# Методологија интерне ИТ Ревизије

# Садржај

1. Елементи у спровођењу ИТ ревизије
2. Безбедност информационих система
3. Спровођење ИТ ревизије, пример: контрола креденцијала

# Елементи у спровођењу ИТ ревизије

# ИТ управљање (IT *governance*)

- **Циљ ревизије:** Обезбедити уверење да су успостављене потребне руководеће и организационе структуре и процеси за постизање циљева и за подршку стратегије компаније.
- **Области**:
  1. Процена ИТ стратегије и процеса за развој, одобрење, имплементацију и одржавање стратегије, као и процеса усклађивања са стратегијама и циљевима организације.
  2. Процена ефикасности структуре ИТ управљања у циљу утврђивања да ли ИТ одлучивање и перформансе подржавају стратегије и циљеве организације.
  3. Процена ИТ политика, стандарда и процедура као и процеса за њихово креирање, одобрење, објављивање, имплементацију и одржавање у циљу утврђивања да ли подржавају ИТ стратегију и да ли су у складу са регулаторним и законским захтевима.
  4. Процена праћења и извештавања о кључним показатељима перформанси (КПИ) како би се утврдило да ли руководство прима довољно информација правовремено.

# ИТ управљање (IT *governance*)

Најчешће коришћени стандарди ИТ управљања *су*:

1. CobIT (верзија 2019 и претходне)
2. ISO 27000
3. ITIL - Information Technology Infrastructure Library

- Основни циљеви ИТ управљања су:
  - Да ИТ доноси вредност компанији
  - Да се адекватно управља ИТ ризиком

- Ревизија игра значајну улогу у контроли имплементације ИТ управљања:
  - Проверава усклађеност управљања компанијом и управљања ИТ-јем, као и усклађеност ИТ функције са мисијом, визијом, вредностима, циљевима и стратегијама организације
  - Проверава усаглашеност са регулативом и даје препоруке утемељене у доброј стручној пракси вишем менаџменту
  - Помаже иницијативама унапређења ИТ управљања
  - Помаже унапређењу ИТ процеса
  - Адресира финансијске аспекте ИТ-ја: ИТ инвестиције (ROI), набавке, итд.

# ИТ организациона структура

- Унутар организације, ИТ одељење (сектор, служба ...) може бити структурисано на различите начине, при чему организациона шема мора пружити јасну дефиницију хијерархије и надлежности. Најчешће ИТ функције у компанији су:
  - Управљање ИТ пројектима
  - Управљање апликативним развојем система (IT development)
  - Управљање ИТ операцијама (IT operations)
    - Управљање рачунарским мрежама и комуникацијама
  - Управљање корисничким захтевима и инцидентима (IT help / service desk)
  - Управљање информационом сигурношћу
  - Управљање набавкама
  - Управљање квалитетом (IT testing) итд.
- ИТ ревизор треба да упореди структуру ИТ, улоге и одговорности запослених у ИТ, уређеност односа са другим организационим структурама и описима послова.
- Важна контрола у ИТ-ју је сегрегација дужности, која ограничава могућност да ће једна особа бити одговорна за функције на такав начин да може доћи до прикривања грешака или проневера.

# ИТ унутрашња регулатива

Усаглашеност ИТ политика, стандарда и процедура је често обавезна провера у склопу ИТ ревизије!

- ИТ стратегија дефинише на који начин информациони системи подржавају, одржавају и помажу раст компаније. Стратешке смернице могу се дефинисани самостално или као интегралне компоненте стратегије компаније.
- Корпоративне политике су документи високог нивоа који постављају тон организације као целине. Политике на нивоу ИТ-ја као одељења дефиншу циљеве и директиве нижег нивоа.
- Корпоративни стандарди су документи који постављају посебне критеријуме и референцирају се на политике. ИТ стандарди дефинишу специфичан ниво конфигурације и перформанси.
- ИТ процедуре и радне инструкције представљају документоване, дефинисане кораке који помажу у постизању циљева политике и достизању стандарда. Да би биле ефикасне и спродовиве, процедуре морају бити правовремено измењене и комуниците извршиоцима.

# ИТ финансије, извештавање и КПИ

- Управљање ИТ финансијама - ИТ буџет треба да буде повезан са ИТ плановима и на краткорочном и дугорочном нивоу. ИТ набавке треба да буду саставни део ИТ финансијског плана. ИТ ревизор би требао да провери усаглашеност планираних и извршених набавки.
- ИТ перформансе представљају меру испуњења ИТ циљева. Више различитих алата и техника могу помоћи у праћењу и мерењу перформанси, а међу најпознатијима је *Six Sigma*. ИТ ревизор би требао да провери да ли се перформансе прате и на који начин се ова информација повратно користи.
- ИТ извештавање представља периодичну активност којом ИТ извештава менаџмент о активностима и изазовима у претходном периоду, као и плановима о наредном. ИТ извешавање најчешће је прилагођено потребама ИТ надзорног одбора (*IT steering committee*), извршног одбора или (ређе) управног одбора.

# Управљање ИТ пројектима

- Приступ управљању ИТ пројектима зависи од величине и сложености организације. Процеси управљања пројектима укључују следеће фазе :
  1. Иницирање
  2. Планирање
  3. Извршавање
  4. Контролисање
  5. Затварање
- Када анализира контекст пројекта, ИТ ревизор мора узети у обзир значај пројекта у организацији, везу између стратегије организације и пројекта, однос између конкретног пројекта и других пројеката и везу између пројекта и студије случаја (*business case*).
- Пројектна култура састоји се од заједничких норми, уверења, вредности и претпоставки пројектног тима. Култура пројекта може се дефинисати путем мисије, назива и логотипа пројекта, протокола комуникације, итд.

# Набавка, развој и имплементација (примена) информационих система

- **Циљ ревизије**: Обезбедити уверење да су успостављени неопходан оквир и пракса за набавку, развој, тестирање и имплементацију информационих система који испуњавају стратегију и циљеве организације.
- **Области**:
  1. Процена предложених улагања у набавку, развој, имплементацију, одржавање и накнадно повлачење из употребе информационих система у циљу уверења да исти испуњавају пословне циљеве.
  2. Процена оквира (методологије) за управљање пројектима у циљу уверења да су пословни захтеви постигнути на економичан начин уз управљање ризицима.
  3. Процена контрола информационих система током фаза набавке, развоја и тестирања у складу са политикама, стандардима, процедурама организације и спољним захтевима.
  4. Спровођење евалуације система наком имплементације у циљу уверења да су успостављење адекватне контроле и испуњени захтеви пројекта и организације.

# Ревизија аквизиције и развоја апликативних система

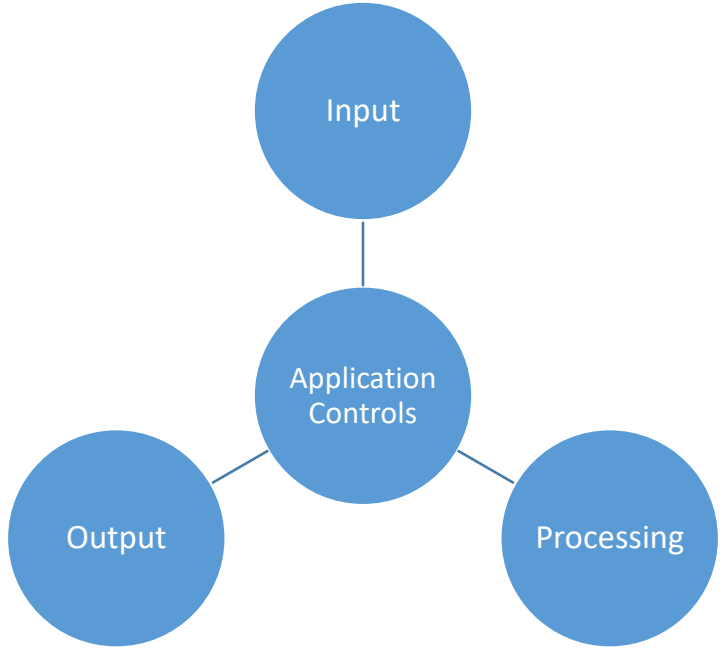
- Уобичајено, ИТ ревизор требао би прегледати следећу документацију у циљу стицања разумевања процеса аквизиције и / или развоја апликативних решења:
  - Методологију развоја информационих система
  - Спецификације функционалног дизајна / пројектну документацију
  - Записе / дневник измена - логове
  - Осталу техничку документацију
  - Корисничка упутства

- Задаци ИТ ревизора у процесу ревизије аквизиције и развоја апликативних система су следећи:
  - Идентификација кључних и значајних компоненти апликације и ток трансакција
  - Идентификација контролних система апликације и процена утицаја слабости контрола
  - Адекватност стратегије тестирања, првенствено тестирања кључних контрола како би се осигурала њихова адекватност, функционалност и ефикасност.

# Развој апликативних решења (апликација)

- Развој и одржавање апликација представља процес управљања дизајном, кодирањем („програмирањем“), тестирањем и уклањањем грешака софтвера (“багови“), као и сталним унапређењима.

- Кључне контроле:
  - Контроле улаза (*input*): Технике и поступци који се користе за верификацију, потврђивање и уређивање података како би се осигурало да се у рачунар уносе само тачни подаци
  - Контроле обраде (*processing*): Поступци обраде требају да осигурају поузданост обраде апликативних решења.
  - Контроле излаза (*output*): Излазне контроле пружају сигурност да ће се подаци достављени корисницима представити и форматирати на доследан и разумљив начин.



# Апликативне контроле

| Унос | Обрада | Излаз |
|---|---|---|
| Унос мора да буде ауторизован (одобрен). Типови ауторизације укључују:<br>• Контроле приступа<br>• Јединствене лозинке<br>• Идентификација терминала или радне станице клијента итд.<br><br>Додатне контроле уноса су:<br>• Очекиване вредности / опсег<br>• Укупан износ<br>• Укупан број ставки<br>• Hash / check sum вредности итд. | Обрада мора да буде ефикасна и тачна, као и да се извршава над унетим подацима који су проверени улазним контролама. Неке од контрола обрада су:<br>• Провера редоследа<br>• Ограничена провера на узорку<br>• Провера опсега<br>• Провера валидности<br>• Провера оправданости<br>• Провера постојања у шифарницима<br>• Верификација кључева<br>• Контролни бројеви и суме<br>• Провера комплетности<br>• Провера дуплираних уноса<br>• Разне логичке провере итд. | Неке од контрола које прикази резултата обраде морају да задовоље су:<br>• Приказ свих резултата обраде<br>• Контрола комплетности приказа<br>• Контрола грешака на приказу<br>• Контрола присутпа резултатима обраде<br>• Верификација пријема извештаја<br>• Генерисање системких записа<br>• Контрола тачности приказа итд. |

# Тестирање апликативних контрола

- Процесом тестирања се утврђује
  - да су захтеви корисника имплементирани,
  - да систем ради онако како је предвиђено,
  - да унутрашње контроле раде како је планирано.

- Два основна приступа тестирању укључују :
  - „Одоздо на горе“ (*bottom up*) — Тестирају се прво најмање појединачне целине, а затим односи између њих у већим целинама горе док се не спроведе комплетно тестирање система.
  - „Одозго на доле“ (*top down*) — Тестира се комплетан систем, преко већих појединачних целина (нпр. модула) према доле, до појединачних целина.

# Типови тестирања

## Тестирање целина

- Тестира се програмска логика у појединачним целинама или модулима
- Циљ је обезбедити потврду да се интерне операције у оквиру целине извршавају у складу са функционалном спецификацијом
- Користи се сет тестних сценарија и корака чији је фикус на контролној структури процедуралног дизајна

## Тестирање интерфејса и интегративности

- Хардверски или софтверски тест који треба да потврди да везе / конеције између две или више компоненти или система успешно преносе информације једна ка другој

## Системско тестирање

- Серија тестова која треба да осигура да се измене или нова апликација успешно интегрису у остатак информационог система

## *Final acceptance testing*

- Тестирање које се извршава приликом фазе интеграције и треба да потврди да је ново стање система у потпуности усаглашено са захтевима пројекта

# *Final Acceptance Testing*

| Quality Assurance Testing (QAT) | User Acceptance Testing (UAT) |
|---|---|
| • Фокусира се на техничке аспекте апликације<br>• Потврђује да апликација ради како је документовано тестирањем логичког дизајна и саме технологије<br>• Осигурава да апликација испуњава документоване техничке спецификације и резултате<br>• Укључује минимално учешће крајњих корисника<br>• Изводи га ИТ одељење | • Фокусира се на функционалне аспекте апликације<br>• Осигурава да је систем спреман за продукцију и да испуњава све документоване захтеве<br>• Изводи се у сигурном тестном окружењу који опонаша продукционо окружење што је могуће боље<br>• Тестови се извршавају из перспективе крајњег корисника<br>• Изводи их крајњи корисници |

- Тестирање интегритета података представља скуп значајних тестова који испитују тачност, потпуност, доследност и ауторизацију података који се тренутно налазе у систему, односно свим појединачним компонентама система.
- Тестирање интегритета најчешће подрзумева тестирање валидности података у свим базама, на основу очекиваних вредности и дозвољених опсега, као и тест референцијалног интегритета, односно везе између шифарних и трансакционих табела.

# Имплементација и пуштање у продукцију

- Након успешног тестирања систем се имплементира у складу са процедурама контроле измена у продукцији; план спровођења треба припремити (много) пре датума примене.
- Сваки корак постављања продукционог окружења треба да буде документован, укључујући дефинисане одговорности, на који начин ће корак бити верификован и поступке повратка на претходно стање у случају неуспешне имплементације.

**PRE IMPLEMENTATION — активности које претходе процесу имплементације**

- Gap analysis, улоге и одговорности, динамика спровођења, контрола ризика, повратак на претходно стање у случају неуспешне имплементације и сл.

**POST IMPLEMENTATION — Успостављање метрика и кључних параметара након имплементације**

- Израда SLA са најмање следећим дефинисаним вредностима: време у коме је систем оперативан (нпр. 24/7, 9-17 и сл.), време у коме је могуће пружити подршку, време од појаве инцидента на систему до враћања у предвиђено стање и сл.

- Издрада плана  обука и трансфера знања, што укључује технички тренинг за ИТ и тренинг за крајње кориснике

# Одржавање система у продукцији – управљање променама

- Након имплементације, систем улази у текућу фазу развоја или одржавања. Пракса одржавања система односи се пре свега на процес управљања променама у апликативним системима уз задржавање интегритета измена и изворног и извршног кода. За потребне ефикасног извршавања промена, потребно је успоставити стандардни процес управљања променама.
- Управљање променама је процес документовања и одобравања свих захтева за промене. Захтеви за промену се покрећу од стране крајњег корисника или запослених у тимовима за развој и одржавање система. Процес управљања променама треба да укључи следеће процедуре:

  - Званични процес управљања променама
  - Процес тестирања промена
  - Управљање хитним променама
  - Процес имплементације промена у продукцију и
  - Управљање неовлашћеним променама

# Одржавање и управљање информационим системима - ИТ Операције

- **Циљ ревизије**: Обезбедити уверење да процеси за оперативни рад информационих система, њихово одржавање и управљање услугама испуњавају стратегије и циљеве организације.
- **Области**:
  1. Процена оквира и успостављених пракси управљања ИТ услугама у циљу утврђивања да ли је обезбеђен жељени нивоа услуга и контрола задатих од стране компаније, као И да ли су испуњени стратешки циљеви.
  2. Процена активности ИТ операција (нпр. пуштање аутоматизованих обрада, управљање конфигурацијама, управљање капацитетима и перформансама) у циљу утврђивања да ли су ефикасно контролисани и да ли подржавају циљеве организације.
  3. Процена управљања животним циклусом сервиса и опреме у циљу утврђивања да ли И даље подржавају ефикасне пословне функције
  4. Процена процеса управљања проблемима и инцидентима у циљу утврђивања да ли се проблеми и инциденти правовремено спречавају, откривају, анализирају, да ли се о њима извештава и да ли се адекватно решавају.

# Одржавање и управљање информационим системима - ИТ Операције

- Управљање ИТ услугама (*IT Service Management - ITSM*): представља подршку пословним потребама кроз имплементацију и управљање ИТ услугама. Људи, процеси и елементи информационих технологија су основни сегменти ИТ услуга.
- Основне претпоставке управљања ИТ услугама су :
  - ИТ-јем се може управљати кроз низ дискретних процеса. Ови процеси пружају „услугу“ послу и међусобно су зависни.
  - Уговори о нивоу услуге (SLA) детаљно наводе очекивања од услуга.
  - Да би се осигурао висок ниво услуге, ITSM метрике се упоређују са очекивањима из SLA -а.
- Два најпознатија оквира упрацљања ИТ услугама су *The IT Infrastructure Library* (*ITIL*) и ISO 20000-1 – Управљање услугама

# Одржавање и управљање информационим системима - ИТ Операције

- Функција ИТ операција је одговорна за сталну подршку рачунарском окружењу организације, обезбеђујући да:
  - Рачунарске обраде буду извршене
  - Информације се обрађују у сигурном окружењу
  - Крајњи корисници (интерни и екстерни) добијају предвиђени ниво услуге
- ИТ операције поступају по разрађеним процедурама и радним инструкцијама, које укључују :
  - Техничка упутства за употребу рачунарске опреме и токове информација
  - Упутсва за коришћење система и апликације за надзор и мониторнг рачунарске инфраструктуре
  - Методологију за откривање системских и апликацијских грешака и
- ИТ операције одговорне су и за извршење аутоматизованих обрада (job-ова)

# Одржавање и управљање информационим системима - ИТ Операције

- Да би апликативни системи оптимално радили, хардвер се мора редовно сервисирати. Основни документ управљања хардверском инфраструктуром представља развијен формални план одржавања, одобрен од стране менаџмента
  - Важно! Решавање непланираних хардверских инцидената може изазвати трошкове одржавања који прелазе планирани буџет!

- Управљање капацитетима реализује се кроз план капацитета (*Capacity Management Plan*), који треба да буде изграђен на основу информација добијених од стране и корисника и техничког особља, а требало би га ажурирати најмање једном годишње.

# Управљање резервним копијама

| Карактеристике | Full Backup | Incremental Backup | Differential Backup |
|---|---|---|---|
| **Опис и намена** | Копира фајлове и фолдере на бекап медијум (траке, дискове ...) | Копира фалове и фолдере који су нови или измењени у односу на последњи бекап | Копира фајлове и фолдере који су различити или новији у односу на последњи full backup |
| **Предности** | Креира се јединствена архива што убрзава процес опоравка | Захтева мање времена и мање простора у односу на full backup | Бржи од пуног бекапа; захтева само последњу пуни и последњи диференцијални бекап за опоравак |
| **Мане** | Захтева највише времена и простора | Сви претходни сетови су неопходни за пун опоравак, што захтева додатно време | Захтева више времена и простора од инкременталног бекапа |

# Управљање ИТ инвентаром и средствима

- Да би се постигли циљеви управљања ИТ инвентаром, средства морају бити прецизно идентификована. Евиденција ИТ инвентара и сваког ИТ средства треба да садржи :
  - Опште карактеристике (назив, тип, власника задуженог за одржавање итд.)
  - Вредност за организацију
  - Импликације губитка и приоритет опоравка
  - Локацију
  - Класификацију сигурности / ризика

- Управљање ИТ инвентаром основни је предуслов за развијање исправне стратегије безбедности. То је уједно и први корак у управљању софтверским лиценцама.

# Управљање инцидентима и проблемима

- Управљање инцидентима фокусира се на пружање континуитета услуге путем уклањања или смањења штетних ефеката поремећаја ИТ услуга.
- Критични елемент процеса управљања инцидентима је приоритизација инцидената - морају се узети у обзир и хитност и утицај.

**Problem Management**

- Смањује број и / или критичност инцидената
- Унапређује квалитет ИТ услуга

**Incident Management**

- Реакција на проблеме по откривању
- Основни циљ је вратити угрожени сервс у стање нормалног функционисања што је пре могуће

# Управљање проблемима и инцидентима

## Интервјуи са запосленима

- Да ли су развијене процедуре за евидентирање, анализу, решавање и ескалацију проблема и инцидентата?
- Да ли се ове радње благовремено спроводе?

## Процедуре и документа

- Да ли су процедуре за документовање, оцењивање, решавање и ескалацију проблема и инцидената адекватне?
- Да ли је прикупљање и анализа ИТ статистика адекватна, тачна и потпуна?
- Да ли су сви идентификовани проблеми евидентирани ради верификације и решавања?

## Системски логови и записи

- Да ли системски записи садрже адекватан ниво информација за потребе анализе инцидената и проблема?
- Да ли су идентификовани значајни и понављајући проблеми и предузете активности да се спречи њихово понављање?
- Постоје ли у записима понављајући инциденти и проблеми који нису документовани у складу са процедурама?

# Управљање променама у ИТ операцијама

- Процес управљања променама се спроводи у ситуацијама када је:
  - Хардвер промењен,
  - Софтвер инсталиран или надограђен,
  - Мрежни уређаји су конфигурисани.
- Управљање променама у ИТ операцијама део је ширег процеса управљања променама. Поступци се могу разликовати у зависности од врсте захтева за промену, укључујући:
  - Хитне промене
  - Велике промене
  - Мање промене

# Безбедност информационих система

# Заштита информационих система

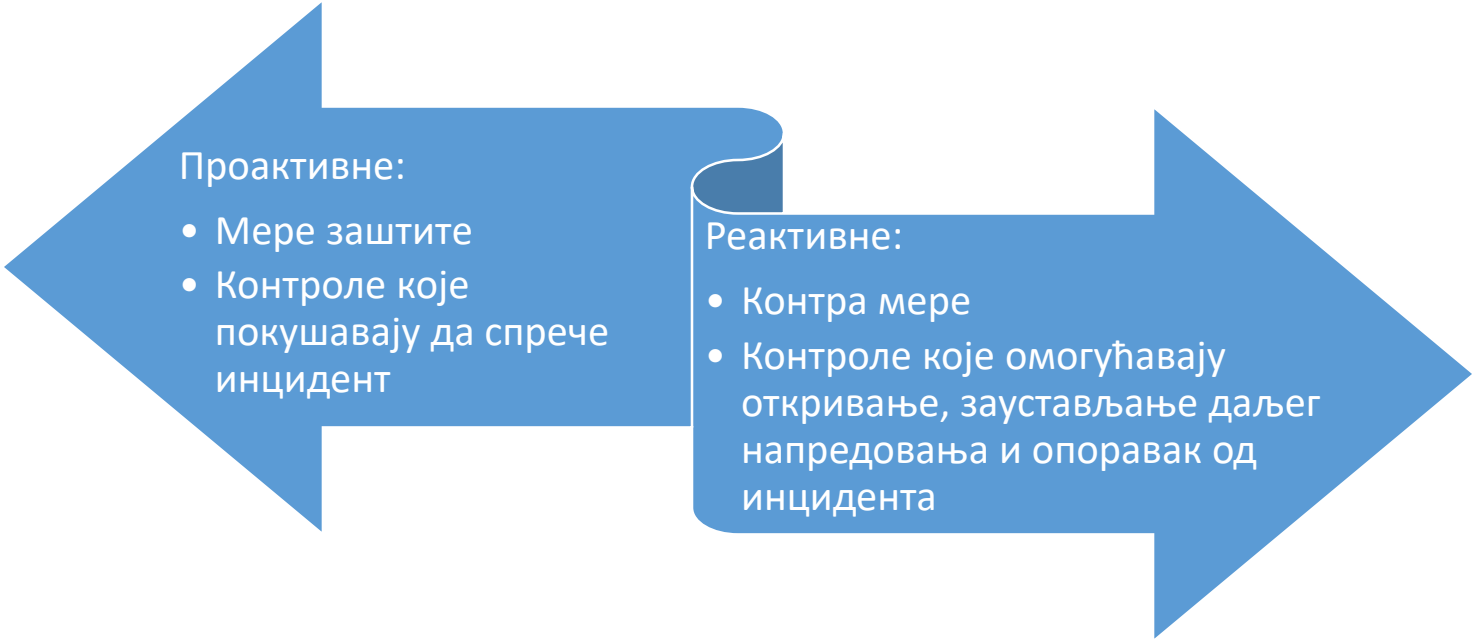
- **Циљ ревизије**: Обезбедити уверење да безбедносне политике, стандарди, процедуре и контроле обезбеђују поверљивост, интегритет и доступност информационих средстава у организацији.
- **Области**:
  1. Евалуација политика, стандарда и процедура за безбедност информација и усклађености са добром стручном праксом и важеће регулативе.
  2. Процена дизајна, имплементације, одржавање, праћења и извештавања о физичким и логичким контролама како би се утврдило да ли су информациона добра адекватно заштићена.
  3. Процена процеса и поступака који се користе за складиштење, преузимање, транспорт и одлагање информационих добара како би се утврдило да ли су адекватно заштићена.
  4. Процена процеса управљања безбедносним инцидентима у циљу утврђивања да ли се исти правовремено спречавају, откривају, анализирају, да ли се о њима извештава и да ли се адекватно решавају.

# Заштита информационих система

- Систем управљања информационом сигурношћу (*ISMS*) представља оквир политика, процедура, смерница и придружених ресурса за успостављање, примену, рад, надгледање, преглед, одржавање и побољшање безбедности информација за све врсте организација.
- ИСМС је дефинисан у смерницама серије стандарда ISO / IEC 2700X, који се најчешће користи као критеријум за успостављање *ISMS* у оквиру организације.
- Најважнији циљеви информационе безбедности као функције у служби испуњења пословних захтева организације су :
  - Стална доступност информационих система и података (***availability***)
  - Интегритет информација које се чувају на рачунарским системима (***integrity***)
  - Поверљивост података (***confidentiality***)
  - Усклађеност са важећим законима, прописима и стандардима

# Безбедносне контроле

- Ефикасна безбедносна контрола је она која спречава и / или открива инцидент и омогућава опоравак од штетног догађаја.
- Безбедносне контроле могу бити :



# Безбедносне контроле

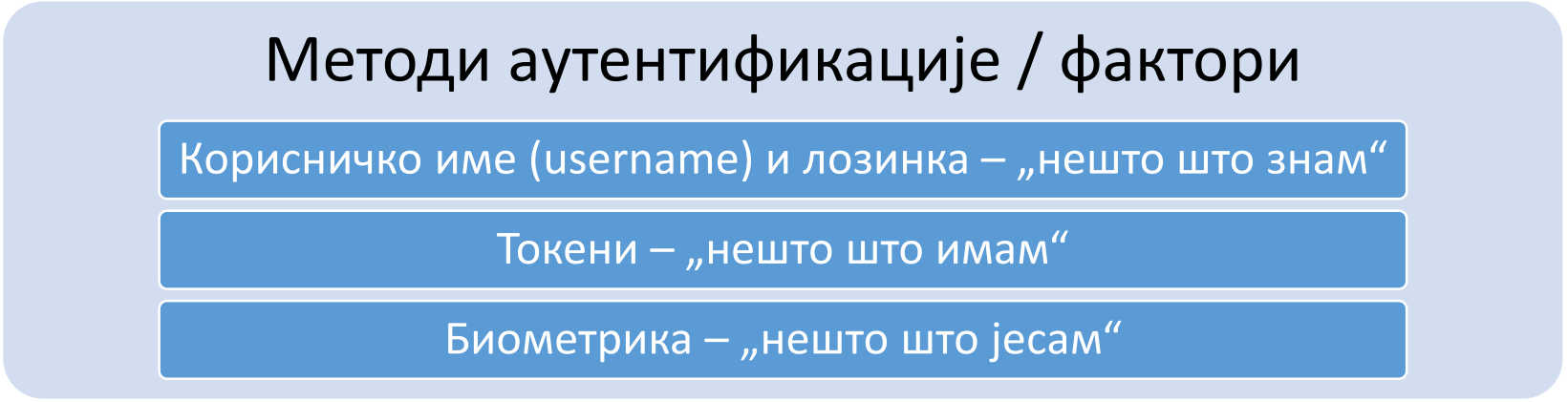
| | |
|---|---|
| Управљачке | Контроле у вези са надзором, извештавањем, поступцима и радњама сигурносних процеса. Оне укључују политике, процедуре, развој запослених и извештавање о усклађености са релевантним законским оквиром. |
| Техничке | Контроле које су познате и као логичке контроле и које се имплементирају употребом технологије, сотвера и ИТ опреме. Примери укључују фиревалл системе, мрежне или хост системе за откривање напада (IDS), лозинке и антивирусни софтвер. Техничке контроле захтевају исправно дефинисане управљачке (административне) контроле да би правилно функционисале. |
| Физичке | Разне физичке баријере попут брава, ограда, зидова, али и надзорних CCTV система и других уређаја који су инсталирани да физички ограниче приступ објекту или хардверу. Физичке контроле захтевају одржавање, надгледање и способност процене и реаговања на узбуну уколико се појави проблем и покушај компромитације. |

# Идентификација и аутенти(фи)кација

- Логичка идентификација и аутентификација приступа (I&A) је процес утврђивања и доказивања идентитета корисника. За већину система I&A је прва линија одбране, јер спречава неовлашћене особе (или неовлашћене процесе) да прођу у рачунарски систем или приступе информационин средствима.
- Неке уобичајене рањивости у I&A укључују:
  - Слабе методе аутентификације
  - Коришћење једноставних или лако погодљивих лозинки
  - Пропусте који корисницима омогућавају да заобиђу механизам за потврду идентитета
  - Одсуство енкрипције у процесима за аутентификацију и заштиту информација
  - Ниска свест корисника и ризицима повезаним са дељењем елемената за потврду идентитета

# Методе аутентификације

- Мултифакторска аутентификација је комбинација више метода аутентификације.
- *Single Sign On* (SSO) је процес обједињавања свих елемената - идентификације, аутентификације и ауторизације, у једну, централизовану административну функцију.



# Ауторизација

- Ауторизација представља скуп правила приступа која одређују који елемент информационог система (запослени, уређај, сервис ...) може чему да приступи.
- Контрола приступа се често заснива на принципу најмањих привилегија (*least privilege*), а односи се на одобравање корисницима само оних приступа који су потребни за обављање њихових дужности.
- Контролне листе приступа (*access-control list, ACL*) представљају скуп дозвола или забрана различитих типова приступа одређеном ИТ систему.
- Ризици повезани са системима ауторизације су следећи :
  - Онемогућавање услуга (*denial of service, DoS*)
  - Погрешно конфигурисан комуникациони софтвер
  - Погрешно конфигурисани уређаји на корпорацијској рачунарској инфраструктури
  - Системи нису правилно осигурани
  - Лоша физичка сигурност (последично и лоша логичка сигурност) рачунара удаљених корисника

# Логичке контроле

- Логичке контроле приступа су основне контроле које се користе за управљање и заштиту информационих средстава. Неадекватне логичке контроле омогућавају техничке изложености, односно неовлашћене активности које ометају нормалне обраде и приступе системима. То укључује :
  - „Цурење“ података односно неовлашћено копирање података неауторизованим лицима
  - Прислушкивање рачунарских мрежа, услед неадеватне заштите података у транспорту
  - Искључивање система неадекватним коришћењем привилегија или путем малициозног софтвера (хакерски напади, рачунарски вируси и сл.)

# Ревизија логичких контрола

- Један од најчешћих задатака ИТ ревизије је анализа и процена ефикасности логичких контрола приступа. Да би логичке контроле могле бити ефикасно процењене, неопходно је стећи техничко и организационо разумевање ИТ окружења организације, укључујући следеће безбедносне слојеве:
  - Рачунарска мрежа
  - Оперативни системи у употреби
  - Базе података
  - Апликативни систем
- Логичке контроле дефинише (и у одређеним ситуацијама оперативно додељује) власник информација или ИТ средстава. Одобрене приступе треба редовно преиспитивати да би се осигурало да су и даље валидни. Такође, ИТ ревизор треба да се увери да су приликом додељивања логичких контрола у обзир узети следећи принципи:
  - *Need-to-know*
  - Најмањих привилегија за обављање посла (*least privilege*)
  - Принцип доследности
  - Принцип транспарентности

# Ревизија логичких контрола

- Најчешћа провера логичких контрола је провера приступа информационом систему. Неке од активности ревизије које се том приликом спроводе су:
  - Провера да ли постоје процедуре за додавање нови корисника, брисање / архивирање старих корисника или измена неких од параметара постојећих корисника
  - Провера политике лозинки – да ли лозинке задовољавају нивое сложености, да ли се периодично мењају и да ли су прописане мере које су корисници дужни да поштују како се не би неовлашћено открили неауторизованим лицима
  - Провера да ли се периодично врше провере права приступа у циљу одржавања ажурности информација и валидности права приступа
  - Провера да ли постоје проедуре за превенцију и детекцију неауторизованог приступа као и прописане мере за отклањање евентуалне настале штете (нпр. неауторизованих измена, враћање нарушеног интегритета података, неовлашћеног увида у податке и сл.)

# Системски записи (логови)

- Системски записи требали би бити заштићени јаким контролама приступа како би се спречио неовлашћени приступ и модификација. ИТ ревизор би требао да се увери да се записи не могу мењати или обрисати, а да о томе не остане адекватан траг.
- Системски логови омогућавају увид у историјат промена различитих ИТ система, али и историјат провеме права приступа, промена привилегија као и покушаје неовлашћених и заустављених / спречених приступа одређеним сегментима система.
- Адекватни системски логови представљају вредан доказ у поступку ревизије, а највећи ризик представља њихово ограничено чување услед знатне величине коју заузимају на смештајним капацитетима организације.

# Управљање безбедностим инцидентима

- Да би се штета од безбедносних инцидената свела на минимум, требало би успоставити дефинисану и правовремену способност реакције на инцидент.
- У идеалном случају, треба формирати организациони тим за одговор на инциденте рачунарске безбедности (computer security incident response team - CSIRT) или рачунарски тим за реаговање у ванредним ситуацијама (computer emergency response team - CERT), с јасним линијама извештавања и одговорностима.
- ИТ ревизор би требао да обезбеди уверење CSIRT / CERT активно укључује кориснике како би им помогао у ублажавању ризика који произилазе из безбедносних пропуста као и да спрече, тј. сведе на најмању огућу меру штету насталу од последица сигурносних инцидената.
- Важно је утврдити постојање и адекватност формалног, документованог плана и који садржи поступке идентификације рањивости, извештавање и поступке реаговања на уобичајене или ванредне безбедносне претње / проблеме.

# Високотехнолошки криминал

- Важно је да ИТ ревизор познаје и разуме разлике између злоупотребе рачунара и високотехнолошког криминала, како би адекватно реаговао у случају да идентификује неку од активности која се може окарактерисати као кривично дело. Неки од примера злоупотребе рачунарских система укључују :
  - Онемугућавање услуге (*denial of service – DoS*)
  - Хаковање
  - Појаву малициозног софтвера (вируси, црви, тројанци)
  - Претње и уцене упућене уобичајеном каналима комуникације (нпр. e-mail)
    - „Пецање“ (*phishing*)
  - Погађање лозинки
  - Прислушкивање и измена мрежног саобраћаја (нпр. *man-in-the-middle* напад) итд.

# Малициозни код

- Постоје две основне методе за спречавање и откривање злонамерног софтвера који напада рачунаре и мрежне системе :
  - Постојање адекватних политика и процедура (превентивне контроле), и
  - Постојање техничких контрола (детективне контроле), попут антивирусниг софтвера
- Ниједна метода није ефикасна самостално, без друге.

# Спровођење ИТ ревизије, пример: контрола креденцијала

# Студија случаја

- Компанија из области енергетике назива „Енергија“ запошљава 3000 радника, од чега 2200 ради у производњи а 800 у централи.
- Запослени у производњи и радници на терену имају мобилне уређаје које користе за пријем имејл порука, на којима се налази и апликација за радне налоге.
  - Сваки радник добија свој мобилни уређај са јединственим бројем телефона, на коме се већ налази е-маил адреса радника коју подешава компанијски ИТ (у формату : ime.SREDNJESLOVO.prezime@energija.com)
  - Такође, приликом преузимања мобилног телефона, радник добија ИД од 6 цифара уз помоћ кога се пријављује у апликацију за радне налоге. Шифра се иницијално добија од стране техничког особља и увек је иста за нове кориснике – „Шифра123!“, а запосленима се саветује да је промене „што је пре могуће“

# Студија случаја

- Запослени у централи раде у Виндовс мрежи, којој приступају користећи доменски налог формата **ime.SREDNJESLOVO.prezime (npr. Ivana.M.Nikolic)**. Од приступа ресурсима, запосленима у централи је омогућено следеће :
  - Сваки запослени добија свој десктоп рачунар и мобилни уређај са јединственим бројем телефона, на коме се већ налази е-маил адреса радника коју подешава компанијски ИТ радника (у формату: ime.SREDNJESLOVO.prezime@energija.com)
  - Запослени раде у следећим апликацима:
    - Core sistem за управљање пословима из области енергетике: постоје модули за производњу, набавке, финансије, планирање, маркетинг и ЉР. Core sistem-у се приступа путем Single Sign On (SSO) система. Свако ко има доменски налог, може да приступи модулу за планирање, без обзира да ли га користи или не.
    - Књига улазних фактура (KUF) представља посебну апликацију којој приступ има ограничен број запослених, а која има свој посебан систем права приступа, и коју користи 25 радника из финансија
    - Топ менаџмент има приступ удаљеној веб апликацији Групе, чија је компанија „Енергија“ чланица, којој приступају користећи креденцијале (корисничко име и лозинку) који су добијени од стране групног сектора за ИТ
- Запослени у Сектору за ИТ имају приступ централном *windows* server-у (домен контролер) на коме се управља правима приступа централизовано.
  - Запослени у служби за одржавање база података, имају приступ core апликацији која, осим што омогућава SSO приступ, има и функционалност додавања других корисничких налога
  - Запослени у служби за одржавање мреже, која се састоји од 5 извршилаца, има приступ мрежним уређајима које одржавају. Ова лица не би требала да имају приступ core апликацији

# Студија случаја

- Од ИТ сектора добијени су следећи подаци:
  - Списак доменских налога садржи укупно 910 корисничких имена, од којих је активно 890
  - Списак ID-јева за апликацију радних налога садржи 2317 корисничких шифри и сви су активни

- Од сектора за ЉР добијена је информација да је од почетка рада „Енергије“ у централи било укупно 912 запослених а у производњи 2320 запослених.

- ИТ ревизор је извршио тестирање шифри за апликацију радних налога на узорку од 50 случајно одабраних ID-јева и утврдио да 35 њих има исту шифру која им је иницијално додељена – „Шифра 123!“

- ИТ ревизор је интервјуисао кључне запослене у Сектору за ИТ и добио следеће информације:
  - Због интерности групног ИТ-ја који је спор у додељивању нових шифри, дешава се да неки менаџери користе исти налог за приступ веб апликацији групе
  - У апликацији KUF тренутно права има тачно 25 запослених али пошто апликацију одржава вендор, потребно је сачекати више од две недеље да се списак достави – ИТ не зна детаље
  - Сви мрежни инжењери имају активни доменски налог

# Студија случаја - задатак

- ИТ ревизор је добио задатак да изврши ревизију адекватности управљања ИНТЕРНИМ креденцијалима, да идентификује ризике и изда препоруке које за циљ имају унапређење система интерних контрола.

# Студија случаја – чињенице и налази

1. У централи ради укупно 800 запослених, а активних налога има 890. Такође, постоји и 20 неактивних налога :
   - НАЛАЗ: 90 налога припада запосленима који више не раде у централи, 20 налога је исправно деактивирано а 2 налога су обрисана.
   - Препорука : ...?

2. У производњи ради укупно 2200 запослених, а активних налога у апликацији за радне налоге има 2317 и сви су активни :
   - НАЛАЗ: 317 налога припада запосленима који више не раде у производњи, очигледно је да се налози никада не деактивирају, а 3 налога су обрисана.
   - Препорука : ...?

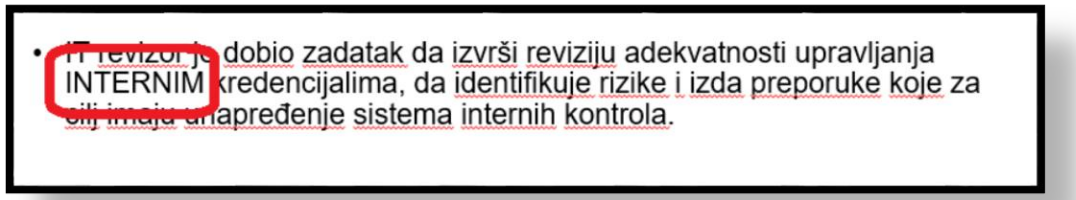
3. Шифре додељује ИТ и идентичне су за све ИД-јеве, при чему не постоји контрола која ће форсирати промену након иницијалног логовања:
4. НАЛАЗ: На основу узорка, утврђено је да је 70% шифара идентично и да су иницијалне.
5. Препорука : ...?

# Студија случаја – чињенице и налази

4. Сви мрежни инжињери имају доменски налог. У систему где постоји SSO, следи да се они, као и други запослени, могу приступити Core апликацијама :
   - НАЛАЗ: ...?
   - Препорука: ...?

5. Добијена је информација да „у апликацији KUF тренутно права има тачно 25 запослених“ али „пошто апликацију одржава вендор, потребно је сачекати више од две недеље да се списак достави“.
   - Да ли можемо да утврдимо да је овде све у раду? Зашто?
   - НАЛАЗ: ...?
   - Препорука : ...?

6. „Због интерности групног ИТ-ја који је спор у додељивању нових шифри, дешава се да неки менаџери користе исти налог за приступ web апликацији групе“.
7. Да ли ово налаз? Шта је SCOPE ревизије?
8. НАЛАЗ: ...?
9. Препорука : ...?



# Преглед налаза

| Р. бр. | Налаз | Prioritet (rizik) |
|---|---|---|
| **1** | Неадекватно управљање доменским налозима (у централи) | **СРЕДЊИ** |
| **2** | Неадекватно управљање налозима у апликацији за радне налоге (у производњи) | **СРЕДЊИ** |
| **3** | Неадекватно управљање лозинкама у апликацији за радне налоге | **НИЗАК** |
| **4** | Мрежни инжињери имају приступ core апликацијама | **СРЕДЊИ** |
| **5** | Неадекватан надзор - контрола (monitoring) над апликацијом KUF | **ВИСОК** |
| **6** | Неефикасно (неадекватно) управљање налозима за веб апликацију (менаџери) | ВАН ДЕЛОКРУГА |

# Користан линк

- Information Systems Audit & Assurance Guidance:
  - https://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/Pages/default.aspx