IAPS 1013

VLIV ELEKTRONICKÉHO OBCHODOVÁNÍ NA ÚČETNÍ ZÁVĚRKU

(Tento pokyn je platný)

OBSAH

	Odstavce
Úvod ……	1-5
Schopnosti a znalosti ……...	6-7
Znalost podnikatelské činnosti/podnikání ……..	8-18
Odhalení rizika ……	19-24
Posouzení vnitřní kontroly ……..	25-34
Vliv elektronických záznamů na důkazní informace ……...	35-36

Mezinárodní auditorský pokyn pro praxi IAPS 1013 „Vliv elektronického obchodování na účetní závěrku“ je nutné chápat v kontextu Předmluvy k mezinárodním standardům pro kontrolu kvality, audit, ověřování a související služby, která stanoví pravidla a rozsah použití těchto pokynů.

Tento pokyn nevytváří nové základní principy a postupy. Jeho účelem je pomoci auditorům a rozvíjet dobrou praxi poskytnutím:

(a) návodu na uplatnění standardů ISA, pokud auditovaný subjekt využívá veřejnou síť, jakou je například Internet, v elektronickém obchodování
(b) materiálu pro zvýšení povědomí o problematice auditu účetní závěrky v této rychle se rozvíjející oblasti.

Auditor využije odborného úsudku k tomu, aby určil rozsah, v jakém lze auditorských postupů popsaných v tomto pokynu využít, a to vše s ohledem na požadavky ISA a konkrétní situaci auditovaného subjektu.

IAPC schválil a vydal tento pokyn v březnu 2002.

Úvod

1. Cílem tohoto pokynu je poskytnout návod auditorům v případě, kdy se auditovaný subjekt zabývá podnikatelskou činností, kterou provozuje prostřednictvím počítačů připojených do veřejné sítě, jakou je například Internet (elektronické obchodování, e-commerce[1]). Návod v tomto pokynu je relevantní v souvislosti s uplatňováním ISA 300 „Plánování", ISA 310 „Znalost podnikání" a ISA 400 „Vyhodnocení rizik a vnitřní kontrola".

2. Tento pokyn zmiňuje zvláštní skutečnosti, které pomohou auditorovi při posuzování významu elektronického obchodování pro podnikatelskou činnost auditovaného subjektu a vlivu elektronického obchodování na auditorovo hodnocení rizika pro účely vyslovení výroku o účetní závěrce. Účelem posouzení auditorem není vyslovit výrok nebo poskytnout radu ohledně systémů nebo činnosti auditovaného subjektu v oblasti elektronického obchodování.

3. Komunikace a provádění transakcí pomocí sítí a počítačů nejsou novým prvkem podnikatelského prostředí. Například obchodní procesy často vyžadují spojit se se vzdáleným počítačem, využít počítačové sítě nebo elektronickou výměnu dat (Electronic Data Interchange – „EDI"). Ovšem zvýšené využívání Internetu při elektronickém obchodování se zákazníkem, podniky, vládou a zaměstnanci s sebou přináší nová rizika, kterým musí auditovaný subjekt čelit a která musí auditor posoudit při plánování a provádění auditu účetní závěrky.

4. Internet je celosvětovou sítí počítačových sítí; sdílenou veřejnou sítí, která umožňuje komunikovat s jinými subjekty a osobami na celém světě. Komunikace je vzájemná, tj. každý počítač připojený na Internet může komunikovat s kterýmkoli jiným počítačem připojeným na Internet. Internet je síť veřejná, na rozdíl od soukromých sítí, které umožňují přístup pouze oprávněných osobám nebo subjektům.Využívání veřejné sítě s sebou přináší zvláštní rizika, kterým musí auditovaný subjekt čelit. Nárůst využívání Internetu bez toho, že auditovaný subjekt věnuje těmto rizikům náležitou pozornost, může ovlivnit hodnocení rizika auditorem.

5. Tento pokyn byl vypracován pro případ, kdy auditovaný subjekt podniká prostřednictvím veřejné sítě, jakou je Internet. Mnohé návody, které obsahuje, se dají využít i v soukromé síti auditovaného subjektu. Mnohé návody se také dají využít při auditu subjektů, které vznikly především za účelem elektronického obchodování, ale cílem pokynu není zabývat se všemi otázkami auditu těchto subjektů.

