Fakulteta za elektrotehniko, računalništvo in informatiko

Revidiranje informacijskih sistemov

ITK 3 UN IS, ITK 3 UN TK

Predavanje 4 od 14

Maribor, 7. november 2014

Vsebina tretjega predavanja

- Odprte zadeve predhodnega predavanja
- Kratka ponovitev vsebine predhodnega predavanja
- Dogovor o nadomeščanju
- Revizijska dokumentacija (nadaljevanje)
- Faze revizije
- Revizijska dokazila (začetek)
- Za razmislek
- Zaključek / povzetek

Odprte zadeve predhodnega predavanja

- Vprašanj ni bilo

Kratka ponovitev vsebine predhodnega predavanja

- Revizija informacijskih sistemov - organizacije
- Smisel revizije
- Revizijska dokumentacija
- Za razmislek

Kratka ponovitev vsebine predhodnega predavanja

Revizija informacijskih sistemov - organizacije

- V Sloveniji
  - Slovenski inštitut za revizijo
  - Agencija za javni nadzor nad revidiranjem
  - Računsko sodišče Republike Slovenije
- V tujini
  - ISACA (*Information System Audit and Control Association*)
  - IT Governance institute
- Slovenski odsek ISACA

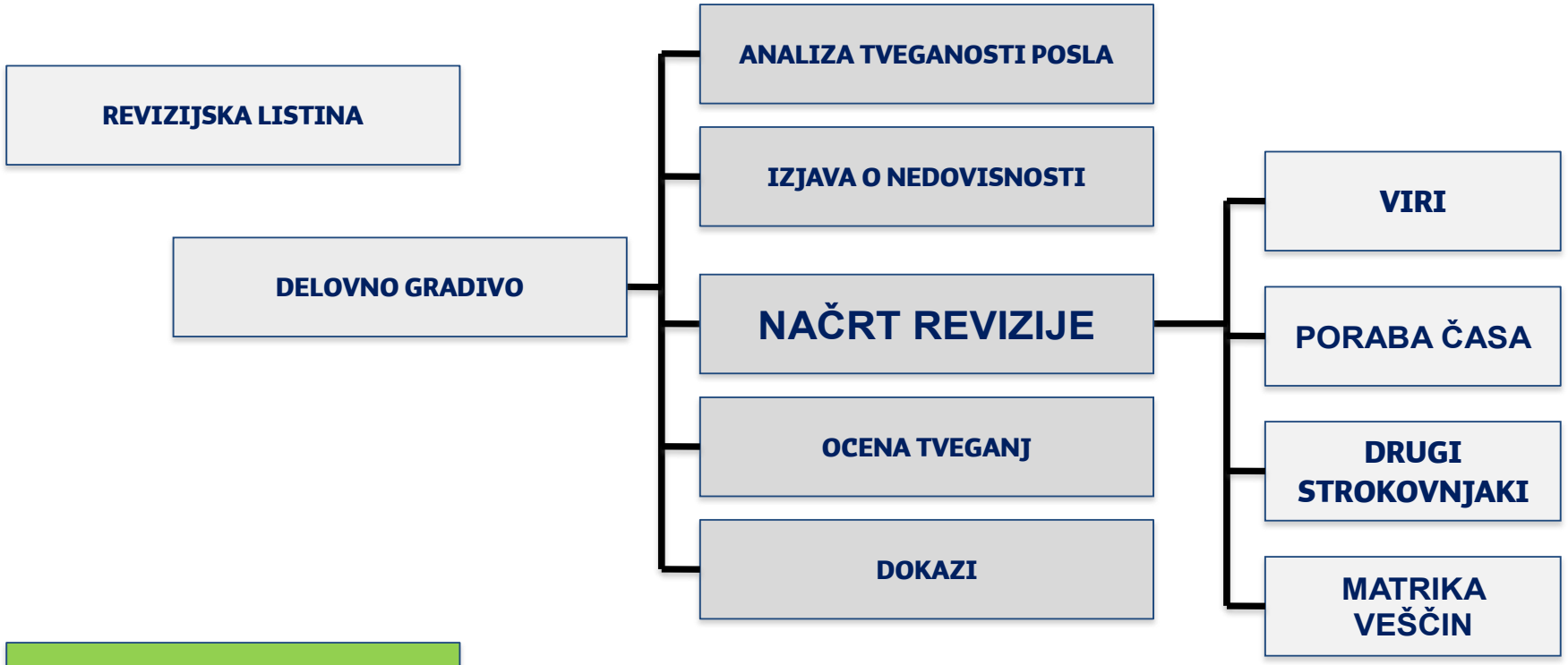
Kratka ponovitev vsebine predhodnega predavanja

