Matej Kostrec

Legislatíva, štandardy a normy platné pre oblasť auditu informačných systémov

Príspevok poskytuje prehľad platnej legislatívy z oblasti bezpečnostného auditu informačných systémov, prehľad noriem a štandardov, ktoré sú prijaté a odporúčané medzinárodnými inštitúciami zaoberajúcimi sa auditom v jeho podstate, ale aj auditom informačných systémov. Normy sú návodom pre audítorov, ako vykonávať audit, na čo sa zamerať, na čo nezabudnúť. Vznikli na základe najlepších osvedčených praktík používaných svetovými renomovanými audítorskými firmami.

1. Legislatíva upravujúca problematiku auditu informačných systémov

Problematika bezpečnostného auditu informačných systémov (IS) a najmä bezpečnosti dát v informačných systémoch je natoľko aktuálnou v súčasnom prostredí elektronizácie poskytovaných služieb, že je absolútnou nevyhnutnosťou, aby bola riešená aj na úrovni legislatívy. Uvedieme si najdôležitejšie zákony prijaté v SR, ktoré sa venujú bezpečnostnému auditu IS.

Zákon č. 428/2002 Z. z. o ochrane osobných údajov
Cieľom zákona je ochrana osobných údajov fyzických osôb pri ich spracúvaní v IS.

Znenie
§ 4 ods. 1 písm. o – ustanovuje, že pod auditom bezpečnosti IS sa rozumie nezávislé odborné posúdenie spoľahlivosti a celkovej bezpečnosti informačného systému z hľadiska zabezpečenia dôvernosti, integrity a dostupnosti spracúvaných osobných údajov.

§ 15 ods. 5 – ustanovuje, že audit bezpečnosti IS so zameraním na kontrolu bezpečnosti osobných údajov v IS môže vykonať iba externá, odborne spôsobilá právnická alebo fyzická osoba, ktorá sa nepodieľala na vypracovaní bezpečnostného projektu predmetného informačného systému, a nie sú pochybnosti o jej nezaujatosti.

§ 49 ods. 2 písm. b – ustanovuje, že ak prevádzkovateľ IS na žiadosť Úradu pre ochranu údajov nezabezpečil vykonanie auditu bezpečnosti informačného systému alebo zabezpečil vykonanie auditu bezpečnosti informačného systému v rozpore s týmto zákonom, alebo včas nepredložil hodnotiacu správu podľa § 15 ods. 4, 5, alebo predložil hodnotiacu správu, ktorá nekonkretizuje zistené nedostatky, môže mu Úrad pre ochranu údajov uložiť sankciu vo forme pokuty.

Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností
Cieľom zákona je ochrana utajovaných skutočností, práva a povinnosti právnických a fyzických osôb pri tejto ochrane.

Znenie
V prílohe 4 písmeno b – ustanovuje povinnosť podnikateľom predkladať ako súčasť bezpečnostného dotazníka podnikateľa aj audítorské správy vrátane správ z bezpečnostného auditu IS.

Zákon č. 215/2002 Z. z. o elektronickom podpise

Cieľom zákona je úprava vzťahov vznikajúcich v súvislosti s vyhotovovaním a používaním elektronického podpisu, práva a povinnosti fyzických a právnických osôb pri používaní elektronického podpisu, hodnovernosť a ochrana elektronických dokumentov podpísaných elektronickým podpisom.

Znenie
§ 13 ods. 3 písm. e – ustanovuje žiadateľovi o akreditáciu povinnosť predložiť Národnému bezpečnostnému úradu výsledok bezpečnostného auditu jeho činnosti.

§ 25 – tento paragraf je celý venovaný ustanoveniam o bezpečnostnom audite IS.
Ods. 1 – ustanovuje povinnosť každej akreditovanej certifikačnej autorite opakované podrobovanie sa externému bezpečnostnému auditu každoročne.
Ods. 2 – ukladá povinnosť každej akreditovanej certifikačnej autorite predložiť záverečnú správu o výsledkoch auditu Národnému bezpečnostnému úradu spolu s prípadnými opatreniami na nápravu a s lehotami, v ktorých sa zistené nedostatky odstránia, a to do 30 dní od ukončenia auditu.
Ods. 3 – ustanovuje právo i povinnosť Národnému bezpečnostnému úradu uložiť každej akreditovanej certifikačnej autorite opatrenia na nápravu a lehotu, v ktorej je povinná nedostatky odstrániť, ak zo záverečnej správy o výsledkoch auditu zistí, že akreditovaná certifikačná autorita porušila povinnosti ustanovené v tomto zákone.

