naprosto souhlasím: 0, Spíše souhlasím: 5, Nevím: 2 Procentuální vyjádření naplnění cíle: 71 %

Realizace případové studie v praxi umožnila úspěšné využití navržených praktik, procesů a rolí metodického rámce CCGM a prokázala validitu a správnost metodického rámce CCGM. Případová studie prokázala, že navržený metodický rámec CCGM lze v organizaci implementovat a využívat k řešení problémů a plnění úloh governance a managementu využívání služeb cloud computingu. Hodnocení metodického rámce CCGM odbornými IT pracovníky potvrdilo správnost, úplnost a srozumitelnost navržených metodických prvků (principů, procesů a rolí) metodického rámce CCGM.

V kapitole 8 autorka této doktorské disertační práce popsala a vyhodnotila případovou studii praktické aplikace metodického rámce Cloud computing governance a management (CCGM) ve velké IT organizaci. Validita a správnost navrženého metodického rámce Cloud computing governance a management (CCGM) byla prokázána během pilotního nasazení služby cloud computingu v modelu veřejného cloud computingu do produktivního provozu a vyhodnocením názorů IT specialistů prostřednictvím individuálního dotazníku.

9 Závěry práce

Hlavním cílem této doktorské disertační práce bylo navrhnout metodický rámec pro governance a management využívání služeb cloud computingu nazvaný autorkou jako metodický rámec Cloud computing governance a management (zkráceně metodický rámec CCGM) z pohledu spotřebitele služeb cloud computingu. Autorkou této doktorské disertační práce navržený metodický rámec CCGM je postavený na metodických rámcích SOA Governance, COBIT 5 a ITIL 2011. Obsah jimi definovaných metodických prvků přizpůsobuje a rozšiřuje o aspekty specifické pro governance a management služeb cloud computingu z pohledu spotřebitele služeb. Doktorská disertační práce přinesla v této oblasti jeden z prvních ucelených přístupů ke zkoumané oblasti. Validita a aplikovatelnost metodického rámce v praxi byla potvrzená pomocí případové studie (kapitola 8).

Tato doktorská disertační práce umožnila nalezení odpovědí na výzkumné otázky definované v kapitole 1.4. Pro jejich nalezení autorka v doktorské disertační práci analyzovala stávající široce akceptované metodické rámce IT governance a IT managementu z hlediska využívání služeb cloud computingu. Bylo zjištěno, že žádný z analyzovaných metodických rámců primárně nepodporuje prostředí governance a managementu využívání služeb cloud computingu z pohledu spotřebitele služeb, avšak obsah jimi definovaných metodických prvků lze modifikovat o specifika vyplývající z využívání služeb cloud computingu. Nalezení odpovědí na výzkumné otázky bylo umožněno identifikací aktuálního stavu reálného prostředí governance a managementu služeb cloud computingu z pohledu spotřebitele. Výsledky hodnocení podpory specifik governance a managementu využívání služeb cloud computingu z pohledu spotřebitele metodickými rámci SOA Governance, COBIT 5 a ITIL 2011 prokázaly, že tyto rámce neposkytují plnou podporu specifikům služeb cloud computingu, přičemž byly identifikované oblasti těchto rámců nutné k modifikaci pro prostředí využívání služeb v modelu veřejného cloud computingu. V jednotlivých kapitolách se autorce této doktorské disertační práce podařilo naplnit cíle doktorské disertační práce definované v kapitole 1.3. Doktorská disertační práce přispívá k vyplnění mezery ve stávajících metodických rámcích IT governance a IT managementu a poskytuje středně velkým a velkým obchodním společnostem vystupujících v roli spotřebitele služeb cloud computingu nástroj pro governance a management služeb v modelu veřejného cloud computingu.

9.1 Ověření výzkumných otázek

Pro naplnění cílů této doktorské disertační práce byly v kapitole 1.4 stanoveny dvě výzkumné otázky. Tabulka 48 uvádí kapitoly, ve kterých byly nalezeny odpovědi na výzkumné otázky.

Tabulka 48: Vyhodnocení ověření výzkumných otázek doktorské disertační práce, zdroj: (autor)

ID	Výzkumné otázky doktorské disertační práce	Kapitoly
VO1	Jak je ve stávajících metodických rámcích IT governance a IT management podporován governance a management služeb cloud computingu z hlediska spotřebitele služeb?	Kapitola 4
VO2	V jakých oblastech, do jaké míry a jakým způsobem je možné přizpůsobit metodické rámce IT governance a IT managementu pro governance a management služeb cloud computingu z hlediska spotřebitele služeb?	Kapitola 4

Odpověď na výzkumnou otázku VO1 „Jak je ve stávajících metodických rámcích IT governance a IT managementu podporován governance a management služeb cloud computingu z hlediska spotřebitele

služeb?“ byla nalezena v kapitole 4 a dílčích podkapitolách. Metodické rámce jsou klíčové pro vytvoření a udržování systému governance a managementu IT služeb. Jsou prostředkem komunikace mezi byznysem a IT a napomáhají efektivně řídit provoz IT služeb. Široce uznávanými a akceptovanými metodickými rámci pro governance a management IT služeb jsou SOA Governance, COBIT 5 a ITIL 2011. Ačkoliv tyto rámce poskytují metodiky pokrývající různě širokou oblast governance anebo managementu IT služeb, analýza výše jmenovaných metodických rámců provedená autorkou této doktorské disertační v kapitole 4 prokázala, že specifika prostředí governance a managementu využívání služeb cloud computingu z pohledu spotřebitele metodické rámce zohledňují pouze v malé míře nebo je prakticky nezohledňují. Nalezená odpověď na výzkumnou otázku VO1 je autorkou této doktorské disertační práce formulována následovně: „Stávající metodické rámce pro IT governance a IT management nedostatečně podporují governance a management služeb cloud computingu z hlediska spotřebitele služeb“.

Odpověď na výzkumnou otázku VO2 „V jakých oblastech, do jaké míry a jakým způsobem je možné přizpůsobit metodické rámce IT governance a IT managementu pro governance a management služeb cloud computingu z hlediska spotřebitele služeb?“ byla nalezena v kapitole 4. Na základě analýzy uvedených metodických rámců (kapitola 4), autorka této doktorské disertační práce argumentuje, že principy a procesy těchto metodických rámců mohou být po jejich přizpůsobení specifickým aspektům využívání služeb cloud computingu aplikovatelné při návrhu governance a managementu služeb cloud computingu. Jelikož se jedná o procesně orientované rámce, přizpůsobení je patrné zejména na úrovni procesů a jednotlivých procesních aktivit. Dále pak na úrovni principů a rolí. Metodické prvky definované v metodickém rámci SOA Governance lze přizpůsobit pro governance využívání služeb cloud computingu prostřednictvím návrhu nových nebo modifikací stávajících řídících principů, řídících procesů, řízených procesů, rolí a artefaktů s ohledem na specifika využívání služeb cloud computingu z pohledu spotřebitele. Metodické prvky definované v metodickém rámci ITIL 2011 lze přizpůsobit prostřednictvím návrhu nových nebo modifikací stávajících rolí a procesů, které mohou sloužit jako základ pro návrh modelu pro řízení služeb cloud computingu z pohledu spotřebitele služeb. Metodické prvky definované v metodickém rámci COBIT 5 lze přizpůsobit pro governance a management využívání služeb cloud computingu prostřednictvím modifikace stávajících governance a management procesů. Nalezená odpověď na výzkumnou otázku VO2 je autorkou této doktorské disertační práce formulována následovně: „Metodické rámce pro IT governance a IT management lze přizpůsobit pro prostředí využívání služeb cloud computingu z hlediska spotřebitele služeb cloud computingu. Metodickými prvky, které je možno přizpůsobit jsou řídící principy, procesy, role a artefakty.“

9.2 Splnění cílů práce

Hlavním cílem doktorské disertační práce bylo navrhnout metodický rámec pro governance a management využívání služeb cloud computingu (metodický rámec Cloud computing governance a management) z pohledu spotřebitele služeb cloud computingu. Pro dosažení hlavního cíle práce byly v kapitole 1.3 definovány dílčí cíle. Tabulka 49 uvádí kapitoly, ve kterých byly naplněny hlavní cíl a dílčí cíle této doktorské disertační práce.

Tabulka 49: Vyhodnocení splnění cílů doktorské disertační práce, zdroj: (autor)

ID	Cíl doktorské disertační práce	Typ cíle	Kapitoly
HC	Návrh metodického rámce pro governance a management využívání služeb cloud computingu (metodický rámec Cloud computing governance a management) z pohledu spotřebitele	Hlavní cíl	Kapitola 5, 6 a 7

ID	Cíl doktorské disertační práce	Typ cíle	Kapitoly
	služeb cloud computingu.		
DC1	Analýza stávajících metodických rámců IT governance a IT managementu z hlediska prostředí cloud computingu z pohledu spotřebitele služeb.	Dílčí cíl	Kapitola 4
DC2	Vymezení a sjednocení pojmů governance služeb cloud computingu (cloud computing governance) a management služeb cloud computingu (cloud computing management).	Dílčí cíl	Kapitola 6 a 7
DC3	Přizpůsobení a rozšíření metod metodických rámců SOA Governance a COBIT 5 se zohledněním specifik vyplývajících z prostředí využívání služeb cloud computingu z pohledu spotřebitele služeb pro návrh modelu pro governance využívání služeb cloud computingu (Cloud computing governance).	Dílčí cíl	Kapitola 6
DC4	Přizpůsobení a rozšíření metod metodických rámců ITIL 2011 a COBIT 5 se zohledněním specifik vyplývajících z prostředí využívání služeb cloud computingu z pohledu spotřebitele služeb pro návrh modelu řízení životního cyklu služeb cloud computingu (Cloud computing management).	Dílčí cíl	Kapitola 7
DC5	Ověření navrženého metodického rámce pro governance a management využívání služeb cloud computingu (Cloud computing governance a management) z pohledu spotřebitele služeb cloud computingu na případové studii.	Dílčí cíl	Kapitola 8

Metodický rámec CCGM byl navržen s cílem poskytnout jednotný, konzistentní, flexibilní a generický rámec pro governance a management využívání služeb cloud computingu, který spotřebiteli služeb cloud computingu umožní vytvoření specifického modelu Cloud computing governance a Cloud computing managementu v konkrétním podniku a realizaci benefitů z využití služby cloud computingu optimalizací nákladů a rizik z využívání služeb cloud computingu. V kapitole 2 byla autorkou této doktorské disertační práce popsána základní teoretická východiska a koncepty. Důležité vstupy pro návrh metodického rámce CCGM byly formulovány na základě autorkou této doktorské disertační práce provedené analýzy současného stavu výzkumu v oblasti aplikace praktik IT governance a IT managementu do prostředí cloud computingu. Výsledky analýzy současného stavu výzkumu v oblasti aplikace praktik IT governance a IT managementu do prostředí cloud computingu autorka této disertační práce popsala v kapitole 3. Dále autorka této doktorské disertační práce provedla analýzu současných široce akceptovaných rámců pro IT governance a IT management z hlediska prostředí cloud computingu z pohledu spotřebitele služeb (DC1).

Jelikož oblast governance a managementu služeb cloud computingu není plně standardizovaná, definice různých autorů na to, jakým způsobem definovat a vymezit governance a management využívání služeb cloud computingu, se odlišují a neexistuje jednotná všeobecně přijatá definice cloud computing governance a cloud computing managementu. Pro potřeby této disertační práce tedy autorka na základě získaných teoretických poznatků z kapitol 2, 3 a 4 formulovala definici pojmu governance služeb cloud computingu (kapitola 6) označovanou anglickým výrazem cloud computing governance a definici pojmu management služeb cloud computingu (kapitola 7) označovanou anglickým pojmem cloud computing management (DC2).

Na základě získaných teoretických poznatků byl autorkou této doktorské disertační práce formulován navržený metodický rámec CCGM (kapitola 5). Východiskem metodického rámce CCGM jsou

metodické rámce SOA Governance, COBIT 5 a ITIL 2011 a to zejména z důvodu jejich servisní orientace a procesního zaměření. SOA a cloud computing sdílejí princip orientace na služby a tím i některé základní zásady, čímž se stává cloud computing ideálním prostředím pro aplikaci metod SOA governance. ITIL poskytuje nástroj pro řízení životního cyklu IT služeb a zaměřuje se na způsob, jak plánovat, navrhovat a implementovat efektivní procesy řízení IT služeb. COBIT poskytuje soubor governance a management procesů pro oblast řízení informačních technologií. Autorkou této doktorské disertační práce navržený metodický rámec CCGM vzniknul jako rozšíření obsahu metodických prvků těchto metodických rámců o aspekty specifické pro governance a management služeb cloud computingu z pohledu spotřebitele služeb (DC3 a DC4).

Metodický rámec CCGM obsahuje definici modelu pro governance a management služeb cloud computingu z pohledu spotřebitele služeb, které autorka této doktorské disertační práce navrhla a pojmenovala jako Cloud computing governance a Cloud computing management. Pro návrh modelu Cloud computing governance autorka této disertační práce přizpůsobila a rozšířila metody metodických rámců SOA Governance a COBIT 5 se zohledněním specifik vyplývajících z prostředí využívání služeb cloud computingu z pohledu spotřebitele služeb (DC3). Cloud computing management navrhla autorka této disertační práce jako přizpůsobení a rozšíření metod metodických rámců ITIL 2011 a COBIT 5 se zohledněním specifik vyplývajících z prostředí využívání služeb cloud computingu z pohledu spotřebitele služeb (DC4).

Navržený metodický rámec CCGM byl autorkou této doktorské disertační práce ověřen metodou případové studie v reálném byznys prostředí (DC5). Ověření navrženého metodického rámce CCGM ve formě plánování, realizace a vyhodnocení případové studie je popsané v kapitole 8.

9.3 Přínosy doktorské disertační práce

Vědecký přínos doktorské disertační práce lze spatřovat v netriviálním a inovativním přizpůsobení stávajících znalostí, přístupů a metodik v oblasti IT governance a IT managementu a na jejich základě vytvoření nových metodik pro řešení problému governance a managementu využívání služeb cloud computingu z pohledu spotřebitele. Tento problém se objevil spolu s relativně nedávným nástupem éry cloud computingu. Gregor (2013) přínosy vědeckého výzkumu metody Design Science Research nazývá jako exaptace a zlepšení (Gregor, a další, 2013). Nové technologie vyžadují nové anebo vylepšené aplikační přístupy pro řešení souvisejících specifických problémů. Tato doktorská disertační práce je netriviální exaptací známých metod IT governance a IT managementu pro novou a specifickou oblast využívání služeb cloud computingu, kdy governance a management služeb cloud computingu z pohledu spotřebitele se svými charakteristickými vlastnostmi odlišuje od governance a managementu služeb IT nebo služeb SOA. Pro praxi přináší autorkou této doktorské disertační práce navržený metodický rámec CCGM metody, jejichž aplikace v praxi umožní zlepšení v podobě účinnějšího a efektivnějšího využití služeb cloud computingu. Praktická využitelnost navrženého metodického rámce CCGM byla ověřena metodou případové studie.

Jelikož výstupem této doktorské disertační práce je artefakt metodický rámec, lze přínosy doktorské disertační práce lze rozdělit na teoretické přínosy a na praktické přínosy. Teoretickými přínosy jsou:

- identifikace specifik governance a managementu služeb cloud computingu z pohledu spotřebitele služeb cloud computingu,
- sjednocení pojmů governance služeb cloud computingu (cloud computing governance) a management služeb cloud computingu z pohledu spotřebitele (cloud computing management),

- analýza současných metodických rámců IT governance a IT managementu z hlediska prostředí využívání služeb cloud computingu z pohledu spotřebitele,
- přizpůsobení a rozšíření vybraných metodických rámců IT governance a IT managementu se zohledněním specifik vyplývajících z prostředí využívání služeb cloud computingu z pohledu spotřebitele,
- návrh a specifikace procesů governance a managementu služeb cloud computingu z pohledu spotřebitele,
- návrh modelu Cloud computing governance z pohledu spotřebitele včetně definice kroků potřebných pro jeho implementaci,
- návrh modelu řízení životního cyklu cloud služeb (Cloud computing management) z pohledu spotřebitele služeb,
- návrh specifikace rolí a souvisejících odpovědností souvisejících s implementací metodického rámce CCGM z pohledu spotřebitele.

Praktický přínos doktorské disertační práce byl potvrzený ověřením navrženého metodického rámce CCGM v rámci případové studie (kapitola 8). Při tomto ověření se autorkou této disertační práce navržený metodický rámec CCGM ukázal jako využitelný v reálním prostředí velkého podniku. Z praktického hlediska lze za přínos dále považovat začlenění výstupů této doktorské disertační práce do modelu Management podnikové informatiky (MBI) v podobě rozšíření objektů modelu MBI a zahrnutím metod specifických pro oblast governance a managementu využívání služeb cloud computingu do řízení podnikové informatiky. Na základě navrženého metodického rámce CCGM autorka této doktorské disertační práce navrhla, popřípadě se podílela na návrhu objektů modelu MBI uvedených v Tabulce 50.

