Konceptuální model zajišťování a prokazování shody v prostředí BPMS a SOA

Ivana Šabatová
Vysoká škola ekonomická v Praze
Fakulta informatiky a statistiky
Katedra systémové analýzy
nám. W. Churchilla 4, 130 67 Praha 3
e-mail: sabi@sabi.cz

Abstrakt: *Zajišťování a prokazování shody procesů a služeb s regulatorními požadavky, standardy a s požadavky businessu se stává komplexní úlohou zejména v prostředí vysoce regulovaném s vysokou mírou dynamiky změn. Tento příspěvek představuje koncept kontinuálního řízení shody v servisně orientovaných systémech se zaměřením na využití pokročilých nástrojů pro automatizaci procesů. Konceptuální model zajišťování a prokazování shody v prostředí BPMS a SOA je návrh postupu inspirovaný známým Demingovým cyklem (Plan – Do – Check – Act). Jedná se o rozpracování metodiky zajišťování shody vytvořené v rámci verifikace návrhu algoritmu shody publikovaného v Journal of System Integration Šabatová (2015).*

Klíčová slova: shoda, business proces, kontrolní proces, cílový proces, klíčový indikátor zajištění (Key Assurance Indicator), klíčový indikátor bezpečnosti (Key Security Indicator).

Abstract: *Compliance achievement and assurance of processes and services with regulatory requirements, standards, and business requirements becomes a complex task especially in the highly regulated and turbulently changing environment. Conceptual Model of Compliance Assurance in BPMS and Service Oriented Systems environment brings a method inspired by well-known Deming Cycle (Plan – Do – Check – Act). This work represents elaboration of the compliance assurance methodology developed within compliance algorithm verification published in Journal of System Integration by Šabatová (2015).*

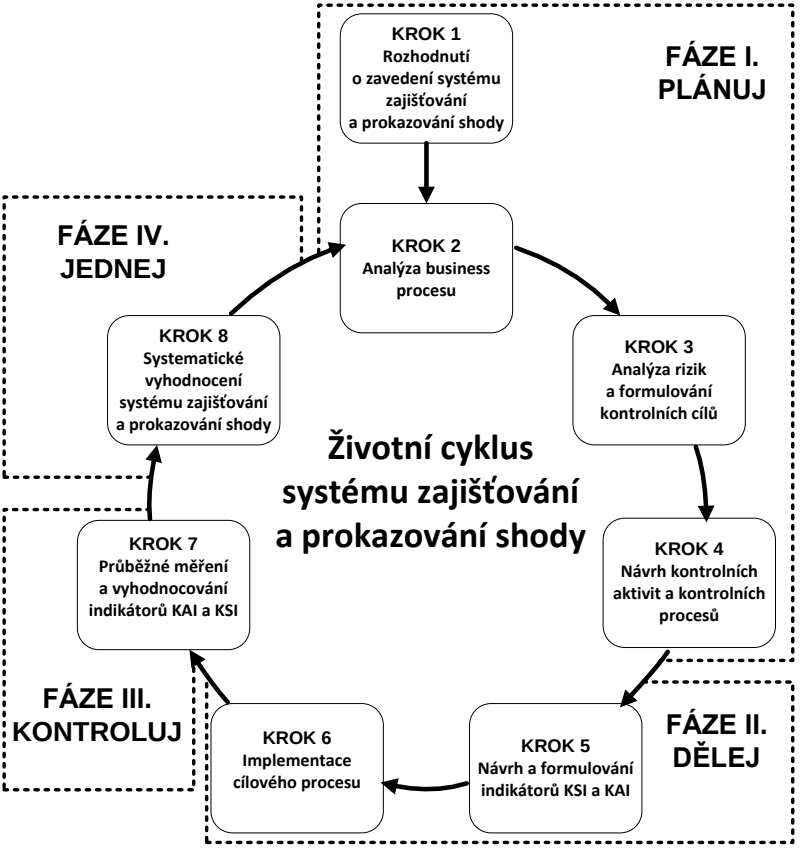
Keywords: Compliance, Business Process, Control Proces, Target Process, Key Assurance Indicator (KAI), Key Security Indicator (KSA).

1. Úvod

Tato metodika představuje doporučený postup při zavádění systému zajišťování a prokazování shody vedoucí od identifikace požadavků na zajištění a prokazování shody v rámci organizace, přes návrh a vývoj kontrolních procesů, až po návrh a implementaci indikátorů pro vyhodnocení a prokazování shody, včetně neustálého zlepšování tohoto systému. Vychází ze zkušenosti získané při verifikaci návrhu algoritmu shody, který je popsán v článku Building Assurance of Regulatory Compliance in Dynamic Service Oriented Systems. Vytvoření této metodiky bylo inspirované modifikací Demingova cyklu PDCA, jak jen například použil Doucek Doucek (2008) pro životní cyklus zvládání bezpečnostního incidentu. Tento přístup vedl k myšlence navrhnout tzv. životní cyklus systému zajišťování a prokazování shody tak, jak je vyobrazen na obrázku 1.