§ 26a ods. 1 písm. i – ukladá Národnému bezpečnostnému úradu možnosť sankcionovať, a to aj opakovane akreditovanú certifikačnú autoritu, ktorá nesplní povinnosť podrobiť sa auditu podľa § 25 ods. 1 alebo nepredloží záverečnú správu o výsledku auditu v lehote podľa § 25 ods. 2 vo forme uloženia pokuty.

Zákon č. 610/2003 Z. z. o elektronických komunikáciách
Cieľom zákona je úprava podmienok na poskytovanie elektronických komunikačných sietí a elektronických komunikačných služieb, podmienok na používanie rádiových zariadení, štátnu reguláciu elektronických komunikácií, práv a povinností podnikov a používateľov elektronických komunikačných sietí a elektronických komunikačných služieb, úprava podmienok na ochranu týchto sietí a služieb, na efektívne využívanie frekvenčného spektra a čísel, na ochranu súkromia a údajov a pôsobnosť orgánov štátnej správy v elektronických komunikáciách.

Znenie
§ 46 ods. 4 – ukladá každému podniku poskytujúcemu verejnú sieť alebo verejnú službu, ktorý nie je podľa zákona povinný vykonávať nezávislý audit, povinnosť poskytnúť na nahliadnutie svoju účtovnú závierku Telekomunikačnému úradu Slovenskej republiky na základe jeho požiadania.

Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy
Cieľom zákona je okrem práv a povinností subjektov verejnej správy, ktoré zabezpečujú prevádzku informačných systémov verejnej správy, úprava základných podmienok na zabezpečenie integrovateľnosti a bezpečnosti informačných systémov verejnej správy.

Znenie
Informačné systémy verejnej správy si vzhľadom na charakter údajov, ktoré spracúvajú, a povinnosti spojené s ich poskytovaním, vyžadujú zvýšený dôraz na riešenie ich bezpečnosti. Požiadavky na bezpečnosť a bezpečnostný audit sú však v tomto zákone riešené len rámcovo

a všeobecne. Informačná bezpečnosť je zákonom upravená formou odvolávania sa na štandardy vydávané výnosmi príslušných ministerstiev, ktoré zabezpečujú aj kontrolu a audit dodržiavania výnosov.

Zákon č. 618/2003 Z. z. o autorskom práve a právach súvisiacich s autorským právom
Cieľom zákona je úprava vzťahov vznikajúcich v súvislosti s vytvorením a použitím vedeckého diela – informačných systémov, počítačových programov a prác spojených s ich tvorbou, s výrobou a použitím zvukového záznamu, zvukovoobrazového záznamu a v súvislosti so zhotovením a použitím databázy tak, aby boli chránené práva a oprávnené záujmy autora IS, jeho prvkov a zhotoviteľa databázy.

Znenie
§ 81 ods. 1 písm. o – ustanovuje povinnosť pre organizáciu kolektívnej správy, ktorej autor udelil oprávnenie na výkon kolektívnej správy práva na odmenu za ďalší predaj originálu diela, vyhotoviť každoročne do 30. júna výročnú správu o činnosti a hospodárení za predchádzajúci kalendárny rok, ktorá obsahuje aj účtovnú závierku overenú audítorom.

Zákon č. 483/2001 Z. z. o bankách
Cieľom zákona je legislatívna úprava vzťahov súvisiacich so vznikom, organizáciou, riadením, podnikaním a so zánikom bánk so sídlom na území Slovenskej republiky a úprava vzťahov na účel regulácie a kontroly bánk s cieľom bezpečného fungovania bankového systému.

