

ПРИСТУП МЕТОДОЛОГИЈИ ИНТЕГРАЛНОГ УПРАВЉАЊА РИЗИКОМ У ОРГАНИЗАЦИЈИ

Зоран Кековић

Универзитет у Београду, Факултет безбедности

Горан Глишић и Ненад Комазец

Министарство одбране Републике Србије, Војна академија

У динамичном окружењу свака организација би морала да обезбеди процес управљања ризицима, који ће бити у стању да непрестано детектује промене и одговара на њих. Методологија процене ризика описана у овом раду је општег карактера и стога може бити примењена на широк спектар активности, одлука и операција било којих јавних, приватних или друштвених предузећа, асоцијација, група или појединаца. Ипак, њена примена подразумева одређене предуслове којима се овај рад такође бави.

Кључне речи: *ризик, организациони циљеви, иштићене вредности, методологија процене, управљање ризицима.*

Увод

Независно од врсте и величине, организације се суочавају са ризицима који могу утицати на остваривање њихових циљева. Ти циљеви могу се односити на разне организацијске активности, од стратешких иницијатива до операција, процеса и пројеката, и могу се огледати у друштвеним, заштитним, безбедносним и исходима који се односе на окружење, затим у виду комерцијалних, финансијских и економских мера, друштвених, културних, политичких, као и утицајима на репутацију.

Све активности организације укључују ризике којима се мора управљати. Процес управљања ризицима доприноси одлучивању тиме што узима у обзир неизвесност и могућност појаве будућих, намераваних или ненамераваних, догађаја и околности и њихових утицаја на прихваћене циљеве.

Суштинска фаза управљања ризицима је процена ризика. У оквиру систематизације радних места у разним пословним јединицама и организацијама формирано су тимови за процену ризика, а оперативном особљу је у опису радног места, као један од радних задатака, наведено и поштовање начела управљања ризицима. Руководиоцима је као обавеза прописано праћење спровођења, као и вођење релевантних евиденција и прикупљање података од значаја за управљање ризицима. На тај начин управљање ризицима постаје саставни део организационе културе, са визијом да постане доминантан метод у пословању.

Основни предуслови

При процени ризика организација мора да обави процес идентификације, анализе и оцене свих разумно предвидивих ризика, као што су: општи пословни, ризици на раду и у радној околини, правни ризици, ризици од криминалног деловања, од деловања нелојалне конкуренције, од деловања осталих трећих лица, од пожара и елементарних непогода, као и од неусаглашености организације корисника са стандардима менаџмента квалитетом организације.

Основни оперативни приоритети у изради и примени методологије за процену ризика су *нормативно регулисање* те материје, као и *информатичка подршка*.

Нормативно регулисање подразумева следеће поступке у изради и примени методологије за процену ризика:

- одредити параметре за оцену нивоа ризика и односне акције;
- прописати све обрасце у области процене ризика, начин попуњавања и примене;
- прописати начин комуникације између организационих јединица одговорних за послове процене ризика – узимајући у обзир правила сигурности, безбедности и заштите података;
- систематизовати радна места која ће се бавити проценом и управљањем ризиком као јединим задатком са довољним бројем извршилаца;
- прописати поступак процене и управљања ризиком у промету роба и услуга, с обзиром на информатичка ограничења и потребу сарадње са другим субјектима;
- приступити дефинисању критеријума за повлашћене учеснике у поступку, како би им се одредио одговарајући статус и третирање у анализи ризика. Омогућити организацијама које послују у складу за законом брзо кретање роба и услуга у складу са принципима слободне трговине, а ресурсе усмерити ка стварним ризицима.

Испуњавањем тих предуслова моћи ће да се изради спроводиво оперативно Упутство о садржају и начину рада на пословима процене и управљања ризиком у области заштите лица, имовине и пословања привредних и других субјеката.

