Fakulteta za elektrotehniko, računalništvo in informatiko

Revidiranje informacijskih sistemov

ITK 3 UN IS, ITK 3 UN TK

Predavanje 6 od 14

Maribor, 28. november 2014

Vsebina šestega predavanja

- Odprte zadeve predhodnega predavanja
- Kratka ponovitev vsebine predhodnega predavanja
- Dogovor o nadomeščanju - 2
- Dogovor o kolokviju
- Tveganja (nadaljevanje in zaključek)
- Kontrole
- Zaključek / povzetek

Odprte zadeve predhodnega predavanja

- Vprašanj ni bilo

Kratka ponovitev vsebine predhodnega predavanja

- Definicije
- Revizija in tveganje
- Ovrednotenje tveganj
- Izvor tveganj
- Vrste tveganj

Kratka ponovitev vsebine predhodnega predavanja

Vrste tveganj

- **vgrajeno** tveganje (inherent risk)
- tveganje za **nedelovanje vgrajenih kontrol** (control risk)
- **revizijsko** tveganje (detection risk, audit risk)

Kratka ponovitev vsebine predhodnega predavanja

Pomembnost

- Definicija
- V IKT
- Primeri

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 peto predavanje?
  - Pregledati / prenesti šesto – to predavanje?

Dogovor o nadomeščanju - 2

- Predavanja so, dne 14.11.2014, odpadla zaradi zdravstvenih težav predavatelja, na predavanjih 21.11.2014 ste izbrali možnost.
- Dogovor:
- Predavanje bomo nadomestili **v sredo, 03.12.2014** med **13:30** in **16:10**
- Lokacija: G2 – seminarska soba- 1. nadstropje.

Dogovor o kolokviju

- Kolokvij bo: **10.12.2014** ob 13.30 v G2
- Termin je nadomeščanje odpadlega predavanja z dne 24.10.2014 (dogovor na predavanju 7.11.2014).

Tveganja – Revizijsko tveganje

Audit Risk = Inherent Risk x Control Risk x Detection Risk

- *Inherent Risk* (IR) – sum, da obstaja pomembna pomanjkljivost (če ni kontrol)
- *Control Risk* (CR) – tveganje, da IR ne bo pravočasno preprečen ali identificiran z interno kontrolo, politiko ali proceduro.
- *Detection Risk* (DR) – tveganje, da revizor ne bo zaznal finančno pomembne pomanjkljivosti.

Tveganja – Revizijsko tveganje: primeri

- Vgrajeno tveganje je 50 %
- Verjetnost, da se napako najde v sklopu revizije je 80 %
- Kakšno je revizijsko tveganje?

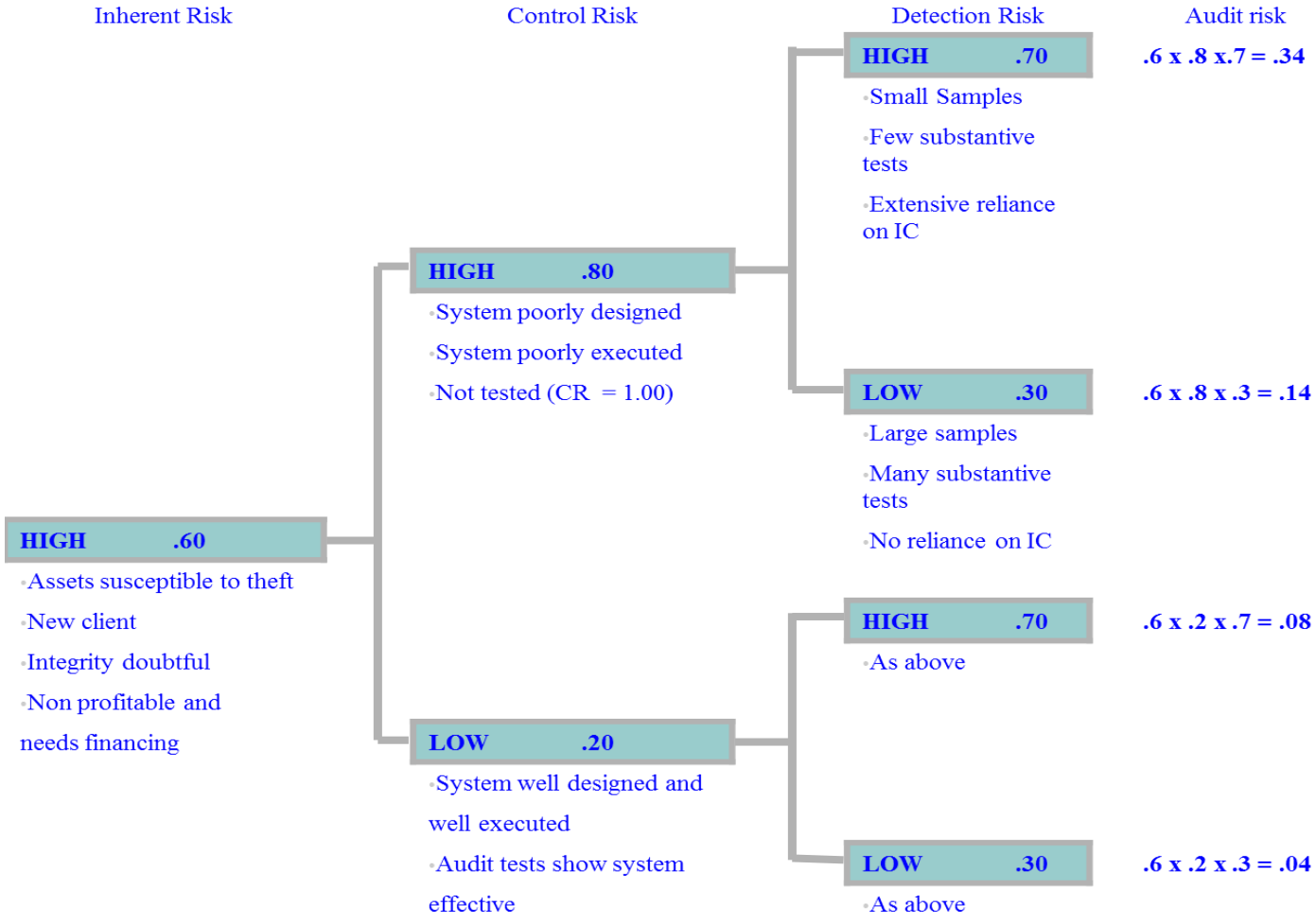
AR=IR x CR x DR= ?

