UDK: 005.334

PRISTUP METODOLOGIJI PROCENE RIZIKA

*Keković Z.[1], Glišić G.[2], Komazec N.[2]
[1]*Fakultet bezbednosti, Univerzitet u Beogradu*
[2]*Vojna akademija, Beograd*

Sažetak: Metodologija procene rizika opisana u ovom radu je opšteg karaktera i stoga može biti primenjena na širok spektar aktivnosti, odluka i operacija javnih, privatnih ili društvenih preduzeća, asocijacija, grupa ili pojedinaca. Ipak, njena primena podrazumeva određene uslove kojima se ovaj rad takođe bavi.

Ključne reči: rizik, organizacioni ciljevi, štićene vrednosti, metodologija procene, upravljanje rizicima.

1. Uvod

Nezavisno od vrste i veličine, organizacije se suočavaju s rizicima koji mogu uticati na ostvarivanje njihovih ciljeva. Ti ciljevi se mogu odnositi na različite organizacijske aktivnosti − od strateških inicijativa do operacija, procesa i projekata, i mogu se ogledati u društvenim, zaštitnim, bezbednosnim i ishodima koji se odnose na okruženje, zatim u vidu komercijalnih, finansijskih i ekonomskih mera, društvenim, kulturnim, političkim, kao i uticajima na reputaciju.

Sve aktivnosti organizacije uključuju rizike kojima je potrebno upravljati. Proces upravljanja rizicima doprinosi odlučivanju tako što uzima u obzir neizvesnost i mogućnost pojave budućih, nameravanih ili nenameravanih događaja i okolnosti i njihovih uticaja na prihvaćene ciljeve.

Suštinska faza upravljanja rizicima je procena rizika. U okviru sistematizacije radnih mesta u različitim poslovnim jedinicima i organizacijama ob-

*Corresponding author: e-mail: zorankekovic@yahoo.com

razovani su timovi za procenu rizika, a operativnom osoblju u opisu radnog mesta je navedeno i poštovanje načela upravljanja rizicima kao jedan od radnih zadataka,. Rukovodiocima je, kao obaveza, propisano praćenje sprovođenja, kao i vođenje relevantnih evidencija i prikupljanje podataka od značaja za upravljanje rizicima. Na taj način, upravljanje rizicima postaje sastavni deo organizacione kulture, s vizijom da postane dominantan metod u poslovanju.

2. Osnovni uslovi

Pri proceni rizika organizacija obavlja proces identifikacije, analize i ocene svih razumno predvidivih rizika kao što su: opšti poslovni rizici, rizici na radu i u radnoj okolini, pravni rizici, rizici od kriminalnog delovanja, rizici od delovanja nelojalne konkurencije, delovanja ostalih trećih lica, od požara i elementarnih nepogoda, kao i od neusaglašenosti organizacije korisnika sa standardima menadžmenta kvalitetom organizacije.

Osnovni operativni prioriteti u izradi i primeni metodologije za procenu rizika su *normativno regulisanje* ove materije i *informatička podrška.*

Normativno regulisanje podrazumeva sledeće instrumente u izradi i primeni metodologije za procenu rizika:

1) odrediti parametre za ocenu nivoa rizika i odnosne akcije;
2) propisati sve obrasce u oblasti procene rizika, način njihovog popunjavanja i primene;
3) propisati način komunikacije između organizacionih jedinica odgovornih za poslove procene rizika – uzimajući u obzir pravila sigurnosti, bezbednosti i zaštite podataka;
4) sistematizovati radna mesta koja će se baviti procenom i upravljanjem rizikom kao jedinim zadatkom s dovoljnim brojem izvršilaca;
5) propisati postupak procene i upravljanja rizikom u prometu roba i usluga s obzirom na informatička ograničenja i potrebu saradnje s drugim subjektima, i
6) pristupiti definisanju kriterijuma za povlašćene učesnike u postupku, kako bi im se ustanovili odgovarajući status i tretman u analizi rizika.

Ispunjenjem ovih uslova moći će da se sačini sprovodivo operativno uputstvo o sadržaju i načinu rada na poslovima procene i upravljanja rizikom u oblasti zaštite lica, imovine i poslovanja privrednih i drugih subjekata.

