Systém interních kontrol v podnikové architektuře

Martin Tománek a Jiří Voříšek
Vysoká škola ekonomická v Praze
Fakulta informatiky a statistiky
nám. W. Churchilla 4
130 67 Praha 3
Česká republika
e-mail: xtomm28@vse.cz , vorisek@vse.cz

Abstrakt:*V dnešní turbulentní době je důležité, aby společnosti dokázaly pružně a efektivně reagovat na změny v prostředí. Velké společnosti jsou však natolik komplexními systémy, že procesní, organizační změny a změny IT architektury jsou velice náročné a často nepřinášejí očekávané přínosy. K řízení této komplexity se využívá poznatků z architektury, nazývané podniková architektura. Pro efektivní řízení IT nabírá na významu koncept IT Governance, který se zabývá mj. interními kontrolami. Tato práce se zabývá propojením poznatků z podnikové architektury a z IT Governance a návrhem interních kontrol v podnikové architektuře, které vhodně doplní současnou literaturu i praxi.*

Klíčová slova: Podniková architektura, interní kontroly, COBIT, TOGAF, IT Governance, audit, architektura informačních systémů, audit podnikové architektury

Abstract: *In order the enterprise architecture delivers the expected benefits the IT Governance and Architecture Governance must be in place. The main task of the IT and Architecture Governance is to establish internal controls in the enterprise architecture. These internal controls described in the current literature are focused mainly on enterprise architecture definition, content and roles. From author's point of view the focus should be concentrated more on IT investment process (control EA1), alignment of IT projects with enterprise architecture (control EA2) and use of enterprise architecture repository as a strategic communication tool (control EA3).*

Keywords: Enterprise Architecture, COBIT, TOGAF, IT Governance, information systems architecture, Enterprise Architecture audit

1. Úvod

Pojmy podniková architektura (Enterprise Architecture, EA), IT Governance a systém interních kontrol se v dnešní době používají často, přičemž definice těchto pojmů není ustálená a lidé si je vykládají různými způsoby. Tato práce objasňuje tyto pojmy, jejich vzájemné vztahy, použití a přínosy. K vysvětlení a objasnění těchto pojmů práce vychází z nejlepších současných praktik zabývajících se danou problematikou. Pro objasnění konceptu podnikové architektury práce vychází z architektonického rámce TOGAF verze 9 (Open Group, 2009), v případě IT Governance a systému interních kontrol je východiskem auditorský rámec COBIT verze 4.1 (IT Governance Institute 2007a).

Podniková architektura se zabývá analýzou současného stavu organizace, vytvářením cílového stavu organizace, který odráží strategické a podnikové požadavky, a návrhem, jak se k cílovému stavu organizace efektivně dostat.

Systém interních kontrol je součástí IT Governance, kde cílem je zajistit, aby v organizaci existovaly takové mechanismy, které vedou k efektivnímu využívání IT zdrojů a k zajištění, že řízení IT je v souladu s mezinárodními standardy.

Systém interních kontrol v podnikové architektuře má tedy za úkol zajistit, že zdroje určené pro podnikovou architekturu jsou efektivně vynaloženy a že podniková architektura přispívá k realizaci celopodnikových cílů. Interní kontroly jsou důležité z důvodu, že většinou není problém s obsahem podnikové architektury, ale problém bývá s její implementací, užitím a reálnými přínosy. Interní kontroly by se tedy měly zaměřit na tento aspekt podnikové architektury. Pro ohodnocení současných interních kontrol a k identifikaci mezer se používá audit podnikové architektury, který má za úkol zjistit, zdali je IT v organizaci správně řízeno (Brown 2011).

Proč je vlastně kladen stále větší důraz na systém interních kontrol a podnikovou architekturu? Sarbanes-Oxley Act (SOX) (Sarbanes-Oxley, 2002) určuje osobní odpovědnost vedení firmy veřejných i neveřejných organizací za zavedení a udržování adekvátního systému interních kontrol a směrnic pro finanční řízení organizací. Podniková architektura svým pokrytím umožňuje porozumět podniku a za její pomoci zavést systém interních kontrol. Avšak podniková architektura je v praxi stále brána jako problém IT oddělení a kontrolní mechanismy jsou tudíž vnímány také jako problémy výhradně týkající se IT. Kromě shody se zákonem SOX, (Winter, Schelp 2008) také rozvádí užití podnikové architektury jako zdroj informací pro zhodnocení souladu se Solvency II, Basel II, COSO a COBIT.

Systémem interních kontrol v podnikové architektuře se zabývá například (Finkelstein 2004), který k vytvoření podnikové architektury používá Zachmanův architektonický rámec, na kterém demonstruje modely vhodné pro zachycení požadavků na systém interních kontrol při navrhování procesů, dat, aplikací, řídicích struktur atd. Nicméně však také uvádí, že vrstva definující interní kontroly většinou chybí a tuto mezeru má podle jeho názoru vyřešit zákon SOX.

Definicí kontrol v podnikové architektuře se podrobně zabývá (Kyriazoglou 2010), který definuje kontroly pro: výběr rámce a definici EA, existenci plánu pro implementaci EA, existenci vhodné organizační struktury pro vývoj EA, formulaci a definici jednotlivých částí podnikové architektury.

V této práci budeme na audit podnikové architektury nahlížet skrz rámce COBIT v9 a TOGAF v4.1, které jsou v současné době označované jako nejlepší praktiky. *Cílem této práce je na základě komparativní analýzy těchto dvou rámců identifikovat další interní kontroly, které by vhodně doplnily kontroly popsané v současné literatuře. Jako největší nedostatek současných kontrol vidíme jejich zaměření na obsah architektury, a ne na architekturu jako na nástroj pro transformaci organizace a umožnění dosažení vytyčených strategických cílů.*

K dosažení cíle této práce budou nejdříve v druhé a třetí kapitole charakterizovány rámce TOGAF v9 a COBIT v4.1. Čtvrtá kapitola porovnává oba rámce a pátá kapitola na základě obou rámců a na základě modelu SPSPR (Voříšek a kol., 2008) navrhuje doplňující vnitřní kontroly v podnikové architektuře.

Práce byla vypracovaná v rámci řešení grantu GAČR P403-10-0092 „Advanced Principles and Models for Enterprise IT Management“ a GAČR P403-11-0574 „Enterprise Architecture frameworks in Cloud Computing environments“.

2. Podniková architektura (EA) a TOGAF

Architektura původně vznikla ve stavebnictví a to již v období starověkého Egyptu při stavění pyramid. Cílem stavitelské architektury je zajistit praktičnost a užitečnost stavby, statiku a stabilitu stavby a v neposlední řadě estetický vzhled stavby.

