

CobiT® 4.1 a jeho vzťah k ITIL®



Autor: Jiří Skála

Kontakt: jiri.skala@itsmf.cz

Spoločnosť: itSMF Czech Republic

Dátum: 6. február 2008

**Odborná konferencia *itSMF* Slovensko
Riadenie IT služieb na Slovensku**

***itSMF* Slovensko**

Agenda

- Obsah a struktura CobiT[®] 4.1
- Rozsah a spôsob popisu IT procesů v CobiT[®] 4.1
- Rozšíření CobiT[®] 4.1 o koncept Value IT
- Vzájemný vztah CobiT[®] a ITIL[®]
- Implementace IT procesů s využitím CobiT[®] a ITIL[®]

IT management versus IT governance

- **IT management** se soustředí na efektivní poskytování služeb a produktů IT a na účinné řízení rozvoje a provozu IT
- Snahou **IT managementu** je efektivně a účinně realizovat stanovené cíle, a proto se orientuje na taktické a operativní řízení
- **IT management** je realizován zejména v rámci útvarů IT
- Mezinárodně uznávaným rámcem **IT managementu** je ITIL®
- **IT governance** je odpovědností nejvyššího vedení, které svým příkladem, organizačním uspořádáním a vnitřními procesy zajišťuje, že IT přispívá a prohlubuje strategii a dlouhodobé cíle organizace
- **IT governance** má širší pojetí a jeho snahou je definovat strategické cíle IT v souladu s potřebami a zájmy celé organizace
- Mezinárodně uznávaným rámcem **IT governance** je CobiT®

Zdroj: Sborník přednášek konference ICTM 2005, str. 44

Co je CobiT[®]?

- CobiT[®] = Control Objectives for Information and related Technology
- CobiT[®] Mission:
 - „To research, develop, publicise and promote an authoritative, up-to-date, internationally accepted IT governance control framework for adoption by enterprises and day-to-day use by business managers, IT professionals and assurance professionals“ (Zdroj: CobiT 4.1, Framework)
 - Zkoumat, vyvíjet, publikovat a rozšiřovat směrodatný, aktuální a mezinárodně přijímaný řídicí rámec IT governance určený k podnikovému nasazení a každodennímu používání business manažery, IT odborníky a specialisty na oblast „assurance“
- CobiT[®] umožňuje prezentovat IT činnosti vůči okolí, jež nemá detailní znalosti o IT prostředí a o IT technologiích
- Cílem CobiT[®] je vytvořit rámec pro řídicí a kontrolní systém fungující nad IT prostředím, který bude nastaven ve shodě s ostatními řídicími a kontrolními systémy podniku

Historie CobiT

- Vlastníkem CobiT je **ITGI (IT Governance Institute)** založený v roce 1998 sdružením **ISACA (Information Systems Audit and Control Association)**.
 - Historie verzí:
 - **CobiT 1st Edition** vyšel v roce 1996 (vydavatelem je ISACA)
 - **CobiT 2nd Edition** vyšel v roce 1998 (vydavatelem je již ITGI)
 - **CobiT 3rd Edition** vyšel v roce 2000
 - **CobiT 4.0** vyšel v prosinci 2005

CobiT 4.0 je rozšířením CobiT 3rd Edition, tzn. že (podle ITGI):

 - CobiT 4.0 nenahrazuje CobiT 3rd Edition
 - Implementace systémů IT governance podle CobiT 3rd Edition zůstávají platné a jsou plně kompatibilní i s CobiT 4.0 - **CobiT 4.1** vyšel v dubnu 2007
- CobiT 4.1 je částečnou aktualizací CobiT 4.0

