Ревизија информационих система

Теме у овом модулу

- Окружење контрола базираних на информационим технологијама
- Мануелне контроле зависне од информационих технологија
- Апликационе контроле – “ход кроз систем”
- Тестирање апликационих контрола
- Интерфејс и тестирање контрола интерфејса
- Опште контроле базиране на информационим технологијама (ITGC)
- Промене програма
- Програмске операције
- Опште контроле базиране на информационим технологијама – “ход кроз систем” и тестирање

Због чега је битно вршити ревизију контрола базираних на информационим технологијама?

Због чега је битно вршити ревизију контрола базираних на информационим технологијама? (наставак)

- Велики број организација данас у значајној мери се ослања на употребу информационих технологија.
- Од интерних ревизора се очекује да врше процену контрола базираних на информационим технологијама.
- Од ефикасности контрола базираних на информационим технологијама зависи поузданост електронских доказа ревизије.

Опште разумевање информационих технологија

Разумевање окружења информационих система на нивоу предузећа

- Идентификовање значајних апликација и инфраструктуре

Сврха

- Однос који постоји између значајних процеса и апликација
- Однос који постоји између апликација и инфраструктуре

Циљеви контрола базираних на информационим технологијама

Контроле базиране на информационим технологијама дефинисане су на такав начин да обезбеде остваривање контролних циљева који се односе на захтеве за обезбеђење сигурности информација. Основни циљеви ових контрола су следећи:

Поверљивост:
Доприноси заштити поверљивих информација од злоупотребе од стране неовлашћених корисника. На пример:
- финансијски подаци,
- бројеви кредитних картица;
- бројеви социјалног осигурања.

Напомена: Овај циљ се директно односи на интерне и екстерне захтеве за заштиту приватности података.

Интегритет:
Штити интегритет значајних ресурса информационих технологија, као што су:
- хардвер (“Hardware”),
- софтвер (“Software”),
- база података.

Расположивост:
Обезбеђује расположивост значајних ресурса информационих технологија (нпр. хардвер, софтвер, подаци).

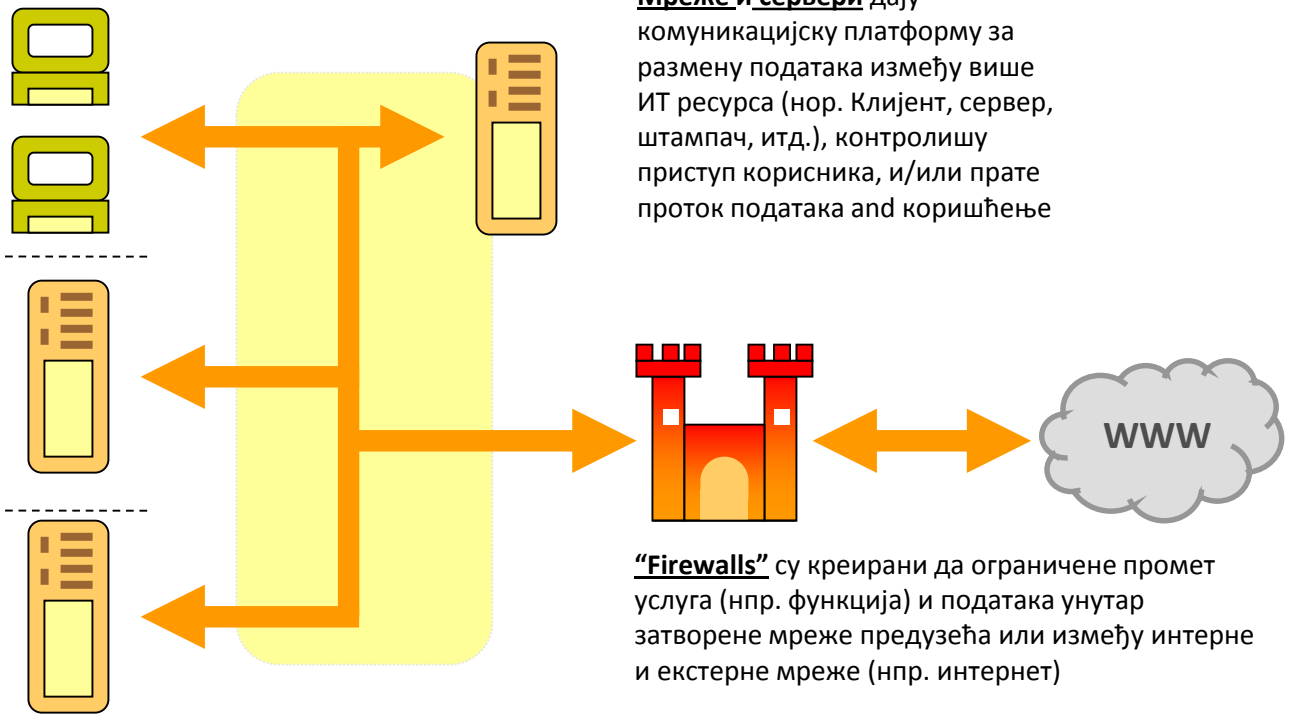
Терминологија и типологија информационих технологија

- Архитектура информационих система у организацијама разликује се у зависности од специфичних пословних захтева. Наредни графички приказ даје поједностављен приказ основних компоненти и појмова:

Персонални рачунари, за које се често користи појам **клијенти**, или "хост" апликација на хардверу или средство приступа ресурсима путем мреже (интранет или интернет)

У случају постојања изузетно интензивних апликација, по питању коришћења ресурса (нпр. ERP, итд.), организације се ослањају на **апликационе сервере** ради процесирања информација

Апликациони сервери су често допуњени са **серверима база података**, које служе као "домаћин" серверима база података који се користе за чувања података апликације



