1) Vývoj, druhy a obsah auditu IS

1. Popište vývoj auditu IS ve světě a v ČR.

- první civilizace, pouze ústní informace o stavu majetku vládců
- Řecko a Řím – audit veřejných účtů, aby úředníci nezneužívali svou pravomoc
- Středověk – v Anglii vyšší úředníci kontrolovali práci nižších úředníků, první rozdělení zodpovědnosti (jeden shromažďoval platby, jiný evidoval…)
- Průmyslový revoluce – první státem registrované společnosti, audity akcionářů, auditor sám musel být akcionářem (nízká objektivita)
- přelom 19. a 20. Století – audit na prověření hospodářské činnosti managementu – neefektivní
- konec 70. let 20. Století – vznik EDP, audit jako forma umění
- 80. Léta 20. Století – audit jako inženýrská disciplína, vzniká ISACA, audit IS jako doplněk finančního

- v ČR od 1989, 1992 zákon č. 524/1992 o auditorech a Komoře auditorů ČR, poslední zákonná úprava č. 93/2009, 1996 – začíná se prosazovat audit IS, 1997 ČR členem ISACA

2. J**akými krizemi prošla v historii auditorská profese, jaké byly příčiny a důsledky?**
Na přelomu tisíciletí prošla auditorská profese krizí. Byla vyvolána finančními skandály několika velkých firem (Enron, WorldCom, Parmalat).
Příčinou krize - finanční audity nesignalizovaly dopředu žádné problémy v hospodaření těchto firem a nebyly tak schopny ochránit majetek investorů a akcionářů. V případě bankrotu Enronu audit vykonávala renomovaná auditorská a poradenská firma Arthur Andersen, která patřila mezi tzv. „velkou pětku“.
Za zmínku stojí **tři obecné příčiny**: konflikt zájmů organizací pověřených výkonem auditu, globalizace podniků a pomalé akceptování nových forem auditu.
Po skandálu v roce 2002 musela firma Arthur Andersen ukončit svoji činnost, přestože byla později Nejvyšším soudem Spojených Států rehabilitována. Její návrat mezi auditorské firmy se však již neuskutečnil.

3. Jaké instituce zabezpečují profesi auditora IS na mezinárodní a národní úrovni? Jaké aktivity vyvíjejí?
Mezinárodně:
ISACA – certifikace auditorů ve 4 oblastech, vydávání časopisu, pořádání seminářů, spolu s ITGI (IT governance institut) nejdůležitější autorita v oblasti výzkumu, vydávání standardů a vzdělávání v oblasti řízení a správy IS.
INTOSAI – audit státních podniků
IIA – interní audit
AITP – informace a školení o vývojových trendech
ACCA – sdružení účetních

Národně:
ISACA Czech republic
KAČR (Komora auditorů)
CIIA (Český institut interních auditorů)

4. Definujte pojmy kontrola, audit, ujištění (assurance) obecně a ve vazbě na IS.
Audit vs. Ujištění – Audit představuje specifickou formu ujištění.
<u>Vazba na IS :</u>

- Kontrola –např. kontrola správnosti vstupních dat
- Audit IS – Audit objektů v prostředí, kde jsou používány informační technologie. Jeho cílem je kvalitativně a/nebo kvantitativně přispět ke správné organizaci informačního systému tak, aby byly splněny požadavky uživatelů. Objekty mohou být organizace a řízení IS, základní i aplikační software, technické vybavení, telekomunikační systémy, procesy tvorby a údržby systémů, ochrana a bezpečnost systému, data (databáze).
- Ujištění – objektem může být SW aplikace, kterou vytvořil IT profesionál (odpovědná strana), ale využívají ji účetní (stakeholder)

Obecně:

Kontrola	Control objective, control	Prověření dílčích aspektů, jevů, procesů s předem určenou hodnotou. Jeden kontrolní cíl může být zajištěn řadou různých kontrol.
Audit	Audit	Komplexní, formalizované nezávislé prověření kontrol (existence, realizace, efektivnosti) vzhledem k existujícím standardům
Ujištění	Assurance	Komplexní nezávislé prověření kontrol, které jsou delegovány na jiné subjekty (existence, realizace, efektivnosti) vzhledem k cílům řízení

5. **Jaké jsou základní vlastnosti a druhy auditu? Aplikujte různá kriteria dělení.**
   Audit musí splňovat čtyři základní vlastnosti, kterými jsou:
   komplexnost – musí postihnout všechny relevantní aspekty a vazby,
   objektivnost – musí se opírat o existující standardy, případně zkušenosti, pokud standardy neexistují,
   nezávislost - auditor nemá s objektem auditu ani se zadavatelem auditu žádné spojení, které by představovalo konflikt zájmů,
   formalizovanost - proces auditu se musí řídit metodikou a existujícími standardy.

   Druhy auditu jsou:
   1) Dle aplikace – technologický a profesionální
   2) Dle vykonavatele auditu – interní a externí
   3) Dle ekonomického a časového hlediska – jednorázový a průběžný
   4) Dle věcného zaměření – bezpečnosti, projektu, kontrolního systému, operační a legálnosti programového vybavení
   5) Dle metodologie – substantivní, procesně orientovaný, založený na kontrolách a riziku
   6) Dle vazby na právní systém – forenzní, due dilligence (předinvestiční prověrka), ostatní

6. **Jakým způsobem se vyvíjel obsah/záběr auditu IS a jaký je jeho současný stav?**
   Obsah, respektive záběr auditu prošel vývojem, který lze stručně shrnout do těchto etap:
   1. etapa hodnocení výsledků zpracování na počítačích – obsahem auditu jsou vstupy, zpracování a výstupy informačních systémů

   2. etapa hodnocení rizika a kontrol počítačového zpracování – obsah se rozšiřuje na preventivní hodnocení spolehlivosti a průkaznosti počítačově zpracovávaných transakcí

   3. etapa hodnocení a optimalizace procesů IT i navazujících procesů – obsah se dále rozšiřuje z oblasti čistě „počítačové— do oblastí souvisejících (např. postavení útvaru IS/IT v rámci organizace, realizace přidané hodnoty k businessu procesům pomocí IS/IT)

   Současný stav – snaha sjednotit terminologii, vazba na služby, upřednostňování pohledu zákazníka, pohled životního cyklu na řízení IT, důležitá je bezpečnost informací. Domény ISACA – ochrana informačních aktiv, řízení ŽC systému a infrastruktury, IT Governance, postupy auditu

7. **Jako druhy certifikací, standardů a jiných dokumentů nabízí organizace ISACA?**
   Druhy certifikací:
   CISA – oblast auditu, kontroly, řízení a bezpečnosti
   CISM – oblast managementu informační bezpečnosti
   CGEIT – oblast IT governance
   CRISC – oblast řízení rizik

ISACA vydává standardy, které jsou závazné pro interní a externí auditory – členy ISACA a držitele titulu CISA. Standardy se dělí na:

- standardy (Standards) – definují povinné požadavky pro profesi a postup auditu,
- návody (Guidelines) – představují návody pro aplikaci standardů,

- procedury (Procedures) – zahrnují příklady postupů auditu IS, o které se auditor může opřít při provádění různých druhů auditu IT/IS.

Kromě auditorských standardů ISACA ještě vydává standardy pro odborníky na kontroly (Standards for Control Professionals). Kromě těchto standardů existuje ještě profesionální etický kodex, který určuje, jaké jsou hlavní zásady auditorské profese.

8. **Popište rozdíly mezi finančním auditem a auditem IS.**
   Finančí audit je základem všech ostatních typů auditů. Jeho funkce se postupně rozšířily z kontroly finančního hospodaření firem na další oblasti, a to na oblast souladu se standardy (tzv. compliance audit) a oblast efektivního využívání zdrojů (tzv. operational nebo performace audit).
   Audit informačního systému je specifický proces, který se zabývá posuzováním a poradenstvím objektů v prostředí, kde se používají informační technologie. Jeho cílem je kvalitativně a/nebo kvantitativně přispět ke správné organizaci informačního systému tak, aby byly splněny požadavky uživatelů.

2) Standardy a audit IS

1. **Vysvětlete význam a různá hlediska pro dělení standardů z pohledu auditu IS.**
   Význam – jedná se o normy, politiky, zákony, metriky, nejlepší praktiky, metodiky, modely, rámce apod. podle kterých je možné provádět audit a porovnávat s nimi skutečný stav objektu.

Standardy auditu

Standardy pro externí audit – standardy ISACA, ITAF (obecné, prováděcí, výstupní standardy)
Standardy pro interní audit - zákon č. 320/2001 Sb. o finanční kontrole, standardy IIA (Institut interních auditorů)

Standardy IS/IT

Standardy bezpečnosti (sada norem ISO/IEC 27000, hodnocení bezpečnosti IT produktů ISO/IEC 15408),
Standardy kvality (ČSN EN ISO 9000:2005)

2. **Vysvětlete pojmy Corporate Governance, Enterprise Governance a IT Governance, jejich význam a vazby pro audit IS.**

Corporate governance - Jedním z největších propagátorů tohoto konceptu je OECD. Iniciativy CG mají za cíl vytvářet statutární orgány, které jsou odpovědnější vůči akcionářům tím, že se snaží vyvažovat moc výkonného managementu se schopností statutárních orgánů jednat v zájmu vlastníků. Základními principy governance přístupů jsou:

- **princip otevřenosti**: základ důvěry, která je podstatná pro vztahy mezi podnikateli a těmi, kteří se na jejich úspěchu podílejí (akcionáři, banky, investoři),
- **princip poctivosti**: přímé jednání a pravdivý charakter všech finančních/účetních zpráv
- **princip odpovědnosti:** nezbytnou součástí řízení organizací je nezávislé ověřování poskytovaných informací a stanovení odpovědnosti za jejich případnou nepravdivost a nesoulad se regulacemi.

Základním dokumentem formulujícím zásady Corporate Governance je dokument Kodex správy a řízení společností založený na Principech OECD.

Enterprise Governance - aplikace governance principů do další úrovně řízení organizací. Jedná se o definování a zavádění procesů, struktur a kontrolních systémů napříč organizací, které zvýší ziskovost investic a usnadní průhlednost procesů při současném snížení rizika spojeného s působením prostředí a zaváděním nových technologií. Důraz je tak kladen na

- řízení podnikových rizik,
- procesy nabývání majetku (akvizice a fúze),
- výkonnost vedení (hodnocení míry dosažení stanovených cílů).

IT Governance - V současné době je ITG formálně vymezený styl řízení IT, který oproti předchozím modelům řízení nově definuje postavení a odpovědnost útvaru IT na jedné straně a vlastníků a exekutivy podniků na

straně druhé. Cílem této koncepce je překonat bariéry mezi těmito úrovněmi řízení organizací a zdůraznit fakt, že přestože je oblast IT formálně řízena vedoucím příslušného útvaru, odpovědnost za vývoj IT leží především na statutárních orgánech a nejvyšším vedení organizací.

3. **Vysvětlete pojem IT Governance, komu je tento rámec určen a jakým způsobem se dotýká činnosti statutárních orgánů a managementu organizací?** Viz otázka č. 2

4. **Popište pět základních cílů IT Governance.**
    - Propojení strategií (soulad mezi investicemi IS/IT a strategií podniku)
    - Generování hodnot (hodnota, kterou IT přinese businessu, je potřeba sladit business a IT pohled, mají jiné metriky, je třeba najít společný jazyk)
    - Řízení rizik (identifikace rizik, odpovědnost za jejich řízení je na nejvyšším vedení, vnitřní kontrolní systém, rychlá a včasná reakce na rizika)
    - Řízení zdrojů (řízení nejen finančních zdrojů – i personálních, materiálních atd.)
    - Měření realizace (metriky pro každou dimenzi, nejen finanční, využití BSC – i dimenze procesní, zákaznická a personální)

5. **Uveďte, jaké druhy standardů týkajících se profese auditora IS vydává ISACA ev. jiné organizace. K jednotlivým druhům uveďte příklady.**

ISACA

standardy (Standards) – definují povinné požadavky pro profesi a postup auditu,

návody (Guidelines) – představují návody pro aplikaci standardů,

procedury (Procedures) – zahrnují příklady postupů auditu IS, o které se auditor může opřít při provádění různých druhů auditu IT/IS.

Kromě auditorských standardů ISACA ještě vydává standardy pro odborníky na kontroly (Standards for Control Professionals). Kromě těchto standardů existuje ještě profesionální etický kodex, který určuje, jaké jsou hlavní zásady auditorské profese.

ITAF rozlišuje tři kategorie standardů:
Obecné (General): jsou společné pro všechny druhy ujištění a týkají se takových fenoménů, jako je profesní nezávislost, objektivita, potřebné znalosti, kompetence, dovednosti.