Obsah CobiT[®] 4.1

- CobiT[®] 4.1 je dvousetstránkový PDF dokument, který obsahuje:
 - **Executive Overview** = 4-stránkový manažerský souhrn účelu CobiT[®]
 - **CobiT[®] Framework** = 20-stránkový popis koncepce CobiT[®] a způsobu jeho používání
 - Popis **34 procesů** rozdělených do **4 domén** (viz násl. snímek)
 - Pro každý z těchto procesů je definován:
 - **Process description** = cíl a účel procesu (1 str. A4)
 - **Control objectives** = několik dílčích kontrolních cílů (1-3 str. A4)
 - **Management guidelines** = definice vstupů do / výstupů z ostatních procesů, seznam klíčových aktivit procesu a rolí, resp. funkcí, které je provádějí (RACI matice), cíle a metriky (1 str. A4)
 - **Maturity model** = kritéria vyspělosti procesu pro zařazení na škále 0 – 5
 - **8 příloh** = celkem 44 stran, mimo jiné i slovník pojmů

Seznam IT procesů podle CobIT[®] 4.1

• **PO – Plan and Organise**

- PO1 Define a Strategic IT Plan
- PO2 Define the Information Architecture
- PO3 Determine Technological Direction
- PO4 Define the IT Processes, Organisation and Relationships
- PO5 Manage the IT Investment
- PO6 Communicate Management Aims and Direction
- PO7 Manage IT Human Resources
- PO8 Manage Quality
- PO9 Assess and Manage IT Risks
- PO10 Manage Projects

• **AI – Acquire and Implement**

- AI1 Identify Automated Solutions
- AI2 Acquire and Maintain Application Software
- AI3 Acquire and Maintain Technology Infrastructure
- AI4 Enable Operation and Use
- AI5 Procure IT Resources

• **DS – Deliver and Support**

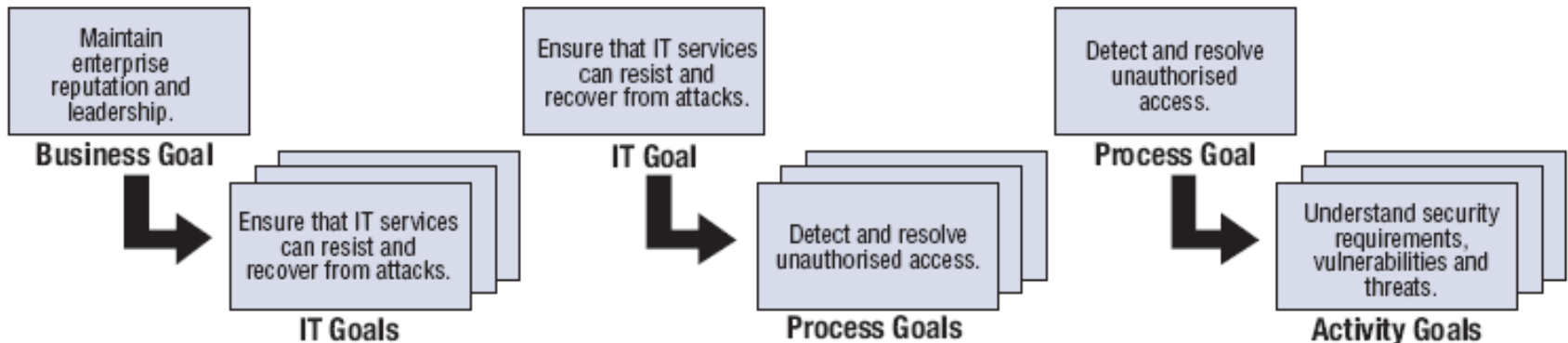
- DS1 Define and Manage Service Levels
- DS2 Manage Third-party Services
- DS3 Manage Performance and Capacity
- DS4 Ensure Continuous Service
- DS5 Ensure Systems Security
- DS6 Identify and Allocate Costs
- DS7 Educate and Train Users
- DS8 Manage Service Desk and Incidents
- DS9 Manage the Configuration
- DS10 Manage Problems
- DS11 Manage Data
- DS12 Manage the Physical Environment
- DS13 Manage Operations

• **ME – Monitor and Evaluate**

- ME1 Monitor and Evaluate IT Performance
- ME2 Monitor and Evaluate Internal Control
- ME3 Ensure Compliance With External Requirements
- ME4 Provide IT Governance