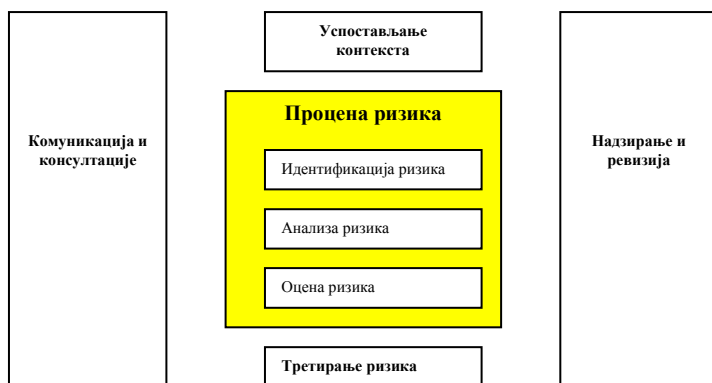
Имајући у виду досадашња искуства са временом потребним за израду и имплементацију процена ризика и неопходност увођења што квалитетнијих алата за процену ризика, у складу са новим ризицима, приступа се доради/допуни постојећих алата процене ризика, уз поштовање оперативних приоритета:

- активирање порука/налога процене ризика преко свих критеријума (већи број карактера – могућност уноса квалитетније поруке и налога за поступање);
- нови критеријум/допуна старих критеријума у складу са општим приоритетима безбедности;
- мерљивост резултата по врсти, броју, фискалном ефекту и сл.;
- аналитички алати у информативном систему;
- процена ризика у евиденцији идентификованих активности;
- утврђивање начина попуњавања записника о ризицима (исказ о ризицима);
- процена ризика при потврди услуге;
- обједињавање свих база података у јединствену базу података.

Од немерљивог значаја су претходно прикупљени подаци о свему што би могло помоћи при одређивању критеријума, као и њихова систематизација у употребљиву базу података. У том смислу користе се сазнања и подаци свих пословних јединица, али и разни јавно публиковани подаци, као и подаци других државних органа и организација, као што су нпр. МУП, БИА, Војска, Пореска управа, Народна банка, Агенција за привредне регистре и други.

Процес процене ризика

Процена ризика је свеукупан процес идентификовања, анализе и оцене ризика.¹



Слика 1 – Процес управљања ризицима¹

¹ ISO TC 223/SC: Управљање ризицима – Упутство о принципима и имплементацији управљања ризицима.

Идентификовање ризика

Идентификовање ризика подразумева процес проналажења, прописивања и карактерисања елемената ризика који су релевантни за циљеве управљања ризицима, односно процене ризика. Организација би требало да идентификује изворе ризика, догађаје или низ околности, као и њихове потенцијалне последице. Циљ тог корака је састављање *свеобухватне листе ризика* заснованих на оним догађајима и околностима које могу помоћи, спречити, умањити или успорити остваривање циљева. Свеобухватна идентификација и регистрација ризика је од суштинске важности, јер се ризик који у том стадијуму није идентификован искључује из даље анализе. Идентификација би требало да укључи све ризике без обзира на то да ли су под контролом организације или нису, односно и спољне и унутрашње.

У идентификовању ризика веома су битне релевантне и ажуриране информације, што се односи и на одговарајуће претходне информације о ризику, уколико је могуће доћи до информација такве врсте. Људи који имају одговарајуће знање такође би требало да буду укључени у идентификовање ризика. Након идентификовања онога шта би могло да се деси неопходно је узети у разматрање и узроке и сценарије који показују до каквих последица може доћи. Сви важнији узроци требало би да буду узети у разматрање.

При идентификовању ризика такође је важно узети у разматрање и ризике који су у вези са неискоришћеним приликама.

Анализа ризика

Анализа ризика односи се на разумевање ризика. Она пружа улазну информацију о оцени ризика и одлукама да ли ризици треба да се решавају и које су то одговарајуће (најприхватљивије) стратегије у третирању ризика. Обухвата разматрање узрока и извора ризика, њихових позитивних и негативних последица, као и вероватноћу појављивања тих последица. Такође, могу се идентификовати и фактори који утичу на појаву последица и вероватноћу њиховог појављивања. Ризик се анализира тако што се одређују последице и вероватноћа њиховог настанка, као и остале особине ризика. Догађај или низ околности могу имати вишеструке последице и утицати на већи број циљева. Такође, треба размотрити постојећу контролу ризика и њену ефикасност.

Начин на који су вероватноћа настанка ризика и његове последице изражени и начин на који се они комбинују ради оцењивања степена ризика варираће у зависности од типа ризика и сврхе у које ће се излазна информација о процени ризика користити. Сви они морају бити у складу са критеријумом ризика. Такође, важно је размотрити међузависност различитих ризика и њихових извора.