Na základě stavitelské architektury vzniká na přelomu 20. a 21. století (Zachman, 1987) nově i koncept, který je nazýván podniková architektura. Cíle této architektury jsou však oproti stavebnictví odlišné. Podle společnosti Gartner (Gartner 2012) je „*podniková architektura procesem efektivní transformace podnikové vize a mise do změny podniku pomocí vytváření, komunikování a zlepšování klíčových požadavků, principů a modelů, které popisují budoucí stav podniku a umožňují jeho vývoj*“.

V celé řadě případů (Kaoutar, Bounabat, 2010), (Winter, Schelp, 2008), (Scott, 2009) však EA slouží k propojení IT cílů s celopodnikovými cíli za účelem efektivnějšího, flexibilnějšího a transparentnějšího hospodaření s IT zdroji. Tohoto propojení je však obtížné dosáhnout z důvodu, že diskuze byznys a IT pracovníků se většinou soustředí kolem projektů, procesů nebo aplikací. Přičemž projekty jsou příliš krátkodobé, procesy jsou příliš detailní a diskuze kolem aplikací je příliš technicky zaměřená, takže jim byznys lidé nerozumí. Jako řešení (Scott, 2009) navrhuje vytvoření „Capability maps“ (mapy podnikových schopností), které jsou součástí byznys architektury a popisují schopnosti podniku, které jsou zapotřebí pro vytvoření či udržení konkurenční výhody podniku. Jiný přístup navrhuje (Voříšek a kol. 2008) v modelu SPSPR, který definuje zodpovědnosti jednotlivých typů manažerů (vrcholový management, vlastníci byznys procesů, CIO, střední a operativní IT management) za definici podnikových cílů a jejich podporu pomocí IT.

Cílem podnikové architektury je dále pružně reagovat na stále se měnící a vysoce konkurenční prostředí, kdy porozumění podniku a podnikovým schopnostem vede k lepšímu vyhodnocování a reakcím na příležitosti (Shields, 2011). Hybnou sílou transformace podnikové architektury jsou však implementační projekty, které reflektují dlouhodobé záměry firmy ve formě cílové architektury (Ross et al., 2006) a jsou v souladu s architektonickými principy (Hugoson et al., 2010). Pro řízení organizačních změn vidí (Shields, 2011) podnikovou architekturu a řízení projektového portfolia jako nejdůležitější prvek organizace.

Pro vytváření, implementaci a rozvoj podnikové architektury slouží architektonický rámec TOGAF. TOGAF (The Open Group Architecture Framework) je vlastněn a spravován konsorciem The Open Group. Toto neziskové konsorcium je tvořeno řadou expertů z celého světa. Mezi členy patří IT dodavatelé, IT odběratelé, poradenské firmy, vládní organizace a univerzity. Základní vizí tohoto konsorcia je „Boundaryless Information Flow™“ tedy bezbariérový tok informací uvnitř i vně organizací založený na otevřených standardech, globální výměně a využití informací. TOGAF definuje ADM (Architecture Development Method) jako procesní model sloužící pro vytvoření a řízení vývoje podnikové architektury. TOGAF v základní verzi popisuje vytvoření a řízení tří typů architektur: byznys architektura, architektura informačních systémů a technologická architektura. Architektura informačních systémů se dále dělí na aplikační a informační architekturu.

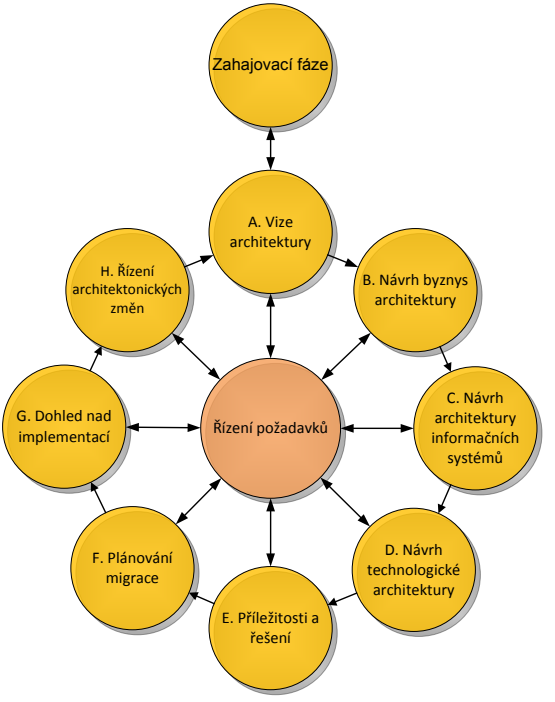
Podle (Voříšek et al., 2008) si „*významnou pozici mezi IT architekturami získává architektura IT služeb*“, protože vytváří rozhraní mezi byznys a IT architekturami a je komunikačním nástrojem mezi byznys a IT manažery.

Aziz et al., 2005 poukazuje na fakt, že většinou není problém s obsahem podnikových architektur, ale s řízením podnikové architektury, kdy je důležitá governance (dohled, řízení) nad vytvářením a používáním podnikové architektury. Mezi příčiny neúspěchů patří například: nedostatečná komunikace a propagace architektonických artefaktů, nevhodné umístění IT oddělení v organizaci a nedostatečné pravomoci, nedostatek zapojení vedoucích pracovníků atd.

2.1 Architecture Development Method (ADM)

Největší předností rámce TOGAF v9 je iterativní procesní model, který je znázorněn na obrázku 1. Samotné iterace (fáze) mohou probíhat jak na úrovni jednotlivých procesů, tak i mezi procesy, ale také v rámci celého procesního modelu za pomoci procesu řízení požadavků.

ADM se skládá z deseti fází, přičemž osm z nich tvoří jeho jádro (A-H). Proces vývoje podnikové architektury začíná v zahajovací fázi. Cyklus vývoje podnikové architektury navzájem spojuje proces řízení požadavků, který reflektuje neustálé změny v prostředí a měnící se požadavky zúčastněných stran. Díky tomuto procesu je možné se ve vývoji architektury vrátit o krok zpět či až na začátek vývoje.



Obrázek 1: Architecture Development Method (Open Group 2009), *přeloženo autory práce*

Zahajovací fáze

Na začátku vývoje podnikové architektury je zapotřebí porozumět konceptu celého podniku, podnikovým směrnicím a začlenění architektury do organizačního rámce. Dochází zde k identifikaci očekávaných potřeb a přínosů hlavních zúčastněných stran a sponzora architektury.

A. Vize architektury

Vize architektury popisuje přínosy architektury a požadované nové schopnosti podniku, které umožní dosáhnout podnikových strategických cílů. Nejdůležitějším úkolem je dosáhnout podpory managementu na všech úrovních, identifikace jejich záměrů a cílů. Vize architektury mimo jiné slouží i k ospravedlnění investic do architektury.