Znenie
§ 6 ods. 12 – ustanovuje, že pri výkone bankového dohľadu nad jednotlivými bankami a pobočkami zahraničných bánk a bankového dohľadu na konsolidovanom základe, Národná banka Slovenska spolupracuje s orgánmi bankového dohľadu nad bankami a orgánmi, dohľadu nad finančnými inštitúciami a poisťovňami iného štátu, so Slovenskou komorou audítorov a s audítormi a má právo vymieňať si s nimi informácie a upozorniť ich na nedostatky zistené pri vykonávaní bankového dohľadu.

§ 6 ods. 13 – vymedzuje poskytovanie informácií podľa odseku 12 len na účely výkonu bankového dohľadu, dohľadu, auditu a na účely kontroly audítorov.
§ 7 ods. 4 písm. b – ukladá povinnosť každej banke pred začatím vykonávania povolených bankových činností preukázať Národnej banke Slovenska technickú, organizačnú a personálnu pripravenosť na výkon povolených bankových činností banky, existenciu riadiaceho a kontrolného systému banky, vrátane útvaru vnútornej kontroly a vnútorného auditu a systému riadenia rizík.

§ 23 ods. 2 – upravuje povinnosti útvaru vnútornej kontroly a vnútorného auditu. Obdobne § 25 ods. 4 – 6 upravujú práva a povinnosti vedúceho vnútorného auditu.

§§ 40, 47 a 48 – ukladajú bankám povinnosti voči Národnej banke Slovenska v oblasti auditu, ako aj povinnosti pre externé audítorské subjekty zabezpečujúce audítorské aktivity v bankách.

§§ 50, 51 a 54 – ustanovujú práva a povinnosti Národnej banky Slovenska voči bankám v oblasti auditu.

2. Štandardy a normy platné pre oblasť auditu informačných systémov

Špeciálny charakter auditu informačných systémov (IS) a požadovaných vedomostí a zručností na vykonávanie takéhoto druhu auditu si vyžadujú uplatňovanie špecifických noriem prispôsobených tejto disciplíne. Jedným z cieľov Združenia pre audit informačných systémov a kontrol (ISACA – Information Systems Audit and Control Association) bolo navrhnúť a aktualizovať celosvetovo aplikovateľné štandardy a normy pre túto oblasť. Združenie zostavilo a vydalo súbor noriem pre audit IS, ktorých cieľom je poskytnúť spoločenstvu audítorov základný rámec výkonu ich povolania.

Štruktúra štandardov určených pre audit IS poskytuje viaceré úrovne podpory:

- ***Normy*** stanovujú povinné požiadavky v oblasti auditu IS a reportingu. Informujú:
  - audítorov IS o minimálnej úrovni výkonov potrebných na plnenie úloh stanovených v kódexe profesionálnej etiky,
  - manažérov podniku a ostatné zainteresované strany o činnostiach audítorov v predmetnej oblasti, ktoré môžu očakávať,
  - držiteľov certifikátu CISA (Certified Information Systems Audítor – Certifikovaný audítor informačných systémov) o požiadavkách, ktoré sú kladené na ich výkon.
- ***Smernice*** prinášajú usmernenia a pokyny o aplikovaní noriem vydaných v oblasti auditu IS. Audítor IS sa musí na ne odkazovať pri uplatňovaní noriem, vyjadriť svoj profesionálny úsudok o ich znení pred ich použitím a zdôvodniť každú odchýlku voči týmto smerniciam použitú v praxi.
- ***Procedúry (postupy)*** prinášajú príklady metód, ktoré audítor IS môže aplikovať počas výkonu auditu. Znenie procedúr obsahuje informácie o postupoch, ktoré je potrebné vykonať na aplikovanie noriem auditu IS, avšak nestanovuje povinnosť aplikovania týchto postupov. Cieľom procedúr je poskytnúť čo najväčší počet informácií tak, aby všetky postupy boli v súlade s aplikovanými normami.
- ***Kontroly COBITU*** predstavujú model osvedčených postupov. Pretože manažéri podnikov a spoločností zodpovedajú za ochranu všetkých firemných aktív, mali by si na uplatnenie tejto svojej zodpovednosti stanoviť vhodný vnútorný kontrolný systém. Cobit poskytuje podrobnú sadu kontrol a kontrolných techník riadenia prostredia informačných systémov. V Cobite je výber najvhodnejších prvkov pre konkrétny audit založený na výbere konkrétnych IT procesov a aplikovaní príslušných kontrolných metód a kritérií na vybrané procesy. Štruktúra Cobitu je organizovaná podľa procesov riadenia IT a jeho model je určený nielen riadiacim pracovníkom, ale najmä audítorom IS. Jeho používanie umožňuje poznať a pochopiť ciele podniku, sprostredkúvať osvedčené postupy a vydať odporúčania, ktoré sú dané všeobecne rešpektovanými štandardmi a normami.

