Fakulteta za elektrotehniko, računalništvo in informatiko

Revidiranje informacijskih sistemov

ITK 3 UN IS, ITK 3 UN TK

Predavanje 5 od 14

Maribor, 21. november 2014

Vsebina četrtega predavanja

- Odprte zadeve predhodnega predavanja
- Kratka ponovitev vsebine predhodnega predavanja
- Dogovor o nadomeščanju
- Dogovor o kolokviju
- Revizijska dokazila (nadaljevanje in zaključek)
- Tveganja
- Pomembnost
- Za razmislek
- Zaključek / povzetek

Odprte zadeve predhodnega predavanja

- Vprašanj ni bilo

Kratka ponovitev vsebine predhodnega predavanja

- Revizijska dokumentacija (nadaljevanje)
- Faze revizije
- Revizijska dokazila (začetek)
- Za razmislek

Kratka ponovitev vsebine predhodnega predavanja

Revizijska dokumentacija (nadaljevanje)

- Vrste storitev
- Postopek revizije
- Preliminarna raziskava

Kratka ponovitev vsebine predhodnega predavanja

Faze revizije

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

Kratka ponovitev vsebine predhodnega predavanja

Revizijska dokazila (začetek)

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

Kratka ponovitev vsebine predhodnega predavanja

Za razmislek

- Grobi načrt revizije
  - Varnostno kopiranje osebnega računalnika
- vprašanja za diskusijo

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 četrto predavanje?
  - Pregledati / prenesti peto (to) predavanje?

Dogovor o nadomeščanju - 1

- Predavanja so, dne 24.10.2014, odpadla zaradi zdravstvenih težav predavatelja, na predavanjih 7.11.2014 ste izbrali možnost.
- Dogovor:
- Predavanje bomo nadomestili **v sredo, 10.12.2014** med **13:30** in **16:10**
- Lokacija: G2 – seminarska soba- 1. nadstropje.

Nadomeščanje - 2

- Predavanja so, dne 10.11.2014, odpadla zaradi zdravstvenih težav predavatelja, moramo jih nadomestiti!
- Predlog:
- a) Predavanje nadomestimo **v sredo, 3.12.2014** med **13:30** in **16:10**
  Lokacija: G2 – seminarska soba- 1. nadstropje
- b) drugo

Kolokvij

- Na predavanju 7.11.2014 smo izbrali termina 21.11.2014 in 28.11.2014 med **13:15** in **14:00**
- Zaradi zdravstvenih težav predavatelja so odpadla tudi predavanja dne 14.11.2014
- ste preverili pri ostalih predmetih

PREDLOG:

- Kolokvij: **3.12.2014** (ko nadomeščamo 10.11.2014) ali **10.12.2014** (ko nadomeščamo 24.10.2014)

Revizijska dokazila - nadaljevanje

- Viri za pridobivanje dokazov

Viri za pridobivanje dokazov

- Pri ugotavljanju **zadostnosti**, **relevantnosti** in **ustreznosti** dokazov je pomemben njihov izvor. Dokaze lahko pridobimo od:
  - revizorjev
  - revidiranca
  - tretjih oseb
  - iz računalniškega sistema

Viri za pridobivanje dokazov
Dokazi revizorjev

- Lastne dokaze lahko pridobimo z opazovanjem in/ali testi. Metode vključujejo:
  - vprašalnik,
  - strukturiran intervju,
  - direktno opazovanje
- Zasnova metod in izkušnje revizorja lahko bistveno vplivajo na zadostnost, relevantnost in ustreznost dokazov.

Viri za pridobivanje dokazov
Dokazi revizorjev

- Revizor mora izločiti nasprotujoče si razlage ugotovitev. Proces vključuje naslednje postopke preverjanja veljavnosti:
  - interna veljavnost (internal validity) – pomeni, da je A (program revizije) povzročil B (učinek izmerjen pri reviziji)
  - veljavnost zasnove (construct validity) – se nanaša na preverjanje ali revizor meri ali opazuje to kar je bilo predvideno.
  - zunanja veljavnost (external validity) – se nanaša na zmožnost posplošitve ugotovitev.