Metodika představuje celkem čtyři hlavní fáze a osm dílčích kroků:

- **Fáze I. Plánuj**
  Krok 1: Rozhodnutí o zavedení systému zajišťování a prokazování shody
  Krok 2: Analýza business procesu
  Krok 3: Analýzy rizik a formulování kontrolních cílů
  Krok 4: Návrh kontrolních aktivit a kontrolních procesů
- **Fáze II. Dělej**
  Krok 5: Formulování indikátorů KAI a KSI
  Krok 6: Implementace cílového procesu
- **Fáze III. Kontroluj**
  Krok 7: Průběžné měření a vyhodnocování indikátorů KAI a KSI
- **Fáze IV. Jednej**
  Krok 8: Systematické vyhodnocení systému zajišťování a prokazování shody



Obrázek 1: Postup zavedení systému zajišťování a prokazování shody;
zdroj: autorka

2. Krok 1: Rozhodnutí o zavedení systému zajišťování a prokazování shody

První krok celého postupu představuje zahájení iniciativy, která se musí uskutečnit na úrovni strategického managementu dané organizace. Pokud má organizace zpracovaný business plán například formou modelu motivace businessu BMM viz obrázek 2 převzatý z OMG (2015), je potřeba vycházet z tohoto konkrétního modelu. Pokud organizace nemá takový model k dispozici, je potřeba vytvořit formou dekompozice alespoň částečný model motivace businessu popisující potřebné elementy business plánu pro dílčí řešenou oblast. Je potřeba si ale uvědomit, že v takovém případě můžeme opominout důležité aspekty, které mohou zajišťování shody v této dílčí oblasti ovlivňovat, proto je vždy lepší pracovat s úplným modelem. Elementy BMM, které jsou pro zavedení systému zajišťování a prokazování shody podstatné, jsou:

- Požadované výsledky (Desired Results)
- Strategické cíle
  Operativní cíle
- Ovlivňovatelé (Influencers)
  Externí ovlivňovatelé (External Influencers)
- Předpisy (Directives)
  Business politiky (Business Policies)
  Business pravidla (Business Rules)

Z externích elementů BMM pak do podkladů pro další práci doplňujeme:

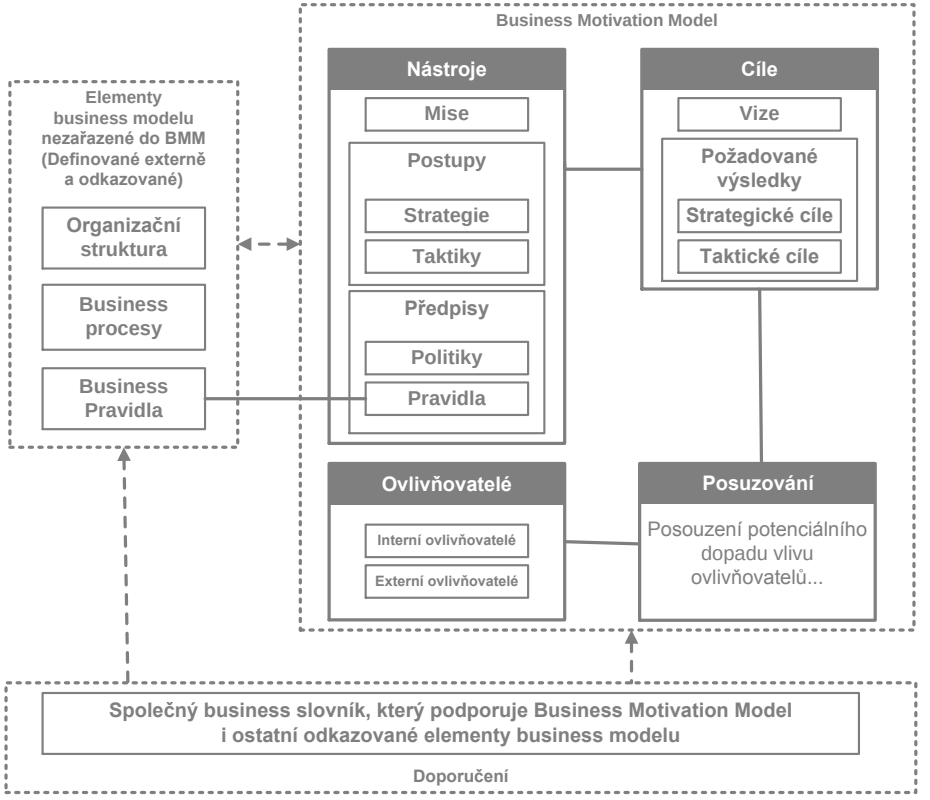
- Business procesy (Business Processes)
- Jednotný business slovník (Common Business Vocabulary)

Pro vlastní realizaci systému zajišťování a prokazování shody je nezbytný jednotný business slovník, ze kterého čerpáme definice potřebných datových objektů a jejich atributů, a zároveň tento jednotný slovník doplňujeme o business objekty a jejich atributy, které identifikujeme a navrhujeme v průběhu. Standard pro tvorbu business slovníku vydalo OMG (2015b). Rovněž je výhodné mít k dispozici celkový přehled o procesním řízení v dané organizaci, například globální procesní model uvádějící komplexní přehled všech v organizaci identifikovaných a řízených procesů a metodiku používanou pro management procesů.

