ECOVIS RG
– Jak efektivně podpořit statutární audit IT auditem

Igor Barva, 3.11.2022

ECOVIS Česká republika

ECOVIS blf
- 14 profesionálů, z toho 5 statutárních auditorů
- Auditorské služby
- Partneři: Jan Bláha, Miloš Fiala
- V ECOVISu od 2006

ECOVIS FACTA
- 30 profesionálů
- Účetní a daňové služby
- Partner: Simona Fialová
- V ECOVISu od 2020

ECOVIS Ježek, advokátní kancelář
- 10 profesionálů
- Partner: Mojmír Ježek
- V ECOVISu od 2019

ECOVIS CBC Tax
- 3 profesionálové
- Daňové služby
- Partner: Hans van Capelleveen
- V ECOVISu od 2016

ECOVIS Corporate Finance
- 3 profesionálové
- Finanční poradenství
- Partner: Jan Slabý
- V ECOVISu od 2005

ECOVIS RG
- 4 profesionálové
- Partner: Igor Barva
- V ECOVISu od 2020

Finanční versus IT audit

Finanční audit

- je nezávislé ověření účetních výkazů auditorem v míře dostatečné k vyslovení názoru, zda předložené účetní výkazy jsou pravdivé a věrné a zda jsou v souladu s odpovídajícími předpisy.

IT audit

- je ověření řídících kontrol v prostředí Informačních technologií respektive infrastruktury. Hodnocení získaných evidencí určí, zdali informační systémy chrání informační aktiva, jejich integritu a účinně podporují cíle organizace.

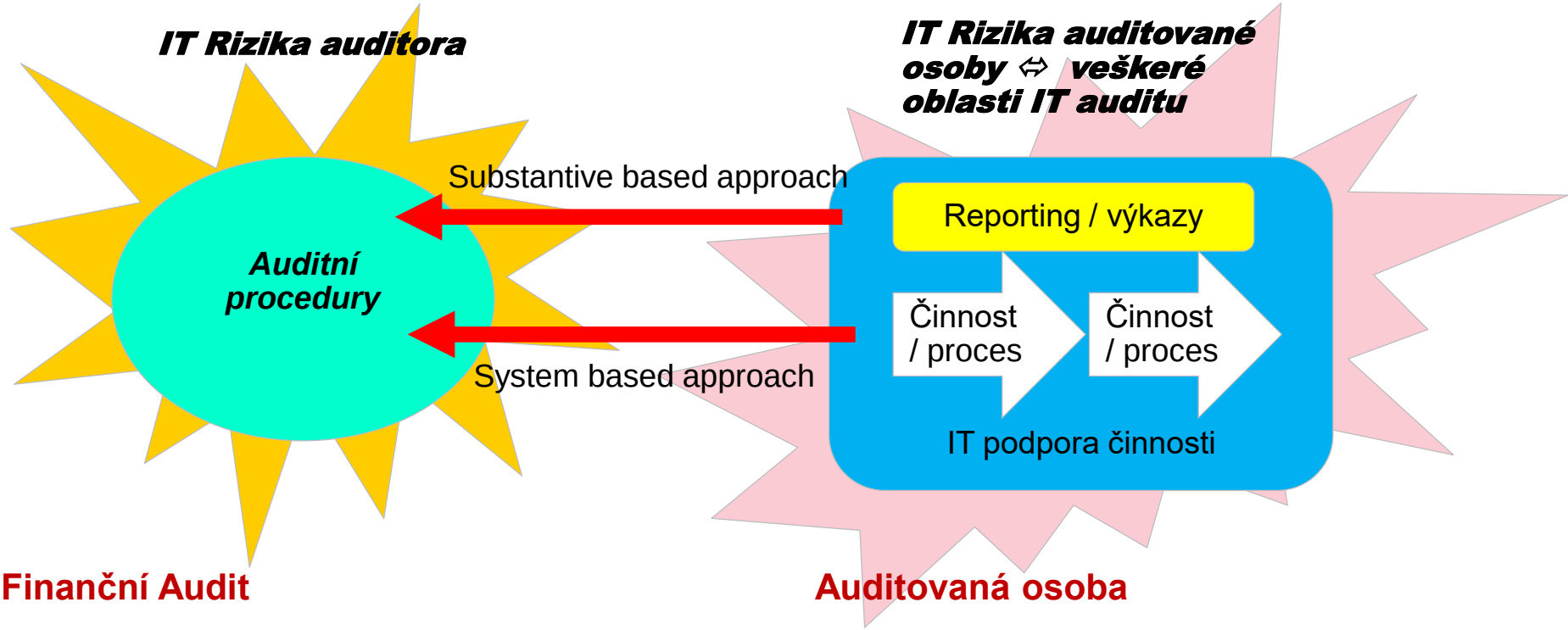
Jaká je závislost klienta resp. jeho fin. výkazů na IT a automatizovaném zpracování dat a procesů v aplikacích?