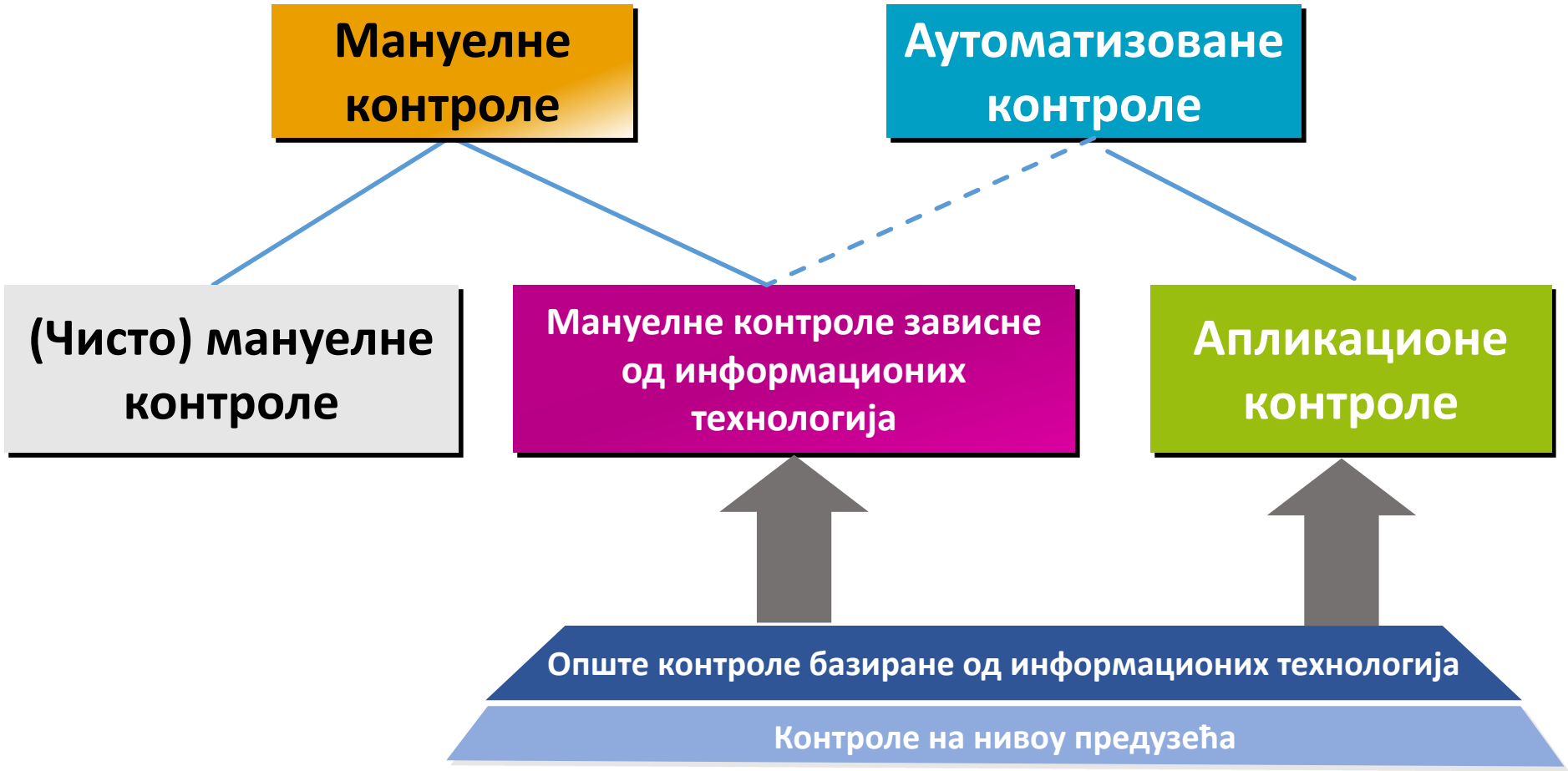
Мреже и сервери дају комуникацијску платформу за размену података између више ИТ ресурса (нор. Клијент, сервер, штампач, итд.), контролишу приступ корисника, и/или прате проток података and коришћење

"Firewalls" су креирани да ограничене промет услуга (нпр. функција) и података унутар затворене мреже предузећа или између интерне и екстерне мреже (нпр. интернет)

Преглед контрола базираних на информационим технологијама

- Када говоримо о контролама базираним на информационим технологијама разликујемо две основне категорије**. Апликационе контроле**, које се налазе у оквиру “стандардних” пословних процеса (нпр. набавка, приходи, итд.), и које обезбеђују аутоматизам контролних функција, и **опште контроле базиране на информационим технологијама (ITGC),** које пружају потпору захтевима контрола у оквиру стандардних процеса подршке базираних на информационим технологијама.

Класицификација контрола



Аутоматизоване наспрам мануелних контрола

- Контрола може бити и аутоматизована и мануелна.

Аутоматизоване наспрам мануелних контрола (наставак)

Техника контроле	Аутоматизована компонента	Мануелна компонента
• Ауторизација: Трансакције су одобрене у складу са општим и посебним принципима и политикама управе.	• "Online" праћење ауторизације	• Мануелно одобрење са мануелним потписом
• Очекивање: Генерисање извештаја којима се нешто прати; резултати се анализирају до краја.	• Аутоматизована излазна контрола базирана на очекивањима идентификованим током обраде података.	• Анализа и правовремено разрешење очекивања
• Контроле интерфејса: Комплетан и тачан трансфер података између система.	• Аутоматизована праћење преноса података и корекција грешака	• Анализа и правовремено разрешење очекивања

Аутоматизоване наспрам мануелних контрола (наставак)

Техника контроле	Аутоматизована компонента	Мануелна компонента
• Подела дужности: Подела дужности и одговорности за ауторизовање трансакција, евидентирање трансакција, и заштита.	• Параметри приступа су систему у складу са одговорностима запосленог	• Одговарајућа подела одговорности
• Приступ систему: Ограничења која постоје за кориснике унутар информационог система – окружење, утврђена и дефинисана путем права приступа конфигурисаних у систему.	• Контролна листа одобрења и приступа • Параметри приступа систему у складу са одговорностима запосленог	• Одобрења ауторизације • Периодична анализа и праћења приступних профила корисника

Мануелне контроле зависне од информационих технологија

- Контроле које врши особа, уз ослањање на резултат аутоматизованог процеса
- То су углавном детекционе контроле које се ослањају на компјутерске информације или на рад компјутера.
- На пример, менаџмент анализира недељне извештаје о очекиваним резултатима, и истражује значајна очекивања. Пошто се менаџмент ослања на компјутерски извештај да би идентификовао очекивања, ми такође утврђујемо да ли постоје контроле чији је циљ да обезбеде комплетност и тачност тог извештаја.