Smisel revizije

- Kdo je zainteresiran za revizijo IS?
- Odvisnost podjetij od IKT

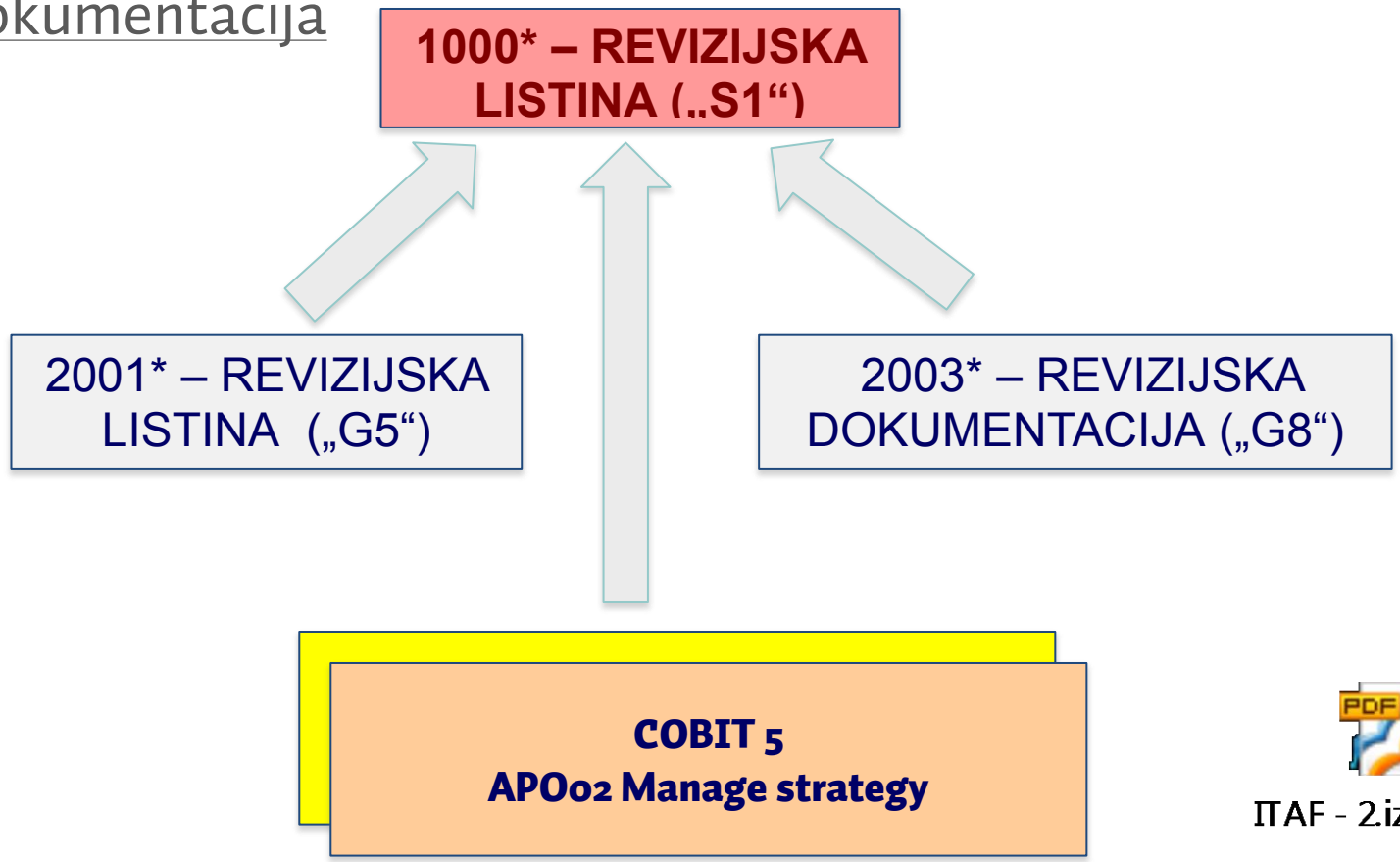
Kratka ponovitev vsebine predhodnega predavanja