Tabulka 50: Seznam nově navržených a rozšířených objektů MBI na základě metodického rámce CCGM, zdroj: (autor)

Typ objektu	ID	Název objektu
Faktor	F100	Cloud computing
Faktor	F101	Veřejný (Public) cloud computing
Faktor	F102	Soukromý (Private) cloud computing
Faktor	F103	Hybridní (Hybrid) cloud computing
Faktor	F104	Komunitní (Community) cloud computing
Faktor	F105	Osobní cloud computing
Faktor	F106	SaaS – (Software as a Service)
Faktor	F107	IaaS – (Infrastructure as a Service)
Faktor	F108	PaaS – (Platform as a Service)
Skupina úloh	TG007	Cloud Governance a Cloud Management
Úloha	U052A	Cloud Governance
Úloha	U053A	Cloud management
Úloha	U054A	Hodnocení připravenosti pro přijetí cloud služeb
Úloha	U056A	Řízení rizik cloud computingu
Úloha	U061A	Finanční řízení služeb cloud computingu
Úloha	U062A	Řízení souladu s interními standardy a normami, s legislativními a regulatorními

Typ objektu	ID	Název objektu
		předpisy a smluvními požadavky
Úloha	U063A	Řízení exit strategie
Úloha	U064A	Řízení portfolia poskytovatelů služeb cloud computingu
Úloha	U065A	Řízení portfolia služeb cloud computingu
Úloha	U066A	Řízení smluv o poskytování služby cloud computingu
Úloha	U067A	Plánování přechodu na využívání služby cloud computingu
Úloha	U068A	Testování a validace služby cloud computingu
Úloha	U069A	Řízení přístupu uživatele ke službě cloud computingu
Úloha	U070A	Řízení nasazení služby cloud computingu do produktivního provozu
Úloha	U071A	Řízení událostí provozu služby cloud computingu
Úloha	U072A	Řízení incidentů provozu služby cloud computingu
Úloha	U073A	Řízení problémů provozu služby cloud computingu
Úloha	U074A	Řízení požadavků na službu cloud computingu
Úloha	U075A	Řízení požadavků na přístup ke službě cloud computingu
Úloha	U076A	Monitorování provozu služby cloud computingu
Úloha	U077A	Řízení nepřetržitého zdokonalování služby cloud computingu

Přínosem navrženého metodického rámce CCGM oproti identifikovanému stavu výzkumu v oblasti governance a managementu služeb cloud computingu z pohledu spotřebitele služeb cloud computingu je poskytnutí jednotného a komplexního metodického rámce pro governance a management využívání služeb cloud computingu, který jasně vymezuje cloud computing governance a cloud computing management a poskytuje konzistentní a detailní definici principů, procesů a rolí, na jejichž základě lze vybudovat specifický model Cloud computing governance a Cloud computing management v konkrétním podniku.

9.3.1 Srovnání návrhu metodického rámce CCGM s aktuálním mezinárodním výzkumem v dané oblasti

Tabulka 51 uvádí srovnání navrženého metodického rámce CCGM vzhledem ke zdrojům identifikovaným v kapitole 1.2.1. Návrh metodik pro cloud computing governance a cloud computing management je stále otevřeným výzkumným problémem, jehož dílčími oblastmi se specificky zabývá řada autorů. Výzkumné práce pokrývající pouze úzce vymezenou oblast governance a managementu služeb cloud computingu jsou analyzovány v kapitole 3.

Tabulka 51: Srovnání navrženého metodického rámce CCGM vůči identifikovaným zdrojům vzhledem k jejich obsahovému zaměření, zdroj: (autor)

Zdroj / Obsahové zaměření	(Bounagui, a další, 2014)	(Bounagui, a další, 2015)	(Bailey, a další, 2014)	(Ahmad, a další, 2011)	(Saidah, a další, 2014)	(Rehman, a další, 2015)	(Schneider, a další, 2015)	(Prasad, a další, 2014)	Metodický rámec CCGM (autor)
Předmět	CC management	CC management	CC management	CC management	CC management	CC management	CC management	CC governance	CC governance, CC management
Soubor governance principů a procesů	—	—	—	—	—	—	—	—	++
Role a odpovědnosti	+	—	+	+	+	—	—	++	++
Model životního cyklu governance	—	—	—	—	—	—	—	—	++
Definice požadavků na budoucí stav, studie proveditelnosti, návrh strategie	—	+	—	—	—	—	+	—	++
Model hodnocení zralosti přijetí služeb cloud computingu	—	—	—	—	—	—	—	—	++
Řízení rizik	+	+	+	+	+	—	—	—	++
Řízení souladu	+	—	—	+	+	—	—	—	++
Řízení exit strategie	—	—	—	—	+	—	+	—	++

Zdroj / Obsahové zaměření	(Bounagui, a další, 2014)	(Bounagui, a další, 2015)	(Bailey, a další, 2014)	(Ahmad, a další, 2011)	(Saidah, a další, 2014)	(Rehman, a další, 2015)	(Schneider, a další, 2015)	(Prasad, a další, 2014)	Metodický rámec CCGM (autor)
Řízení portfolia poskytovatelů	—	+	—	—	—	+	+	—	++
Řízení smluv, SLA	+	+	—	—	+	—	+	—	++
Řízení výběru služby	—	+	—	—	—	+	+	—	++
Plánování přechodu	—	+	—	—	—	—	+	—	++
Testování	—	+	—	+	—	—	+	—	++
Řízení přístupu	—	—	—	+	+	—	—	—	++
Monitorování provozu služby	—	—	—	+	+	+	+	—	++
Řízení událostí, incidentů a problémů	—	—	—	—	+	—	—	—	++
Řízení změn	—	—	—	—	+	—	—	—	++
Řízení nepřetržitého zdokonalování	—	+	—	—	+	+	—	—	++
Identifikace procesů	Ne	Ano	Ne	Ne	Ano	Ne	Ne	Ne	Ano
Definice procesů	Ne	Ne	Ne	Ne	Ne	Ne	Ne	Ne	Ano

Legenda	Aspekt není řešen	—	Aspekt je řešen	+	Aspekt je detailně řešen	++

Metodický rámec CCGM oproti identifikovaným dokumentům obsahuje definici principů a procesů governance služeb cloud computingu z pohledu spotřebitele, kterou žádný z dokumentů neobsahuje, a to i přes fakt, že existuje konsenzus nad nutností governance rámce pro prostředí cloud computingu. Pravděpodobnou příčinou této mezery může být skutečnost, že řada autorů problematiku governance služeb cloud computingu často neodděluje od managementu služeb cloud computingu nebo tyto dvě oblasti vzájemně zaměňuje. Governance struktury a role metodického rámce CCGM navazují na governance struktury a role pro prostředí governance služeb cloud computingu, které ve svém článku identifikoval Prasad (2014). Metodický rámec CCGM přebírá pro oblast governance od Prasad (2014) potřebu vytvoření výboru v čele s vedoucím IT pro prostředí cloud computingu a řídící skupiny, která bude provádět expertízu a rozhodování týkající se služeb v prostředí cloud computingu. Tyto governance struktury jsou v metodickém rámci CCGM doplněny o dvě další struktury zohledňující navržený model cloud computing governance metodického rámce CCGM a pro tyto struktury jsou navíc oproti Prasad (2014) definovány role a související odpovědnosti. Žádný z dostupných dokumentů neposkytuje návrh modelu pro governance využívání služeb cloud computingu (cloud computing governance) založený na detailní definici principů, procesů, organizačních struktura a rolí. Tuto mezeru pokrývá navržený Referenční model cloud computing governance metodického rámce CCGM. Dále na rozdíl od identifikovaných dokumentů metodický rámec CCGM obsahuje definici životního cyklu cloud computing governance, která vznikla přizpůsobením SOA Governance vitální metody pro prostředí governance služeb cloud computingu.

Bonagui (2015) definuje v rámci domény cloud migrace seznam aktivit souvisejících s plánováním, realizací a hodnocením úspěšnosti migrace. Metodický rámec CCGM navazuje na tyto aktivity v oblasti plánování, přizpůsobuje je pro potřeby strategické fáze managementu služeb cloud computingu a doplňuje je o detailní popis. Současně se zaváděním služeb cloud computingu autorka této doktorské disertační práce identifikovala potřebu realizovat analýzu a hodnocení připravenosti organizace pro přijetí služeb cloud computingu. Z tohoto důvodu obsahuje metodický rámec CCGM návrh modelu pro hodnocení míry schopnosti organizace přijmout služby cloud computingu nazvaný jako Cloud computing maturity model. Takovýto model pro hodnocení zralosti podniku spotřebitele služeb cloud computingu žádný z identifikovaných dokumentů nenavrhuje. Kritéria charakterizující specifické oblasti managementu služeb cloud computingu (jmenovitě Řízení rizik, Řízení souladu, Řízení exit strategie, Řízení portfolia poskytovatelů, Řízení smluv, SLA, Řízení výběru služby, Plánování přechodu, Testování, Řízení přístupu, Monitorování provozu služby, Řízení událostí, incidentů a problémů, Řízení změn a Řízení nepřetržitého zdokonalování) nejsou v identifikovaných dokumentech uvedených v Tabulce 51 popsána na detailní úrovni a to i přes to, že Bounagui (2015) a Saidah (2014) dokonce mluví o procesně orientovaném managementu služeb cloud computingu. Procesy po pokrytí oblasti řízení služeb cloud computingu žádný z identifikovaných dokumentů nedefinuje. Metodický rámec definuje pro tyto oblasti managementu služeb cloud computingu detailně navržené procesy a doplňuje navíc výše vyjmenované oblasti managementu služeb cloud computingu o finančního řízení služby cloud computingu, řízení portfolia služeb cloud computingu, řízení přístupu uživatele ke službě cloud computingu, řízení nasazení služby cloud computingu do produktivního provozu a řízení požadavků na službu cloud computingu. Navržený metodický rámec CCGM tak komplexně a přehledně seskupuje jednotlivé oblasti managementu služeb cloud computingu prostřednictvím souboru procesů do fází životního cyklu služby cloud computingu definované z pohledu spotřebitele služeb cloud computingu. Pro každý proces je navíc definována role včetně vymezení odpovědnosti ve vztahu k procesu.

Na návrhu metodického rámce CCGM se autorka této disertační práce podílela samostatně.

9.4 Zhodnocení využitelnosti dosažených výsledků

Soubor autorkou této disertační práce navržených principů a procesů metodického rámce CCGM poskytuje návod, jakým způsobem může spotřebitel realizovat model governance a managementu využívání služeb cloud computingu, který je kompatibilní s normou ISO/IEC 17998:2012 Information technology – SOA Governance Framework a metodickými rámci COBIT a ITIL. Tato kompatibilita přináší výhodu zejména v případě, kdy organizace vystupující v roli spotřebitele služby cloud computingu již některou z uvedených metodik implementovala. Spotřebiteli by měla doktorská disertační práce umožnit se orientovat v problematice governance a managementu služeb cloud computingu, měla by být východiskem při strategickém rozhodování o využití služeb cloud computingu ve vazbě na strategické cíle a měla by zabezpečit využívání služeb cloud computingu v souladu s SLA a s potřebami byznysu.

9.5 Náměty pro další vědecký výzkum

Navazující vědecký výzkum zaměřený na problematiku governance a managementu služeb cloud computingu z pohledu spotřebitele se může zaměřit na následující oblasti:

- doplnění procesních diagramů navržených cloud computing governance a management procesů,
- definice a doplnění metrik pro měření a hodnocení výkonnosti navržených cloud computing governance a management procesů,
- vyjádření vazeb mezi rolemi a procesy prostřednictvím přiřazení odpovědností jednotlivých rolí k procesu a jejich zobrazení pomocí matice odpovědnosti RACI tak, aby bylo zřejmé, kdo zodpovídá za realizaci procesu, kdo má řídící a rozhodovací pravomoc nad procesem, kdo poskytuje rady a konzultace ve vztahu k procesu a kdo je informován o průběhu procesu nebo o učiněných rozhodnutí týkajících se procesu,
- detailnější rozpracování jednotlivých procesních aktivit,
- ověření procesních aktivit, které nebyly v rámci případové studie plně aplikovány, a to z důvodu, že IT organizace implementovala ITIL na velice dobré úrovni, a že v rámci případové studie nedošlo k realizaci celého životního cyklu služby cloud computingu,
- doplnění metod nastavení parametrů služeb cloud computingu,
- doplnění metod integrace služeb cloud computingu s IT službami,
- specifikace provádění auditu v prostředí služeb cloud computingu
- doplnění úvahy, jak se bude lišit aplikovatelnost metodického rámce CCGM v malých a středních podnicích,
- posouzení využitelnosti metodického rámce CCGM pro oblast veřejné správy.

10 Přehled použité literatury

[1] **ACETO, Giuseppe, BOTTA, Alessio, de DONATO, Walter. 2012.** Cloud monitoring: Definitions, issues and future directions. *1st International Conference on Cloud Networking (CLOUDNET)* [online]. IEEE, 2012. s. 63-67. ISBN: 978-1-4673-2798-5. Dostupný z (DOI): 10.1109/CloudNet.2012.6483656.

[2] **ADJEI, Joseph Kwame. 2015.** Explaining the role of trust in cloud computing services. *Info* [online]. Emerald Group Publishing Limited, 2015. roč. 17, č. 1, s. 54-67. ISSN: 1463-6697. Dostupný z (DOI): 10.1108/info-09-2014-0042.

[3] **AHMAD, Rizwan, JANCZEWSKI, Lech. 2011.** Governance Life Cycle framework for Managing Security in Public Cloud: From User Perspective. *IEEE 4th International Conference on Cloud Computing* [online]. Washington (DC, USA): IEEE, 2011. s. 372-381. ISBN: 978-0-7695-4460-1/11. Dostupný z (DOI): doi: 10.1109/CLOUD.2011.117.

[4] **ALJOUMAH, Eman, AL-MOUSAWI, Fajer, IMTIAZ, Ahmad, AL-SHAMMRI, Maha, AL-JADY, Zahraa. 2015.** SLA in Cloud Computing Architectures: A Comprehensive Study. *International Journal of Grid Distribution Computing* [online]. roč. 8, č. 5, s. 7-32. ISSN: 2005-4262. Dostupný z (DOI): 10.14257/ijgdc.2015.8.5.02.

[5] **ALOSAIMI, Rana, ALNUEM, Mohammad. 2016.** A survey on security risk management frameworks in cloud computing. *Computer Science & Information Technology (CS & IT)* [online]. Academy & Industry Research Collaboration Center (AIRCC), 2016. roč. 6, s. 01-11. ISSN: 2231-5403. Dostupný z (DOI): 10.5121/csit.2016.60901.

[6] **AMANATULLAH, Yanuarizki, LIM, Charles, IPUNG, Heru Purnomo. 2013.** Toward cloud computing reference architecture: Cloud service management perspective. *International Conference on ICT for Smart Society (ICISS)* [online]. IEEE, 2013. ISBN: 978-1-4799-0145-6. Dostupný z (DOI): 10.1109/ICTSS.2013.6588059.

[7] **ARMBRUST, Michael, FOX, Armando, GRIFFITH, Rean, JOSEPH, Anthony, KATZ, Randy, KONWINSKI, Andrew, LEE, Gunho, PATTERSON, David, RABKIN, Ariel, STOICA, Ion, ZAHARIA, Matei. 2009.** Above the Clouds: A Berkeley View of Cloud Computing. *Electrical Engineering and Computer Sciences University of California at Berkeley* [online]. Berkeley (USA): UC Berkeley Reliable Adaptive Distributed Systems Laboratory, 2009. Technical Report No. UCB/EECS-2009-28. Dostupný z: http://robocup.csu.edu.cn/web/wp-content/uploads/2014/2014/01/FirstWeek/114.pdf.

[8] **BADIDI, Elarbi. 2016.** A broker-based framework for integrated SLA-aware SaaS Provisioning. *International Journal on Cloud Computing: Services and Architecture (IJCCSA)* [online]. roč. 6, č. 2. ISSN: 2231-5853. Dostupný z: http://airccj.org/ijccsa/ijccsa2016.html. Dostupný z (DOI): 10.5121/ijccsa.2016.6201.

[9] **BAILEY, Elana, BECKER, Jack D. 2014.** A Comparison of IT Governance and Control Frameworks in Cloud Computing. *Twentieth Americas Conference on Information Systems (AMCIS 2014 Proceedings)*. Savannah (USA): AIS Electronic Library, 2014. ISBN 978-0-692-25320-5.

[10] **BARDE, Anurag S. 2013.** Cloud Computing and Its Vision 2015!!. *International Journal of Computer and Communication Engineering* [online]. roč. 2, č. 4. ISSN: 2010-3743. Dostupný z (DOI): 10.7763/IJCCE.2013.V2.225

[11] **BISKE, Todd. 2008.** *SOA Governance: The key to successful SOA adoption in your organization.* Birmingham: Packt Publishing, 2008. s. 214. ISBN 978-1-84719586-9.

[12] **BISONG, Anthony, RAHMAN, Syed (Shawon) M. 2011.** An Overview of the Security Concerns in Enterprise Cloud Computing. *International Journal of Network Security & Its Applications (IJNSA)*. AIRCC Publishing Corporation, 2011. roč. 3, č. 1, s. 30-45. ISSN: 0974-9330. Dostupný z (DOI): 10.5121/ijnsa.2011.3103.

[13] **BOND, James. 2015.** *The Enterprise Cloud - Best Practices for Transforming Legacy IT*. Sebastopol (USA): O'Reilly Media, Inc., 2015. s. 396. ISBN: 978-1491907832.

[14] **BOUNAGUI, Yassine, HAFIDDI, Hatim, MEZRIOUI, Abdellatif. 2014.** Challenges for IT Based Cloud Computing Governance. *9th International Conference on Intelligent Systems: Theories and Applications (SITA-14)*. Rabat: IEEE, 2014. s. 1-8. ISBN: 978-1-4799-3566-6.

[15] **BOUNAGUI, Yassine, HAFIDDI, Hatim, MEZRIOUI, Abdellatif. 2015.** Requirements definition for a holistic approach of cloud computing governance. *12th International Conference of Computer Systems and Applications (AICCSA)* [online]. IEEE/ACS: 2015. ISSN: 2161-5330. Dostupný z (DOI): 10.1109/AICCSA.2015.7507245.

[16] **BOYNE, George Alexander. 2003.** Sources of Public Service Improvement: A Critical Review and Research Agenda. *Journal of Public Administration Research and Theory*. roč. 13, č. 3, s. 367-394. ISSN: 10531858.