Tveganja – Revizijsko tveganje: primeri

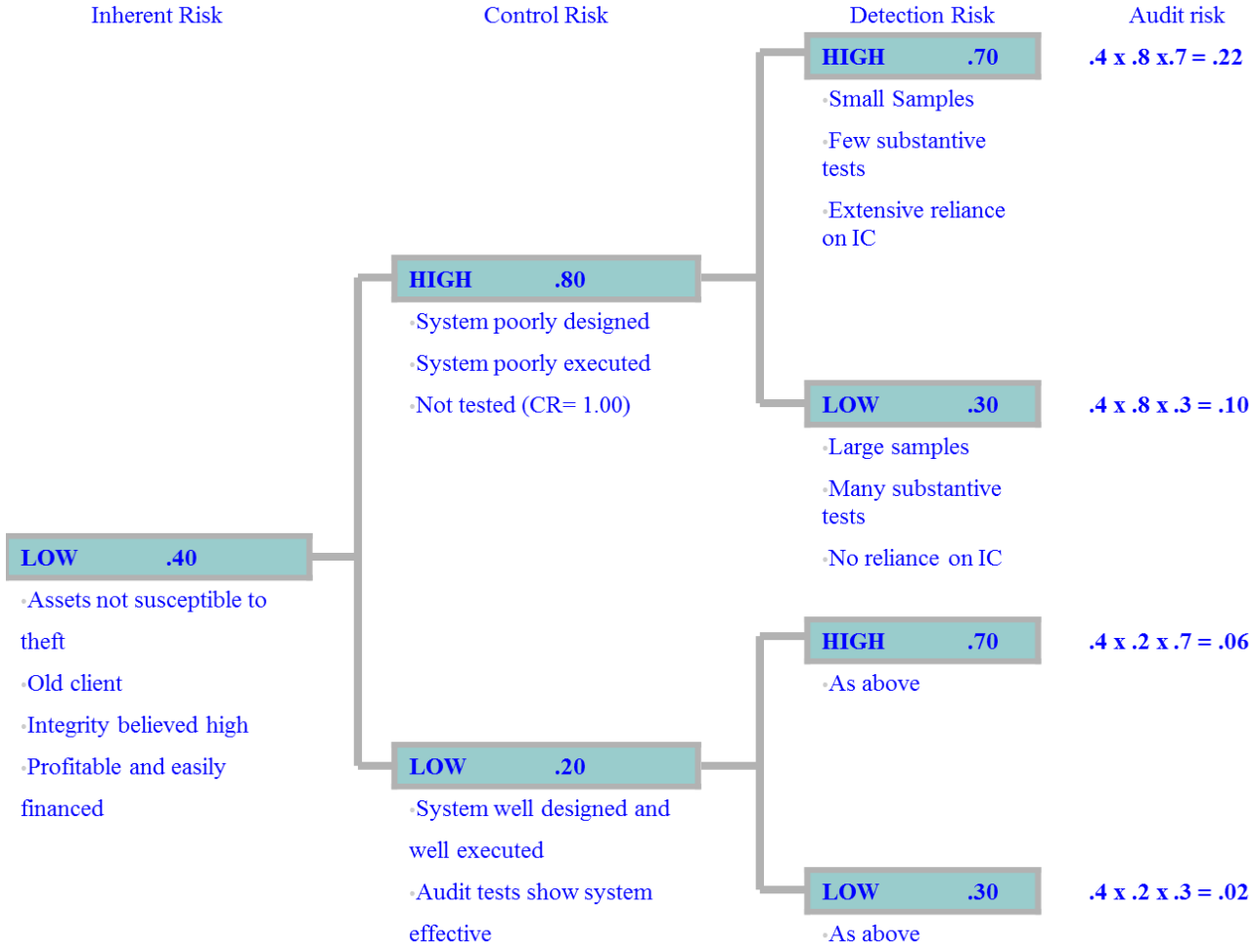
- Vgrajeno tveganje je 50 %
- Verjetnost, da se napako najde v sklopu revizije je 80 %
- Kakšno je revizijsko tveganje?