Revizijska dokumentacija



Kratka ponovitev vsebine predhodnega predavanja

Revizijska dokumentacija



ITAF - 2.izd (SLO)

Kratka ponovitev vsebine predhodnega predavanja

Za razmislek

- www strani organizacij
- ITAF – 1001

Kratka ponovitev vsebine predhodnega predavanja

- Ali so kakšna vprašanja vezana na predhodno predavanje?
- Ali so kakšne nejasnosti?
- Ali ste uspeli na UM Moodle predmeta Revidiranje IS (9371):
  - Pregledati / prenesti tretje predavanje?
  - Pregledati / prenesti četrto – to predavanje?

Dogovor o nadomeščanju

- Predavanja so 24.10.2014 odpadla zaradi zdravstvenih težav predavatelja

- Predavanje moramo nadomestiti. Možnosti so:
  - izpeljati predavanja kakšen drug dan /morda sreda popoldan v prvi polovici decembra
  - v decembru (5.12., 12.12. in 19.12.) predavanja med 13.15 in 16.40 – 4 šolske ure
  - drugo

Revizijska dokumentacija - nadaljevanje

- Vrste storitev
- Postopek revizije
- Preliminarna raziskava

Revizijska dokumentacija – Vrste poslov za področje IKT

Vrste storitev:

- Revizija - visoka raven zagotovila, pritrditveno (pozitivno) mnenje.
  - Revizija zagotavlja visoko, vendar ne popolno (absolutno) raven zagotovila o učinkovitosti kontrolnih postopkov. To je običajno izraženo kot sprejemljivo zagotovilo ob priznavanju dejstva, da je popolno zagotovilo mogoče redko doseči zaradi dejavnikov, kot so potreba po presoji, uporaba preizkušanja, naravne omejitve delovanja notranje kontrole, in ker je veliko dokazov, ki jih ima na voljo strokovnjak za revidiranje in dajanje zagotovil za IT, po svoji naravi prej prepričljivih kot neizpodbitnih

[vir: ITAF: stran 82]

Revizijska dokumentacija – Vrste poslov za področje IKT

Vrste storitev:

- Pregled - zmerna raven zagotovila, izraženo nikalno zagotovilo.
  - Pregled zagotavlja zmerno raven zagotovila o učinkovitosti kontrolnih postopkov. Raven dobljenega zagotovila je manjša, kot ga daje revizija, ker je obseg dela manj obsežen kot pri reviziji, vrsta, čas in obseg izvedenih postopkov pa ne dajejo zadostnih in ustreznih revizijskih dokazov, da bi strokovnjak za revidiranje in dajanje zagotovil za IT lahko izrazil pozitivno mnenje. Cilj pregled a je omogočiti strokovnjaku za revidiranje in dajanje zagotovil za IT, da potrdi, ali je na podlagi postopkov njegovo pozornost pritegnilo kar koli, zaradi česar strokovnjak za revidiranje in dajanje zagotovil za IT meni, da na podlagi opredeljenih sodil kontrolni postopki niso bili uspešni (izraženo nikalno zagotovilo)

[vir: ITAF: stran 82]

Revizijska dokumentacija – Vrste poslov za področje IKT

Vrste storitev:

- Dogovorjeni postopki - brez zagotovila, poročilo o dejanskih izsledkih.
  - Izvajanje dogovorjenih postopkov se ne konča z izražanjem kakršnega koli zagotovila strokovnjaka za revidiranje in dajanje za gotovil za IT. Strokovnjak za revidiranje in dajanje zagotovil za IT je zadolžen za izvedbo določenih postopkov, da zagotovi zahtevane informacije tistim strankam, ki so se dogovorile za postopke, ki jih je treba izvesti. Strokovnjak za revidiranje in dajanje zagotovil za IT izda poročilo o dejanskih izsledkih tistim strankam, ki so se dogovorile za postopke. Iz tega poročila izoblikujejo prejemniki svoje lastne ugotovitve, ker strokovnjak za revidiranje in dajanje zagotovil za IT ni sam določil vrste, časa in obsega postopkov, da bi lahko izrazil kakršno koli zagotovilo. Poročilo je omejeno na tiste stranke (npr. regulativni organ), ki so se dogovorile za postopke, ki jih je treba izvesti, saj drugi ne poznajo razlogov za te postopke in bi njihove izide lahko napačno razlagali. [vir: ITAF: stran 82]