Zavedení systému zajišťování a dosahování shody má jednoznačně charakter interního projektu, proto zde není uvedena žádná konkrétní projektová metodika. Zde prezentovaný koncept předpokládá, že organizace využije postupy, dokumenty a pravidla projektového řízení tak, jak je má standardně zavedené. Případová studie je dokument shrnujícím všechny aspekty, informace a argumenty potřebné pro rozhodnutí o zavedení systému zajišťování a prokazování shody. Zejména uvádí informace o nákladech, přínosech, variantách, rizicích apod. viz OGC (2007). Je důležitým podkladem pro rozhodnutí odpovědných osob o zavedení systému zajišťování a prokazování shody.

Do systému zajišťování a prokazování shody může být zahrnuto několik procesů, nebo jeden jediný proces, nebo všechny v organizaci identifikované a řízené procesy. Vždy je to otázkou konkrétní situace vymezené na jedné straně potřebami a povinnostmi dané organizace, na straně druhé prostředky dostupnými pro realizaci takového systému. Protože tato metodika je zaměřena na využití pokročilých systémů pro

automatizaci procesů, což jsou například systémy hodnocené v rámci studie „Magic Quadrant for Intelligent Business Process Management Suites“ společnosti Gartner viz Sinur (2012), můžeme ji v plném rozsahu použít de facto pouze pro procesy, které jsou automatizovány v rámci některého z takových nebo obdobných systémů, jejichž model procesu odpovídá standardu Business Process Model and Notation 2.0 (BPMN 2.0) vydaný OMG (2013). Základní přehled o druhém kroku je uveden v tabulce 1.



Obrázek 2: Business Motivation Model dle OMG (2015);
zdroj: OMG (2015)

Tabulka 1: Krok 1 Rozhodnutí o zavedení systému zajišťování a prokazování shody (zdroj autorka)

CÍL:	**Dosáhnout rozhodnutí o zavedení systému zajišťování a dosahování shody.**
AKTIVITY:	❒ Ustavení řídícího týmu, určení rolí a odpovědnosti. ❒ Identifikace procesů, u kterých má být systém zaveden. ❒ Vytvoření a schválení plánu obsahujícího minimálně potřebné zdroje, rozpočet a časový harmonogram. ❒ vytvoření a schválení případové studie (Business Case)
VÝSTUPY:	Projektový plán Případová studie (Business Case) Seznam relevantních procesů

3. Krok 2: Analýza business procesu

Postup analýzy business procesů s cílem automatizovat je pomocí BPMS jsem podrobně popsala v Šabatová (2013). Analýza business procesu musí být provedena ve vztahu k cílům organizace a k rizikům identifikovaným na základě posouzení externích a interních ovlivňovatelů dle BMM viz OMG (2015) na cíle organizace, případně na další elementy konkrétního business modelu dané organizace.

V rámci druhého kroku provedeme podrobnou analýzu řešeného business procesu včetně informačního modelu (zejména modelu datových objektů a jejich atributů). Základní přehled o druhém kroku je uveden v tabulce 2.

Tabulka 2: Krok 2 Analýza business procesů; zdroj autorka

CÍL:	Poznání business procesu, u kterého bylo rozhodnuto zavést automatizované zajišťování a prokazování shody a všech relevantních aspektů.
AKTIVITY:	❒ Rekapitulace business plánu organizace ve vztahu k řešenému business procesu, pokud není k dispozici, provede se identifikace cílů organizace a identifikace externích ovlivňovatelů dle BMM viz OMG (2015). ❒ Vytvoření modelu business procesu, včetně topologie procesu v notaci BPMN a včetně informačního modelu (zejména modelu datových objektů a jejich atributů).
VÝSTUPY:	Model business procesu (AS-IS) Revidovaný model motivace businessu ve vztahu k řešenému procesu

4. Krok 3: Analýza rizik a formulování kontrolních cílů

V kroku tři se dostáváme ke konkretizaci zadání pro automatizaci dosahování a prokazování shody. Kroky tři, čtyři a pět jsou vzájemně provázané a podle zkušenosti z případových studií je nutné se z pátého kroku vrátit ke čtvrtému a třetímu kroku a návrh klíčových indikátorů shody (KAI) a klíčových indikátorů bezpečnosti a (KSI) upravit tak, aby odpovídaly realizovatelným návrhům kontrolních aktivit. Podrobnější popis indikátorů KAI a KSI uvádím dále v popisu kroku 5. Je to podobné

jako při návrhu klíčových indikátorů výkonnosti (KPI) business procesů. Často se v praxi setkávám se situací, kdy management organizace navrhne metriky, které ale není možné měřit bez neúměrného úsilí, někdy vůbec ne. Totéž se nám může stát i při návrhu klíčových indikátorů shody a klíčových indikátorů bezpečnosti.