  Cobit obsahuje:

  - ✓ **Ciele kontroly** – stanovenie predmetu, cieľov a úrovne kontroly pre audit IS
  - ✓ **Kontrolné praktiky** – praktické usmernenia a postupy realizácie cieľov auditu
  - ✓ **Smernice na vykonávanie auditu** – inštrukcie pre každú oblasť kontroly, na posúdenie kontrolovaných prvkov, ich porovnávanie so štandardmi a na stanovenie miery rizika pri neuspokojivých kontrolách
  - ✓ **Usmernenia pre riadenie spoločnosti** – inštrukcie a návody, ako hodnotiť a zlepšovať výkonnosť IS procesov pomocou metrológie, modelov a kritických faktorov pre dosiahnutie úspechu riadenia týchto procesov. Usmernenia sú

orientované na samohodnotenie priebežných auditov a kontrol so zameraním na:

- *meranie výkonnosti* – Do akej miery IT spĺňa potreby spoločnosti?
- *definovanie profilu kontrol IS* – Ktoré procesy IT sú najvýznamnejšie pre spoločnosť? Aké sú základné faktory kontroly pre dosiahnutie úspechu spoločnosti?
- *súdnosť* – Aké sú riziká, že ciele nebudú dosiahnuté?
- *benchmarking (porovnanie s konkurenciou)* – Čo robia konkurenti? Ako merať a porovnávať výsledky?

2.1 Normy auditu IS

Normy auditu IS poskytujú jasné a prehľadné metódy na ohodnotenie podnikateľských rizík súvisiacich s IT. Sú podporou pre manažérov pri riadení rizík a rozhodovaní o efektívnejšom využívaní zdrojov IS. Súčasne sú vrcholným manuálom pre každého audítora IS, ktorý mu poskytuje základný rámec aktivít spojených s auditom informačných systémov.

Norma S1 – Charta auditu (Písomné vyhlásenie auditu)

Cieľom tejto normy auditu IS je stanovenie a vydanie pokynov o dodržiavaní náležitostí Charty auditu počas výkonu auditu.

Znenie normy

- Predmet a ciele auditu IS, zodpovednosť, právomoci a povinnosti zúčastnených strán musia byť náležite zdokumentované v charte auditu alebo v poverovacom liste.
- Charta auditu alebo poverovací list musia byť schválené na príslušnej kompetentnej úrovni podniku alebo spoločnosti.

Komentár

- Ak ide o vyhlásenie realizácie interného auditu IS, musí byť predmet charty auditu zameraný na aktivity vykonávané v podniku. Vykonávanie takéhoto druhu auditu by sa malo vykonávať raz ročne alebo častejšie, ak sú zodpovednosti za IS zdieľané alebo prišlo k ich zmene. Interný audítor IS môže prostredníctvom poverovacieho listu dostať presné kompetencie a predmet auditu vopred alebo potvrdiť výsledky zistení následne po realizácii špecifických auditov alebo kontrol.
- Ak ide o vyhlásenie realizácie externého auditu IS, musí byť poverovací list vydaný a schválený pre každý audit alebo kontrolu vopred.
- Charta auditu alebo poverovací list musia byť dostatočne detailné, aby bol v nich jasne stanovený predmet, zodpovednosti a ciele auditu.
- Charta auditu alebo poverovací list musia byť pravidelne revidované, aby bolo zabezpečené, že predmet a zodpovednosti sú správne zdokumentované.

Norma S2 - Nezávislosť

Cieľom tejto normy auditu IS je stanovenie a vydanie pokynov a návodov o nezávislosti audítorov počas vykonávania auditu.