Сигурност у оцене ризика и њихова осетљивост на предуслове и претпоставке треба да буду размотрени у анализи и да ефективно буду пренети доносиоцима одлука и осталим заинтересованима уколико се то захтева. Фактори, попут размимоилажења у мишљењима експерата или ограничења моделима, треба да буду јасно предочени, а можда чак и наглашени.

Анализи ризика треба се прићи са различитим степеном детаљности, који зависи од ризика, сврхе анализе и информација, података и извора који су доступни. Анализа се може поделити на квалитативну, полуквантитативну и квантитативну или њихову комбинацију, у зависности од околности. У пракси, квалитативна анализа се често примењује прва ради долажења до опште индикације степена ризика и откривања највећих ризика. Где год је то могуће и одговарајуће, требало би да се изврши и одређенија, квантитативна анализа ризика као следећи корак.

Последице се могу одредити израдом модела исхода неког догађаја или низа догађаја, или екстраполацијом из експерименталних проучавања или из доступних података. Последице се могу изразити у виду одређених и неодређених утицаја. У неким случајевима неопходно је располагати са више од једне нумеричке или описне вредности како би се прецизирале последице за различита времена, места, групе или ситуације.

Оцена ризика

Циљ оцене ризика је помоћ у доношењу одлука на основу резултата анализе ризика о томе којим се ризицима треба бавити и о приоритетима третирања ризика.

Оцена ризика обухвата поређење степена ризика који су пронађени у току процеса анализе и критеријума за ризике који су утврђени у току разматрања читавог контекста. Циљеви организације и опсег околности до којих може доћи такође треба да буду разматрани. У ситуацијама где треба да се направи избор између опција, он ће зависити од контекста организације. Одлуке треба да узму у обзир шири контекст ризика и укључе разматрање толеранције ризика које су пронашле друге организације, а од којих организација има користи. Одлуке, такође, треба да узму у обзир законска ограничења.

Уколико степен ризика не задовољи критеријум за ризике – тим ризиком се треба бавити (ризик би требало да буде разматран – третиран).

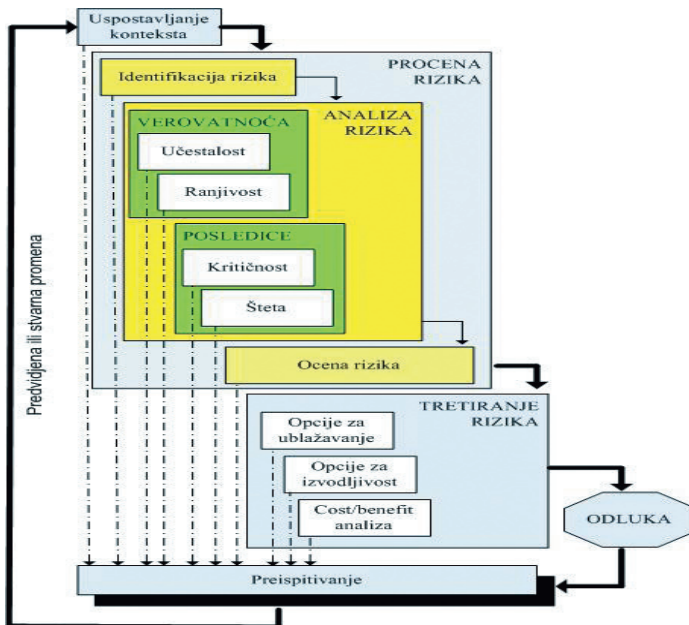
У неким условима оцена ризика може довести до одлуке о наставку даље анализе. Оцена ризика може, такође, водити и ка одлуци о томе да се ризик даље не ублажава ни на који други начин осим реализацијом постојеће контроле ризика. Та одлука зависиће од утицаја склоности организације ка ризику и постављених критеријума за ризике (које је она утврдила).

Методологија процене ризика

Да би било успешно и одрживо, управљање ризицима би требало да буде интегрисано у организацију и подржано од менаџмента. Концепт за управљање ризицима помаже организацијама да ефикасно управљају ризицима кроз примену процеса управљања ризицима на разним нивоима и у оквиру специфичних подручја организације. Такав концепт треба да омогући да се информације о ризику, настале у оквиру тог процеса, адекватно процесуирају и користе у доношењу одлука на релевентним нивоима организације.