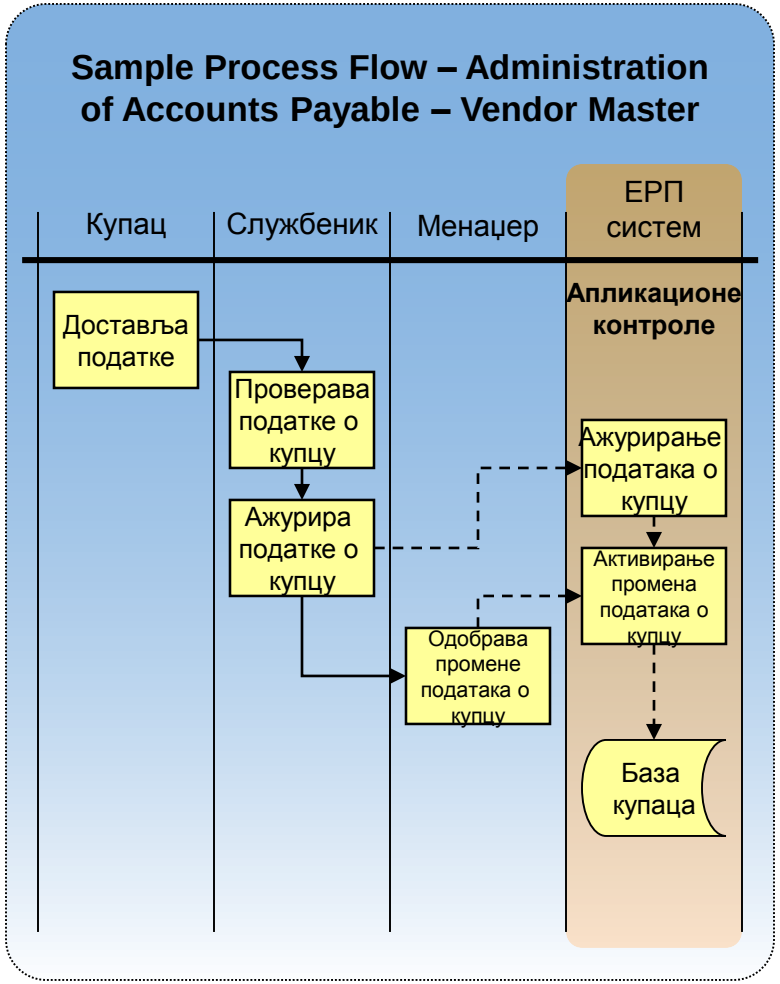
Мануелне контроле зависне од информационих технологија

- Врсте контрола зависних од информационих технологија
  - Стандардни извештаји креирани у систему
  - Упитници/”ad-hoc” извештаји
- Питања у вези тестирања
  - За које сврхе се извештај користи?
  - Како се користе за сврхе контроле?
  - Комплетност, тачност, интегритет и постојање
  - Поновна калкулација

Апликационе контроле

Апликационе контроле су системске контроле у оквиру стандардног пословног процеса, чија је сврха увођење специфичних захтева. Апликационе контроле су по природи превентивне контроле. Ово су примери контрола:

- Контроле логичког приступа
- Контроле уноса података/тачности уноса (нпр. провера тачности уноса броја кредитне картице)
- Правила функционалности (нпр. електронски рутинг и потпис налога за набавку)
- Унете вредности базирају се на унапред дефинисаним вредностима (нпр. вредности у ценовнику)
- Радни кораци базирају се на унапред дефинисаној транзицији статуса (нпр. отворено > анализирано > затворено)
- Аутоматизовани ревизорски уноси
- Аутоматизоване калкулације



Примери за процес набавке

- Захтеви за набавку су одобрени “online” на основу ауторизација одобрених од стране менаџмента.
- Налози за набавку праве се само за одобрене захтеве за набавку.
- Фактуре се плаћају тек након спровођења троструког повезивања између налога за набавку, налога за пријем (пријемнице) и налога за отпрему (отпремнице).

Неадекватан дизајн апликационих контрола

Узети у обзир препоруке за напредовање

Апликационе контроле – “ход кроз систем”

Због чега радимо “ход кроз систем”?

- Да бисмо потврдили наше разумевање процедура процеса
- Да бисмо потврдили да контроле функционишу
- Да бисмо упоредили како крајњи корисник разуме функционисање апликационих контрола у односу на то како оне стварно раде

Тестирање апликационих контрола

- Заинтересовани смо за следеће компоненте апликационих контрола:
  - Параметри конфигурације и аутоматизоване контроле
  - Контрола и приступ базама података
  - Заобилажење контрола
  - Подела дужности и функција приступа
  - Контроле у оквиру интерфејса

Тестирање апликационих контрола (наставак)

- Како тестирати апликационе контроле:
  - Зависиће од врсте апликације (нпр. САП, ЈД Едвардс)
  - Зависиће од тога да ли је апликације креирана у складу са специфичним захтевима купца или не
- Основни кораци при тестирању:
  - Утврдити начин на који је систем конфигурисан
  - Урадити тест трансакције у оквиру апликације
  - Тестирати сигурност приступа функцијама за конфигурисање система
  - Тестирати управљање променама

Интерфејс и тестирање контрола интерфејса

- Интерфејс **НИЈЕ** контрола; он је део процеса.
- Интерфејс може бити:
  - Потпуно аутоматизован
  - Делимично аутоматизован
  - Мануелан
- Контроле око интерфејса морају да обезбеде тачност, комплетност и правовременост у кретању података.