Schopnosti a znalosti

6. Míra schopností a znalostí, které jsou potřebné pro porozumění vlivu elektronického obchodování na audit, se liší podle složitosti činností auditovaného subjektu v oblasti

[1] IAPS používá termín elektronické obchodování.(e-commerce). V podobném kontextu se používá i elektronické podnikání (e-business). Neexistuj všeobecně platné definice těchto termínů a často se zaměňují. Pokud se rozlišují, elektronické obchodování se používá výhradně při obchodování (nákup a prodej zboží a služeb) a elektronické podnikání se používá pro všechny podnikatelské aktivity, obchodní i neobchodní, jako jsou například vztahy a komunikace se zákazníky.

elektronického obchodování. Auditor posoudí, zda zaměstnanci, kteří byli na zakázku přiděleni, mají odpovídají znalosti z oblasti informačních technologií[2] a podnikání přes Internet, aby mohli provést audit. Pokud má elektronické obchodování významný vliv na činnost auditovaného subjektu, odpovídající znalost IT a podnikání přes Internet je nezbytná pro:

- Pochopení, v rozsahu, v jakém mají vliv na účetní závěrku:
  - strategie a činnosti auditovaného subjektu v oblasti elektronického obchodování,
  - technologií, jejichž využití auditovanému subjektu umožňuje elektronicky obchodovat, a znalostí IT a schopností zaměstnanců,
  - rizik, která s sebou přináší elektronické obchodování, a přístupu auditovaného subjektu k řízení těchto rizik, především přiměřenost vnitřního kontrolního systému, včetně bezpečnostní infrastruktury a souvisejících kontrol, které mají vliv na proces finančního výkaznictví

- Určení charakteru, časového plánu a rozsahu auditorských postupů a ohodnocení důkazních informací,

- Posouzení vlivu závislosti auditovaného subjektu na elektronickém obchodování na jeho schopnost dodržet předpoklad časově neomezeného trvání.

7. Auditor se za určitých okolností může rozhodnout využít práce experta, například pokud auditor usoudí, že je vhodné prověřit kontroly pokusem o narušení bezpečnostního systému auditovaného subjektu (testy zranitelnosti nebo průniku). Pokud auditor práci experta využije, získá dostatečné a vhodné důkazní informace, že jeho práce je přiměřená pro účely auditu v souladu s ISA 620 „Využití práce experta". Auditor může také posoudit, jak práce experta zapadá do práce ostatních auditorů a jaké postupy jsou uplatněny ve vztahu k rizikům, která byla prací experta odhalena.

Znalost podnikání

8. ISA 310 „Znalost podnikání" vyžaduje, aby auditor získal dostatečné znalosti podnikání, které mu umožní odhalit a pochopit události, transakce a postupy, které mohou mít výrazný vliv na účetní závěrku nebo zprávu auditora. Znalosti podnikání zahrnují všeobecné znalosti ekonomiky a odvětví, ve kterém auditovaný subjekt podniká. Nárůst elektronického obchodování může mít výrazný vliv na tradiční podnikatelské prostředí auditovaného subjektu.

9. Znalost podnikání je pro auditora zásadní při hodnocení důležitosti elektronického obchodování pro podnikatelskou činnosti auditovaného subjektu a jeho vlivu na auditorské riziko. Auditor posuzuje změny podnikatelského prostředí auditovaného subjektu a odhalená podnikatelská rizika, které souvisí s elektronickým obchodováním a které mají vliv na účetní závěrku. Přestože auditor získá velké množství informací dotazováním u osob, které

[2] Mezinárodní standardy v oblasti vzdělávání IEG 11 „Informační technologie v účetním kontextu", který vydal Výbor pro vzdělávání IFAC a který v širším smyslu definuje oblasti a speciální znalosti a schopnosti, jež se vyžadují od všech účetních odborníků v souvislosti s informačními technologiemi využitými v podnikání.

odpovídají za finanční výkaznictví, dotazování u osob, které se přímo podílejí na elektronickém obchodování auditovaného subjektu, jako například u ředitele IT (Chief Information Officer) nebo jiné osoby na stejné hierarchii, může být také užitečné. Při získávání a aktualizaci znalosti podnikání auditovaného subjektu auditor posuzuje následující skutečnosti, pokud mají vliv na účetní závěrku:

- podnikatelskou činnost auditovaného subjektu a odvětví, ve kterém podniká (odst.10-12),
- strategii auditovaného subjektu pro oblast elektronického obchodování (odst. 13),
- rozsah činnosti auditovaného subjektu v oblasti elektronického obchodování (odst. 14-16),
- dohody auditovaného subjektu o využívání služeb externích dodavatelů/poskytovatelů (outsourcing) (odst.17-18).