Viri za pridobivanje dokazov
Dokazi revidiranca

- Revizor lahko kot dokaz upošteva tudi podatke, ki mu jih posreduje revidiranec.

- V primerih, ko so dokazi pridobljeni od revidiranca signifikantni glede na celotno dokazno gradivo, mora revizor pridobiti dodatne dokaze o zanesljivosti teh podatkov.

- Revizor lahko potrebne dokaze pridobi:
  - s testiranjem učinkovitosti kontrol glede zanesljivosti podatkov
  - z izvajanjem direktnih testov nad podatki
  - s kombinacijo obeh pristopov

Viri za pridobivanje dokazov
Dokazi revidiranca

- Kadar izvedeni testi pokažejo napake v podatkih mora revizor preučiti signifikantnost napak.

- V primeru signifikantnih napak razglasimo podatke za neveljavne ali nezanesljive takrat:
  - lahko iščemo podatke iz drugih virov,
  - ponovno določimo revizijske cilje tako, da nam neveljavnih podatkov ni potrebno uporabiti
  - uporabimo podatke, vendar v poročilu jasno opozorimo na omejitve, ki izhajajo iz uporabljenih podatkov

Viri za pridobivanje dokazov
Podatki tretjih oseb

- Podatke lahko pridobimo od oseb, ki niso direktno povezane/vključene v revizijo.
- Podatki so lahko že bili revidirani ali jih lahko brez težav revidiramo sami.
- Pogosto pa ne bomo mogli dobiti ustreznih dokazov o veljavnosti in zanesljivosti podatkov.
- Vplivi podatkov so podobni kot v primeru, ko podatke dobimo od revidiranca.

Viri za pridobivanje dokazov
Podatki iz računalniškega sistema

- Tudi za podatke iz računalniških sistemov moramo pridobiti ustrezne dokaze o veljavnosti in zanesljivosti, kadar gre za podatke, ki so ključni za podano revizijsko mnenje.
- To dosežemo s pregledom splošnih in aplikacijskih kontrol.
- Dokaze moramo pridobiti ne glede na to ali smo podatke iz sistema dobili (od zaposlenih) ali smo jih pridobili sami.
- Kadar ne gre za ključne podatke, vendar jih kljub temu vključimo v poročilo moramo obvezno navesti vir podatkov in ali so bili preverjeni ali ne. Na ta način zadostimo standardom poročanja.
- Včasih si lahko pomagamo z ugotovitvami drugih revizorjev.

Viri za pridobivanje dokazov

- pregled organizacijske strukture
- IS dokumentacija, standardi in prakse
- sistemska dokumentacija (diagrami, priročniki, specifikacije)
- intervjuji s primernim IKT in drugim osebjem
- opazovanje izvajanja operacij in izvrševanja nalog s strani zaposlenih (IS in področja domene)
- izbira in preverjanje ključnih kontrol (IKT in ne IKT okolje)
- uporaba tehnik vzorčenja, kjer so primerne
- uporaba posebnih revizijskih orodij (CAAT*)

**CAAT – Computer Assisted Audit Techniques*

Tveganja

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

Tveganja - definicija

- Tveganje je verjetnost pojava neželenega dogodka, ki bo privedel do finančne škode ali škode v drugi obliki.
- Možnost pojava takšnega dogodka imenujemo izpostavljenost.
- Tveganje **se realizira** zaradi izpostavljenosti.
- **Kontrole** lahko *zmanjšajo* ali *odstranijo* tveganje oziroma izpostavljenost tveganju (*o kontrolah bomo govorili na 6. predavanju*).

Revizija in tveganje

- Strategija revizije naj bi temeljila na tveganjih.
- Za največji učinek revizije je potrebno vire (revizorja) optimalno izkoristiti, saj so viri dragi in omejeni.
- Izvedba analize tveganj je pomemben korak pri planiranju revizijskega pregleda.