Znenie

- Profesionálna nezávislosť
  Audítor IS musí byť vo všetkých aspektoch auditu nezávislý od kontrolovaného subjektu – tak v oblasti postojov, ako aj používaných metodík.
- Organizačná nezávislosť
  Audítor IS musí byť nezávislý od organizačnej zložky a aktivít, ktoré kontroluje, aby dosiahol cieľ stanovený v predmete auditu.

Komentár

- Charta auditu alebo poverovací list musia obsahovať klauzulu o nezávislosti audítora a jeho zodpovednosti počas vykonávania auditu.
- Vo všetkých prípadoch a za každých okolností musí audítor IS preukázať svoju nezávislosť tak v postojoch, ako aj metodikách.
- Ak nie je dodržaná nezávislosť, či už v postoji, alebo metodike, musia byť tieto náležitosti oznámené príslušným stranám.
- Audítor IS musí byť štatutárne nezávislý od kontrolovaného útvaru.
- Nezávislosť musí byť pravidelne vyhodnocovaná audítorom IS, ako aj riadiacimi pracovníkmi, prípadne auditným výborom, ak existuje.
- Ak to nie je zakázané inými odbornými normami alebo regulačnými úradmi, audítor IS nemusí byť nezávislý, vrátane výberu metód, v prípade, že povaha jeho odbornosti v oblasti IS nespadá do predmetu konkrétneho auditu.

Norma S3 – Etika a profesionálnosť

Cieľom tejto normy auditu IS je stanovenie a vydanie pokynov a návodov určených audítorom IS, aby dodržiavali Kódex profesionálnej etiky audítora IS vydaný ISACA, a vykonávali svoje povolanie s využitím všetkých získaných odborných vedomostí a zručností.

Znenie

- Audítor IS musí dodržiavať Kódex profesionálnej etiky audítora IS vydaný ISACA.
- Audítor IS musí vykonávať svoje povolanie s využitím všetkých získaných odborných vedomostí a zručností a musí rešpektovať všetky odborné normy platné v oblasti auditu.

Komentár

- Kódex profesionálnej etiky audítora IS vydaný ISACA je pravidelne aktualizovaný, aby bol v súlade s vývojom nových trendov a požiadaviek na profesiu audítora. Audítori IS musia držať krok s novými trendmi Kódexu profesionálnej etiky a dodržiavať ho pri plnení záväzkov vyplývajúcich z roly audítora IS.
- Normy auditu IS vydávané ISACA sú pravidelne aktualizované, aby bolo zabezpečené nepretržité upresňovanie ich znenia, a upravované, ak je to potrebné na vyrovnanie sa s problémami, ktorým čelia audítori pri výkone ich povolania. Audítori IS musia poznať posledné verzie platných noriem a vykonávať svoje povolanie s využitím všetkých získaných odborných vedomostí a zručností.
- Akékoľvek porušenie Kódexu profesionálnej etiky alebo noriem auditu môže viesť k prešetreniu správania sa audítora a k začatiu disciplinárneho konania.

- Audítori IS musia byť v kontakte s členmi ich audítorského tímu, bdieť nad ich dodržiavaním Kódexu profesionálnej etiky a rešpektovaním platných noriem počas vykonávania auditu IS.
- Audítori IS musia adekvátnym spôsobom riešiť všetky problémy spojené s dodržiavaním profesionálnej etiky alebo noriem auditu IS počas výkonu auditu. Ak nie je dodržaná profesionálna etika alebo normy auditu, musí audítor požiadať o okamžité ukončenie auditu.
- Audítor IS musí zachovávať bezchybný postoj a bezúhonnosť a nesmie používať metódy, ktoré by mohli byť interpretované ako nelegálne, v rozpore s etikou alebo považované za neprofesionálne na splnenie cieľov auditu.

Norma S4 – Odborné vedomosti a zručnosti

Cieľom tejto normy auditu IS je stanovenie a vydanie pokynov na účely nevyhnutnej potreby získavania a udržiavania si vedomostí a zručností u audítorov.