V analýze provozních rizik se musíme zaměřit zejména na externí ovlivňovatele, mezi které řadíme zejména zákony, předpisy a normy tvořící regulatorní požadavky, se kterými je organizace povinna nebo dobrovolně chce dosáhnout shody a být schopna tuto shodu prokazovat. Příklady takových externích ovlivňovatelů jsou například Sarbanes–Oxley Act, Basel III, ISO 270001, ISO 9001 a mnohé další.

Ve finančních institucích se například v rámci procesů tzv. underwritingu, které zahrnuje vyjednávání a uzavírání smluvních závazkových vztahů, setkáváme s pojmem úvěrová rizika. Na rozdíl od provozních rizik úvěrová rizika a jejich řízení představují součást business procesu a v rámci provozních rizik a k opatření k eliminaci úvěrových rizik přistupujeme jako k business aktivitám, nikoliv jako ke kontrolním aktivitám. Toto se ale může případ od případu lišit.

Řada metodických rámců a norem se zaměřuje na různé konkrétní oblasti provozních rizik a doporučuje pro jejich eliminaci konkrétní kontrolní aktivity. Například CoBIT® publikovaný ITG (2007a, 2007b) přinesl návrh kontrolních aktivit eliminujících rizika v oblasti zajištění bezpečné dodávky IT služeb odpovídající potřebám businessu. Speciální vydání NIST 800-53 od NIST (2007) se zaměřuje výhradně na kontrolní aktivity eliminující rizika v oblasti IT bezpečnosti. Pro systém zajišťování a prokazování shody je podstatné podchytit všechna provozní rizika týkající se daného business procesu, protože analýza rizik je základním východiskem pro formulování kontrolních cílů. Představuje vyhodnocení propojení mezi business cíli organizace a externími ovlivňovateli podle Business Motivation Modelu (BMM) viz OMG (2015). Zejména je nutné vyhodnotit vzájemné vztahy mezi externími ovlivňovateli, business cíli organizace, byznys politikami a business pravidly dané organizace ve vztahu k řešenému procesu. Z prvků strategického business plánu je také potřeba identifikovat vazby na další business procesy.

Pro identifikaci, popis a modelování provozních rizik jsou používány různé metody a přístupy, jak jsme popsali například v dokumentu Risk Analysis Modeling, Refsdal et al. (2011). Mimo standard používaný pro řízení rizik v oblasti informační bezpečnosti ISO/IEC 27005:2008 viz ISO (2008) je pro management provozních rizik například k dispozici norma ISO 31000:2009 Risk management – Principles and guidelines viz ISO (2009), která je zaměřena více obecně bez vztahu k jakékoliv specifické funkční oblasti organizace.

Tyto dvě metodiky i další již výše uvedená norma NIST Special Publication 800-53 viz NIST (2007) přistupují k řízení rizik identifikovaných a strukturovaných podle určitých aktiv, která představují součást hmotného a nehmotného majetek organizace. Ontologie modelu rizika a jeho výpočet se u těchto metodik významně liší, takže obvykle není možné jednoduše konsolidovat řízení rizik přes všechny business funkce organizace. Každý funkční útvar organizace totiž používá metody nejlepší praxe, šablony a podpůrné nástroje a systémy pro řízení rizik specifické pro svou oblast. Pro účely zavedení systému dosahování a prokazování shody proto musíme často pracovat s riziky a jejich hodnocením v různých podobách a zdrojích.

Na rozdíl od výše uvedených metodik zaměřených na rizika aktiv, existuje ještě metodický rámec publikovaný a dále rozvíjený a aktualizovaný organizací Comitee of

Sponsoring Organizations of the Treadway Commission (COSO) nazvaný COSO Enterprise Risk Management – Integrated Framework viz COSO (2015). Tento rámec je zaměřený na identifikaci a strukturování rizik podle cílů organizace. Je proto vhodnější a lépe propojitelný s metodikou BMM viz OMG (2015) a určitě stojí za pozornost. Základní přehled o třetím kroku je uveden v tabulce 3.