B. Návrh byznys architektury

Na základě vize architektury se popisuje současná a cílová byznys architektura. V této architektuře se úsilí byznys architektů soustředí na formulaci a dekompozici podnikové strategie založené na výrobcích anebo službách. Definují se organizační, funkční, procesní, informační a zeměpisné aspekty podnikání a jejich vzájemné vztahy. Důležitou činností je analýza rozdílů mezi současnou a cílovou byznys architekturou, která v dalších fázích povede k požadavkům na transformaci celého podniku.

C. Návrh architektury informačních systémů

Na základě navržené byznys architektury se odvozuje architektura informačních systémů, pod kterou se rozumí datová a aplikační architektura.

Aplikační architektura definuje hlavní druhy aplikací, které jsou zapotřebí pro zpracování dat a k IT podpoře podnikových procesů. Důležité je zachytit hlavní funkce a komponenty aplikací včetně datových objektů, které tyto aplikace spravují.

Smyslem datové architektury je nadefinování datových objektů, které jsou zapotřebí pro podporu byznys architektury a jsou popsané na takové úrovni, aby byly srozumitelné širokému spektru uživatelů.

D. Návrh technologické architektury

Technologická architektura vychází z architektury informačních systémů a dále ji rozpracovává do technologických komponent, jako je hardware a software dostupný na trhu anebo vyvinutý interně.

E. Příležitosti a řešení

Zde se hodnotí cílové architektury, zda vycházejí z podnikových strategických cílů a zda jsou schopny realizovat požadované přínosy. Konsolidují se a analyzují se rozdíly mezi současnými a cílovými architekturami, na jejichž základě se vytvářejí různé varianty a scénáře řešení. Výstupem této fáze je implementační a migrační strategie, která definuje postup jak dosáhnout cílové architektury.

F. Plánování migrace

V této fázi se hodnotí jednotlivá řešení z pohledu nákladů a očekávaných přínosů. Výstupem z této fáze je seznam projektů seřazený podle výhodnosti a důležitosti. Z tohoto seznamu se vyberou ty projekty, které se vyplatí implementovat a začne se

plánovat provedení jednotlivých migračních projektů včetně termínů a potřebných zdrojů.

G. Dohled nad implementací

Obsahem této fáze je programový management, který koordinuje a řídí jednotlivé projekty. Cílem tohoto programu je uřídit veškeré migrační projekty a jejich návaznosti tak, aby byly úspěšně ukončeny včas, v daném rozpočtu a požadované kvalitě.

H. Řízení architektonických změn

V této fázi se hodnotí dosažené výsledky projektů z minulé fáze. Výsledky se porovnávají s cílovou architekturou a na jejich základě se mění současná architektura směrem k cílové.

Řízení požadavků

Řízení požadavků je specifický proces, který umožňuje iterativnost procesu vývoje podnikové architektury. V průběhu celého vývoje podnikové architektury mohou vznikat nové požadavky anebo ty stávající se mohou měnit, proto je nutné mít mechanismus, na jehož základě je možné se vracet mezi jednotlivými fázemi a hodnotit požadavky a jejich dopad na podnikovou architekturu.

Modifikace ADM dle modelu SPSPR

Model SPSPR navržený Voříškem (Voříšek a kol., 2008) přináší modifikaci zefektivňující metodu ADM tím, že mezi fáze „Návrh byznys architektury“ a „Návrh architektury informačních systémů“ vkládá dvě další fáze: „Návrh architektury IT služeb byznysu“ a „Rozhodnutí o sourcingu IT služeb“. Tato úprava řeší i požadavek Hamletta [Hamlett, 2007] na promítnutí rozsahu outsourcovaných IT služeb do celkového konceptu podnikové architektury: „S*polečnost, která se rozhodla outsourcovat svoje IT služby, musí změnit zaměření své podnikové architektury z provozního, technického a orientovaného na životní cyklus IT systémů na řízení podniku (podnikání), dílčím zaměřením na správu smluv a podpůrné kompetence“.*

Základní myšlenka této modifikace spočívá v tom, že v případě outsourcovaných IT služeb (např. formou SaaS) zákaznický podnik nezná a ani nechce znát (aby se nemusel zabývat technickými detaily, které jsou v kompetenci jiného subjektu) aplikační, datovou a technologickou architekturu outsourcovaných služeb. Tyto architektury outsourcovaných služeb jsou zcela v kompetenci externího dodavatele a pro zákaznický podnik jsou nepodstatné. To znamená, že pro tyto IT služby je možné fáze C a D přeskočit. V modifikaci tak na fázi „návrh byznys architektury“ navazuje fáze „návrh architektury IT služeb“, která definuje obsah, objem, kvalitu a limitní cenu všech IT služeb poskytovaných byznysu. V následující fázi, tj. ve fázi „Rozhodnutí o sourcingu IT služeb“, se určí, které IT služby budou zajišťovány interně a které externě. Fáze C a D, tj, návrh aplikační, datové a technologické architektury, se pak realizují pouze pro IT služby, které budou zajišťovány interně.

3. COBIT

Vedení společnosti je zodpovědné za nastavení strategického směru, kterým se organizace vydá, a současně musí trvat na interních kontrolách, které zajistí, že nižší vrstvy v podniku (podnikové architektuře) se budou orientovat stejným směrem, budou

mít cíle sladěné s celopodnikovými cíli a měření výkonnosti IT bude podporovat výkonnost organizace (Rafej, 2011).

COBIT je auditorský rámec, který se zabývá systémem interních IT kontrol a IT Governance. Cílem rámce COBIT a IT Governance je zajistit efektivní využívání IT zdrojů pomocí vytvoření interních kontrol a jejich dodržování. Dalším cílem je také propojení IT cílů s celopodnikovými cíli.