Prováděcí (Performance): týkají se způsobu řízení jednotlivých aktivit auditorů, jako například plánování, zajišťování zdrojů, dohled, řízení rizika, významnost nálezů, vedení dokumentace apod.

Výstupní (Reporting): určují druhy výstupních zpráv, způsob jejich zveřejňování a projednávání.

6. **Popište účel a obsah dokumentu ITAF.**

V roce 2007 vznikla potřeba různé standardy zpřehlednit a provázat je do jednotného rámce. Tak vznikl dokument ITAF – IT2 Assurance Framework.
Jeho cílem je poskytnout profesionálům v oblasti auditu/ujištění a dalším zainteresovaným stranám informace týkající se návrhu, tvorby, realizace a zpracování výstupů z těchto aktivit. Je upřednostněn pohled věcného zaměření.

ITAF rozlišuje tři kategorie standardů:
Obecné (General): jsou společné pro všechny druhy ujištění a týkají se takových fenoménů, jako je profesní nezávislost, objektivita, potřebné znalosti, kompetence, dovednosti.

Prováděcí (Performance): týkají se způsobu řízení jednotlivých aktivit auditorů, jako například plánování, zajišťování zdrojů, dohled, řízení rizika, významnost nálezů, vedení dokumentace apod.

Výstupní (Reporting): určují druhy výstupních zpráv, způsob jejich zveřejňování a projednávání.

Uvedené tři druhy standardů jsou podporovány zvláštními návody (guidelines) a technikami (techniques).

Návody (IT Assurance Guidelines) se dále podle svého předmětu dělí do čtyř skupin:

Celopodnikové, řízení IT, procesy auditu a ujištění IT, řízení IT auditu a ujištění

7. Uveďte standardy důležité pro interní audit, jeden z nich si vyberte a popište jeho obsah podrobněji.

Zákon č. 320/2001 Sb. o finanční kontrole stanoví povinnost jednotlivým správcům státního rozpočtu službu interního auditu v organizaci zřídit. Zároveň upravuje postavení a funkce interního auditu.
Zjišťuje dodržování právních předpisů, včasné rozpoznání rizik a přijímání odpovídajících opatření, zda řídící kontroly poskytují spolehlivé a včasné informace vedení, zda jsou plněna provozní a finanční kritéria, zda vnitřní kontrolní systém reaguje včas na změny podmínek.

Standard 1300 Quality Assessment and Improvement Program. Jde o standard, který vydala organizace IIA a který upravuje postup hodnocení útvarů interního auditu.
Má dvě části:
S1311 – Internal Assessments upravuje možnost interního hodnocení útvarů (průběžné a periodické), S1312 – External Assessments upravuje variantu „sebehodnocení s nezávislým ověřením.

8. Co může být předmětem norem pro informační bezpečnost? Uveďte příklady.

Bezpečnost informací (Information Security) se týká zachování důvěrnosti, integrity a dostupnosti informací a s nimi spojené priority např. autentičnost, odpovědnost, nepopiratelnost, hodnověrnost. Přitom

- důvěrnost (Confidentiality) je zajištění, že informace jsou přístupné nebo sděleny pouze těm, kteří k tomu mají oprávnění,
- integrita (Integrity) je zajištění správnosti a úplnosti informací,
- dostupnost (Availability) je zajištění, že informace je pro oprávněné uživatele přístupná v okamžiku potřeby.

Příklady norem:

- normy pro zavedení a certifikaci ISMS (sada norem ISO/IEC 27000),
- alternativní normy zabývající se identifikací, zavedením a hodnocením tzv. „base practices— pro různé domény (ISO/IEC 21827),
- hodnocení bezpečnosti IT produktů (ISO/IEC 15408, TCSEC, ITSEC).

9. Popište koncepci norem ISO 27000, vyberte si dvě normy z této sady a podrobněji popište jejich obsah.

- ISO 27000 - definice pojmů a terminologický slovník pro všechny ostatní normy z této série byl vydán v květnu 2009.
- ISO 27001 (BS7799-2) - hlavní norma pro Systém řízení bezpečnosti informací (ISMS), uvádí 11 oblastí bezpečnosti – fyzická, prostředí, řízení přístupu, klasifikace aktiv, řízení kontinuity činností organizace atd.
- ISO 27002 – popis sady kontrol informační bezpečnosti, které mají snižovat rizika v oblasti informační bezpečnosti.
- ISO 27003 - návod pro návrh a zavedení ISMS v souladu s ISO 27001.
- ISO 27004 – metriky a návody na měření a prezentaci efektivity ISMS
- ISO 27005 – Risk management
- ISO 27006 – požadavky na organizace udílející certifikaci, podklad pro auditory
- ISO 27011 - doporučení a požadavky na řízení bezpečnosti informací v prostředí telekomunikačních operátorů.
- ISO 27799 - doporučení a požadavky na řízení bezpečnosti informací ve zdravotnických zařízeních.

10. Popište koncepci normy ISO/IEC 21827 IS – Systems Security Engineering – Capability Maturity Model (SSE-CMM) (ČSN ISO/IEC 21827)

Na rozdíl od sady ISO 27000 využívá CMM model a snaží se respektovat specifika různých domén řízení v organizacích. Jejím cílem není popis konkrétního systému řízení informační bezpečnosti nebo procesů jeho

zavádění, ale spíše popisuje praktiky, které se ukázaly jako vhodné z hlediska praxe. CMM potom představuje metriku pro hodnocení zralosti bezpečnostních praktik v organizacích.

Norma rozlišuje dvě oblasti: oblast security engineering a oblast projektovou (organizační). Pro každou oblast definuje procesní oblasti (pro každou oblast 11 procesních oblastí) a dále pro každou procesní oblast uvádí tzv. dobré praktiky (base practices).

11. Popište cíl, koncepci a základní pojmy normy ISO/IEC 15408 – Evaluation Criteria for IT Security

Jde o Standard pro hodnocení bezpečnosti a zajištění produktů. Cílem je zabránit neoprávněnému prozrazení dat, jejich modifikaci nebo ztrátě. Hodnocení IT produktů podle ISO 15408 je možné aplikovat jak pro zajištění bezpečnosti produktu vyvíjeného na míru, tak jako garance dodavatele produktu o jeho bezpečnostních vlastnostech. Uživatelům může zase standard sloužit jako nástroj pro určení toho, jak daná aplikace nebo systém splňuje jejich požadavky.
ISO 15408 prezentuje dvě kategorie požadavků bezpečnosti: funkční požadavky a požadavky na záruky. Standard neurčuje model pro vývoj aplikací, ale zmiňuje obecně hlavní etapy vývoje, např. definování požadavků bezpečnosti, definování specifikací, hrubý návrh systému, programování a implementace.

Standard má tři části:

• ISO/IEC 15408 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model: úvod a obecný model; je úvodem k CC, definuje obecné pojmy a principy hodnocení bezpečnosti IT a prezentuje obecný model hodnocení.
• ISO/IEC 154088 Part 2: bezpečnostní funkční požadavky; ustavuje množinu funkčních komponent jako standardní způsob vyjadřování funkčních požadavků pro TOE. Katetrizuje množinu funkčních komponent, rodin a tříd.
• ISO/IEC 154088 Part 3:: Požadavky na záruku bezpečnosti; ustavuje množinu měřítek, kterými je vyjádřena kvalita dílčích prvků vývojového a realizačního procesu. Tato část je určena především pro tvůrce TOE.

12. Popište vývoj a obsah pojmu kvalita obecně a jeho specifika ve vazbě na IS.

Jakost (kvalita) je stupeň splnění požadavků souborem inherentních charakteristik, přičemž

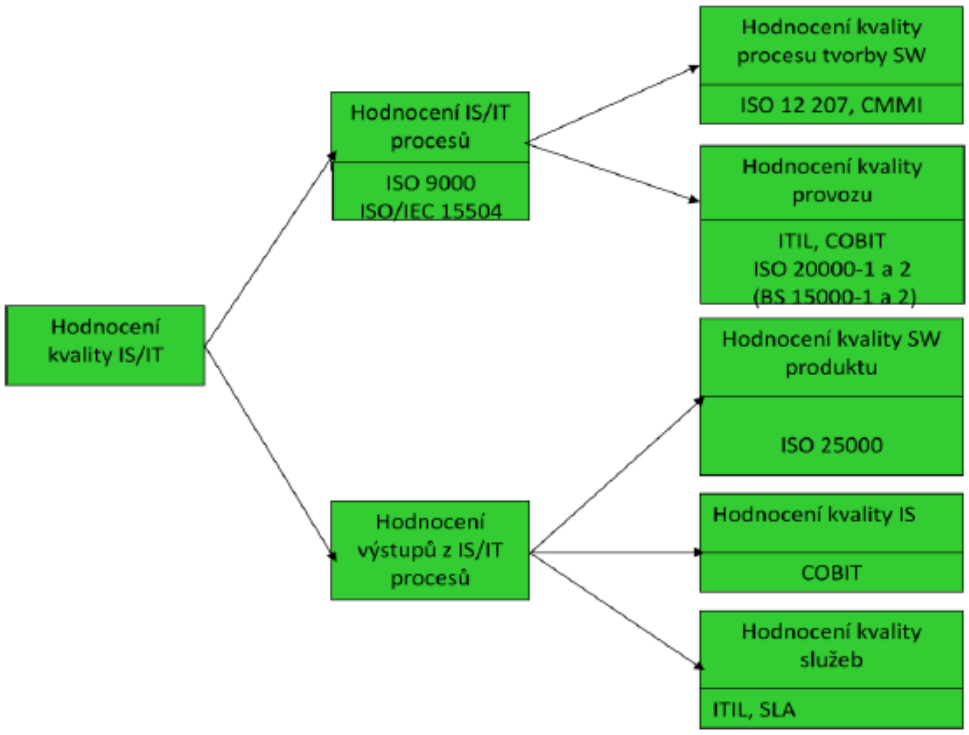
• *požadavek* je potřeba, která je stanovena buď spotřebitelem, závazným předpisem, nebo se obvykle předpokládá,
• *inherentní charakteristiky* jsou vnitřní vlastnosti produktu/procesu kvality, které k němu existenčně patří, tyto charakteristiky mohou být měřitelné (kvantitativní), nebo neměřitelné (kvalitativní).

Kvalita IS je určena požadavkem uživatele, respektive informační potřebou uživatele. V procesně řízených organizacích je tato potřeba ovlivněna kvalitou business procesu, inherentními charakteristikami informačních systémů, tj.

o inherentními charakteristikami softwarových produktů,
o charakteristikami jejich vývoje, implementace a provozování,

inherentními charakteristikami systému poskytování služeb, tj.
o kvalitou služeb IT ,
o kvalitou informací,
o kvalitou uživatelů (určenou jejich znalostmi a dovednostmi

13. **Jak je možné kategorizovat normy, zabývající se různými aspekty kvality IS?**



14. **Vysvětlete cíl a obsah sady norem ISO/IEC 25000 označovaných zkratkou SQuaRE.**

Cílem je sjednotit doposud roztříštěné normy pro hodnocení kvality SW produktů do jednoho rámce.
SQuaRE – Software Quality Requirements and Evaluation

ISO/EIC 25000 – obecný přehled, plánování a řízení kvality
ISO/EIC 25001 – model kvality
ISO/EIC 25002 – vyhodnocování kvality
ISO/EIC 25003 – požadavky na kvalitu
ISO/EIC 25004 – rozvoj kvality

Tři druhy kvality softwaru – vnitřní kvalita (ISQ), vnější kvalita (ESQ), kvalita užití (IUSQ)

15. **Uveďte příklady zákonů ČR relevantních pro audit IS, dva z nich si vyberte a popište jejich obsah podrobněji.**

<u>Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti</u>

Zákon upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy.

Obsah:

- vymezuje pojmy, jako např. utajovaná informace, újma zájmu České republiky a její kategorie, stupně utajení, druhy zajištění ochrany
- definuje náležitosti bezpečnosti informačních a komunikačních systémů nakládajících s utajovanými informacemi a požadavky na jejich certifikaci,
- způsoby doložení bezpečnostní způsobilosti při provádění citlivých činností a proces bezpečnostního řízení, který tuto způsobilost dokládá,
- upravuje činnost Národního bezpečnostního úřadu.