Každý z těchto bodů je dále podrobně rozepsán.

Podnikatelská činnost auditovaného subjektu a odvětví, ve kterém podniká

10. Činnosti v oblasti elektronického obchodování mohou být doplňkem tradiční podnikatelské činnosti auditovaného subjektu. Auditovaný subjekt může využívat Internet například pro prodej tradičních výrobků (knih nebo CD), které jsou dodávány tradičním způsobem na základě smlouvy plněné přes Internet. Na druhou stranu může elektronické obchodování být novým druhem podnikatelské činnosti a auditovaný subjekt může využívat svoji webovou stránku k prodeji a dodávání digitálních výrobků po Internetu.

11. Internet nemá jasné, pevně vymezené geografické linie dopravy, které jsou charakteristické pro fyzický obchod se zbožím a službami. V mnoha případech, zvláště pokud lze zboží nebo služby dodat po Internetu, elektronické obchodování vedlo ke snížení nebo odstranění mnoha časových a vzdálenostních omezení.

12. Některá odvětví jsou pro elektronické obchodování vhodnější a elektronické obchodování v těchto odvětvích je rozvinutější. Pokud odvětví, ve kterém auditovaný subjekt podniká, je výrazně ovlivněno elektronickým obchodováním přes Internet, podnikatelská rizika, která mají vliv na účetní závěrku, mohou být větší. Mezi odvětví, která se pod vlivem elektronického obchodování mění, patří:

- počítačový software,
- obchodování s cennými papíry,
- bankovnictví,
- cestovní ruch,
- knihy a časopisy,
- hudební nahrávky;
- reklama,
- média
- vzdělávání.

Elektronické obchodování výrazně ovlivňuje i mnoho dalších odvětví ve všech oblastech podnikání.

Strategie auditovaného subjektu pro oblast elektronického obchodování

13. Strategie auditovaného subjektu pro oblast elektronického obchodování, včetně způsobu využití informačních technologií k elektronickému obchodování, a vlastní hodnocení přijatelné míry rizika, může mít vliv na bezpečnost účetních záznamů a úplnost a spolehlivost finančních informací. Mezi skutečnosti, které mohou být pro auditora při posuzování strategie pro oblast elektronického obchodování relevantní v kontextu porozumění kontrolnímu prostředí, patří:

- zapojení osob pověřených řízením do posouzení souladu činnosti v oblasti elektronického obchodování s celkovou podnikatelskou strategií auditovaného subjektu,

- zda elektronické obchodování podporuje novou činnost auditovaného subjektu či zda jeho cílem je zefektivnit stávající činnosti nebo pro ně získat nové trhy,

- zdroje příjmů auditovaného subjektu, změna jejich struktury (například zda auditovaný subjekt vystupuje jako samostatný subjekt nebo jako zprostředkovatel prodeje zboží či služeb),

- posouzení vedení, jak elektronické obchodování ovlivňuje příjmy auditovaného subjektu a jeho finanční potřeby,

- postoj vedení k riziku a jakým způsobem tento postoj ovlivňuje rizikový profil auditovaného subjektu,

- rozsah, v jakém vedení odhalilo příležitosti a rizika v oblasti elektronického obchodování v předložené strategii, která je podpořena odpovídajícími kontrolami, nebo zda se elektronické obchodování vyvíjí náhodně v reakci na příležitosti a rizika, která vyvstanou,

- závazek vedení ve vztahu k odpovídajícím kodexům nejlepší praxe nebo programům na zvýšení bezpečnosti webových stránek.

Rozsah činností auditovaného subjektu v oblasti elektronického obchodování

14. Rozlišné subjekty využívají elektronické obchodování různým způsobem. Elektronické obchodování lze využít například pro:

- poskytování informací o auditovaném subjektu a jeho činnostech, k nimž mají přístup třetí strany – investoři, zákazníci, dodavatelé, věřitelé a financující subjekty a zaměstnanci,
- usnadnění transakcí se stálými zákazníky tím, že se transakce uzavírají přes Internet,
- získání přístupu na nové trhy a k novým zákazníkům jako důsledek poskytování informací a zpracovávání transakcí přes Internet,
- přístup k poskytovatelům aplikačních služeb,
- vytvoření zcela nového podnikatelského modelu.