Интерфејс и тестирање контрола интерфејса (наставак)

Врсте интерфејс контрола:

- Извештаји о очекивањима
- Усаглашавања
- Двоструко тестирање
- Аутоматизовано праћење, детекција и корекција грешака
- Ограничен приступ програмима интерфејса
- Контроле везане за управљање променама у окружењу интерфејс програма

Интерфејс и тестирање контрола интерфејса (наставак)

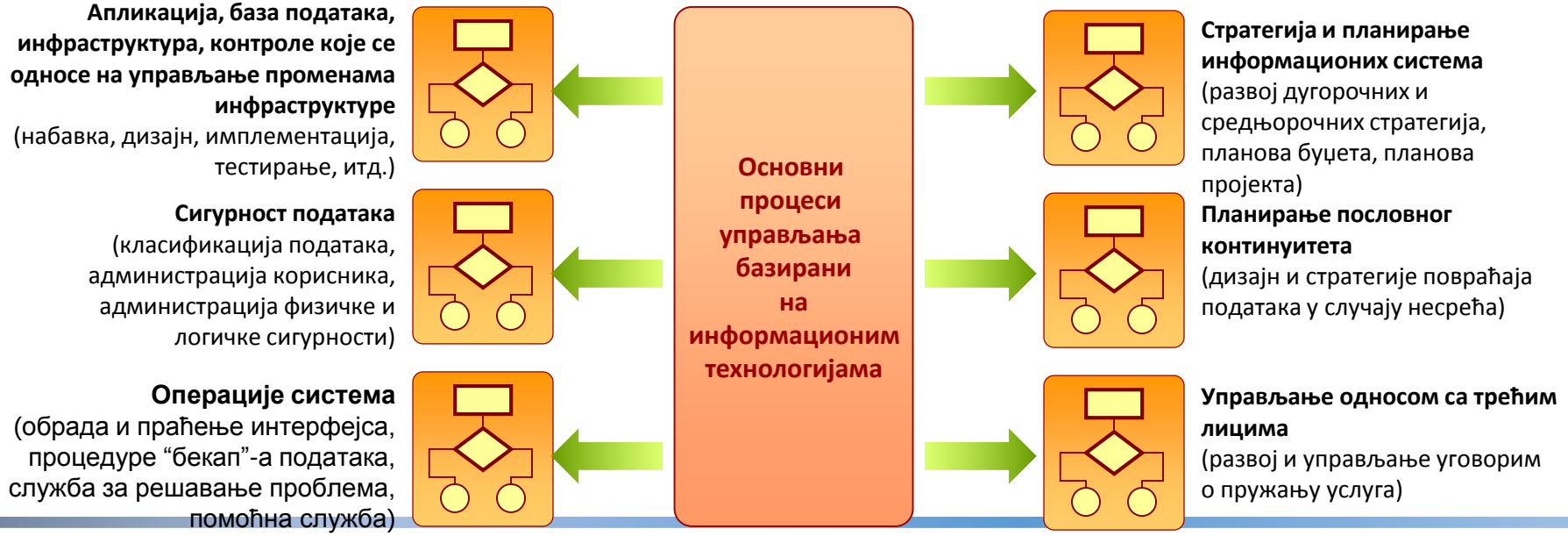
- Одговарајућа комбинација интерфејс контрола варираће у зависности од врсте и комплексности интерфејса.
- Процедуре за тестирања интерфејс контрола исте су као и за тестирање мануелних или аутоматизованих контрола.

Опште контроле базиране на информационим технологијама - дефиниција

- Дефинишу се као “контроле које имају широк утицај на системе за подржавање процеса који су предмет ревизије, укључујући и контроле од којих су друге контроле (било мануелне или аутоматизоване) зависне.”
- То су процеси које функција, зависна од информационих технологија, користи за управљање и контролу окружења информационих технологија (људи, процеси, технологија).
- Опште контроле зависне од информационих технологија пружају поверење да процеси зависни од информационих технологија конзистентно функционишу.

Опште контроле базиране на информационим технологијама - преглед

- Опште контроле базиране на информационим технологијама (ITGC) дизајниране су на начин да омогуће остваривање циљева поверљивости, интегритета и расположивост. ITGC пружају критичну подршку интегритету процеса, података и апликационих функција базираних на информационим технологијама, и налазе се у оквиру следећих традиционални управљачких функција/процеса базираних на информационим технологијама. ITGC могу бити мануелне и аутоматизоване:



Тестирање општих контрола базираних на информационим технологијама

- Тестирање апликационе контроле или мануелне контроле зависне од информационих технологија пружа поуздање да су контроле ефикасности функционисале у том тренутку.
- На који начин долазимо до поуздања да су ове контроле функционисале током целе пословне године, или да ће наставити са функционисањем?
  - Вршимо процену и тестирање општих контрола базираних на информационим технологијама.

Основне опште контроле базиране на информационим технологијама

Приступ програмима и подацима

- Механизми безбедносних контрола
- Снажан систем или корисничке идентификације
- Процедуре безбедносних контрола
- Подела дужности

Приступ програмима и подацима – механизми безбедносних контрола

Циљ: Утврдити да ли је логички и физички приступ ресурсима информационих технологија на одговарајући начин ограничен.

Елементи битних контрола и питања која треба узети у обзир приликом тестирања:

- Приступ информационим ресурсима ограничен је само на ауторизоване појединце.
- Јединствене корисничке идентификације обезбеђују постојање индивидуалне одговорности.
- Постоје комплексне лозинке за приступ.
- Постоје ефективни механизми логовања и менаџмент анализе.