<u>Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů</u>

- upravuje práva a povinnosti při zpracování osobních údajů,
- stanoví podmínky, za nichž se uskutečňuje předání osobních údajů do jiných států,
- zřizuje Úřad pro ochranu osobních údajů

Obsah zákona:

- definuje pojmy, jako například osobní údaj, citlivý údaj, anonymní údaj, subjekt údajů, zpracování – shromaždování – uchování – blokování - likvidace osobních údajů, správce – zpracovatel osobních údajů,
- práva a povinnosti správců a zpracovatelů osobních údajů,

- podmínky předání osobních údajů do jiných států,

postavení a působnost úřadu pro ochranu osobních údajů, jeho organizaci a činnost

Zákon č. 227/2000 Sb., o elektronickém podpisu
Zákon č.137/2006 Sb., o veřejných zakázkách
Zákon č.365/2000 Sb., o informačních systémech veřejné správy

16. Co je obsahem zákonů SOX a BASEL II, jaký mají vliv na auditorskou profesi.

SOX – Vznikl jako reakce na skandály spojené s podvodnými účetními praktikami velkých firem, jako je Enron, Tyco nebo WorldCom. SOX se zabývá průhledností a odpovědností za účetní informace firem a formuluje nové požadavky na to, jakým způsobem obchodní společnosti mají zaznamenávat, sledovat a zveřejňovat finanční informace.
Z hlediska auditu je nejdůležitější sekce 404, která požaduje na společnostech, aby součástí každé výroční zprávy byla zpráva managementu o interních kontrolách, která musí obsahovat kromě jiného popis a hodnocení těchto kontrol. Je určen pro americké firmy, ale může se týkat i poboček v ČR.

BASELII – týká se hlavně bank a finančních institucí, obsahuje standardy posilující bezpečnost a stabilitu těchto institucí. Má tři pilíře: požadavek na minimální kapitál, proces dozorného posouzení (posuzování rizik a kapitálové přiměřenosti) a požadavky na tržní disciplínu (aby měla veřejnost dostatek informací). Zavádí nové postupy pro výpočet rizika a z toho plynoucích požadavků na alokaci kapitálu

3) Metodiky auditu IS

1. Popište příčiny vzniku Governance přístupů a způsob jejich aplikace na různých úrovních řízení organizací.

V posledních několika letech se celosvětově opakovaly problémy, které v globální a integrované ekonomice mají za následek krach mnoha velkých firem a často i destabilizaci daného odvětví. Jako reakce na tuto situaci vznikla systémová koncepce nazývaná Corporate governance (CG). Governance přístupy také vznikly, protože bylo třeba donutit statutární orgány, aby byly odpovědnější a dělaly, co je v zájmu akcionářů.

CG se v poslední době rozpracovává do dalších úrovní, které umožňují její rychlou implementaci na úrovni podniků, útvarů IT a projektů IT. Tak nyní existují čtyři základní úrovně „governance" přístupů:
1. Corporate governance
2. Enterprise governance
3. IT Governance
4. Project governance

Na úrovni IT Governance se sledují dva základní cíle:
• zvyšování hodnoty podnikatelských procesů pomocí IT - tento cíl je řízen vazbou IT na podnikatelské procesy,
• omezování rizika spojeného s pořízením a provozem IT — tento cíl je řízen podnikovým systémem odpovědností.

2. Jaké jsou základní principy (domény) IT Governance?

Domény:

- Propojení strategií (soulad mezi investicemi IS/IT a strategií podniku)
- Generování hodnot (hodnota, kterou IT přinese businessu, je potřeba sladit business a IT pohled, mají jiné metriky, je třeba najít společný jazyk)
- Řízení rizik (identifikace rizik, odpovědnost za jejich řízení je na nejvyšším vedení, vnitřní kontrolní systém, rychlá a včasná reakce na rizika)
- Řízení zdrojů (řízení nejen finančních zdrojů – i personálních, materiálních atd.)
- Měření realizace (metriky pro každou dimenzi, nejen finanční, využití BSC – i dimenze procesní, zákaznická a personální)

3. Čím se zabývá organizace INTOSAI?

Jejím cílem je sjednocování metodik auditů hospodaření s prostředky procházejícími státním rozpočtem, především řeší audit státní správy. Předmětem INTOSAI je úprava pravidel a řízení organizací, které provádějí

externí finanční audity státních organizací a které jsou nejčastěji podléhají přímo parlamentu. Tyto organizace se označují jako SAI – Supreme Audit Institutions. Organizace SAI mohou provádět tři druhy auditů:

1) finanční audit – jeho cílem je prověřit správnost a úplnost vykazování transakcí s veřejnými prostředky,
2) audit provozní – jeho cílem je prověřit efektivnost vynakládání prostředků,
3) audit souladu s existujícími standardy – jeho cílem je prověřit dodržování platných zákonů a norem.

4. Popište principy metodiky auditu IS podle INTOSAI.

INTOSAI - především audit státní správy
Principy - audit má dva hlavní cíle:

- Hodnoceni interních kontrol:
  - Audit obecných kontrol — hodnocení interních kontrol všech IS organizace - odpovědnost za IS, řízení procesů IT, realizace interních auditů IS, hodnocení rizik, existence postupů týkajíc! se informační bezpečnosti, soulad IS se zákony, další
  - Audit aplikačních kontrol - zaměřuje se hlavně na hodnocení spolehlivostí IS
  - Audit kontrol vývoje systémů - pokrývá kontroly celého Životního cyklu aplikace
- Hodnocení IS z pohledu tzv. „**3-E**" (**hospodárnost (economy)** - minimalizace nákladů na zdroje, **efektivnost (efflciency)** - vztah mezi vstupy a výstupy ve formě nákladů, **účelnost (effectiveness)** - stupeň dosaženi cílů a vztah mezi skutečnosti a záměrem:
  - Audit provozní IS - hodnotí účelnost, účinnost a úspornost provozu IS - tři etapy: hodnoceni tvorby/pořízení IS, hodnocení řízení IS (využívání a kvalita Informací) a hodnocení dopadu IS na společnost (kvalita služeb)

5. Porovnejte metodiku INTOSAI a Cobit.

COBIT - sada všeobecně přijímaných procesů, návodů na hodnocení, ukazatelů a nejlepších praktik pro maximalizaci užitku z informačních technologií. Metodika obsahuje několik dokumentů, kde každý z nich je určen jiné profesi. COBIT tedy spíše ukazuje, jak efektivně řídit IT/informatiku v organizaci.
INTOSAI - poskytuje návody na provádění auditů/ujištění IS v organizacích státní správy. Audit IS chápe jako audit výkonu.

Kritérium	**INTOSAI - IS**	**COBIT**
Komu je primárně určena	Pro finanční auditory	Pro management (business i IT)a auditory IS
Co je jejím cílem	Obecné prověření interních kontrol administrativních a finančních aplikací	Obecné a detailní prověření interních kontrol Informačních systémů a informačních technologií
Rozsah	26 stran	Cobit audit guidelines více než 200 stran
Forma dokumentu	Auditorský návod (guideline)	Auditorská metodika
Rozsah definovaných kontrol	2 oblasti /druhy auditu 10 procesů 16 kontrolních cílů	4 domény 34 procesů 318 kontrolních cílů
Druhy kontrol	Obecné Aplikační	Obecné , Aplikační vyjmenované mimo rámec
Komplexita metodiky	Malá, nezahrnuje vazby na podnikatelské cíle, nebere v úvahu specifika informačních technologií, neobsahuje model vyspělosti, kritické faktory úspěchu, metriky.	Velká, hodnocení se snaží provázat s podnikatelskými cíli, bere v úvahu technologickou infrastrukturu, zahrnuje model vyspělosti, kritické faktory úspěchu, metriky

6. Popište cíl, principy a vazby metodiky IT Assurance Guide k metodice Cobit?

Cíl: poskytnutí návodů pro jednotlivé etapy a činnosti životního cyklu auditu - jaké kroky má auditor realizovat a jaké druhy testů je potřeba provést ve vazbě na jednotlivé procesy Cobitu; audit je chápán jako projekt, který má nějaký životní cyklus

Principy: doporučení a testy jsou formulované zvlášť pro obecné kontroly, aplikační kontroly a specifické kontrolní cíle procesu.

Každý projekt ujištění musí splňovat:

- Vždy jde o vztah mezi 3 stranami
- Musí být definovaný předmět auditu/ujištění
- Musí být definovaná vhodná kritéria auditu/ujištěni
- Musí být definován proces auditu/ujištěni
- Musí být zformulován závěr auditu/ujištění

Životní cyklus - etapy:

- Plánování (činnosti: stanovení základních parametru, plánováni projektu, definování obecných cílů, výběr vhodného rámce)
- Stanovení rozsahu (činnosti: business ale. IT cíle, klíčové IT procesy a kontrolní cile)
- Realizace (činnosti: upřesnění porozumění objektu a rozsahu auditu, testování efektivnosti návrhu kontrol, testování výstupu kontrol klíčových kontrolních cílů, zdokumentování, formulace a zveřejněni závěru auditu

Etapy jsou rozpracovány do dílčích činností = IT Assurance Map

7. Co je součástí popisu procesu podle dokumentu IT Assurance Guide?

Součástí popisu procesu je:

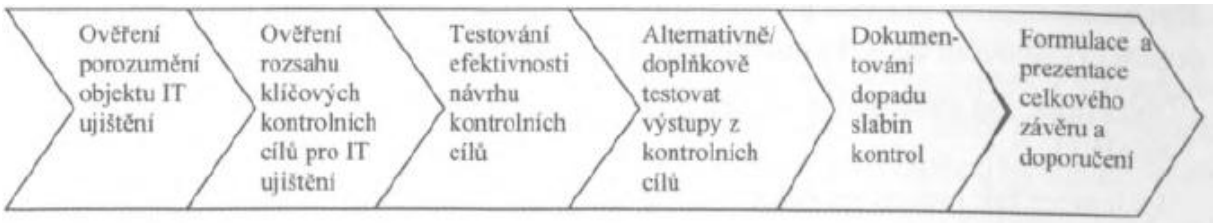
- Pro každý dílčí proces:
  - Kontrolní cíl, ovladače rizika, ovladače hodnot o Kroky pro testování návrhu kontrol - A
- Pro každý proces
  - Kroky pro testování výstupu kontrolních cílů — B
  - Kroky pro dokumentování dopadu slabin kontrol - C

U obecných kontrol jsou všechny kroky, u aplikačních kontrol není krok dokumentování slabin kontrol, protože vlastníky procesů jsou manažeři a ne IT specialisté.

8. Popište životní cyklus auditu podle dokumentu IT Assurance Guide.

Vlastní postup projektu ujištění dokument IT Assurance Guide popisuje pomocí životního cyklu, který se skládá ze tří základních etap: plánování, stanovení rozsahu a realizace. Každá z těchto základních etap je dále rozpracována do dílčích činností. Celý model se označuje termínem IT Assurance Map.

- **Plánování**
  - Stanovení základních parametrů projektu ujištění
  - Předběžný výběr vhodného kontrolního rámce (např. 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 (viz obrázek níže)**
  - Upřesnění porozumění objektu ujištění
    - Identifikace a potvrzení klíčových procesů
    - Zhodnocení zralosti procesů
  - Upřesnění rozsahu kontrolních cílů hodnoceného objektu
    - Aktualizace výběru kontrolních cílů
    - Úprava kontrolních cílů podle objektu
    - Navržení detailního programu auditu
  - Testování efektivnosti návrhu kontrol klíčových kontrolních cílů
    - Testování a hodnocení kontrol
    - Aktualizace/hodnocení zralosti procesů
  - Testování výstupu kontrol klíčových kontrolních cílů
    - Zhodnocení kontrol
    - Testování a hodnocení kontrol
  - Zdokumentování vlivu nalezených slabin kontrol
    - Určení zbytkového (reziduální) provozního nebo projektového rizika
    - Vyčíslení rizika
  - Zformulování a zveřejnění celkového závěru a doporučení



Obrázek 23: Doporučené kroky etapy Realizace [ITGI_2007]

9. **Zvolte si příklad a prezentujte na něm hlavní etapy auditu podle dokumentu IT Assurance Guide.**

IT Assurance Road map:

- o Plánování
- o Určování rozsahu
- o Realizace:
  - o Vyjasňování porozumění předmětu IT Assurance
  - o Vyjasnění rozsahu kontrolních cílů
  - o Testování efektivnosti návrhu kontrol
  - o Testování výstupů kontrolních cílů
  - o Dokumentování dopadu slabin kontrol
  - o Vytvoření a prezentování závěrů a doporučení

10. **Popište historii a princip metodiky Cobit 4 (využijte k tomu tzv. Kostku Cobit).**

Historie:

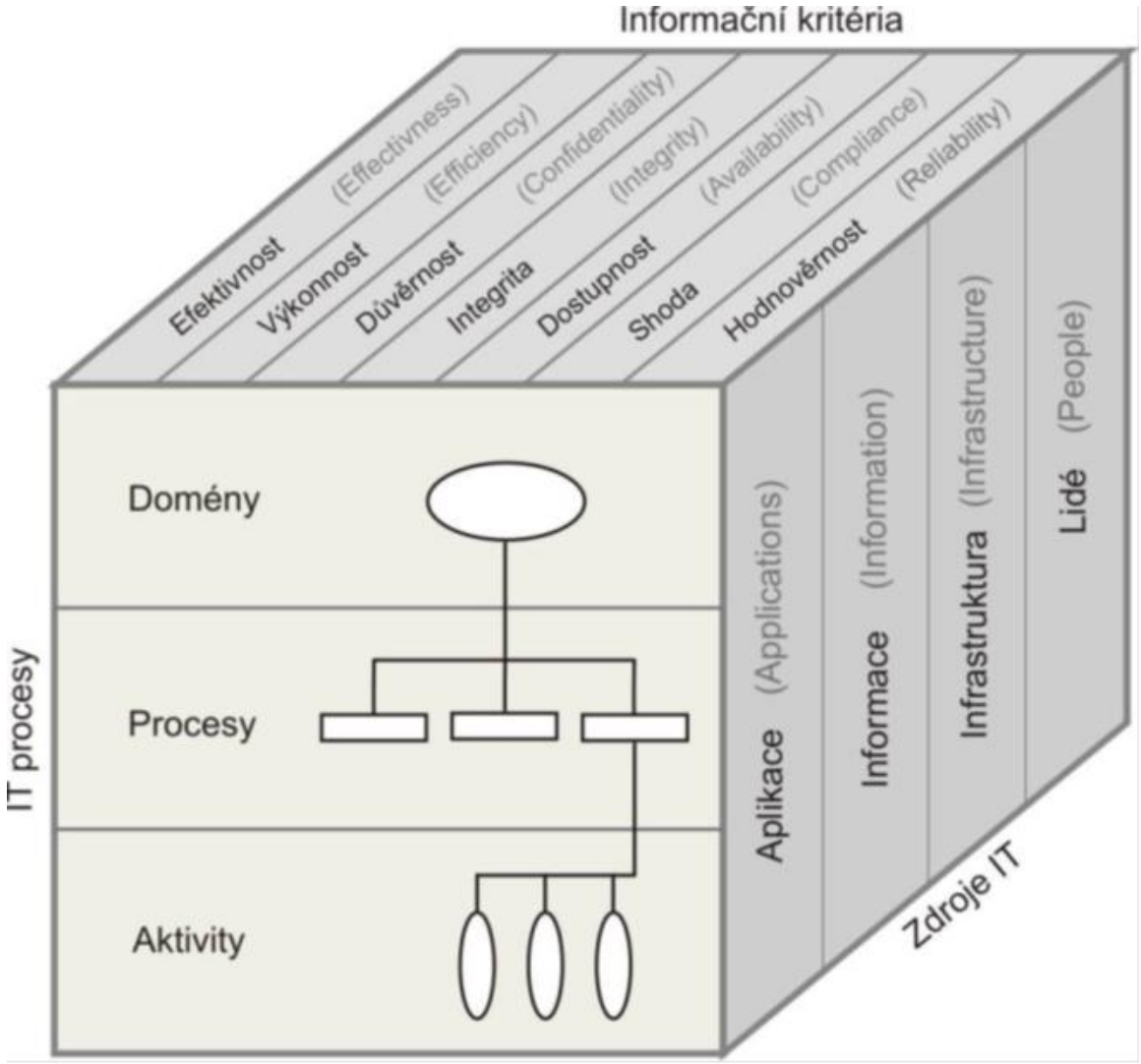
- 1998 verze 1 - vydána IT Governance Institutem a ISACA
- 2000 verze 3
- 2007 verze 4
- 2012 verze 5

Několik klíčových dokumentů. 34 procesů, popisuje koncepci řízení informatiky pomocí IT Governance

Princip - základní princip je postaven na propojení tří různých aspektů řízení IT:

- Informační kritéria (dle organizace ve formě požadavků na vlastnosti - kritéria): efektivnost, výkonnost, dostupnost, důvěryhodnost, shoda, hodnověrnost
- Zdroje IT - aplikace, informace, infrastruktura a lidé
- Procesy - mapa procesů, 4 domény

Princip je zobrazován pomocí tzv. kostky COBIT (IT procesy. Zdroje IT a Informační kritéria)



11. Podrobněji popište procesní dimenzi metodiky Cobit.

Popis procesů - Návod pro manažery (management guidelines):

- každý proces je popsán pomocí vazeb na vlastnosti informace (P-primární, S-sekundární)
  - kritéria informací (účelnost, účinnost, důvěrnost, integrita, dostupnost, soulad s normami, spolehlivost)
- každý proces je popsán pomocí vazeb na plnění cílů ITG (P,S)
- každý proces je popsán pomocí vazeb na jednotlivé zdroje
  - zdroje
    - aplikace (automatizované systémy, ruční procedury)
    - informace, infrastruktura (HW, OS atd.) a lidé (interní, externí)
- každý proces je popsán tabulkou vstupů do a výstupu z ostatních procesů
- každý proces je popsán pomocí RACI Chart (diagram který určuje kdo je za proces a jednotlivé aktivity (odpovědný, právně odpovědný, konzultant, informován)
- pro každý proces jsou definované cíle a metriky určující míru jejich dosažení. Rozlišují se:
  - úrovně cílů metrik (cíle - podnikatelské, IT útvarů, procesní)
  - druhy metrik (výstupní metriky a performance indikátory – realizace)

12. Co je obsahem popisu každého procesu v metodice Cobit?

Popis 34 procesů rozdělených do 4 domén; pro každý z těchto procesů jsou definovány:

- **cíl a účel procesu** (Process description, 1 str. A4),
- **kontrolní cíle** (Control objectives, 1-3 str. A4),
- **manažerské návody** (Management Guidelines): popis vazeb mezi procesy formou vstupů a výstupů, seznam klíčových aktivit procesu a rolí, resp. funkcí, které je provádějí formou tzv. RACI diagramu, cíle a metriky (1 str. A4),
- **kritéria zralosti procesu** pro zařazení do úrovní 0-5 (Maturity model, 1 str. A4),

Dodatek: **Mapa procesů** vychází ze čtyř domén, které kopírují životní cyklus řízení IT a jsou označovány zkratkou, tvořenou počátečními písmeny anglického názvu domény:

- PO: Plan and Organise (Plánování a organizace).
- AI: Acquire and Implement (Akvizice a implementace).
- DS: Deliver and Support (Dodávka a podpora).
- ME: Monitor and Evaluate (Sledování a hodnocení).

13. Jaké druhy kontrol se rozlišují v metodice Cobit?

V metodice Cobit se rozlišují dva základní druhy kontrol:

Obecné kontroly (IT General Controls), které jsou součástí IT procesů a služeb a týkají se například tvorby systémů, řízení změn, bezpečnosti, provozu apod. Jsou plně v odpovědnosti IT specialistů, a proto tvoří i hlavní náplň metodiky.

- kontrolní cíle procesů: jsou specifické pro každý proces; identifikují se podobně jako proces, tedy počátečními písmeny domény, číslem procesu a dále za tečkou číslem kontrolního cíle (např. P05.4 Řízení nákladů). Dohromady představují kompletní sadu požadavků, které by měly zajistit efektivní kontrolu daného procesu (Tabulka 15),
- obecné cíle procesů, které doplňují specifické kontrolní cíle a jsou společné pro všechny procesy. Označují se PCn, kde „PC" je zkratkou anglického názvu Process Control a „n" je číslo kontroly. Kontrol je celkem šest a jsou popsány jen stručně několika větami:

- PC1 Cíle procesů,
- PC2 Vlastnictví procesu,
- PC3 Opakovatelnost procesu,
- PC4 Role a odpovědnosti (odpovědnost za aktivity procesu),
- PC5 Politiky, plány a procedury (dokumentace, školení),
- PC6 Zlepšování realizace procesu (vzory, metriky).

Aplikační kontroly (Application Controls), jsou součástí aplikačního software, podporujícího business procesy. V širším pojetí jde nejen o automatizované kontroly, zabudované do aplikací, ale také o ruční kontroly, které se zaměřují např. na úplnost a správnost transakcí, řízení přístupu k datům (autorizace), na oddělení odpovědností při tvorbě aplikací, školení, testování a provozu dané aplikace. Filosofie metodiky předpokládá, že návrh a automatizace těchto kontrol je v odpovědnosti IT specialistů a je pokryta procesy v doméně AI - Pořízení a implementace, zatímco jejich provoz a kontrola je v odpovědnosti vlastníků business procesů. Aplikační kontroly mají označení ACn (počáteční písmena anglického názvu Application Control a číslo kontroly).

V dokumentu Cobit 4.1 jsou podobně jako obecné kontroly procesů popsány jen obecně. Aplikačních kontrol je šest:

- AC1: Příprava zdrojových dat (dokumentů) a jejich autorizace,
- AC2: Shromažďování dat a jejich vstup,
- AC3: Kontroly správnosti, úplnosti a pravosti (spolehlivosti),
- AC4: Integrita zpracování a hodnověrnost,
- AC5: Kontrola výstupů, konsolidace, ošetření chyb,
- AC6: Správnost, originalita a autentizace předávaných výstupů.

14. S jakými druhy cílů a metrik se pracuje v metodice Cobit? Jakou mají vzájemnou vazbu?

Úrovně cílů:

- podnikatelské cíle (Business Goals),
- IT cíle (cíle řízení oblasti IT, IT Goals),
- cíle IT procesů (IT Process Goals),
- cíle IT aktivit (Activity Goals).

Metriky, které zahrnuje metodika Cobit, se dělí na dva druhy:

- Outcome measures - **výstupní metriky** (ve verzi Cobit 3 KGI- Key Goal Indicators), které pomáhají hodnotit míru splnění cíle na dané úrovni (např. počet stížností na externě dodávané služby),
- Performance indicators - Výkonnostní metriky/ukazatele plnění (ve verzi Cobit 3 KPI -Key Performance Indicators). Pomáhají hodnotit průběh plnění cílů (např. procento dodavatelů, kteří jsou předmětem pravidelného monitoringu).

Vzájemná vazba: Cíle a metriky jsou provázány. Metriky pomáhají určit míru splnění cílů.

15. Vysvětlete princip modelů zralosti a způsob jejich využití v metodice Cobit.

Model zralosti v Cobitu rozlišuje 6 úrovní daného procesu dle CMMI. Každá úroveň je krátce popsána tak, aby pomohla manažerovi určit, na jaké úrovni se proces v nachází.

0 – **neexistující**

1 - **Počáteční –** proces probíhá nekonsistentně dle situace

2 - **Opakující se, ale intuitivní -** existuje obecné přesvědčení, proces je závislý na jednotlivcích, neexistuje formalizované předávání know-how

3 – **Definovaný -** proces je normalizovaný, neexistují kontroly, školení

4 – **Řízený a měřitelný** - existuji kontroly. Je určená odpovědnost, probíhá kontrola a vyhodnocování procesu na základě kvalitativních a kvantitativních ukazatelů

5 – **Optimalizovaný**- používají se best-practices, proces je optimalizován na základě výsledků měření a kontrol, proces je neustále zlepšován

Využití v metodice Cobit:

Model pomáhá vzájemně porovnávat jednotlivé procesy; není vždy nutné dosáhnout nejvyšší úrovně zralosti - závisí na strategických cílech, rovnováze mezi náklady a přínosy, míře rizika a zajištění souladu s legislativou.

16. Vysvětlete principy Cobit 5 a jeho rozdíly proti verzi 4.1.

Principy: Cobit 5 je možné velmi přehledně charakterizovat pomocí pěti základních principů. Tyto principy nebyly v předchozí verzi jasně definovány, některé dokumenty (Risk IT a Val IT) je zcela postrádaly. Těmito principy jsou: Uspokojení potřeb zájmových skupin, „End-to-end" pokrytí podniku, Aplikace jednoho integrovaného rámce, Podpora holistického přístupu, Oddělení úrovně řízení „Governance" od úrovně řízení „ Management.

Rozdíly:

- Cobit 5 přináší poměrně velké změny v koncepci a obsahu jednotlivých procesů. I když na první pohled nedošlo k velké změně v počtu procesů (Cobit 4.1 –obsahuje 34 procesů, Cobit 5 obsahuje 37 procesů), hlavní změny se odehrály na úrovni cílů kontrol/řízení (Control Objectives- v terminologii Cobit 4.1) a praktik procesů/řízení (Process Practices v terminologii Cobit 5).
- Došlo k novému kaskádování cílů a metrik
- RACI diagram (RACI Chart) se obsahově rovněž změnil. Ve verzi Cobit 4.1 byly odpovědnosti formou R-Resposible, A-Accountable, C-consulted a I-Informed uvedeny ke kaţdé aktivitě procesu a uvaţoval se omezený počet rolí. Ve verzi Cobit 5 jsou odpovědnosti přiřazeny ke kaţdé praktice a počet rolí byl rozšířen.
- Cobit 5 opouští model hodnocení zralosti procesů, který byl typický pro verzi Cobit 4.1 a který vycházel z modelu CMM (Capability Maturity Model). Přechází na model, který se označuje zkratkou PAM (Process Assessment Model) a je formulován v normě ISO/IEC 15504.
- Zatímco cílem verze Cobit 4.1 bylo úspěšné zavedení procesů podporujících IT Governance, cílem verze Cobit 5 je zavedení GEIT (Governance of Enterprise of IT).