Tabulka 3: Krok 3 Definice kontrolních cílů a formulování indikátorů
(zdroj autorka)

CÍL:	**Identifikace rizik a definování kontrolních cílů pro daný business proces**
AKTIVITY:	❒ Provedení analýzy rizik procesu ve vztahu k definovanému business plánu a jeho relevantním elementům, zejména k cílům organizace, případně definovaným politikám a business pravidlům (viz. BMM) a k externím vlivům. ❒ Provedení rozdílové analýzy mezi regulatorními požadavky na proces, cíli procesu a současným stavem popsaným v AS-IS analýze business procesu. ❒ Návrh kontrolních cílů a jejich schválení vlastníkem procesu nebo jinou odpovědnou osobou či osobami.
VÝSTUPY:	Identifikovaná a popsaná rizika business procesu Formulované kontrolní cíle daného business procesu

5. Krok 4: Návrh kontrolních aktivit a kontrolních procesů

Kontrolní aktivitou rozumíme nástroj pro eliminaci identifikovaných provozních rizik. Může se například jednat o business politiky, business pravidla, postupy, návody nebo organizační opatření. Mohou mít administrativní, organizační, technický, nebo právní charakter. V rámci metodologie zajišťování a prokazování shody kontrolní aktivitou rozumíme nástroje pro dosažení kontrolních cílů, jež jsme identifikovali a navrhli v kroku třetím.

Ve čtvrtém kroku navrhujeme pro každý identifikovaný a popsaný kontrolní cíl soubor kontrolních aktivit, resp. kontrolní proces. Některá kontrolní aktivita/kontrolní proces může podporovat více kontrolních cílů. Před zahájením realizace kontrolních aktivit/procesů formou návrhu a vývoje kontrolních procesů, je nutné získat souhlas oprávněných osob s jejich zavedením, vždy musí být schváleny minimálně vlastníkem procesu. Kontrolní procesy tak doplní business proces o kontrolní aktivity zajišťující dosažení kontrolních cílů ergo shodu business procesu s požadavky, pro jejichž zajištění byl odpovídající kontrolní cíl navržen. Základní přehled o čtvrtém kroku je uveden v tabulce 4.

Tabulka 4: Krok 4: Návrh kontrolních aktivit a kontrolních procesů; zdroj autorka

CÍL:	Navrhnout kontrolní aktivity resp. kontrolní procesy k zajištění příslušných kontrolních cílů a jejich schválení.
AKTIVITY:	❒ Vytvoření návrhu kontrolních aktivit resp. kontrolních procesů k zajištění kontrolních cílů a jejich schválení. ❒ Modelování kontrolního procesu a jeho ověření (TO-BE) v BPMN, včetně vytvoření informačního modelu.
VÝSTUPY:	Detailní popis kontrolních aktivit a kontrolních procesů. Model kontrolního procesu (TO-BE). Informační model kontrolního procesu, zejména obsahující model datových objektů a jejich atributů pro výpočet indikátorů KSI a KAI.

6. Krok 5: Návrh a formulování indikátorů KSI a KAI

Pro prokazování shody slouží indikátory bezpečnosti (KSI), které vyjadřují míru správného fungování kontrolních procesů. Pro vyhodnocení celkové shody dané instance procesu s relevantními požadavky používáme indikátor zajištění shody KAI.

- **Klíčový indikátor shody** (Key Assurance Indicator = KAI)
  KAI měří správnou funkci kontrol resp. kontrolních aktivit.
- **Klíčový indikátor bezpečnosti** (Key Security Indicator = KSI)
  KSI měří účinnost a úplnost kontrol resp. kontrolních aktivit.

Jinými slovy, KSI nám říká, zda jsou kontrolní aktivity implementovány a používány. Tyto indikátory nám ukazují, jak se nám daří dosahovat stanovených kontrolních cílů.

Indikátory KAI vyjadřují úroveň shody s regulatorními požadavky, kterých daný cílový proces dosahuje, zatímco indikátory KSI vyjadřují úroveň bezpečnosti poskytovanou implementovanými kontrolami, resp. kontrolními procesy. Původní návrh a definice těchto indikátorů vychází z dokumentu Protection and Assessment Model, Julisch (2010, 2011) a Sinclaire (2009). Definice indikátorů byla následně rozvedena a konkretizována v Šabatová (2011b, 2015) s využitím konkrétních příkladů jak indikátory formulovat pomocí jazyka Property Specification Language (PSL) popsaném podrobně například v Accellera (2007). Pro jiné kontrolní cíle uvedených vzorových business procesů či pro úplně jiné business procesy provedeme návrh indikátorů KSI a KAI analogicky.

Pro návrh indikátorů bezpečnosti a indikátorů shody vždy vycházíme z pregnantně formulovaných kontrolních cílů. Návrh kontrolních aktivit a kontrolních procesů z kroku čtvrtého využijeme zejména v oblasti definice datového modelu, protože datové objekty a jejich atributy představují proměnné, které budeme potřebovat pro výpočet hodnot indikátorů pro každou proběhlou instanci procesu. Základní přehled o pátém kroku je uveden v tabulce 5.