[17] **BRANDIS, Knud, DZOMBETA, Srdan, HAUFE, Knut. 2013.** Towards a framework for governance architecture management in cloud environments: A semantic perspective. *Future Generation Computer Systems* [online]. Elsevier B.V., 2013. roč. 32, s. 274–281. ISSN: 0167-739X. Dostupný z (DOI): https://doi.org/10.1016/j.future.2013.09.022

[18] **BUCHALCEVOVA, Alena, POUR, Jan. 2015.** Business Informatics Management Model. *Advances in Computer Science and Ubiquitous Computing*. Springer Singapore, 2015. roč. 373 of the series Lecture Notes in Electrical Engineering, s. 65-71. ISBN: 978-981-10-0281-6.

[19] **BUCHALCEVOVÁ, Alena. 2005.** *Metodiky vývoje a údržby informačních systémů.* 1.vyd. Praha: Grada, 2005. ISBN 80-247-1075-7.

[20] **BUCHALCEVOVÁ, Alena. 2003.** *Návrh metodického rámce IS/ICT.* Praha: 2003. Doktorská disertační práce. Vysoká škola ekonomická v Praze, Fakulta informatiky a statistiky, Katedra informačních technologií.

[21] **BUYYA, Rajkumar, BROBERG, James, GOSCINSKI, Andrzej M. 2011.** *Cloud Computing Principles and Paradigms.* New Jersey: Wiley Publishing, 2011. ISBN 978-0-470-88799-8.

[22] **CABINET OFFICE. 2011.** *ITIL Service Design.* United Kingdom: The Stationery Office, 2011. ISBN 9780113313051.

[23] **CAO, Chaojie, ZHAN, Zhiqiang. 2011.** Incident management process for the cloud computing environments. *International Conference on Cloud Computing and Intelligence Systems (CCIS)*. IEEE, 2011. ISBN: 978-1-61284-204-2.

[24] **CARROLL, Noel, HELFERT, Markus, LYNN, Theo. 2014.** Towards the Development of a Cloud Service Capability Assessment Framework. *Continued Rise of the Cloud, Advances and Trends in Cloud Computing*. Springer London, 2014. s. 289-336. ISBN: 978-1-4471-6451-7.

[25] **ČESKÝ STATISTICKÝ ÚŘAD. 2015.** *Klasifikace ekonomických činností (CZ-NACE)* [online]. Český statistický úřad (ČSÚ), 2015 [cit. 2016-04-10]. Dostupný z : https://www.czso.cz/csu/czso/klasifikace_ekonomickych_cinnosti_cz_nace.

[26] **CHANG, Hsia-Ching, WANG, Chen-Ya. 2015.** Cloud Incident Data Analytics: Change-Point Analysis and Text Visualization. *IEEE, Hawaii International Conference on System Sciences (HICSS)*. s. 5320-5330. ISBN: 978-1-4799-7367-5.

[27] **CHOU, David C. 2015.** Cloud computing: A value creation model. *Computer Standards & Interfaces*. roč. 38, s. 72–77. Dostupný z (DOI): 0.1016/j.csi.2014.10.001.

[28] **CICHONSKI, Paul, MILLAR, Tom, GRANCE, Tim, SCARFONE, Karen. 2012.** *Computer Security Incident Handling Guide.* NIST National Institute of Standards and Technology U.S. Department of Commerce, 2012. Dostupný z (DOI): 10.6028/NIST.SP.800-61r2

[29] **CISCO. 2015.** *Cloud Computing Changing the Role and Relevance of IT Teams* [online]. Cisco Systems, 2015 [cit. 2015-12-18]. Dostupný z: http://www.cisco.com/c/dam/en/us/solutions/collateral/data-center-virtualization/cloud-infrastructure/cis-cep-changing-role-and-relevance-of-it-teams.pdf

[30] **CLOUD SECURITY ALLIANCE (CSA). 2016a.** *Cloud Controls Matrix v3.0.1* [online]. Cloud Security Alliance (CSA), 2016 [cit. 2016-08-28]. Dostupný z: https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/.

[31] **CLOUD SECURITY ALLIANCE (CSA). 2016b.** *The Treacherous 12. Cloud Computing Top Threats in 2016.* [online]. Cloud Security Alliance (CSA), 2016 [cit. 2016-08-30]. Dostupný z: https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf.

[32] **CLOUD SECURITY ALLIANCE (CSA). 2016c.** *CSA Security, Trust & Assurance Registry (STAR). Cloud Security Alliance - Certification* [Online]. Cloud Security Alliance (CSA), 2016 [cit. 2016-09-08]. Dostupný z: https://cloudsecurityalliance.org/star/.

[33] **COMUZZI, Marco, JACOBS, Guus, GREFEN, Paul. 2013.** Understanding SLA Elements in Cloud Computing. *Collaborative Systems for Reindustrialization, 14th IFIP WG 5.5 Working Conference on Virtual Enterprises, PRO-VE 2013* [online]. Springer Berlin Heidelberg, 2013. s. 385-392. ISBN: 978-3-642-40543-3. Dostupný z (DOI): 10.1007/978-3-642-40543-3_41.

[34] **COOK, Nigel, MILOJICIC, Dejan, TALWAR, Vanish. 2012.** Cloud management. *Journal of Internet Services and Applications* [online]. Springer London, 2012. roč. 3, č. 1, s. 67–75. ISSN: 1869-0238. Dostupný z (DOI): 10.1007/s13174-011-0053-8.

[35] **COPIE, Adrian, FORTIS, Teodor-Florin, MUNTEANU, Victor Ion. 2013.** From Cloud Governance to IoT Governance. *27th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*. IEEE, 2013. s. 1229-1234. ISBN: 978-0-7695-4952-1.

[36] **COPIE, Adrian, FORTIS, Teodor-Florin, MUNTEANU, Victor Ion. 2012.** Service Datastores in Cloud Governance. *10th International Symposium on Parallel and Distributed Processing with Applications (ISPA)*. IEEE, 2012. s. 473-478. ISBN: 978-1-4673-1631-6.

[37] **COPIL, Georgiana, TRUONG, Hong-Linh, DUSTDAR, Schahram. 2015.** Supporting Cloud Service Operation Management for Elasticity. *International Conference on Service-*

Oriented Computing (ICSOC 2015) [online]. Goa (India): Springer, Berlin, Heidelberg, 2015. s. 123-138. ISBN: 978-3-662-48616-0. Dostupný z (DOI): 10.1007/978-3-662-48616-0_8.

[38] **COUTINHO, Rafaelli de C., DRUMMOND, Lúcia M. A., FROTA, Yuri. 2013.** Optimization of a Cloud Resource Management Problem from a Consumer Perspective. *Euro-Par 2013: Parallel Processing Workshops*. Springer-Verlag Berlin Heidelberg, 2013. č. 8374 of the series Lecture Notes in Computer Science, s. 218-227. ISBN: 978-3-642-54420-0.

[39] **CSCC. 2015.** *Practical Guide to Cloud Service Agreements Version 2.0* [online]. Cloud Standards Customer Council, 2015 [cit. 2016-02-22]. Dostupný z: http://www.cloud-council.org/deliverables/CSCC-Practical-Guide-to-Cloud-Service-Agreements.pdf.

[40] **C-SIG SLA. 2014.** *Cloud Service Level Agreement Standardisation Guidelines* [online]. European Commission, Cloud Select Industry Group on Service Level Agreements Subgroup, 2014 [cit. 2016-02-26]. Dostupný z: https://ec.europa.eu/digital-single-market/en/news/cloud-service-level-agreement-standardisation-guidelines.

[41] **CSMIC. 2014.** *Service Measurement Index Framework Version 2.1* [online]. Carnegie Mellon University Silicon Valley, 2014 [cit. 2016-03-08]. Dostupný z: http://csmic.org/downloads/SMI_Overview_TwoPointOne.pdf.

[42] **DEHGHANI, Mojgan, EMADI, Sima. 2015.** Developing a Framework for Evaluating Service Oriented Architecture Governance with Approach COBIT. *Science Journal (CSJ)*. Sivas (Turkey): Cumhuriyet University Faculty of Science, 2015. roč. 36, č. 4 Special Issue. ISSN: 1300-1949.

[43] **DMTF. 2010.** *Architecture for Managing Clouds. A White Paper from the Open Cloud Standards Incubator* [online]. Document Number: DSP-IS0102. Distributed Management Task Force, Inc. (DMTF), 2010 [cit. 2014-09-11]. Dostupný z: http://www.dmtf.org/sites/default/files/standards/documents/DSP-IS0101_1.0.0.pdf.

[44] **DOELITZSCHER, Frank, REICH, Christoph, KNAHL, Martin, PASSFALL, Alexander, CLARKE, Nathan. 2012.** An agent based business aware incident detection system for cloud environments. *Journal of Cloud Computing: Advances, Systems and Applications*. roč. 1, vyd. 9. ISSN: 2192-113X.

[45] **DOHNAL, Jan. 2012.** *Úloha: IT Governance (U051A)* [online]. MBI (Management Byznys Informatiky), 2012 [cit. 2016-02-16]. Dostupný z: http://mbi.vse.cz/mbi/index.html#obj/TASK-84.

[46] **DOHNAL, Jan, POUR, Jan. 2013.** Řízení podnikové informatiky a podpora byznysu. *Česká společnost pro systémovou integraci.* Praha (Česká republika): 2013. č. Systémová integrace 2/2013, ISSN: 1214-6242.

[47] **DOUCEK, Petr, NOVÁK, Luděk, SVATÁ, Vlasta. 2008.** *Řízení bezpečnosti informací.* Praha: Professional Publishing, 2008. ISBN 978-80-86946-88-7.

[48] **DUTTA, Arnab, PENG, Guo Chao Alex, CHOUDHARY, Alok. 2013.** Risks in enterprise cloud computing: the perspective of IT experts. *Journal of Computer Information Systems* [online]. roč. 53, č. 4, s. 39-48. ISSN: 2380-2057. Dostupný z (DOI): http://dx.doi.org/10.1080/08874417.2013.11645649.

[49] **EMEAKAROHAA, Vincent C., NETTO, Marco A.S., CALHEIROS, Rodrigo N., BRANDIC, Ivona; BUYYA, Rajkumar, DE ROSE, César A.F.. 2012.** Towards autonomic detection of SLA violations in Cloud infrastructures. *Future Generation Computer Systems*

[online]. Elsevier B.V., 2012. roč. 28, č. 7, s. 1017–1029. Dostupný z (DOI): https://doi.org/10.1016/j.future.2011.08.018.

[50] **ENISA. 2009.** *Cloud Computing. Benefits, risks and recommendations for information security* [online]. European Network and Information Security Agency, 2009 [cit. 2013-11-28]. Dostupný z: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment.

[51] **ENISA. 2012.** *Introduction to Return on Security Investment* [online]. European Network and Information Security Agency, 2012 [cit. 2014-01-11]. Dostupný z: https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment.

[52] **ERL, Thomas. 2007a.** *Service-Orientation and the Concept of "Application"* [online]. ServiceOrientation.com. SOA Principles of Service Design, 2007 [cit. 2014-05-28]. Dostupný z: http://serviceorientation.com/serviceorientation/service_orientation_and_the_concept_of_application.

[53] **ERL, Thomas. 2007b.** *SOA Principles of Service Design.* USA: Prentice Hall, 2007. s. 608. ISBN-13: 978-0-13-234482-1.

[54] **ERL, Thomas, BENNETT, Stephen, GEE, Clive, LAIRD, Robert, MANES, Anne Thomas, SCHNEIDER, Robert, SHUSTER, Leo, TOST, Andre, VENABLE, Chris. 2011.** *SOA Governance: Governing Shared Services On-Premise & in the Cloud.* USA: Prentice Hall/PearsonPTR, 2011. ISBN: 978-0-13-815675-6.

[55] **EUROPEAN COMMISSION. 2016.** *Evropská komise spouští štít EU–USA na ochranu soukromí, který přináší solidnější ochranu transatlantických toků údajů* [online]. Press Release Database, 2016 [cit. 2016-09-20]. Dostupný z: http://europa.eu/rapid/press-release_IP-16-2461_cs.htm.

[56] **FEUERLICHT, George, THAI TRAN, Hong. 2015.** Adapting Service Development Life-Cycle for Cloud. *Proceedings of the 17th International Conference on Enterprise Information Systems*. Barcelona (Spain): 2015. s. 366-371. ISBN: 978-989-758-098-7.

[57] **FEUERLICHT, George. 2010.** Next Generation SOA: Can SOA Survive Cloud Computing? *Advances in Intelligent Web Mastering – 2 - Proceedings of the 6th Atlantic Web Intelligence Conference - AWIC'2009*. Prague (Czech Republic): Springer Berlin Heidelberg, 2010. s. 19-29.

[58] **FEUERLICHT, George, BURKON, Lukas, SEBESTA, Michal. 2011.** Cloud Computing Adoption: What are the Issues? *Systems Integration (Systemova Integrace)*. Prague: 2011. roč. 18, č. 2, s. 187-192. ISSN: 1210-9479.

[59] **FEUERLICHT, George, SCHNEIDER, Soeren, TRANTER, Leon. 2012.** Towards Enterprise Architecture for Cloud Computing Environments. *Proceedings of the 11th Workshop of on e-Business*. Orlando: 2012.

[60] **FORTINOVÁ, Jana. 2013.** Risks of Cloud Computing. *Systémová integrace 3/2013*. Praha: 2013. r. 20, č. 3. ISSN: 1214-6242.

[61] **FORTIS, Teodor-Florin, MUNTEANU, Victor Ion. 2014.** From Cloud Management to Cloud Governance. *Continued Rise of the Cloud. Advances and Trends in Cloud Computing.* Springer London, 2014. s. 265-287. ISBN: 978-1-4471-6452-4. ISSN: 1617-7975.

[62] **FORTIS, Teodor-Florin, MUNTEANU, Victor Ion, NEGRU, Viorel. 2012.** Towards an Ontology for Cloud Services. *Sixth International Conference on Complex, Intelligent and Software Intensive Systems (CISIS)*. IEEE, 2012. s. 787-792. ISBN: 978-0-7695-4687-2.

[63] **GAI, Keke, LI, Saier. 2012.** Towards Cloud Computing: A Literature Review on Cloud Computing and its Development Trends. *Fourth International Conference on Multimedia Information Networking and Security*. IEEE, 2012. s. 142-146. ISBN: 978-1-4673-3093-0.

[64] **GÁLA, Libor, BUCHALCEVOVÁ, Alena, JANDOŠ, Jaroslav. 2012.** *Podniková architektura.* Řepín: Nakladatelství Tomáš Brucker, 2012. ISBN 978-80-904661-6-6.

[65] **GÁLA, Libor, POUR, Jan, ŠEDIVÁ, Zuzana. 2015.** *Podniková informatika.* 3. vyd. Praha: Grada, 2015. s. 240. ISBN 978-80-247-5457-4.

[66] **GAO, Fangjian, SCHNEIDER, Stephan. 2012.** Cloud-Frameworks: Eine Übersicht aus der Wirtschaftsinformatik-Perspektive (Cloud-Frameworks: An Information Systems Perspective). *Proceedings of ConLife Academic Conference* [online]. Dostupný z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2189464.

[67] **GREGOR, Shirley, HEVNER, Alan R. 2013.** Positioning and presenting design science research for maximum impact. *Society for Information Management and The Management Information Systems Research Center Minneapolis, MN, USA, Journal MIS Quarterly*. Minneapolis (USA): 2013. roč. 37, č. 2, s. 337-356. ISSN 0276-7783.

[68] **GUPTA, Rajeev, PRASAD, K. Hima, LUAN, Laura. 2009.** Multi-dimensional Knowledge Integration for Efficient Incident Management in a Services Cloud. *International Conference on Services Computing*. IEEE, 2009. s. 57-64. ISBN: 978-1-4244-5183-8.

[69] **GUTIERREZ, Anabel, BOUKRAMI, Elias, LUMSDEN, Ranald. 2015.** Technological, organisational and environmental factors influencing managers' decision to adopt cloud computing in the UK. *Journal of Enterprise Information Management*. Emerald Group Publishing Limited, 2015. roč. 28, č. 6, s. 788-807. ISSN: 1741-0398.

[70] **HAIMES, Yacov Y., HOROWITZ, Barry M., GUO, Zhenyu, ANDRIJCIC, Eva, BOGDANOR, Joshua. 2015.** Assessing Systemic Risk to Cloud-Computing Technology as Complex Interconnected Systems of Systems. *Systems Engineering* [online]. Wiley Online Library, 2015. roč. 18, č. 3. Dostupný z (DOI): 10.1002/sys.21303.

[71] **HARLILI, Akbar Khrisna. 2014.** Risk Management Framework With COBIT 5 And Risk Management Framework for Cloud Computing Integration. *International Conference of Advanced Informatics: Concept, Theory and Application (ICAICTA)*. s. 103-108. ISBN: 978-1-4799-5100-0.

[72] **HAUPTVOGEL, Roman. 2013.** *Metodika budovania IS v architektúre orientovanej na služby.* Praha, 2013. Doktorská disertační práce. Vysoká škola ekonomická, Fakulta informatiky a statistiky.

[73] **HEILIG, Leonard, LALLA-RUIZ, Eduardo, VOß, Stefan. 2016.** A cloud brokerage approach for solving the resource management problem in multi-cloud environments. *Computers & Industrial Engineering* [online]. Elsevier Ltd., 2016. roč. 95, s. 16-26. Dostupný z (DOI): https://doi.org/10.1016/j.cie.2016.02.015.

[74] **HEININGER, Robert, WITTGES, Holger, KRCMAR, Helmut. 2012.** Literaturrecherche zu IT-Servicemanagement im Cloud Computing. *HMD Praxis der Wirtschaftsinformatik*.

Gabler Verlag, 2012. roč. 49, č. 6, s. 15-23. ISSN: 2198-2775. Dostupný z (DOI): 10.1007/BF03340753.

[75] **HENDERSON, John C., VENKATRAMAN, N. 1993.** Strategic alighnment: Leveraging information technology for transforming organization. *IBM systems journal*. roč. 32, č. 1. ISSN: 0018-88670.