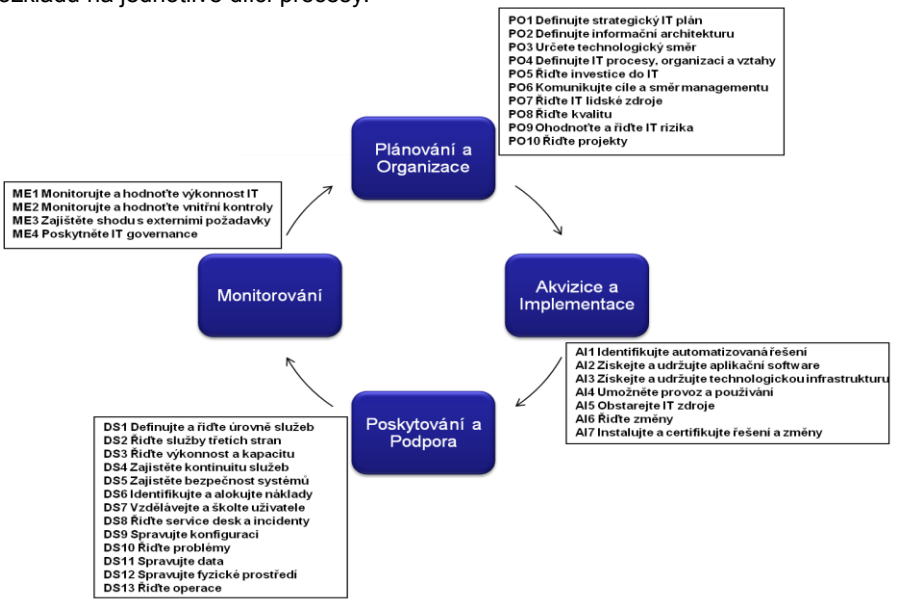
Základem rámce COBIT verze 4.1 je procesní rámec skládající ze čtyř procesních domén a dále dělící se na 37 základních procesů. Dá se říci, že COBIT obsahuje sadu „nejlepších praktik" sloužící auditorům pro hodnocení jednotlivých procesů. Každý proces obsahuje cíl, kontrolní cíle, aktivity, role, vstupy a výstupy, způsob měření vyspělosti procesu a návod na auditování.

3.1 Procesní rámec COBIT v4.1

COBIT v4.1 definuje svůj procesní rámec tak, aby jednotlivé procesy byly srozumitelné širší skupině lidí, a ne jen IT odborníkům anebo auditorům. Procesní rámec definuje na nejvyšší úrovni 4 agregované procesní domény, které jsou dostatečně obecné na to, aby pokryly většinu IT procesů. Tyto domény vychází ze všeobecného procesního rámce Plan → Build → Run → Monitor. COBIT je pojmenovává následovně:

1. Plánování a Organizace (Plan)
2. Akvizice a Implementace (Build)
3. Poskytování a Podpora (Run)
4. Monitorování (Monitor)

Na následujícím obrázku jsou znázorněny jednotlivé procesní domény včetně jejich rozkladu na jednotlivé dílčí procesy.



Obrázek 2: Procesní rámec COBIT (IT Governance Institute 2007b), *přeloženo autory práce*

Plánování a organizace (PO, Plan and Organise)

Tato procesní doména pokrývá strategické a taktické řízení IT procesů ve snaze co nejefektivněji dosáhnout podnikových a IT cílů. Strategický IT plán má vycházet z celopodnikové strategie a jeho vize, mise a prostředky pro dosažení strategických cílů mají být plánovány a komunikovány kontinuálně tak, aby celá organizace věděla, jakým směrem se IT ubírá.

Z podnikové i IT strategie vycházejí požadavky na celkovou informační architekturu podniku, která je podpořena informačními technologiemi. Na delší časový horizont je proto vhodné definovat i technologický směr IT, aby nedocházelo k nasazování různých technologických platforem a aplikací, které ve finále povedou k vyšším nákladům a zvýšené komplexnosti informační architektury. Organizační struktura včetně nadefinovaných procesů by měla opět vycházet z IT strategie a umožňovat identifikaci například, kterých lidí s určitými schopnostmi je nedostatek, které procesy je třeba zavést anebo u kterých procesů je třeba zvýšit vyspělost, a dále například nadefinovat jednotlivé zodpovědnosti a normy.

Plánování a organizace se však nezabývá jen strategickou úrovní ale i taktickou a operativní, kam spadá například řízení investic do IT, řízení lidských zdrojů, řízení kvality, řízení rizik, projektové a programové řízení.

Akvizice a implementace (AI, Acquire and Implement)

Tato procesní doména realizuje nadefinovanou IT Strategii v předešlé doméně tím, že převádí strategické plány do požadavků na jednotlivé IT řešení (aplikace a technologická infrastruktura). Tyto IT řešení je možné dále realizovat buď vlastními silami anebo si nechat IT řešení vytvořit od třetí strany. Po získání IT řešení je dále nezbytné zabezpečit integraci do stávajícího IT prostředí a provést implementaci řešení. Jakmile je řešení naimplementováno, je nutné zajistit jeho podporu a řízení změn tak, aby IT řešení kontinuálně podporovalo stále se měnící podnikové požadavky na IT.

Poskytování a podpora (DS, Deliver and Support)

V této procesní doméně se klade důraz na efektivní poskytování a podporu IT služeb. Jedním z procesů je například definování a řízení úrovní služeb tak, aby IT služby byly dodávány v požadované kvalitě a za dohodnutou cenu. Důležitým aspektem je i řízení třetích stran, které pomáhá držet náklady na IT a kvalitu na přijatelné úrovni. IT řešení je nutné i neustále monitorovat, zlepšovat a minimalizovat dopady na uživatele v případech výpadků IT služeb jako například nedostupnost služby, vyčerpaná disková kvóta či nízká průchodnost sítě.

V první doméně se definuje organizační struktura a procesy. Jednou z významných organizačních jednotek je Service Desk, který vykonává procesy jako například řízení incidentů, poskytování podpory, adresování jednotlivých požadavků na ostatní organizační jednotky atd. Pro redukci incidentů slouží proces řízení problémů, kde se analyzují příčiny vzniku jednotlivých incidentů a vytváří se řešení, jak tyto problémy vyřešit.

Další skupinou procesů nacházející se v této doméně je řízení fyzického prostředí čili infrastruktury, řízení dat, operací a konfigurace jednotlivých elementů IT prostředí. Jednou z kritické oblasti je i řízení bezpečnosti a možnosti obnovení provozu po výpadku či katastrofě.

Monitorování (ME, Monitor and Evaluate)

Měřením a řízením IT se zabývá poslední procesní doména. V podniku by měly být zavedeny procesy, které nezávisle měří výkonnost IT a shodu s interními i externími předpisy.

Je zde uveden i proces „Monitorujte a hodnoťte systém vnitřních kontrol“, který v podstatě popisuje úroveň implementace rámce COBIT v podniku. Posledním procesem je „Poskytujte IT Governance“, který se zaobírá dozorem nad procesy z předešlých domén a zajišťuje, že se dané procesy vykonávají. Mezi kontrolní cíle například patří zajištění, že IT strategie je ve shodě s podnikovou strategií, IT přináší očekávanou hodnotu podniku, rizika jsou řízena, výkonnost a zdroje jsou řízeny atd.