15. Rozsah využívání elektronického obchodování ovlivňuje charakter rizik, kterým musí auditovaný subjekt čelit. Bezpečnostní problémy se mohou objevit, pokud auditovaný subjekt má webovou stránku. I v případě, kdy třetí strany nemají interaktivní přístup, mohou informační stránky poskytovat přístup k finančním záznamům auditovaného subjektu. Bezpečnostní infrastruktura a související kontroly by u webové stránky, která je využívána pro transakce s obchodními partnery, nebo u vysoce integrovaných systémů, měly být rozsáhlejší (viz odstavce 32–34).

16. Jakmile auditovaný subjekt více využívá elektronické obchodování a jeho vnitřní systémy se stávají integrovanějšími a složitějšími, je pravděpodobnější, že nové způsoby uzavírání obchodů se budou lišit od tradičních forem obchodu a objeví se nová rizika.

Dohody auditovaného subjektu o využívání služeb externích dodavatelů/poskytovatelů (outsourcing)

17. Mnoho subjektů nedisponuje odborníky pro zřízení a provozování vnitropodnikových systémů, které jsou potřebné pro elektronické obchodování. Tyto subjekty jsou závislé na poskytovatelích internetových služeb, poskytovatelích aplikačních služeb a poskytovatelích datového prostoru/obsahu, kteří poskytují většinu nebo všechny služby v oblasti IT potřebné pro elektronické obchodování. Auditovaný subjekt může také využít služeb obslužné organizace pro další funkce související s činností v oblasti elektronického obchodování, například plnění objednávek, dodávku zboží, provoz zákaznických linek a některé účetní činnosti.

18. Jestliže auditovaný subjekt využívá služeb obslužné organizace, některá pravidla, postupy a záznamy vedené obslužnou organizací mohou být relevantní pro audit účetní závěrky auditovaného subjektu. Auditor posuzuje dohody o externích službách, které auditovaný subjekt využívá, aby zjistil, jak auditovaný subjekt reaguje na rizika, která vznikají při využívání služeb externích dodavatelů/poskytovatelů. ISA 402 „Zvažované skutečnosti týkající se subjektů využívajících služeb servisních organizací“ poskytuje vodítko pro posouzení vlivu obslužné organizace na kontrolní riziko.

Identifikace rizik

19. Vedení čelí celé řadě podnikatelských rizik, která souvisí s elektronickým obchodováním, včetně:

- ztráty integrity transakcí, kterou může doprovázet nedostatek odpovídajících auditorských podkladů v písemné nebo elektronické podobě,
- všudypřítomná bezpečnostní rizika související s elektronickým obchodováním, včetně virových útoků a možnosti podvodů ze strany zákazníků, zaměstnanců a jiného neoprávněného přístupu,
- nevhodná účetní pravidla například pro aktivaci výdajů, jakými jsou náklady na vývoj webové stránky, nepochopení složitých smluvních ujednání, rizika převodu vlastnických

práv, převody cizí měny, rezervy na záruční opravy a reklamace, otázky účtování výnosů, jako například:

- zda auditovaný subjekt je samostatnou jednotkou nebo zprostředkovatelem a zda se vykazuje hrubé tržby nebo pouze provize,
- zda je jiným subjektům poskytován reklamní prostor na webové stránce auditovaného subjektu a jakým způsobem se stanoví a vypořádají výnosy (například směnný obchod),
- řešení množstevních slev a zavádějících prodejů (například zboží v určité hodnotě zdarma),
- časové rozlišení tržeb (například zda jsou tržby uznávány až po dodání zboží a služeb),

- nesplnění daňových povinností a jiných právních a regulačních požadavků, především pokud je přes Internet elektronicky obchodováno se zahraničím,
- neošetření závaznosti smluv, které jsou evidovány pouze v elektronické podobě,
- přílišné spoléhání na elektronické obchodování při umístění důležitých obchodních systémů nebo jiných obchodních transakcí na Internetu,
- selhání a „pády“ systémů a infrastruktury.