[76] **HILL, Richard, HIRSCH, Laurie, LAKE, Peter, MOSHIRI, Siavash. 2013.** *Guide to Cloud Computing: Principles and Practice.* London (UK): Springer-Verlag London, 2013. ISBN 978-1-14471-4602-5.

[77] **HOBFELD, Tobias, SCHATZ, Raimund, VARELA, Martin, TIMMERER, Christian. 2012.** Challenges of QoE Management for Cloud Applications. *Communications Magazine* [online]. IEEE, 2012. roč. 50, č. 4, s. 9-16. ISSN: 0163-6804. Dostupný z (DOI): 10.1109/MCOM.2012.6178831.

[78] **HSU, Wen-Hsi Lydia. 2012.** Conceptual Framework of Cloud Computing Governance Model - An Education Perspective. *IEEE Technology And Engineering Education (ITEE)* [online]. IEEE, 2012. roč. 7, č. 2. Dostupný z: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.464.2321&rep=rep1&type=pdf.

[79] **Hui-MIN, Zhang, HAI-RONG, Hu, YANG-XIA, Xiang, LU-LU, Fang. 2013.** The Research and Design of Cloud Computing Framework Model Based on SOA. *International Workshop on Cloud Computing and Information Security (CCIS 2013)*. Atlantis Press, 2013.

[80] **IBM. 2009.** SOA Governance and Service Lifecycle Management [online]. IBM, 2009 cit. 2014-04-14]. Dostupný z: http://www-01.ibm.com/software/solutions/soa/gov/.

[81] **IDG CZECH REPUBLIC. 2015.** *The year 2015 is to be one of digital transformation of the economy* [online]. CIO Business World, červen 2015, Sv. Speciální vydání TOP ICT společností v České republice, červen 2015 [cit. 2016-01-28]. Dostupný z: https://www.flowmon.com/getattachment/af321f6e-9952-4e19-ab71-e2eb24e739f8/TOP-100-ICT-Companies-in-the-Czech-Republic-Yearbo.aspx.

[82] **ISACA. 2014a.** *About COBIT 5* [online]. COBIT 5 an ISACA framework. ISACA, 2014 [cit. 2014-07-09]. Dostupný z: https://cobitonline.isaca.org/about.

[83] **ISACA. 2014b.** *Controls & Assurance in the Cloud: Using COBIT 5.* ISACA, 2014. ISBN 978-1-60420-464-3.

[84] **ISACA. 2012a.** *Calculating Cloud ROI: From the Customer Perspective* [online]. ISACA, 2012 [cit. 2014-08-10]. Dostupný z: https://www.isaca.org/knowledge-center/research/researchdeliverables/pages/calculating-cloud-roi-from-the-customer-perspective.aspx.

[85] **ISACA. 2012b.** *Cobit 5 Enabling Processes.* ISACA, 2012. ISBN 978-1-60420-241-0.

[86] **ISACA. 2012c.** *COBIT 5: A business framework for Governance and Management of enterprise IT.* United States of America: ISACA, 2012. ISBN 978-1-60420-237-3.

[87] **ISACA. 2015.** *COBIT 5 Publications Directory*. *COBIT 5* [online]. Information Systems Audit and Control Association, 2015 [cit. 2015-11-01]. Dostupný z: http://www.isaca.org/COBIT/Pages/Product-Family.aspx.

[88] **ISO/IEC 17998. 2012.** *ISO/IEC 17998:2012 Information technology -- SOA Governance Framework* [online]. Standards catalogue ISO/IEC JTC 1 Information technology. ISO

(International Organization for Standardization), 2012 [cit. 2013-12-05]. Dostupný z: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=61240.

[89] **ISO/IEC 38500. 2015.** *International standard ISO/IEC 35800 - Corporate governance of information technology* [online]. ISO/IEC 38500:2015. Dostupný z: https://www.iso.org/standard/62816.html.

[90] **IYER, Bala R., HENDERSON, John C. 2010.** Preparing for the Future: Understanding the Seven Capabilities of Cloud Computing. *MIS Quarterly Executive*. roč. 9, č. 2, s. 117-131. ISSN: 1540-1960.

[91] **JÄNTTI, Marko, HOTTI, Virpi. 2015.** Defining the relationships between IT service management and IT service governance. *Information Technology and Management*. Springer US, 2015. ISSN: 1385-951X.

[92] **JAVERI, Fateme, JAZI, Mohammad Davarpanah, AJOUDANIAN, Shohreh, PANAH, Homayoon Yazdan, HOJAJI, Fazilat, JAFARI, Saeid, BEHROOZ, Mojgan. 2013.** Presenting a model for the deployment of Service-Oriented Architecture Governance (SOA Governance) in Information & Communication Technology Department of Isfahan Municipality. *International Research Journal of Applied and Basic Sciences*. roč. 5 č.11, s. 1438-1445. ISSN: 2251-838X.

[93] **JELÍNEK, Petr, ŠILD, Vladimír, VOŘÍŠEK, Jiří. 2007.** Kategorizace a architektury informatických služeb. *Systémová integrace*. Praha: Česká společnost pro systémovou integraci, 2007. roč. 14, č. 3. ISSN: 1214-6242.

[94] **JOSHI, Karuna. 2011.** DC Proposal: Automation of Service Lifecycle on the Cloud by Using Semantic Technologies. *The Semantic Web proceedings of 10th International Semantic Web Conference*. Springer Berlin Heidelberg, 2011. s. 285-292. ISBN: 978-3-642-25093-4.

[95] **JOUKHADAR, George, RABHI, Fethi. 2013.** Effective Governance During SOA Lifecycle - Theory and Practice. *Service Research and Innovation, Third Australian Symposium, ASSRI 2013*. Sydney (Australia): Springer International Publishing Switzerland, 2013. s. 15–28. ISBN: 978-3-319-07950-9.

[96] **JOUKHADAR, George, RABHI, Fethi. 2015a.** SOA Governance – Road into Maturity. *Australasian Conference on Information Systems*. Adelaide: 2015. ISBN: 978-0-646-95337-3.

[97] **JOUKHADAR, George, RABHI, Fethi. 2015b.** SOA in practice – a study of governance aspects. *Information Systems Frontiers*. Springer US, 2015. ISSN: 1572-9419.

[98] **KARIM, Raed, DING, Chen, MIRI, Ali. 2013.** An End-to-End QoS Mapping Approach for Cloud Service Selection. *IEEE Ninth World Congress on Services (SERVICES)* [online]. ISBN: 978-0-7695-5024-4. Dostupný z (DOI): 10.1109/SERVICES.2013.71.

[99] **KÖNIGSBERGER, Jan, SILCHER, Stefan, MITSCHANG, Bernhard. 2014.** SOA-GovMM: A Meta Model for a Comprehensive SOA Governance Repository. *15th International Conference on Information Reuse and Integration (IRI)*. IEEE, 2014. s. 187-194, ISBN: 978-1-4799-5880-1.

[100] **KRATZKE, Nane. 2012.** Cloud Computing Costs and Benefits An IT Management Point of View. *Cloud Computing and Services Science*. Springer New York, 2012. s. 185-203. ISBN: 978-1-4614-2326-3. ISSN: 1865-4924.

[101] **KREGER, Heather, HARDING, Chris . 2012.** *The Open Group SOA Governance Framework Becomes an International Standard* [online]. The Open Group Blog. The Open Group, 2012 [cit. 2014-07-01]. Dostupný z: http://blog.opengroup.org/2012/10/12/the-open-group-soa-governance-framework-becomes-an-international-standard/.

[102] **Laird, Robert. 2011.** *SOA Sets the Stage for Cloud: SOA Governance Makes It Work* [online]. Issue LVI. Service Technology magazine, 2011 [cit. 2013-12-26]. Dostupný z: http://www.servicetechmag.com/system/application/views/I56/1111-2.pdf.

[103] **LAMBERTH, Sabrina, WEISBECKER, Anette. 2010.** Wirtschaftlichkeitsbetrachtungen beim Einsatz von Cloud Computing. *Vom Projekt zum Produkt. Fachtagung des GI-Fachausschusses Management der Anwendungsentwicklung und -wartung im Fachbereich Wirtschaftsinformatik (WI-MAW).* Aachen (Germany): 2010. s. 123-136. ISBN: 978-3-88579-272-7.

[104] **LEWIS, Grace A., SMITH, Dennis B., KONTOGIANNIS, Kostas. 2010.** *A Research Agenda for Service-Oriented Architecture (SOA): Maintenance and Evolution of Service-Oriented Systems* [online]. Federal Government Contract Number FA8721-05-C-0003, Pittsburgh: Carnegie Mellon University, Software Engineering Institute, 2010 [cit. 201-05-16]. Dostupný z: http://www.sei.cmu.edu/reports/10tn003.pdf.

[105] **LINTHICUM, David S. 2009.** *Cloud Computing and SOA Convergence in Your Enterprise. A Step-by-Step Guide.* USA: Pearson Education, Inc., 2009. ISBN: 978-0-13-600922-1.

[106] **LIU, Sen, YANG, Yang, QU, Wen Guang, LIU, Yuan. 2016.** The business value of cloud computing: the partnering agility perspective. *Industrial Management & Data Systems.* Emerald Group Publishing Limited, 2016. roč. 116, č. 6, s. 1160-1177. ISSN: 0263-5577.

[107] **LOW, Chinyao, CHEN, Yahsueh, WU, Mingchang. 2011.** Understanding the determinants of cloud computing adoption. *Industrial Management & Data Systems* [online]. Emerald Group Publishing Limited, 2011. roč. 111, č. 7, s. 1006-1023. ISSN: 0263-5577. Dostupný z: http://www.emeraldinsight.com/doi/abs/10.1108/02635571111161262.

[108] **LUTHRIA, Haresh, RABHI , Fethi A. 2015.** Service-Oriented Architecture as a Driver of Dynamic Capabilities for Achieving Organizational Agility. *The Handbook of Service Innovation.* Springer London, 2015. s. 281-296. ISBN: 978-1-4471-6589-7.

[109] **MACLENNAN, Elzavita a Van Belle, Jean-Paul. 2014.** Factors affecting the organizational adoption of service-oriented architecture (SOA). *Information Systems and e-Business Management.* Springer Berlin Heidelberg, 2014. roč. 12, č. 1, s. 71-100. ISSN: 1617-9846.

[110] **MAGHRABI, Louai, PFLUEGEL, Eckhard. 2015.** Moving Assets to the Cloud: A Game Theoretic Approach Based on Trust. *International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*. London: IEEE, 2015. s. 1-5. ISBN: 978-1-4673-6797-4.

[111] **MANGALARAJ, George, SINGH, Anil, TANEJA, Aakash. 2014.** IT Governance Frameworks and COBIT - A Literature Review. *AMCIS 2014 Proceedings (Americas' Conference on Information Systems), Strategic and Competitive Use of Information Technology*. Savannah (Georgia, USA): 2014. ISBN: 978-0-692-25320-5.

[112] **MARTENS, Benedikt, TEUTEBERG, Frank. 2011.** Risk and Compliance Management for Cloud Computing Services: Designing a Reference Model. *Association for Information Systems, AIS Electronic Library (AISeL), Proceedings of the Seventeenth Americas*

Conference on Information Systems [online]. Detroit: 2011. Paper 228. Dostupný z: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1230&context=amcis2011_submissions.

[113] **MARTENS, Benedikt, WALTERBUSCH, Marc, TEUTEBERG, Frank. 2012.** Costing of Cloud Computing Services: A Total Cost of Ownership Approach. *45th Hawaii International Conference on System Sciences* [online]. IEEE, 2012. s. 1563-1572. Dostupný z: https://www.computer.org/csdl/proceedings/hicss/2012/4525/00/4525b563.pdf.

[114] **MEDHIOUB, Manel, KIM, Tai-Hoon. 2017.** Adaptive Risk Management Framework for Cloud Computing. *IEEE 31st International Conference on Advanced Information Networking and Applications* [online]. Dostupný z (DOI): 10.1109/AINA.2017.143.

[115] **MINOR, Mirjam, SCHULTE-ZURHAUSEN, Eric. 2014.** Towards Process-Oriented Cloud Management with Case-Based Reasoning. *Case-Based Reasoning Research and Development proceedings of 22nd International Conference, ICCBR 2014* [online]. Springer International Publishing, 2014. s. 305-314. ISBN: 978-3-319-11209-1. Dostupný z (DOI): 10.1007/978-3-319-11209-1_22.

[116] **MIRCEA, Marinela. 2010.** SOA, BPM and Cloud Computing: Connected for Innovation in Higher Education. *International Conference on Education and Management Technology ICEMT 2010* [online]. Cairo (Egypt): IEEE, 2010. s. 456-460. ISBN: 978-1-4244-8618-2. Dostupný z (DOI): 10.1109/ICEMT.2010.5657616.

[117] **MITRE. 2015.** *Cloud SLA Considerations for the Government Consumer* [online]. Case Number 15-2504. The MITRE Corporation, 2015 [cit. 2015-10-30]. Dostupný z: https://www.mitre.org/publications/technical-papers/cloud-sla-considerations-for-the-government-consumer-0.

[118] **MOLNÁR, Zdeněk, MILDEOVÁ, Stanislava, ŘEZANKOVÁ, Hana, BRIXÍ, Radim, KALINA, Jaroslav. 2012.** *Pokročilé metody vědecké práce.* Praha: Profess Consulting, s.r.o., 2012. ISBN 978-80-7259-064-3.

[119] **MONTES, Jesús, SÁNCHEZ, Alberto, MEMISHI, Bunjamin, PÉREZ, María S., ANTONIU, Gabriel. 2013.** GMonE: a Complete Approach to Cloud Monitoring. *Future Generation Computer Systems* [online]. Elsevier B. V., 2013. roč. 29, č. 8, s. 2026-2040. ISSN: 0167-739X. Dostupný z (DOI): https://doi.org/10.1016/j.future.2013.02.011.

[120] **MOURAD, Mohamed B Al, HUSSAIN, Mohammed. 2014.** The Impact of Cloud Computing on ITIL Service Strategy Processes. *International Journal of Computer and Communication Engineering* [online]. 2014. roč. 3, č. 5, s. 367-371. ISSN: 2010-3743. Dostupný z (DOI): 10.7763/IJCCE.2014.V3.351.

[121] **MUNTEANU, Victor Ion, EDMONDS, Andrew, BOHNERT, Thomas M. 2014.** Cloud Incident Management, Challenges, Research Directions, and Architectural Approach. *IEEE/ACM 7th International Conference on Utility and Cloud Computing (UCC)* [online]. London, (UK): IEEE, 2014. s. 786-791. ISBN: 978-1-4799-7881-6. Dostupný z (DOI): 10.1109/UCC.2014.128.

[122] **MUNTEANU, Victor Ion, FORTIŞ, Teodor-Florin, COPIE, Adrian. 2013.** Supporting Cloud Governance through Technologies and Standards. *Proceedings of the 7th International Symposium on Intelligent Distributed Computing - IDC 2013, Intelligent Distributed Computing VII* [online]. Prague (Czech Republic): Springer International Publishing Switzerland, 2013. ISBN 978-3-319-01571-2. Dostupný z (DOI): 10.1007/978-3-319-01571-2_32.

[123] **NABEEH, Nada A., EL-GHAREEB, Haitham A., RIAD, A. M. 2015.** Integrating Software Agents and Web Services in Service Oriented Architecture Based Cloud Services Discovery Framework. *Journal of Convergence Information Technology (JCIT)*. 2015. roč. 10, č. 1, s. 67-79. ISSN: 19759320.

[124] **Nařízení 2016/679. 2016.** Nařízení Evropského parlamentu a Rady ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). *Úřední věstník Evropské unie*. EUR-Lex, Evropský parlament a Rada Evropské unie, 2016. Dosupný z: http://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A32016R0679.

[125] **NEKVASIL, Marek. 2008.** Možnosti hodnocení efektivity investic do IT. *Systémová integrace 3/2008* [online]. Praha: Česká společnost pro systémovou integraci, 2008. roč. 15, č. 3. ISSN: 1214-6242. Dostupný z: http://www.cssi.cz/cssi/moznosti-hodnoceni-efektivity-investic-do-it.

[126] **NIEMANN, Michael, ECKERT, Julian, REPP, Nicolas; STEINMETZ, Ralf. 2008.** Towards a Generic Governance Model for Service-oriented Architectures. *14th Americas Conference on Information Systems (AMCIS 2008)*. Toronto (Canada): Association for Informations Systems AIS Electronic Library, 2008. ISBN: 978-0-615-23693-3.

[127] **NIST. 2013.** *NIST Cloud Computing Standards Roadmap* [online]. Special Publication 500-291, Version 2. National Institute of Standards and Technology, NIST Cloud Computing Standards Roadmap Working Group, 2013 [cit. 2013-11-14]. Dostupný z: https://www.nist.gov/sites/default/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf. Dostupný také z archivu dokumentů NIST: https://www.nist.gov/itl/nist-cloud-computing-related-publications.

[128] **NOURBAKHSH, Azamossadat, SHARIATPANAHI, Shahed Kazemi, BEREHLIA, Sasan. 2015.** The impact of service-oriented architecture on the scheduling algorithm in cloud computing. *International Research Journal of Applied and Basic Sciences* [online]. roč. 9, č. 3, s. 387-392, ISSN: 2251-838X. Dostupný z: http://irjabs.com/files_site/paperlist/r_2532_150323193302.pdf.

[129] **NOVOTNY, Alexander, BERNROIDER, Edward W.N., KOCH, Stefan. 2012.** Dimensions and Operationalisations of IT Governance: A Literature Review and Meta-Case Study. *CONF-IRM 2012 Proceedings* [online]. Dostupný z: http://aisel.aisnet.org/confirm2012/23.