Revizijska dokumentacija – Vrste poslov za področje IKT

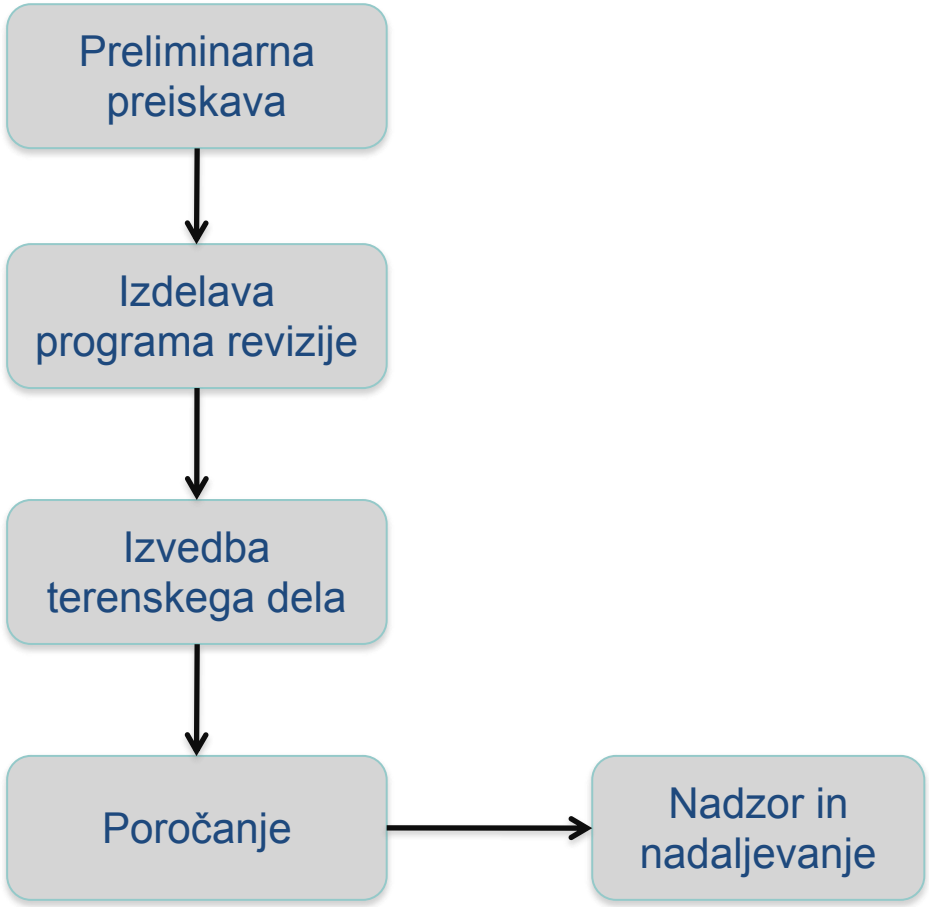
Vrste storitev (ponovno):

- Revizija - visoka raven zagotovila, pritrditveno (pozitivno) mnenje.
- Pregled - zmerna raven zagotovila, izraženo nikalno zagotovilo.
- Dogovorjeni postopki - brez zagotovila, poročilo o dejanskih izsledkih.

Revizija in pregled sta lahko neposredna ali potrditvena. V primeru potrditvene potrebujemo izjavo vodstva, ki je vodilo pri izvedbi storitve. Obe vrsti storitev vključujeta:

- načrtovanje posla,
- ovrednotenje učinkovitosti zasnove in delovanja kontrolnih postopkov,
- oblikovanje sklepa in poročanje o zasnovi in učinkovitosti kontrol na podlagi sodil.

Revizijska dokumentacija – Postopek revizije



Revizijska dokumentacija – Preliminarna raziskava

Namen: spoznavanje revidirane enote

Izvajanje:

- Ogled prostorov,
- Poizvedovanje pri osebju,
- Analiza stanja.