- Prakticky neexistují klienti bez IT. Míra a kvalita automatizace resp. závislosti na IT je různá.

Jaké postupy IT auditu efektivně podpoří postupy a závěry finančního auditu?

- Vazby většinou nejsou přímé
- Nutné postupovat přes rizika a kontroly v systémovém přístupu k auditu

IT rizika auditované osoby X IT rizika auditora



Finanční Audit

- Produkt = Ověření výkazů
- IT = Poskytuje IT věrný obraz
- Která část výkazů závisí na IT?
- Může IT audit mít přidanou hodnotu?

Auditovaná osoba

- Produkt = provoz činnosti
- IT = podpora činnosti

Techniky IT auditu

ITGC – Obecné IT kontroly

- **Obecné IT kontroly se zaměřují na kontroly prostředí IT jako takového. Klasickým příkladem jsou kontroly provozních serverů a nastavení sítí, přístupy do IT prostředí, kontroly vývoje a změn, řízení dostupnosti atp.**

ITAC – Aplikační kontroly

- **Souvisejí především s ověřením kontrolních mechanismů zabudovaných do automatizovaných procesů organizace a zpracovávající související informace (data).**

D&I: Design & Implementation vnitřních kontrol a jejich porozumění

„Jediným účelem kontroly je zmírnit riziko. Kontrola bez cíle zmírnění rizika je neutrální ve své funkci. Riziko tedy musí existovat, než bude možné ho zmírnit vnitřní kontrolou.“

Společnosti často ve své provozní slepotě tuto skutečnost ignorují a auditoři, pokud začínají dokumentací systému a vnitřních kontrol, které existují, aniž by se zamysleli nad existencí a popsáním rizika. Tento přístup může mít za následek spoustu zbytečné práce při dokumentování procesů a kontrol, které se mohou později ukázat jako zcela irelevantní pro cíle auditu.

ITGC + ITAC – Fin audit - RESTAURACE

Finanční audit = audit dodávek a kvality jídel a nápojů v restauraci

Data = potraviny; zpracování dat = receptury; výkazy = prodeje

- Byla veškerá jídla vydána? Měla veškerá jídla správné parametry (chuť množství knedlíků, váha masa, míra nápojů? Byla veškerá jídla zaplacena dle objednávek?

ITGC = audit prostředí kuchyně a skladů

- Má restaurace potvrzení od statika budovy? Je používána pitná voda? Mají elektrické spotřebiče příslušné revize?
- Jsou potraviny správně skladovány (odděleně a za příslušných parametrů)?
- Jsou jednotlivé části přípravy správně řízeny z pohledu hygieny?
- Jsou knihy všech receptur přístupné příslušným kuchařům?

ITAC = audit potravin a přípravy jídel

- Jsou potraviny dostupné a čerstvé, jsou řádně ošetřovány, kdo s nimi naposledy nakládal, jsou vydávána ze skladu ve správném pořadí, kdy proběhla naposledy kontrola jejich kvality
- Jsou receptury při přípravě používány bez odchylek v postupech, jsou automatizované kontroly (např. nastavení časů a teplot vaření) v souladu s recepty
- Odpovídá skladba jídel objednávkám, jaké jsou časy výroby od jejich objednání do dodání servisu, počty reklamací apod.

ITAC – kontroly v aplikacích a datech

Code Review – White box aplikace (makra, sestavování report = řízek.)

- Musí být přístup k zdrojovému kódu (nepravděpodobné)
- Musí být přístup k vývojové dokumentaci (často nedostupná)
- Následně lze v kódu samotném identifikovat kontrolní mechanismy, ohodnotit jejich rozsah a účinnost (nutná znalost alespoň základů programování a jazyka)

CAAT – analýza dat

- Nutný přístup k datům. Zpracování spec. nástroji (ACL, IDEA) nebo xls, SQL.
- Analýza 100% všech záznamů na podezřelé transakce, odchylky, trendy, výběr vzorků (je-li třeba).