Активном и свеобухватном проценом ризика менаџмент организације треба да:

- артикулише и одобри политику управљања ризицима;
- обавести све заинтересоване стране о предностима управљања ризицима;
- дефинише индикаторе перформанси (успеха) управљања ризицима који одговарају организационим перформансама;
- осигура подударност циљева управљања ризицима са циљевима и стратегијом организације;
- обезбеди законитост и сагласност са правним актима;
- обезбеди расподелу потребних ресурса за потребе управљања ризицима.



Слика 2 – Графички приказ методологије процене ризика

Ради дефинисања критеријума за процену ризика (поглавље 4), методологија процене ризика треба да обухвати следеће:

- Како ће бити дефинисана вероватноћа.
- Како ће бити утврђен ниво ризика.
- Природа и типови последица које се могу појавити и како ће се мерити.
- Ниво на ком ризик постаје подношљив / толеранција ризика.
- Временски оквир вероватноће и/или последице.
- Који ниво ризика захтева третирање.
- Да ли комбинација више ризика треба да се узме у обзир.

То је могуће постићи познавањем организације и њених односа са спољашњим и унутрашњим субјектима.

Штићене вредности организације су:

– номиналне (људи, средства, објекти, инсталације, постројења, информације...) и

– неноминалне (углед, имиџ, морал...).

Ризик од дешавања негативног догађаја, односно од реализације претњи у одређеној организацији, дефинишу одређени фактори. По месту и правцу деловања могу да се поделе на спољне и унутрашње.

Спољни фактори представљају активност различитих субјеката, догађаја или појава, а физички се не налазе у кругу или просторијама организације.

Спољни фактори могу бити:

- макролокација,
- микролокација,
- конкуренција.

Унутрашњи фактори представљају активност различитих субјеката, догађаја или појава, а физички се налазе у кругу или просторијама организације.

Унутрашњи фактори могу бити:

- историја негативних догађаја,
- усклађеност организације са прописима,
- величина организације,
- начин организовања,
- едукованост запослених,
- количина вредности у објекту – организацији,
- дневни број странака,
- постојеће обезбеђење.

Безбедност организације може бити нарушена деловањем претњи споља и изнутра. Претње споља могу бити:

1) Природне непогоде:

- а. земљотреси,
- б. поплаве,
- в. олује,
- г. пожари.

2) Напади:

- а. тероризам,
- б. паљевине,
- в. диверзије,
- г. крађе,
- д. преваре,
- ђ. разбојништва,
- е. индустријска шпијунажа,
- ж. рачунарски криминал.

3) Деловање конкуренције

Претње изнутра могу бити:

- а. криминалне радње запослених (саботаже, крађе, утаје, преваре, и сл.),
- б. рачунарски криминал,
- в. штрајкови,
- г. технолошке непогоде (пожар, експлозије, изливање отровних супстанци...).

Претње могу бити и комбиноване, а могућност реализације појединих претњи може да се прикаже нивоом ризика.

Ниво ризика је у директној зависности од учесталости понављања догађаја, рањивости система, односно постојећег стања заштите у систему и последица које се догађају по систем ако ризик прерасте у негативан догађај.

Процена ризика обухвата:

- израчунавање вероватноће реализације претње и
- последицу негативног догађаја.

Ниво ризика израчунава се по следећем обрасцу:

$$NR = V \times P$$

$$V = U \# R$$

$$P = \check{S} \# K$$

где је :

NR – израчунати (одређени) ниво ризика,

V – вероватноћа да одређени ризик резултира негативним догађајем,

P – последице или ефекат који негативан догађај оставља на вредности организације,

U – учесталост или фреквенција дешавања (појављивања),

R – рањивост или осетљивост организације на могућност реализације претњи и претварања у негативан догађај,

Š – штета, вредност (величина) оштећења штићене вредности на којој је негативни догађај изазвао последице,

К – критичност, вредност или важност штићене вредности за организацију на којој је негативан догађај изазвао последице.

Учесталост се односи на понављање одређене претње у неком периоду. Може се степеновати на следећи начин: 1 – врло ретко, 2 – повремено, 3 – често, 4 – претежно и 5 – веома често.