Rezultati:

- Določimo obseg in cilje revizije,
- Identificiramo potencialna tveganja in izpostavljenost,
- Določimo relevantne standarde in zakone za področje revizije,
- Določimo kontrole za izvajane aktivnosti.

Faze revizije IS

- Določitev posla
- Načrtovanje
- Izvajanje
- Poročanje
- Po-revizijski pregled

Faze revizije IS – Revizijska listina

- ITAF: 1001 (stran: 13) Standard „S1“
- Oblikujemo jo preden začnemo z revizijskim poslom.
- Namen je enako razumevanje posla.
- S podpisom listine se obe stranki obvežeta za izvedbo posla pod pogoji opredeljenimi v listini.
- Oblika listine ni strogo predpisana vendar vsebuje standardne vsebinske sklope.

ITAF – SLO (2 izdaja)

Faze revizije IS – Revizijska listina

Vsebina listine:

- Namen revizije,
- Odgovornost revizorja in odgovornost poslovodstva,
- Področje revizije in zakoni, katerim se podrejamo,
- Izjava o tveganju neodkritih pomembnih dejstvih,
- Dostop do informacij v okolju naročnika,
- Način zaračunavanja,
- Po potrebi tudi druge določbe.

Faze revizije IS – Preden se dogovorimo

- Preverimo ali izpolnjujemo pogoj o neodvisnosti
- Preverimo ali imamo ustrezna znanja oziroma bomo lahko najeli primerne veščake (specialiste področij)
- Preučimo organizacijsko strukturo in pridobimo osnovne podatke o stanju IT revidirane enote
- Ocenimo tveganost sprejetja revizijskega posla
- Preučimo namen revizijskega posla in skladnost s standardi – morda ne gre za revizijo
- Uporabimo lahko samoocenitveni vprašalnik

Faze revizije IS – Preden se dogovorimo

ITAF

1002 / 2002 – Organizacijska neodvisnost

1003 / 2003 – Strokovna neodvisnost

1006 / 2006 – Strokovna usposobljenost

1202 / 2202 – Ocenjevanje tveganja pri revizijskem načrtovanju

Faze revizije IS - Obseg revizije

Določitev obsega revizije

- **Obseg izhaja iz ciljev revizije**
- Pri določanju obsega si pomagamo z:
  - Pomembnost končnega revizijskega poročila in potrebe uporabnikov poročila (ITAF 1204),
  - Razumevanjem področja, ki ga revidiramo,
  - Upoštevamo zakonske in pravne zahteve,
  - Upoštevamo strukturo notranjih kontrol,
  - Ugotovitve in priporočila predhodnih revizij (ITAF 1206),
  - Preučimo potencialne vire podatkov za pridobivanje dokazov in zanesljivost teh podatkov,
  - Preučimo ali lahko uporabimo rezultate drugih revizorjev ali ekspertov (ITAF 2206).

Faze revizije IS - Obseg revizije

Pri določanju obsega upoštevamo naslednje:

- Kateri elementi izsledkov so potrebni?
- Ali je dovolj da pomanjkljivost ugotovimo ali je potrebno raziskati tudi vzrok in posledico?
- Ali bomo morali stanje preučiti glede na dan kriterij?
- Ali se bodo ugotovitve nanašale samo na vzorec oziroma primer, ki ga obravnavamo ali bomo morali ugotovitev posplošiti?
- Kaj so relevantni viri podatkov? Kdo ima podatke (ljudje, datoteke, računalniški sistemi)? Bodo podatki na voljo? Ali so zanesljivi?
- Kakšno zanesljivost informacije potrebujemo?
- Statistični vzorec, ali vzorec po lastni presoji?

Faze revizije IS – Pomisleki pri določanju obsega

Pri določanju obsega se bomo pogosto soočili s kompromisi:

- Manjši obseg -> manjše zagotovilo
- Omejitve časa in virov

- Ali je zmanjšan obseg sprejemljiv?