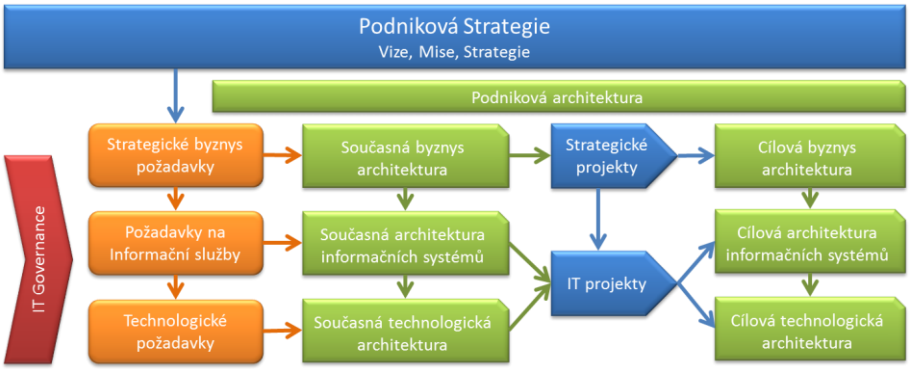
4. Srovnání rámců a jejich provázanost

Oba rámce společně usilují o propojení IT zdrojů, procesů a informací se strategickými cíli, o integraci a institucionalizaci nejlepších praktik, umožnění plně čerpat výhody z informací, infrastruktury, HW, SW a o ochranu digitálních aktiv organizací. Dále podporují zákonné a požadavky nejlepších praktik jako auditovatelnost, bezpečnost, odpovědnost a accountabilitu (Open Group, 2009)

Syntézu obou rámců zachycuje obrázek 3. Na obrázku je znázorněna podniková strategie, požadavky plynoucí z podnikové strategie, dopad požadavků na podnikovou architekturu, projekty implementující změnu podnikové architektury a vztah k IT Governance.

Podniková strategie klade požadavky na změnu podniku, konkurenčních schopností, služeb a výrobků. Tyto strategické požadavky jsou označeny jako strategické byznys požadavky. Role podnikové architektury je provést analýzu dopadů těchto strategických byznys požadavků na současnou byznys architekturu a vytvořit cílovou byznys architekturu. Od té se pak odvíjejí požadavky na IT služby a technologické požadavky. Na základě těchto požadavků se provádí analýza dopadů na současné IT architektury a vytváří se cílové architektury. Pomocí projektů se implementuje podniková strategie a mění se současný stav podniku, popsaný v současných architekturách, na cílový stav podniku sladěný s podnikovou strategií, cílové architektury.

IT Governance zajišťuje, že požadavky na IT vycházejí z podnikové strategie a podnikových cílů. Největší důraz má být kladen na schvalování a řízení IT projektů, aby vynaložené prostředky přinesly očekávané přínosy a plně podpořily podnikovou strategii.



Obrázek 3: Vliv podnikové strategie na podnikovou architekturu,
zdroj: autoři práce

Jednou ze základních podmínek úspěšně implementované podnikové architektury je právě IT Governance. Bez IT Governance zůstává podniková architektura jen teoretických konceptem či modelem a stěží přinese očekávané přínosy organizaci. Proto COBIT svým zacílením na IT Governance výrazně zvyšuje šanci, že organizace dosáhne přínosů vyplývajících z rámce TOGAF.

Implementace rámce COBIT ve velkých organizacích (bez zavedené podnikové architektury) bývá velice náročná, protože například:

- chybí nadefinované procesy a vlastníci procesů. Poté je těžké sjednotit procesní cíle s organizačními cíli;
- IT je tak komplexní, že mu management organizace nerozumí a dál utrácí peníze na jednotlivé izolované IT projekty, aniž by sledoval a mohl hodnotit vliv jednotlivých IT projektů na výkonnost organizace,
- chybí přehled popisující vztah mezi procesy a aplikacemi, kdo tyto aplikace vlastní a jaké jsou náklady na chod jednotlivých aplikací.

COBIT pomáhá při zavádění rámce TOGAF v následujících aspektech:

- převádí byznys požadavky na IT požadavky. Přičemž TOGAF resp. podniková architektura umožňuje tyto požadavky řídit a efektivně implementovat v organizaci,
- definuje základní sadu kontrolních cílů, které podporují IT Governance a při jejich existenci výrazně přispívají k úspěšnosti zavádění rámce TOGAF,
- poskytuje základní sadu metrik, které vypovídají o výkonnosti jednotlivých procesů (včetně architektonických procesů),
- poskytuje základní přehled procesních vstupů a výstupů, které mohou sloužit mimo jiné pro vytváření procesního modelu organizace,
- každý IT proces definovaný v rámci COBIT obsahuje tabulku RACI (responsible, accountable, consulted and informed), která definuje odpovědnosti v organizaci za jednotlivé aktivity. Tato tabulka se hodí v rámci TOGAF například pro analýzu zúčastněných stran a pro definici odpovědností včetně IT Governance,

- definuje u každého procesu model vyspělosti, který se dá použít pro analýzu současného stavu se stavem cílovým resp. analýza současné architektury a cílové architektury.

5. Systém vnitřních kontrol v podnikové architektuře

(Kyriazoglou, 2010) definuje následující kontroly pro podnikovou architekturu:

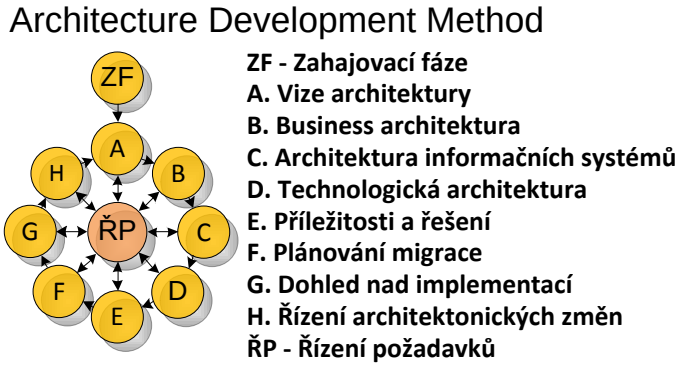
- existence rámce a definic podnikové architektury (popis co je podniková architektura, definice základních pojmů a výběr rámce, který bude použit pro vývoj podnikové architektury),
- existence manažerského plánu pro návrh a implementaci podnikové architektury (definuje postup, jak bude podniková architektura vytvořena. Vychází z vybraného rámce),
- existence specifických rolí pro vývoj podnikové architektury,
- formulace a dokumentace částí podnikové architektury (organizační struktura, operační model, podnikové procesy, strategické cíle, vize, mise, strategie, repositář podnikové architektury).

Výše uvedené kontroly jsou dle názoru autorů tohoto článku zaměřeny pouze na statickou část podnikové architektury. Tyto kontroly mají za úkol zjistit, zdali existuje rámec podnikové architektury, specifický plán pro implementaci, role zodpovědné za podnikovou architekturu a knihovna (repository) obsahující zdokumentované elementy podnikové architektury.