AR=IR x DR=0,5 x (1-0,8)=0,1

Tveganja – Revizijsko tveganje: grafično



Tveganja – Revizijsko tveganje: grafično



Tveganja – Revizijsko tveganje: vaja

- Vgrajeno tveganje, da bo računalnik v učilnici Amper dobil virus je 85 %.

- Kontrole za vgrajeno tveganje so:
  - preprečimo uporabo zunanjih nosilcev (ključki, CD-ji, ipd.)
  - namestimo antivirusni program, ki se dnevno samodejno posodablja (CR je 20%)

- Kakšen je potreben obseg testiranja, ki ga mora izvesti revizor?

- Predpostavka : revizijsko tveganje naj bo 5%

Tveganja – Revizijsko tveganje: vaja 1

$$DR = \frac{AR}{IR * CR}$$

$$DR = \frac{AR}{IR * CR} = \frac{0,05}{0,85 * 0,20} = 0,29$$

Tveganja – Revizijsko tveganje: vaja 2

- AR=5 %
- IR= 70 %
- CR = 50 %

$$DR = \frac{AR}{IR * CR} = \frac{0,05}{0,70 * 0,50} = 0,143 = 14,3\%$$

- Predpostavimo, da bomo za dosego 14 % tveganja odkritja morali izvesti 20 substantive testov.
- Zunanji revizor oceni, da je IR 80 % namesto 70 %. Koliko testov bo moral izvesti? **20,5**

Kaj pa če IR oceni na 70 % in CR na 20 %?

DR= 36 % -> št. testov = 14,9 = 15

Tveganja – Dejstvo

- Ker revizija temelji na pomembnosti in revizijskem tveganju je zagotovilo za delovanje IKT veljavno znotraj razumnih in praktičnih mej.

- Primer:
  Opravljena revizija ne pomeni, da na nobenem računalniku v podjetju ne moremo dobit virusa. Lahko pa z veliko gotovostjo trdimo, da ga na strežniku ne bo.

Tveganja – Dejstvo - nadaljevanje

- presoja glede pomembnosti in obsega izvedenih testov je prepuščena revizorju
- povečan obseg testov bo zmanjšal tveganje poslovanja in revizijsko tveganje verjetno pa tudi stopnjo finančne pomembnosti (materiality)
- povečan obseg po drugi strani poveča stroške revizije (velikost vzorca), ki so lahko neproporcionalno veliki glede na učinek
- ker ni 100 % verifikacije revizijskega tveganja ne more zmanjšati na 0
- revizijsko tveganje lahko ocenimo na podlagi ocene obsega izvedenih revizijskih testov

Tveganja – Dejstvo - nadaljevanje

- revizijsko tveganje in finančna pomembnost sta pomembna za planiranje revizijskega postopka in ovrednotenje rezultatov (katere pomanjkljivosti so pomembne za poročanje)
- finančna pomembnost vpliva na planiran obseg revizije, obseg testiranj in zadostnost revizijskih dokazov.
- meja, kaj je finančno pomembno in kaj ne, ni jasno postavljena in je odvisna od primera

- v splošnem velja, da bo revizor dal 95 % zagotovilo oziroma, da je stopnja revizijskega tveganja 5 %

Tveganja – Napake: definicija

- **Napake so nenamerne pomanjkljivosti sistema**.