Промене програма – ауторизоване промене и значајне процедуре

Циљ: Утврдити постојање контрола које обезбеђују да су све промене система одобрене од стране одговарајућег нивоа менаџмента.

Елементи битних контрола и друга питања:

- Организација има установљене процесе управљања променама.
- Сви захтеви за промене система/апликације се документују.
- Ревизорски траг промена који се може пратити све до иницијалних захтева

Промена програма – тестирање промена програма

Циљ: Утврдити постојање контрола које обезбеђују да су све промене апликација тестиране, оцењене и одобрене пре имплементације.

Елементи битних контрола и друга питања:

- Установљено је окружење за тестирање које је независно од производње.
- Само мали број особа треба да има приступ да пренесе промене у производњу.

Методи тестирање компјутерских операција

- “Бекап”/повраћај података
- Тестирање “бекап”-а и повраћаја података
- Приступ “бекап” медијима и местима за чување података
- Управљање проблемима

Компјутерске операције – “бекап”/повраћај

Циљ: Утврдити да ли је менаџмент имплементирао одговарајуће процедуре чувања и безбедности података, трансакција и програма.

Елементи битних контрола и питања која треба узети у обзир приликом тестирања:

- Одговорност за вршење “бекап”-а додељена је особљу из сектора информационих технологија.
- План вршења “бекап”-а и захтеви за задржавање програма/података су дефинисани и у употреби.
- “Бекап” се чува на одвојеном и сигурном место на ком им се може лако приступити када настане потреба за тим.

Компјутерске операције – приступ “бекап” медијима и местима за чување података

Циљ: Утврдити да постоје одговарајуће контроле над “бекап” медијима у оквиру система и апликација, али такође да ли само ауторизоване особе имају приступ “бекап” тракама и местима где се чувају.

Елементи основних контрола и питања која треба узети у обзир приликом тестирања:

- “Бекап” медији се локално одржавају и обезбеђени су од неауторизованог приступа.
- Користе се контроле физичког и логичког приступа у циљу спречавања неауторизованог приступа “бекап” подацима.

Компјутерске операције – управљање проблемима

Циљ: Утврдити да је менаџмент правовремено дефинисао и имплементирао процедуре управљања проблемима у циљу евидентирања, анализе и разрешења инцидената, проблема и грешака у системима и апликацијама.

Елементи основних контрола и питања која треба узети у обзир приликом тестирања:

- Постоји формално праћење окружења производње.
- Бележење и извештавање о свим инцидентима у производњи се прате до разрешења.
- Сви инциденти/грешке које је корисник идентификовао се бележе/приказују у извештајима и истражују до разрешења.

Тестирање општих контрола базираних на информационим технологијама

Циљ: Оценити дизајн и функционалну ефективност контрола.

- Ефективност дизајна:
  - Документовање општих контрола зависни од информационих технологија.
  - “Ход кроз систем” општих контрола зависни од информационих технологија или упити и посматрање.
  - Оценити недостатке.
- Функционална ефективност:
  - Тестирати контроле.
  - Оценити функционалне недостатке.

Ефективне опште контроле базиране на информационим технологијама

Када опште контроле базиране на информационим технологијама функционишу на планиран начин оне:

- **Пружају** основу за стицање поуздања да системи конзистентно функционишу и да ће наставити да функционишу
- **Не пружају** основу за стицање поуздања о тачности извештаја и обраде података

Физичке контроле и контроле окружења

Шта мора да буде заштићено:

- Људски живот (запослени, посетиоци, уговорне стране, итд).
- Средства предузећа (зграда, опрема, итд.)
- Софтвер и хардвер
- Информације и подаци
- Радне процедуре
- Окружење

Физичке контроле и контроле окружења (наставак)

Претње и слабости:

- Претње из окружења (земљотреси, пожари, поплаве, тероризам, вандализам, итд).
- Претње које долазе од средстава компаније (електрична струја, клима уређаји, уређаји за грејање, комуникационе линије, итд.)
- Неовлашћен физички приступ
  - Крађа опреме, компјутерских уређаја, физичких и електронских података, докумената, итд.)
  - Модификовање и неодговарајући приступ информацијама и подацима
  - Лако кварљиви електронски уређају и вандализам
  - Заобилажење интерних логичких контрола и одложена обрада
- Људске грешке
- Грешке у хардверу

Физичке контроле и контроле окружења (наставак)

Чување и контроле:

- Процедуре и политике физичког обезбеђења
- Контролни системи на бази електронског приступа
- Алармни систем против провале
- Обезбеђење у просторијама предузећа, испред улаза у предузеће, други против провални системи
- Противпожарни уређаји и противпожарне процедуре
- Непрекидно снабдевање струјом, помоћни генератори
- Температура, уређаји за праћење влажности, клима уређаји
- Заштита каблова и опреме
- Процедуре функционисања опреме и одржавање
- Многе друге …

Контроле логичког приступа

- Могућност приступ јесте способност да се нешто уради са компјутерским ресурсима (нпр. Користе, мењају, итд.)
- Контрола приступа јесте средство којим је та могућност експлицитно ограничена (обично путем физичких или системских контрола)
- Контролама логичког приступа одређено је не само ко или шта (нпр. у случају процеса) ће имати приступ специфичних информационим ресурсима, већ и врста дозвољеног приступа.

Контроле логичког приступа (наставак)

- Критеријуми за приступ систему (критеријуми за одобравање или одбијање приступа систему)
    - Идентитет
    - Улога
    - Локација
    - Време
    - Трансакција
- Основни облици приступа
    - Приступ систему у циљу уноса података
    - Приступ систему у циљу брисања података
    - Приступ систему у циљу тражења података
    - Приступ систему у циљу извршења наредби

Пример типичан тест контрола логичког приступа

Одабрати популацију постојећих или нових корисника и изабрати узорак.