CAAT – rekalkulace (Black Box aplikace = Johančino tajemství)

- Nutný přístup k datům a rovněž k metodě zpracování dat v aplikací = popisy nebo alespoň analytická dokumentace z vývoje.
- Vytvoření prakticky kopie metody zpracování (programu) auditorem a následné porovnání výsledků a vysvětlení odchylek.
- De facto vytvoření dlouhodobě použitelných substantivních testů nad 100% dat.

ITAC – kontroly v aplikacích a datech

Použití ITAC

- **Velmi záleží na povaze činnosti a míře automatizace procesů**
- **záleží na rizicích auditu a povaze automatizace procesů**
- **Musí být přístup k vývojové dokumentaci (často nedostupná) nebo**
- **Musí existovat znalost (metody a postupy) automatizovaného zpracování**
- **ITAC je náročnou činností (Pravidlo 1:1:1)**
  - Pochopit a definovat vlastní postup (design kontrolního postupu)
  - Automatizovat vlastní postup (odstranění lidského faktoru)
  - Dokumentace vytvořeného postupu
- **ITAC nelze použít bez ITGC ⇔ aplikace a data jsou jen tak dobré, jak dobré je prostředí, ve kterém jsou provozována)**
- **ITAC se musí vyplatit (velké nebo víceleté zakázky)**

Definice poptávky služeb IT Auditora při přípravě auditu

Výběr relevantních auditních zakázek (audit planning)

- Je vhodný / nutný / aplikovatelný systém based approach (SysBA)?
- Jaké údaje / procesy závisí na SysBA a jak jsou rizikové pro výrok auditora
- Co je možné ověřit postupy IT auditora a kterými?

Dohoda o rozsahu zapojení IT auditora (předaudit)

Jakou míru ujištění získám zapojením vybraných postupů IT auditora pro svůj finanční audit?

- ITGC – IT General controls (ISO 27002)
- ITAC – IT Application controls (process based internal controls)
- CAAT – Computer Assiseted Audit Techniques - definice

Samotné provedení prací (předaudit + audit)

- ITGC+ITAC (předaudit) => úspora rozsahu procedur pro plánování auditu
- CAAT (audit) => nahrazení / automatizace samotných auditních postupů (xls/ACL)

Děkujeme za pozornost

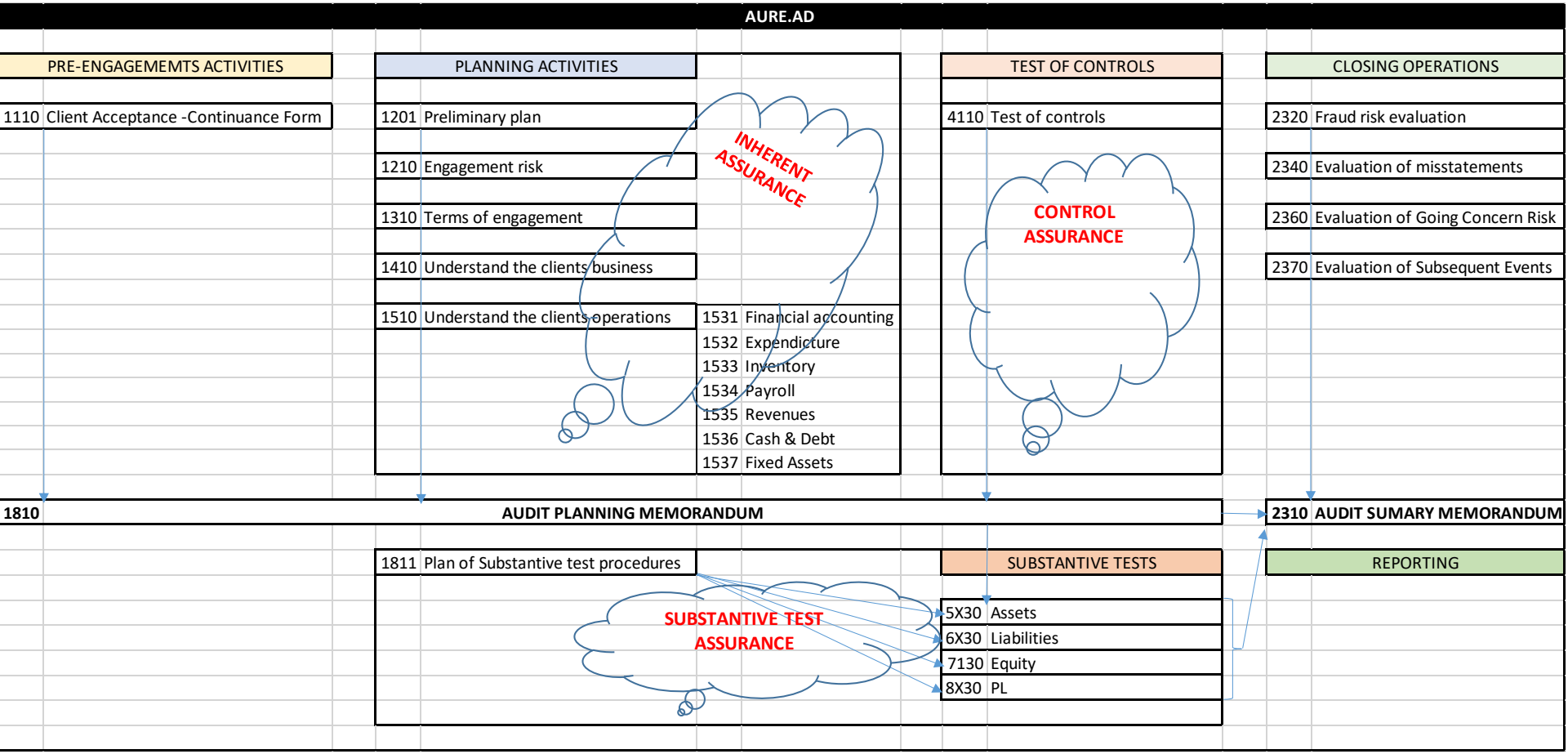
ECOVIS RG s.r.o.