4) Obecné nástroje/postupy auditu

1. Vyjmenujte základní etapy postupu auditu a porovnejte tyto etapy s postupem uvedeným v dokumentu IT Assurance Guide.

Etapy auditu:

- Uzavření smlouvy na audit
- Předběžně plánování
- Vytvoření plánu auditu
- Realizace auditu
- Závěr a vydám auditorské zprávy
- Sledování plnění závěrů auditorské zprávy

IT Assurance Guide etapy:

- Plánováni
- Stanovení rozsahu
- Realizace

Etapy	Etapy podle IT Assurance Guide	Činnosti	Výstupy
0. Etapa: Uzavření smlouvy na audit	Plánování a určování rozsahu	Specifikace • předmětu auditu • cílů auditu • rozsahu auditu • kriteria hodnocení • organizace auditu • harmonogram • výstupů • cena auditu • obecných standardů (ochrana tajemství)	Podepsaná smlouva na audit
1. Etapa: Předběžné plánování		• Porozumění podnikatelským procesům • Porozumění architektuře IS/IT • Porozumění systému vnitřních kontrol	• Potvrzení správnosti porozumění • Dokumentace auditu • Dokumentace architektury IS/IT • Program auditu
2. Etapa: Vytvoření plánu	Testování návrhu kontrol (A)	• Hodnocení kontrol • Plán testů • Určení potřebných zdrojů pro audit a jejich rozvrh	Plán auditu
3 Etapa Realizace auditu	Testování výstupu kontrol (B)	• Realizace testů kontrol • Realizace podrobných testů • Analýza a vyhodnocování výsledků	• Výsledky testů • Předběžná auditorská zpráva
4. Etapa Závěr a vydání auditorské	Dokumentace dopadu slabin (C)	• Rozhovor s managementem • Zpracování auditorské zprávy a výroku	Výsledná auditorská zpráva
5. Etapa: Sledování plnění závěrů auditorské		Vytvoření plánu sledování	Průběžná hlášení managementu

2. Jaké body upřesňující předmět smlouvy na audit IS jsou důležité?

- Předmět auditu
- Cíl auditu
- Rozsah
- Organizace
    - vedoucího auditorského týmu a jeho členy,
    - místo v organizaci zadavatele auditu, kde budou členové týmu studovat dokumentaci, vést rozhovory, zpracovávat podklady,
    - kontaktní osobu z organizace zadavatele,
    - pravidla pro komunikaci mezi členy týmu a zaměstnanci organizace zadavatele auditu,
    - prostředky, které bude auditor používat (CAAT – Computer Assissted Audit Techniques).
- Harmonogram
- Výstup
    - počet (výstup musí být vždy minimálně jeden – závěrečná auditorská zpráva), pokud je výstupů více, mělo by se určit k jakým etapám (krokům, činnostem) v harmonogramu se budou vázat, nebo zda budou mít pravidelný průběh (např. každý týden, měsíc),
    - komu budou výstupy určeny,
    - v jaké formě se adresátům dodají (písemně, elektronicky) a jakými kanály (osobně, mailem, kurýrem, poštou),
    - zda se zpracují dvě verze zpráv: jedna pro manažery, druhá pro IT specialisty,
    - jaký bude stupeň utajení výstupů,
    - zda bude součástí výstupů i jejich prezentace,

    - do jaké doby má auditovaný subjekt nebo zadavatel auditu reagovat s připomínkami k výstupům auditu.
- Cena

Dále by měla obsahovat:

- práva auditovaného (odstoupit od smlouvy, hodnotit kvalitu apod.),
- právo auditora na přístup k informacím, lokacím, zařízením, softwaru apod. relevantním danému předmětu a cíli,
- prohlášení auditora o zachování mlčenlivosti o získaných informacích,
- další části, které jsou běžnými součástmi smluv na dodávku služeb (identifikace stran, sankce a penále, náhrada škody, smírčí soud, způsoby ukončení smlouvy, apod.) a které by měly být vypracovány ve spolupráci s právníky obou stran.

3. Popište obsah etapy předběžného plánování a její výstupy.

K naplánování činnosti auditor potřebuje porozumět:

- Podnikovým procesům (ověření, zda jsou namodelované procesy aktuální, tam, kde nejsou definovány, se musí auditor seznámit např. s organizační strukturou)
- Architektuře IS/IT
- Systému vnitřních kontrol (je možné auditovat, zda je kontrola efektivní, nebo zda vůbec existuje)

Pokud v podniku chybí dokumentace (nebo je zastaralá), auditor ji musí vytvořit. Samozřejmě se tím zvýší cena a prodlouží doba auditu.

Výstupy z etapy předběžného plánování:

- Potvrzení správnosti porozumění (procesům, technologiím, kontrolnímu systému) – bez porozumění by auditor neměl pokračovat v auditu
- Dokumentace auditu (popis práce a výstupů auditora, podklady pro důkazy auditu)
- Dokumentace architektury IS
- Program auditu (základní kontrolní body)

4. Popište různé úrovně kontrol a rizik, vazby mezi nimi a metodiky, které je upravují.

Kontroly – úrovně

- Interní kontroly podniku (COSO)
- Kontroly IS/IT (Cobit, ITIL)
- Kontroly informační bezpečnosti (ISO 27002) Rizika - úrovně
- Řízení celopodnikových rizik (COSO ERM)
- Řízení rizik IT (Risk IT)
- Řízení rizik bezpečnosti Informací (ISO 27005)

Vazby:

Kontroly slouží pro eliminaci potenciálních rizik. Vazby jsou v rámci jednotlivých úrovní - př. Řízení rizik IT je vázáno na kontroly IS/IT.

5. Vysvětlete princip metodiky COSO (COSO Internal Control a COSOP ERM).

COSO Internal Controls - určen pro budování integrovaného systému interních kontrol. Popisuje organizaci vnitřního kontrolního systému. Kontrolám IS/IT se věnuje jen okrajově (spíše finanční rizika) a tak je doporučováno použití metodiky Cobit. Tři dimenze:

- Účelnost a hospodárnost provozních aktivit, spolehlivost finančního výkaznictví, soulad s regulacemi
- Komponenty interních kontrol - hodnocení efektivity. Identifikace a tok informaci, kontrolní činnosti, identifikace a analýza rizik, kontrolní prostředí
- Kategorie interních kontrol dle struktury procesu a organizace

COSO ERM - klade důraz na vybudování systému interních kontrol, risk managementu a vykazování. Dále vede ke zlepšování úrovní zralosti procesu řízení rizik. Tři dimenze:

- Strategické cíle, operační využití zdrojů, výkaznictví, kompatibilita
- Komponenty procesu řízení - interní prostředí, stanovení cílů. identifikace události, ohodnoceni rizika, reakce na riziko, kontrolní činnosti, informace a komunikace, monitorování
- Úrovně, na kterých se mohou komponenty realizovat - obchodní společnost, podnikatelská jednotka, divize, entita

6. **Porovnejte etapy procesu řízení rizika podle ISO 27005 a metodiky Risk IT**

ISO 27005 – Etapy

- Určeni kontextu - stanovení kritérií pro řízeni rizik
- Hodnoceni rizik - analýza a vyhodnocení
- Zvládání rizik - výběr a přijímání opatření pro snížení rizika, akceptace rizika

Risk IT - etapy

- Risk Governance - zavedení a udržování procesu řízení rizik, řízení rizik - rizikový apetit (míra akceptovatelného rizika), tolerance (přijatelné odchylky od stanovené míry) odpovědnost, kultura řízení rizik
- Risk Evaluation - shromažďování dat, analýza rizik, údržba profilu rizika
- Risk Response - popis rizika, řízení rizika, reakce na události

7. **Uveďte a definujte základní pojmy procesu řízení rizik.**

Základní pojmy:

Aktiva - co má hodnotu pro podnik a je nutné to chránit (lidé, infrastruktura, informace, majetek)
Hrozba - situace nebo událost, která muže způsobil škodu
Agent hrozby - to, co využije slabiny aktiva
Událost hrozby - působení hrozby na slabinu aktiva
Slabina - vlastnost, která může být využita hrozbou
Prostředky ochrany - kontroly nebo měřítka, která zvyšují pružnost, odolnost a spolehlivost IT služeb
Riziko - pravděpodobnost, že hrozba využije slabinu aktiva a způsobí škody
Residuální riziko — riziko spojené s událostí, kde existující kontrola redukuje dopad této události

8. **Vysvětlete princip mapy rizik.**

Princip: dvě hodnoty - pravděpodobnost rizika a výše škody daného aktiva -> zanese se do mapy. V mapě jsou vyznačeny hranice (šikmé čáry) mezi kategoriemi rizik:

- Příležitostí - nízká rizika, je možné je ignorovat nebo využít
- Přijatelným rizikem - v rizikovém apetitu, nevyžadují opatření
- Nepřijatelným rizikem - mimo rizikový apetit, možno řešit časem
- Zásadně nepřijatelným rizikem - mimo rizikový apetit, nutno řešit rychle

9. **Diskutujte různé hlediska pro kategorizaci rizik.**

Viz otázka č. 8 – mapy rizik

Rizika celopodniková - riziko, že bude negativně ovlivněna kvalita kontrolního systému, tj. účelnost a hospodárnost provozních aktivit, spolehlivost finančního výkaznictví a soulad s regulacemi

Rizika IS/IT - riziko, že bude porušena kvalita IS, tj. účelnost, účinnost, souladu s regulacemi a spolehlivost.

Rizika bezpečnosti informací - riziko, že bude porušena důvěrnost, integrita a dostupnost aktiv.

10. **Popište různé druhy analýzy rizik.**

- **Základní přístup** — rychlé zavedení bezpečnostních opatření, analýza se v podstatě nedělá, pro srovnání se bere nějaká metodika a porovnává se se skutečností - co není implementováno, tak se zavádí - klad je rychlost a úspora, zápor - poddimenzování nebo předimenzování (není přizpůsobeno konkrétní situaci
- **Neformální přístup** - vychází se ze zkušeností osoby, která analýzu provádí a zná prostředí - klad je rychlost a úspora, zápor - subjektivní přístup na základě znalostí
- **Podrobná analýza rizik** - nejpřesnější, ale i nejnáročnější z hlediska času i peněz, nejprve se identifikují a hodnotí aktiva, následné se posuzují hrozby a odhaduje se zranitelnost aktiv
- **Kombinovaný přístup** - podrobně se hodnotí pouze vybraná rizika (aktiva) a pro ostatní se provede jednodušší a méně časově i finančně náročná analýza

Další metody:

- **Kvantitativní** - vyjadřuje se číselně (např. finance) - metoda očekávaných ztrát
- **Kvalitativní**- rizika vyjádřená v diskrétní škále (př. 1-10, A-D, apod). Přiřazování hodnot pomocí analytických postupů a subjektivního vyjádření (hlavní nedostatek), př. metoda brainstormingu, metoda bodového hodnocení - pravděpodobnost a dopad -> mapa rizik

11. Uveďte různé druhy nástrojů pro podporu procesu řízení rizik, v čem se liší a jaké mají představitele.

Druhy nástrojů:

- **Nástroje pro řízení rizik bezpečnosti informací** - spíše jednorázové nástroje, specializace na zavedení ISMS na základě analýzy rizik a příprava na certifikaci ISO 27001, př. CRAMM
- **Nástroje pro průběžné (každodenní) řízeni rizik** - registr rizik, kvalitativní analýza rizik, př. Enterprise Risk Register
- **Nástroje pro řízení celopodnikových rizik** - tzv. ERM (Enterprise Risk Management) software, podpora redukce rizika i průběžného zlepšování této oblasti, př. SAS
- **Nástroje pro komplexní řízení rizik** - tzv. GRC (Governance, Risk and Compliance) software, širší funkcionalita než ERM, zahrnuje: řízení auditu, politik, souladu a rizik, př. OpenPages, Oracle atd**.**

12. Vysvětlete pojetí kontroly jako procesu a jako systému.

Kontrola jako proces - souhrn činností, při kterých se provádí prověrky nebo audity. Hlavní vlastnosti jsou nezávislost, objektivnost, komplexnost a formalizovanost. Příkladem může být certifikační audit informační bezpečnosti.