- Потврдити да је ниво приступа у складу са улогом запосленог

Идентификовати популацију корисника којима више није дозвољен приступ систему, по основу тога што су напустили предузеће током вршења ревизије, и изабрати узорак из те популације.

- Потврдити да је дозвола за приступ избрисана или онемогућена

Идентификација и аутентификација

- Идентификација је начин на који корисник открива свој идентитет систему
- Аутентификација јесте средство којим се проверава тачност захтев
  - Нешто што појединац зна (тајна, нпр. лозинка, матични броја ЈМБГ)
  - Нешто што појединац има (јединствени број за приступ систему)
  - Нешто што појединац јесте (биометријске карактеристике – глас, динамика писања, или отисак приста)

Вежбање у групама

Питања и одговори

Концепти проневере

Циљеви предавања

По завршетку ове сесије бићете у могућности да:

- Разумете концепт проневере
- Демонстрирате већи степен свесности приликом ревизије о могућности постојања проневера
- Идентификујете изворе података за идентификовање ризика од проневере
- Идентификујете елементе професионалног скептицизма
- Идентификујете превентивне и детективне контроле у циљу спречавања настанка проневера

Шта подразумевамо под проневером?

Одговори

Измењени подаци у извештајима

Недозвољена апропријација

Намерна проневера у корист или на штету организације извршена од стране лица унутар, или ван организације

Врсте проневере

Од стране менаџмента

- Манипулација књиговодственим подацима (проневера менаџмент је нетачно финансијско извештавање).

Од стране запосленог

- Крађа средстава предузећа (готовине, залиха, итд.) (проневера запосленог јесте провера коју је запослени извршио на штету организације).

Свест о постојању проневере

Проневера

- Намерна превара са циљем остварења неисправног или незаконитог износа добитка

Грешка

- Радња, тврдња или уверење које ненамерно одступа од тачног, правог, или истинитог

Питања у вези проневере

За потребе ревизије финансијски извештаја:

- Проневера се дефинише као намерна радња извршена од стране једне или више особа из групе менаџмента, запослених или трећих лица, чија је последица грешка од материјалног значаја у финансијским извештајима.

Морају постојати следећа три елемента:

- Погрешне тврдње од материјалног значаја
- Намера да се превара изврши
- Ослањање “жртве” на тврдње и насталу штету

Питања у вези проневере (наставак)

Проневера наспрам грешке:

- Грешка се дефинише као ненамерна погрешна тврдња у финансијским извештајима.
- И проневера и грешка узрокују настанак погрешних тврдњи у финансијским извештајима. Основни фактор којим се разликује проневера од грешке јесте да ли је радња која је узроковала настанак погрешне тврдње намерна радња или не.

Ко врши проневеру и зашто?

Не постоји “општи профил за проневеру”…

Сумњив је свако ко има прилику да изврши проневеру, по притиском је да изврши проневеру, или подржава вршење проневере…