Koraki pri ovrednotenju tveganj

- Model za ovrednotenje tveganj vključuje naslednje korake:
  - določitev faktorjev tveganja
  - presojo o relativni pomembnosti faktorjev tveganja
  - določanje prisotnosti faktorja tveganja v revidirani enoti
  - ocenitev stopnje tveganja
  - razporejanje revizijskih virov glede na stopnjo tveganja

Tveganja
Presoja in intuicija

- se pogosto uporablja
- temelji na izkušnjah in znanju revizorja
- gre za presojo "po občutku„

- tveganja ovrednotimo kot
  - (sprejemljiva)
  - **nizka,**
  - **srednja,**
  - **visoka**

Tveganja
Ocenitveni pristop

- dodeli utež in stopnjo tveganja vsaki karakteristiki, ki jo ocenjujemo
- skupno tveganje se izračuna ko vsota po vseh karakteristikah, kjer je tveganje karakteristike produkt uteži in stopnje.

Tveganja
Skupno tveganje

KAKOVOST INTERNIH KONTROL	**UTEŽNI FAKTOR 30 %** **STOPNJA TVEGANJA: dobra kontrola 0, slaba 4**
LIKVIDNOST VPLETENIH SREDSTEV	**UTEŽNI FAKTOR 25 %** **STOPNJA TVEGANJA: brez 0, gotovina 4**
KOMPLEKSNOST OPERACIJ IN SISTEMOV	**UTEŽNI FAKTOR 20 %** **STOPNJA TVEGANJA: preprosto 0, zelo kompleksno 4**
STABILNOST ORGANIZACIJE IN SISTEMOV	**UTEŽNI FAKTOR 15 %** **STOPNJA TVEGANJA: stabilen 0, kaotičen 4**
ČAS OD ZADNJE INTERNE REVIZIJE	**UTEŽNI FAKTOR 10 %** **STOPNJA TVEGANJA: nenehno 0, pred več kot 3 leti 4**

Tveganja
Tehnika Delphi

- namen je zmanjšati vpliv posameznega ocenjevalca
- ocenjevalci anonimno ocenijo utež in stopnjo tveganja (lahko uporabimo vprašalnik)
- ocene krožijo med ocenjevalci za uskladitev
- želja je, da se doseže konsenz glede dodeljenih vrednosti

Tveganja
Kvantitativna metoda

- pri kvantitativni metodi tveganje ocenimo na podlagi razpoložljivih podatkov (številk)
- kvantitativno (številčno) izrazimo
  - potencialni vpliv
  - pogostost pojava

ALE = I x F

ALE – Annual loss exposure
I – ocenjen vpliv
F – pogostost (frekvantnost) pojava

Tveganja
Kvantitativna metoda - vaja

- Po kvantitativni metodi ocenite tveganje za računalniško učilnico Amper. V učilnici se nahaja:
  - 20 PC računalnikov (560 EUR) + monitorji (50 EUR)
  - projektor (620 EUR)
  - omrežna napeljava (1200 EUR)
  - brezžični usmerjevalnik (*wireless router*) (120 EUR)
  - programska oprema (300 EUR /PC)
  - strežnik (2500 EUR)

Tveganja
Primeri

- Tipični primeri IT tveganj so:
  - v podjetju se tveganja ne ocenjujejo, kar vpliva na napačno implementacijo kontrol
  - odgovornosti niso jasno opredeljene in ni ustrezne vpletenosti vodstva, kar pripelje so neustreznega ločevanja nalog (*segregation of duties*)
  - slab nadzor in slabi postopki dela osebja lahko povzročijo težave z neustreznimi dostopi (*access control*)
  - odprti sistemi (brez kontrol) in pomanjkanje ozaveščenosti uporabnikov bodo skupaj s človeškimi napakami povzročili nesprejemljivo stopnjo tveganja za določen sistem.

Tveganja
Izvor tveganj

- Tveganje računalniških sistemov pogosto izhaja iz:
  - napačne hrambe zapisov
  - prekinitev poslovanja
  - napačnih odločitev vodstva
  - prevar in vdorov
  - izgube ali uničenja sredstev
  - konkurenčne prednosti drugih
  - prevelikih stroškov
  - ohromelosti poslovanja (možni različni vzroki)

Tveganja
Vrste tveganj

- Pri revizijskem pregledu se praviloma srečamo s tremi vrstami tveganj:
  - **vgrajeno** tveganje (*inherent risk*)
  - tveganje za **nedelovanje vgrajenih kontrol** (*control risk*)
  - **revizijsko** tveganje (*detection risk, audit risk*)

Tveganja – Vgrajeno tveganje

- vgrajeno tveganje je verjetnost pomembnih izgub, ki bi nastale preden upoštevamo pristope za zniževanje tveganja.