[130] **NUSSBAUMER, N, XIAODONG, Liu. 2013.** Cloud Migration for SMEs in a Service Oriented Approach. *IEEE 37th Annual Computer Software and Applications Conference Workshops (COMPSACW)* [online]. Japan: IEEE, 2013. s. 457-462. ISBN: 978-1-4799-2159-1. Dostupný z (DOI): 10.1109/COMPSACW.2013.71.

[131] **ODELL, Laura A., WAGNER, Ryan R., WEIR, Tristan J. 2015.** *Department of Defense Use of Commercial Cloud Computing Capabilities and Services* [online]. Alexandria (Virginia): Institute for Defense Analyses (IDA), 2015 [cit. 2015-12-18]. Dostupný z: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=AD1002758.

[132] **OECD. 2015.** *G20/OECD Principles of Corporate Governance* [online]. Organisation for Economic Co-operation and Development (OECD), OECD under responsibility of the Secretary-General of the OECD, 2015 [cit. 2015-12-26]. Dostupný z: http://www.oecd.org/corporate/principles-corporate-governance.htm.

[133] **ONDRUŠKA, Marek. 2011.** *Governance reference model from system point of view.* Systémové přístupy ‘11 - Systémové myšlení jako změna paradigmatu. Praha: Nakladatelství Oeconomica, Vysoká škola ekonomická v Praze, Katedra systémové analýzy, 2011. ISBN 978-80-245-1844-2.

[134] **ONDRUŠKA, Marek. 2010.** Model propojení IT Governance a životního cyklu aplikace. *Systémová integrace 3/2010* [online]. Praha: Česká společnost pro systémovou integraci, 2010. roč. 17, č. 3. ISSN: 1214-6242. Dostupný z: http://www.cssi.cz/cssi/model-propojeni-it-governance-zivotniho-cyklu-aplikace.

[135] **OPARA-MARTINS, Justice, SAHANDI, Reza, TIAN, Feng. 2016.** Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective. *Journal of Cloud ComputingAdvances, Systems and Applications* [online]. ISSN: 2192-113X. Dostupné z (DOI): 10.1186/s13677-016-0054-z

[136] **OPARA-MARTINS, Justice, SAHANDI, Reza, TIAN, Feng. 2014.** Critical Review of Vendor Lock-in and Its Impact on Adoption of Cloud Computing. *International Conference on Information Society*. London (UK): IEEE, 2014. s. 92-97. ISBN: 978-1-9083-2038-4. Dostupné z (DOI): 10.1109/i-Society.2014.7009018

[137] **OPEN DATA CENTER ALLIANCE. 2013.** *Open Data Center Alliance Usage Model: Cloud Maturity Model Rev. 2.5.* [online]. Open Data Center Alliance, Inc., 2013 [cit. 2015-02-19]. Dostupný z: https://opendatacenteralliance.org/accelerating-adoption/usage-models/.

[138] **ORACLE. 2013.** *Oracle SOA Governance* [online]. Oracle, 2013 [cit. 2015-02-10]. Dostupný z: http://www.oracle.com/us/products/middleware/soa/governance/overview/index.html.

[139] **OROZCO, Jorge, TARHINI, Ali, MASA’DEH, Ra’ed (Moh’d Taisir), TARHINI, Takwa. 2015.** A Framework of IS/Business Alignment Management Practices to Improve the Design of IT Governance Architectures. *International Journal of Business and Management* [online]. Canadian Center of Science and Education, 2015. roč. 10, č. 4. ISSN 1833-8119. Dostupný z (DOI): http://dx.doi.org/10.5539/ijbm.v10n4p1.

[140] **OTT, C., KORTHAUS, A., BÖHMANN, T., ROSEMANN, M., KRCMAR, H.. 2010.** Towards a Reference Model for SOA Governance. *CAiSE Forum-2010* [online]. Hammamet (Tunisia): 2010. Dostupný z: http://ceur-ws.org/Vol-592/Paper04.pdf

[141] **OWUONDA, Stephen O., ORWA, Dan. 2016.** Cloud Computing Governance Readiness Assessment: Case Study of a local Airline Company. *International Journal of Applied Information Systems (IJAIS)* [online]. roč. 10, č. 8. ISSN: 2249-0868. Dostupné z: http://www.ijais.org/research/volume10/number8/owuonda-2016-ijais-451543.pdf.

[142] **PAVLÁT, David. 2013.** *K právní ochraně osobních údajů při jejich předávání v rámci cloudových služeb* [online]. Úřad pro ochranu osobních údajů, 2013 [cit. 2015-12-06]. Dostupný z: https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=3002.

[143] **PAVLÁT, David. 2015.** *Neplatnost rozhodnutí Komise o tzv. Safe Harbor - doporučení Úřadu* [online]. Úřad pro ochranu osobních údajů - Názory Úřadu. Úřad pro ochranu osobních údajů, 2015 [cit. 2015-12-05]. Dostupný z: https://www.uoou.cz/neplatnost-rozhodnuti-komise-o-tzv-safe-harbor-doporuceni-uradu/d-17119/p1=1099.

[144] **PAVLÁT, David. 2016.** *Štít EU-USA na ochranu soukromí* [online]. Úřad pro ochranu osobních údajů, 2016 [cit. 2016-08-16]. Dostupný z: https://www.uoou.cz/stit-eu-usa-na-ochranu-soukromi/d-20435.

[145] **PEFFERS, Ken, TUUNANEN, Tuure, ROTHENBERGER, Marcus A., CHATTERJEE, Samir. 2008.** A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems* [online]. roč. 24, č. 3, s. 45-78. ISSN:0742-1222. Dostupný z (DOI): ISSN:0742-1222.

[146] **PEIRIS, Chris, BALACHANDRAN, Bala, SHARMA, Dharmendra. 2010.** Governance Framework for Cloud Computing. *GSTG International Journal of Computing* [online]. roč. 1, č. 1. Dostupný z: http://dl6.globalstf.org/index.php/joc/article/view/431.

[147] **POLASH, Fahad, SHIVA, Sajjan. 2015.** Building Trust in Cloud: Service Certification Challenges and Approaches. *Ninth International Conference on Complex, Intelligent, and Software Intensive Systems* [online]. Blumenau (Brazil): IEEE, 2015. s. 187 – 191. ISBN: 978-1-4799-8870-9. Dostupný z (DOI): 10.1109/CISIS.2015.25.

[148] **PRASAD, Acklesh, GREEN, Peter. 2015.** Governing cloud computing services: Reconsideration of IT governance structures. *International Journal of Accounting Information Systems* [online]. Elsevier B.V., 2015. roč. 19, s. 45–58. Dostupný z (DOI): https://doi.org/10.1016/j.accinf.2015.11.004.

[149] **PRASAD, Acklesh, GREEN, Peter, HEALES, Jon. 2014.** On governance structures for the cloud computing services and assessing their effectiveness. *International Journal of Accounting Information Systems* [online]. Elsevier B.V., 2014. roč. 15, č. 4, s. 335-356. Dostupný z (DOI): https://doi.org/10.1016/j.accinf.2014.05.005.

[150] **PRÖHL, Thorsten, REPSCHLÄGER, Jonas, EREK, Koray, ZARNEKOW, Rüdiger. 2012.** IT-Servicemanagement im Cloud Computing. *HMD Praxis der Wirtschaftsinformatik* [online]. 2012. roč. 49, č. 6, s. 6–14. ISSN: 2198-2775. Dostupný z (DOI): 10.1007/BF03340752.

[151] **RAJMOHAN, B, BALASHANKAR, M. 2014.** The Cloud and SOA - Creating the Architecture for Today and Future. *International Journal of Research in Engineering & Advanced Technology*. roč. 1, č. 6. ISSN: 2320 - 8791.

[152] **RAMAKRISHNAN, Mala, SWAROOP, Jyothi, LIPPERT, Cathy, FAY, Sharon. 2013.** *Top Reasons to Implement SOA Governance - An Oracle White Paper* [online]. Oracle Corporation, 2013 [cit. 2014-06-21]. Dostupný z: http://www.oracle.com/us/technologies/soa/implement-soa-governance-1970613.pdf

[153] **REHMAN, Zia ur, HUSSAIN, Omar K., PARVIN, Sazia. 2012.** A Framework for User Feedback Based Cloud Service Monitoring. *Sixth International Conference on Complex, Intelligent, and Software Intensive Systems*. Palermo: IEEE, 2012. s. 257-262. ISBN: 978-1-4673-1233-2.

[154] **REHMAN, Zia-ur, HUSSAIN, Omar Khadeer, HUSSAIN, Farookh Khadeer. 2015.** User-side cloud service management: State-of-the-art and future directions. *Journal of Network and Computer Applications* [online]. Elsevier B.V., 2015, s. 108-122. Dostupný z (DOI): https://doi.org/10.1016/j.jnca.2015.05.007

[155] **RITCHEY, Ron. 2009.** *Governance Considerations for the Cloud*. SCAP – NIST. Booz Allen Hamilton, Inc, 2009 [cit. 2014-12-14]. Dostupný z: https://scap.nist.gov/events/2009/itsac/presentations/day3/Day3_Cloud_Ritchey.pdf

[156] **ROBBINS, Stephen P., COULTER, Mary. 2012.** *Management.* 11.vyd. New Jersey: Pearson Education, Inc., 2012. ISBN 978-0-13-216384-2.

[157] **Robrecht, Alexander, a další. 2014.** Entscheidungsunterstützung für Cloud Computing – ITIL Service Lifecycle. *HMD Praxis der Wirtschaftsinformatik* [online]. Gabler Verlag, 2014. roč. 49, č. 6, s. 24–32. ISSN: 2198-2775. Dostupný z (DOI): 10.1007/BF03340754.

[158] **ROLAND, Pavel, YATES, Mark. 2015.** *Survey: Public Sector Attitudes to Cloud and Shared Services in the Czech Republic* [online]. #CEMA22668. IDC research document, International Data Corporation (IDC), IDC Government Insights, 2015 [cit. 2016-12-11]. Dostupný z: https://www.idc.com/getdoc.jsp?containerId=CEMA22668.

[159] **ROSS, Peter, BLUMENSTEIN, Michael. 2013.** Cloud computing: the nexus of strategy and technology. *Journal of Business Strategy*. Emerald Group Publishing Limited, 2013. roč. 34, č. 4, s. 39-47. ISSN: 0275-6668.

[160] **ROZHODNUTÍ 2000/520/ES. 2000.** Rozhodnutí Komise ze dne 26. července 2000 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně poskytované podle zásad "bezpečného přístavu" a s tím souvisejících "často kladených otázek" vydaných Ministerstvem obchodu Spojených států. *Úřední věstník Evropské unie*. Úřední věstník L 215 , 25/08/2000 S. 0007 – 0047. EUR-Lex, Evropská komise, 2000. Dostupný z: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32000D0520&from=CS.

[161] **ROZHODNUTÍ 2010/87. 2010.** Rozhodnutí Komise ze dne 5. února 2010 o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích podle směrnice Evropského parlamentu a Rady 95/46/ES. *Úřední věstník Evropské unie*. EUR-Lex, Evropská komise, 2010. Dostupný z: http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A32010D0087.

[162] **ROZHODNUTÍ 2016/1250. 2016.** Prováděcí rozhodnutí Komise EU (2016/1250) ze dne 12. července 2016 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající úrovni ochrany poskytované štítem EU-USA na ochranu soukromí. *Úřední věstník Evropské unie.* EUR-Lex, Evropská komise, 2016. oznámeno pod číslem C(2016) 4176. Dostupný z: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.CES&toc=OJ%3AL%3A2016%3A207%3ATOC.

[163] **SAIDAH, Ahmed Shaker, ABDELBAKI, Nashwa. 2014.** A New Cloud Computing Governance Framework. *CLOSER 2014 - 4th International Conference on Cloud Computing and Services Science*. Barcelona (Spain): Springer, 2014. ISSN 1865-0937, ISBN 978-3-319-25413-5.

[164] **SARIPALLI, Prasad, WALTERS, Ben. 2010.** QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security. *IEEE 3rd International Conference on Cloud Computing (CLOUD)*. IEEE, 2010. s. 280-288. ISBN: 978-1-4244-8207-8.

[165] **SCHEPERS, T.G.J., IACOB, M.E., VAN ECK, P.A.T. 2008.** A lifecycle approach to SOA governance. *Proceedings of the 2008 ACM symposium on Applied computing*. USA: 2008. s. 1055-1061. ISBN: 978-1-59593-753-7.

[166] **SCHLOSSER, Frank, WAGNER, Heinz-Theo. 2011.** IT Governance Practices For Improving Strategic And Operational Business-IT Alignment. *PACIS 2011 Proceedings*. ISBN: 978-1-86435-644-1.

[167] **SCHNEIDER, Stephan, SUNYAEV, Ali. 2015.** CloudLive: a life cycle framework for cloud services. *Electronic Markets* [online]. Springer Berlin Heidelberg, 2015. roč. 25, č. 4, s. 299-311. ISSN: 1422-8890. Dostupný z (DOI): 10.1007/s12525-015-0205-y.

[168] **SELČAN, Vladimír. 2011.** Služby v podnikovej architektúre. *Systémová integrace 1/2011* [online]. Praha: Česká společnost pro systémovou integraci, 2011. roč. 18, č. 1, s. 70-83. ISSN: 1214-6242. Dostupný z: http://www.cssi.cz/cssi/sluzby-v-podnikovej-architekture.

[169] **SELIG, Gad J. 2015.** Implementing Effective IT Governance and IT Management. 2. edice. Van Haren Publishing, 2015. ISBN: 978-94-018-0008-2.

[170] **SIMORJAY, Frank. 2014.** *Data classification for cloud readiness.* Microsoft Corporation, 2014.

[171] **SMĚRNICE 95/46/ES. 1995.** Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. *Úřední věstník Evropské unie*. L 281 , 23/11/1995 S. 0031 – 0050. EUR-Lex, Evropský parlament a Rada, 1995. Dostupný z: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:31995L0046&from=CS.

[172] **SMĚRNICE 2016/680. 2016.** Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV. *Úřední věstník Evropské unie*. EUR-Lex, Evropský parlament a Rada, 2016. Dosutpný z: http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32016L0680.

[173] **SMITH, Heather A., MCKEEN, James D. 2003.** Developments in practice VII: developing and deliveringthe IT value proposition. *Communications of the Association for Information Systems* [online]. č. 11, s. 438-450. ISSN: 1529-3181. Dostupný z: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=2715&context=cais.

[174] **STANLEY, Ronald. 2014.** Cocreation and Implementing ITIL Service Management in the Cloud: A Case Study. *The 8th International Conference on Knowledge Management in Organizations*. Springer Netherlands, 2014. s. 61-71. ISBN: 978-94-007-7286-1.

[175] **STIENINGER, Mark, NEDBAL, Dietmar, WETZLINGER, Werner, WAGNER, Gerold, ERSKINE, Michael A.. 2014.** Impacts on the Organizational Adoption of Cloud Computing: A Reconceptualization of Influencing Factors. *Procedia Technology* [online]. Elsevier Ltd, 2014. roč. 16, s. 85-93. ISSN: 2212-0173. Dostupný z (DOI): https://doi.org/10.1016/j.protcy.2014.10.071.

[176] **ŠUBRTA, Václav. 2015.** Metody dynamických úprav SLA pro cloudové služby. *Systémová integrace 3/2015* [online]. Praha: Česká společnost pro systémovou integraci, 2015. roč. 22, č. 3. ISSN: 1214-6242. Dosutpný z: http://www.cssi.cz/cssi/metody-dynamickych-uprav-sla-pro-cloudove-sluzby.

[177] **SUICIMEZOV, Natalia, GEORGESCU, Mircea Radu. 2014.** IT Governance in Cloud. *Emerging Markets Queries in Finance and Business (EMQ 2013), Procedia Economics and*

Finance [online]. Elsevier B.V., 2014. roč. 15, s. 830-835. Dosutpný z (DOI): https://doi.org/10.1016/S2212-5671(14)00531-0.

[178] **SULTAN, Nabil Ahmed. 2011.** Reaching for the "cloud": How SMEs can manage. *International Journal of Information Management*. Elsevier B.V., 2011. roč. 31, č. 3, s. 272-278. ISSN: 0268-4012.

[179] **SUN, Yuanhui, XIAO, Zongshui, BAO, Dongmei, ZHAO, Jie. 2010.** An architecture model of management and monitoring on Cloud services resources. *3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*. IEEE, 2010. ISSN: 2154-7491.

[180] **SUN, Le, DONG, Hai, HUSSAIN, Farookh Khadeer, HUSSAIN, Omar Khadeer, CHANG, Elizabeth. 2014.** Cloud service selection: State-of-the-art and future research directions. *Journal of Network and Computer Applications* [online]. Elsevier B.V., 2014. roč. 45, s. 134-150. ISSN: 1084-8045. Dostupný z (DOI): http://doi.org/10.1016/j.jnca.2014.07.019.

[181] **SUSANTI, Fitri, SEMBIRING, Jaka. 2011.** The mapping of interconnected SOA governance and ITIL v3.0. *International Conference on Electrical Engineering and Informatics (ICEEI)* [online]. Bandung (Indonesia): IEEE, 2011. s. 1-5. ISBN: 978-1-4577-0752-0, ISSN: 2155-6830. Dostupný z (DOI): 10.1109/ICEEI.2011.6021574.

[182] **SUTHERLAND, Susan. 2013.** Convergence of interoperability of cloud computing, service oriented architecture and enterprise architecture. *The Society of Digital Information and Wireless Communications (SDIWC)*. ISBN: 978-0-9853483-3-5.

[183] **SVATÁ, Vlasta. 2011.** *Audit informačního systému.* 1.vyd. Příbram: PBtisk Příbram, 2011. s. 219. ISBN 978-80-7431-034-8.

[184] **SVATÁ, Vlasta. 2007.** *Information Systems Management.* Praha: Vysoká škola ekonomická v Praze, Nakladatelství Oeconomica, 2007. ISBN 978-80-245-1257-0.