- Ker se revizija izvaja na podlagi testov ali vzorčenja je smiselno ločiti med tremi tipi napak:
  - znane napake (*known errors*)
  - verjetne napake (*likely errors*)
  - možne napake (*possible errors*)

Tveganja – Napake: tipi napak

- Znane napake so napake, ki jih je revizor dejansko odkril med izvajanjem testov (substantive tests).
- Verjetne napake so napake do katerih pridemo z oceno na podlagi vzorčenja in dejansko odkritih napak. Verjetne napake vključujejo vse znane napake.
- Možne napake predstavljajo zgornjo mejo napak, ko posplošujemo ugotovitve na celotno populacijo. Možne napake so implicitne pri statističnem in ne-statističnem vzorčenju, vendar jih lahko ovrednotimo le na podlagi statističnega vzorčenja. Možne napake vključujejo znane in verjetne napake.

Tveganja – Napake

- Pri planiranju revizije moramo določiti takšen obseg, da možne napake ne bodo presegle meje finančne pomembnosti.
- V primeru, da možne napake dosežejo mejo finančne pomembnosti moramo izdati negativno mnenje ali zbrati dodatne dokaze za zmanjšanje negotovosti.
- Veliko revizorjev pri planiranju upošteva samo znane napake zato obstaja tveganje, da podcenimo obseg napak, saj možne napake presegajo znane napake.

Kontrola

- Kaj je?
- Definicija
- Vpliv kontrol na tveganja in povezava s stroški
- Kategorije kontrol
- Lastnosti kontrol
- Zahteve za uporabo kontrol
- Delitev kontrol
- Ovrednotenje kontrol
- Povezanost kontrol
- Uporaba kontrol

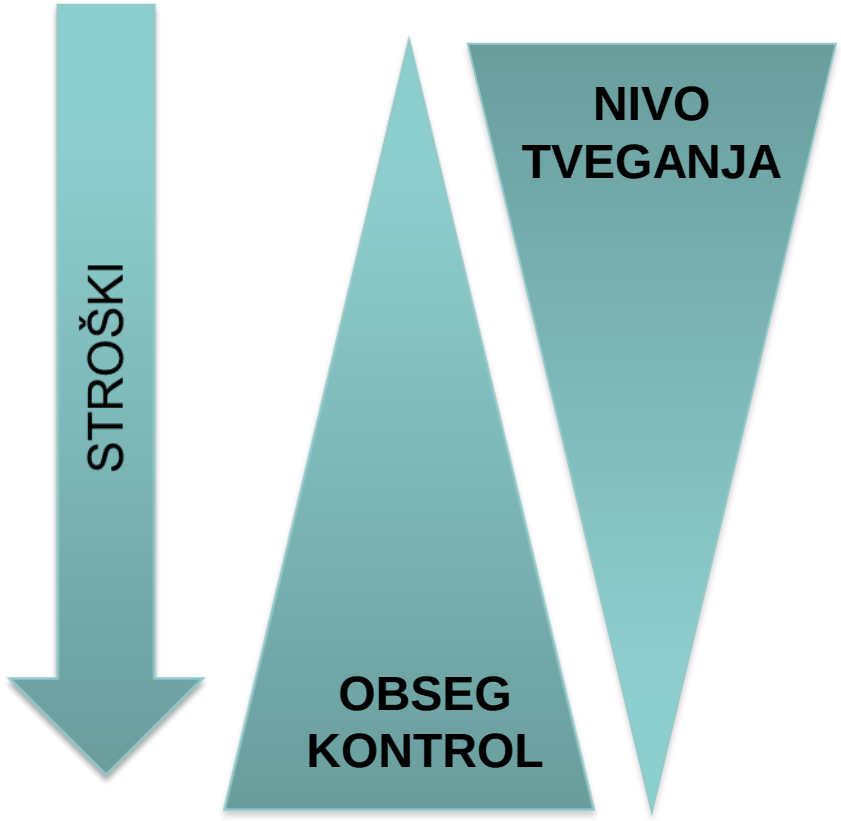
Kontrola – Kaj je?

- Kontrola (ang. Control) je sredstvo za izvajanje nadzora.
- Namen kontrol je omogočiti doseganje poslovnih ciljev.
- Kontrola je lahko ročni ali avtomatski postopek.
- Praviloma bo kontrola zmanjšala tveganje za poslovno aktivnost ali proces.

Kontrola – Definicija

Kontrola je kakršnakoli (nadzorna/kontrolna) akcija vodstva, katere rezultat je izpolnitev ciljev in nalog organizacije.

Kontrola - Vpliv kontrol na tveganja in povezava s stroški



Kontrola – Kategorije kontrol

- Ločimo dve osnovni kategoriji kontrol:
  - **splošne** ali **IKT kontrole** (*general or ICT*) – obravnavajo IKT kot celoto in zagotavljajo neprekinjeno in pravilno delovanje.
  - **aplikacijske kontrole** (*application*) – računalniško podprt postopek vgrajen v programsko opremo ali povezane ročne postopke, katerega namen je nadzor obdelave različnih tipov transakcij.