Tabulka 5: Krok 5: Návrh indikátorů KAI a KSI; zdroj autorka

CÍL:	Návrh indikátorů (slovní vyjádření) a jejich ověření vůči kontrolním cílům a z hlediska jejich aplikovatelnosti a realizovatelnosti. Definice přesných indikátorů KAI a KSI pomocí formulace kontrolní politiky.
AKTIVITY:	❒ Návrh indikátorů shody (KAI) a indikátorů bezpečnosti (KSI) popisnou formou (lidským jazykem). ❒ Ověření aplikovatelnosti a realizovatelnosti indikátorů, případně jejich úprava. ❒ Vyjádření ověřených indikátorů KSI a KAI formulací kontrolní politiky. ❒ Ověření a validace realizovatelnosti kontrolního procesu ve vztahu k návrhu indikátorů.
VÝSTUPY:	Definované, ověřené a schválené indikátory: indikátor shody (KAI) a indikátor bezpečnosti (KSI).

7. Krok 6: Implementace cílového procesu

Implementace kontrolního procesu představuje jeho integraci s řešeným business procesem, čímž vznikne implementace cílového procesu. Jedná se o kritické místo celého životního cyklu systému zajišťování a prokazování shody. V rámci tohoto kroku musí být v testovacím a později v pilotním prostředí ověřena úplnost navržených kontrolních procesů spolu s ověřením pokrytí všech odpovídajících kontrolních cílů, tedy to, zda je skutečně implementací kontrolních aktivit dosaženo shody a že tuto shodu jsme schopni průběžně prokazovat. Pokud proces ověřování odhalí jakoukoliv nekonzistenci nebo chybějící prvek, musí se implementační tým vrátit do předcházejících kroků v plánovací fázi a neúplný koncept doplnit. V takovém případě obvykle dochází k revizi definice kontrolních cílů, návrhu kontrolních procesů a jejich informačního modelu, ale často musí být také přeformulovány indikátory KAI a KSI.

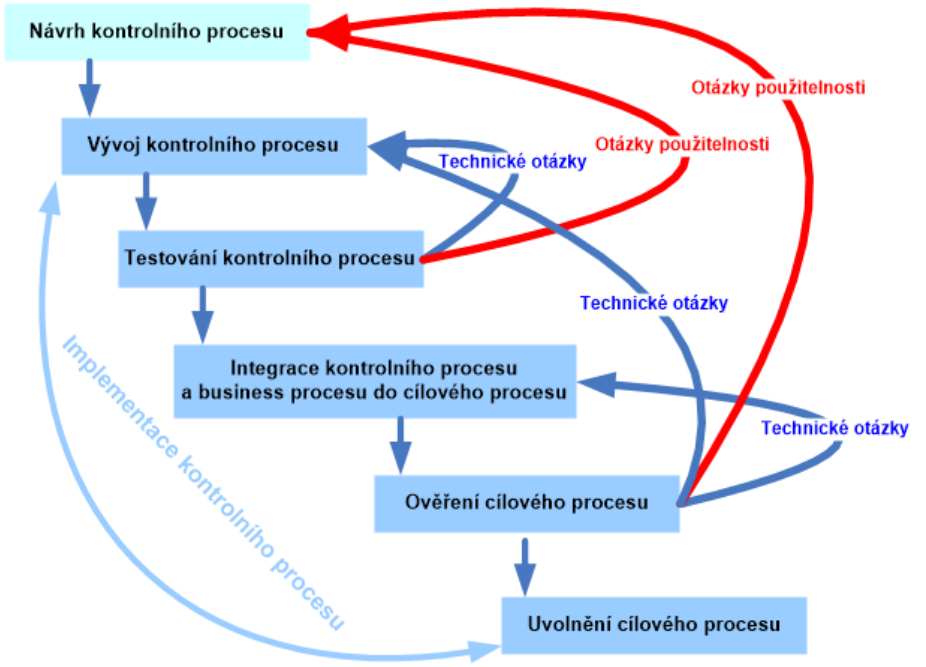
Tabulka 6: Krok 6: Implementace cílového procesu; zdroj autorka

CÍL:	Vyvinout kontrolní procesy k zajištění příslušných kontrolních cílů a integrovat je v rámci business procesu a tím dosáhnout implementace cílového procesu.
AKTIVITY:	❒ Vyvinutí kontrolního procesu včetně integrace na podpůrné systémy. ❒ Cyklické ověřování cílového procesu formou standardního nebo rozšířeného procesu uvolňování IT služeb. ❒ Vytvoření dokumentace a proškolení vykonavatelů cílového procesu a jeho managementu (vlastníka procesu, dispečera a dalších).
VÝSTUPY:	Plně otestovaný a zdokumentovaný cílový proces implementovaný do produkčního prostředí.