[185] **SYNEK, Miloslav, KISLINGEROVÁ, Eva. 2010.** *Podniková ekonomika.* 5. přepracované a doplněné vydání. Praha: C. H. Beck, 2010. ISBN: 978-80-7400-336-3.

[186] **TANIMOTO, Shigeaki, HIRAMOTO, Manami, IWASHITA, Motoi, SATO, Hiroyuki, KANAI, Atsushi. 2011.** Risk Management on the Security Problem in Cloud Computing. *First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering (CNSI)*. IEEE, 2011. s. 147-152. ISBN: 978-1-4577-0180-1.

[187] **THE CABINET OFFICE. 2011.** *ITIL Service Strategy.* United Kingdom: The Stationery Office (TSO), 2011. ISBN 9780113313044.

[188] **THE DPSA. 2012.** *Public Service Corporate Governance of Information and Communication Technology Policy Framework* [online]. Department Public Service and Administration Republic of South Africa, 2012 [cit. 2014-06-02]. Dostupný z: http://www.gov.za/sites/www.gov.za/files/CGICTPolicyFramework.pdf.

[189] **THE OPEN GROUP. 2013a.** *Service Oriented Architecture: What Is SOA?* [online]. Service Oriented Architecture. The Open Group, 2013 [cit. 2014-05-05]. Dostupný z: http://www.opengroup.org/soa/source-book/soa/p1.htm.

[190] **THE OPEN GROUP. 2013b.** *Service-Oriented Architecture – SOA and Enterprise Architecture. Service Oriented Architecture* [online]. Service Oriented Architecture. The Open

Group, 2013 [cit. 2014-05-05]. Dostupný z: http://www.opengroup.org/soa/source-book/soa/p2.htm.

[191] **THE OPEN GROUP. 2009.** *SOA Governance Framework.* [Technical Standard]. United Kingdom: The Open Group, 2009. ISBN: 1-931624-82-8.

[192] **THE STATE OF QUEENSLAND. 2016.** *Risks of cloud computing* [online]. Business and industry portal, 2016 [cit. 2016-07-28]. Dostupný z: https://www.business.qld.gov.au/business/running/technology-for-business/cloud-computing-business/cloud-computing-risks.

[193] **TRAN, Hong Thai, FEUERLICHT, George. 2015.** Service Repository for Cloud Service Consumer Life Cycle Management. *ESOCC 2015 4th European Conference on Service-Oriented and Cloud Computing* [online]. Taormina (Italy): Springer International Publishing, 2015. s. 171-180. ISBN: 978-3-319-24072-5. Dostupný z (DOI): 10.1007/978-3-319-24072-5_12.

[194] **TSAI, Wei-Tek, SUN, Xin, BALASOORIYA, Janaka. 2010.** Service-Oriented Cloud Computing Architecture. *Seventh International Conference on Information Technology*. Las Vegas: IEEE, 2010. ISBN: 978-1-4244-6270-4.

[195] **TSALIS, Nikolaos, THEOHARIDOU, Marianthi, GRITZALIS, Dimitris. 2013.** Return on Security Investment for Cloud Platforms. *5th International Conference on Cloud Computing Technology and Science (CloudCom)*. s. 132-137. ISBN: 978-0-7695-5095-4.

[196] **UNNAMALAI, V.E., THRESPHINE, J.R. 2014.** *Service-Oriented Architecture for Cloud Computing. International Journal of Computer Science and Information Technologies*. roč. 5, č. 1, s. 251-255. ISSN: 0975-9646.

[197] **ÚOOÚ. 2013.** *Standardní smluvní doložky* [online]. Předávání osobních údajů do zahraničí, Úřad pro ochranu osobních údajů (ÚOOÚ), 2013 [cit. 2014-05-11]. Dostupný z: https://www.uoou.cz/standardni-smluvni-dolozky/ds-3505/archiv=0&p1=1633.

[198] **VAN GREMBERGEN, Wim. 2004.** *Strategies for Information Technology Governance.* Belgium: Idea Group, 2004. ISBN: 1-59140-141-0.

[199] **VAN GREMBERGEN, Wim, DE HAES, Steven. 2009.** *Enterprise Governance of Information Technology - Achieving Strategic Alignment and Value.* Springer, 2009. ISBN: 978-0-387-84882-2.

[200] **VAN GREMBERGEN, Wim, DE HAES, Stewen. 2012.** *Business Strategy and Applications in Enterprise IT Governance.* USA: IGI Global, 2012. ISBN 978-1-4666-17800-3.

[201] **VEBER, Jaromír, FOTR, Jiří, KOTOUČOVÁ, Jiřina, MALÝ, Milan, MLÁDKOVÁ, Ludmila, NOVÝ, Ivan; ŠVECOVÁ, Lenka, VODÁČEK, Leo. 2011.** *Management: Základy – moderní manažerské přístupy – výkonnost a prosperita.* Praha: Management Press, s. r. o., 2011. ISBN 978-80-7261-200-0.

[202] **VENTICINQUE, Salvatore, AVERSA, Rocco, DI MARTINO, Beniamino, RAK, Massimilano, PETCU, Dana. 2010.** A Cloud Agency for SLA Negotiation and Management. *Euro-Par 2010 Parallel Processing Workshops*. Springer Berlin Heidelberg, 2010. s. 587-594. ISBN: 978-3-642-21878-1.

[203] **VOŘÍŠEK, Jiří, POUR, Jan. 2012.** *Management podnikové informatiky.* Příbram: PBtisk Příbram, 2012. ISBN: 978-80-7431-102-4.

[204] **VOŘÍŠEK, Jiří, POUR, Jan. 2015.** Model for Management of Business Informatics. *Current Issues of Science and Research in the Global World*. London (UK): Taylor & Francis Group, 2015. ISBN: 978-1-138-02739-8.

[205] **VOŘÍŠEK, Jiří, BASL, Josef, BRUCKNER, Tomáš, BUCHALCEVOVÁ, Alena, GÁLA, Libor, KUNSTOVÁ, Renáta, MARYŠKA, Miloš, NOVOTNÝ, Ota, POUR, Jan, ŠIMKOVÁ, Eva. 2010.** *Principy a modely řízení podnikové informatiky.* Praha: Vysoká škola ekonomická v Praze, nakladatelství Oeconomica, 2010. ISBN 978-80-245-1440-6.

[206] **VOŘÍŠEK, Jiří, JANDOŠ, Jaroslav, FEUERLICHT, Jiří. 2011.** SPSPR Model - Framework for ICT Services Management. *Journal of Systems Integration* [online]. Praha, 2011. roč. 2, č. 2. ISSN: 1804-2724. Dosutpný z (DOI): http://dx.doi.org/10.20470/jsi.v2i2.85.

[207] **WANG, Heyong, HE, Wu, WANG, Feng-Kwei. 2012.** Enterprise cloud service architectures. *Information Technology and Management*. Springer US, 2012. roč. 13, č. 4, s. 445-454. ISSN: 1385-951X.

[208] **WANG, Shangguang, LIU, Zhipiao, SUN, Qibo, ZOU, Hua, YANG, Fangchun. 2014.** Towards an accurate evaluation of quality of cloud service in service-oriented cloud computing. *Journal of Intelligent Manufacturing*. Springer US, 2014. roč. 25, č.. 2, s. 283-291. ISSN: 1572-8145.

[209] **WARD, Jonathan Stuart, BARKER, Adam. 2015.** Cloud cover: monitoring large-scale clouds with Varanus. *Journal of Cloud Computing* [online]. roč. 4, č. 16. Dostupný z (DOI): 10.1186/s13677-015-0041-9.

[210] **WATTAL, S, IBM INDIA LTD., NOIDA, India, KUMAR, A. 2014.** Cloud computing - An emerging trend in information technology. *2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*. IEEE, 2014. s. 168-173. ISBN: 978-1-4799-2900-9.

[211] **WEISS, Daniel, REPSCHLAEGER, Jonas, ZARNEKOW, Rüdiger, SCHROEDL, Holger. 2013.** Towards a Consumer Cloud Computing Maturity Model - Proposition of Development Guidelines, Maturity Domains and Maturity Levels. *PACIS 2013 Proceedings* [online]. Dostupný z: http://aisel.aisnet.org/pacis2013/211/.

[212] **WILLIAMS, Bill. 2012.** *The Economics of Cloud Computing*. Indianapolis: Cisco Press, 2012. ISBN-13: 978-1-58714-306-9.

[213] **WILSON, Piers. 2011.** Positive perspectives on cloud security. *Information Security Technical Report* [online]. Elsevier B.V., 2011. roč. 16, č. 3–4, s. 97–101. Dostupný z (DOI): https://doi.org/10.1016/j.istr.2011.08.002.

[214] **WP 196. 2012.** Stanovisko č. 05/2012 ke cloud computingu. *01037/12/CS WP 196, Pracovní skupina pro ochranu údajů zřízená podle článku 29*, 2012. Dostupný z: https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=16709.

[215] **WU, Xu. 2015.** A New Trust Model in Cloud Computing Environments. *International Journal of Hybrid Information Technology*. roč. 8, č. 3, s. 177-184. ISSN: 1738-9968.

[216] **YANG, Xiaolong, ZHANG, Huimin. 2012.** Cloud Computing and SOA Convergence Research. *Fifth International Symposium on Computational Intelligence and Design* [online]. Hangzhou (China): IEEE, 2012. roč. 1, s. 330-335. ISBN: 978-1-4673-2646-9. Dostupný z (DOI): 10.1109/ISCID.2012.90.

[217] **YIN, Robert K. 2009.** *Case Study Research: Design and Methods.* 4.vyd. USA: SAGE Publications, Inc., 2009. ISBN 978-1-4129-6099-1.

[218] **YOUSSFI, Karim, BOUTAHAR, Jaouad, ELGHAZI, Elghazi. 2014.** A Tool Design of Cobit Roadmap Implementation. *(IJACSA) International Journal of Advanced Computer Science and Applications* [online]. roč. 5, č. 7, s. 86-94. ISSN: 2156-5570. Dostupný z (DOI): 10.14569/IJACSA.2014.050714.

[219] **ZÁKON Č. 101/2000 SB. 2000.** Zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů. *Portál Veřejné Správy, Zákony.* Wolters Kluwer ČR, 2000.

[220] **ZÁKON Č. 89/2012 SB. 2012.** Zákon č. 89/2012 Sb., občanský zákoník. Praha: Wolters Kluwer ČR, 2012.

[221] **ZHANG, Xuan, WUWONG, Nattapong, LI, Hao, ZHANG, Xuejie. 2010.** Information Security Risk Management Framework for the Cloud Computing Environments. *10th IEEE International Conference on Computer and Information Technology (CIT 2010)* [online]. Bradford (UK): IEEE, 2010. s. 1328-1334. ISBN: 978-1-4244-7548-3. Dostupný z (DOI): 10.1109/CIT.2010.501.

[222] **ZHAO, Jun-Feng, ZHOU, Jian-Tao. 2015.** Strategies and Methods for Cloud Migration. *International Journal of Automation and Computing* [online]. Springer-Verlag, 2015. roč. 11, č. 2, s. 143-152. ISSN: 476-8186. Dostupný z (DOI): 10.1007/s11633-014-0776-7.

[223] **ŽAMBERSKÝ, Martin. 2013.** Softwarové pirátství v době Cloud Computingu. *Systémová integrace 1/2013* [online]. Praha: Česká společnost pro systémovou integraci, 2013. roč. 20, č. 1, ISSN: 1214-6242. Dostupný z: http://www.cssi.cz/cssi/softwarove-piratstvi-v%C2%A0dobe-cloud-computingu.

11 Seznam použitých termínů a zkratek

Tato kapitola definuje nejdůležitější pojmy a zkratky používané v této doktorské disertační práci. Cílem je sjednocení existujících definic jednotlivých pojmů z analýzy informačních zdrojů pro potřeby a zaměření této doktorské disertační práce.

Tabulka 52: Seznam nejdůležitějších termínů, zdroj: (autor)

Termín	Zkratka	Význam
Cloud computing		*„Model, který umožňuje ubikvitní, pohodlný, na vyžádání a přes síť dostupný přístup ke sdílenému souboru konfigurovatelných výpočetních zdrojů, které mohou být velice rychle poskytnuty a nasazeny s minimálním úsilím nebo bez přímé interakce s poskytovatelem služeb“* (NIST, 2013).
Cloud computing governance	CCG	CCG je soubor politik, pravidel, omezení, organizačních struktur, rolí a odpovědností uzpůsobených pro prostředí cloud computingu z pohledu spotřebitele služeb, které se soustředí na zabezpečení efektivního využívání služeb cloud computingu při minimalizaci souvisejících nákladů a rizik tak, aby služby cloud computingu přispívaly k tvorbě očekávané byznys hodnoty v souladu s potřebami podniku a zainteresovaných stran.
Cloud computing management	CCM	Cloud computing management je výkonný řídicí systém, který zabezpečuje efektivní využívání služeb cloud computingu a zajišťuje, že cíle stanovené cloud computing governance budou dosaženy prostřednictvím souboru aktivit, které realizují plánování, výběr, osvojení, nasazení, provoz, monitorování a ukončení využívání služeb cloud computingu poskytovaných externím poskytovatelem služeb cloud computingu.
Dohoda o úrovni služby	SLA	Dohoda mezi poskytovatelem a spotřebitelem služeb, která obsahuje popis služby, definici cílů úrovně služby, definici odpovědností, akceptované využití služeb, omezení související se službami, výkonnostní parametry služeb a platební podmínky využití služeb.
Charakteristiky cloud computingu		Charakteristikami cloud computingu jsou samoobslužná a automatická administrace služeb cloud computingu na základě poptávky, přístup ke službě cloud computingu přes síť, sdílení zdrojů, rapidní elasticita a měřitelnost služeb cloud computingu.
Informační technologie	IT	Informační technologie zahrnují všechny prvky, které s nimi souvisí, jmenovitě informační systémy, procesy, služby, struktury atd.
IT governance		IT governance zabezpečuje neustálé vyhodnocování obchodních podmínek a potřeb zainteresovaných stran, na jejichž základě stanovuje požadovanou úroveň podnikových cílů, stanovuje způsob dosažení těchto cílů a sleduje výkon a dodržování shody reálně dosažených cílů s plánovanými podnikovými cíli (ISACA, 2012c).
IT management		Součástí IT managementu aktivity, které se soustředí na plánování, tvorbu, provozování a monitorování činností ve shodě s požadavky governance za účelem dosažení podnikových cílů (ISACA, 2012c).
IT služba		ITIL 2011 (2011) IT službu následovně (The Cabinet Office, 2011): *„IT služba je služba poskytovaná poskytovatelem IT služeb. IT služba se skládá z kombinace informačních technologií, lidí a procesů. Zákaznicky orientovaná IT služba přímo podporuje obchodní procesy jednoho nebo více zákazníků a cílové hodnoty úrovně této služby by měly být definovány v dohodě o úrovni služby. Ostatní IT služby,*

Termín	Zkratka	Význam
		nazývané podpůrné služby, nejsou přímo využívány byznysem, ale jsou vyžadovány poskytovatelem služeb pro zabezpečení dodávky zákaznicky orientovaných IT služeb.“
Information Technology Infrastructure Library	ITIL	ITIL je standardizovaná metodologie nejlepších zkušeností z praxe pro řízení IT služeb. ITIL je vytvořen formou souboru nezávazných doporučení vycházejících z nejlepších zkušeností z praxe IT, kdy si každý podnik při implementaci ITIL může podle svých individuálních potřeb zvolit k realizaci pouze ta doporučení, která jsou pro něj optimální. ITIL poskytuje praktiky, na jejichž základě je možno vytvořit a realizovat IT Service Management (ITSM) pro řízení životního cyklu služeb (The Cabinet Office, 2011).
Management byznys informatiky	MBI	Management podnikové informatiky (MBI) je konzistentní a flexibilní metodický rámec řízení podnikové informatiky a nejlepších praktik v oboru (Voříšek, a další, 2012).
Management IT služeb		Podstatou managementu IT služeb je řízení životního cyklu IT služeb ve smyslu řízení kvality IT služeb s cílem podporovat dosažení potřeb podniku prostřednictvím řízení životního cyklu služeb a souvisejících IT schopností, kapacit a zdrojů podle specifických požadavků podniku (The Cabinet Office, 2011). Management IT služeb je realizován souborem procesů a procedur ovlivňovaných politikami IT governance, které zajišťují plánování, návrh, realizaci, testování, produktivní nasazení, monitorování a podporu provozu IT služeb, které budou v souladu s principy IT governance a servisními dohodami poskytovat funkcionalitu očekávanou pro podporu příslušného obchodního procesu a budou dostatečně spolehlivé a výkonné.
Metodický rámec		Rámec je dle Svatá (2011) „*popis opakovatelných řešení při návrhu struktury a chování prvků IS*“ (Svatá, 2011). Metodický rámec je chápán jako uspořádaná skupina metodik, což Svatá (2011) definuje jako „*souhrn doporučených praktik a postupů*“ (Svatá, 2011).
On-premise IT řešení		IT systémy instalované na firemní IT infrastruktuře.
Poskytovatel služeb cloud computingu		*Poskytovatel služeb cloud computingu je jedinec nebo organizace zodpovědná za zabezpečení dostupnosti služeb pro spotřebitele služeb cloud computingu. Poskytovatel služeb cloud computingu vytváří služby cloud computingu, řídí technickou infrastrukturu potřebnou pro poskytování služeb, poskytuje služby dle dohodnuté úrovně služeb a chrání bezpečnost a soukromí služeb“* (NIST, 2013).
Servisně orientovaná architektura	SOA	Existuje řada definic pro pojem servisně orientovaná architektura (SOA), které se liší v závislosti na autorovi. Různí autoři používají pro vysvětlení pojmu SOA odlišné výrazové prostředky, avšak význam definic je v podstatě shodný. Pro potřeby této doktorské disertační práce jsou nejvhodnější definice konsorcia The Open Group (2013a), které říká, že *„servisně orientovaná architektura (SOA) je architektonický styl, který podporuje servisní orientaci“* (The Open Group, 2013a) a *„může být použit k vybudování podnikového IT“* (The Open Group, 2013b) a definice Thomase Erla (2007b), který definuje servisně orientovanou architekturu (SOA) následovně (Erl, 2007b): *„SOA zavádí architektonický model, jehož cílem je zvýšení účinnosti, agility a produktivity podniku, kdy služby reprezentují prvky logického řešení systému s cílem zabezpečit dosažení strategických cílů servisní orientace.“* Na základě dostupných definic lze servisně orientovanou architekturu definovat jako přístup k realizaci architektury informačních systémů, a to jak po