Запослени: Јелена Јелић

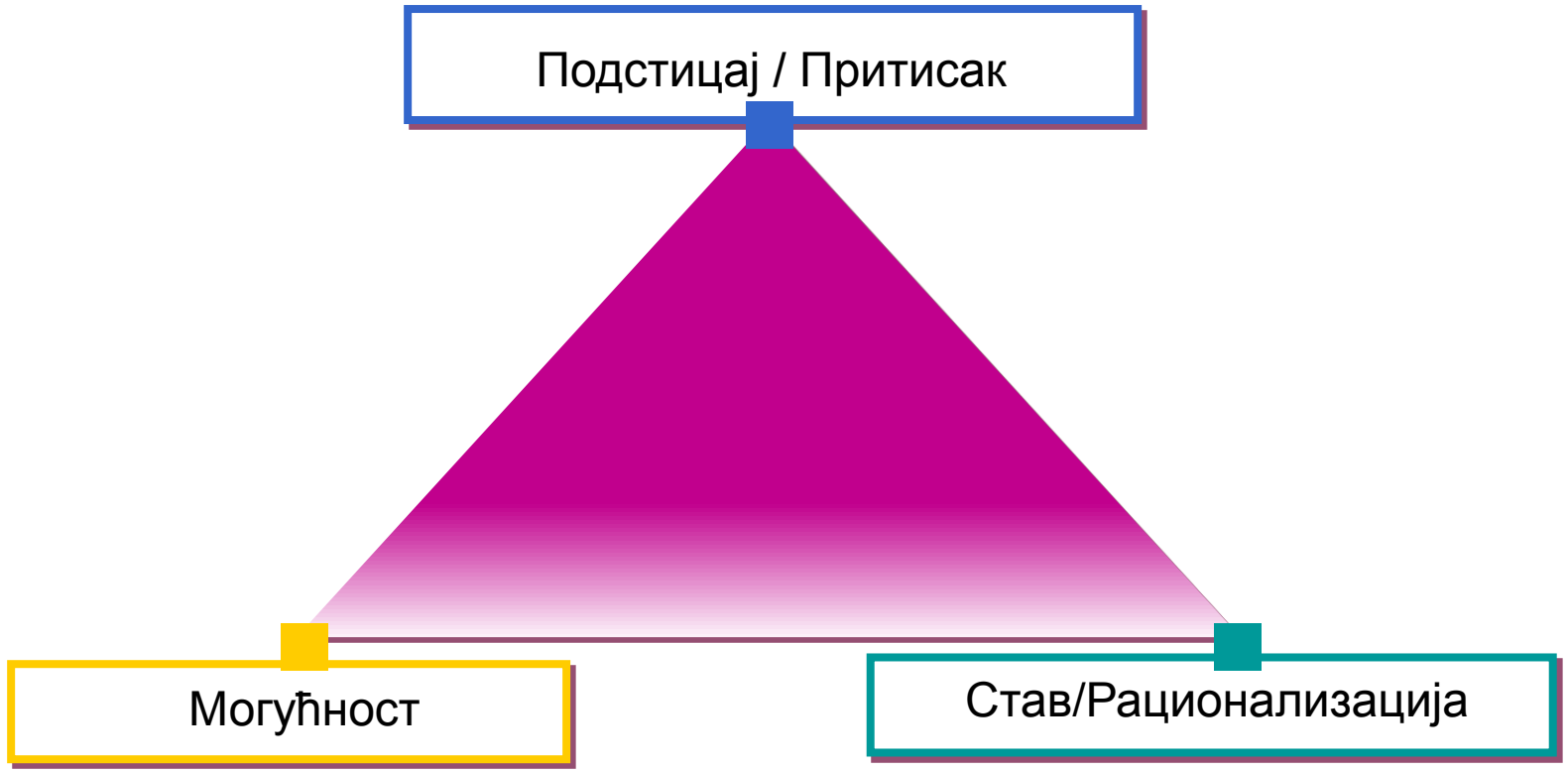
Позиција: Финансијски службеник

Одговорност: Евидентирање прилива средстава и усаглашавање стања средстава са изводом

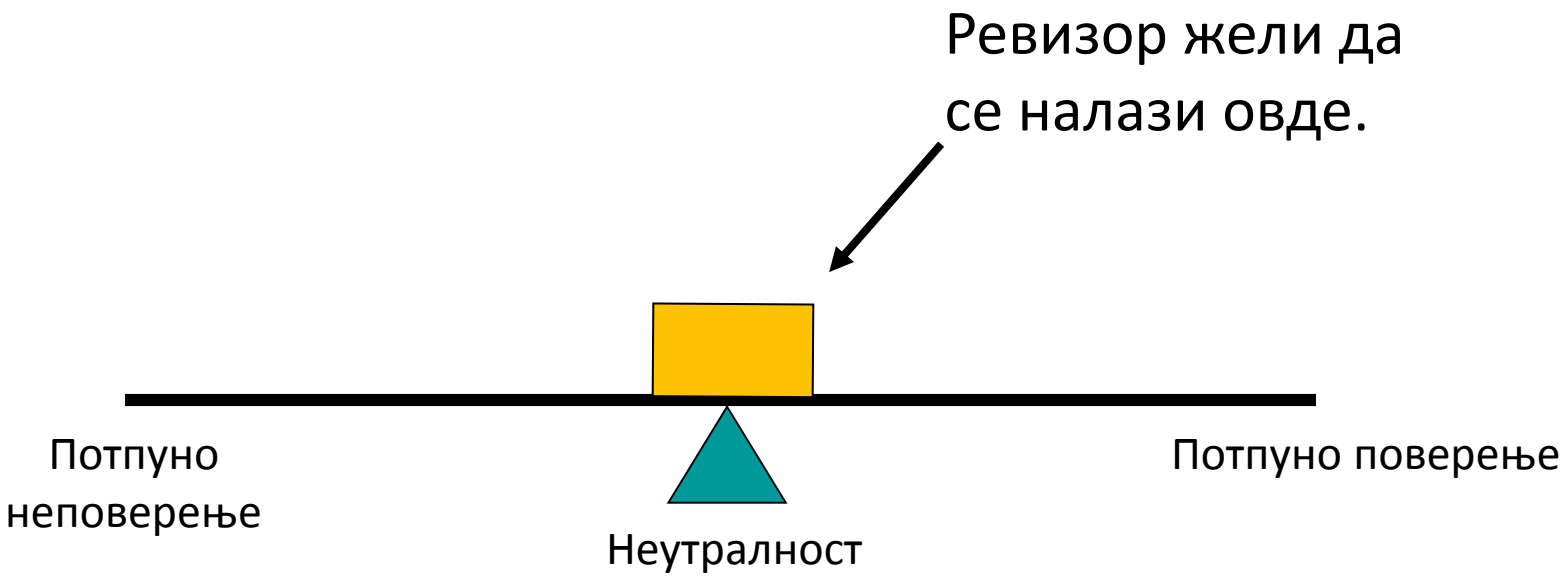
Укупно година у организацији: осам година

Породично стање: Самохрана мајка са троје деце. Једно дете болује од болести које мајчино здравствено осигурање не покрива.

Троугао проневере



Циљ ревизорског рада



Професионални скептицизам

Професионални скептицизам је став који подразумева следеће:

- Радознао ум и критичан став према доказима.
- Признавање да постоји могућност постојања проневере, без обзира на претходна искуства са организацијом.
- Спремност да постоје ревизорски докази који противречи или стављају под питање поузданост докумената или излагања менаџмента.
- Воља да се изазове и испрати до краја све што нема смисла.

Ризици од проневере: Индикатори

- Запослени не поштују контроле и процедуре система
- Дослух запослених са купцима/добављачима услуга
- Неадекватно разумевање процеса од стране менаџмента
- Слабе контроле праћења: постојање неразјашњених изузетака
- Запослени живи изнад свог стандарда
- Одсуство поделе дужности (посебно у областима где се манипулише новцем)

Одговорности интерних ревизора

- **Од интерних ревизора се не очекује да буду експерти за област истраживања проневере**
- **Од интерних ревизора се очекује да имају довољно знања:**
  - Да идентификује индикаторе проневере.
  - О карактеристикама проневере, техникама за извршење проневера, и о врстама проневера везаних за активности које су предмет ревизије.
  - Да стекне мишљење о адекватности и ефективности процеса управљања ризиком, контролних процеса и процеса управљања.
  - О вероватноћи настанка значајних грешака, неправилности, или неусаглашености.