Na Veselou 962, Beroun 266 01
E-Mail: igor.barva@ecovis.cz
GSM: +420 603 892 662
Internet: www.ecovis.com/prague


Bup Slides
Jak správně určit potřebu postupů IT auditu na zakázce Fin. auditu?

Postupy při zvažování využití IT Auditu

auditní nástoj Aure.Ad - www.attis.cz – nástin metodiky



Zvážení inherent assurance pro využití postupů IT auditu

Fin. Audit Planning Phase – inherent assurance

- Vedoucí auditní zakázky musí svážit zapojení (ano/ne) a definice případné míry zapojení IT auditu do auditních postupů. Možné prvotní přizvání IT experta nemá-li vedoucí auditní zakázky zkušenosti s využitím s potencionálním i přínosy IT auditu.
- Bude finanční audit využívat testy kontrol (pokud ne ITGC a velká část ITACnení relevantní) – zbývá pouze analýza dat a případná pomoc s tvorbou substantivních testů (nepravděpodobný scénář)
- Pokud finanční audit bude používat testy kontrol, pak závisí na zvážení rizik

1400 – Understanding Client Business

- Nakolik je obor závislý na IT (Telekomunikace, finance, média X řízení projektů X cestovní ruch)?
- Možné přizvání IT experta k posouzení situace, ale rozhodnutí náleží vedoucímu auditní zakázky.

1500 - Understand the clients operations (ISA 315)

- Nakolik je auditovaný klient ve svých hlavních činnostech závislý na podpoře IT
- Nakolik je výsledek fin auditu závislý na podkladech z IT systémů
- V případě silné závislosti mohou být IT prostředí a postupy sami o sobě jedním z hlavních provozních činností (první možná subdodávka)

Zvážení inherent assurance pro využití postupů IT auditu

Fin. Audit Planning Phase – inherent assurance

1500 - Understand the clients operations (ISA 315)

Porozumění IT prostředí klienta zahrnuje mj. následující:

- Neexistují zásady / postupy zajišťující efektivní dohled nad vedením nebo pracovníky IT;
- Požadavek na spolehlivost je kladen na systémy / programy, které zpracovávají data nebo údaje pro finanční výkaznictví;
- Neexistuje neoprávněný přístup k datům. Je možné zničení dat, zaznamenání neautorizovaných nebo neexistujících transakcí nebo nepřesné zaznamenávání transakcí;
- Výdaje na IT a investice do IT odpovídají riziku a jeho důležitosti ve společnosti;
- Existuje pravidelné zálohování dat
- Existuje pravidelné vyhodnocování problémů v IT a doba jejich odstranění

Posuzování interních kontrol

Fin. Audit Planning Phase – inherent assurance

1500 - Understand the clients operations (ISA 315)

- **D&I: Design (popis) & Implementation (Implementace) vnitřních kontrol a jejich porozumění**

Interní kontroly lze obecně klasifikovat jako **všudypřítomné kontroly** (na úrovni entit), které se zabývají všudypřítomnými riziky (obchodní, fraud, GITC atd.) a **specifické kontroly** (transakční), které řeší konkrétní rizika.