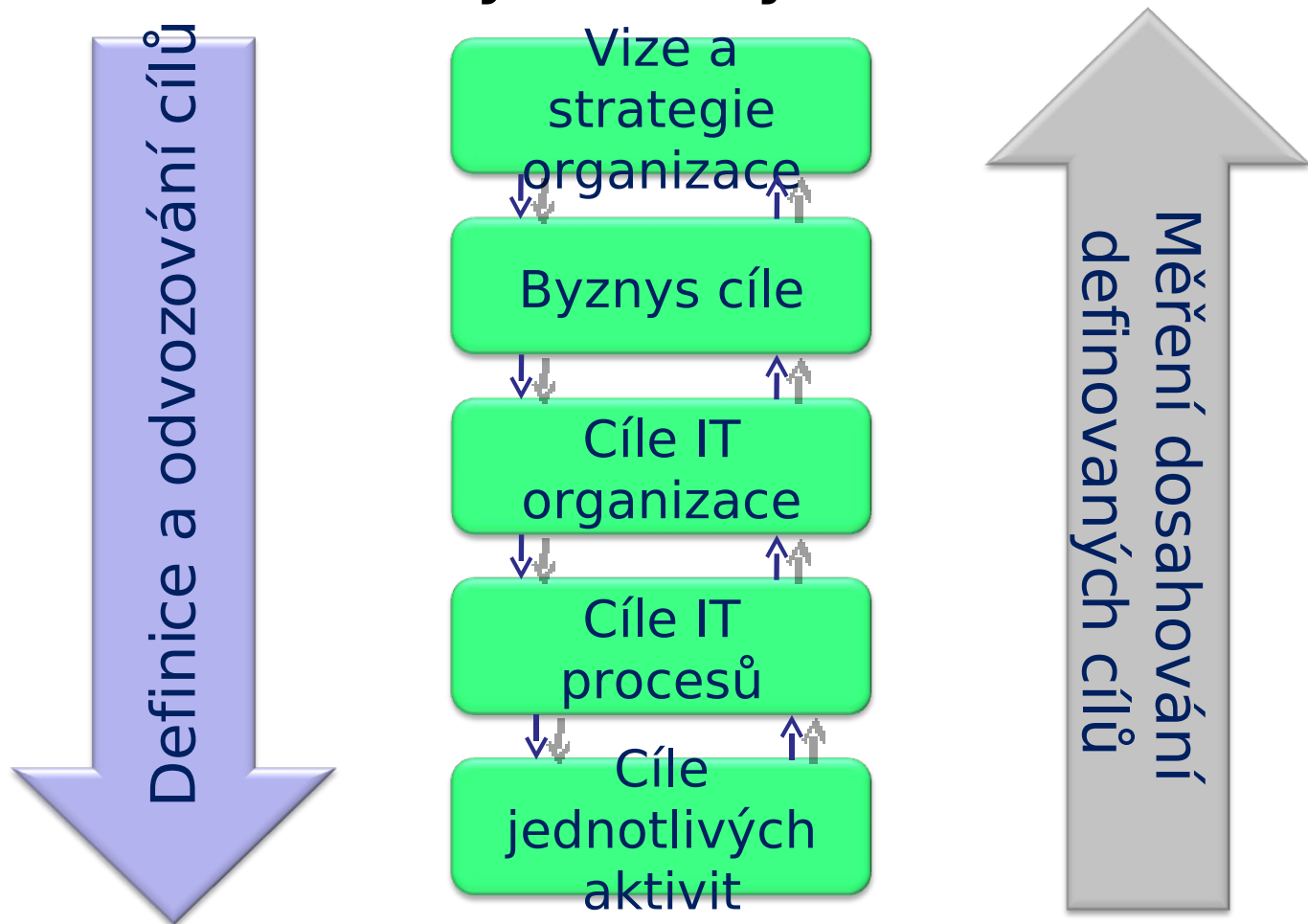
Hierarchizace cílů (princip)

- CobiT[®] 4.1 obsahuje (mimo jiné):
 - Výčet sedmnácti podnikových cílů majících přímý vztah k IT (tzv. „IT-related business goals“) uspořádaných do čtyř dimenzí podle metodiky Balanced Scorecard
 - Výčet 28 strategických IT cílů (tzv. „IT goals“)
 - Mapování výše uvedených podnikových cílů na strategické IT cíle
 - Mapování těchto IT cílů na procesní cíle každého z 34 IT procesů