Kontrola jako systém - systém dílčích kontrol, který pomáhá plnit stanovené cíle. Hlavní vlastnosti jsou účelnost, hospodárnost a efektivnost. Příkladem je vnitřní kontrolní systém

13. Co je obsahem zákona 320/2001 Sb., o finanční kontrole.

Zákon vymezuje uspořádání a rozsah finanční kontroly vykonávané mezi orgány veřejné správy, mezi orgány VS a žadateli nebo příjemci veřejné finanční podpory a uvnitř orgánů VS. Stanoví předmět, hlavní cíle a zásady finanční kontroly vykonávané podle tohoto zákona a podle zvláštních právních předpisů.

Zákon rozlišuje mezi pojetím kontroly jako procesu a kontroly jako systému, i když terminologicky pro obě pojetí používá termín systém. Říká, že finanční kontrola je částí systému finančního řízení a že je tvořena:

- systémem finanční kontroly vykonávané kontrolními orgány (pojetí kontroly jako procesu),
- systémem finanční kontroly vykonávané podle mezinárodních smluv (pojetí kontroly jako procesu),
- vnitřním kontrolním systémem v orgánech veřejné správy (pojetí kontroly jako systému).
    - **řídící kontrolu**: finanční kontrolu zajišťovanou odpovědnými vedoucími zaměstnanci jako součást vnitřního řízení orgánu VS při přípravě operací před jejich schválením, při průběžném sledování uskutečňovaných operací až do jejich konečného vypořádání a vyúčtování a následném prověření vybraných operací v rámci hodnocení dosažených výsledků a správnosti hospodaření,
    - **interní audit:** organizačně oddělené a funkčně nezávislé přezkoumávání a vyhodnocování přiměřenosti a účinnosti řídící kontroly, včetně prověřování správnosti vybraných operací. Podle zákona má realizovat finanční audity, audity systémů a audity výkonu.

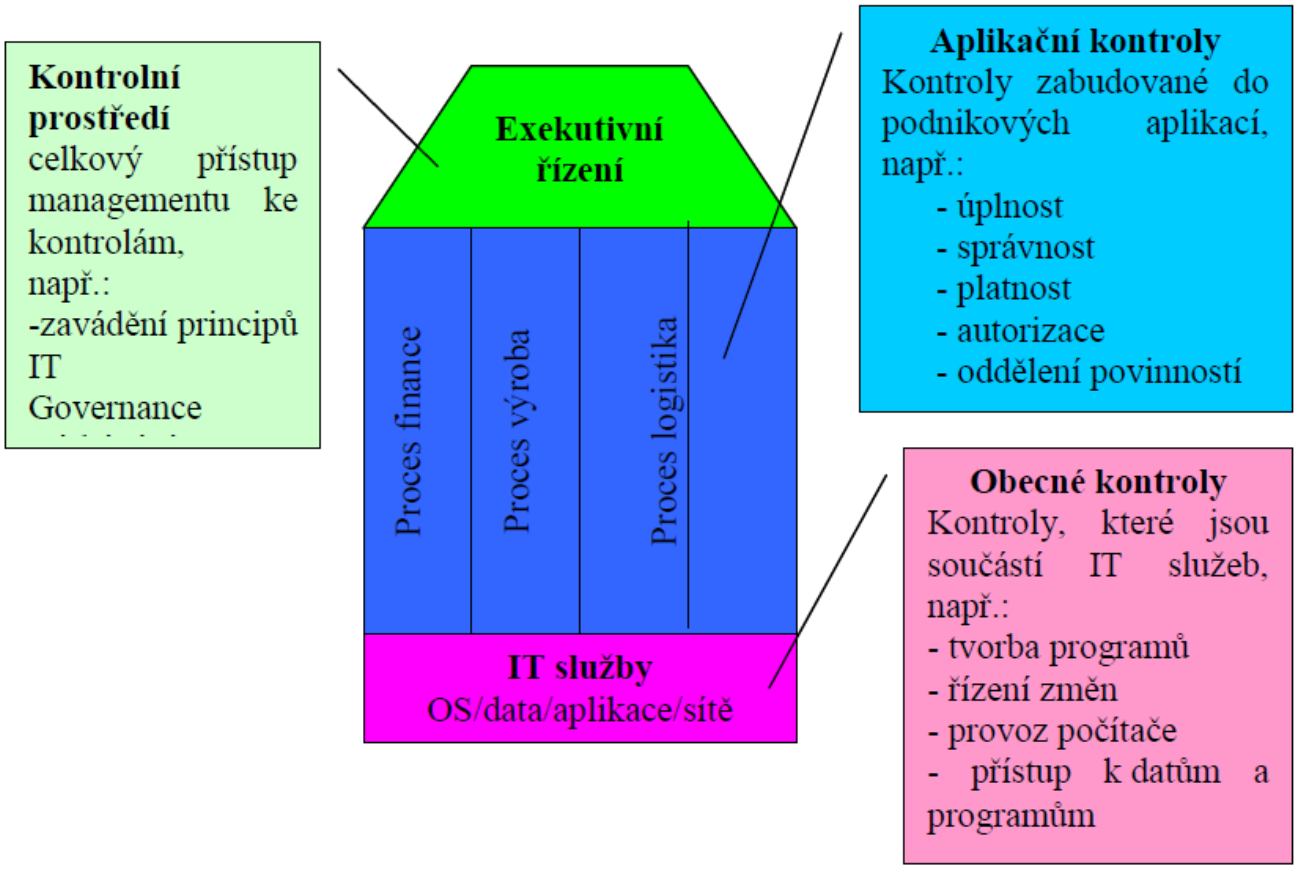
Mezi hlavní cíle finanční kontroly patří:

- **dodržování právních předpisů a opatření** přijatých orgány veřejné správy v mezích těchto předpisů při hospodaření s veřejnými prostředky k zajištění stanovených úkolů těmito orgány,
- **zajištění ochrany veřejných prostředků proti rizikům**, nesrovnalostem nebo jiným nedostatkům způsobeným zejména porušením právních předpisů, nehospodárným, neúčelným a neefektivním nakládáním s veřejnými prostředky nebo trestnou činností,
- **včasné a spolehlivé informování vedoucích orgánů veřejné správy** o nakládání s veřejnými prostředky, o prováděných operacích, o jejich průkazném účetním zpracování za účelem účinného usměrňování činnosti orgánů veřejné správy v souladu se stanovenými úkoly,
- **hospodárný, efektivní a účelný výkon veřejné správy**.

14. Uveďte různá hlediska pro dělení kontrol.

- hledisko osoby vykonávající kontrolu (externí, interní)
- hledisko využití počítačů (automatizovaná, ruční)
- hledisko času (preventivní, průběžná, následná)
- hledisko rozsahu (komplexní, dílčí)

15. Vysvětlete rozdíl mezi Kontrolním prostředím, aplikačními kontrolami a obecnými kontrolami IT, uveďte příklady.



16. Uveďte různá hlediska pro dělení testů

- Hledisko osoby vykonávající testy (interní, externí, vývojové, provozní, programové, uživatelské)
- Hledisko etap auditu (test návrhu kontrol, test výstupu kontrolních cílů)
- Hledisko druhů kontrol (aplikační, obecné, podrobné testy)
- Hledisko míry spolupráce s uživateli (black box testy, white box testy)
- Hledisko životního cyklu aplikací (alfa (návrháři), beta (uživatelé) testy)
- Hledisko objektu testování (test webových aplikací, test ERP systému, test firewallu, test databáze apod.)
- Hledisko způsobu získání informací (dotazování, inspekce, pozorování, shromažďování, znovuzpracování)

17. Jaké druhy a techniky testů existují z hlediska jejich automatizované podpory.

Druhy:

- Testování bez počítače - auditor si vytvoří testovací soubory, ručně je zpracuje a následně porovná s výsledkem automatizovaného zpracování - vhodné pro jednorázové testování
- Testování s počítačem - testování s využitím nástrojů CAAT
- Testování přes počítač - pro testování automatických kontrol, vyžaduje velké zkušenosti z oblasti struktury aplikaci a programování - vhodné pro online testováni

Techniky:

- Technika testovacích dat - testování probíhá na stejném systému, kde jsou živá data (off-line testování)
- Paralelní simulace - testování probíhá na systému se stejnou funkcionalitou (off-line testování)
- Integrované testování - testovací data se zpracovávají souběžně s živými daty (on-line testování)
- Zabudovaný auditní modul - umožňuje v systému nastavit různé reporty a logy monitorující průběh zpracování živých dat (on-line testování)

18. Vysvětlete rozdíl mezi klasickým a moderním pojetím architektury IS.

Klasické pojetí:

Architektura IS zachycuje obecný návrh, jednotlivé komponenty a vazby IS. Nebere v úvahu podnikatelské procesy a je statická. Je zaměřena na HW. SW a data. Dva základní druhy:

- **Globální architektura** - zachycuje jednotlivé komponenty a jejich vazby, pohled procesní a funkční, dimenze pohledů na komponenty jsou: datová, funkční, organizační, personální, softwarová
- **Dílčí architektura** - podmnožina globální architektury, popisuje podrobněji jednotlivé komponenty, nejčastější jsou technologická (HW), softwarová (SW) a datová (data a datové modely) architektura

Moderní pojetí:

Je upřednostňován pojem architektura podniku (Enterprise architecture) a zahrnuje komplexnější popis všech klíčových prvků a uplatňuje dynamický pohled na architekturu (je to současně proces). Zaměřuje se na všechny klíčově procesy podniku (nejen IT). S rozmachem Governance vzniká pojem EA Govcrnance (praxe a orientace, pomocí které se řídí a kontrolují EA a další architektury). Zahrnuje:

- Implementaci kontrol do procesů návrhu a monitorování
- Zavedení procesů pro podporu efektivního řízení procesů
- Vytvoření postupů zajišťujících odpovědnost

19. Vysvětlete historii normy ISO 42010, jaké jsou náležitosti pro popis rámců architektur v připravované verzi normy?

V roce 2006 byla přijata jako norma ISO/EIC 42010:2007 Systems and software engineering – Recomended practice for architectural description of software-intensive systems. Tato notma reagovala na rychlý rozvoj různých rámců, z nichž každý upřednostňoval jiný pohled na architekturu. Cílem bylo vytvořit „meta rámec". V současné době probíhá její revize a počítá se s novou verzí. Ta definuje rámec architektury jako „pravidla a postupy pro popis architektury zavedené v rámci určité domény nebo pro potřebu určité zájmové skupiny (stakeholder community)".

Každý rámec by měl splňovat tato pravidla:

- Musí zahrnovat různé cíle architektury vtažené k různým zájmům uživatelů
- Musí definovat různé skupiny uživatelů s různými zájmy
- Musí obsahovat sadu různých pohledů na architekturu, které rámují cíle
- Musí obsahovat sadu pravidel pro vazby mezi modely

20. Uveďte členění rámců EA (Enterprise Architecture), vyberte si jeden z rámců a popište jeho obsah podrobněji.

Dělení:

- Pro vládní a veřejné instituce - většinou jsou závazné, vznikají na národní úrovni např. úpravou obecných rámců. př. FEAF
- Pro organizace působící v rezortu obrany - př. DoDAF, MODAF
- Specifické rámce pro konkrétní odvětvi - jsou velice detailní a popisují konkrétní odvětví, př. N1H (zdravotnictví), eTom (telekomunikace)
- Otevřené - volně dostupné, př. TOGAF
- Proprietární - poskytuji je firmy jako svá řešení, př. Gartner, IAF

Příklady rámců:

- **TOGAF** - nejužívaněji, vychází z rámce ministerstva obrany USA (TAFIM). od verze 8 se zaměřuje na podnikovou architekturu jako celek, v současnosti je aktuální verze 9 a zastřešuje jí organizace Open Group, rozlišuje 4 typy architektur
    - Business - zachycuje prostředí businessu
    - Aplikační - logický model aplikací jako logické celky
    - Datová - logický model dat nezávislý na technologiích
    - Technologická - základ pro IT Infrastrukturu - HW, sítě, komunikační technologie

  Dokument má 3 části:
    - Část popisující uzavřený životní cyklus tvorby architektury (ADM - Archtecture Development Model)
    - virtuální sklad architektonických aktiv (Enterprise Continuum)
    - přehled nástrojů a technik pro plnění výše uvedeného (Resourcc Base)
- **Zachman** - organizace činností podle pohledů a potřeb uživatelů architektury, nevychází z procesů
- **FEAF** - rámec závazný pro federální úřady USA, je velmi komplexní, 5 referenčních modelů, 3 úrovně uživatelů - všichni uživatelé, business uživatelé a uživatelé a vývojáři IT

21. Diskutujte význam rámců EA pro audit IS.

Pro auditora mají architektonické rámce význam ten, že popisují komplexní strukturu podnikové architektury, její jednotlivé části (taxonomii), kdo za ně odpovídá a na jakých úrovních detailu by se měly vytvářet. Vzhledem k rozsahu modelů je jasné, že se ať již organizace k nějakému rámci hlásí nebo si ji auditor vybere jako kriterium sám, dokumentace EA v daném podniku nebude splňovat všechny doporučené náležitosti. Auditor může však pomocí modelu zmapovat, jaké části architektury jsou popsané a jaké případně by bylo vhodné doplnit vzhledem k předmětu auditu. V každém případě je znalost různých architektonických rámců pro auditora ale i ostatní zaměstnance, kteří odpovídají za EA, žádoucí. Zcela nezbytná je pro velké a střední organizace.