20. Některým podnikatelským rizikům, která vznikají v souvislosti s elektronickým obchodováním, může auditovaný subjekt čelit zaváděním odpovídající bezpečnostní infrastruktury a souvisejících kontrol, které většinou zahrnují opatření na:

- ověření totožnosti zákazníků a dodavatelů,
- zajištění integrity transakcí,
- získání souhlasu s obchodními podmínkami, včetně podmínek dodání, úvěrových podmínek a postupů pro řešení sporů, které zajistí evidování transakcí a procesů tak, aby druhá strana nemohla odepřít svůj souhlas s dohodnutými podmínkami (uznání závazku);
- získání plateb nebo bezpečných úvěrových nástrojů od zákazníků
- vytvoření bezpečnostních protokolů a protokolů ochrany informací.

21. Auditor využívá získané znalosti podnikání k odhalení událostí, transakcí a postupů, které souvisí s podnikatelskými riziky elektronického obchodování auditovaného subjektu a které podle úsudku auditora mohou vyústit ve významné nesprávnosti v účetní závěrce nebo mohou mít výrazný vliv na auditorské postupy či výrok auditora.

Právní a regulační otázky

22. Doposud nebyl vytvořen všeobecný mezinárodní právní rámec elektronického obchodování ani účinná infrastruktura, která by jej podporovala (elektronický podpis, registry dokumentů, mechanismy řešení sporů, ochrana spotřebitele, atd.). Vnímání elektronického obchodování se v právních rámcích v různých právních řádech liší. Vedení ovšem musí zvážit právní a regulační otázky, které souvisí s elektronickým obchodováním, například zda auditovaný subjekt disponuje odpovídajícími nástroji pro vykázání daňové povinnosti, především daně z

příjmu a DPH v různých právních řádech. Mezi faktory, které vedou ke vzniku daňových povinností u elektronického obchodování, patří místo:

- právní registrace auditovaného subjektu,
- kde fyzicky provozuje činnost,
- kde je umístěna jeho webová stránka,
- odkud je dodáváno zboží a služby,
- kde se nacházejí jeho odběratelé nebo kam je dodáváno zboží a služby.

Tyto faktory se mohou v jednotlivých právních řádech lišit a může vzniknout riziko, že daně z transakcí mezi různými právními řády nebudou řádně vykázány.

23. Právní a regulační otázky, které se vztahují k elektronickému obchodování, zahrnují:

- dodržování národních a mezinárodních požadavků na důvěrnost informací,
- dodržování národních a mezinárodních požadavků pro regulovaná odvětví,
- vymahatelnost smluv,
- legálnost konkrétních činností, například hraní hazardních her přes Internet,
- riziko praní špinavých peněz,
- porušení práv duševního vlastnictví.

24. ISA 250 „Přihlížení k zákonům a nařízením při auditu účetní závěrky“, aby si auditor při plánování a provádění auditorských postupů a hodnocení a sestavování zpráv o jejich výsledcích uvědomil, že porušení zákonů a předpisů za strany auditovaného subjektu může mít významný vliv na účetní závěrku. ISA 250 dále vyžaduje, aby auditor před naplánováním auditu získal všeobecné povědomí o právním a regulačním rámci, který se vztahuje na auditovaný subjekt a odvětví, ve kterém podniká; a zjistil, zda auditovaný subjekt tento rámec dodržuje. Rámec může v konkrétních případech zahrnovat i určité právní a regulační otázky, které se týkají elektronického obchodování auditovaného subjektu. ISA 250 uznává, že cílem auditu není odhalit porušování zákonů a předpisů, auditor přesto musí provést postupy, které by odhalily případy porušování těch zákonů a předpisů, které se vztahují na sestavování účetní závěrky. Pokud vyvstane právní či regulační otázka, která podle úsudku auditora může vyústit ve významnou nesprávnost v účetní závěrce nebo výrazně ovlivnit auditorské postupy či zprávu auditora, auditor posoudí, způsob, jakým vedení tuto otázku řeší. V některých případech je při posuzování právních a regulačních otázek, které vzniknou při elektronickém obchodování auditovaného subjektu, nutné využít služeb právníka se znalostmi právních aspektů elektronického obchodování.