Faze revizije IS – Zmanjšanje obsega

V določenih primerih revizije ne bomo mogli izvesti v predvidenem obsegu. Razlogi za to so lahko:

- Zunanji faktorji na katere revidirana enota nima vpliva,
- Preprečitev dostopa do virov informacij (dokumentov, zapisov, ljudi, računalniške opreme),
- Neutemeljeno omejevanje časa za izvedbo revizije
- Vplivanje na izbiro ali izvedbo revizijskih postopkov ali omejitev transakcij, ki se pregledajo,
- V takšnih primerih v poročilu vključimo omejitve, ki so nastopile, v ekstremnih primerih lahko od revizije odstopimo, vendar je o tem potrebno poročati.

Faze revizije IS – Program revizije

- **Namen:** Sistematična izvedba revizije, zmanjšanje revizijskih tveganj, zagotovitev ponovljivosti
- **Izvajanje**: določimo postopke s katerimi bomo dosegli zadane cilje (kaj bomo pregledali, kaj bomo testirali)
- **Rezultati**: program revizije
- ITAF 1201 in 2201

Faze revizije IS – Izvedba - delo na terenu

- **Namen**: preiskati predmet revizije, zbrati zadostne dokaze za revizijsko mnenje
- **Izvajanje**: pregled zapisov, ocenjevanje informacij, zbiranje dokazov, ocenitev učinkovitosti kontrol
- **Rezultati**: delovni dokumenti rezultatov revizijskega pregleda
- ITAF 1203 in 2203

Faze revizije IS – Izvedba - delo na terenu

Na primer: Spoznavanje revidirane enote

- ugotoviti potrebe organizacije in vodstva
- poiskati ključne aktivnosti podjetja
- spoznati organizacijsko strukturo – kdo je kdo v podjetju
- pridobivanje osnovne dokumentacije o IKT okolju
  - seznam strojne in programske opreme
  - seznam internih pravilnikov, standardov vezanih na IKT
  - pogodbe z zunanjimi izvajalci (vsaj SLA-ji)

Faze revizije IS – Izvedba

- Razlika med preliminarno preiskavo in delom na terenu
- Namen preliminarne preiskave je ugotoviti ali določene kontrole sploh obstajajo.
- Na terenu preverimo:
  - učinkovitost kontrol
  - primernost kontrol

Faze revizije IS – Poročanje

- **Namen**: Izdaja revizijskega mnenja
- **Izvajanje**:
  - priprava pisnega poročila,
  - predstavitev rezultatov revidirancu,
  - uskladitev poročila z revidirancem.
- **Rezultati**:
  - revizijsko poročilo (ugotovitve + priporočila)
  - predstavitev poročila vodstvu

- ITAF – 1401 / 2401

Faze revizije IS – Nadzor in nadaljevanje

- **Namen:**
- ugotoviti ali so se priporočila upoštevala,
- ali so korektivni ukrepi izvedeni in dosegajo pričakovane rezultate
- **Izvajanje:**
- pregled odzivov revidirane enote, po potrebi izvedba testov
- **Rezultati:**
- podana priporočila zapremo

- ITAF – 1402 / 2402

Faze revizije IS – Nadzor in nadaljevanje

Kdaj lahko priporočila zapremo?

1. priporočilo je bilo učinkovito implementirano
2. alternativne akcije so bile izvedene, ki so dosegle predvidene rezultate
3. okoliščine so se spremenile tako, da priporočila niso več smiselna
4. priporočila se niso implementirala navkljub izvedbi vseh možnosti za izvedbo
5. poslovodstvo je sprejelo tveganja in to tudi ustrezno dokumentiralo

- ocenimo ali gre za zadevo, ki jo je smiselno v bodoče ponovno slediti/preiskovati.

Revizijska dokazila

- definicija
- značilnosti revizijskih dokazov
- način pridobivanja dokazov
- vrste oziroma oblike dokazov
- problemi zbiranja dokazov
- zanesljivost dokazov
- revizijski testi

Revizijska dokazila
Definicija

- Revizijski dokaz je informacija, katere namen je dokazati ali podpreti ugotovitev.