Znenie normy

- Audítor IS musí byť odborne zdatný, t. j. mať potrebné vedomosti a zručnosti pre úspešné vykonanie cieľov auditu.
- Audítor IS si musí udržiavať a zvyšovať úroveň týchto odborných vedomostí a zručností formou účasti na programoch ďalšieho odborného vzdelávania.

Komentár

- Audítor IS musí preukázať dostatočnú odbornú spôsobilosť (schopnosti, znalosti, skúsenosti súvisiace s plnením úloh príslušného auditu) ešte pred začiatkom auditu. V opačnom prípade, t. j. ak nespĺňa odbornú spôsobilosť, musí audítor IS odmietnuť poverenie alebo odstúpiť z realizácie príslušného auditu.
- Ak má audítor potrebnú odbornú spôsobilosť, musí tiež spĺňať požiadavky na odbornú prípravu a ďalší odborný rozvoj.
- Audítor IS by mal chápať podstatu kontrolovanej činnosti. Rozsah požadovaných vedomostí by mal byť daný povahou podniku, jeho prostredím, rizikami a cieľmi auditu.
- Ak audítor IS vedie pracovný tím poverený výkonom auditu, musí preukázať, že všetci členovia tímu majú dostatočnú úroveň odbornej spôsobilosti na plnenie úloh auditu.

Norma S5 - Plánovanie

Cieľom tejto normy auditu IS je stanoviť príslušné normy a vydať pokyny na plánovanie auditov.

Znenie normy

- Audítor IS musí plánovať rozsah auditov IS, aby splnil ich ciele a zabezpečil súlad so všetkými relevantnými platnými zákonmi a odbornými normami.
- Audítor IS musí vypracovať a zdokumentovať aj návrh plánu auditu založený na rizikových oblastiach, ktoré bude potrebné auditovať ad-hoc.

- Audítor IS musí vypracovať a zdokumentovať plán, ktorý popíše charakter, ciele, trvanie, rozsah auditu a potrebné zdroje.
- Audítor IS musí tiež vypracovať program auditu a procedúry, ktoré budú aplikované.

Komentár

- V prípade plánovania interných auditov musí byť plán auditov IS vypracovaný alebo aktualizovaný minimálne raz ročne. Tento plán by mal slúžiť ako rámec kontrolnej činnosti auditovaných aktivít a mal by stanoviť zodpovednosti, ktoré budú definované v charte každého auditu. Nový plán alebo jeho aktualizovaná verzia musia byť schválené auditným výborom, ak existuje.
- V prípade plánovania externých auditov IS by mal byť pripravený plán, ktorý musí obsahovať ciele jednotlivých auditov.
- Audítor IS musí už vo fáze plánovania zabezpečiť, aby počas výkonu auditu boli všetky dokumenty a auditované prvky náležitým spôsobom uzavreté proti zmenám. Stratégia auditu, prahy tolerancie a zdroje môžu byť počas auditu menené.
- Plán auditu si môže vyžiadať úpravu počas vykonávania auditu s cieľom riešiť problémy (nové riziká, nesprávne predpoklady alebo závery už vykonaných procedúr), ktoré môžu vzniknúť počas auditu.

Norma S6 – Realizácia auditu

Cieľom tejto normy auditu IS je stanoviť príslušné normy a vydať pokyny na aktivity spojené s vykonávaním auditu.

Znenie normy

- Monitorovanie a dohľad – Práca audítorov IS musí byť monitorovaná, aby bolo jasne potvrdené, že ciele auditu boli dosiahnuté a platné odborné normy boli rešpektované.
- Dôkazné prvky – Počas auditu musí audítor IS zozbierať relevantné dôkazy, spoľahlivé a dostatočné na splnenie cieľov auditu. Závery auditu musia byť podložené primeranou analýzou a vysvetlením založeným na dôkazných prvkoch.
- Dokumentácia – Proces vykonania auditu musí byť zdokumentovaný formou popisu činností audítora a dôkazných prvkov podporujúcich závery a zistenia audítora IS.