Interní kontroly zabývající se podnikovou architekturou však mohou vzniknout i na základě průniku rámce COBIT a TOGAF, čímž se zabývá následující kapitola.

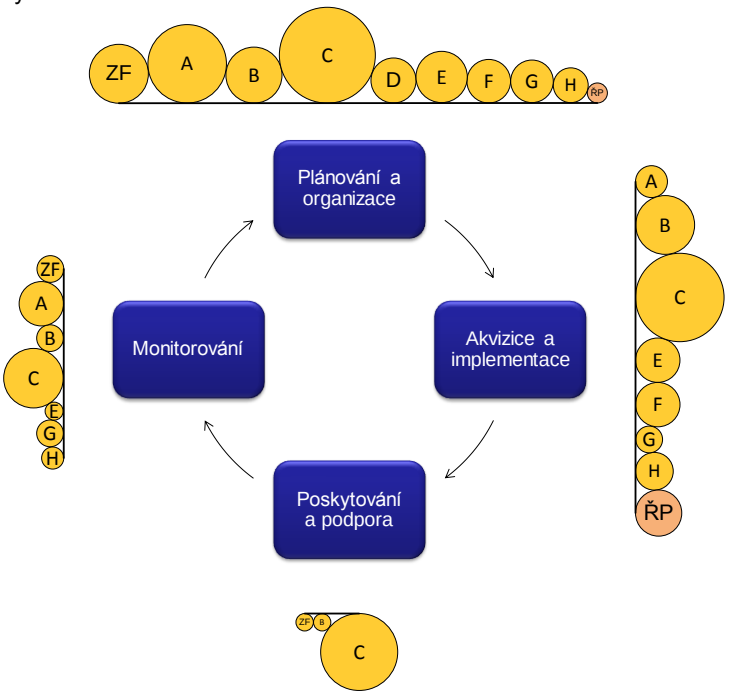
5.1 Mapování rámce TOGAF a COBIT za účelem nadefinování interních kontrol

Při návrhu systému vnitřních kontrol v podnikové architektuře práce vychází z mapování rámce TOGAF a COBIT (IT Governance Institute 2007a). Pro zjednodušení mapování, práce používá zkratky pro jednotlivé fáze v ADM. Následující obrázek ilustruje ADM pomocí zkratek.



Obrázek 4: ADM vyjádřený zkratkami, přeloženo autory

Na následujícím obrázku je znázorněn pohled na systém vnitřních kontrol v podnikové architektuře. Tento systém interních kontrol je pro názornost vyjádřen procesními doménami z rámce COBIT. Kolečka reprezentují jednotlivé fáze z ADM a jejich velikost odpovídá počtu požadavků ze systému vnitřních kontrol, které jsou pokryty v jednotlivých fázích ADM.



Obrázek 5: Mapování rámce COBIT a TOGAF na základě (IT Governance Institute 2007a), *obrázek vytvořen autory práce*

Z obrázku 5 vyplývá, že nejvíce kontrol zahrnují procesní domény „Plánování a organizace“ a „Akvizice a implementace“, které pokrývají celý ADM. Z pohledu podnikové architektury je nejvíce požadavků z interních kontrol kladeno na první fáze a to „A vize architektury“, „B byznys architektura“ a „C architektura informačních systémů“. Procesní doména „Poskytování a Podpora“ se soustředí pouze na architekturu informačních systémů.

Jednotlivé interní kontroly nacházející se v procesních doménách je možné najít v rámci COBIT (IT Governance Institute 2007b).

V následujících kapitolách se článek zabývá hlubší analýzou a mapováním relevantních COBIT procesů ve vztahu k podnikové architektuře.

PO1 Definujte strategický IT plán

Zabývá se sjednocením byznys a IT pohledu na potřeby organizace a vytvořením strategického IT plánu, který reflektuje současné a budoucí potřeby organizace. Zajišťuje prioritizaci IT cílů v návaznosti na podnikové cíle.

PO2 Definujte informační architekturu

Kontrolní cíle, metriky a model vyspělosti se používají pro zhodnocení informační architektury. Informační architektura je dle COBIT myšlena jako podnikový datový model, který zajišťuje datovou konzistenci a integritu napříč celým podnikem. Tento podnikový datový model je zapotřebí zohlednit při vývoji informačního systému organizace, který podporuje podnikové procesy.

Tento proces je prvním, který se v COBIT v4.1 zabývá architekturou. Ve smyslu rámce COBIT se tato architektura zaměřuje pouze na datovou architekturu, která svou existenci umožní efektivnější vývoj aplikací. O aplikační architektuře a architektuře IT služeb se COBIT nezmiňuje. Z tohoto důvodu autoři článku v COBIT v4.1 shledávají mezeru v interních kontrolách. *Tuto mezeru navrhují odstranit vytvořením dvou nových procesů a to PO11 Definice architektury IT služeb a PO12 Rozhodnutí o sourcingu IT služeb* a to ve smyslu modifikace ADM popsané v kapitole 2.1. Detailní definice těchto dvou nových procesů je však nad rámec tohoto článku.

PO3 Určete technologický směr

Tento proces nejvíce podporuje fázi „D Technologická architektura“. Soustředí se přitom na vytvoření technologického plánu, který bude podporovat současnou a budoucí IT infrastrukturu, která bude sloužit k uspokojení podnikových cílů za pomocí standardizace a integrace informačních systémů. V rámci tohoto procesu vznikají i technologické standardy a monitoruje se technologický trend na trhu. Z pohledu IT Governance tento proces zavádí „IT architecture board“, který vytváří technologickou architekturu a zajišťuje shodu s technologickými standardy.

PO4 Definujte IT procesy, organizaci a vztahy

Tento proces nejvíce podporuje fázi „B Byznys Architektura“. Soustředí se na definici IT procesů, organizační struktury IT útvarů a vztahů. Přitom klade důraz na stanovení jednotlivých organizačních rolí a jejich odpovědností.

PO6 Komunikujte cíle a směr managementu

Tento proces zajišťuje, že jsou strategické informace v organizaci sdíleny. Může se jednat například o vytváření různých směrnic a následně zajištění, že lidé tyto směrnice dodržují.

PO10 Řiďte projekty a AI6 Řiďte změny

Projektový a programový management pokrývá TOGAF fáze, které se zabývají migrací či transformací organizace směrem k cílové podnikové architektuře. V těchto fázích (F, G, H) se připravuje a realizuje program a z něj plynoucí jednotlivé projekty. V rámci projektového a programového managementu také dochází k realizaci architektonické vize a jednotlivých dílčích cílů.

V těchto implementačních fázích často dochází k identifikaci neodhalených problémů, realizaci očekávání atd., které mohou ovlivňovat předešlé fáze a proto projektový a programový management v největší míře souvisí s TOGAF fází Řízení požadavků.