- za ocenitev tveganja mora dobro poznati okolje, kjer lahko tveganje nastopi

Tveganja – Tveganje kontrol

- ocenjuje verjetnost, da so kontrole za upravljanje vgrajenih tveganj neučinkovite
- za oceno tveganja je potrebno ugotoviti katere kontrole se uporabljajo za posamezna tveganja
- po uvedbi kontrol nam ostane določena stopnja tveganja (*residual risk*), ki jo sprejmemo

Tveganja – Vgrajeno tveganje

- vgrajeno tveganje je verjetnost pomembnih izgub, ki bi nastale preden upoštevamo pristope za zniževanje tveganja.

- za ocenitev tveganja mora dobro poznati okolje, kjer lahko tveganje nastopi

Tveganja – Pomembnost

- (ang: materiality)
- Definicija
- Pomembnost v IKT
- Primeri

Tveganja – Pomembnost : definicija

- Informacije so pomembne takrat, ko lahko njih opustitev ali napačna navedba vpliva na poslovne odločitve uporabnikov, zasnovane na računovodskih izkazih.
- Pomembnost je odvisna od posamezne postavke ali napake, ocenjene v posameznih okoliščinah, nje opustitve ali napačne navedbe
- Pomembnost se torej nanaša ne stopnjo natančnosti računovodskih izkazov – večja je pomembnost, večja je natančnost in obratno.

MSR_320

Tveganja – Pomembnost v IKT

- pomembnost se ne naša zgolj na računovodske izkaze, temveč tudi na poslovne aktivnosti in računalniški sistem.
- pomembnost računovodskih izkazov se ocenjuje glede na celotne računovodske izkaze
- za poslovne aktivnosti pomembnost ocenjujemo za posamezno operacijo, kot tudi za povezane operacije
- za računalniški sistem pomembnost ocenjujemo za specifičen sistem, ki ga obravnavamo in tudi druge povezane sisteme
- pomembne pomanjkljivosti v poslovnih aktivnostih ali računalniškem sistemu lahko, ni pa nujno, vplivajo na računovodske izkaze.

Tveganja – Pomembnost - primeri

- sistem neprekinjenega napajanja sam po sebi ni pomemben v navezi s strežniki, ki so nanj priključeni, pa lahko postane izjemno pomemben
- obsežna uporaba piratske programske opreme lahko postane finančno pomembna (material), saj lahko pride do tožb, legalizacije programske opreme, izguba ugleda, ipd.
- širjenje informacij o novih produktih, postopkih dela, skrivnih recepturah lahko imajo pomembne finančne posledice.
- učinek slabe kvalitete izdelkov, kršitev okoljevarstvenih predpisov, ipd.

Tveganja – Revizijsko tveganje

- Pomembne pomanjkljivosti v poslovnih aktivnostih in računalniškem sistemu pomenijo poslovno tveganje.

- **Revizijsko tveganje** je tveganje, da revizor ne odkrije pomembnih napak ali pomanjkljivosti med izvajanjem revizijskega postopka.

Tveganja – Revizijsko tveganje: definicija

- **Revizijsko tveganje** je verjetnost, da bo revizor izdal pozitivno mnenje v primeru, ko obstajajo pomembne napake ali pomanjkljivosti pri predmetu revizije.

- Revizijsko tveganje je odvisno od potrebnega zagotovila:
  - manjše kot je tveganje, večje je zagotovilo in obratno

- Ker revizija temelji na testih in vzorčenju revizijskega tveganja, ni možno revizijskih tveganj zmanjšat na nič.