Zdroj: CobiT[®] 4.1, diagram 16

Diagram vztahů mezi cíli jednotlivých úrovní



Zdroj: Jan Tolar, HP

Ukázka vzájemného provazování cílů

Business Goals		IT Goals					CobIT Information Criteria						
							Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
1	Zvýšení podílu na trhu	10	16				∨	∨					
2	Růst příjmů	10	16				∨	∨					
3	Řízení provozních rizik	2	8	9	10	21			∨	∨	∨		
4	Trvalá dostupnost služeb	...											
5	Nabídka konkurenceschopných služeb	...											
6	Redukce provozních nákladů	...					∨	∨					
7	Shoda s interními předpisy	...											
8											
9											
10											
11											

IT Goals		IT Processes					CobIT Information Criteria						
							Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
1	...	PO1	PO2	PO10	AI1	ME1	P	P		S	S		
2	Zajištění shody s požadavky na řízení IT	PO1	PO4				P	P					
...	...	PO1	PO4				P	P					
8	Správa a ochrana IT majetku	PO9	DS5	DS9	DS12	ME2	S	S	P	P	P	S	S
9							
10	Realizace projektů on time/on budget a v odpovídající kvalitě	PO8	PO10				P	P		S			S
...							
16	Zajištění nákladově efektivní kvality služeb a připravenosti na změny	PO5	DS6	ME1	ME3		P	P					P
...							
21	Zajištění důvěryhodnosti automatizovaných byznys transakcí	PO6	AI7	DS5			P			P	S	S	
22							
23							
24							
25							