Kontrola – Splošne kontrole

- Splošne kontrole praviloma pokrivajo naslednja področja:
  - delovanje procesnega centra
  - nabavo in vzdrževanje sistemske programske opreme (ne aplikacije in druge programe)
  - varnost dostopa (fizično in logično)
  - razvoj in vzdrževanje programske opreme
  - podporo IS oddelkom (npr. tajništvo)

Kontrola – Aplikacijske kontrole

- v splošnem kontrole razdelimo glede na tri osnovne funkcije vsakega IS (vnos, obdelava, izpis)
- posebno pozornost je potrebno posvetiti vmesnikom, saj gre za "vrata" v zunanji svet in so bolj izpostavljeni
- med bolj pomembna področje uvrščamo tudi vhodne kontrole, saj z njimi nadzorujemo vnos podatkov v sistem
  - preverjamo prisotnost podatkov,
  - format
  - smiselnost

Kontrola – Lastnosti kontrol

- Strošek kontrole ne sme biti večji kot je pridobitev z njeno uporabo.
- Kontrola mora biti učinkovita.
- Zaposleni kontrole ne smejo dojemati kot prisilo ali omejitev. Zaželeno je, da kontrolo sprejmejo za svojo .
- Idealno je kontrola vgrajena v funkcije in opravila organizacije.
- Kontrola naj bo izbrana tako, da bo sprejeta kot pridobitev.

Kontrola – Zahteve za uporabo kontrol

- Revizor mora razumeti izvor in namen kontrole, ki se uporablja v aplikaciji ali poslovanju preden lahko sodi o njenih prednostih in pomanjkljivostih.
- Poiskati moramo osnovo za kontrolo, ki je lahko:
  - standard,
  - navodilo,
  - norma (*benchmark*)

Kontrola – Zahteve za uporabo kontrol

- principi internih kontrol
- operativni standardi za ročne in avtomatizirane operacije
- standardi razvoja in vzdrževanja aplikacijskih sistemov
- tehnični standardi iz področja IS
- operativni standardi iz področja IS
- administrativni standardi iz področja IS
- industrijski standardi
- splošno sprejeti standardi za: računovodstvo, procesiranje podatkov, revizijo, varnosti
- organizacijska pravila in postopki
- filozofije nadzora, ki jo prakticira vodstvo
- nivo tveganja sistema ali operacije
- toleranca vodstva glede tveganj za posamezna področja
- področje dela (bančništvo, zavarovalništvo, ipd.)

Kontrola – Delitev kontrol

- Kontrole lahko delimo na različne načine:
  - glede na tip – upravljavske, fizične, tehnične
  - glede na področje delovanja – aplikacijske, omrežne, razvojne, operativne, varnostne, kontrole integritete
  - glede na cilj –
    - neposredne (*directive*),
    - preventivne (*preventive*),
    - preiskovalne (*detective*),
    - korektivne (*corrective*) in
    - obnovitvene (*recovery*).

Kontrola – Neposredne kontrole

- so akcije, politike, postopki, direktive ali napotki vodstva, ki spodbudijo nek željen dogodek, da se manifestira.
- vplivajo na celoten proces ali operacijo
- naslavljajo naslednja področja:
  - uporabnost,
  - možnost vzdrževanja,
  - revidiranja,
  - nadzora,
  - varovanja kot tudi integriteto podatkov
  - in zanesljivost ter dostopnost sistemskih virov

Kontrola – Preventivne kontrole

- so vsi standardi, metode, prakse, orodja in tehnike (ročne ali avtomatske), katerih rezultat bo kvaliteten in zanesljiv sistem
- te kontrole tudi zmanjšajo nastop nezaželenih dogodkov (npr. vdorov, kraj, ipd.) kot tudi napak in nepravilnosti.
- kontrole naslavljajo področja kot je:
  - možnost vzdrževanja,
  - varnost,
  - uporabnost in
  - možnost nadzora.

