# Otázky k předmětu Řízení kvality (audit) IS:

13 Popište cíl, principy a vazby metodiky IT Assurance Guide k metodice Cobit? Popište životní cyklus auditu podle dokumentu IT Assurance Guide.

**IT Assurance Giude** je založen na etapách a činnostech (testech), které jsou společné každému auditu.

**IT Assurance Guide**: Using COBIT je jedním z devíti základních dokumentů tvořících COBIT 4.1. Představuje společně s IT Governance Implementation Guide: Using COBIT and Val IT dokumenty určené auditorům, resp. assurance profesionálům. Cílem tohoto dokumentu je poskytnout návody pro jednotlivé etapy a činnosti životního cyklu auditu a ujištění 🡺 tj. kroky, které musí auditor realizovat a jaké druhy testů je třeba provést ve vazbě na procesy COBIT 4.1

Obsahově IT Assurance Guide navazuje na Cobit 4.1, především na cast věnovanou kontrolním cílům. Umožňuje tak provést audit/ujištění procesu vzhledem k těmto doporučeným cílům.

**AUDIT** = objektivní ověření stavu, jevu, záměru, skutečnosti se stavem nebo jevem žádoucím, tj. modelem, normou, standardem apod.

x

**UJIŠTĚNÍ** (assurance) = audit delegovaný na jiné subjekty vzhledem k cílům řízení, tedy vytvoření závěru o zkoumaném předmětu, za který je odpovědný někdo jiný.

Každý projekt ujištění splňovat pět vlastností:

1. musí jít o *vztah mezi třemi partnery*: poskytovatelem ujištění, odpovědnou stranou za hodnocený projekt a příjemcem výstupu;
2. musí být *definován předmět ujištění*;
3. musí být *definována vhodná kritéria ujištění*;
4. musí být *definován proces ujištění*;
5. musí být *zformulován závěr ujištění*.

Životní cyklus auditu/ujištění dle IT Assurance Guide má 3 etapy:

* Plánování
  + Stanovení základních parametrů projektu ujištění
  + Předběžný výběr vhodného kontrolního rámce (Cobit, COSO, ISO)
  + Plánování projektu ujištění na základě analýzy rizika
  + Realizování obecného hodnocení
  + Stanovení rozsahu a definování obecných cílů iniciativy.
* Stanovení rozsahu
  + Business cíle
  + IT cíle
    - klíčové IT procesy a IT zdroje
      * Klíčové kontrolní cíle
        + Přizpůsobené klíčové kontrolní cíle
* Realizace.
  + Upřesnění porozumění objektu ujištění
  + Upřesnění rozsahu kontrolních cílů hodnoceného objektu
  + Testování efektivnosti návrhu kontrol klíčových kontrolních cílů
  + Testování výstupu klíčových kontrolních cílů
  + Zdokumentování vlivu nalezených slabin kontrol
  + Zformulování a zveřejnění celkového závěru a doporučení.

IT Assurance Guide poskytuje doporučení na několika úrovních:

* **procesně specifická doporučení** jakým způsobem ověřit zda bylo dosaženo kontrolních cílů a jakým způsobem dokumentovat zjištěné slabiny a
* na úrovni kontrolních cílů **doporučení plynoucí z testování návrhu kontrol** pro každý specifický kontrolní cíl.

Poskytuje rovněž generická doporučení aplikovatelná na všechny procesy a kontrolní cíle.