Termín	Zkratka	Význam
		stránce aplikační, tak po stránce technologické, kdy jednotlivé prvky logického řešení systému vystupují jako služby, jejíž cílem je zvýšit efektivitu, agilitu a produktivitu podniku.
Služba cloud computingu		Služba cloud computingu je IT služba poskytovaná poskytovatelem služeb cloud computingu v prostředí cloud computingu. Dle Voříšek (2010) se jedná o IT služby s kontinuální spotřebou/ disponibilitou.
Služba SOA		Služba v prostředí SOA je základním prvkem servisně orientovaného logického řešení. Služba SOA musí splňovat jasně vymezené návrhové charakteristiky, kterými jsou dohoda o službě, volná vazba služby, abstrakce služby, znovupoužitelnost služby, autonomie služby, bezstavovost služby, zjistitelnost služby, skladatelnost služby, servisní orientace a interoperabilita služby (Erl, 2007b).
SOA governance		SOA Governance je definována jako kombinace organizačních struktur, lidí, technologií, politik a procesů uvnitř organizace, která zajišťuje, že SOA bude fungovat správně a v souladu s potřebami realizace byznys procesů podniku (Biske, 2008).
Spotřebitel služeb cloud computingu		*„Spotřebitel služeb cloud computingu je jedinec nebo organizace, která získává a využívá služby cloud computingu, které jsou dodávané poskytovatelem služeb cloud computingu. Spotřebitel služeb cloud computingu službu vybírá z katalogu služeb poskytovatele, žádá příslušnou službu, ustanovuje smlouvu o poskytování služby a o úrovni služby s poskytovatelem služeb cloud computingu a užívá danou službu a platí poskytovateli služeb cloud computingu v závislosti na jejím využití“* (NIST, 2013).
Veřejný cloud computing		Služby v modelu veřejného cloud computingu jsou poskytovány širokému počtu spotřebitelů. Poskytovatel je obvykle externí společnost, což znamená, že služby cloud computingu jsou dodávány prostřednictvím třetí strany.
The Control Objectives for Information and Related Technology	COBIT	COBIT je rámec pro oblast governance a managementu informačních technologií založený na souboru dobrých praktik (ISACA, 2012c). COBIT v aktuální verzi 5 je založen na pěti klíčových principech, kterými jsou uspokojení potřeb a tvorba přidané hodnoty zainteresovaným stranám, zabezpečení komplexního celopodnikového řízení, použití jednotného integrovaného rámce, aplikace holistického přístupu a oddělení governance od managementu (ISACA, 2012c).

Seznam zkratek

API – Application Programming Interface (aplikační programovací rozhraní)

APO – Align, Plan, Organise

APT – Advanced Persistent Threat

BAI – Build, Acquire, Implement

CAPEX – Capital Expenditure (kapitálové náklady)

CCGM – Cloud computing governance a management

CIO – Chief Information Officer

CMMI – Capability Maturity Model Integration

COBIT – Control Objectives for Information and Related Technology

CSA – Cloud Security Alliance

DDoS – Distributed denial of service (distribuované odepření služby)

DSS – Deliver, Service, Support

ENISA – European Network and Information Security Agency (Evropská agentura pro bezpečnost sítí a informací)

IaaS – Infrastructure as a service (infrastruktura jako služba)

IRR – Internal Rate of Return (vnitřní výnosové procento)

ISMS – Information Security Management Systém (Systém řízení bezpečnosti informací)

ISO – Mezinárodní organizace pro normalizaci

IT – Informační technologie

ITSM – Information technology service management

MBI – Management Byznys Informatiky

MEA – Monitor, Evaluate, Assess

NIST – National Institute of Standards and Technology

NPV – Net Present Value (čistá současná hodnota)

OPEX – Operating Expenditures (provozní náklady)

PaaS – Platform as a service (platforma jako služba)

PP – Payback Period (doba splácení)

ROI – Return on Investment (návratnost investice)

ROSI – Return On Security Investment (návratnost investice do bezpečnosti)

SaaS – Software as a Service (software jako služba)

SLA – Service Level Agreement (dohoda o úrovni služeb)

SLO – Service Level Objectives (cíle úrovně služby)

SOA – Servisně orientovaná architektura

TCO – Total Cost of Ownership (celkové náklady na vlastnictví)

12 Seznam obrázků

13 Seznam tabulek

14 Příloha A: Cloud computing management role a odpovědnosti

Příloha A popisuje jednotlivé role v rámci řízení životního cyklu služby cloud computingu včetně definice jejich základních odpovědností.

Chief Information Officer (CIO)

Popis role: CIO navrhuje a realizuje cloud computing strategii v souladu s IT strategií a byznys strategií s cílem umožnit byznysu dosažení strategických a provozních cílů využitím služeb cloud computingu. Řídí a kontroluje IT aktiva, IT zdroje, IT schopnosti a kapacity s cílem zvýšit provozní efektivitu využívaných služeb při minimalizaci nákladů a rizik s nimi souvisejícími.

CIO odpovídá zejména za:

- realizace cloud computing strategie,
- připravenost organizace pro přijetí služeb cloud computingu,
- realizace systému pro řízení životního cyklu služby cloud computingu,
- zvládání rizik vyplývajících z využívání služeb cloud computingu,
- realizace portfolia poskytovatelů služeb cloud computingu,
- realizace portfolia služeb cloud computingu,
- finanční plánování využívání služby cloud computingu,
- realizace a udržování cloud computing management struktury,
- realizace exit strategie.

Cloud computing analytik

Popis role: Cloud computing analytik přezkoumává a analyzuje byznys záměry a požadavky a potřeby byznys procesů s cílem identifikovat změny, které vedou ke zlepšení výkonnosti podnikání. Cloud computing analytik za tímto účelem provádí analýzu a logický návrh informačního systému podniku na základě byznys požadavků. Analyzuje, navrhuje, modeluje a optimalizuje byznys procesy a definuje jejich podporu prostřednictvím služeb cloud computingu. Zabývá se identifikací efektů z využití služeb cloud computingu a spolupracuje s projektovým týmem při plánování a realizaci projektu adopce služby cloud computingu.

Cloud computing analytik odpovídá zejména za:

- analýza byznys požadavků na funkcionalitu služby cloud computingu,
- zdokumentování obchodního případu a opodstatněnosti využití služby cloud computingu,
- provedení technické studie proveditelnosti využití služby cloud computingu.

Manažer řízení rizik cloud computingu

Popis role: Manažer řízení rizik cloud computingu realizuje aktivity řízení rizik vyplývající z využití služeb cloud computingu s cílem optimalizovat toto riziko na úroveň, která je pro podnik akceptovatelná. Manažer řízení rizik cloud computingu posuzuje a analyzuje jednotlivá rizika z využití služeb cloud computingu, navrhuje opatření k minimalizaci potenciálních rizik, kontroluje ochranná a zabezpečovací opatření a vypracovává související dokumentaci.

Manažer řízení rizik cloud computingu odpovídá zejména za:

- posuzování rizik vyplývajících z využívání služeb cloud computingu včetně identifikace, analýzy a hodnocení rizik,
- identifikace a ohodnocení klíčových aktiv z hlediska rizik z využívání služeb cloud computingu,

- tvorba pravidelných zpráv o posuzování rizik z využívání služeb cloud computingu,
- sběr dat a hodnocení reportů o bezpečnostních incidentech,
- návrh, realizace a posouzení účinnosti opatření ke snížení významnosti rizika,
- tvorba, udržování a komunikace interních standardů pro řízení rizik z využívání služby cloud computingu a budování povědomí o rizicích vyplývajících z využívání služeb cloud computingu,
- podílení se na přípravě školících materiálů a podkladů pro interní bezpečnostní školení,
- podpora hodnocení a výběru poskytovatelů služeb cloud computingu,
- podpora hodnocení a výběru služeb cloud computingu,
- podpora při realizaci interního auditu,
- podpora při návrhu pohotovostních plánů a při plánování exit strategie.

Finanční manažer služeb cloud computingu

Popis role: Finanční manažer služeb cloud computingu plánuje, řídí, koordinuje a hodnotí aktivity IT oddělení při využívání služeb cloud computingu a zodpovídá za tvorbu finančních analýz, rozpočtování a účetnictví ve vztahu k využití služeb cloud computingu.

Finanční manažer služeb cloud computingu odpovídá zejména za:

- tvorba a udržování finančních modelů pro analýzy nákladů a přínosů souvisejících s využíváním služeb cloud computingu a pro hodnocení efektivnosti vložených nákladů do využívání služby cloud computingu,
- realizace nákladových analýz využívání služby cloud computingu,
- finanční plánování a odpovědnost za sestavování rozpočtů pro zavedení služby cloud computingu, pro provoz a pro ukončení využívání služby cloud computingu,
- kontrola skutečně vynaložených nákladů a jejich srovnání s rozpočtem,
- odpovědnost za řízení fakturace využívání služby cloud computingu,
- hodnocení efektivnosti investic do využívání služby cloud computingu,
- analýza smluv o poskytování služeb cloud computingu z hlediska finančního plnění,
- podpora plánování exit strategie a koordinace finančních postupů v případě realizace exit strategie.

Manažer pro řízení souladu služeb cloud computingu s legislativou

Popis role: Manažer pro řízení souladu služeb cloud computingu s legislativou zajišťuje, že služby cloud computingu jsou využívány v souladu s interními standardy a normami, s legislativními a regulatorními předpisy a smluvními požadavky.

Manažer pro řízení souladu služeb cloud computingu s legislativou odpovídá zejména za:

- definice a realizace postupů pro zajištění souladu využívaných služeb cloud computingu s interními standardy a normami, s legislativními a regulatorními předpisy a smluvními požadavky,
- definice, hodnocení a udržování aktuálnosti požadavků na využívání služeb cloud computingu vyplývajících z interních standardů a norem, z legislativních a regulatorních předpisů a ze smluv,
- identifikace a hodnocení klíčových oblastí využívání služeb cloud computingu z hlediska dodržování souladu s interními standardy a normami, s legislativními a regulatorními předpisy a smluvními požadavky,

- tvorba analýz a hodnocení plnění požadavků vyplývajících z interních standardů a norem, z legislativních a regulatorních předpisů a ze smluv,
- posuzování dodržování souladu s legislativou poskytovateli při analýze a hodnocení poskytovatelů služeb cloud computingu,
- analýza smluv o poskytování služeb cloud computingu z hlediska plnění legislativy,
- plánování komunikace požadavků vyplývajících z interních standardů a norem, z legislativních a regulatorních předpisů a ze smluv zainteresovaným stranám,
- podpora při analýze rizik vyplývajících z využití služby cloud computingu, podpora při uzavírání smluv o poskytování služby cloud computingu, podpora plánování exit strategie.

Manažer cloud exit strategie

Popis role: Manažer cloud exit strategie zodpovídá za plánování, definici a realizaci exit strategie pro případ ukončení využívání služby cloud computingu.

Manažer cloud exit strategie odpovídá zejména za:

- tvorba plánů exit strategie služby cloud computingu,
- definice exit strategie služby cloud computingu v SLA,
- koordinaci aktivit a zdrojů potřebných pro plánování a realizaci exit strategie služby cloud computingu,
- realizace exit strategie služby cloud computingu,
- koordinace aktivit jednotlivých týmů a rolí při plánování a realizaci exit strategie cloud computingu.

Manažer portfolia poskytovatelů a řízení vztahu s poskytovateli

Popis role: Manažer portfolia poskytovatelů je zodpovědný za budování a udržování vztahů s předem schválenými poskytovateli služeb cloud computingu a hodnotí poskytovatele vzhledem k požadavkům byznysu a dodržování smluvních závazků. Provádí analýzu a výběr poskytovatelů s cílem jejich případného schválení a zařazení do portfolia poskytovatelů.

Manažer portfolia poskytovatelů odpovídá zejména za:

- návrh strategie hodnocení a výběru poskytovatelů služeb cloud computingu,
- analýza trhu služeb cloud computingu z hlediska jejich poskytovatelů,
- realizace hodnocení a výběr poskytovatele služeb cloud computingu,
- vytváření, udržování, rozvoj a ukončení vztahu s poskytovatelem služeb cloud computingu,
- sledování výkonnostních charakteristik poskytovatelů služeb cloud computingu, periodické hodnocení poskytovatelů v portfoliu poskytovatelů služeb cloud computingu z hlediska souladu s požadavky na poskytovatele služeb cloud computingu,
- správa databáze poskytovatelů služeb cloud computingu,
- plánování komunikační strategie, komunikace s poskytovateli služeb cloud computingu, řízení interakcí mezi relevantním IT personálem zabezpečujícím provoz služby cloud computingu a poskytovatelem služeb cloud computingu,
- podpora hodnocení rizik souvisejících s využíváním služby computingu od daného poskytovatele, podpora plánování exit strategie, podpora plánování výběru služby cloud computingu, podpora plánování SLA.

Manažer katalogu služeb cloud computingu

Popis role: Manažer katalogu služeb cloud computingu je odpovědný za vytvoření a správu portfolia služeb cloud computingu, a to jak aktuálně využívaných, tak i potenciálních služeb cloud computingu a zodpovídá za rozvoj, podporu a správu katalogu služeb cloud computingu.

Manažer Katalogu služeb cloud computingu odpovídá zejména za:

- vytvoření a udržování katalogu služeb spotřebitele služeb cloud computingu,
- přesnost a aktuálnost dat v katalogu služeb spotřebitele služeb cloud computingu,
- periodické hodnocení služeb v portfoliu služeb cloud computingu z hlediska souladu s požadavky na službu cloud computingu,
- podpora hodnocení rizik souvisejících s využíváním služby computingu,
- podpora pro týmy zabezpečující provoz služby cloud computingu.

Cloud SLA manažer

Popis role: Cloud SLA manažer identifikuje požadavky na smlouvy o poskytování služby cloud computingu v souladu s byznys potřebami, v součinnosti s poskytovatelem služeb cloud computingu sjednává podmínky uzavření smlouvy o poskytování služby cloud computingu, rozvíjí, provádí a zpřesňuje postupy pro hodnocení smluvních podmínek a zajišťuje, že všechny smlouvy o poskytování služby cloud computingu jsou dodržovány a splňují minimální požadavky na podporu byznys procesů při současné minimalizaci rizik z nich vyplývajících.

Cloud SLA manažer odpovídá zejména za:

- definice návrhu smluv o poskytování služby cloud computingu,
- definice úrovně kvality služby cloud computingu potřebné pro zajištění byznys potřeb,
- smluvní jednání s poskytovatelem služeb cloud computingu,
- vyjednávání, správa, prodloužení a ukončení smluv o poskytování služby cloud computingu,
- sledování narušení podmínek smluv o poskytování služby cloud computingu,
- vymáhání povinností a práv vyplývajících ze smluv o poskytování služby cloud computingu a řešení sporů s poskytovatelem služby cloud computingu.

Manažer služeb cloud computingu

Popis role: Manažer služeb cloud computingu zajišťuje, že vybraná služba cloud computingu bude naplňovat požadavky byznys potřeb s důrazem na tvorbu hodnoty služby cloud computingu pro byznys. Manažer služeb cloud computingu realizuje aktivity hodnocení a výběru služby cloud computingu.

Manažer služeb cloud computingu odpovídá zejména za:

- návrh strategie hodnocení a výběru služeb cloud computingu,
- analýza trhu služeb cloud computingu,
- realizace hodnocení a výběru služby cloud computingu,
- podpora plánování SLA,
- podpora při analýze rizik vyplývajících z využití služby cloud computingu

Manažer přechodu na využití služby cloud computingu

Popis role: Manažer přechodu na využití služby cloud computingu řídí a koordinuje aktivity a potřebné IT, personální a finanční zdroje v souvislosti s projektem přechodu na využití služby cloud computingu.

Manažer přechodu na využití služby cloud computingu odpovídá zejména za:

- plánování projektu přechodu služby cloud computingu do produktivního provozu,
- posouzení priorit a dopadu všech souvisejících aktivit s plánováním přechodu služby do produktivního provozu,
- řízení a koordinace postupů, aktivit a zdrojů souvisejících s plánováním přechodu služby do produktivního provozu,
- dokumentace všech postupů, aktivit a zdrojů souvisejících s plánováním přechodu služby do produktivního provozu,
- přezkoumání plánů přechodu služby cloud computingu do produktivního provozu.

Cloud test manager

Popis role: Cloud test manager zajišťuje plánování a provádění testů souvisejících s adopcí služby cloud computingu. Vyhodnocuje výsledky testů z hlediska funkcionality, výkonnosti a kompatibility služby cloud computingu v plánovaném provozním prostředí.

Cloud test manager odpovídá zejména za:

- tvorba metodiky testování služeb cloud computingu
- návrh a realizace testů, příprava testovacích případů a testovacích dat v testovacím prostředí poskytovatele služeb cloud computingu, dokumentování provedených testů,
- testování výkonu a zátěže služeb cloud computingu při podpoře kritických byznys transakcí,
- sledování chyb, analýza chyb, hlášení problémů a komunikace s poskytovatelem služeb cloud computingu
- validace výsledků testování,
- komunikace výsledků testů zainteresovaným stranám.