Proces řízení změn zajišťuje, že veškeré změny jsou kontrolovaně řízeny. Změny se však netýkají jen IT infrastruktury, dat a aplikací, ale také například podnikových procesů a chování lidí. Změny jsou implementovány jednotlivými projekty, které

spadají do programu. Každá změna musí mít odhadnutý dopad, měla by být prioritizována a musí být schválena.

AI1 Identifikujte automatizovaná řešení

Tento proces v doméně Akvizice a Implementace zajišťuje, že požadavky na nové aplikace anebo rozšíření či integrace stávajících řešení jsou v souladu s podnikovými požadavky. Tento proces pokrývá TOGAF fáze, kde se definuje základní vize architektury, jednotlivé dílčí architektury a poslední fázi, kde se identifikují jednotlivé příležitosti a dostupná řešení na trhu či uvnitř organizace. Jednotlivé požadavky na aplikace či informační systémy vycházejí z cílové architektury, které se vytvářejí z podnikových cílů a z podnikové a IT strategie.

DS11 Spravujte data

Řízení dat má dopad na architekturu informačních systémů, především na datovou architekturu. Účelem řízení dat je zajistit jejich kvalitu, přesnost, celistvost a dostupnost. Jedním aspektem řízení dat je i obnova dat, zálohování a řízení životního cyklu.

ME1 Monitorujte a hodnoťte výkonnost IT

Metriky by měly vycházet z potřeb organizace a slouží k měření výkonnosti IT. Na základě metrik dochází k reportování a v případě výjimek se spouští opravné aktivity. Cílem měření je také zvýšení transparentnosti například nákladů. Na základě měření procesů je možné realizovat aktivity zlepšující procesy. Jednoduše řečeno „nedá se řídit něco, co není měřeno“.

K měření se používají data, která jsou používána různými aplikacemi. K měření je nutné znát současnou datovou architekturu a vědět, kde se nacházejí jaké informace. I cílová architektura by měla odrážet požadavky na měření a efektivní reportování.

ME3 Zajistěte shodu s externími požadavky

Informační systémy by měly vyhovovat externím požadavkům. Proto je nutné navrhovat informační systémy, aby byly ve shodě s bezpečnostními rámci, finančními a dalšími zákony. Tyto požadavky je nutné zohlednit při navrhování celkové datové a aplikační architektury.

5.2 Interní kontroly

Na základě provedeného mapování je možné vytvořit seznam interních kontrol, které mohou doplnit interní kontroly nadefinované v (Kyriazoglou 2010).

Název kontroly	**EA1 Shoda IT projektů s podnikovou architekturou**
Cíl kontroly	Cílem kontroly je určit, zda IT projekty (nové i běžící) jsou ve shodě s podnikovou architekturou.
Postup kontroly	1. Zjistěte, zdali je zástupce podnikové architektury součástí procesu schvalování interních investic do IT a součástí projektového nebo programového výboru. 2. Analyzujte projektové záměry, zdali vznikly na základě požadavků plynoucích ze změn podnikové architektury.

Závěr kontroly	IT projekty musí být ve shodě s podnikovou architekturou a až na výjimky (IT projekty zaměřené na optimalizaci technologické architektury) by měly být iniciovány pouze na základě požadavků plynoucích ze změn podnikové architektury. Jestliže podniková architektura nevytváří žádné změnové projekty, poté existuje riziko, že podniková architektura neslouží svému účelu a to k transformaci organizace a efektivnější reakci na strategické změny v okolí. Jestliže investice do IT a IT projekty obcházejí analýzu dopadů na podnikovou architekturu, poté existuje riziko, že jednotlivé projekty přinesou jen lokální přínosy a mohou být v rozporu se strategickými cíli organizace.
Nápravné akce	Úprava procesu schvalování investic a nových IT projektů o nutné vyjádření a schválení ze strany podnikové architektury. Začlenění zástupce podnikové architektury do řízení každého programu.

Název kontroly	**EA2 Užití EA repositáře (EAR) jako strategického komunikačního nástroje**
Cíl kontroly	Cílem kontroly je zhodnotit, zda repositář podnikové architektury obsahuje všechny důležité strategické informace a je používán jako hlavní komunikační médium.
Postup kontroly	Zjistěte, zda EAR obsahuje 1. všechny elementy, které mají být zachyceny v EAR (např. dle EAR metamodelu), 2. definici všech IT služeb, které jsou zapotřebí pro pokrytí požadavků byznys procesů, 3. strategický IT plán a technologický směr. Zjistěte, zdali EAR je užíván jako centrální nástroj pro komunikaci strategie. Zjistěte, zdali EAR je užíván při řízení IT projektů.
Závěr kontroly	Podniková architektura slouží jako strategický nástroj pro řízení komplexnosti a organizačních změn. Z tohoto důvodu by měla obsahovat všechny významné elementy, které tvoří podnikovou architekturu. V oblasti IT má navíc obsahovat definici všech IT služeb, strategický IT plán a určení technologického směru, kterým se organizace bude ubírat. Všechny informace musí být sdíleny, aby strategie byla řádně komunikována. Knihovna (repository) má navíc sloužit jako zdroj informací pro jednotlivé IT projekty. Např. z hodnot parametrů objem a kvalita IT služby se odvozují konkrétní technické parametry aplikací a technologické infrastruktury.

Nápravné akce	Chybějící elementy podnikové architektury by měly být vytvořeny a řízeny. IT projekty mají používat informace uložené v EAR.

Název kontroly	**EA3 Změny aplikací a IT infrastruktury musí být v souladu s cílovými stavy jednotlivých architektur**
Cíl kontroly	Cílem kontroly je zajistit, že veškeré změny IT vycházejí z požadavků podnikové architektury a jsou v souladu s cílovými stavy jednotlivých architektur.
Postup kontroly	Ujistěte se, že • změny IT služeb, • změny aplikací a jejich licencí, • změny IT infrastruktury vycházejí z požadavků podnikové architektury.
Závěr kontroly	Jestliže změny IT nevycházejí z podnikové architektury (resp. z podnikové strategie), poté IT nebude v souladu s podnikovými cíli a finanční prostředky nebudou efektivně vynaloženy.
Nápravné akce	Při nákupu IT zdrojů či změn infrastruktury musí dojít ke schválení ze strany podnikové architektury. Rozpočet na IT prostředky musí být centrálně řízen a prioritizován.

Aby podniková architektura přinesla očekávané přínosy, musí fungovat IT a Architecture Governance. IT Governance má zajistit definování rolí, odpovědností, pravomocí a pravidel tak, aby IT zdroje byly využívány efektivně a přispívaly k dosažení podnikových cílů. Na druhé straně Architecture Governance má zajistit definování, porozumění a používání architektonických komponent napříč organizací za pomoci definování pravidel, rolí, odpovědností a pravomocí.