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

NADALJEVANJE NA PREDAVANJIH št.6 – 28.11.2014

Tveganja – Revizijsko tveganje: primeri

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

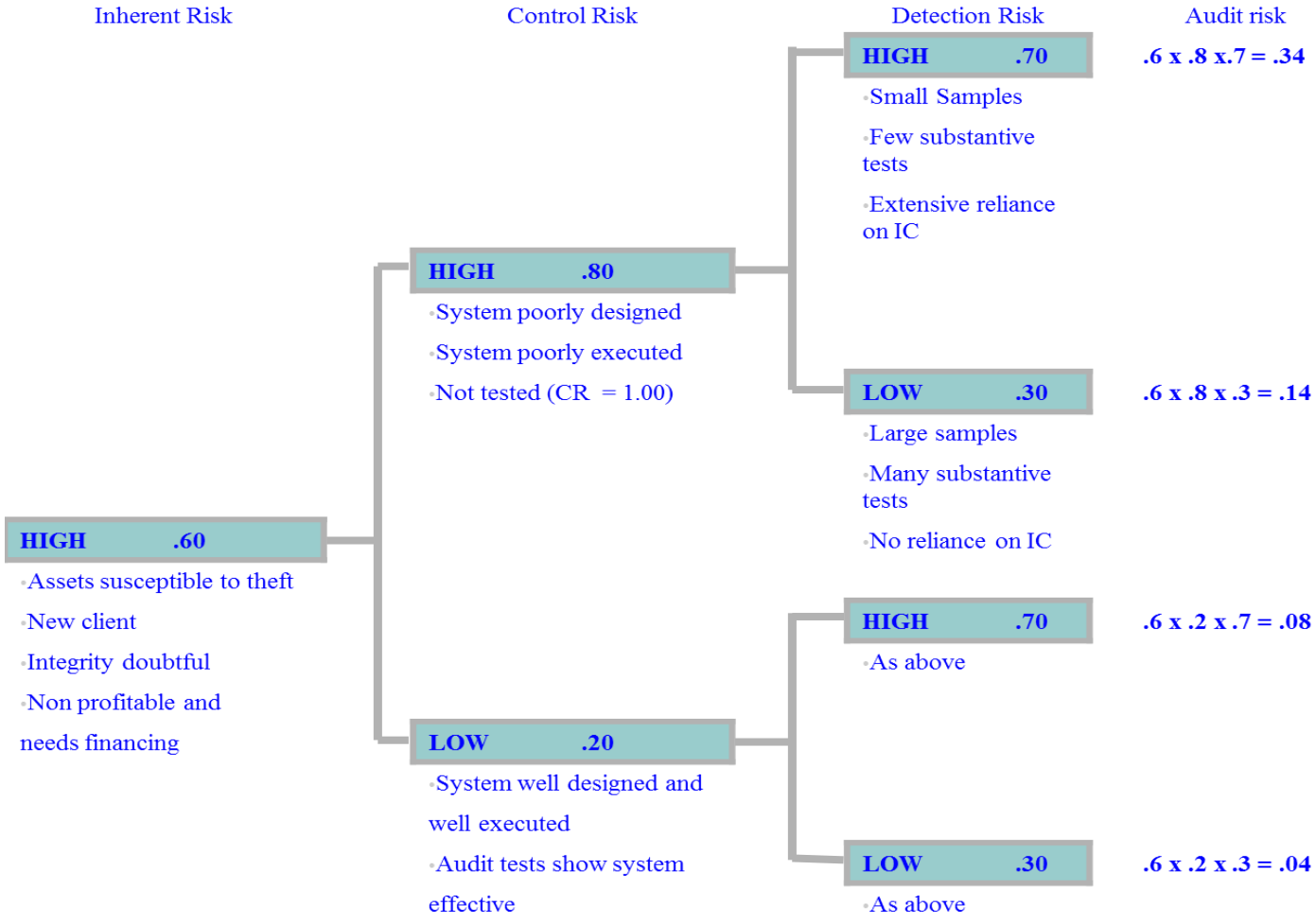
AR=IR x CR x DR= ?