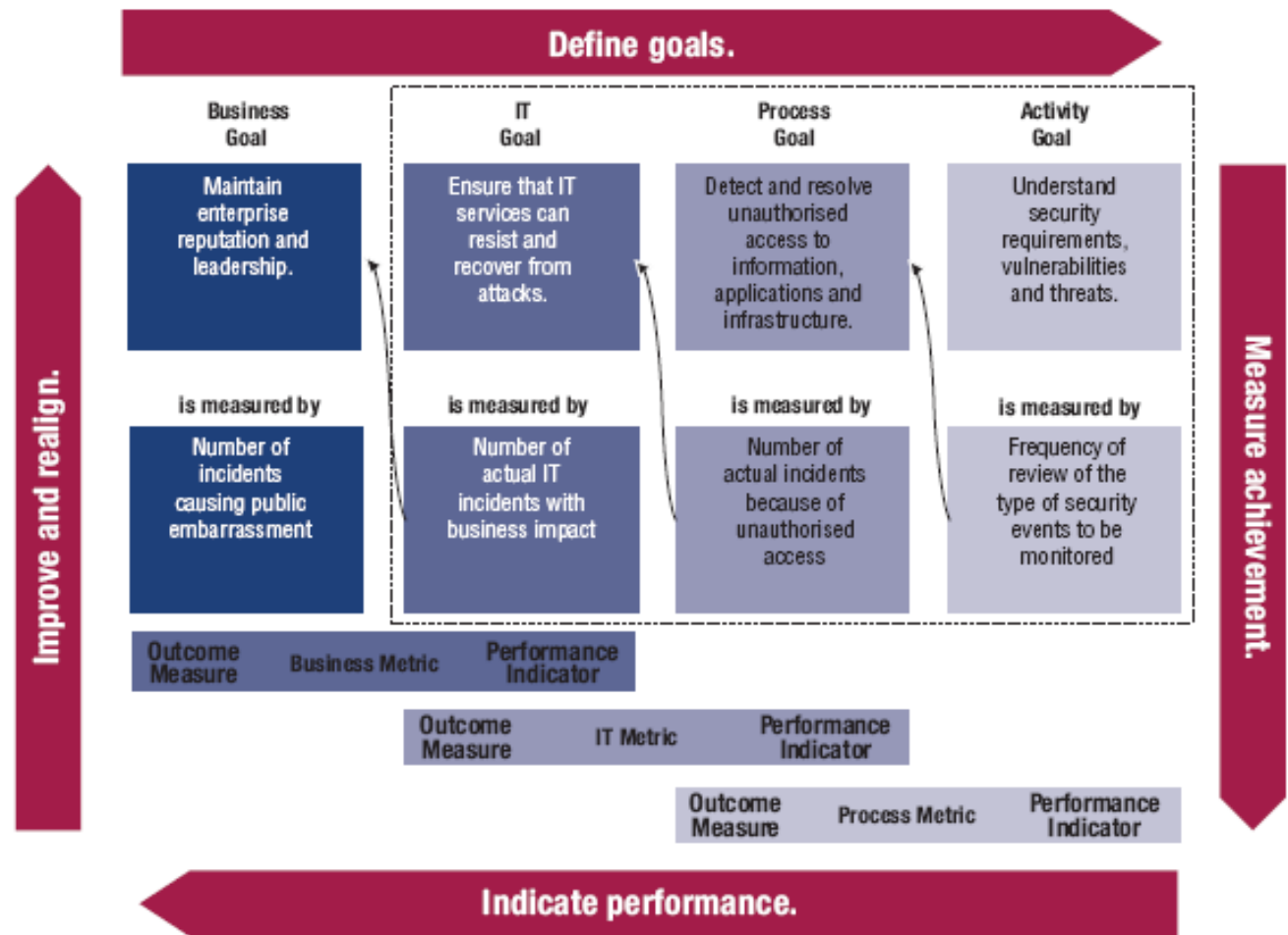
Zdroj: Jan Tolar, HP

Metriky v CobiT[®] 4.1

- Míru dosahování cílů je třeba měřit, a to ze dvou pohledů pomocí tzv.:
 - **Outcome measures** = tzv. **'lag indicators'**, které měří výsledek, tzn. měří to, zda bylo dosaženo cíle; v CobiT 3rd Edition tzv. **'Key Goal Indicators'** (KGI)
 - **Performance indicators** = tzv. **'lead indicators'**, které jsou indikací toho, zda bude cíle dosaženo, tedy vypovídají o pravděpodobném výsledku dříve, než je výsledek samotný znám; v CobiT 3rd Edition tzv. **'Key Performance Indicators'** (KPI)
- **Outcome measures** vztahující se k cílům jedné úrovně lze zároveň považovat za **performance indicators** vztahující se k cílům vyšší úrovně – příklad viz násl. snímek

Konkrétní příklad „dvojjedinosti“ metrik v CobiT[®] 4.1

- Uvedený příklad se vztahuje k procesu „DS5 Ensure Systems Security“
- CobiT[®] 4.1 tedy již nedefinuje dvě množiny metrik (KGI a KPI) jako tomu bylo ve verzi 3rd Edition, ale definuje metriky pro jednotlivé hierarchické stupně cílů



Zdroj: CobiT 4.1, diagram 19

Hlavní přínosy CobiT[®] 4.1

- CobiT[®] 4.1 představuje snadno uchopitelný auditní a řídicí rámec, který umožňuje přímo a konkrétním způsobem propojit IT strategii s celopodnikovou strategií, resp. nastavit řízení IT prostředí ve shodě s požadavky businessu. To je umožněno především:
 - Hierarchizací cílů, tj. vydefinováním podnikových cílů majících přímý vztah k IT, jejich namapováním na konkrétní IT cíle a provázáním těchto IT cílů s procesními cíly
 - Vydefinováním metrik pro měření cílů na všech hierarchických stupních
 - Vydefinováním IT procesů, které umožňují dosahovat těchto cílů, a způsobu měření jejich vyspělosti („maturity levels“)
- CobiT[®] 4.1 zahrnuje všechny aspekty a oblasti řízení IT prostředí
- Další přednosti CobiT[®] 4.1 oproti předchozím verzím:
 - Procesní rámec podle CobiT[®] 4.1 je v souladu s ITIL[®] a ISO/IEC 20000
 - Metriky jsou lépe konstruovány s ohledem na možnost jejich získávání
 - Popis procesů je dobrým základem pro jejich implementaci
- CobiT[®] 4.1 stejně jako mnoho dalších publikací ITGI je volně ke stažení na webových stránkách www.isaca.org