Komentár

- Úlohy a zodpovednosti audítorského tímu musia byť stanovené na začiatku auditu, pričom musia byť definované minimálne rozhodovacie, výkonné a revízne roly.
- Práca vykonávaná počas auditu musí byť organizovaná a zdokumentovaná podľa vopred definovaných postupov. Dokumentácia by mala obsahovať prvky, ako sú ciele a rozsah auditu, jeho program, zrealizované etapy a kroky, zhromaždené dôkazy, zistenia a odporúčania.
- Dokumentácia o audite by mala byť dostatočne jasná a obšírna, aby nezávislá tretia osoba mohla opätovne vykonať všetky úlohy zrealizované počas auditu a dospieť k tým istým zisteniam.
- Dokumentácia o audite by mala obsahovať informácie o identite a úlohách osôb, ktoré vykonali jednotlivé úlohy auditu. Vo všeobecnosti by každá úloha, každé rozhodnutie, etapa alebo zistenie auditu zrealizované jedným alebo viacerými členmi tímu mali byť preskúmané iným členom tímu, menovaným v závislosti od dôležitosti auditovaného prvku.

- Audítor IS by mal plánovať využitie dostupných dôkazov v súlade s cieľmi auditu, s plynúcim časom a kapacitami tak, aby boli k dispozícii v najvhodnejšom okamihu na príslušné aktivity.
- Dôkazy použité pri audite musia byť postačujúce, spoľahlivé a relevantné, aby potvrdili stanovisko alebo zistenia audítora IS. Ak podľa audítora získané dôkazy nespĺňajú tieto kritériá, musí získať ďalšie potrebné dôkazy.

Norma S7 – Správa o audite

Cieľom tejto normy auditu IS je stanoviť príslušné normy a vydať pokyny na zostavenie správy, ktorú o vykonaní auditu audítor IS musí vypracovať.

Znenie normy

- Výsledkom práce audítora IS musí byť záverečná správa o vykonaní auditu, ktorá musí mať náležitú formu. Správa musí obsahovať údaje o podniku, príjemcoch dokumentu a prípadné obmedzenia jeho distribúcie.
- Správa musí obsahovať údaje o predmete, cieľoch, čase, povahe, trvaní a rozsahu vykonaného auditu.
- Správa musí obsahovať závery, zistenia a odporúčania auditu, ako aj prípadné obmedzenia, rezervy alebo návrhy, ktoré audítor považuje za vhodné uviesť do záverečnej správy.
- Audítor IS musí doložiť k správe dostatočné a náležité dôkazy, ktoré potvrdzujú vykazované výsledky.
- Pri odovzdávaní správy musí byť správa podpísaná audítorom IS, opatrená dátumom a distribuovaná podľa ustanovení daných v charte o audite alebo poverovacom liste.

Komentár

- Forma a obsah správy sa vo všeobecnosti menia v závislosti od typu auditovanej organizačnej zložky alebo cieľov. Audítor IS môže vykonávať jednu z nasledujúcich operácií:
  - Audit (priamy alebo audit dokumentov)
  - Kontrola (priama alebo kontrola dokumentov)
  - Dohodnuté postupy.
- Ak musí audítor IS podať stanovisko k celkovej kontrole v súlade so znením cieľov auditu a ak dôkazy naznačujú nedostatočnosť niektorých informácií, nesmie audítor IS vydať záver, že kontroly sú postačujúce a účinné. Správa audítora musí uvádzať a popísať aj dôkazy, ktoré nevykazujú dostatočné náležitosti na použitie kontrolných kritérií.
- Audítor IS musí predložiť príslušným riadiacim pracovníkom návrh svojej správy a prediskutovať s nimi jej obsah pred jej finalizáciou a distribúciou.
- Ak audítor IS zistí závažné nedostatky v kontrolovanej oblasti, musí o tom informovať auditný výbor alebo zodpovedných riadiacich pracovníkov a uviesť v správe, že boli odhalené takéto závažné nedostatky.
- Ak audítor IS zostaví viaceré správy, tak finálna správa musí obsahovať referenčné odvolávky na všetky tieto správy.
- Audítor SI by mal zvážiť, či bude informovať riadiacich pracovníkov o nedostatkoch, ktoré interná kontrola považuje za menej závažné. Audítor môže prípadne oznámiť

auditnému výboru alebo zodpovednému pracovníkovi, že takého menej závažné nedostatky už boli komunikované s riadiacim pracovníkom.
- Audítor IS je povinný vyžiadať si a preskúmať vyjadrenia k zisteniam a odporúčaniam z predchádzajúcich auditov, aby zistil, či boli včas prijaté a zrealizované nápravné opatrenia.