Kontrola – Preiskovalne kontrole

- namen kontrol je dobiti povratno informacijo glede učinkovitosti (doseganje ciljev in izpolnitev standardov) direktnih in preventivnih kontrol
- zaznajo napake in nepravilnosti kot tudi značilnosti sistema glede kvalitete, nadzora in varnosti, ki se jim mora vodstvo posvetiti
- te kontrole nam dajo informacijo glede primernosti in popolnosti revizijskih sledi

Kontrola – Korektivne kontrole

- zagotavljajo informacijo, postopke in navodila za odpravo napak in nepravilnosti, ki smo jih odkrili
- lahko samo identificirajo mesto, kjer je popravek potreben (*corrective action*) ali popravek celo izvedejo
- naslavljajo področje uporabnosti in možnosti revizije

Kontrola – Obnovitvene kontrole

- zajemajo rezervne kopije, obnovo, restavriranje in ponovni zagon aplikacijskega sistema po kakršnikoli prekinitvi
  - pravočasna izdelava rezervnih kopij
  - rotiranje podatkov in datotek
  - točke preverjanja (*checkpoint*)
  - procedure ponovnega zagona (*restart/rerun*)
  - ohranitev zapisov in datotek (*record and file retention*)
  - sistemski in drugi dnevniki (*journaling*)
  - beleženje dogodkov z namenom obnove stanja (*recovery logging*)
  - načrt neprekinjenega poslovanja (*contingency plan*)

Kontrola – Komplementarne kontrole

- Komplementarna kontrola dopolnjuje eno ali več obstoječih kontrol in s tem izboljša njeno učinkovitost.

- Komplementarna kontrola se razlikuje od kompenzacijske kontrole po tem, da lahko nadgradi kontrolo, ki je sama po sebi dobra z namenom izboljšanja.

Kontrola – Primeri komplementarnih kontrol

- Požarni zid na osebnem računalniku dopolni varnost vgrajeno v operacijski sistem.
- RSA kartica dopolni varnost prijave.
- JavaScript skripta za preverjanje vnosa dopolni preverjanje pravilnosti podatkov v poslovni logiki.
- Ročne kontrole lahko dopolnijo avtomatske in obratno.

Kontrola – Ovrednotenje kontrol

- Revizor bo pogosto ocenjeval tudi moč in pomanjkljivosti kontrol.
- Naleti lahko na naslednje primere:
  - poslovna funkcija, sistem, postopek je lahko preveč/premalo nadzorovan
  - lahko je preveč kontrol na enem področju in premalo na drugem
  - kontrole se lahko prekrivajo ali podvajajo.
- Predlaga lahko dodatne kontrole ali ukinitev določenih kontrol.

Kontrola – V premislek...

- Pri vrednotenju kontrol upoštevamo:
  - povezanost kontrol
  - pridobivanje relevantnih in zanesljivih informacij
  - možnost uporabe kompenzacijskih kontrol
  - pomembnost revizijskih ugotovitev
  - materialnost ugotovitev - > ne pozabimo: materialnost je relativna!!!
  - upoštevajte "celotno sliko" ne posameznih dejstev

Kontrola – Analiza stroškov in koristi

(ang: *cost/benefit analysis*)

- analizo je priporočljivo izdelati v času načrtovanja vseh vrst kontrol, izvajanja kontrol in vzdrževanja le-teh

- teoretično naj stroški vpeljave, izvajanja in vzdrževanja kontrol ne bi nikoli presegli koristi – včasih je stroške težko ali nepraktično vrednotit.

Kontrola – Dejstva

- sistemi z visokim tveganjem in kompleksni sistemi zahtevajo več kontrol
- pretirana uporaba kontrol je draga, zaplete postopke, zmanjša zmogljivost sistema in ovira funkcije
- sistemski uporabniki želijo malo varnostnih kontrol in kontrol integritete

Kontrola – Kompenzacijske kontrole

- Kompenzacijska kontrola je dodatna kontrola, ki poveča moč obstoječe kontrole nekega področja.

- Gre za vzpostavljanje ravnovesja, kjer za šibko kontrolo na enem področju vpeljemo močno kontrolo na drugem področju, ki "kompenzira" šibkost prve in ustvari ravnovesje

Kontrola – Primer:

- **Šibka kontrola**: LAN ima odprte mrežne priključke.
- **Močna kontrola**: Administrator je obveščen po SMS-u, če se v omrežju pojavi računalnik z MAC naslovom, ki ni na seznamu.

Kontrola – Kdaj potrebujemo kompenzacijske kontrole?

- Ročne kontrole so šibke -> iščemo močne računalniške kontrole
- Računalniške kontrole so šibke - > iščemo močne ročne kontrole
- Kontrole vmesnikov med ročnimi in avtomatskimi sistemi so šibke - > iščemo močne kontrole v sistemih pošiljanja ali sprejemanja
- splošne kontrole so šibke - > iščemo močne povezane aplikacijske kontrole