- ITAF – 1205 / 2205

Revizijska dokazila
Značilnosti revizijskih dokazov

Značilnosti revizijskih dokazov:

- **zadosten** – stvaren, primeren in prepričljiv do te mere, da bi druga oseba prišla do istih zaključkov kot revizor.
- **relevanten** – podpira revizorjeve ugotovitve in priporočila, je skladen z namenom in cilji revizije.
- **zanesljiv** in najboljši dosegljiv z uporabo ustreznih revizijskih tehnik.
- **uporaben** – pomaga doseči zadane cilje.
- **veljaven** – v času preiskave mora imeti veljavnost (npr. pridobimo ustrezno verzijo dokumenta)

Revizijska dokazila
Način pridobivanja dokazov

Način pridobivanja dokazov:

- opazovanje
- poizvedovanje
- intervju
- testiranje

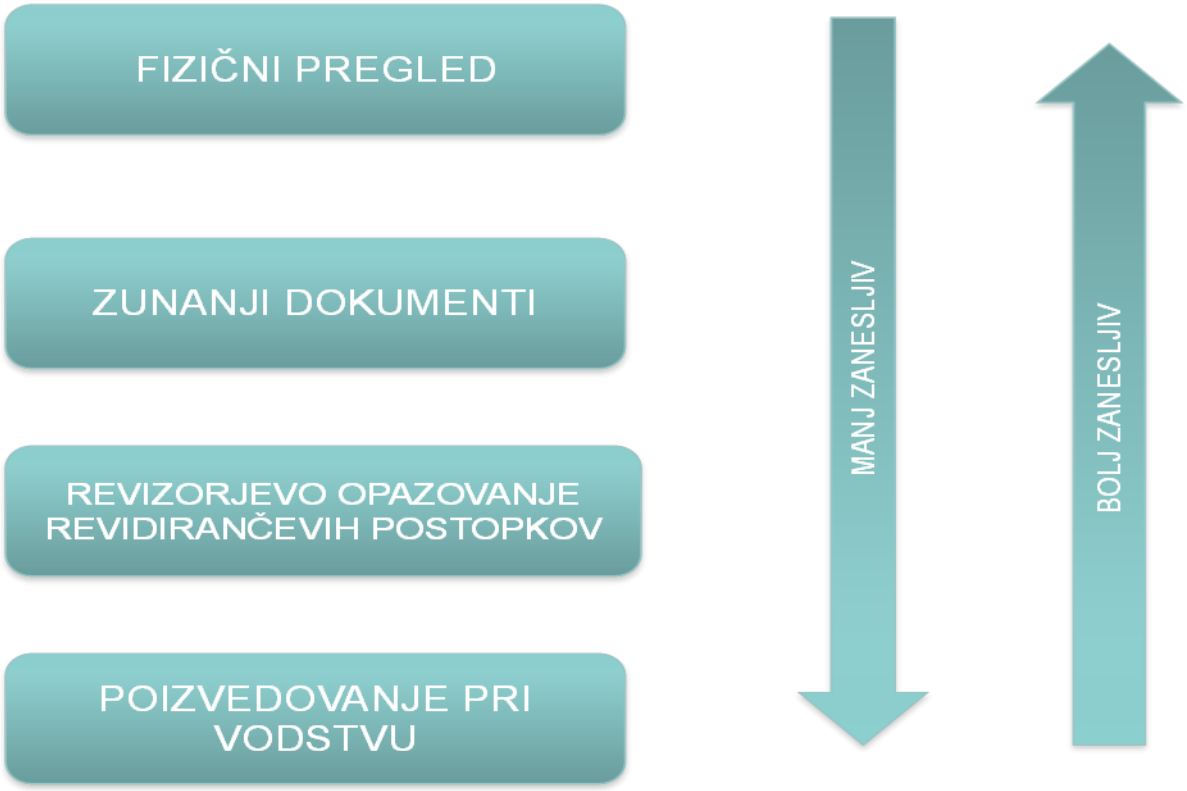
Revizijska dokazila
Vrste oziroma oblike dokazov

- **fizični dokazi** – pridobljeni z opazovanjem ljudi, lastnine ali dogodkov. Lahko so v obliki fotografij, načrtov, ipd.
- **pričanje/izpoved** – lahko je v obliki pisma, izjave, vprašalnika ali intervjuja. So manj prepričljivi, saj gre za mnenje drugih oseb. Kadar je mogoče jih podpremo z drugimi dokumenti.
- **uradni dokumenti** v pisni obliki (fizični ali elektronski) – zajemajo pisma/e-pošto, dogovore, pogodbe, direktive, ipd. Vir dokumenta vpliva na njegovo zanesljivost in zaupanje.
- **analitični dokaz** – pridobljeni s poizvedbami v sistemu, primerjavami s standardi, preteklimi operacijami/transakcijami, ipd.