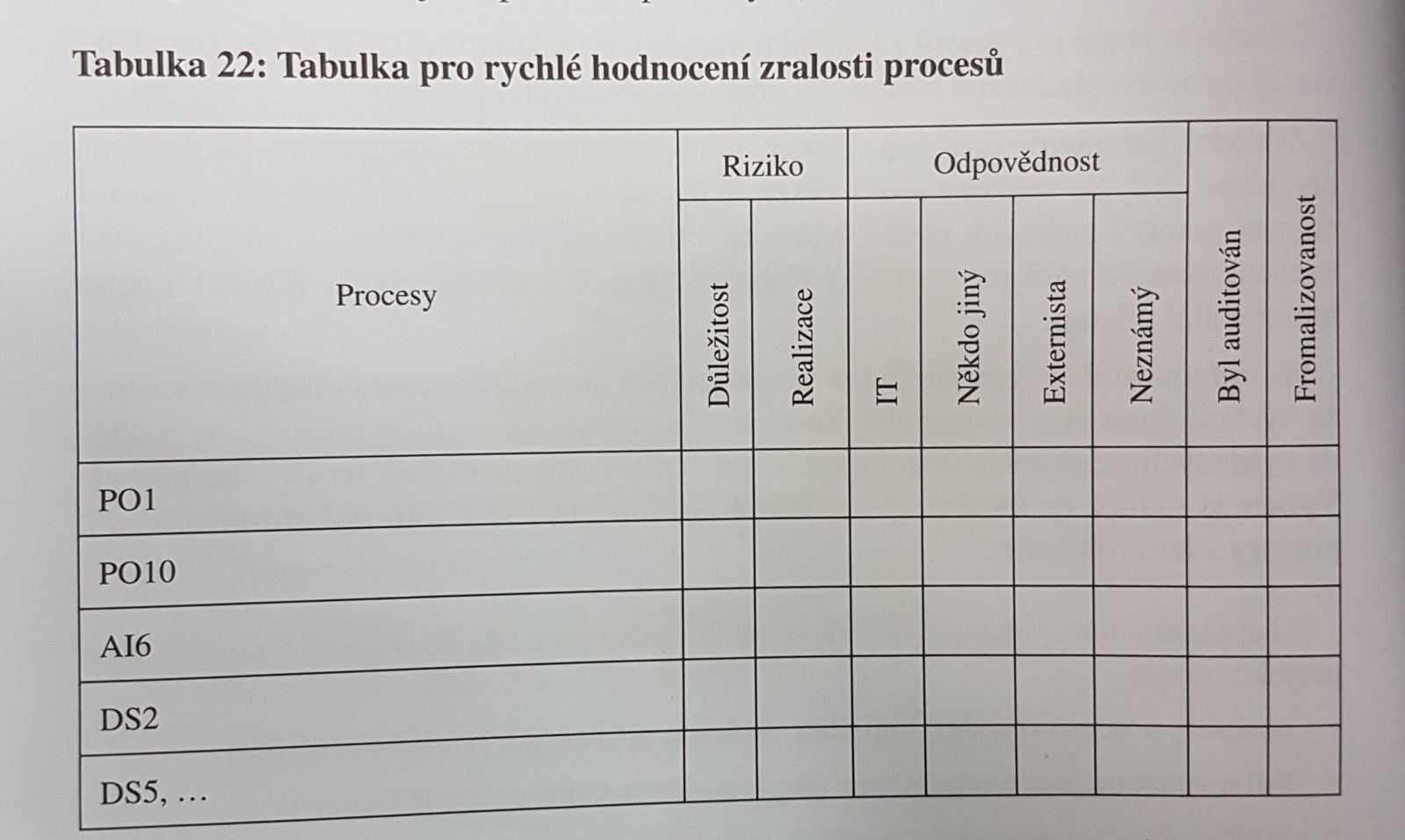
Hlavními komponentami IT Assurance Guide jsou:

* Kontrolní cíle pro jednotlivé procesy definované v rámci COBIT Framework, představující zamýšlené výsledky a účel dosažený implementací kontrol;
* Drivery hodnot a rizik co by příklady benefitů a rizik, které mohou plynout z dobrých / špatných kontrol;
* Kroky testování v rámci procesu ujištění na úrovni jednotlivých kontrolních cílů, odvozené z kontrolních praktik.

14 Co je součástí popisu procesu podle dokumentu IT Assurance Guide?

**Součástí** popisu procesu podle dokumentu IT Assurance Guide je hodnocení zralosti IT procesů vhodných pro audit/ujištění. Podle zamýšlené hloubky auditu je hodnocení zralosti IT procesu :

* rychlé – spočívá ve získání odpovědí na následující otázky a jejich doplnění do jednoduché tabulky
  + Důležitost: jak důležitý je process pro organizaci (1 vůbec není důležitý – 5 velmi důležitý
  + Realizace: Jak process probíhá (1 velmi dobře – 5 nevím nebo špatně)
  + Formalizovanost: existuje k danému procesu nějaká smlouvanebo jasně definovaná procedura? (Ano/NE)
  + Existence Auditu: byl process již předmětem auditu (ANo/NE)
  + Odpovědnost: kdo je za process odpovědný (Jméno nebo nevím)



* podrobné – je založeno na atributech, například:
  + povědomí a komunikace
  + politiky, plány, procedura
  + nástroje a automatizace
  + dovednosti a znalosti
  + odpovědnost (accountability, responsibility)
  + stanovení cílů a metriky

15 Popište historii a princip metodiky Cobit4.1, procesní rámec.

Cobit obecně: Sada dokumentů „best practises“ v oblasti řízení IT, všeobecně přijímaných kontrolních cílů pro oblast IT, pro IT staff a auditory (externí i interní).