Posouzení vnitřní kontroly

25. Vnitřní kontroly mohou snížit rizika související s elektronický obchodováním. V souladu s ISA 400 „Vyhodnocení rizik a vnitřní kontrola“ auditor posuzuje kontrolní prostředí a kontrolní postupy, které auditovaný subjekt uplatnil u elektronického obchodování, a to v rozsahu, v jakém ovlivňují tvrzení účetní závěrky. Za určitých okolností, například pokud systém elektronického obchodování je vysoce automatizovaný, objem transakcí je veliký či

není uchovávána elektronická dokumentace včetně auditorských záznamů, může auditor stanovit, že není možné snížit auditorské riziko na přijatelně nízkou úroveň pouze použitím testů věcné správnosti. Za těchto okolností se často používají CAAT (viz IAPS 1009 „Softwarové techniky pro podporu auditu“).

26. Vedle zajištění bezpečnosti, integrity transakcí a nastavení procesů, jak je uvedeno dále, jsou pro elektronické obchodování auditované subjektu zvláště důležité tyto prvky vnitřní kontroly:
    - udržování integrity kontrolních postupů v rychle se měnícím prostředí elektronického obchodování,
    - zajištění přístupu k odpovídajícím záznamům pro potřeby auditovaného subjektu a pro účely auditu.

Bezpečnost

27. Bezpečnostní infrastruktura auditovaného subjektu a související kontroly jsou obzvlášť důležitým prvkem vnitřního kontrolního systému v případě, kdy třetí strany mají přístup do informačního systému auditovaného subjektu přes veřejnou síť, například Internet. Informace jsou zabezpečeny, pokud byly dodrženy požadavky na autorizaci, ověření, zachování důvěrnosti informací, integritu, nepopiratelnost a dostupnost.

28. Auditovaný subjekt obvykle čelí bezpečnostním rizikům, která souvisí se zaznamenáváním a zpracováním transakcí elektronického obchodování, pomocí bezpečnostní infrastruktury a souvisejících kontrol. Bezpečnostní infrastruktura a související kontroly mohou zahrnovat pravidla ochrany informací, hodnocení rizika ochrany informací a standardy, opatření, praxe a postupy, v rámci kterých jsou zaváděny a udržovány jednotlivé systémy, včetně fyzických opatření a logických a jiných technických pojistek, jako jsou identifikátory uživatelů, hesla a zabezpečení systému proti průniku zvenčí (tzv. firewall). Podle rozsahu, v jakém ovlivňují tvrzení účetní závěrky, posuzuje auditor také:

    - účinné využití zabezpečení systému proti průniku zvenčí a programů antivirové ochrany pro zabezpečení systémů před instalací nepovoleného nebo škodlivého softwaru, dat nebo jiných materiálů v elektronické formě,
    - účinné využití šifrování včetně:
        - zachování důvěrnosti a bezpečnosti přenosů například povolením dešifrovacích klíčů,
        - zamezení zneužití šifrovací technologie například pomocí kontroly a ochrany privátních dešifrovacích klíčů,
    - kontroly vývoje a zavádění podpůrných systémů pro elektronické obchodování,
    - zda existující bezpečnostní kontroly jsou dostatečně účinné i u nových technologií, které narušují bezpečnost Internetu,
    - zda kontrolní prostředí podporuje zavedené kontrolní postupy. Některé technicky vyspělé kontrolní postupy, jako například šifrovací systémy založené na digitálních certifikátech, nemusí být účinné, pokud fungují v neodpovídajícím kontrolním prostředí.

Integrita transakcí

29. Auditor posuzuje úplnost, přesnost, včasnost a autorizaci informací, které jsou zaznamenávány a zpracovány ve finančních záznamech auditovaného subjektu (integrita transakcí). Charakter a míra propracovanosti elektronického obchodování auditovaného subjektu ovlivňují charakter a rozsah rizik, která souvisí se zaznamenáváním a zpracováním transakcí elektronického obchodování.

30. Auditorské postupy týkající se integrity informací, které se vztahují k transakcím elektronického obchodování, v účetním systému, se zaměřují především na spolehlivost systémů, které zaznamenávají a zpracovávají tyto informace. V propracovanějších systémech spustí první krok, například přijetí objednávky zákazníka přes Internet, automaticky posloupnost ostatních kroků zpracování transakce. Na rozdíl od auditorských postupů používaných pro tradiční obchodní činnosti, které se většinou zaměřují odděleně na kontrolní procesy, které se vztahují na jednotlivé fáze zaznamenání a zpracování transakce, auditní postupy pro propracované elektronické obchodování se často zaměřují na automatické kontroly, které se týkají integrity transakcí při jejich zaznamenávání a následném automatickém zpracování.