На пример: *организација – компанија за трговину нафтним дериватима. У протеклом периоду била је пет пута нападнута. Учесталост је 2 – повремено.*

Рањивост представља постојеће стање заштите организације, односно осетљивост организације на претње. Може се степеновати на следећи начин: 1 – врло велика, 2 – велика, 3 – средња, 4 – мала и 5 – врло мала.

На пример: *организација – компанија за трговину нафтним дериватима. Има само физичко обезбеђење. Рањивост 2 – велика.*

Вероватноћа представља комбинацију учесталости дешавања одређене претње и рањивости организације по датој претњи. Може се степеновати на следећи начин:

1 – ретко, 2 – мало вероватно, 3 – умерено вероватно, 4 – вероватно и 5 – скоро сигурно.

На пример: *организација – компанија за трговину нафтним дериватима. У протеклом периоду била је три пута нападнута. Има само физичко обезбеђење. Учесталост је 2 – повремено, рањивост 2 – велика, а вероватноћа 3 – умерено вероватно.*

Табела 1 – Матрица вероватноће

		Рањивост				
		Врло велика	Велика	Средња	Мала	Врло мала
Учесталост		1	2	3	4	5
Врло ретко	1	3	2	1	1	1
Повремено	2	4	3	2	2	1
Често	3	5	4	3	2	2
Претежно	4	5	4	3	3	3
Стално	5	5	5	4	3	3

Штета је мера оштећења вредности и може резултирати у различитим степенима. Штета се може степеновати са: 1 – врло мала; 2 – мала; 3 – средња; 4 – велика и 5 – врло велика.

На пример: *организација – складиште. Извршен је физички напад при којем је настала штета од 1.000 динара, јер је поломљено стакло на кућици чувара. Штета је 1 – врло мала.*

Критичност је мера вредности, односно важности штићене вредности за организацију. Може се степеновати према следећем: 1 – врло велика; 2 – велика; 3 – средња; 4 – мала и 5 – врло мала.

На пример: *организација – складиште. Извршен је физички напад. Нападнута је и оштећена кућица чувара. Критичност је 5 – врло мала.*

Последице представљају ефекат негативног догађаја по вредности организације, а манифестују се кроз величину губитка (штету) у односу на критичност (важност) штићене вредности. Последице се могу степеновати на следећи начин: 1 – врло лака; 2 – лака; 3 – средње тешка; 4 – тешка и 5 – изразито тешка.

На пример: *организација – складиште. Извршен је физички напад. Нападом је настао губитак од 1.000 динара, јер је поломљено стакло на кућици чувара. Нападнута је и оштећена кућица чувара. Штета је 1 – врло мала, критичност је 5 – врло мала, а последица је 1 – врло мала.*

Табела 2 – Матрица последица

КРИТИЧНОСТ		Врло велика	Велика	Средња	Мала	Врло мала
		1	2	3	4	5
ШТЕТА	1	3	2	1	1	1
	2	4	3	2	2	1
3	5	4	3	2	2	
4	5	4	3	3	3	
5	5	5	4	3	3	

Према нивоу ризика сви процењени ризици могу се сврстати у следеће категорије:

1. Врло мали ризик, занемарљив (NR = 1 и 2).
2. Мали ризик (NR = 3, 4 и 5).
3. Умерено велики ризик (NR = 6, 8 и 9).
4. Велики ризик (NR = 10, 12, 15 и 16).
5. Изразито велики ризик (NR = 20 и 25).

Табела 3 – Матрица ризика

ПОСЛЕДИЦЕ		Врло лаке	Лака	Средње тешка	Тешка	Изразито тешка
		1	2	3	4	5
БЕРОВАТНОЋА	1	1	2	3	4	5
	2	2	4	6	8	10
3	3	6	9	12	15	
4	4	8	12	16	20	
5	5	10	15	20	25	

Процењени ризици се према датој категоризацији могу сврстати у:

1) ПРИХВАТЉИВЕ (NR = 1, 2, 3, 4 и 5) и

2) НЕПРИХВАТЉИВЕ (NR = 6, 8, 9, 10, 12, 15, 16, 20 и 25).

По завршетку процеса процене ризика приступа се процесу третирања ризика. Избор одговарајуће опције за третирање ризика обухвата балансирање трошкова и напора у примени опције и користи која се може из тога извући.

Велики број опција за третирање ризика може бити разматран и примењен појединачно или у комбинацији. Организација може имати користи од усвајања комбинације опција за третирање ризика.

Одлуке треба да узму у обзир ретке, али озбиљне ризике који могу оправдати акције третирања ризика које нису оправдане (дозвољене) по строго економским правилима.

Ради ефективног третирања ризика, а на основу извршене процене, потребно је дефинисати:

- опције за ублажавање ризика,
- опције за изводљивост примењених стратегија и
- анализу односа цене и користи.

Опције за ублажавање

На основу степена прихватљивости ризика потребно је одредити стратегије којима се врши третирање ризика. Могу се применити следеће стратегије:

1. Избегавање ризика тако што се неће почети или наставити са активношћу која може довести до појаве ризика.
2. Тражење могућности за почетак или наставак активности која може довести до мањег ризика или га одржати.
3. Утицај на вероватноћу.
4. Утицај на последице.
5. Подела ризика са још једном или више страна.
6. Задржавање ризика, свесним избором или несвесно.

Опције за изводљивост

Свака опција за третирање ризика треба да буде узета у обзир по етапама процене ризика. Анализа сваке опције мора узети у обзир и цену измене процедура или производа у складу са мерама за третирање ризика.

На пример: *постоји реална опасност од крађа у продавницама мало-продаје. Могућа стратегија којом се елиминише ризик је затварање продавница и онемогућавање уласка лопова. Предложена стратегија није добра зато што затварањем продавница онемогућавамо улазак редовних муштерија и тиме угрожавамо посао.*

Дакле, потребно је пронаћи такву стратегију која ће омогућити нормално функционисање, а уједно спречити или свести на минимум могућност крађа.

Анализа цена/корист:

Анализа цена/корист је последњи корак у провођењу процене ризика с обзиром на предузете стратегије за третирање ризика. Потребно је утврдити колика је стварна цена имплементације предложених опција за третирање ризика и одредити величину финансијских и других трошкова који настају применом предложених мера.

На пример: *Нема смисла потрошити 100.000 динара на сигурносну опрему за спречавање крађе робе вредне 1.000 динара, нарочито ако се ризик од крађе може пренети на осигуравајућу кућу.*

Критеријуми за процену ризика

У табели 4 приказани су критеријуми за категорисање ризика, путем прорачунавања ризика из вредности вероватноће наступања догађаја и вредности могућих опасних последица догађаја.

Табела 4 – Критеријуми за категорисање ризика

КРИТЕРИЈУМ ЗА ПРОРАЧУН РИЗИКА					
Вероватноћа		Последица		Ризик	
Учесталост	Вредност	Озбиљност	Вредност	Категорија	Оцена
Ретко	0,1	Материјална штета која не прелази износ од <i>сто хиљада динара</i> или изазивање опасности за здравље људи или за имовину малог обима.	1	Оптимални – ризик прихватљив, редовно пратити стање	0–2
Мало вероватно	0,3	Материјална штета која прелази износ од <i>сто хиљада динара</i> или изазивање опасности за здравље или тело људи или за имовину мањег обима.	2	Средњи – ризик смањити на разумну меру.	3–4
Умерено вероватно	0,5	Материјална штета која прелази износ од <i>четристо педесет хиљада динара</i> или изазивање опасности за живот или тело људи или за имовину средњег обима или нарушавање пословног угледа или кредитне способности или одавање пословне тајне.	3	Висок – пре даљег рада мора се смањити ризик.	>4
Вероватно	0,8	Материјална штета која прелази <i>милион и петсто хиљада динара</i> или изазивање опасности за живот или тело људи или за имовину већег обима или одавање пословне тајне из користољубља.	4	Степен ризика добија се множењем бројчаних вредности вероватноће наступања опасности и последице, за сваку ставку из Листе ризика организације.	
Скоро извесно	1,0	Материјална штета која прелази износ од <i>пет милиона динара</i> или изазивање опасности за живот или тело људи или за имовину већег обима или одавање пословне тајне из користољубља или у погледу нарочито поверљивих података.	5		

Критеријуми за прорачун ризика

Учесталост		ВЕРОВАТНОЋА			НИВО РИЗИКА			В*П
		Равњивост	У#Р	Штета	Критичност	Ш#К		
1)	врло ретко – нема утицаја	врло велика – уопште нема заштите	ретко	врло мала – до 1.000 динара, стрес код људи	врло велика – потпуни прекид функционисања организације	врло лака	врло мали ризик, занемарљив	
								повремено – до 25%
3)	често – до 50%	средња – само техничка	умерено вероватно	средња – од 10.001 до 100.000 динара теже повреде код људи	средња – могуће функционисање уз повећане напоре и допунска средства	средње тешка	умерено велики ризик	
								претехно – до 75%
5)	веома често – преко 75%	врло мала – све врсте обезбеђења	скоро сигурно	врло велика – преко милион динара, људски губици	врло мала – решавање у ходу, редовним активностима	изразито тешка	изразито велики ризик	

Интегрално управљање ризиком

Од када је фокус процене ризика померен од ризика који потичу из једног извора (нпр. испуштање токсичних материја из индустријског постројења са великим локалним последицама) ка мултиплим изворима ризика (као што је испуштање карбон-диоксида са глобалним последицама по животну средину) порастао је значај интердисциплинарног приступа. Конвенционални приступ управљања ризицима који је, углавном, везан за дисциплинарну подвојеност замењен је холистичким и интегрисаним приступом. Елиминисање једног извора опасности може генерисати другу опасност. Даглас наводи пример азбеста, као средства превенције од пожара, чији је проналазак праћен великим публицитетом (Доуглас, М (1985) *Risk acceptability According to the Social Sciences*, New York: RusselSage Foundation). Много година касније откривена су штетна дејства азбестних влакана као извора плућних болести.

Л. Дринен и А. Меконил уочавају да, колико год да су прецизне процене ризика, не може се занемарити чињеница да су прихватљивост и толерантност на појединачне опасности у крајњем одређени људским фактором. С друге стране, индустријски и друштвени развој значе да се ризици константно мењају. Поменути примери имају велики утицај на развој методологије процене ризика. Наступањем интерних и екстерних догађаја контекст и знање се мењају, приступа се мониторингу и ревизији, неки ризици се појачавају и избијају на површину, док се други умањују. Организација би морала да обезбеди процес управљања ризицима, који ће бити у стању да континуирано детектује и одговара на промене.

Као резултат претходног увиђања потребно је све ризике представити на интегралној мапи ризика, што је изванредан алат који омогућава већу прегледност и систематичност ризика и хазарда, и нарочито бољу комуникацију са другим линијама и нивоима менаџмента. Што је још важније, мапе ризика омогућавају да се лакше уочавају везе између ризика и хазарда, па тиме и интердисциплинарни увид у царство ризика, са нагласком на континуираном развоју метода процена ризика.

Закључак

Све активности организације укључују ризике којима се мора управљати. Процес управљања ризицима доприноси одлучивању тиме што узима у обзир неизвесност и могућност појаве будућих догађаја и околности и њихових утицаја на прихваћене циљеве. Иако је пракса управљања ризицима развијана током времена и у домену различитих сектора, да би задовољила различите потребе, њен општи оквир, састављен од основних елемената, може допринети ефективном и кохерентном управљању ризицима у организацији.

Приступ управљању ризицима, описан у овом раду, може бити употребљен у оквиру широког спектра различитих контекста, као што су пројекти, функције, имовина, производ или активност. Избор одговарајућег приступа управљању ризицима подржаће и ојачати везе између одређених производа, активности или функција и општих циљева организације. То значи да је предуслов управљања ризицима разумевање и познавање неке организације, њених процеса, циљева, културе и контекста у којем она делује.

Ни најбоља методологија процене ризика не доноси сама по себи резултате. Управљање ризиком мора бити прихваћено као део рутинских послова организације и обавеза сваког појединца и пословне функције. То је оно што овај посао разликује од, на пример, управљања људским ресурсима, финансија, маркетинга и сл., где је прецизиран делокруг рада.

Литература

1. Douglas, M.: *Risk acceptability According to the Social Sciences*, New York: Russel Sage Foundation, 1985.
2. Drennan, L., McConnell, A.: *Risk and Crisis Management in the Public Sector*, Routledge, London and New York, 2007.
3. ISO TC 223/SC: Управљање ризицима – Упутство о управљању и имплементацији управљања ризицима.
4. ASIS INTERNATIONAL: General security risk assessment guideline.