22. Jaké typy služeb ujištění mohou poskytovat auditoři IS?

Návod G20 rozvádí základní náležitosti uvedené ve standardu a podrobněji definuje používané termíny. Uvádí, že typy služeb ujištění, nabízených auditory, mohou být:

• audit přímý a atestační (direct, attest),
• přezkoumání (review) přímé a nepřímé (direct, attest),
• ověřování postupů (agreed-upon-procedures).

23. Vysvětlete rozdíl mezi auditem, přezkoumáním a ověřováním.

Audit představuje specifickou formu ujištění, při které profesionál-auditor realizuje formální, nezávislé a systematické prověření objektu zájmu proti známým a vhodným standardům nebo proti tvrzením managementu. Audit vyžaduje formální přístup, soulad se specifickými standardy a návody a dodrţování specifických formátů auditorských zpráv.

Přezkoumání poskytuje v porovnání s auditem nižší míru ujištění o efektivnosti kontrol, protože se neprovádí v takovém, a tudíž není auditor schopen vyjádřit pozitivní názor (pozitivní ujištění). Cílem přezkoumání je zjistit, zda neexistují nějaké skutečnosti, které by mohly negativně ovlivnit hodnocení auditora. Používá se např. tam, kde došlo k nějakým významným změnám v IS a je potřeba se ujistit, že tyto změny neovlivnily negativně systém kontrol.

Ověřování postupů představuje nejnižší formu ujištění. Jejím cílem není hodnocení efektivnosti kontrol, ale pouze jejich existence a realizace. V tomto případě auditor pouze formuluje nálezy, ale nedělá závěry.

24. Co by měly obsahovat společné části auditorských zpráv?

Identifikační a popisné údaje:

- název zprávy
- identifikace adresáta
- popis rozsahu auditu
- identifikace účelu zprávy
- informace o omezeních
- názor auditora
- podpis auditora
- adresa auditora
- datum zpracování zprávy

25. Jaké typy prohlášení by měly obsahovat auditorské zprávy?

typy prohlášení:

- Že za údržbu struktury efektivních kontrol je odpovědné vedení organizace
- Že auditor prováděl hodnocení s cílem vyjádřit názor na efektivnost kontrolních postupů
- Že byl audit proveden v souladu se standardy ISACA nebo jinými
- Že může dojit k neúmyslným chybám v důsledku nevyhnutelných omezení
- Že není vhodné se spoléhat na výsledek hodnocení v budoucnu vzhledem k měnícím se okolnostem a podmínkám
- že audit není určen pro detekci všech slabin kontrol, protože neprobíhá nepřetržitě

26. Uveďte základní kategorie CAAT, jejich funkcionalitu a představitele.

CAAT – specializovaný software pro práci auditora

Obecný auditní SW (Generalized Audit Software - GAS) - jsou standardní počítačové programy nebo skupiny programů, které představují v současné době nejpopulámější kategorii CAAT. Umožňují odhalit podvody, testují systémy zabudovaných kontrol a zvyšují efektivitu testování.
Představiteli těchto softwarových produktů jsou například ACL43 (Audit Command Language), CA44 Easytrieve, SAS45 - Statistical Analysis System, IDEA46 (Interactive Data Extraction and Analysis) nebo TopCAAT47.

Customizované výběry a skripty je další populární kategorie CAAT. Využívají se především tam, kde nelze použít jiné nástroje. Hlavní funkce jsou: výběr dat, stratifikace dat, výběr vzorků, identifikace chybějících dat v řadách, statistická analýza, výpočty.

Utility jsou počítačové programy vytvářené výrobci hardwaru nebo dodavateli softwaru. Prověřují zpracování, testování programů, systémové činnosti a provozní procedury, hodnotí činnost datových souborů a analyzují systémy pro účtování poplatků za čerpání počítačových zdrojů.

Mapující a monitorující aplikační software zahrnují specializované nástroje pro analýzu toku dat podle logiky zpracování aplikací. Dokumentují logiku, cesty, podmínky kontrol a posloupnosti operací.

Auditní expertní systémy pomáhají auditorům při rozhodování, protože obsahují a zpřístupňují znalosti expertů v této oblasti.

5) Vybrané druhy auditů

1. Uveďte dílčí cíle auditu útvaru IT a doporučená kriteria pro jejich hodnocení.

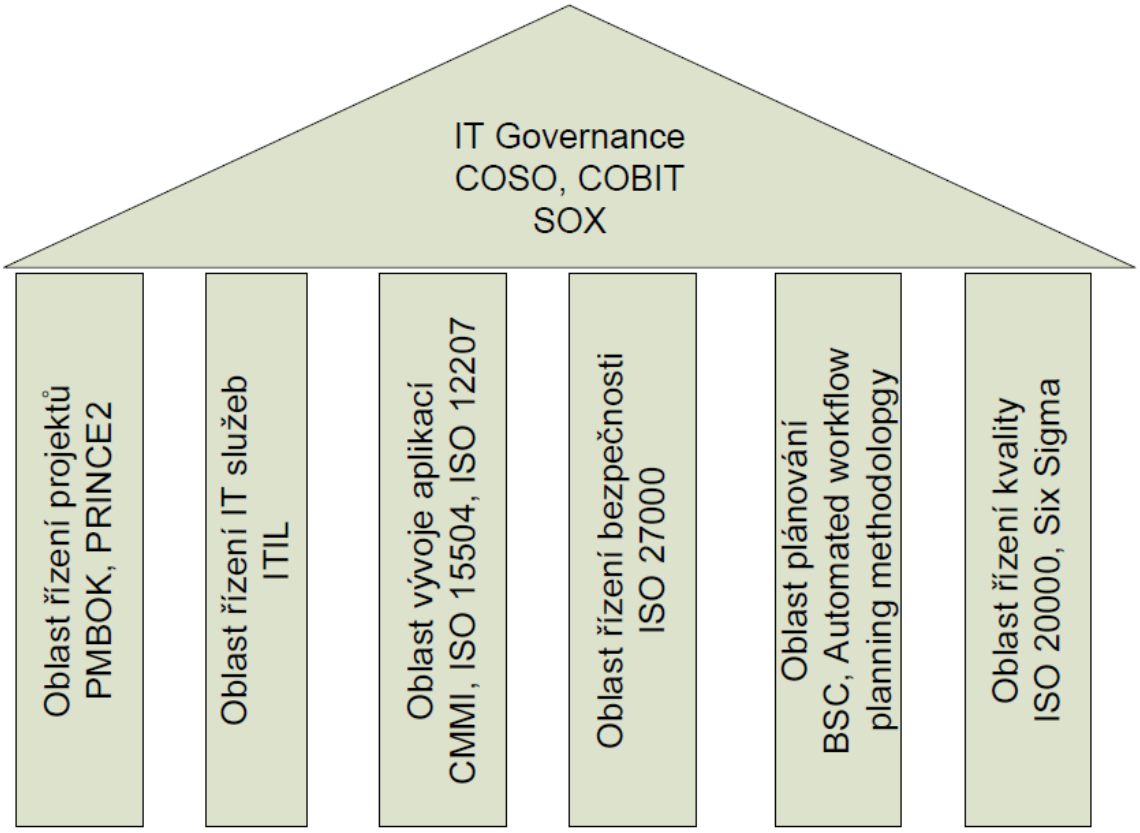
Cílem auditu útvaru IT je hodnotit účelnost a účinnost jeho fungování.

Dílčí cíl/audit	**Procesy podle metodiky Cobit**	**Jiná kriteria**
Hodnocení vazeb mezi strategií podniku a strategií rozvoje IT/IS (IT Governance),	PO1 Define a strategic IT plan ME4 Provide IT governance	ISO/IEC 38500:2008 Corporate governance for IT G18 IT Governance
Hodnocení politik a postupů útvaru IT/IS (standardů),	PO8 Manage quality ME3 Ensure compliance with external requirements	Není k dispozici
Hodnocení způsobu řízení a financování útvaru IS/IT,	DS6 Identify and allocate costs ME2 Monitor and evaluace internal control	TCO Ukazatelé hodnoty IT
Hodnocení způsobu řízení a financování projektů ,	PO5 Manage the IT investment ME2 Monitor and evaluate internal control	Metodika Val IT
Hodnocení organizační struktury na úrovni podniku a útvaru IS/IT,	PO4 Define IT processes, organization and relationships	G39 IT Organisation
Hodnocení služeb poskytovaných třetí stranou	DS2 Manage third –party services	ITIL
Hodnocení úrovně automatizace řízení útvaru IT.	Není k dispozici	Porovnání s jinými organizacemi podobného zaměření

Každý z těchto dílčích cílů může být samostatným auditem, který hodnotí dílčí aspekt fungování útvaru.

2. **Diskutujte audit politik a postupů útvaru IT (druhy standardů, příklady)**

Nezbytnost *hodnocení politik a postupů útvaru IT/IS (standardů)*, vychází z předpokladu, že pokud má vedení organizace stanovené konkrétní cíle v oblasti IT, potom musí vybudovat mechanismus politik a standardů, které plnění těchto cílů usnadní.
Standardy se mohou dělit na externí a interní. Na nejvyšší úrovni jsou externí standardy- rozhoduje management. Nejčastěji se týkají takových oblastí, jako vnitřní kontrolní systém, řízení projektů, řízení bezpečnosti, řízení kvality atd.



Interní standardy mohou být s celopodnikovou platností nebo s platností v rámci útvaru IS/IT. Při určení rozsahu auditu by toto mělo být upřesněno.

3. **Diskutujte audit způsobu řízení a financování útvaru IT (modely financování útvaru, systémy zúčtování za poskytované služby, rozpočet útvaru, způsoby vykazování hodnoty IT ve vazbě na podnikovou strategii).**

Nejčastější modely pro financování útvaru IS/IT:

- útvar IS/IT nemá povahu střediska, náklady na IT/IS jsou režijními náklady, rozpočet pro IT je součástí celopodnikového plánování,
- financování IT je založeno na business metrikách (např. náklady na IT se rozpočítávají v rámci podniku mezi jednotlivé podnikatelské subjekty podle jejich podílu na tržbách),
- financování IT je založeno na IT metrikách. To znamená, že se sleduje čerpání jednotlivých zdrojů IT a činnost útvaru se financuje na základě nákladů potřebných pro tyto zdroje,
- model přímého financování vychází z předchozího modelu, ale náklady určené čerpáním zdrojů se rozpočítávají přímo konkrétním uživatelům (útvarům, střediskům), např. náklady na aplikaci CRM útvaru marketingu,
- model financování se opírá o předem dohodnuté ceny IT služeb. Tento model funguje tam, kde jsou homogenní služby, jako např. roční cena provozu PC. Pokud jsou ale součástí

poskytování služeb ve větším objemu i nestandardní služby, nebo pokud je třeba rozlišovat různé úrovně služeb, potom není tento model vhodný,

- financování se opírá o cenu business transakce (např. cena faktury). Tento model je z pohledu uživatelů nejlepší, ale současně představuje velký problém pro útvar IS/IT, protože stanovit spravedlivě tyto ceny není jednoduché vzhledem ke složitosti a propojení systémů a procesů podílejících se na těchto transakcích,
- financování vychází z předchozích modelů, ve kterých se stanovuje cena za jednotku služeb IT, ale tato cena zahrnuje ziskovou složku. Získané peníze se potom investují do projektů. Někdy se tento modle označuje jako interní outsourcing. To znamená, že jde o obdobný model, jako při poskytování služeb externím poskytovatelem. Tento model není častý a využívá se tam, kde se organizace připravuje na vyčlenění útvaru IS/IT do samostatného právního subjektu, tzn. při přechodu na externí outsourcing.

Systémy zúčtování za poskytované služby se liší v tom, jakým způsobem se přiřazují náklady za čerpání IT zdrojů uživatelům. V úvahu připadají dva modely:

- *nákladový model* - celkové náklady na IS/IT (přímé, nepřímé, režijní) se rozpočítávají např. podle počtu uživatelů nebo organizačních jednotek; jde o nejčastější model,
- *model ABC* (Activity Based Costing, v případě IT jde spíše o model SBC – Service Based Costing) - přímé, nepřímé náklady se zjišťují podle jednotlivých služeb (např. help desk) a dále se rozpočítávají podle jednotek služeb (požadavek na help desk), které mohou být rozúčtovány jednotlivým uživatelům. Režijní náklady se formou procentní marže připočítávají k přímým a nepřímým nákladům služby.