31. V prostředí elektronického obchodování jsou kontroly integrity transakcí často navrhovány pro:
    - ověření vstupních dat,
    - zabránění duplikace nebo vynechání transakce,
    - zajištění, aby obchodní podmínky byly dohodnuty před zpracováním objednávky, včetně dodacích a úvěrových podmínek, tj. například vyžadovat, aby byla provedena platba při zadání objednávky,
    - rozlišení prohlížení stránky a objednávání zákazníkem, zajištění, aby druhá strana transakce nemohla později odepřít svůj souhlas s dohodnutými podmínkami (nepopiratelnost); a zajištění, že transakce probíhají pouze s oprávněnými stranami, pokud je to vhodné,
    - zamezení neúplnému zpracování tak, že se zajistí, aby byly všechny kroky provedeny a zaznamenány (například u obchodně odběratelské transakce: přijetí objednávky, přijetí platby, dodání zboží/služby a aktualizace účetního systému) nebo aby nebyly provedeny a zaznamenány a objednávka byla odmítnuta,
    - zajištění správné distribuce údajů o transakci všemi systémy sítě (například při centrálním sběru dat jsou data rozesílána jednotlivým manažerům, kteří transakci provedou),
    - zajištění, aby záznamy byly odpovídajícím způsobem uchovány, zálohovány a zabezpečeny.

Nastavení procesů

32. Nastavení procesů se týká způsobu, jakým jsou jednotlivé systémy informačních technologií navzájem integrované a jakým způsobem fungují jako jeden systém. V prostředí elektronického obchodování je důležité, aby transakce, které generuje webová stránka auditovaného subjektu, byly správně zpracovány vnitřními systémy auditovaného subjektu, tj. účetním systémem, systémy řízení dodavatelsko-odběratelských vztahů a systémy řízení zásob (tzv. „back office" systémy). Mnohé webové stránky nejsou automaticky integrovány s vnitřními systémy.

33. Způsob, jakým účetní systém auditovaného subjektu zaznamenává a zpracovává transakce elektronického obchodování, může ovlivnit:

- úplnost a přesnost zpracování transakcí a uchování informací,
- načasování uznání výnosů z tržeb, nákupů a jiných transakcí,
- odhalení a zaznamenání sporných transakcí.

34. Pokud je to významné pro tvrzení účetní závěrky, auditor posuzuje kontroly, které řídí integraci transakcí elektronického obchodování s vnitřními systémy, a kontroly změn systémů a převodu dat do automatických procesů.

Vliv elektronických záznamů na důkazní informace

35. O transakcích elektronického obchodování nemusí existovat žádné písemné záznamy a elektronické záznamy lze snadněji zničit či pozměnit bez zanechání stopy. Auditor posuzuje, zda pravidla ochrany informací a zavedené bezpečnostní kontroly jsou dostatečné, aby zamezily nepovoleným změnám účetního systému nebo záznamů a nebo systémů, které poskytují data pro účetní systém.

36. Auditor může při posuzování integrity elektronických záznamů prověřit automatické kontroly, jako například testy integrity záznamů, elektronická časová razítka, digitální podpisy a kontroly verzí. V závislosti na hodnocení těchto kontrol může auditor také posoudit, zda je nutné provést další postupy, například potvrzení podrobností transakcí nebo zůstatků účtů u třetích stran (viz ISA 505 „Externí konfirmace").

„Tento mezinárodní auditorský pokyn pro praxi IAPS 1013 „Vliv elektronického obchodování na účetní závěrku“ zveřejněný Radou pro auditorské a ujišťovací standardy (IAASB) Mezinárodní federace účetních (IFAC) v anglickém jazyce a publikovaný v příručce Handbook of International Auditing, Assurance, and Ethics Pronouncement 2005 Edition, byl přeložen do českého jazyka Komorou auditorů České republiky v červnu 2005 a je reprodukován se souhlasem organizace IFAC v červenci 2005. S postupem překladu mezinárodních auditorských a ujišťovacích standardů byla organizace IFAC seznámena a překlad byl proveden v souladu s „Oznámením zásad překladu standardů a návodů vydaných organizací IFAC.“ Schválený text všech mezinárodních auditorských a ujišťovacích standardů je ten, který organizace IFAC publikovala v anglickém jazyce.“