Revizijska dokazila
Problemi zbiranja dokazov

- Kdaj je natisnjen dokument primeren dokaz?
- Kdaj je elektronski dokument primeren dokaz?
- Kako zbrati dokaze na določen dan (npr. 31.3.2009)?
- Delo na produkciji!?

Revizijska dokazila
Zanesljivost dokazov



Vir: ExamMatrix CISA Exam Review Vol. 1 - Theory

Revizijska dokazila
Revizijski testi

- definicija
- vrste revizijskih testov
- tveganja pri testih skladnosti
- primeri testov skladnosti
- tveganje pri vsebinskem preverjanju
- primeri vsebinskega preverjanja

Revizijska dokazila
Revizijski testi - definicija

Revizijski test je preizkus, ki se opravi z namenom pridobitve dokaza za posamezno ugotovitev ali del ugotovitve izraženo v mnenju

Revizijska dokazila
Revizijski testi - vrste revizijskih testov

Ločimo:

- teste skladnosti (*compliance test*) – revizorju zagotovi dokaze o obstoju internih kontrol, politike in postopki pa so učinkoviti.

- (*substantive test*) – preveri pravilnost izračunov.

  Ločimo:

  - test transakcije (*test of transactions*)
  - test stanja na računu (*test of balances*)
  - analitičen postopek pregleda

pravilnost zneskov/ vrednosti

pravilnost postopka izračuna

Revizijska dokazila
Revizijski testi - tveganja pri testih skladnosti

(*„Compliance test sampling risk“*)

Ločimo dve vrsti tveganj povezanih z vzorcem:

- **preveliko** zanašanje na kontrole, ki nakazujejo, da vzorec podpira planirano stopnjo zaupanja za kontrolo, kadar dejanska skladnost kontrole NE upravičuje takšnega zaključka.
- **premalo** zanašanje na kontrole, ki nakazujejo, da vzorec NE podpira planirane stopnje zaupanja za kontrolo, kadar dejanska skladnost kontrole podpira takšen zaključek.

Revizijska dokazila
Revizijski testi - primeri testov skladnosti

- Ali se gesla periodično spreminjajo?
- Ali se načrt neprekinjenega poslovanja redno testira?
- Ali se sistemski dnevniki pregledujejo?
- Ali se rezervne kopije („*backup*“) preverjajo („*restore*“)?
- Ali se incidenti beležijo in ustrezno obravnavajo?

Revizijska dokazila

Revizijski testi - tveganje pri vsebinskem preverjanju

(„*Substantive test sampling risk*“)

- napačen zaključek/potrditev (*incorrect acceptance*), da vzorec podpira ugotovitev, da NI **pomembno napačnih*** izračunov, kadar so izračuni pomembno napačni.

- napačno zavrnitev (*incorrect rejection*), da vzorec podpira ugotovitev o **pomembno napačnih*** izračunih, kadar so le-ti pravilni.

* pomembno napačni (ang. materially) – gre za to, da revizor določi prag,
kaj je takšna finančna škoda, da ogroža podjetje ostalo ga ne zanima oziroma o tem ne poroča

Revizijska dokazila
Revizijski testi - primeri vsebinskega preverjanja

- preverjanje števila izvedenih transakcij na računu s podatki v log datotekah
- preračun obresti za en mesec
- preverjanje zaloge v računalniški evidenci z dejansko zalogo
- izpis vseh transakcij nekega uporabnika po času

Revizijska dokazila

Nadaljevanje prihodnjič - na predavanju 5

- življenjski cikel dokazov
- viri za pridobivanje dokazov

Ta razmislek / do naslednjič

- Razmisliti
  - Grobi načrt revizije
- Pripraviti vprašanja za diskusijo

Zaključek / povzetek

Pridobili ste informacije o:

- Nadomeščanju odpadlega predavanja (dogovor)
- Revizijska dokumentacija (nadaljevanje)
- Faze revizije
- Revizijska dokazila (začetek)
- Za razmislek / do naslednjič

Za konec

- Pripombe
- Komentarji
- Predlogi