

Доц. др Миле Станишић¹

Универзитет Сингидунум, Београд

ИНТЕРНА РЕВИЗИЈА У ФУНКЦИЈИ УПРАВЉАЊА РИЗИКОМ У ПРИВРЕДНИМ ДРУШТВИМА

САЖЕТАК: Последњих година интерна ревизија је добила важну улогу у управљању ризиком у привредним друштвима, иако и даље управљање ризицима остаје кључна одговорност вишег руководства и надзорног одбора. Третман ризика од стране интерне ревизије се захтева Законом о привредним друштвима, Законом о банкама, Законом о осигурању, и другим законима. Интерна ревизија има мандат широког обухвата да покрива финансијске ризике, оперативне ризике, ризике информационе технологије, правне и стратешке ризике, на макро и микро нивоу у односу на све наведене ризике. Да би утврдили постојање одговарајућих процеса управљања ризиком, као и то да су ови процеси адекватни и ефективни, надзорни одбори у овој улози могу захтевати подршку функције интерне ревизије - кроз испитивање, процењивање, извештавање и препоручивање унапређења у вези адекватности и ефективности процеса управљања ризиком. Интерни ревизори делују кроз уверавање и саветодавну функцију у циљу идентификовања, вредновања и имплементирања методологије за управљање ризицима и контрола за смањење тих ризика.

Кључне речи: интерна ревизија, управљање ризицима, категорије ризика, привредна друштва, процена ризика.

1 mile.stanistic@singidunum.ac.rs

УВОД

Интерни ревизори имају кључну улогу у оцењивању ефикасности управљања ризиком пословања и давању препорука за побољшање. Стандарди интерне ревизије које је донео Институт интерних ревизора утврђују да делокруг интерне ревизије обухвата системе управљања ризиком и контроле. То укључује оцењивање поузданости извештавања, ефикасности и ефикасности пословања и усклађености са законима и прописима. Испуњавајући своје одговорности, интерни ревизори помажу руководству и надзорном/упрвном одбору и одбору за ревизију прегледањем, оцењивањем, извештавањем и давањем препорука за побољшање адекватности и ефикасности управљања ризиком пословања предузећа или друге организације.

У многим компанијама у свету интерни ревизори имају кључну улогу у континуираном функционисању управљања ризиком пословања кроз обезбеђивање објективног праћења примене политика и процедура управљања ризиком и ефикасности тих процеса. Интерни ревизори могу вршити испитивања за потребе процене целокупног процеса управљања ризиком пословања или његових подпроцеса. У тој улози, интерни ревизори могу подржавати руководство пружањем уверавања о:

- Процесима управљања ризиком пословања, и о концепту и о функцији
- Ефикасности и ефикасности начина решавања ризика и повезаних контролних активности
- Потпуности и тачности извештавања о управљању ризиком пословања.

Интерни ревизори, поред функције уверавања, понекад делују у консултантској улози, за унапређење процеса управљања ризиком пословања у организацији. У том својству, интерни ревизори могу, између осталог, промовисати развој општег разумевања управљања ризиком пословања, подучавати руководство о концептима управљања ризиком пословања, бити медијатори радионица на тему ризика и обезбеђивати инструменте и технике којима се руководиоцима помаже да анализирају ризике и осмишљавају контролне активности.

Функција интерне ревизије постоји да помогне организацији да управља свим својим ризицима и да промовише ефикасне процесе управљања. Стандарди захтевају да интерна ревизија помогне организацији да управља ризицима помоћу:

- Идентификовања и процене изложености значајним ризицима.
- Доприноса побољшању система за управљање и контролу над ризицима.
- Праћење и процена система за управљање ризицима.

Свака интерна ревизија мораће да одреди који је најбољи начин да се обаве те активности полазећи од своје постојеће улоге и пословне културе унутар организације. Услед тога, појединачни процеси реализације тих захтева разликоваће се од организације до организације. Циљ овог рада је да истражи све могућности доприноса функције интерне ревизије у управљању ризицима, чији захтев се поставља од више Српских закона.

ЗАКОНОДАВНИ ОКВИР ИНТЕРНЕ РЕВИЗИЈЕ У РЕПУБЛИЦИ СРБИЈИ

Постоји законски услов да многе организације морају да имају интерну ревизију у својој организационој структури. Та обавеза је регулисана следећим законима: Закону о привредним друштвима, Закону о банкама, Закону о добровољним пензијским фондовима и пензијским плановима, Закону о инвестиционим фондовима, Закону о осигурању, Закону о буџетском систему, за јавна предузећа и министарства Републике Србије и друге јавне институције донешен је Правилник о заједничким критеријумима за организовање и стандардима и методолошким упутствима за поступање и извештавање интерне ревизије у јавном сектору.

У Закону о привредним друштвима у члану 452. став 1. тачка 3. је речено да послови унутрашњег надзора нарочито обухватају **проверу спровођења политика управљања ризицима.**²

Према Закону о банкама интерна ревизија је дужна да обезбеди да се ризици на одговарајући начин **идентификују и контролишу.**³

У Закону о осигурању⁴ у члану 137. је наведено да интерна ревизија друштва за осигурање спроводи сталну и свеобухватну контролу

2 Закон о привредним друштвима, "Службени гласник РС", бр. 36/2011, 99/2011, 83/2014, 5/2015

3 Закона о банкама, „Службени гласник РС“, бр. 107/2005, 91/2010 и 14/2015

4 Закон о осигурању, "Сл. гласник РС", бр. 55/2004, - др. закони, 119/2012, 116/2013 и 139/2014.

свих активности из пословања друштва, а нарочито идентификацију ризика којима је друштво за осигурање изложено или се може очекивати да буде изложено.