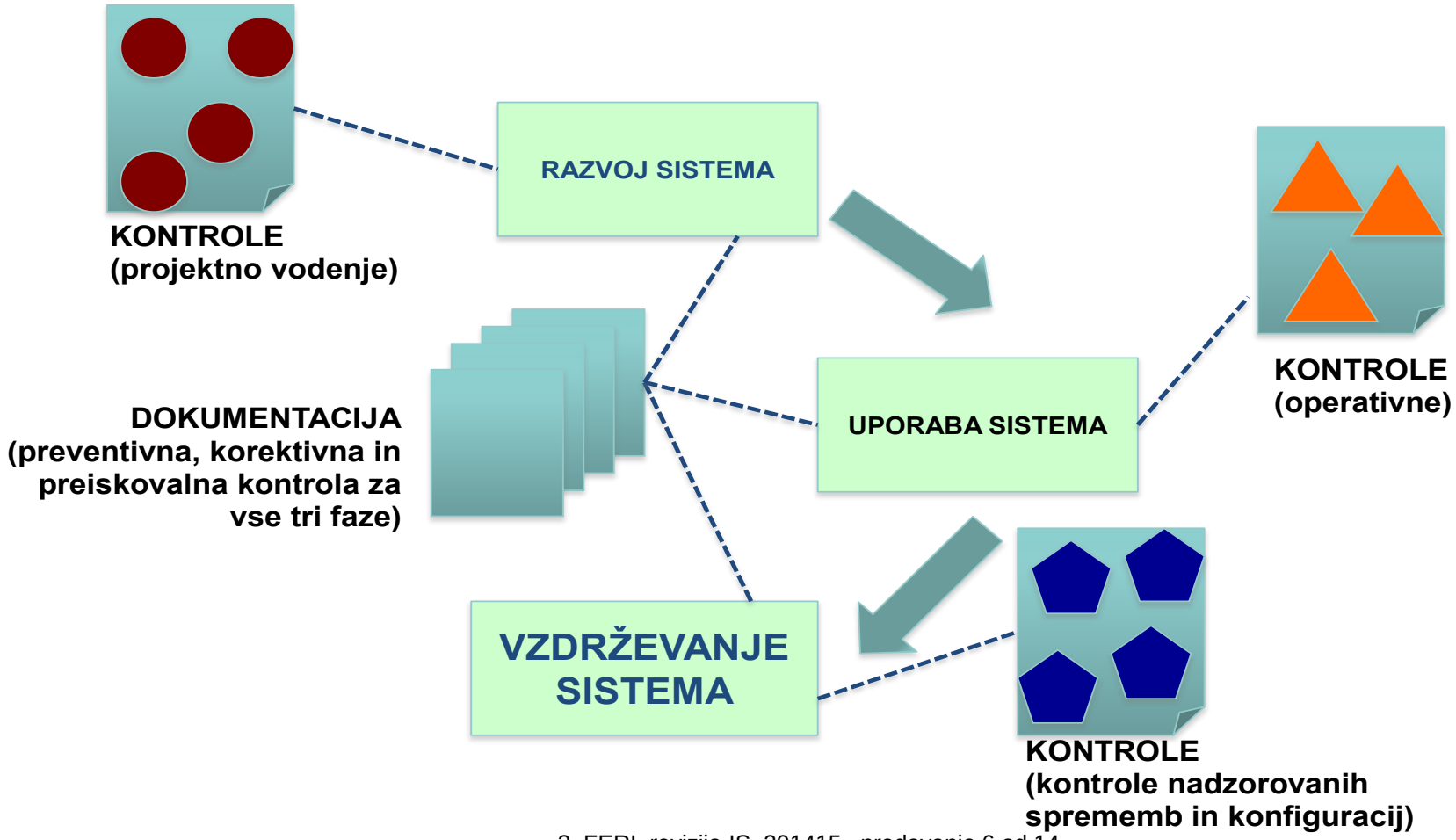
Kontrola – Primer:

- Šibka kontrola: Računalniška učilnica je zmeraj odprta (ni fizične kontrole)
- Kakšna je kompenzacijska kontrola?