Norma S8 – Činnosti po skončení auditu

Cieľom tejto normy auditu IS je stanoviť príslušné normy a vydať pokyny na činnosti po skončení auditu IS a kontrolu nápravných opatrení na zistenia auditu.

Znenie normy
- Po zostavení a vydaní správy o zisteniach a odporúčaniach auditu je audítor IS povinný vyžiadať si príslušné informácie a analyzovať ich tak, aby mohol vyhodnotiť, či boli v stanovených termínoch prijaté riadiacimi pracovníkmi príslušné nápravné opatrenia.

Komentár
- Ak boli opatrenia navrhované riadiacimi pracovníkmi pre implementovanie odporúčaní komunikované alebo prediskutované s audítorom IS, musia byť vo finálnej správe o audite zaznamenané ako odpovede a vyjadrenia riadiacich pracovníkov k predmetným zisteniam.
- Povaha, dĺžka trvania a rozsah monitorovania auditovaných činností musia zohľadňovať závažnosť zistení a dôsledky neprijatia nápravných opatrení. Čas monitorovania auditovaných činností závisí od odborného posúdenia viacerých hľadísk zo strany audítora, a to najmä povahy, rozsahu alebo závažnosti zistených rizík a od nákladov s tým spojených.
- Monitorovací proces musí byť stanovený audítorom IS, aby bolo overené, že opatrenia prijaté riadiacimi pracovníkmi boli skutočne aplikované do praxe, resp. že títo akceptovali riziko a prevzali na seba zodpovednosť za jeho neriešenie. Zodpovednosť za monitorovací proces môže byť stanovená už v charte o audite alebo poverovacom liste.
- V závislosti od rozsahu a cieľov auditu môžu externí audítori IS zveriť internému auditu monitorovanie plnenia dohodnutých odporúčaní.
- Ak riadiaci pracovníci poskytnú informácie o opatreniach prijatých na implementáciu odporúčaní a audítor IS má pochybnosti o kvalite týchto informácií, je potrebné pristúpiť k procedúram overovania skutočnosti pred uzavretím aktivít monitorovania.
- Správa o stave monitorovacích aktivít, najmä o schválených, ale neimplementovaných odporúčaniach, by mala byť predložená auditnému výboru (ak existuje) alebo príslušnej vyššej riadiacej úrovni spoločnosti.
- Audítor IS by mal ako súčasť monitorovacích aktivít určiť, či sú jeho zistenia naďalej platné a do akej miery, ak boli nedostatočne uplatnené nápravné opatrenia.

2.2 Smernice auditu IS

Smernice na vykonávanie auditu a usmernenia riadenia spoločnosti uvádzajú príklady metrologických ukazovateľov posúdenia výkonnosti IS v spoločnosti. Na základe kritických referenčných ukazovateľov je možné merať a vyhodnotiť výsledky IT procesov a posúdiť ich efektívnosť s vyčíslením pozitívnych prvkov. Prezentované modely poskytujú možnosť

posúdenia kapacít a porovnávania sa s konkurenciou. Pomáhajú manažérom posúdiť zistenia a výsledky kontroly a auditu IS, ale aj identifikovať potreby overovania, prijímania nápravných opatrení a stanovenia stratégie auditov IS na budúce obdobia. Tieto smernice nie je možné považovať za vyčerpávajúce a (samozrejme) môžu existovať iné podobné procedúry a kontroly, ktoré by mohli viesť k podobným výsledkom. Neexistuje ani žiadna garancia, že použitie týchto smerníc je zabezpečením dosiahnutia výsledku. Pri stanovovaní postupov auditu IS sa musí každý audítor spoľahnúť na svoj vlastný profesionálny úsudok, a to v závislosti od okolností, auditovaných systémov a technologického prostredia.

npor. JUDr. Matej Kostrec
Akadémia Policajného zboru Bratislava
Katedra manažmentu a informatiky
tel.: 0961057464
e-mail: matej.kostrec@minv.sk