Затим у истом члану Закона је наглашено да интерна ревизија контролише и процењује адекватност и примену прописаних политика и **процедура контроле ризика**, а Програмом рада интерне ревизије уређују се јасно и детаљно дефинисани **ризичи** и области пословања у којима ти ризици могу настати (члан 139. Закона).

У члану 141. Закона о осигурању још је више наглашена улога интерне ревизије, те је наведено, “ако интерна ревизија утврди да друштво за осигурање не поступа у складу са правилима о управљању ризиком и због тога друштву прети великвидност или несолвентност или утврди да је угрожена сигурност пословања, односно да су угрожени интереси осигураника, дужна је да о томе одмах, а најкасније у року од 24 часа од тренутка сазнања, обавести управу и надзорни одбор друштва за осигурање.” Дакле, из овога навода се види да је интерној ревизији дата улога да пали црвени аларм када оцени да је то неопходно.

ДЕФИНИСАЊЕ РИЗИКА И УПРАВЉАЊА РИЗИКОМ ПОСЛОВАЊА

Ризик је концепт који ревизори и директори користе за изражавање својих забринутости око могућих ефеката несигурног окружења. Пошто будућност не може са сигурношћу да се предвиди, ревизори и директори морају да размотре низ могућих догађаја који би се могли десити. Сваки од тих догађаја би могао имати материјални ефекат, то јест значајну последицу, на привредно друштво и његове циљеве. Стандарди интерне ревизије дефинишу ризик као: “Могућност догађаја који ће утицати на остварење циљева. Ризик се мери у смислу његовог утицаја и вероватноће.” Поред ове дефиниције ризика дефиницију је дао и COSO.

„Управљање ризиком предузећа је процес који спроводе управни одбор субјекта, управа и остало особље, а који се примењује код одређивања стратегије у целом предузећу, пројектован тако да идентификује потенцијалне догађаје који могу да утичу на субјекат и да управља ризицима да

би били у оквиру апетита за ризик субјекта како би се могло дати разумно уверавање у вези са остварењем циљева субјекта.“⁵

Ниједан циљ се не може остварити без присуства ризика. Део умешности управљања ризиком је учење о томе како и када прихватити ризик. Ова грана науке о доношењу одлука се назива “анализа ризика.” Несигурност и случајност постоје у природи. Ризик није нешто око чега треба да се брине, али је нешто чиме треба управљати. Управљање ризиком укључује анализу ризика и одговарајуће кораке који проистичу из разумевања и свести о последицама управљања у несигурном свету. Пошто се људи удружују како би радили у предузећу, природна варијација понашања је повезана са несигурношћу окружења. Стога су анализа ризика, процена ризика и управљање ризиком део савремених средстава планирања управљања. Веза између ревизије и управљања је процена ризика и његових последица на остваривање установљених циљева.

Као што је речено *Стандарди* дефинишу ризик као „*неизвесност јављања догађаја који може да утиче на остварење циљева*“. Ризик није у потпуности нешто лоше, јер је одређени ризик неопходан ако посао треба да успе и да се добије награда за то. Па ипак, ризици могу да спрече, и спречавају, руководиоце да остваре своје пословне циљеве, а у екстремним случајевима, они чак могу допринети уништењу организације.

Ризик је, такође, нешто више од „догађања лоших ствари“. Пропуштене пословне могућности могу да буду једнако скупе и погубне за организацију. У стварности, успешно пословање захтева да се средства и ресурси организације изложе ризику да би се постигли стратешки и оперативни циљеви. Стандарди интерне ревизије дефинисали су управљање ризиком као, „Процес идентификовања, процене, управљања и контроле потенцијалних догађаја или ситуација у циљу обезбеђивања разумног степена уверавања у погледу остваривања циљева организације.“ Улога ефикасног управљања ризицима у организацији се стога састоји у успостављању равнотеже између позитивних и негативних аспеката везаних за пословне ризике, како би организација на најбољи начин остврила своје циљеве уз најниже трошкове.

Када су процењени релевантни ризици менаџмент одлучује како ће на то одговорити, у смислу ублажавања ризика. Приликом разматрања својих акција које ће предузети менаџмент оцењује ефекат на вероватноћу

5 Committee of Sponsoring Organizations, *Enterprise Risk Management*, COSO, September 2004, p. 16.

и утицај ризика, као и на трошкове и добити, тако што одабере одговор који своди резидуални (преостали) ризик у оквиру жељеног нивоа ризика. Менаџмент утврђује све могућности које могу да буду на располагању, и разматра ризик на нивоу ентитета или портфолиа и утврђује да ли укупан резидуални ризик је у оквирима прихватљивог нивоа ризика за ентитет. Ризици се могу ублажити на неки од начина управљања ризиком. Одговори на ризике, односно предузимање акција у вези ризика, разврставају се у следеће категорије:

- *Избегавање* – Напуштање активности које доприносе ризику. Избегавање ризика може да укључује напуштање линије производа, смањење експанзије на неко географско тржиште, или продају одељења.
- *Смањење* – Предузима се акција да се смањи вероватноћа или утицај ризика, или оба. Овим се по правилу обухвата било која од многих свакодневних пословних одлука.
- *Подела одговорности за ризик* – Смањење вероватноће или утицаја ризика преношењем дела ризика или поделом одговорности за ризик. Уобичајене технике обухватају куповину производа осигурања, ангажовањем у трансакцијама хеџинга, или ангажовањем спољних извора за неку активност.
- *Прихватање* – Не предузимају се акције које би могле да утичу на вероватноћу или утицај ризика.

Стандарда интерне ревизије наводе три посебне активности које интерни ревизори морају да предузму, како би помогли организацији у пословима управљања ризицима: (1) интерни ревизори морају да помогну организацији да идентификује и процени изложености значајним ризицима (*Стандард 2110*), (2) интерни ревизори морају помоћи да се побољша управљање ризицима и системи контроле (*Стандард 2110*), и (3) интерни ревизори морају да прате и процењују систем за управљање ризицима (*Стандард 2110.A1*).

ПРОЦЕНЕ РИЗИКА ПОСЛОВАЊА

Најбоља методологија рада интерне ревизије је она која је фокусирана на обављање ревизије засноване на управљању ризиком процеса, који је у складу са концептима управљања ризиком предузећа (*УРП- eng. ERM - Enterprise risk management*). Међутим, такође је могуће применити ове

концепте и на ревизију самог процеса УРП. Таква ревизија била би релевантна у следећим околностима:

- Предузеће примењује обиман процес УРП, а ревизорски тим жели да оцени колико ефективно тај процес функционише.
- Предузеће је почело са имплементацијом процеса УРП, а ревизорски тим жели да идентификује главне области у којима постоје пропусти у имплементацији.
- Предузеће још нема формалан процес УРП, а ревизорски тим жели да идентификује области које би захтевале највећу пажњу уколико предузеће одлучи да започне са имплементацијом процеса УРП. Области које треба да буду у фокусу би биле идентификоване на основу оцене ревизорског тима тренутних, неформалних процедура које могу да подрже један формалнији процес УРП и оних процедура које би биле потребне.⁶

Постоје неке кључне карактеристике које су неопходне за одржавање ефективног процеса управљања ризиком предузећа. Следећа кључна питања ће помоћи у обради кључних атрибута у управљању ризиком предузећа:

- Да ли предузеће има конкретну стратегију/политику која се односи на управљање ризиком?
 - Ако је тако, да ли је та стратегија/политика јасно артикулисана и схваћена у целој организацији?
 - Да ли она артикулише филозофију предузећа када је реч о предузимању ризика?
- Да ли постоје циљеви сектора или појединаца које подржавају активности управљања ризиком на годишњем нивоу?
 - Да ли су ови циљеви у складу са укупном стратегијом/политиком УРП и да ли је подржавају?
- Да ли је толеранција предузећа у погледу ризика јасно дефинисана и артикулисана?

⁶ Видети више: The Institute of Internal Auditors, The Role of Internal Auditing in Enterprise-wide Risk Management, IIA, USA, 2004, pp. 1-2.

- Да ли је ова толеранција ризика утврђена на одговарајућем нивоу у предузећу (нпр. надзорни одбор, виша управа, комитет за управљање ризиком, овлашћени појединци итд.)?
- Да ли су тамо где је то потребно утврђени нивои који се могу квантификовати (нпр. лимити, границе, финансијски утицај итд.)?
- Да ли постоји формална организациона структура управљања ризиком?
 - Да ли она извештава довољно висок ниво у оквиру организације?
 - Да ли су обим ове функције и одговорност за њу јасно назначени?
 - Да ли је подршка више управе јасно артикулисана?
 - Да ли она функционише у складу са културом предузећа?

Процена ризика је полазна тачка за конкретне активности УРП. Има неколико кључних атрибута који су неопходни за ефективно обављање процеса процене ризика. Следећа питања ће помоћи код обраде кључних атрибута у процени ризика:

- Да ли је универзум ризика развијен тако да обухвата све кључне ризике са којима се предузеће суочава?
 - Да ли су формиране области и категорије како би се утврдио формалан модел ризика који је прилагођен предузећу?
 - Да ли су сви ризици дефинисани коришћењем речи и идеја које су у складу са начином на који предузеће говори, односно да ли је створен заједнички језик ризика?
 - Да ли су ризици повезани са стратегијом предузећа?
- Да ли је формално процењен утицај сваког ризика?
 - Да ли су узети у обзир и финансијски и нефинансијски утицаји (нпр. стратешки, репутација, правни, здравствени и безбедносни итд.)?

- Да ли су идентификовани и размотрени реални најгори сценарији?
- Да ли постоји консензус око утицаја ризика?
- Да ли је вероватноћа тог утицај утврђена за сваки ризик?
 - Да ли је вероватноћа својствена или се њоме може управљати?
 - Да ли постоји консензус око вероватноће ризика?
- Да ли је утврђена толеранција управе у погледу мере прихватања сваког ризика?
 - Да ли та толеранција одговара процењеној вероватноћи, омогућавајући јасну процену разлике између постојеће вероватноће и вероватноће која се толерише?
 - Да ли постоји консензус о толеранцији ризика?
- Да ли постоје други критеријуми процене (нпр. могућност управљања, ефикасност) које управа користи код процене ризика?
 - Да ли је процена ових критеријума на одговарајући начин повезана са осталим критеријумима који се користе код процене?
- Да ли су кључни или примарни ризици идентификовани за компанију?

Интерни ревизори морају да помогну организацији да идентификује и процени изложености значајним ризицима (*Стандард 2110*). Већина интерних ревизора је идентификовање и процену излагања ризицима обављала рутински кроз процену ризика. Док је раније то била само активност која се препоручује, од интерних ревизора се сада очекује да идентификују и процене изложености значајним ризицима у оквиру нормалног обављања својих дужности у организацији (*Практични саветник 2100-3*).

Макро процена

Процена ризика целе организације може се описати као идентификовање и процена изложености ризицима на стратешком или макро нивоу организације. Потпуно познавање пословања, његове укупне стратегије, променљивог спољног окружења, питања која су значајна за учеснике и примарних ризика организације представљају предуслове за успешан про-

грам процене ризика за целу организацију. Циљ овакве макро процене је да се обезбеди поглед са врха према доле на све кључне ризике који утичу на организацију у целини.

Учешће интерне ревизије у макро процени варираће у зависности од нивоа активности извршног руководства у том подручју. Ако је руководство већ покренуло процес процене високих ризика, у оквиру укупног система управљања ризицима предузећа, тада интерна ревизија треба своје полазне претпоставке да узме из те процене. У многим организацијама, међутим, таквог процеса нема и можда ће бити потребно да интерна ревизија допринесе његовом успостављању.

Програми макро процене ризика које воде интерни ревизори често обухватају неке, или све од доле наведених корака:

- Позивање кључних играча из целе организације на једнодневни интензивни састанак типа браинсторминг (*brainstorming session*), ради идентификовања и рангирања највећих пословних ризика у целој компанији.
- Спровођење процене ризика са највишим руководством и управним одбором, путем интервјуа, упитника, или комбинације ове две технике, да би се прецизно утврдили најкритичнији ризици виђени из перспективе успешног вођења организације и задовољења захтева свих учесника.
- Преглед годишњег стратешког плана ради идентификовања кључних стратешких ризика организације.
- Потпуна информисаност о профилу променљивих ризика организације путем одржавања кварталних састанака са онима који су одговорни за израду стратешког плана.
- Израда универзума ризика која јасно повезује све пословне активности из перспективе ризика за вредности које поседују акционари.
- Груписање ризика на основу њихових међусобних односа. На пример, у оквиру сваке групе, утицај одређених ризика може да се повећава, или смањује, у зависности од тога да ли други ризици расту или опадају. Такође, у зависности од тога да ли се одређени ризик преноси или дели, може да се јави неки други ризик. Разумевање чињенице да постоје такви утицаји и узајамна зависност, омогућује боље разумевање који су ризици критични и захтевају више пажње.
- Обезбеђење кварталне комуникације са руководством, од нивоа највишег руководиоца према доле, у складу са расположивим вре-

меном и средствима, како би се утврдило мишљење руководства о најновијим стратешким ризицима за организацију.

Када се ризици утврде на највишим нивоима организације, може да се изради оквирни модел ризика специфичан за предузеће. Такви оквирни модели обично ризике сврставају у три до пет категорија, које се даље деле на подкатегије. Са променом стратешких ризика, иновира се и оквирни модел како би се обухватило ново настало окружење ризика. Овај оквирни модел често користи и директор интерне ревизије, да би одредио степене ризика у свету ревизије и развио годишњи план ревизије.

Микро процена

Процена ризика током одређене ревизије конципирана је тако да се идентификује и процени изложеност ризицима на нивоу активности, или на микро нивоу. Поред разумевања производа, услуга, тржишта и других стратешких питања одређеног посла, ефикасна процена на одређеном нивоу захтева од ревизорског тима да размотри ризике пословног процеса, квалитет локалног руководног тима, и различите начине на које појединци могу да се понашају у различитим ситуацијама.

Интерни ревизори процене ризика изводе према оквирном моделу ризика, где су ризици разврстани у категорије и подкатегије. Оквирни модел ризика организације развијен на макро нивоу постаје једно од оруђа које се користи за такве микро процене. Током сваке ревизије, ревизорски тим са оперативним руководством разматра једну по једну подкатегију ризика, постављајући питања о томе да ли у радном окружењу постоје специфични ризици који се уклапају у одговарајућу подкатегију. Категорије тако могу да помогну да се развију идеје и учине мање вероватним да се превиди појава неког значајнијег ризика.

Други приступ се ослања на пословне циљеве неке функције на њеном полазишту. Од руководства се тражи да за сваки циљ идентификује активности, услове или догађаје који би могли да спрече остварење тог циља. Оваква листа препрека представља ризике са којима је свака пословна функција суочена.

Други начини да се ризици идентификују и процене на микро нивоу, од којих се неки обављају ван текуће ревизије, обухватају:

- Организовање семинара за процену ризика за оперативно особље, чиме се даје нова димензија у изради профила организационих ризика.
- Спровођење континуалних процедура ревизије, током којих се траже потенцијални проблеми у некој области на непрекидној основи. Примери обухватају: праћење неочекиваног повећања трошкова у датој области, повећање флукуације особља и кључних показатеља резултата пословања. Такво праћење активности у реалном времену омогућава ревизорском тиму да брже обавести власнике о ризицима, и да одлучи да спроведе иначе непланирану ревизију на основу откривених аномалија.
- Учешће у пројектним тимовима који раде на пројектима високог ризика или на реализацији нових процеса. Такви тимови се обично формирају пре почетка посла, што интерним ревизорима омогућава да делују као консултанти и да помогну у идентификацији ризика и могућих решења од самог почетка. Тако се прикупљају подаци о ризицима и они могу да се користе касније приликом планирања ревизије.

Када је извршена процена ризика, ревизорки тим користи резултате процене функционалних ризика како би обавио ревизију те области. Наглази процене ризика могу да помогну ревизорима да установе на која питања треба да обрате посебну пажњу, да ли би у датом случају с обзиром на врсте ризика више одговарао други тип ревизије, и да ли ревизија треба да буде одложена, или сасвим отказана.

Интерни ревизори ће увидети да је поступак у коме би они сами израдили листу ризика без учешћа других и затим је користили да укажу руководству и особљу на ризике, осуђен на пропаст. Много су ефикаснији тимски приступи процене ризика, уколико је процена ризика од горе према доле и од доле према горе међусобно повезана, уместо да буду независне и да се не базирају једна на другу.

Интерни ревизори треба да обрате пажњу да не идентификују сувише много ризика, јер би то могло да доведе до ситуације да брод који тоне не добије одговарајућу пажњу. Многи стручњаци као основно правило препоручују да се идентификује петнаест до двадесет пет значајних ризика. Стручњаци сматрају да су оперативни и стратешки ризици најважнији за остварење циљева. Пет најзначајнијих питања обухвата неуспех у управљању значајнијим пројектима, неуспех стратегије, неуспех у иновацијама,

лоше управљање у погледу репутације и трговачког имена, недостатак мотивације запослених и лоши резултати рада.

УВЕРАВАЊЕ О ЕФЕКТИВНОСТИ ПРОЦЕСА УПРАВЉАЊА РИЗИКОМ

Уз обављање ревизије засноване на управљању ризиком, корисно би било ако би се обавила и ревизија самог процеса управљања ризиком у компанији. Компанија не мора да има формално имплементиран процес УРП да би таква ревизија била корисна. Ревизија колико ефективно предузеће управља ризицима до прихватљивог нивоа, било да се то ради формално или неформално, је важна за управу. Интерни ревизори треба да дају информације колико ефективно предузеће управља или колико ће ефективно и даље управљати својим кључним ризицима до прихватљивог нивоа. Ревизија ће пружити предузећу значајан увид у потенцијалне активности које ће јој помоћи да боље спроведе активности управљања ризиком.

Интерни ревизори морају да прате и процењују систем за управљање ризицима (2110.A1). Стандард интерне ревизије за спровођење ревизије (2110. A1) јасно наводи да интерни ревизори, у оквиру својих активности, треба да анализирају систем за управљање ризицима за потребе надзорног одбора и вишег руководства. Ово представља нову област за већину одељења интерне ревизије. Нема пуно организација које су утврдиле процесе за обезбеђење адекватности и ефикасности процедура за управљање ризицима. У *Практичним саветницима* и другим изворима наводе се савети како да се оствари овај циљ. У *Практичном саветнику 2110-1* наводе се следећи савети за успостављање процеса процене система за управљање ризицима:

- Ревизорски тим треба да да највиши значај развоју поступка процене и извештавања о систему за управљање ризицима.
- Циљ процене система за управљање ризицима јесте да се испитају, процене, напишу извештаји и дају препоруке за побољшање адекватности и ефикасности процеса управљања ризицима.
- Друге две активности које се траже у Стандардима у вези са ризицима, идентификација и процена изложености ризицима и примена анализе ризика у планирању ревизије, нису довољне када се ради о задатку процене процеса за управљање ризицима.

Да би се образовало мишљење о укупној адекватности програма за управљање ризицима, *Практични саветник 2110-1* наводи да интерни ревизори треба да утврде да се процесима за управљање ризицима остварује пет кључних циљева:

- Идентификовање и утврђивање приоритета ризика који настају из пословне стратегије.
- Руководство и управни одбор треба да утврде који је ниво ризика прихватљив за организацију, укључујући прихватање ризика за извршавање стратешких планова организације.
- Активности на смањењу ризика треба да буду пројектоване и спроведене да би се смањило, или на други начин контролисао ниво ризика који је прихватљив за руководство и управни одбор.
- Спровођење сталних активности праћења ради периодичне процене ризика и ефикасности контроле ризика.
- Периодично извештавање руководства и управног одбора о резултатима процеса за управљање ризицима.

Поред ових пет примарних подручја, постоје и друга питања, односно процеси процене управљања ризицима, које треба узети у обзир када се процењује ефикасност активности управљања ризицима:

- Да ли су процеси управљања ризицима одговарајући за природу делатности организације? У зависности од величине и сложености пословне делатности, процеси управљања ризицима могу да буду формални, неформални, квантитативни или субјективни, и да буду смештени у пословне јединице или централизовани на нивоу компаније. Да ли примењени процес управљања ризицима одговара култури, начину управљања и пословним циљевима организације?
- Да ли је методологија управљања ризицима свеобухватна?
- Да ли кључне групе и појединци који се баве управљањем, укључујући управни одбор и одбор за ревизију разумеју методологију?
- Да ли се на управљање ризицима гледа као на одговорност коју сви имају, или на одговорност једне функције, као што су ревизија или функција управљања ризицима?
- Да ли су сви упознати са документима о начину понашања и управљању ризицима?
- Да ли постоји заједнички речник за управљање ризицима који се користи у целој организацији?
- Да ли постоји одговарајућа свест о главним пословним циљевима компаније и значајним ризицима?

- Да ли су пословни циљеви, ризици и контроле исправно усаглашени?
- Да ли особље довољно добро разуме ризике који су релевантни за појединачне задатке које обавља?
- Да ли особље има довољно знања о основама доброг управљања ризицима и интерне контроле?
- Да ли запослени разумеју сврху контроле? Да ли имају развијен осећај власништва у вези са својим пословним процесима и потенцијалним ризицима за остварење циљева?
- Да ли запослени и спољни консултанти поседују довољно знања, обучености и алате да подрже остварење циљева компаније и да на ефикасан начин управљају ризицима?
- Да ли у буџету за обуку има довољно средстава за обуку у области управљања ризицима?
- Да ли је оперативно особље укључено у идентификацију и реаговање на промене и примену механизма за рано упозорење?
- Да ли је присутан напор да се код запослених развије свест о томе да „ствари треба исправно да се ураде у првом покушају“?
- Да ли постоји одговарајућа и јасна одговорност за испуњење циљева компаније и управљање одговарајућим ризицима?
- Да ли се на различитим нивоима компаније одржавају округли столови и семинари о управљању ризицима и интерној контроли?
- Да ли постоји свест о „покретачким“ догађајима, или учесталости догађаја, за сваки значајнији ризик који треба да упозори руководство на потенцијално значајан проблем?
- Да ли су успостављени индикатори који ће у раној фази да упозоре на неуспех пројекта?
- Колико брзо може организација да реагује на промене у компанији и спољном окружењу?
- Да ли постоје политике и процедуре које описују како треба да се управља већим ризицима?
- Да ли су те политике и процедуре транспарентне и на одговарајући начин саопштене?
- Да ли се одмах примењују неопходне мере за исправку значајнијих пропуста или слабости у организацији?
- Колико су добро најбоље праксе и идеје за унапређење пословања раширене у компанији?

- Колико је поуздано извештавање руководних нивоа о питањима управљања ризицима?
- Да ли постојећи систем информисања даје упавном одбору и руководству довољно унапред упозорења о потенцијалним проблемима? На пример, да ли они добијају правремена упозорења о томе да ли су клијенти задовољни и о понашању запослених?
- Са променом ризика, да ли више руководство и управни одбор имају довољно информација да ефикасно реагују?
- Да ли постоје путеви комуникације којима ће људи да извештавају о сумњи да постоји кршење правила, или друге неправилности?
- Да ли је средина таква да се људи охрабрују да извештавају о проблемима, уместо да „седе на њима“?
- Да ли политика награђивања и захтеви о понашању на раду подстичу добро управљање ризицима и стварно спречавају преузимање безобзирних и лоших ризика?
- Да ли постоји одговарајућа координација активности различитих делова организације?
- У којој мери извршни комитети стављају питања управљања значајнијим ризицима на свој дневни ред?
- Да ли се ризик сматра за приоритетно питање у свакој прилици када се унапређују пословни процеси?
- Да ли су кључне контроле финансијског пословања, оперативног пословања и усклађености са захтевима најсавременије?
- Да ли налази процене управљања ризицима указују на потребу интензивнијег праћења система за управљање ризицима?

Практични саветник 2100-1 даје неколико упутстава за одређивање адекватности и ефикасности било којег система укључујући интерну контролу и системе управљања и управљања ризицима. Да би се одредило да ли је систем адекватан, интерни ревизори би требало да размотре план процеса управљања ризицима да би одредили колико су они ефикасни и економични. Ефикасно осмишљени процеси реализују циљеве прецизно, благовремено и на економичан начин. Економично осмишљени процеси реализују циљеве и задатке уз минималну употребу ресурса. Да би проценили да ли је систем ефикасан, интерни ревизори морају размотрити колико добро руководство управља, или руководи, процесима управљања ризицима.

ИЗВЕШТАВАЊЕ О УПРАВЉАЊУ РИЗИКОМ ПОСЛОВАЊА

Ефективно саопштавања налаза ревизије и кључних активности је основа за реализовање вредности ревизије засноване на управљању ризиком. Када ревизор утврди који ће налази и препоруке бити укључени у извештај, време је да се сачини нацрт извештаја. Има много различитих начина извештавања и формата који се користе и сви могу ефективно да задовоље потребе корисника ревизије. Иако ни један конкретан стил или формат не мора бити бољи од другог, постоје одређени елементи извештавања који могу да буду корисни у саопштавању резултата ревизије засноване на управљању ризиком. Ти елементи пружају читаоцу извештаја следеће:

- Генерални закључак или резиме ревизије;
- Оцене колико ефикасно се управља сваким кључним ризиком до прихватљивог нивоа; и
- Везу између налаза и ризика.

Односно када се утврди које налазе треба укључити у формални ревизорски извештај, ревизор треба да обезбеди да горенаведене три ставке буду адекватно документоване у извештају.

Генерални закључак или извршни резиме

Читаоци извештаја воле да добију коначан закључак или резиме налаза ревизије. Код ревизије засноване на управљању ризиком, тај резиме треба да се фокусира на укупну ефективност управљања ризиком. Ревизор то може да оствари кратким параграфом који садржи текст сличан овоме који следи (у зависности од снаге активности управљања ризиком):

- **Снажно управљање ризиком** – „Укупно гледајући, ризицима који се односе на процес ХУЗ се доследно и ефективно управља до прихватљивог нивоа. Иако можда има места за одређена побољшања, у овом тренутку се никакве значајне промене у активностима управљања ризиком се не сматрају неопходним.“
- **Умерена ефективност управљања ризиком** – „Укупно гледајући, ризицима који се односе на процес ХУЗ се уобичајено управља до прихватљивог нивоа; међутим, има простора да се побољша пројекат (и/или функционисање) процеса како би се обезбедило да се тим ризицима доследно управља до тог нивоа. Најважнија побољшања се односе на...“

- **Слаба ефективност управљања ризиком** – „Укупно гледајући, ризицима који се односе на процес ХУЗ се не управља доследно до прихватљивог нивоа, што представља велику изложеност ризику у овој области. Постоји неодложна потреба да се побољша пројекат (и/или функционисање) процеса, посебно када се ради о...“

Иако формати и стилови извештавања варирају од компаније до компаније, директори воле да прочитају коначан закључак или резиме пре читања детаља. Зато је препоручљиво да се резиме налази на првој страни извештаја. Многа ревизорска одељења имају тај резиме у форми првог пасуса извештаја.

Оцене ефективности индивидуалног управљања ризиком

Уз генерални закључак о ефективности управљања ризиком, ревизор треба да оцени колико ефикасно се управља сваким индивидуалним ризиком до прихватљивог нивоа. Ове процене иду у прилог коначном закључку и такође управи дају увид у конкретна подручја ризика у којима може доћи до изложености. То управи може да помогне да обезбеди да се фокусира на своје ресурсе у најкритичнијим областима. Ефикасност управљања ризиком се означава са: снажно, умерено или слабо.

Веза између налаза и ризика

Ревизија заснована на управљању ризиком може да идентификује прилике за побољшање и пројекта и функционисања процеса. Основни недостаци се односе на то колико ефективно се ризицима управља до прихватљивог нивоа. Зато налазе треба повезати са предметним ризицима као подршку оцени ефективности управљања ризиком за сваки индивидуални ризик.

Друга опција је да се сваки ризик наведе са предметним налазима и препорукама одмах испод ризика. Свакако да постоје многи други начини документовања ове везе. Главни фокус ревизора је да се обезбеди да веза буде јасна како би ишла у прилог индивидуалним оценама ефективности управљања ризиком.

УЛОГА ИНТЕРНОГ РЕВИЗОРА У КОНТРОЛИ РИЗИКА

Питање прихватљивог нивоа ризика зависи од односа између надзорног одбора, менаџмента и интерног ревизора. Надзорни одбор (у банкама је то управни одбор) утврђује такозвани прихватљив ниво ризика, односно апетит према ризику (склоност ка ризику – *Risk Appetite*), који менаџмент прихвата увођењем одговарајућих контрола ризика. У међувремену интерни ревизор ће обезбедити објективне извештаје о систему интерне контроле. Ови извештаји о ревизији ће садржавати преглед нивоа до којег је резидуални ризик, после узимања у обзир контрола, прихватљив, а то значи да ли је овај ризик у складу са дефинисаним апетитом за ризик односно прихватљивој склоношћу ризику. Овај циклус зависности је веома значајан и ослања се на одговарајућа посматрања прихватљивог нивоа ризика.

Изазов за ревизију постаје једноставан, а то је помоћи увођење и добро функционисање управљања ризиком у предузећу у свим процесима. “Функција интерне ревизије треба да помогне организацији тако што ће се идентификовати и оценити значајну изложеност ризику и допринети унапређењу система за управљање и контролу ризика.”⁷ Управљање ризиком предузећа обезбеђује менаџменту функционисање процеса за постављање циљева, и да ти одабрани циљеви подржавају мисију субјекта, који су усклађени са њоме и са апетитом за ризик.

Концепт прихватљивог нивоа ризика има неколико импликација када је у питању интерни ревизор. Потребно је да интерни ревизор утврди који ниво ризика менаџмент прихвата, пре него што почне да обавља компетентан ревизијски посао. “Пре него што оцени контроле менаџмент треба да утврди ниво ризика који он жели да прихвати у области која је предмет прегледа. Интерни ревизори треба да утврде који је то ниво ризика. Он треба да се утврди у контексту смањења потенцијалног утицаја кључних опасности за постизање важнијих циљева за област која је предмет прегледа.”⁸ Контроле које оцењује интерна ревизија ће се обављати повезано са нивоом ризика према којем контрола треба да се одвија. “Када се утврди тај ниво, контроле које сада функционишу се могу оцењивати да би се утврдило колико се очекује да су оне успешне у вези са смањењем ризика до жељеног нивоа.”⁹

7 Institute of Internal Auditors, Standard 2110.

8 Institute of Internal Auditors, Practice Advisory 2120. A4-1.

9 Исто.

Ревизори могу такође да сарађују са менаџерима да би их научили идентификацији ризика и упознали са начином на који се ризик смањује на прихватљив ниво. Уколико менаџмент није утврдио кључне ризике и ниво ризика који жели да преузме, интерна ревизија је у могућности да им помогне кроз радионице за утврђивање ризика или других техника које се користе у организацији.

Када интерни ревизор идентификује и оцени ризике, онда је његов посао да тражи контроле које су уграђене да би штитиле од ризика. О контролама које су неадекватне или неефикасне мора се одмах дискутовати са менаџерима организационог дела где се врши ревизија о предузимању корективних акција. Ефикасност интерне контроле представља степен на коме ће ризик бити или елиминисан или смањен обзиром на предложене контролне мере. Трошкови ефикасности интерне контроле су у сагласности са трошковима испуњења контроле која се пореди са очекиваном коришћу од смањеног ризика.

ПОБОЉШАЊЕ УПРАВЉАЊА РИЗИЦИМА И СИСТЕМА КОНТРОЛЕ

Интерни ревизори морају помоћи да се побољша управљање ризицима и системи контроле (Стандард 2110). Други елемент *Стандарда* за управљање ризицима захтева да у свим пословима ревизије ревизори испољавају иницијативу за побољшање ефикасности управљања ризицима. Посебне сугестије интерни ревизори дају кроз побољшање система интерне контроле. Апсолутно је неопходно да интерни ревизори разумеју да је развијање процеса управљања ризицима интегрални и неопходни део сваке активности усмерене на побољшање интерне контроле.

Суштински елемент ефикасног управљања ризицима јесте потпуно разумевање чињенице **шта су ризици**. У ревизорском смислу ризик се може дефинисати као неизвесност појаве догађаја који би могао негативно да се одрази на остварење циљева. За сврхе управљања, седам кључних питања, наведених у даљем тексту, могу послужити за утврђивање ризика по организацију и за утврђивање потенцијалних начина контролисања или ублажавања изложености ризицима. Следе четири питања идентификовања и кватификовања ризика и три питања која се односе на управљање ризиком и његово ублажавање:

- Шта би могло да се деси и што би негативно утицало на способност организације да оствари своје циљеве и спроведе своје стратегије? (Претње)
- Ако се то деси, какав је потенцијални финансијски ефекат? (Губитак вредности услед изложености ризику)
- Колико често би такав догађај могао да се дешава? (Учесталост)
- Колика је вероватноћа одговора на прва три питања? (Неизвесност)
- Шта се може урадити у циљу спречавања и избегавања, ублажавања и откривања ризика и обавештавања? (Мере заштите и контроле)
- Колико ће то коштати? (Трошкови заштите и контроле)
- Колико би то било ефикасно? (Анализа трошкова/користи или анализа приноса на инвестицију)

Интерни ревизори могу да чине и следеће активности за побољшање управљања ризицима:

- У сваки ревизорски извештај унети детаљну информацију о ризицима, не само у смислу упозорења руководству о подручјима која су изложена потенцијалним ризицима, већ и у смислу доказа о последицама такве изложености, као што је анализа којом се квантификују трошкови ризика. Такве додатне информације помажу руководству да брже реагује на препоруке.
- Ревизори треба да имају едукативну улогу у односу на цело предузеће, посебно на нивоима на којима се доносе стратешке одлуке.
- Повезивање тимова за управљење ризицима или радних група. Ревизори су идеални за активности као што је прикупљање, анализа и припрема историјских података за екстерне консултанте који се ангажују ради процене изложености ризицима, јер поседују потребне ресурсе, познавање система и вештине. Други задаци који одговарају интерним ревизорима укључују организовање групних састанака посвећеним идентификацији ризика и решавању проблема, или помагању оперативним руководиоцима да разумеју релативни значај његових активности за укупну изложеност предузећа ризицима.
- Документовање утврђених техника ублажавања ризика путем састављања референтних приручника о методама управљања ризицима у свакој функционалној области.
- Залагање за успостављање и учешће у раду форума за управљање ризицима, у чијем се саставу често налазе директори делатности, руководиоци пословних јединица и ревизори, који стално про-

цењују и прате профиле ризика сваке пословне јединице. Такви форуми уводе технике и процесе управљања ризицима на нивоу пословне јединице путем идентификовања ризика и ублажавајућих контрола, дефинисања позиција за деловање, праћења активности на ублажавању ризика, достављања периодичних извештаја о ризику и састављања и спровођења планова за смањење ризика. Ревизори могу на ефикасан начин да допринесу том задатку постављајући се као посредници и консултанти у оквиру групе и доприносећи ефикасности укупног процеса управљања ризицима.

- Помоћ у реализацији система за управљање ризицима, што може да укључује преузимање консултантске улоге да би се побољшали основни процеси, при чему треба водити рачуна да се не наруши независност ревизора.

Многе од ових активности спадају у домен консултантске функције. Више руководство предузећа и надзорни одбор треба да одлуче какву ће улогу имати, и да ли ће је уопште имати, интерна ревизија у управљању ризицима организације. Када се то једном одлучи, ове одговорности треба да буду документоване у Повељи о раду интерне ревизије.

ЗАКЉУЧАК

Органи управљања предузећем су одговорни за идентификовање, процењивање и управљање ризицима. Интерна ревизија има задатак да олакша идентификацију и процену ризика и да прати колико се добро управља ризицима предузећа. Она треба да прати, процењује и допринеси побољшању управљања ризицима.

Ризици настају у вези са кључним пословним активностима и компонентама, као и у вези са стратегијама, процедурама, производима, функцијама и структурама. Поред тога, ризици настају и изван организације, нпр. од конкуренције и тржишта. У свакој организацији има бесконачно много ризика. Нажалост, неке организације немају довољно ресурса да идентификују, анализирају, и да контролишу ризике којима су изложене. Увођење формалних процедура процене ризика обезбеђује конзистентан и рационалан метод за одабирање специфичних ризика на које треба да се усмери рад интерне ревизије.

SUMMARY

INTERNAL AUDIT WORK FOR RISK MANAGEMENT IN COMPANIES

In recent years, internal audit has been given an important role in risk management in the companies, although risk management remains a key responsibility of senior management and the board. Treatment of risk by internal audit is required by the Law on Enterprises, the Law on Banks, Insurance Law, and other laws. Internal audit has a wide mandated coverage that includes financial risks, operational risks, the risks of information technology, legal and strategic risks, at both macro and micro levels. To determine the existence of adequate risk management processes, and that these processes are adequate and effective, the boards in this role may require support of internal audit activities - through testing, assessment, reporting and recommending improvements regarding the adequacy and effectiveness of risk management. Internal auditors work through the assurance and consulting function in order to identify, evaluate and implement a methodology for risk management and controls to manage these risks.

Key words: internal audit, risk management, risk categories, company, risk assessment.

ЛИТЕРАТУРА

1. Bolton, G., „Organisational risk management“, *Internal Auditor*, October 1999.
2. Committee of Sponsoring Organizations, *Enterprise Risk Management*, COSO, September 2004.
3. McNamee, D., & Georges, S., *Risk Management: Changing the Internal Auditor's Paradigm*, Institute of Internal Auditors Research Foundation, December 1998.
4. Economist Intelligence Unit in cooperation with MCC Enterprise Risk, *Enterprise Risk Management – Implementing New Solutions*. The Economist Intelligence Unit, 2001.
5. Jerry A. Miccolis, Kevin Hively, Brian E. Merkley, *Enterprise Risk Management – trends and Emerging Practices*, The Institute of Internal Auditors Research Foundation, 2001.
6. Sobel, P., “Integrating Risk Management and ERM”, *Auditors Risk Management Guide*, Chicago: CCH Incorporated, 2004.
7. Professional Briefing Note Thirteen, Managing Risk, IIA UK, *Internal Audit's Role In Managing Risk*.

8. Standards Australia and Standards New Zealand, *Australian/New Zealand Standard 4360:1999: Risk Management*, Standards Australia and Standards New Zealand, 1999.
9. Stanišić, M., *Interna kontrola i revizija*, Univerzitet Singidunum, Beograd, 2015.
10. The IIA-UK and Ireland, *Position Statement on Risk Based Internal Auditing*, London, 2003.
11. The Institute of Internal Auditors, *International Professional Practices framework*. Altamonte Springs, FL: Institute of Internal Auditors, 2011.
12. The Institute of Internal Auditors, *The Role of Internal Auditing in Enterprise-wide Risk Management*, IIA, USA, 2004.

Овај рад је примљен **19.08.2015.** а на састанку редакције часописа
прихваћен за штампу **09.11.2015.** године.