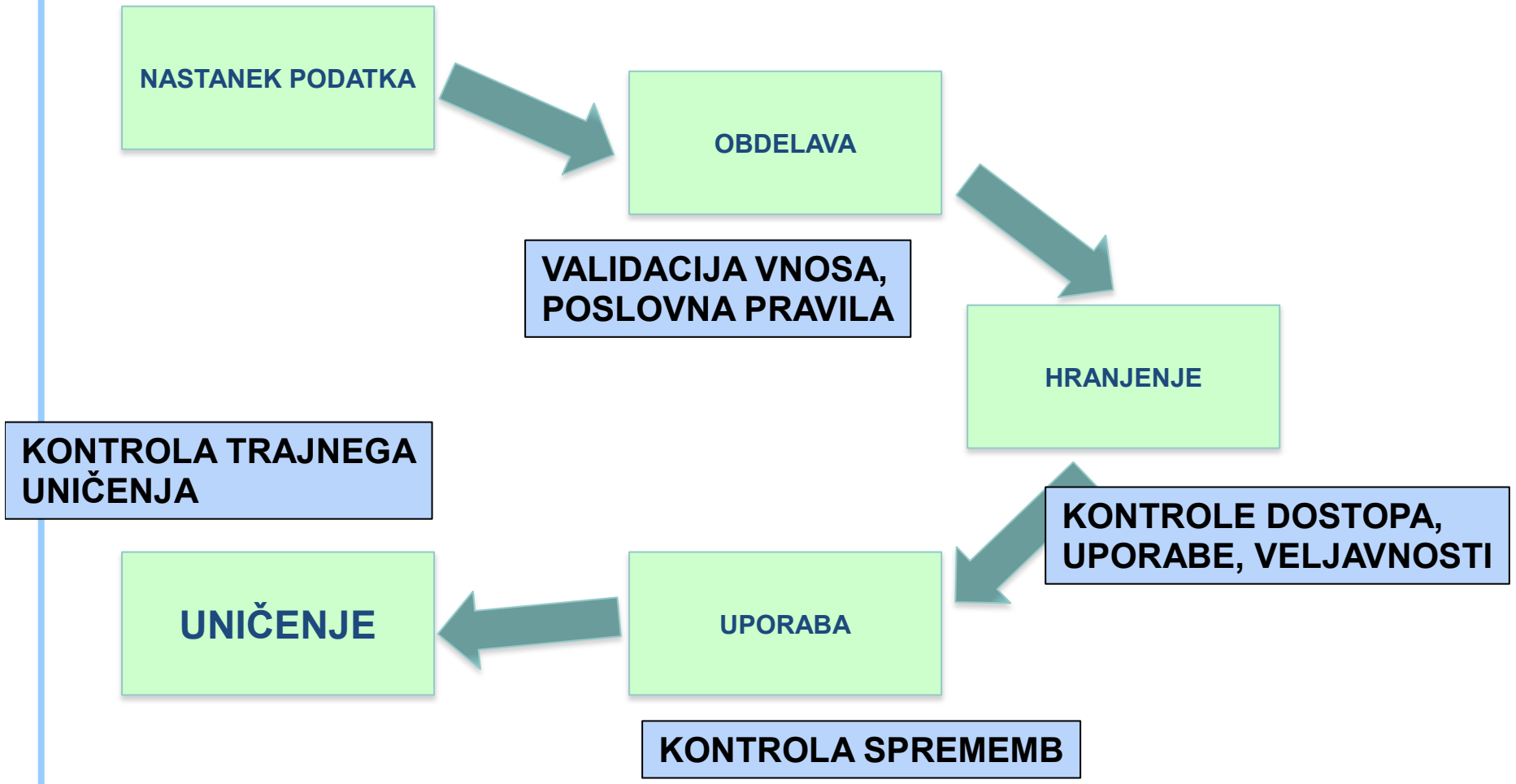
Kontrola – Povezanost kontrol

- Kontrole so medsebojno povezane.
- Pomanjkanje kontrol na enem področju lahko vpliva na delovanje drugih povezanih področij.
- Kontrola, ki je primerna za eno področje ni nujno uporabna na drugem področju, saj je življenjski cikel sistemov ali podatkov različen.

Kontrola – Primer: Življenjski cikel programske opreme



Kontrola – kakšen je življenjski cikel podatka?



Kontrola – Uporaba kontrol

- Vpeljava in uporaba kontrol zahteva sredstva in vire zato je potrebno premisliti o naslednjem:
  - velikosti IKT oddelka
  - velikosti celotne organizacije
  - vrednoti vira ali sredstva, ki ga varujemo
  - nivo in kompleksnost IKT tehnologije v uporabi
  - poslovno domeno kateri organizacija pripada
  - nivo tveganja sistema ali operacije
  - tolerance vodstva glede tveganj
  - zakonske, davčne, računovodske, vladne in druge regulative, ki jih mora organizacija upoštevati

Ta razmislek / do naslednjič

- Razmisliti
  - Kontrole – varnostno kopiranje osebnega računalnika
- Pripraviti vprašanja za diskusijo

Zaključek / povzetek

Pridobili ste informacije o:

- Tveganja
  - Revizijska tveganja
- Kontrole
  - Kaj je? in definicija
  - Vpliv kontrol na tveganja in povezava s stroški
  - Kategorije in lastnosti kontrol
  - Zahteve za uporabo kontrol
  - Delitev in ovrednotenje kontrol
  - Povezanost in uporaba kontrol
- Za razmislek / do naslednjič

Za konec

- Pripombe
- Komentarji
- Predlogi