Nedílnou součástí IT a Architecture Governance jsou interní kontroly v podnikové architektuře. Současná literatura se zaměřuje na kontroly týkající se definice, obsahu a personálního zajištění podnikové architektury. Autoři článku se domnívají, že se kontroly mají více zaměřit na procesy schvalování investic do IT, sladěnost IT projektů s podnikovou architekturou a využití repositáře podnikové architektury jako strategického komunikačního nástroje. Proto v článku navrhli rozšíření kontrol tak, aby bylo možné tento požadavek naplnit.

Tvůrci auditorského rámce COBIT jsou si vědomi významnosti podnikové architektury. Z tohoto důvodu nová verze rámce COBIT v5 (ISACA 2012) již obsahuje proces věnovaný výhradně kontrolám v podnikové architektuře. Kontroly jsou však založeny na procesním rámci TOGAF v9. Z tohoto důvodu tento článek vhodně popisuje problematiku kontrol v podnikové architektuře i z pohledu COBIT v5.

Poděkování

Tento článek vznikl za podpory grantu GAČR P 403-10-0092 (Advanced Principles and Models for Enterprise ICT Management) a za podpory grantu GAČR P403/11/0574 (Enterprise Architecture for Cloud Computing Environments)

Literatura

AZIZ, S. et al. Enterprise Architecture: *A Governance Framework* – Part I: Embedding Architecture into the Organization. Infosys company website: Architecture services - White papers [online]. Vznik 2005 [cit. 2012-03-10]. Dostupné na internetu: www.infosys.com/consulting/architecture-services/white-papers/documents/ea-governance-1.pdf.

BROWN, B. *Check Efficiency with an IT Audit.* Manawatu Standard. Palmerston North, New Zealand, 2011, vydání 20. června, s.9. [cit. 2012-03-01]. ISSN 1176-3558.

CANGEMI, M. What are the Benefits of Implementing CobiT? SOXTelevision [online]. Vznik 2006 [cit. 2012-03-01]. Dostupné na internetu: <http://www.youtube.com/watch?v=bg_GEN8AZA0>

FINKELSTEIN, C. Governance Responsibilities Imposed by Sarbanes-Oxley. *Information Management Magazine* [online]. 2004. no. 10. [cit. 2012-04-30]. Dostupné na internetu: <http://www.information-management.com/issues/20041001/1011132-1.html>.

GARTNER, I. Enterprise Architecture (EA) | Gartner IT Glossary. IT Dictionary, IT Terms | Gartner IT Glossary [online]. Vznik 2012 [cit. 2012-04-29]. Dostupné na internetu: <http://www.gartner.com/it-glossary/enterprise-architecture-ea/>.

HAMLETT, N.: IT Outsourcing Impacts on Enterprise Architecture. [Online] March 2007. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4140968&isnumber=4140956

HUGOSON, M. et al. *Enterprise architecture design principles and business-driven IT management*. International Workshops on Business Information Systems Workshops. Berlin, 2010s. 144–155. ISBN 3642154018. Dostupné z doi: 10.1007/978-3-642-15402-7_20

ISACA. COBIT 5 - A Business Framework for the Governance and Management of Enterprise IT, Information Systems Audit and Control Association, 2012, ISBN 978-1-60420-237-3

IT GOVERNANCE INSTITUTE. COBIT 4.1: framework, control objectives, management guidelines, maturity models. Rolling Meadows, IL: Information Systems Audit and Control Association, 2007a ISBN 19-332-8472-2.

IT GOVERNANCE INSTITUTE. COBIT mapping of TOGAF 8.1 with COBIT 4.0. Rolling Meadows, IL: Information Systems Audit and Control Association, 2007b 281 s. ISBN 978-193-3284-828.

KAOUTAR, E. - BOUNABAT, B. Strategic Alignment Assessment Based on Enterprise Architecture. *International Conference on Information Management and Evaluation. University of Cape Town*, South Africa: Academic Conferences International Limited, 2010. s.179. ISBN 978-1-906638-56-6

KYRIAZOGLOU, J. IT strategic and operational controls. Ely, U.K.: IT Governance, 2010 ISBN 978-184-9280-617.

OPEN GROUP. TOGAF Version 9. Zaltbommel: Van Haren Publishing, 2009, 778 s. ISBN 978-908-7532-307.

RAFEQ, A. Driving business value with effective governance of enterprise IT. Express Computer [online]. Vznik 2011 [cit. 2012-04-25]. Dostupné na internetu: <http://www.expresscomputeronline.com/20110314/techviews01.shtml>

ROSS, J.W. et al. *Enterprise architecture as strategy*: creating a foundation for business execution. Boston: Harvard Business School Press, 2006 234 s. ISBN 15-913-9839-8.

SARBANES, P. - OXLEY, M. Sarbanes-Oxley Act of 2002.Washington, US: Senate and House of Representatives of the United States of America in Congress, 2002. Dostupné na internetu: <http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf>

SCOTT, J. Business Capability Maps: The Missing Link Between Business Strategy and IT Action | Architecture and Governance – Strategic IT Planning and Enterprise Architecture. *Architecture and Governance Magazine* [online]. 2009. no. 5-9. [cit. 2012-04-30]. Dostupné na internetu: <http://www.architectureandgovernance.com/content/business-capability-maps-missing-link-between-business-strategy-and-it-action>.

SHIELDS, R. Reduced Costs, Improved Outcomes | Architecture and Governance – Strategic IT Planning and Enterprise Architecture. *Architecture and Governance Magazine* [online]. 2011. no. 7-1. [cit. 2012-04-30]. Dostupné na internetu: <http://www.architectureandgovernance.com/content/reduced-costs-improved-outcomes>.

STROUD, R.E. The Impact and Opportunity of Compliance and IT Governance. ISACA - Kettle Moraine Chapter [online]. Vznik 2009 [cit. 2012-03-01]. Dostupné na internetu: <http://www.isaca-km.org/meetings%5CTheImpactandOpportunityofComplianceandITGovernance.ppt>

VOŘÍŠEK, J. a kol. *Principy a modely řízení podnikové informatiky*. Praha: Oeconomica, 2008 ISBN 978-80-245-1440-6.

WINTER, R. - SCHELP, J. Enterprise architecture governance: the need for a business-to-IT approach. *Proceedings of the 2008 ACM symposium on Applied computing* [online]. New York, NY, USA: ACM, 2008s. 548–552. [cit. 2012-04-29]. Dostupné na internetu: <http://doi.acm.org/10.1145/1363686.1363820>.

ZACHMAN, J. A. A framework for information systems architecture. *IBM SYSTEMS JOURNAL*, VOL 26. NO 3,. 1987.

JEL: D8, M15, M42