Value IT Framework – Val IT™

- Val IT™ je dalším produktem ITGI; byl publikován v březnu 2006
- Val IT™ rozšiřuje a doplňuje CobiT® o oblast řízení investic do IT. Vztah mezi Val IT™ a CobiT® nejlépe ilustruje tato citace:
 - „Val IT focuses on the investment decision (are we doing the right things?) and the realisation of benefits (are we getting the benefits?), while CobiT focuses on the execution (are we doing them the right way, and are we getting them done well?)“ (Zdroj: z The Val IT Framework, str. 7)
 - Jinými slovy, rámec IT governance se skládá z CobiT® a Val IT™. Např. publikace ITGI o implementaci IT governance má název **IT Governance Implementation Guide: Using COBIT® and Val IT™** a anotace k této publikaci zní: „Provides a generic road map for implementing IT governance using the CobiT® and Val IT™ resources“
 - Smyslem a cílem Val IT™ je zajištění toho, že podnik dostává optimální hodnotu z investic do IT, a to při přiměřených nákladech a akceptovatelné míře známých rizik. Val IT™ nabízí podnikovému managementu a zejm. nejvyššímu vedení sadu procesů a doplňujících praktik, jež jim usnadní výkon a porozumění jejich rolím v oblasti řízení těchto investic

Obsah Val IT™

- Val IT™ se skládá ze 3 základních dokumentů (na dalších se pracuje):
 - Val IT Framework (32 stran)
 - Popisuje principy řízení IT investic a zavádí 3 nové procesy IT governance:
 - **Value Governance** – strategický rámec řízení a kontroly investic
 - **Portfolio Management** – řízení portfolia IT projektů/programů, schvalování investic atd.
 - **Investment Management** – řízení jednotlivých IT projektů/programů v celém jejich ekonomickém životním cyklu
 - Pro každý z těchto 3 procesů definuje 11 – 15 klíčových aktivit a:
 - každou z nich mapuje na související kontrolní cíle jednotlivých CobiT® procesů
 - pro každou definuje rozdělení odpovědností (dle RACI principu) mezi executive management, business management a IT management
 - » Pouze u 5 z celkem 40 aktivit je IT mng. tzv. Responsible nebo Accountable
 - Val IT Business Case (28 stran) – popis konstrukce a struktury

Vztah mezi CobiT[®] a ITIL[®] (1)

- Principy procesů podle CobiT[®] 4.1 a ITIL[®] jsou shodné, ale:
 - Názvy některých procesů a obsah některých definic se někdy mírně liší
 - ITIL[®] neobsahuje některé potřebné IT procesy, např. řízení lidských zdrojů, řízení projektů
- Existuje mnoho tabulek mapujících navzájem procesy podle CobiT[®] a ITIL[®]
 - Na toto téma existují i dvě publikace od ITGI – ta aktuálnější se jmenuje **COBIT Mapping: Mapping of ITIL With COBIT 4.0** a obsahuje mapování jednotlivých kontrolních cílů procesů dle CobiT[®] 4.0 na příslušné procesy ITIL V2 a ještě podrobněji na konkrétní odstavce knih, zejm. **Service Support** a **Service Delivery**
 - Matice vztahů mezi procesy CobiT a ITIL je typu **m:n**
- Vývoj CobiT[®] a ITIL[®] probíhá za vzájemné spolupráce ITGI, OGC ISACA, itSMF – v posledních verzích obou rámců byly odstraněny všechny zásadní vzájemné nekonzistence, takže nic nebrání tomu, používat oba přístupy současně

Vztah mezi CobiT[®] a ITIL[®] (2)