Posuzování interních kontrol

Kvalita je proces, který nikdy nebude dokonalý a proto konečný

1500 - Understand the clients operations (ISA 315)

- **D&I: Design (popis) & Implementation (Implementace) vnitřních kontrol a jejich porozumění**

  Všudypřítomné kontroly (na úrovni entit) se zabývají řízením a slouží k vytvoření celkového kontrolního prostředí. Typické kontrolní procesy zahrnují lidské zdroje, podvody, hodnocení rizik vedením, obecná správa IT, příprava finančních informací (včetně účetních výkazů atd.) U malých účetních jednotek se tyto kontroly budou vztahovat především na vedení.

  Důkladné porozumění všudypřítomným prvkům vnitřní kontroly poskytuje důležitý základ pro posuzování příslušných kontrol nad finančním výkaznictvím na transakční úrovni.

Neignorujme automatizované (IT) kontroly

Velikost vzorku pro testování automatizovaného řízení může být jen jedna položka, protože pro automatizované řízení je pravděpodobné, že ovládání bude fungovat pokaždé stejným způsobem, takže bude reprezentativní pro všechny ostatní položky populace. To by však bylo založeno na předpokladu, že účetní jednotka má účinné obecné IT kontroly (ITGC).

Zvážení control assurance pro využití postupů IT auditu

Fin Audit Test od Controls phase – control assurance

4000 – Audit Assurance Model

Audit assurance model						
	Engagement risk		Engagement risk		Engagement risk	
	Normal		Greater than Normal		Much Greater than Normal	
Inherent assurance	**YES**		**NO**		**NO**	
	Test of control		Test of control		Test of control	
	Effective	Non effective	Effective	Non effective	Effective	Non effective
Control assurance	**YES**	**NO**	**YES**	**NO**	**NO**	**NO**
	Substantive testing		Substantive testing		Substantive testing	
Substantive test assurance (R)	**Basic level**	**Intermediate level**	**Intermediate level**	**Focussed level**	**Focussed level**	**Focussed level**
Kvantil Normalniho normovaneho rozdeleni	**0,7**	**2**	**2**	**3**	**3**	**3**
Auditor assurance obtained to draft the opinion	YES	YES	YES	YES	YES	YES

Pokud je **riziko zakázky Much Greater than Normal**, nelze provádět testy kontrol a veškeré ujištění je získáno prostřednictvím testů věcné správnosti (R-3).

Pokud se auditor rozhodne provádět **Test kontrol**, musí být vytvořen tz. **Rotační plán**, kde jsou naplánované testy pro běžné a následující dvě období.

Auditor provádí testy kontrol dle rotačního plánu - **v případě prováděných testů na úrovni spolehlivosti 90%,** použije se pro dané oblasti R - LOW, namísto R - 0,7; a R - 0,7, namísto 2.

Při aplikaci R - LOW se vzorek pro detailní testování stanovuje úsudkem (1-3 vzorky).

Zvážení control assurance pro využití postupů IT auditu

Kvalita je proces, který nikdy nebude dokonalý a proto konečný

4000 – Test of Controls (ISA 330, 500, 530)

Kdy zvážit použití testů kontrol?

Získané informace o interní kontrole (D&I) použijme k identifikaci klíčových kontrol, na které lze testovat jejich provozní účinnost. Testování ovládacích prvků klíčových kontrol (některé z nich mohou být testované pouze jednou za tři roky – rotační plán) může často vyústit v mnohem méně práce než při provádění rozsáhlých testů věcné správnosti.