Tveganja – Revizijsko tveganje: primeri

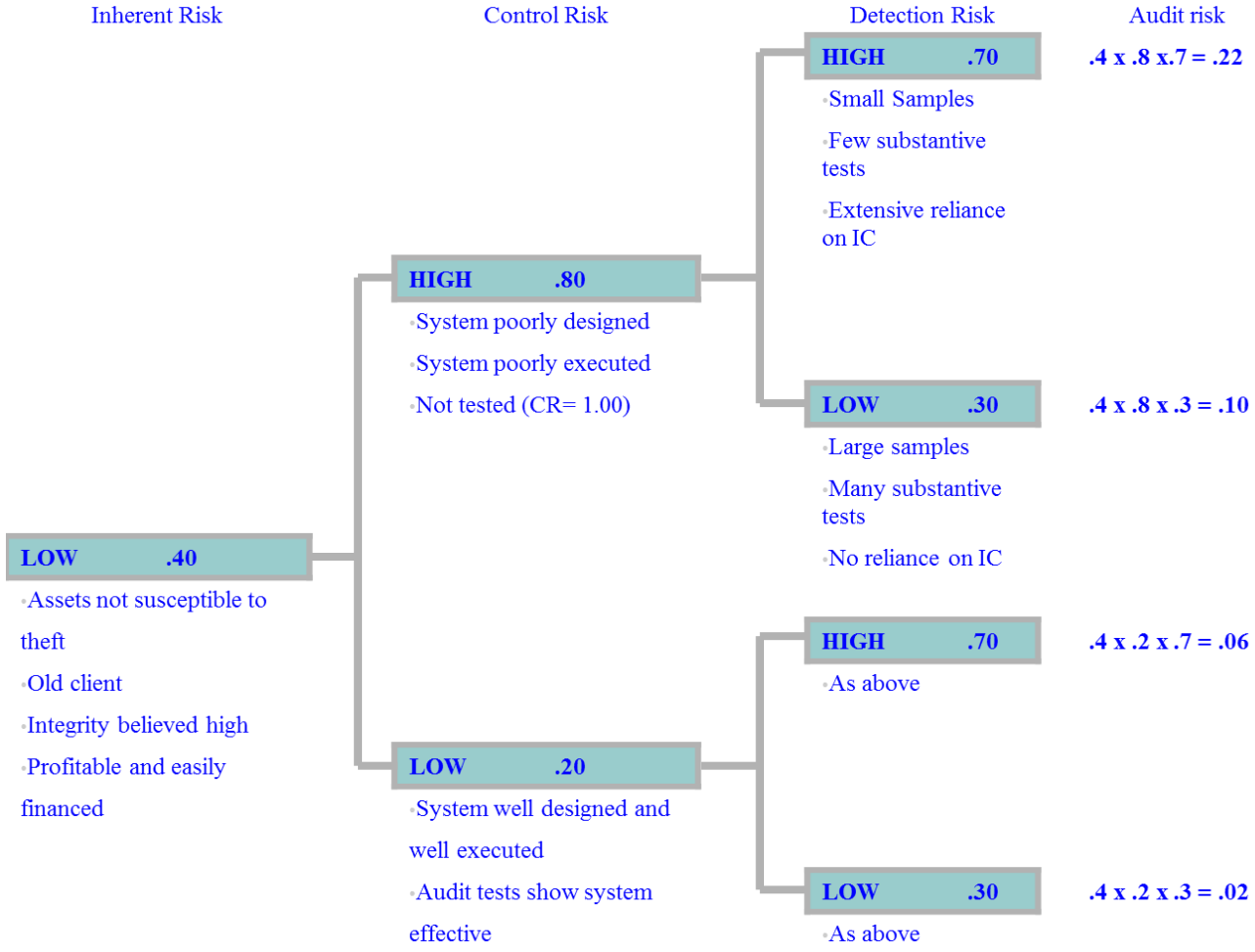
- Vgrajeno tveganje je 50 %
- Verjetnost, da se napako najde v sklopu revizije je 80 %
- Kakšno je revizijsko tveganje?

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 o
- 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.

Ta razmislek / do naslednjič

- Razmisliti
  - Tveganja pri varnostnem kopiranju osebnega računalnika
- Pripraviti vprašanja za diskusijo

Zaključek / povzetek

Pridobili ste informacije o:

- Nadomeščanju odpadlega predavanja (dogovor)
- Dogovor o kolokviju
- Revizijska dokazila
- Tveganja
  - Definicije
  - Revizija in tveganje
  - Ovrednotenje tveganj
  - Izvor tveganj
  - Vrste tveganj
- Za razmislek / do naslednjič

Za konec

- Pripombe
- Komentarji
- Predlogi