Způsoby vykazování hodnoty IT ve vazbě na podnikovou strategii
Ukazuje, jakým způsobem se vykazuje hodnota IT vzhledem k podnikatelským aktivitám. Pro tuto oblast existuje řada metrik, které je možné členit do tříd podle toho, jaké oblasti řízení IT se týká:

- metriky provozních rozpočtů: meziroční vývoj rozpočtů, jejich alokace podle organizační struktury, výše rozpočtu jako procento celkových příjmů/výdajů organizace, výše rozpočtu na jednoho zaměstnance, výše rozpočtu na jednoho uživatele, výše rozpočtu na jednu stanici, podíly jednotlivých položek,

- metriky kapitálových rozpočtů: meziroční vývoj, procento provozního rozpočtu, změny ve struktuře,

- metriky HW/platforem: počet PC a jejich vývoj, počet serverů a jejich vývoj, objem zpracování operačními systémy, počet zaměstnanců/uživatelů na 1 kus, apod.,

- metriky personální: podíl zaměstnanců/uživatelů na jednoho IT zaměstnance, trendy ve vývoji počtu zaměstnanců IT, roční výdaje na školení na jednoho zaměstnance IT, atd.

4. Uveďte dílčí cíle auditu databází a doporučená kriteria pro jejich hodnocení

Audit databáze může zahrnovat tyto dílčí cíle/audity:

- hodnocení vazeb na ostatní vrstvy systému,
- hodnocení životního cyklu databáze,
- hodnocení autentizace a autorizace,
- hodnocení ochrany citlivých dat,
- hodnocení kontinuity provozu databáze,
- hodnocení výkonnosti databáze,
- hodnocení automatizovaných nástrojů auditu databáze.

Kritéria - V metodice Cobit není žádný proces, o který by se auditor mohl opřít. Výjimku představuje dokument organizace ISACA: Oracle Database Security, Audit and Control Features. Ostatní procesy,

návody a postupy se auditu databáze týkají zprostředkovaně a auditor musí zvážit, které z nich do konkrétního auditu zařadí.

5. Diskutujte audit vazeb na ostatní vrstvy systému, strukturu databáze

Audit databáze je příkladem auditu jednoho prvku, ev. vrstvy informačního systému. Každý informační systém má několik vrstev, z nichž každá může být předmětem auditu:

• komunikační vrstva: předmětem auditu jsou bezpečnost a průchodnost sítě (např. šifrování),
• aplikační vrstva: předmětem auditu mohou být kontroly legálnosti aplikací (licenční audit) spojené s inventarizací, dále aplikační kontroly vstupu, zpracování a výstupu
• vrstva operačního systému: předmětem auditu jsou kontroly autentizace, autorizace, a zálohování,
• databázová vrstva: předmětem auditu může být autentizace, autorizace, šifrování, zálohování.

Při auditu je potřeba aplikovat holistický přístup (mít na zřeteli všechny části systému). Chybou by bylo, kdybychom se zaměřili na jednu vrstvu a ostatními se nezabývali. Mezi vrstvami existují vazby.

Dalším důležitým aspektem pro audit DB je potřeba porozumět struktuře databáze. Například databáze Oracle rozlišuje tyto prvky:

• instance: souhrn procesů operačního systému, které zajišťují přístup, aktualizaci a řízení souborů (datových, metadat, kontrolních). Jde o data v databázi vztažená k určitému časovému okamžiku.
• databáze: souhrn fyzických souborů, které se nacházejí na jednom nebo více diskách, které ukládají a organizují data.
• tabulkové prostory: logický souhrn datových souborů, skládají se ze segmentů,
• segment: obsahují data různého druhu (tabulky, indexy), skládají se z extentů,
• extent: logická datová entita, která je tvořena bloky,
• bloky: nejmenší jednotky dat; velikost se musí určit při vytváření databáze.

6. Diskutujte obsah auditu životního cyklu databáze podle jednotlivých etap

<u>Etapa pořízení/návrhu DB</u>

• prověřit postupy výběru tak, aby odpovídaly potřebám organizace, potřeba definovat funkční požadavky (povinné, volitelné),
• prověřit existenci metrik pro hodnocení nové DB,
• prověřit, že pořízená DB odpovídá stanoveným vnitřním nařízením a standardům
• prověřit dokumenty spojené s pořízením a údržbou databáze (cena, služby údržby).

<u>Etapa instalace a testování SW</u>

• v případě potřeby testování DB před instalací je nutné testování provádět odděleně od provozu, ale v podobných podmínkách,
• testuje se a instaluje pouze licencovaný SW,
• instalace se provádí podle návodu dodavatele, veškeré odchylky se konzultují s dodavatelem,
• před naplněním DB se data konsolidují,
• testují se standardně nastavené parametry (např. pro auditování).

<u>Etapa údržby DB</u>

• údržba instalovaného systému se provádí koordinovaně s aktualizacemi návazných systémů (aplikací) a návodů dodavatele,
• údržba se provádí kvalifikovaným personálem vlastním nebo dodavatele
• výjimky v transakcích DB se monitorují, sledují a opravují
• sledují se smlouvy na údržbu, hodnotí se efektivnost údržby,
• existuje proces řízení změn, v jehož rámci se koordinují změny ve všech vrstvách

• zabudované nástroje zaznamenávají všechny důležité nebo neobvyklé změny v DB,
• existuje oddělení odpovědností, především mezi správci aplikací, databáze a sítě,
• existuje proces přidělování přístupových práv,
• monitoruje se využívání systémových práv,
• pravidla pro mazání dat z auditu DB, případně pro jejich archivaci na vhodné velkokapacitní úložiště.

7. Diskutujte obsah audit přístupu do databáze (typy uživatelů, druhy kontrol)

Kontroly přístupu do databáze se týkají těchto kategorií uživatelů:
• přímí uživatelé: pro přístup k databázi využívají DBMS, dotazovací jazyky,
• aplikační uživatelé: pro přístup využívají podnikové aplikace typu ERP systémů, webové aplikace,
• administrátoři: především DBA - databázový administrátor, ale také správce bezpečnosti, sítí, aplikací, systému,
• třetí strany: dodavatelé systému, poskytovatelé služeb údržby apod.
• vývojáři a programátoři aplikací.
Audit přístupu do databáze zahrnuje kontroly autentizace a autorizace. Při auditu přístupu do databáze se musí věnovat zvláštní pozornost administrátorským účtům. Auditor by měl prověřit, komu byl přiznán přístup jako administrátoru databáze (DBA - Database Administrátor Access) a jak je tento přístup využíván. Po prověření autentizačních kontrol se hodnotí, jaká existuje politika a postupy autorizace (přidělování přístupových práv).

8. Diskutujte obsah auditu integrity databáze a ochrany citlivých dat (druhy integrity, druhy kontrol, příklady)

Integritním omezením jsou součástí definice databáze a za jejich splnění odpovídá systém řízení databáze. Může být trojího typu:

• entitní integrita (integrita na úrovni tabulky): vyžaduje, aby každá tabulka měla primární klíč, který je pro každý záznam unikátní, tedy že neexistují duplicitní záznamy,
• referenční integrita: (integrita na úrovni vztahů) zajišťuje spolehlivost vztahu mezi dvěma tabulkami. Záznamy v obou tabulkách jsou synchronizovány a v případě změn dat v jedné tabulce, jsou v druhé měněna stejným způsobem
• doménová integrita (integrita na úrovni pole) zajišťuje, že hodnoty v každém poli jsou platné (tedy struktura poleje spolehlivá). Pole stejného typu jsou v celé databázi definována konzistentně.

Nástroje na ochranu citlivých dat kombinují nástroje pro řízení přístupu k těmto datům a nástroje šifrování. Šifrování přenosu dat má za cíl zabránit odposlechnutí či dokonce pozměnění komunikace. Vedle SSL lze pro šifrování přenosu dat použít i některé další algoritmy (např. v databázi Oracle nástroj Advanced Security Option).

9. Diskutujte obsah auditu kontinuity databáze (druhy záloh, technologie, strategie)

Kontinuita provozu databáze je spojena s procesy zálohování a obnovy databáze. Při jejich auditování nemá auditor lehkou práci, protože neexistuje žádný univerzální recept na to, jak efektivně zálohovat data a provádět jejich obnovu. Obecná kritéria pro posouzení tedy neexistují a měla by proto být v každé organizaci součástí interních standardů (politik a postupů).

• zálohy podle předmětu:
- HW, operační systém, aplikace, data, media, lidé, dokumentace
• zálohy podle provozu:

- on-line zálohy: provádějící se za chodu databáze (nekonzistentní),
- off-line zálohy: provádějí se při vypnuté databázi (konzistentní zálohy),
• zálohy podle objemu:
- inkrementální: zálohují se pouze změny proti předchozí záloze,
- úplné: zálohuje se úplná databáze,
• zálohy podle použitých prostředků:
on-site zálohy: zálohy vlastními prostředky, off-site zálohy: zálohy externími prostředky,
• zálohy podle míry automatizace:
- ruční zálohování: příkazy k zálohování provádí IT pracovník podle definovaných strategií,
- automatizované zálohování: zálohování se provádí automatizovaně, a to buď prostředky zabudovanými v databázi nebo specializovanými prostředky pro zálohování variant těchto procesů, nebo dále podle harmonogramu (např. každý den v určitou hodinu), nebo pravidelných intervalech (např. po 48 hodinách).
• zálohy podle použité technologie

Při hodnocení technologií usnadňujících zálohování a tím i rychlou obnovu podnikání se může auditor setkat se dvěma přístupy:

• výběr univerzálních řešení pro pokrytí všech předpokládaných a možných požadavků aplikací podle principu „jedna velikost pro všechny".
• výběr specifických produktů - pro pokrytí požadavků na zálohování jednotlivých aplikací se vychází z podrobné analýzy potřeb. Tento postup je pracnější, protože vyžaduje tyto kroky:
- provedení analýzy rizik, stanovení parametrů obnovy, výběr technologií pro jednotlivé aplikace.

10. Uveďte dílčí cíle a kriteria pro audit procesu řízení změn

Audit jakéhokoliv procesu IT je v porovnání s jinými druhy auditu poměrně jednoduchou záležitostí. Důvodem je, že existují dvě kvalitní procesně orientované metodiky, které mohou pro tento typ auditu sloužit jako kriterium. Jde o metodiky Cobit a ITIL.

Dílčí cíl/audit	**Procesy podle metodiky Cobit**	**Jiná kriteria**
Standardy a postupy procesu	AI6 Manage changes PC1 – PC6	ITIL ST 4.2 Change management
Hodnocení dopadu, určování priorit, autorizace		
Naléhavé změny		
Sledování a hlášení stavu změn		
Uzavření změny a dokumentace		

11. Diskutujte jednotlivé dílčí cíle auditu procesu řízení změn a doporučené činnosti auditora.

Viz. 10 + následující.
Vzhledem k různému zaměření a cílům metodiky Cobit a ITIL je zřejmé, že jak při implementaci procesů IT, tak i při jejich hodnocení, je výhodné jejich vhodná kombinace. Tuto činnost usnadňují mapující dokumenty, které vydala organizace ISACA (Mapping of ITIL with Cobit 4.1). Přehled dílčích cílů auditu a kriterií
Auditor by podle dokumentu IT Assurance Guide měl prověřit, zda tento formální postup zahrnuje:

- definování rolí a odpovědností,
- klasifikaci a postup stanovení priorit změn,
- hodnocení dopadu změn, schválení změn,
- sledování realizace změn,
- mechanismus pro kontrolu verzí,

- dopad na integritu dat,
- pokyny pro nakládání s naléhavými změnami,
- plánování kontinuity,
- využívání systému pro záznam změn,
- oddělení odpovědností.

Dále má prověřit, že v případě poskytování služeb třetími stranami, jsou i ony součástí procesu a zda jsou ošetřeny ve smlouvách na dodávky služeb.

* Otázka mimo okruhy, která se objevila v testu:

- Rozdíl mezi autoritativním a disciplinárním přístupem auditu.
  - Autoritativní – oddělení autority do nezávislých poradenských firem, zvýšení nezávislosti na podnicích. Ze zákona mají auditoři nárok na všechny informace, o jaké si požádají.
  - Disciplinární – zajišťuje ochranu integrity podniků v sociálních systémech – určuje, jaké informace je možné zveřejňovat mimo podnikový systém. Omezuje autoritu, aby nedocházelo k její koncentraci.