Rozhodnutí otestovat provozní účinnost kontroly je věcí odborného úsudku

„Pokud auditor plánuje použít důkazní informace z předchozího auditu týkající se provozní účinnosti konkrétních kontrol, je povinen zjistit trvalou relevanci těchto důkazů získáním důkazních informací o tom, zda došlo k významným změnám v těchto kontrolách po předchozím auditu. Auditor získá své důkazy provedením šetření v kombinaci s pozorováním nebo inspekcí, aby ověřil porozumění těmto konkrétním kontrolám:

(a) Pokud došlo ke změnám, které ovlivňují trvalou relevanci důkazních informací, auditor ověří kontroly v aktuálním auditu.

(b) Pokud k takovým změnám nedošlo, auditor alespoň jednou prověří kontroly každý třetí audit“

Zvážení control assurance pro využití postupů IT auditu

Fin Audit Test od Controls phase – control assurance

- Pokud byly v plánovací fázi definovány požadavky na ověření IT prostředí, pak musí IT expert ve spolupráci s manažerem auditní zakázky zvážit nutný rozsah ověření ITGC a ITAC.
- ITGC často prověřovány na rotační bázi dle souvisejících rizik
- ITAC jsou prováděny specificky

– Zaměřit se pouze na rizika (respektive kontroly) spojená s auditem

Design - Byly navrženy kontroly, které zmírní existující rizika?

- Kontroly rozlišujme jako Manuální, nebo Automatizované
- Ke kontrole přiřaďme tvrzení (Assertions), které pokrývá
- Ke kontrole přiřaďme jejich četnost (denní, týdenní, mesíční, kvartální, nebo občasná)

4110– Understanding Client Business

- Dokumentace vybraných ITGC a ITAC kontrol dle plánu
- Ukázka ITGC viz vzorový spis Auditora společnosti QRP a.s.

Použití ITAC (CAAT) pro potřeby substantive assurance

Kvalita je proces, který nikdy nebude dokonalý a proto konečný

4000 – Test of Controls (ISA 330, 500, 530)

Kocept maxilmálního vzorku

Určení velikosti vzorku pro test provozní spolehlivosti kontrol

Velikost vzorku = Faktor spolehlivosti ÷ Tolerovatelná odchylka

Tolerovatelná míra odchylky se používá pro testy kontrol, kde auditor stanoví míru odchylky od předepsaných postupů vnitřní kontroly, aby získal odpovídající úroveň ujištění. Maximální přípustná odchylka může být 10%.

Pro testování provozní účinnosti vnitřních kontrol s minimální závislostí na ostatní prováděné práci v rámci auditu se často používá 90% úroveň faktoru spolehlivosti (faktor spolehlivosti = 2,3).

Velikost vzorku = 2,3 ÷ 0,1 = 23

ECOVIS úpravy postupů 2020

Kvalita je proces, který nikdy nebude dokonalý a proto konečný

4000 – Test of Controls (ISA 330, 500, 530)

Určení velikosti vzorku pro test provozní spolehlivosti kontrol (pokračování)

A) Pokud mohou být pro konkrétní tvrzení získány další ujištění (například testy věcné správnosti), mohl by být faktor spolehlivosti snížen tak, že testováním provozní účinnosti kontroly bude získána pouze mírná úroveň snížení rizika. V takovém případě by mohla být použita úroveň faktoru spolehlivosti 80% (související faktor spolehlivosti = 1,61), což má za následek nejmenší velikost vzorku 8.

Velikost vzorku = 1,61 ÷ 0,2 = 8

B) Pro výběr vzorků, kde kontrola neprobíhá na denní bázi, lze velikosti vzorků definovat takto (za předpokladu použité úrovně spolehlivosti 90%):

Týdenní cyklus kontroly: 10

Měsíční cyklus kontroly: 2-4

Čtvrtletní cyklus kontroly: 2

Roční cyklus kontroly: 1

ECOVIS úpravy postupů 2020

Kvalita je proces, který nikdy nebude dokonalý a proto konečný

Co to vše znamená?

Zvýšený důraz na přípravu auditu; znalost klienta a jeho procesů a nastavení kontrolního prostředí.

Přesnou dokumentaci a zvýšený důraz na popis prováděních auditních procedur; přesná a jednoznačná terminologie je nezbytné východisko správného postupu.

Prolnutí jednotlivých fází auditu – test kontrol lze provést ve finální fázi auditu a naopak test věcné správnosti při předauditu.

Postupy při zvažování využití IT Auditu

auditní nástoj Aure.Ad - www.attis.cz – nástin metodiky