1996 Cobit

1998 Cobit 2

2000 Cobit 3

2005 Cobit 4 ISO/IEC 17779

2006 VAL IT

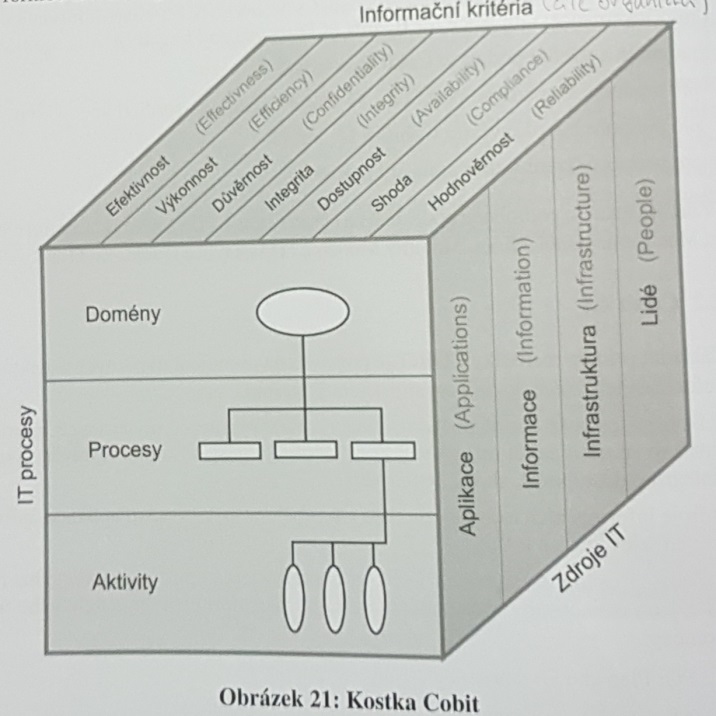
2007 Cobit Assurance ISO/IEC 38500

2009 RISK IT

2011 Process Model Allign with ISO/IEC15504-2

2012 Cobit 5

Základní princip metodiky Cobit 4.1 je postaven na propojení 3 různých aspektů řízení IT v organizacích.

* **Cíle organizace** ve formě požadavků na vlastnosti (**Informační kritéria**) dodávaných informací
* **Zdroje informačních technologií**
* **Procesy**
* 4 domény procesů:

PO Plánování a organizace

AI Pořízení a implementace

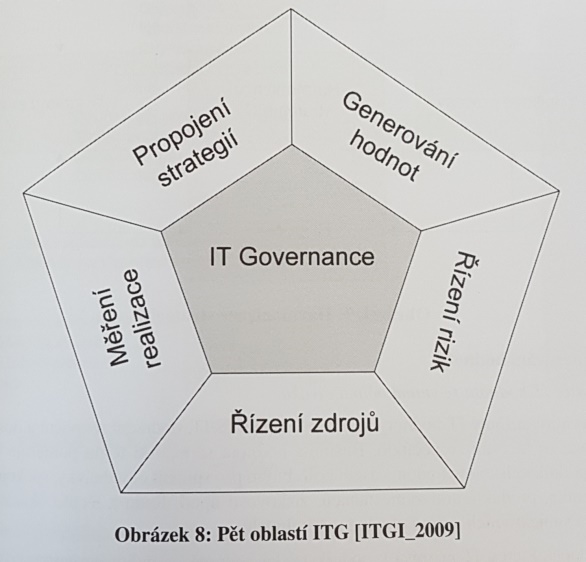
DS Dodávka a podpora

ME Monitorování a hodnocení

* 34 procesů (high level control objectives)
* Aktivity
* 214 kontrolních cílů
* Je procesně orientovaný s vazbou na IT zdroje, požadavky businessu na vlastnosti informací a cíle IT Governance
* Klade důraz na kontroly
* Je orientovaný na propojení různých úrovní cílů a jejich metrik
* Umožňuje hodnocení zralosti procesů
* Má definované vazby na jiné frameworky

Procesy jsou provázány s **IT zdroji,** viz kostka Cobit

Procesy jsou provázány **s požadavky businessu na vlastnosti informací,** viz kostka Cobit

Procesy jsou provázány s **IT Governance**

* Strategic Alignment
* Value Delivery
* Risk mgmt.
* Resource mgmt.
* Performance mgmt.

27 Vysvětlete pojetí kontroly jako procesu a jako systému.Uveďte různá hlediska pro dělení kontrol.

**Kontrola jako process**:

jde o souhrn činností, při kterých oprávněné osoby nebo organizace poskytují prověrky, audity nebo ujištění, že organizace plní svoje cíle.

* Hlavní vlastnosti kontroly jako procesu:
  + nezávislost
  + objektivnost
  + komplexicita
  + formalizovanost

**Kontrola jako system:**

znamená system dílčích control, který pomáhá v rámci organizace plnit stanovené cíle (interní kontrolní system)

* Hlavní vlastnosti kontroly jako system:
  + hospodárnost
  + efektivnost
  + účelnost.

**Dělení Kontrol dle hledisek:**

* Hledisko OSOBY, která ji vykonává : Externí nebo interní kontrola
* Hledisko POUŽITÍ POČÍTAČŮ: Automatizovaná nebo ruční kontrola
* Hledisko ČASU: preventivní, průběžná nebo následná kontrola.
* Hledisko DOBY TRVÁNÍ: Nepřetržitá, občasná pravidelná nebo občasná nepravidelná kontrola.
* Hledisko ROZSAHU: Komplexní nebo dílčí kontrola.