Manažer pro řízení přístupu ke službě

Popis role: Manažer pro řízení přístupu ke službě spravuje a podporuje uživatelské účty a oprávnění přistupovat a využívat funkcionalitu služby cloud computingu.

Manažer pro řízení přístupu ke službě odpovídá zejména za:

- tvorba metodiky pro přístup ke službám cloud computingu,
- definice administrátorských oprávnění k vytvoření uživatelů a definice profilů oprávnění uživatelů pro práci se službou cloud computingu,
- přiřazení, změna nebo odebrání oprávnění uživatelům služby cloud computingu,
- zablokování nebo zrušení přístupu ke službě cloud computingu,
- tvorba doporučení týkajících se přístupové bezpečnosti.

Manažer nasazení služeb cloud computingu

Popis role: Manažer nasazení služeb cloud computingu je odpovědný za plánování a koordinaci aktivit a zdrojů nutných pro nasazení služby cloud computingu do produktivního provozu v produkčním prostředí spotřebitele, provádí dokumentaci nasazení služby, poskytuje technické a aplikační poradenství a podporu během celého procesu nasazení služby a poskytuje zpětnou vazbu o efektivitě nasazení služby cloud computingu do produktivního provozu.

Manažer nasazení služeb cloud computingu odpovídá zejména za:

- realizace exportu dat z interního systému spotřebitele služby cloud computingu, transformace dat, realizace importu dat do produktivního prostředí poskytovatele služeb cloud computingu,

- komunikace s poskytovatelem služeb cloud computingu a s ostatními účastníky projektu,
- identifikace potenciálních problémů a stanovení vhodných opatření,
- návrh a dokumentace pohotovostních plánů pro případ výskytu kritických událostí během fáze přechodu,
- vyhodnocení úspěšnosti přechodu služby cloud computingu do produktivního provozu.

Cloud servis desk manažer

Popis role: Cloud servis desk manažer zajišťuje provoz service desku, přijímání, vyhodnocování a komunikování událostí, incidentů, problémů a uživatelských požadavků vznikajících při využívání služby cloud computingu a eskalaci relevantních informací poskytovateli služby cloud computingu.

Cloud servis desk manažer odpovídá zejména za:

- řízení každodenních činností související s provozem služby cloud computingu,
- přijímání hlášených událostí, incidentů, problémů a požadavků na službu cloud computingu,
- poskytování informací o stavu plnění SLA,
- identifikace odchylek od očekávaného stavu služby cloud computingu a řešení detekovaných odchylek provozu služby cloud computingu,
- řízení tiketů,
- provádění eskalace na technickou či operační podporu nebo podporu poskytovatele služby cloud computingu v případě potřeby,
- komunikace s poskytovatelem služby a přijímání informací o vyřešení eskalovaných odchylek provozu služby cloud computingu,
- poskytování informací o výpadku služby cloud computingu a jiných mimořádných událostech,
- poskytování údajů o klíčových výkonnostních ukazatelích servis desku a trendu jejich vývoje.

Cloud eskalační manažer

Popis role: Cloud eskalační manažer řídí eskalaci informací týkajících se narušení provozu služeb cloud computingu mající podstatný vliv na provádění byznys procesů a na kontinuitu byznysu relevantním stranám spotřebitele a poskytovatele služby cloud computingu.

Cloud eskalační manažer odpovídá zejména za:

- eskalace incidentů, výpadků a problémů služby cloud computingu s vysokou prioritou, které jsou kritické z hlediska podpory byznys procesů službou cloud computingu,
- koordinace a posouzení obsahu a míry kritičnosti eskalací,
- komunikace s interními zúčastněnými stranami spotřebitele služeb a s poskytovatelem služby cloud computingu s cílem eliminovat vliv narušení provozu služby cloud computingu na byznys a obnovit normální provoz služby.

Manažer provozu služeb cloud computingu

Popis role: Manažer provozu služeb cloud computingu zajišťuje řízení událostí vzniklých v souvislosti s provozem a využíváním jednotlivých služeb cloud computingu a související infrastruktury.

Manažer provozu služeb cloud computingu odpovídá zejména za:

- přijetí tiketu o vzniku události v souvislosti s provozem služby cloud computingu,
- zpracování a řešení události vzniklé v souvislosti s provozem služby cloud computingu,
- uzavření zpracované události a vrácení tiketu na servis desk,
- koordinace mezi procesem řízení událostí a ostatními procesy fáze provozu služby cloud computingu.

Cloud incident manažer

Popis role: Cloud incident manažer řídí proces řízení incidentů v souvislosti s provozem služby cloud computingu, provádí analýzu příčin vzniku incidentu, analyzuje dopad incidentu na byznys a připravuje potřebné požadavky na změnu s cílem vyřešit a uzavřít incident.

Cloud incident manažer odpovídá zejména za:

- prvotní identifikace a analýza příčiny vzniku incidentu vzniklého v souvislosti s provozem služby cloud computingu,
- kategorizace a prioritizace incidentu vzniklého v souvislosti s provozem služby cloud computingu,
- určení rizik souvisejících se vznikem incidentu,
- diagnóza a řešení incidentu vzniklého v souvislosti s provozem služby cloud computingu,
- eskalace incidentu vzniklého v souvislosti s provozem služby cloud computingu cloud eskalačnímu manažerovi.

Cloud problém manažer

Popis role: Cloud problém manažer řídí proces řízení problémů v souvislosti s provozem služby cloud computingu, provádí analýzu konkrétních incidentů s cílem identifikovat prvotní příčinu a připravuje potřebné požadavky na změnu s cílem vyřešit problém.

Cloud problém manažer odpovídá zejména za:

- identifikace problému vzniklého v souvislosti s provozem služby cloud computingu,
- zdokumentování problému, kategorizace a prioritizace problému,
- diagnóza příčin problému a stanovení dočasného řešení,
- analýza prvotních příčin problému, uplatňování společného přístupu k analýze prvotních příčin,
- odstranění příčiny a vyřešení problému,
- koordinace mezi procesem řízení problémů a ostatními procesy fáze provozu služby cloud computingu,
- hodnocení řešení známých chyb, komunikace s cloud incident manažerem, společné odsouhlasení dočasného řešení,
- dohled nad změnami nezbytnými k provedení nápravných opatření pro znovuobnovení očekávaného stavu provozu služby cloud computingu,
- tvorba a aktualizace databáze problémů vzniklých v souvislosti s provozem služby cloud computingu,
- koordinace problémů služby cloud computingu s vysokou prioritou, které jsou kritické z hlediska podpory byznys procesů službou cloud computingu,
- komunikace s poskytovatelem služby cloud computingu.

Manažer řízení požadavků na službu cloud computingu

Popis role: Manažer řízení požadavků na službu cloud computingu přijímá, vyhodnocuje a zpracovává požadavky uživatelů na službu cloud computingu včetně analýzy jejich dopadu na byznys.

Manažer řízení požadavků na službu cloud computingu odpovídá zejména za:

- validace požadavku na službu cloud computingu,
- kategorizace a prioritizace požadavku na službu cloud computingu,

- analýza realizovatelnosti požadavku na službu cloud computingu vzhledem k smlouvám o poskytování služeb,
- analýza dopadu požadavku na službu cloud computingu na byznys procesy,
- stanovení způsobu realizace požadavku na službu cloud computingu.

Manažer řízení požadavků na přístup ke službě cloud computingu

Popis role: Manažer řízení požadavků na přístup ke službě cloud computingu poskytuje pomoc, informace a podporu uživatelů v rámci celé organizace při řešení požadavků na přístup ke službě cloud computingu.

Manažer řízení požadavků na přístup ke službě odpovídá zejména za:

- podpora uživatelů služby cloud computingu ve vztahu k jejich oprávnění přístupu k funkcionalitám služby,
- přijetí požadavku na přístup ke službě cloud computingu a jeho zdokumentování,
- verifikace a validace požadavku na přístup ke službě cloud computingu,
- řešení požadavků a problémů týkajících se přístupu ke službě cloud computingu,
- komunikace s Manažerem pro řízení přístupu ke službě.

Cloud monitoring manažer

Popis role: Cloud monitoring manažer navrhuje a implementuje techniky a nástroje monitorování a reportování s cílem identifikovat, zda využívané a aktuálně provozované služby cloud computingu jsou dodávané na úrovni dohodnuté s poskytovatelem služby cloud computingu v SLA.

Cloud monitoring manažer odpovídá zejména za:

- definice požadavků na monitorování parametrů služby cloud computingu v součinnosti s relevantními pracovníky poskytovatele a spotřebitele služby,
- analýza dat o provozu služby cloud computingu,
- stanovení limitních hodnot úrovní metrik služeb cloud computingu, při kterých má být oznámena odchylka,
- eskalace detekovaných odchylek formou vytvoření událostí.

Manažer nepřetržitého zdokonalování služby cloud computingu

Popis role: Manažer nepřetržitého zdokonalování služby cloud computingu realizuje aktivity vedoucí ke zlepšení služeb cloud computingu v rámci životního cyklu služby cloud computingu a hledá příležitost ke zlepšení výkonnosti služby cloud computingu tak, aby služba umožňovala realizovat požadovanou byznys hodnotu. Dále zajišťuje, že strategie nepřetržitého zdokonalování služby cloud computingu je definovaná a související procesy, plány a postupy jsou vytvořeny, implementovány a udržovány.

odpovídá zejména za:

- definice strategie nepřetržitého zdokonalování služby cloud computingu a sdílení vize nepřetržitého zdokonalování služby cloud computingu v rámci organizace,
- definice plánu monitorování služby cloud computingu vzhledem k požadavkům byznysu,
- analýza monitorovaných dat,
- koordinace identifikace a sledování příležitostí pro zdokonalování služby cloud computingu,
- vyhodnocení a návrh doporučení pro zlepšení výkonnosti služby cloud computingu,
- kooperace s manažerem cloud exit strategie a SLA manažerem.

15 Příloha B: Výsledky dotazníkového šetření hodnocení navrženého metodického rámce CCGM

Prvním krokem při tvorbě dotazníku bylo stanovení cíle dotazníku. Cílem dotazníku bylo zjistit správnost, úplnost, srozumitelnost a využitelnost navrženého metodického rámce CCGM a jeho metodických prvků (principů, procesů a rolí). Dále šetření sledovalo, zda metodický rámec CCGM umožnuje efektivně řešit problémy governance a managementu využívání služby cloud computingu z pohledu spotřebitele. Dotazník byl omezen na odborné IT pracovníky IT organizace, kteří se účastnili projektu popsaného v rámci realizace případové studie v kapitole 8. Dotazník byl respondentům doručen prostřednictvím emailu. Jako hodnotící škála pro měření postojů dotazovaných respondentů vůči výrokům byla v dotazníku použita pětistupňová Likertova škála: Naprosto souhlasím, Spíše souhlasím, Nevím, Spíše nesouhlasím, Naprosto nesouhlasím.

Tabulka 53: Výstupy z dotazníkového šetření, zdroj: (autor)

		Vedoucí oddělení IT governance	IT governance specialist	Procesní analytik	IT analytik	Vedoucí týmu IT služby	Vedoucí oddělení řízení provozu IT	Vedoucí týmu IT projekt management
1	Metodický rámec CCGM je pochopitelný a implementovatelný.	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím
2	Cíle, rozsah a struktura metodického rámce CCGM jsou jasně a srozumitelně definovány.	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Spíše souhlasím	Naprosto souhlasím	Naprosto souhlasím	Spíše souhlasím
3	Metodické prvky (principy, procesy a role) metodického rámce CCGM jsou jasně, srozumitelně a korektně definovány.	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Spíše souhlasím	Nevím	Nevím	Spíše souhlasím
4	Metodický rámec CCGM poskytuje potřebné metodiky umožňující zabezpečit efektivní adopci a využívání služby cloud computingu v souladu s byznys požadavky při minimalizaci nákladů a rizik.	Naprosto souhlasím	Spíše souhlasím	Naprosto souhlasím	Spíše souhlasím	Spíše souhlasím	Naprosto souhlasím	Spíše souhlasím
5	Metodický rámec CCGM pokrývá aspekty governance služeb cloud	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Nevím	Nevím	Nevím

		Vedoucí oddělení IT governance	IT governance specialist	Procesní analytik	IT analytik	Vedoucí týmu IT služby	Vedoucí oddělení řízení provozu IT	Vedoucí týmu IT projekt management
	computingu.							
6	Metodický rámec CCGM pokrývá aspekty managementu služeb cloud computingu.	Naprosto souhlasím	Spíše souhlasím	Spíše souhlasím	Naprosto souhlasím	Spíše souhlasím	Naprosto souhlasím	Spíše souhlasím
7	Metodický rámec CCGM poskytuje dostatečnou flexibilitu při návrhu governance a managementu služeb cloud computingu v organizaci.	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím
8	Rozhraní mezi cloud computing governance a cloud computing management je jasně definováno.	Naprosto souhlasím	Naprosto souhlasím	Spíše souhlasím	Spíše souhlasím	Nevím	Nevím	Spíše souhlasím
9	Cloud computing governance napomáhá definovat rozhodovací proces, pravidla a omezení, které na strategické úrovni spravují a ovládají využívání služeb cloud computingu s cílem dosažení potřeb byznysu.	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Nevím	Nevím	Nevím
10	Cloud computing management pokrývá životní cyklus služby cloud computingu.	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím
11	Cloud computing management umožňuje zabezpečit dodání požadovaného objemu služby při daných výkonnostních parametrech a při dané ceně v souladu se strategickými požadavky na službu.	Spíše souhlasím	Naprosto souhlasím	Spíše souhlasím	Naprosto souhlasím	Spíše souhlasím	Spíše nesouhlasím	Spíše souhlasím
12	Procesy metodického rámce CCGM umožňují řešení reálných problémů a umožňují dodání specifických výsledků	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím

		Vedoucí oddělení IT governance	IT governance specialist	Procesní analytik	IT analytik	Vedoucí týmu IT služby	Vedoucí oddělení řízení provozu IT	Vedoucí týmu IT projekt management
	řešení těchto problémů.							
13	Procesy cloud computing governance jsou definovány korektně a na potřebné úrovni detailu.	Naprosto souhlasím	Naprosto souhlasím	Spíše souhlasím	Naprosto souhlasím	Nevím	Nevím	Nevím
14	Procesy cloud computing governance umožňují realizaci modelu governance služeb cloud computingu v konkrétním podniku a zahrnují praktiky a aktivity zaměřené na dosahování cílů IT governance, které určují směr využívání služeb cloud computingu, a umožňují monitorování výstupů.	Naprosto souhlasím	Spíše souhlasím	Naprosto souhlasím	Spíše souhlasím	Nevím	Nevím	Nevím
15	Procesy cloud computing management jsou definovány korektně a na potřebné úrovni detailu.	Naprosto souhlasím	Naprosto souhlasím	Spíše souhlasím	Naprosto souhlasím	Spíše souhlasím	Naprosto souhlasím	Spíše souhlasím
16	Procesy fáze (CM1) Strategie využití služeb cloud computingu zabezpečují realizaci IT strategie prostřednictvím definice interních a externích požadavků, které musí služby cloud computingu splňovat při optimální úrovni nákladů a výši rizika, a dále zabezpečují vytvoření, udržování a ukončení smluvního vztahu s poskytovatelem služeb cloud computingu a vytvoření a udržování portfolia dostupných služeb cloud computingu splňujících potřeby byznysu a externích požadavků.	Naprosto souhlasím	Spíše souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Nevím	Spíše souhlasím

		Vedoucí oddělení IT governance	IT governance specialist	Procesní analytik	IT analytik	Vedoucí týmu IT služby	Vedoucí oddělení řízení provozu IT	Vedoucí týmu IT projekt management
17	Proces fáze (CM2) Výběr služby cloud computingu zabezpečuje aktivity související s výběrem služby cloud computingu, která v optimální míře splňují požadavky vyplývající z předchozí fáze CM1 s důrazem na hodnotu pro byznys.	Naprosto souhlasím	Naprosto souhlasím	Spíše souhlasím	Spíše souhlasím	Naprosto souhlasím	Nevím	Spíše souhlasím
18	Procesy fáze (CM3) Přechod na využívání služby cloud computingu zabezpečují efektivní a účinné plánování nasazení služby cloud computingu o očekávané úrovni kvality do produktivního provozu při naplnění požadavků na službu vyplývajících z fází CM1 a CM2.	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím
19	Procesy fáze (CM4) Provoz služby cloud computingu zabezpečují koordinaci a provádění aktivit potřebných pro sledování výkonnosti služeb cloud computingu, pro realizaci sběru provozních metrik používaných k hodnocení kvalitativní úrovně služeb a pro identifikaci odchylek hodnot metrik od požadovaného stavu, dále zabezpečují že přístup ke službám je umožněn pouze oprávněným uživatelům a že služba uspokojuje potřeby těchto uživatelů vzhledem k plnění jejich pracovního zařazení.	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím

		Vedoucí oddělení IT governance	IT governance specialist	Procesní analytik	IT analytik	Vedoucí týmu IT služby	Vedoucí oddělení řízení provozu IT	Vedoucí týmu IT projekt management
20	Proces fáze (CM5) Nepřetržité zdokonalování služby cloud computingu zabezpečuje, že využívaná služba cloud computingu bude neustále a optimálním způsobem podporovat realizaci byznys procesů, a to jak z hlediska její účinnosti, tak i nákladové efektivity a přijatelné míry rizika.	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím
21	Metodický rámec CCGM jasně stanovuje role a odpovědnosti ve vztahu k procesům.	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Naprosto souhlasím	Spíše souhlasím	Naprosto souhlasím	Naprosto souhlasím
22	Metodický rámec CCGM umožňuje zúčastnění všech zainteresovaných stran v rámci životního cyklu služby cloud computingu.	Spíše souhlasím	Spíše souhlasím	Nevím	Spíše souhlasím	Spíše souhlasím	Nevím	Spíše souhlasím