- CobiT[®] a ITIL[®] mají jiný účel a principiálně slouží odlišným skupinám lidí:
 - ITIL[®] je určen IT manažerům všech úrovní řízení, jimž poskytuje prakticky použitelný návod pro uchopení managementu zdrojů, požadavků, událostí, prvků IT infrastruktury atd.
 - CobiT[®] je určen především následujícím třem skupinám osob, nacházejícím se vně úseku IT:
 - **Management** – rozhoduje o výdajích do rozvoje a provozu IT a posuzuje, zda jsou tyto výdaje správně a efektivně využívány ⇒ CobiT[®] je nástrojem pro definici rámce řízení IT a usnadňuje orientaci managementu v pro ně nečitelném IT prostředí
 - **Uživatelé** – mají stále vyšší potřebu seznámit se s fungováním IT a nalézt přiměřené záruky za správné a bezpečné fungování IT služeb, které využívají
 - **Auditoři** – při své práci neustále naráží na využívání IT. V tomto směru CobiT[®] poskytuje základní rámec pro to, jakým způsobem hodnotit správnost a vhodnost nasazení IT vzhledem k posuzované části organizace

(Zdroj: Sborník přednášek konference ICTM 2005, str. 45)

- ~~Od vydání verze CobiT[®] 4.0 se již dá mluvit o tom, že CobiT[®] mohou efektivně využívat i IT manažeré a specialisté při návrhu a řízení IT~~

Současné používání CobiT[®] a ITIL[®] (1)

- Při designu IT procesů je možno primárně vycházet buďto z CobiT[®] nebo z ITIL[®]
 - CobiT[®] oproti ITIL[®] obsahuje propracovanější systém měření procesů ve vazbě na cíle, a navíc i způsob měření vyspělosti procesů
 - ITIL[®] oproti CobiT[®] obsahuje desítky best practices pro design a řízení procesů, základní procesní schémata, vzory a šablony některých dokumentů, přičemž tyto best practices jsou stále průběžně doplňovány
- Způsob používání CobiT[®] a ITIL[®] je primárně daný velikostí podniku:
 - Pro malé podniky by použití rámce CobiT[®] pravděpodobně přineslo nákladově neodůvodněný nárůst provozních nákladů i administrativy a samozřejmě i vysoké náklady na implementaci samotných procesů
 - Pro velké podniky (cca stovky IT specialistů) je optimální vycházet z

Současné používání CobiT[®] a ITIL[®] (2)

- Není příliš obvyklé implementovat v jednom podniku některé procesy podle CobiT[®] a některé podle ITIL[®], přestože ani takový způsob není z principu zcela vyloučen
- Doporučený postup je:
 - Podrobně se seznámit s tím, jakou strukturu procesů nabízí nejaktuálnější verze CobiT[®] a ITIL[®]
 - Pokud je množina procesů nabízených v ITIL[®] dostačující, používat při jejich implementaci CobiT[®] jako doplňující zdroj informací, a to zejména v těchto oblastech:
 - Definice procesních metrik
 - Definice odpovědností zúčastněných rolí/funkcí (RACI matice)
 - Definice implementačního projektu, zejm. sestavení business case
 - Pokud množina procesů nabízených v ITIL[®] dostačující není, zvolit jako základ řídicího rámce CobiT[®], a při implementaci pak využívat jednotlivé best practices podle ITIL[®], zejména definici dílčích procesních aktivit, doporučení pro tvorbu dokumentace a šablon atd.

Závěrečné shrnutí

- **CobiT[®]** je mezinárodně uznávaným standardem pro **IT governance**, což je strategický rámec pro řízení IT prostředí, jehož smyslem je zajistit soulad mezi řízením podnikové informatiky a podnikového businessu
- **Val IT[™]** doplňuje IT governance o oblast řízení IT investic – v tomto ohledu tedy představuje rozšíření CobiT[®]
- **ITIL[®]** je mezinárodně uznávaným standardem pro oblast **IT managementu** a je plně kompatibilní se současnou verzí CobiT[®] 4.1
- Přestože lze CobiT[®] a ITIL[®] používat každý samostatně, je možné s výhodou využít silných stránek každého z nich:
 - CobiT[®] : propracovaný systém procesního měření
 - ITIL[®] : desítky tipů, návodů, diagramů, šablon a dalších best practices pro design a správu procesů a řízení IT služeb