Основни индикатори проневере: Невербални индикатори

- Изрази лица
- Додиривање носа или лица
- Непрестано трептање очима или потпуно одсуство трептања
- Грицкање усна или стискање усна
- Стављање баријера испред уста
- Одсуство контакта очима
- Немирне руке
- Приметна узнемиреност при савијању руку или ногу

Основни индикатори проневере: Вербални индикатори

- Тон говора
- Избегавање давања одговора на питање
- Усмеравање одговора на другу ствар или појединца
- Другачије објашњавање истог питања када се траже детаљнији одговори
- Причање у другом или трећем лицу
- Несигурност у говору

Начини да се избегне проневера - застрашивање

- Контроле застрашивањем (превенција)
  - Радње које се предузимају да се обесхрабри извршење проневере или да се умањи последица учињене проневере
  - Основни механизми за спречавање проневера у организацији су:
    - Окружење организације
    - Реални циљеви
    - Политика предузећа
    - Политика ауторизације
    - Канали комуникације

Начини да се избегне проневера – детекција

- Детекционе контроле
  - Оценити резултате контролних процедура менаџмента и тестова контрола у циљу детекције индикатора проневере
  - Прихватити да приликом ангажмана у интерној ревизији морамо:
    - Имати довољно знања о карактеристикама проневере
    - Бити свесни постојања могућности за вршење проневере
    - Да оценимо индикатора проневера

Све трансакције

Вероватноћа једне у узорку ако је величина популација 100.000

Број проблематичних трансакција

Величина узорка	10	15	25	50	100
25	0.002	0.004	0.006	0.012	0.025
50	0.005	0.007	0.012	0.025	0.049
100	0.010	0.015	0.025	0.049	0.095
250	0.0250	0.037	0.061	0.118	0.221
500	0.049	0.072	0.118	0.222	0.394
1000	0.096	0.140	0.222	0.395	0.634

Ризик од проневере

ПРИМЕР ЗА ДИСКУСИЈУ

Одливи готовине – “Шема лажног купац”

Општи ризици

Одливи готовине – лажни купац:

- Подаци са лажних докумената унети су у систем за плаћање.
- Фактура је од “консултанта” за “пружене услуге”.
- Одобрење за плаћање је кривотворено.
- Средства су депонована на текућем рачуну консултанта.

Индикатори

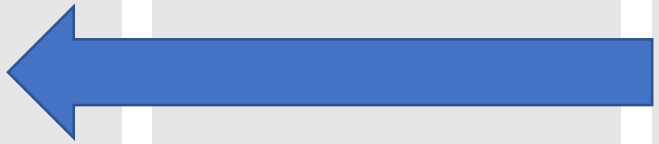
- Јединствена форма фактура
- Непознат купац/уговорна страна
- Адреса:
  - Иста као запосленог
  - Поштански факс, итд.
- На фактури није унет број телефона

Ризици проневере	Индикатори	Кораци превенције	Кораци детекције

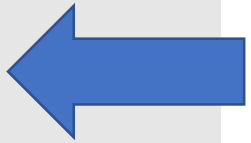
• **Одливи готовине – лажни купац:**
• Подаци са лажних докумената унети су у систем за плаћање.
• Фактура је од “консултант” за “пружене услуге”.
• Одобрење за плаћање је кривотворено.
• Средства су депонована на текућем рачуну консултанта.
	• Јединствена форма структура
	• Непознат купац/уговорна страна
	• Адреса:
	  • Иста као запосленог
	  • Поштански факс, итд.
	• На фактури није унет број телефона
		• Независна провера сваког првог плаћања
		• Периодична провера добављача са којима се мало послује
		• Провера да су роба или средства примљени пре одобрења плаћања
		• Коришћење налога за набавку
		  • Налози за набавку прави систем само за оне купце који се налази у бази.
		• Подела дужности
		  • Контрола приступа система базираног на информационим технологијама не дозвољава службенику који захтева набавку да унесе новог купца у базу података, унесе податке о новом купцу, нити да изврши плаћање.
		• Систем базиран на информационим технологијама не дозвољава да се исти налог за набавку или фактура плати два пута.
			• Коришћење налога за набавку.
			• Усаглашавање свих готовинских рачуна одмах по пријему извода банке.
			• Анализа свих поништених налога за плаћање.
			• Периодична анализа купаца и уговорних страна у циљу утврђивања њиховог постојања и законитости.
			• Анализа 100% свих месечних извештаја о извршеним плаћањима.
			• Коришћење компјутерских техника у откривању индикатора проневере.

Ризици проневере	Индикатори	Кораци превенције	Кораци детекције	Кораци рев. програма

- Тражење индикатора проневере



- Тестирање превентивних контрола



- Тестирање детективних контрола

ПРИРОДА, ВРЕМЕ И ОПСЕГ РЕВИЗОРСКИХ ПРОЦЕДУРА

Документовање проневере

Када се проневера открије, морамо да документујемо следеће:

- **Ко** је био укључен у извршење проневере?
- **Шта** је урађено да би се проневера извршила?
- **Колика** је вредност проневере?
- **Када** је проневера извршена?
- **Где** је проневера извршена?
- **Зашто** је проневера извршена?
- **Како** је проневера извршена?

Питања у вези проневере на бази информационих технологија

- Екстерна проневера на бази информационих технологија
  - Интернет/”online” проневера
    - Б2Б
    - Б2Ц
  - Крађа идентитета
  - Вируси, итд.

Питања у вези проневере на бази информационих технологија (наставак)

- Екстерна проневера на бази информационих технологија
  - Крађа средстава
  - Проневера путем финансијских извештаја
  - Узроци:
    - Мануелно заобилажење контрола
    - Злоупотреба технологије
    - Неовлашћен приступ и лоша подела дужности

Како умањити ризик од проневера на бази информационих технологија

Политике и процедуре

- Писана политика безбедности
- Обуке у циљу повећања нивоа свесности
- Процедуре процене ризика
- “Бекап” и системи за повраћај података
- Праћење и анализа ревизорских логова

Технологија

- Антивирусни програми
- “Firewalls”
- Филтери за електронску пошту
- Тестирање процедуре при нападу и упаду у систем

Закључак

Сада када сте завршили лекцију моћи ћете да: