UDC: 007.3 INFO M: str. 4-9

ПРОЦЕС РЕВИЗИЈЕ ИНФОРМАЦИОНОГ СИСТЕМА
THE INFORMATION SYSTEM AUDIT PROCESS

Милица Боговац

РЕЗИМЕ: Развој и примена стратегије ревизије информационог система засноване на оцени ризика, која је у складу са међународним стандардима, смерницама и процедурама. Планирање ревизија тако да се обезбеди да су информациони и пословни системи заштићени и контролисани. Извођење ревизија информационог система у складу са међународним стандардима и препорукама тако да се постигну планирани циљеви ревизије. Извештавање руководства о уоченим чињеницама, потенцијалним ризицима и резултатима ревизије. Саветовање о управљању ризицима у организацији, уз очување независности и објективности.
Циљ овог рада је указивање на значај процеса ревизије информационог система и његовог утицаја на унапређење ефикасности, ефективности, сигурности и заштите информационог система.
КЉУЧНЕ РЕЧИ: Информациони систем, ревизија информационог система, управљање ризицима, интерне контроле, сигурност и заштита информационог система.
ABSTRACT: Development and implementation a risk-based information system audit strategy for the organization in compliance with information system audit standards, guidelines and procedures. Planning specific audits to ensure that information and business systems are protected and controlled. Conducting audits in accordance with information system audit standards and guidelines to meet planned audit objectives. Reporting to the top management emerging issues, potential risks and audit results. Advise on the implementation of risk management within the organization while maintaining independence.
This work is pointing out the importance of information system audit process and its influence on information system efficiency, effectiveness, security and protection.
KEY WORDS: Information system, information system audit, risk management, internal controls, information system security and protection.

1 УВОД

Информациони систем је један од кључни чинилаца сваког пословања. Управљање информационим системом је активност повезана са коришћењем напредних технологија и високим степеном стручних знања, као и општим знањима из теорије управљања организационим системима. Свака организација у свом пословању сусреће се са значајном количином несигурности која може резултовати материјалним ризиком и губитцима. Успех управљања целокупним пословањем директно је повезан са управљањем ризицима, тј ризици морају бити успешно превазиђени да би се могло успешно управљати организацијом.

2. МЕЂУНАРОДНИ РЕВИЗОРСКИ СТАНДАРДИ И ПРЕПОРУКЕ

Информациони систем (ИС) је уређени скуп људи, података, процеса, комуникационих веза и информационих технологија, који сарађују на подршци и унапређењу свакодневних пословних операција, као и подршци у решавању проблема и доношењу стратешких одлука.

Information System Audit and Control Association (ISACA) основана је са циљем едукације и унапређења рада у областима ревизије и контроле информационих система. Ова институција дефинише глобалне стандарде за управљање информацијама, контролу, заштиту и ревизију ИС.

Поред стандарда, ISACA је дефинисала и Етички кодекс ревизора информационих система као водич за понашање чланова овог института и сертификоване ИТ ревизоре (CISA – certified information systems auditor). Они треба да:

1. Помогну при увођењу и усаглашавању са одговарајућим стандардима, процедурама и контролама информационих система.
2. Своју дужност врше објективно, марљиво и професионално, у складу са професионалним стандардима и најбољим искуствима из праксе.
3. Раде, према највишим стандардима, у интересу клијента ревизије на законит и поштен начин, без укључивања у радње које могу да наруше углед професије.
4. Воде рачуна о приватности и поверљивости информација до којих долазе током свог рада, осим уколико постоји законска или професионална обавеза да поступе супротно. Ове информације не смеју се користити за остваривање сопствене добити или информисање неовлашћених лица.
5. Одржавају своју стручности у потребним областима и сагласни су да ће вршити само оне активности за које знају да ће их извршити са потребном професионалном стручношћу.
6. Обавесте одговарајуће особе о резултатима извршеног рада, информишући их о свим значајним чињеницама уоченим током свог рада.
7. Помажу у стручном информисању клијената ревизије са циљем лакшег и бољег разумевања безбедности и контрола ИС.

Међународни стандарди за ревизију ИС подељени су на неколико нивоа:

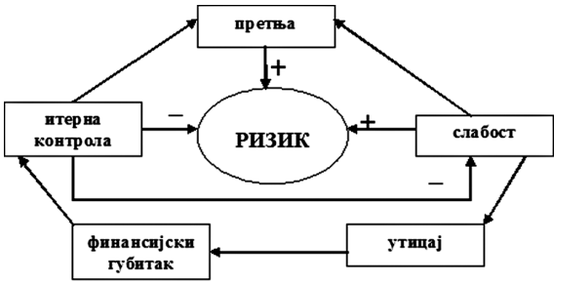
– стандарде, који дефинишу обавезне захтеве,
– смернице, које обезбеђују помоћ у примени Стандарда за ревизију ИС дајући упутства ревизорима информационих система како да примењују прописане стандарде.
– процедуре, које обезбеђују примере могућих процеса које ревизор ИС може да прати током извођења ревизије. У конкретним случајевима, ревизор ИС доноси одлуку о примењивости сваке појединачне процедуре. Документи са процедурама пружају информације како достићи стандарде током вршења ревизије ИС, али нису обавезујући за ревизоре.

2 АНАЛИЗА РИЗИКА И ИНТЕРНЕ КОНТРОЛЕ

Ризик је функција *вероватноће* да одређени *извор претње* искористи потенцијалну *слабост* тако да то резултује одређеним штетним и нежељеним *утицајем* на пословање организације.

– Претња је могућност извора претње да случајно или намерно искористи специфичну слабост система. Претња је само могућност да се искористи слабост, што не значи да ће она бити сигурно искоришћена.
– Слабост је недостатак или рањивост у системским сигурносним процедурама, дизајну, имплементацији или интерним контролама која може бити случајно или намерно искоришћена и као резултат имати сигурносни упад или кршење сигурносне политике система. Да би претња могла да буде успешна, мора постојати слабост која утиче на имовину организације.
– Имовина представља сваки део система, процес или ресурс који има вредност за организацију.
– Утицај или величина ризика је пропорционална вредност пословног губитка и процењене вероватноће претње.

Ризик информационог система дефинише вероватноћу да ће се у току оперативног рада или током његовог развоја и унапређења појавити нежељени и неприхватљиви догађаји. Ризици у информационом систему могу се класификовати у основне типове: предодређени, ризици перформанси, програмски, ризици динамичких планова, трошковни, технички, ризици везани за подршку, ризици развоја и ризици везани за комуникацију.



Slika 1. – *Повезаност ризика и његових елемената*

Процес управљања ризиком представља системску примену управљачке политике, процедура и искустава са задатком постављања контекста, идентификовања, анализе, оцене, обраде, мониторннга и извештавања о ризику. Фазе процеса управљања ризиком су: идентификовање, анализа и превазилажење ризика

Анализа ризика је део планирања ревизије који помаже у идентификовању ризика и рањивости система тако да ревизор може да одреди потребне контроле да би се превазишли ти ризици.

Приликом процене пословних процеса повезаних са информационим системом организације, за ревизоре је неопходно добро познавање веза између њихових ризика и контрола. Ревизори ИС морају да буду у стању да идентификују и разликују типове ризика и контрола које се користе за превазилажење и пословних и ризика информационог система. Они морају да поседују знања о уобичајеним пословним ризицима, ризицима повезаних технологија и релевантним контролама. Такође, морају да прегледају процену ризика и технике руковођења које користе руководиоци и да оцене ризике тако да на прави начин усмере планирање ревизорског рада. Поред разумевања пословних ризика и контрола, ревизори ИС морају да буду свесни чињенице да ризици постоје и у самом процесу ревизије.

Ревизор ИС обично се концентрише на високо-ризичне проблеме повезане са поверљивошћу, доступношћу или интегритетом осетљивих и критичних информација, као и информационих система и процеса који генеришу, управљају и чувају ове информације.

Интерним контролама називају се све политике, процедуре, примери из праксе и организациона структура који се уводе да би смањили ризик. Оне се развијају, на основу усаглашавања или иницијатива руководства, да би се осигурало испуњење пословних циљева организације и спречило или благовремено открили и исправили нежељени ризични догађаји.

Активности и процеси интерних контрола могу бити мануелни или аутоматизовани. Они постоје и функционишу на свим нивоима у организацији како би превазишли изложеност ризицима који потенцијално могу онемогућити пословање у остваривању својих циљева. Највише руководства организације је одговорно за стварања одговарајуће корпоративне културе која ће омогућити и олакшати постојање и рад ефективног и ефикасног система интерних контрола и континуирани мониторинг ефективности овог система, иако сваки запослени у организацији мора дати своје учешће у овом процесу.

Постоје два кључна аспекта која треба одредити – шта треба бити достигнуто и шта треба избећи. Интерне контроле не само да одређују пословне/оперативне циљеве, већ одређују и нежељене догађаје кроз њихову превенцију, детекцију и исправку.

Контроле се класификују се као превентивне, детективне и корективе у својој природи.

У сарадњи са ISACA инсититутом, Институт за управљање информационом технологијом (ITGI) објавио је оквирни систем за управљање и контролу ИТ који обухвата најбоља искуства из праксе – Контролни циљеви за информационе и повезане технологије (Control Objectives for Information and related Technology – CobiT). **CobiT** је водећи систем за управљање, контролу и осигурање информационих и њима сродних технологија.

CobiT је намењен руководству, запосленима и власницима пословних процеса који користе ИТ процесе који обезбеђују поверљивост, интегритет и расположивост осетљивих и критичних информација.

2. РЕВИЗИЈА ИНФОРМАЦИОНОГ СИСТЕМА

Ревизија се може дефинисати као систематичан процес у коме стручне, независне особе објективно прикупљају и оцењују доказе у погледу претпоставки о економским ентитетима или догађајима, са циљем формирања мишљења и извештавања о степену усаглашености посматраних претпоставки и идентификованог скупа стандарда.

Ревизија ИС се може дефинисати као свака ревизија која обухвата делимичну или целокупну анализу и оцену аутоматизованог система обраде информација, повезаних неаутоматизованих процеса и интерфејса између њих.

Ревизијом се утврђује да ли је систем интерних контрола који је успостављен ради управљања ризицима, контроле и руковођења тим процесима адекватан и да ли функционише на начин којим се обезбеђује:

- да су ризици на одговарајући начин идентификовани и контролисани,
- да су међусобни односи чланова руководства успостављени на одговарајући начин (хоризонтална и вертикална повезаност),
- да су битне финансијске, управљачке и оперативне информације и извештаји правовремени, тачни и потпуни,
- да запослени обављају послове у складу са прописаним стандардима и процедурама,
- да су средства економично набављена, да се ефикасно и рационално користе и да су адекватно заштићена,
- да су програми, планови и циљеви организације остварени,
- да су контролни процеси квалитетни и да се стало унапређују,
- да су руководство и запослени благовремено упознати са законима и другом регулативом, као и општим актима који су из њихових делокруга,
- да је пословање усклађено с политиком, плановима, процедурама и прописима.

Потребни су одређени кораци да би се извршио овакав процес. Адекватно планирање је неопходан први корак у извођењу успешне ревизије ИС. Да би се ефективно користили ресурси ревизије ИС, организација мора да оцени свеобухватни ризик за опште области и апликације и да на основу тога изради програм ревизије који се састоји од циљева и ревизорских процедура које доприносе ревизорским циљевима. Процес ревизије захтева од ревизора ИС да прикупља доказе, оцењује јачину и слабости постојећих контрола на основу прикупљених доказа, и да припреми ревизорски извештај који руководство на објективан начин обавештава руководство о овим питањима.

Управљање ревизијом мора да обезбеди адекватне ревизорске ресурсе и временски распоред извођења ревизија, као и накнаде провере статуса корективних акција. Разматрање ревизије треба да обухвати делокруг ревизије, ревизорске циљеве, критеријуме, ревизорске процедуре, доказе, закључке и мишљења, као и извештавање.

Ревизор ИС треба да разуме различите типове ревизије који се могу обављати и њима придружене ревизорске процедуре: финансијске ревизије, оперативне ревизије, интегрисане ревизије, административне ревизије, ревизије информационих система, специјализоване ревизије и судске ревизије.

Ревизорски програми за финансијске, оперативне, интегрисане и административне ревизије ИС заснивају се на делокругу и циљевима конкретног задужења. Ревизори ИС обично оцењују ИТ функције и системе са различитих становишта, као што су безбедност (поверљивост, интегритет, расположивост), квалитет (ефективност, ефикасност), поверљивости (усаглашеност, поузданост), услуга и капацитета.

Ревизорска методологија је скуп документованих ревизорских процедура које су израђене да би се испунили планирани ревизорски циљеви. Њени саставни делови су изјаве о делокругу, о ревизорским циљевима и о програму рада.

Ревизорску методологију одобрава руководство ревизије са намером обезбеђења доследност у ревизорском приступу. Ова методологија треба да буде формализована и објашњена свим ревизорима.

Ревизори ИС су ограничени **ресурс** а информационе технологије стално напредују. Из тог разлога, битно је да ревизори ИС одржавају своју стручност кроз усавршавање постојећих вештина и знања, као и стицање нових знања везаних за ревизорске технике и ИТ. Ревизор ИС мора да разуме технике за управљање пројектима ревизије са ограниченим бројем адекватно обучених ревизора. Међународни стандарди ревизије ИС захтевају да ревизор ИС буде технички стручњак, и да има вештине и знање потребне за обављање ревизорског посла. Приликом планирања ревизије и доделе чланова тима конкретним ревизијама треба узети у обзир њихова знања, вештине и искуства из претходних ревизија.

Све већи број организација користи **приступ ревизија заснованих на ризику** које се прилагођавају развоју континуираног процеса ревизије. Овај приступ се користи за оцену ризика и као подршка одлучивању да ли радити само тестове усаглашености или и детаљнија тестирања. Битно је нагласити да то помаже ревизору и у одређивању природе и опсега тестирања.

Slika 2. – *Приступа ревизији заснован на ризику*

Ревизорски ризик се дефинише као ризик да извештаји садрже материјалне грешке које могу остати неоткривене током ревизије. Он се може категорисати на следећи начин: стално присутан ризик, контролни ризик, ризик детектовања и укупни ревизорски ризик.

Ревизорски ризик се понекад користи за опис нивоа ризика који је ревизор ИС спреман да прихвати током ревизорског ангажовања. Ревизор одреди жељени ниво ризика и према њему прилагођава детаљност свог истраживања како би минимизирао укупни ризик ревизије.

Приликом доношења одлуке које функционалне области ће бити предмет ревизија, ревизор ИС разматра велики број разлитичих субјеката. Сваки од њих са собом носи другачији тип ревизорског ризика, а ревизор треба да процени ове различите ризичне каднидате како би одлучио које високо ризичне области треба да буду предмет ревизије.

Постоји велики број **методологија процене ризика** који су на располагању ревизорима ИС. Од једноставне класификације засноване на мишљењу ревизора – висок, средњи и низак ниво ризика, до сложених израчунавања које обезбеђују нумеричко рангирање ризика.

Циљеви ревизије се често фокусирају на проверу да ли постоје интерне контроле које треба да минимизују пословни ризик. Ови ревизорски циљеви укључују усаглашеност са законским условима и регулативом, као и поверљивост, интегритет, поузданост и расположивост информатичких ресурса. Пре и током ревизије, руководство треба да обезбеди процену општих контролних циљева.

Основни циљ ревизије информационих технологија је да утврди да ли поступци и процедуре доприносе систему интерних контрола који се користе, у следећим областима:

– организационе и управљачке контроле,
– управљање сигурношћу система и контролама приступа,
– оперативне контроле,
– системске контроле и контроле развоја програма,
– физичка безбедности и контроле окружења,
– опоравак после отказа система и планирање континуитета,
– Интернет банкарство.

Планирање ревизија састоји се од краткорочног и дугорочног планирања. Краткорочно планирање узима у обзир ревизорска питања која ће бити обухваћена током године, док се дугорочно планирање односи на планове ревизије засноване на оцени ризика везаних за промене у ИТ стратегији организације.

Анализа адекватности краткорочних и дугорочних планова треба да се обавља барем једном годишње. То је неопходно да би се у обзир узеле нове контроле, промене у технологијама, промене пословних процеса и побољшале технике оцењивања ризика.

Поред годишњег планирања, свака посебна ревизија треба бити адекватно испланирана. Ревизор ИС треба да узме у обзир сва разматрања која могу утицати на свеобухватни приступ ревизији, као што су оцена ризика од стране руководства, захтеви за заштитом података и правна регулатива.

Још једна значајна компонента планирања је усклађивање расположивих ресурса ИТ ревизије са задацима дефинисаним у плану ревизије. Ревизор ИС који припрема план треба да размотри захтеве планираних ревизија, расположиве стручњаке и друга ограничења, и усклади све ове компоненте.

Тестирања усаглашености организације са контролним процедурама утврђују да ли су примењене контроле у сагласности са управљачким политикама и процедурама. Ревизор ИС мора да разуме специфичне циљеве тестирања усаглашености и да тестира контроле. Тестови усаглашености могу се користити за тестирање постојања и ефективности дефинисанх процеса који обухватају документацију и/или аутоматизоване доказе, на пример контроле који омогућавају извршење само ауторизових измена на програмима у продукцији.

Прикупљање доказа за оцењивање интегритета појединачних трансакција, података или других информација (детаљно тестирање) утврђује интегритет стварне обраде података. Оно обезбеђује доказ пуноважност и интегритет ставки у финансијским извештајима и трансакцијама.

Постоји директна повезаност између нивоа интерних контрола и количине потребног детаљног тестирања. Ако резултати тестирања усаглашености утврде постојање

адекватних интерних контрола, онда ревизор може да минимизује детаљно тестирање. С друге стране, уколико тестирање контрола открије слабости у систему интерних контрола то може повећати сумње у потпуност, тачност или пуноважност података, онда су потребна детаљнија тестирања.

Избор узорка се користи када ограничено време и трошкови онемогућују потпуну проверу свих трансакција или догађаја у предефинисној популацији. Подскуп чланова популације се назива узорком, и он се користи за извођење закључка о карактеристикама читаве популације, на основу резултата испитивања карактеристика узорка.

Постоје две основне методе избора узорка које користе ревизори ИС – узорковање атрибута и узорковање одступања. Узорковање атрибута се примењује у ситуацијама тестова усаглашености, бави се присуством или одсуством одређених атрибута и обезбеђује очекиване закључке. Узорковање одступања се углавном примењује на ситуације детаљног тестирања, бави се карактеристикама популације који одступају, и обезбеђује закључке који се односе на одступање од норми.

Доказ је свака информација коју ревизор ИС користи да утврди да ли ентитет или податак који проверава задовољава дефинисане критеријуме или циљеве ревизије. Неопходно је да се ревизорски закључци заснивају на довољним, значајним и одговарајућим доказима. Приликом планирања ревизије ИС, ревизор треба да узме у обзир тип ревизорских доказа које треба да прикупи, јер њихова вредност мора бити усклађена са циљевима ревизије и са разлитим нивоима поузданости.

Ревизорски доказ може да обухвата запажања ревизора ИС, белешке са интервјуа, преписку и интерну документацију, или резултате тестирања. Иако сви докази доприносе доношењу закључака о предмету ревизије, треба проценити њихову поузданост на основу: независности извора доказа, квалификација појединца који обезбеђује информације/доказе, објективности доказа и изабраног тренутка за прикупљање доказа.

Посматрање запослених током обављања њихових обавеза и задатака може помоћи ревизору ИС у идентификовању: стварних функција, стварних процеса/процедура, разумевања сигурности и повезаност извештавања.

Интервјуисање запослених и руководства који раде обраду информација, треба да обезбеди адекватно осигурање да запослени имају потребне техничке вештине и знања да врше своје задатке. Ово је значајан фактор који доприноси ефективном и ефикасном опративном раду.

Computer-Assisted Audit Techniques (CAAT) су битан алат за ревизора ИС у прикупљању информација у електронском окружењу, јер је без њих скоро немогуће прикупити доказе из система који имају различите хардверске и софтверске платформе, различиту структуру података, формате слогова података, функције обраде итд.

Такође, они омогућавају ревизорима ИС да током извођења реивзије самостално и независно од субјекта ревизије прикупљају потребне информације. CAAT омогућују приступ и анализу података за предефинисане циљеве ревизије и извештавање о ревизорским налазима са нагласком на поузданост података које се генеришу/уносе и чувају у систему, као и оних које систем генерише.

Након израде програма ревизије и прикупљања ревизорских доказа, следећи корак је **процена прикупљених информација** како би се оформило ревизорско мишљење. То од ревизора ИС захтева да размотри скуп предности и слабости и на основу тога донесе ревизорске закључке и препоруке за побољшање.

Током ревизије информационог система, ревизор може да открије разноврсне јаке и слабе контроле, које треба узети у обзир када се процењује свеукупна контролна структура. Компензационе контроле се појављују у ситуацијама када једна јака контрола надокнађује слабости друге контролу, док су преклапајуће контроле две јаке контроле.

На завршном састанку који се организује на крају ревизије, ревизор ИС треба да дискутује о налазима и препорукама са руководством и оперативним извршиоцима. Потребно је објаснити циљеве и делокруг ревизије, као и сам процес извођења ревизије ИС. Током завршног састанка, ревизор ИС треба да:

– провери да су чињенице наведене у извештају тачне,
– провери да су препоруке реалне и трошковно оправдане, а уколико нису да пронађе алтернативна решења кроз преговарање са клијентом ревизије, и
– дефинише рокове за имплементацију усаглашених препорука.

Ревизор ИС презентује резултате ревизорског рада различитим нивоима руководства и зато мора да добро познаје технике презентовања које су неопходне да би руководиоце јасно и успешно известио о резултатима.

Ревизори ИС треба да буду свесни да је ревизија стални процес. Ревизија није успешна ако је након извршене ревизије издат извештај, али није урађено накнадно праћење како би се проверило да ли је руководство предузело потребне корективне акције. Потребно је припремити follow-up програм како би утврдио да ли су имплементиране договорене корективне акције. Екстерна ревизија не мора да предузима ове активности али може уколико су они договорени са клијентом.

Екстерна група за ревизију информационих система спроводи ревизију организације или делова организације који се баве обрадом података, развојем, имплементацијом и одржавањем компјутерских апликација. Овим ревизијама процењује се квалитет контрола и мера заштите организационих вредности, ефективно коришћење ресурса за обраду података, усклађеност са управљачким политикама, планирање и имплементација одговарајућих интерних контрола апликација и окружења у којима се оне користе.

Предмети екстерне ревизије су најчешће: стратешка питања, организациона структура, апликативне контроле за значајне и новчане трансакције, мрежни приступ поверљивим информацијама, као и физичке и логичке мере заштите.

Основни циљ **интерне ревизије** је да својом активношћу допринесе што ефикаснијем пословању организације тако што ће највишем руководству пружити независно и објективно мишљење о питањима која су предмет ревизије, као и путем консултантске активности која је усмерена на унапређивање постојећег система интерних контрола и пословања организације.

3. ЗАКЉУЧАК

У савременим условима брзих технолошких и организационих промена, управљање информационим системом и обављање оперативних активности везаних за прикупљање, пренос, обраду и смештање података у електронском облику, потребно је унапредити а пословање осигурати уз што мање трошкове.

Процес ревизије информационог система има велики утицај на повећање ефикасности и ефективности функционисања ИС. Препорука је да се развој и имплементација стратегије, као и управљање информационим системом заснива на оцени ризика, док ће благовремено и адекватно извођење ревизија обезбедити да информациони и пословни системи буду заштићени и контролисани. Извештавање руководства о резултатима ревизије и саветодавна функција ревизије омогућују да се уочени недостаци отклоне и да се постојећи систем побољша на најбољи могући начин.

ЛИТЕРАТУРА

[1] http://www.isaca.org – Information System Audit and Control Association
[2] http://www.infosecurity-magazine.com – часопис InfoSecurity
[3] http://www.itgi.org – IT Governance Insitute
[4] http://www.sans.org – SANS (SysAdmin, Audit, Network, Security) Institute
[5] група аутора, *CISA Review Manual 2007*, Information System Audit and Control Association, USA, 2007
[6] група аутора, *CobiT Control Objectives*, IT Governance Insitute, USA, 2007
[7] група аутора, *IS Standards, and Summaries of Guidelines and Procedures for Auditing and Control Professionals*, Information System Audit and Control Association, USA, 2007
[8] Champlain Jack, *Auditing Information Systems*, John Wiley & Sons Inc., USA, 2003
[9] Sawyer Lawrence, *Sawyer's Internal Auditing*, Institute of Internal Auditors, USA, 2003
[10] часопис Information Systems Control Journal
[11] часопис IT audit

Милица Боговац, Народна банка Србије
Области интересовања: управљање информационим системима, ревизија, сигурност и заштита информационих система, системи за подршку одлучивању и data mining.