Na obrázku 3 je zobrazena tzv. implementační kaskáda kontrolního procesu, která znázorňuje testovací postupy používané v průběhu implementace kontrolního procesu. Podobně jako při použití známého V-modelu z metodiky ITIL Service Transition publikované OCG (2007c) musíme testovat postupně kvalitu technické

realizace oproti detailnímu návrhu kontrolního procesu, ale výsledky integračních testů se již verifikují vůči formulovaným kontrolním cílům, resp. jejich dosažení a zajištění. Tento postup jsem popsala podobněji v kapitolách o implementaci cílového procesu v metodickém dokumentu od Karjoth et al. (2011, 2011b).

Během implementace cílového procesu je nutné postupovat podle standardních postupů managementu uvolňování a managementu změny, jak jsou zavedeny a uplatňovány v dané organizaci. Hlavním výstupem tohoto kroku je plně otestovaný a zdokumentovaný cílový proces implementovaný do produkčního prostředí. Součástí implementace musí být také zaškolení všech vykonavatelů aktivit v rámci cílového procesu, případně dalších spolupracujících osob a managementu. Základní přehled o šestém kroku je uveden v tabulce 6.



Obrázek 3: Implementační kaskáda kontrolního procesu; zdroj: autorka

8. Krok 7: Průběžné měření a vyhodnocování indikátorů KSI a KAI

V prostředí servisně orientované architektury s využitím některé platformy Business proces management systému (BPMS) pro automatizaci cílového procesu probíhá měření indikátorů KSI a KAI kontinuálně. Obdobně jako může dispečer odpovědný za

výkon procesu a dosahování požadovaných indikátorů výkonnosti KPI průběžně (a tím je míněno skutečně v reálném čase) sledovat plnění klíčových ukazatelů výkonnosti či vytíženost kapacit zdrojů procesu nad jeho jednotlivými instancemi i nad procesem jako celkem, může osoba odpovědná za řízení shody, tj. například interní auditor, průběžně sledovat i indikátory bezpečnosti a indikátory shody procesu s jednotlivými odpovídajícími kontrolními cíli.

Takový systém umožňuje kontrolovat stav shody procesu s regulatorními požadavky kdykoliv a v případě indikace jakéhokoliv nedodržení shody okamžitě použít nápravná opatření, nebo alespoň neprodleně upozornit na daný problém a řešit jej. Základní přehled o sedmém kroku je uveden v tabulce 7.

Tabulka 7: Krok 7: Průběžné měření a vyhodnocování indikátorů KAI a KSI; zdroj autorka

CÍL:	Zajistit okamžitou reakci v případě neshody s regulatorním požadavkem.
AKTIVITY:	❒ Sledování hodnot indikátorů KSI a KAI v reálném čase. ❒ V případě zjištění neshody zajistit realizaci nápravných opatření.
VÝSTUPY:	Výkazy o shodě business procesu resp. cílového procesu s regulatorními požadavky. Nápravná opatření v případě neshody a jejich dokumentace.

9. Krok 8: Systematické vyhodnocování systému zajišťování a prokazování shody

Mimo průběžného sledování shody business procesu resp. cílového procesu s odpovídajícími regulatorními požadavky, jak je nastaveno v předchozím kroku, je také potřeba vyhodnocovat systém zajišťování a prokazování shody v pravidelných intervalech, anebo mimořádně při vzniku jakékoliv události, která má na tento systém vliv. Takovými událostmi jsou zejména:

- ❒ Změna strategického business plánu, která se promítá do změny modelu motivace businessu (BMM), nebo jen do některých jeho prvků.
- ❒ Jakákoliv změna business procesu, zejména požadavků na výkon business procesu, nebo zásadní změna v alokaci zdrojů na zajištění daného business procesu.
- ❒ Změna externích ovlivňovatelů business procesu, která se projeví v rámci analýzy rizik některého regulatorního požadavku na zajištění shody, a která ovlivní definici kontrolních cílů procesu.

Tabulka 8: Krok 8: Systematické vyhodnocování systému zajišťování a prokazování shody; zdroj autorka

CÍL:	Zajistit kontinuální relevanci systému zajišťování a dosahování shody.
AKTIVITY:	❒ Zjištění změn majících vliv na daný proces a zajištění jeho shody s regulatorním požadavkem. ❒ V případě dopadu změn na kterýkoliv prvek systému zajišťování a dosahování shody iniciace nové iterace jeho životního cyklu.
VÝSTUPY:	Analýza relevantnosti implementovaného systému zajišťování a prokazování shody včetně případného doporučení.

V pravidelných i mimořádných revizích je zejména potřeba analyzovat relevantnost implementovaného systému zajišťování a prokazování shody vůči aktuálním regulatorním a dalším požadavkům na daný proces. Obzvláště ve vysoce regulovaném a turbulentně proměnlivém prostředí je takováto pravidelná analýza kategorickým imperativem. V tomto kroku musíme formulace kontrolních cílů a všechny od nich odvozené prvky systému zajišťování a prokazování shody konfrontovat s aktualizovaným business plánem organizace a s aktualizovaným výsledkem analýzy rizik. Základní přehled o osmém kroku je uveden v tabulce 8.

10. ZÁVĚR

Navržená metodika zajišťování a prokazování shody je konceptuálním modelem využitelným nezávisle na konkrétních použitých technologických platformách Business Proces Management Systémů a systémů servisně orientované architektury. Může být jakýmsi uceleným vodítkem či inspirací pro interní auditory, analytiky procesů, business architekty i IT systémové architekty při řešení jejich úloh v oblasti řízení rizik souvisejících s potenciálním nedodržením regulatorních či jiných požadavků na business procesy dané organizace.

ZDROJE

Accellera, 2004: Property Specification Language Reference Manual Version 1.1 URL: http://www.eda.org/vfv/docs/PSL-v1.1.pdf

COSO, 2015: Enterprise Risk Management - Integrated Framework. Committee of Sponsoring Organizations of the Treadway Commission. URL: http://www.coso.org/publications/executive_summary_integrated_framework.htm

Doucek P., Novak L., Svatá V., 2008: *Řízení bezpečnosti informací*. Professional Publishing. ISBN 978-80-86946-88

ISO, 2008: ISO/IEC 27005:2008 Information technology - Security techniques - Information security risk management

ISO, 2009: ISO 31000:2009 Risk management – Principles and guidelines.

ISO, 2015: ISO 9001:2015 Quality management systems – Requirements, International Standardization Organization

ITGI, 2007: CoBIT® 4.1. IT Governance Institute. ISBN 1-933284-72-2

ITGI, 2007b: IT Assurance Guide: Using CoBIT® 4.1. IT Governance Institute. ISBN 1-933284-74 9

Julisch K., Miseldine P., Lim H.W., Bielova N., Neuhaus S., Refsdal A., Presenza D., Gallego-Nicasio Crespo B.. Kearney P., 2010: D2.1.2 *Protection and Assessment Model for Multiple Trust Domain.* Official public deliverable of MASTER FP7 216917

Julisch K., Miseldine F., Lim H.W., Bielova N., Neuhaus S., Refsdal A., Presenza D., Gallego-Nicasio Crespo B., Kearney P., Sinclair D., Neisse R., 2011: D2.1.3: *The MASTER Final Protection and Assessment Model.* Official public deliverable of MASTER FP7-216917

Jurič M.B., Mathew Benny, Sarang P., 2006: *Business Process Execution Language for Web Services*. Packt Publishing Ltd. ISBN 1-904811-81-7

Karjoth G., Asnar Y., Louat B., Cui Z., Scholte T., Sinclair D., Sabatova I., 2011: D3.1.3: *Methodology Handbook v.3.* Official public deliverable of MASTER FP7 216917

Karjoth G., Asnar Y., Louat B., Cui Z., Scholte T., Sinclair D., Sabatova I., 2011b: The MASTER Methodology – a Handbook for Practitioners. Official public deliverable of MASTER FP7-216917

NIST, 2007: NIST Special Publication 800-53. National Institute of Standards and Technology, US Department of Commerce, revision 2, 2007. URL: http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf

OMG, 2013: Business Process Model and Notation (BPMN) Version 2.0.2. OMG Document Number: dtc/2009-08-14. URL: http://www.omg.org/spec/BPMN/2.0

OMG, 2015: Business Motivation Model Version 1.3. OMG Standard Document Number: formal/2015-05-19. URL: http://www.omg.org/spec/BMM/1.3

OMG, 2015b: Semantics of Business Vocabulary and Business Rules (SBVR) Version 1.3. OMG Document Number: formal/2015-05-07.
URL: http://www.omg.org/spec/ SBVR/1.3/PDF

Refsdal A., Stølen K., Asnar Y., Kearney P., Di Giacomo V., Presenza D. Sabatova I., Svojanovsky P., 2011: D1.1.3: *Risk Analysis Modelling*. Official public deliverable of MASTER FP7-216917

Šabatová I., Svojanovský P., 2011: D1.3.4: *Security Compliance Guidelines*. Official public deliverable of MASTER FP7-216917

Šabatová I., 2011b: *Kontinuální řízení shody v servisně orientovaných systémech*. Sborník prací účastníků vědeckého semináře doktorského studia 17. února 2011. Vysoká škola ekonomická, Fakulta informatiky a statistiky. Nakladatelství Oeconomia, 2011. ISBN 978-80-245-1761-2

Šabatová I., 2015: Building Assurance of Regulatory Compliance in Dynamic Service Oriented Systems. *Journal of Systems Integration* Vol 6, No 2, pp. 15-31, ISSN: 1804-2724

Sinclair D., Neuhaus S., Gallego-Nicasio-Crespo B., 2009: D3.3.1: *Specification of PRM property language and semantic model for verification and validation*. Official deliverable of MASTER FP7-216917

Sinur J, Schulte W. R., Hill J.B., Jones T., 2012: Magic Quadrant for Intelligent Business Process Management Suites. *Gartner report G00224913*

JEL Classification: G21, M15