Imajući u vidu dosadašnja iskustva s vremenom potrebnim za izradu i sprovođenje procesa procene rizika, kao i neophodnost uvođenja što kvalitetnijih alata za procenu rizika u skladu s novim rizicima, pristupa se doradi/dopuni postojećih alata procene rizika, poštujući operativne prioritete:

1) aktiviranje poruka/naloga procene rizika preko svih kriterijuma (veći broj karaktera − mogućnost unosa kvalitetnije poruke i naloga za postupanje);

2) novi kriterijum/dopuna starih kriterijuma u skladu s opštim prioritetima bezbednosti;

3) merljivost rezultata prema vrsti, broju, fiskalnom efektu i sl.;

4) analitički alati u IS;

5) procena rizika u evidenciji identifikovanih aktivnosti;

6) utvrđivanje načina popunjavanja zapisnika o rizicima (iskaz o rizicima);

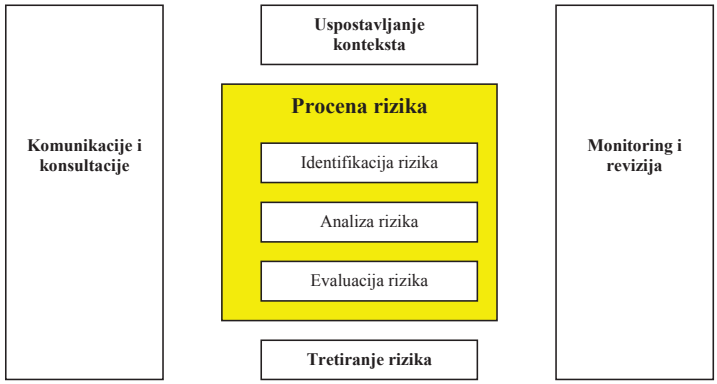
7) procena rizika pri potvrdi usluge, i

8) objedinjavanje svih baza podataka u jedinstvenu bazu podataka.

Od nemerljivog su značaja prethodno prikupljeni podaci o svemu što bi moglo pomoći pri određivanju kriterijuma, kao i njihova sistematizacija u upotrebljivu bazu podataka. U tom smislu se koriste saznanja i podaci svih poslovnih jedinica, ali i različiti javno objavljeni podaci, kao i podaci drugih državnih organa i organizacija kao što su, npr., MUP, BIA, Vojska, Poreska uprava, Narodna banka, Agencija za privredne registre i drugi.

3. Proces procene rizika

Procena rizika je sveukupan proces identifikovanja, analize i ocene rizika.



Slika 1 − *Proces upravljanja rizicima*[1]

[1] ISO TC 223/SC: Risk management – Guidelines on principle and implementation of risk management.

3.1. Identifikovanje rizika

Identifikovanje rizika obuhvata proces utvrđivanja i prepoznavanja elemenata rizika koji su relevantni za ciljeve upravljanja rizicima, odnosno procene rizika. Organizacija bi trebalo da identifikuje izvore rizika, događaje ili niz okolnosti, kao i njihove potencijalne posledice. Cilj ovog koraka je sastavljanje **sveobuhvatne liste** rizika, zasnovanih na događajima i okolnostima koji mogu kreirati, omogućiti, sprečiti, umanjiti ili usporiti ostvarivanje ciljeva. Sveobuhvatna identifikacija rizika je od suštinske važnosti jer se rizik, koji u ovom stadijumu nije identifikovan, isključuje iz dalje analize. Identifikacijom bi trebalo obuhvatiti sve rizike bez obzira na to da li organizacija njima već upravlja. Rizici se uvek identifikuju u odnosu na određene ciljeve, odnosno procenjuje se šta je pretnja određenim vrednostima. Štićene vrednosti organizacije možemo podeliti na: **nominalne** (ljudi, sredstva, objekti, instalacije, postrojenja, informacije...) i **nenominalne** (ugled, imidž, moral...).

Bezbednost organizacije može biti narušena delovanjem pretnji spolja i iznutra. Pretnje spolja mogu biti:

1) prirodne nepogode: zemljotresi, poplave, oluje, požari;
2) napadi: terorizam, paljevine, diverzije, krađe, prevare, razbojništva, industrijska špijunaža, kompjuterski kriminal, i
3) delovanje konkurencije.

Pretnje iznutra mogu biti:

1) kriminalne radnje zaposlenih (sabotaže, krađe, utaje, prevare i sl.);
2) kompjuterski kriminal;
3) štrajk, i
4) tehnološke nepogode (požari, eksplozije, izlivanje otrovnih supstanci...).

Pretnje mogu biti i kombinovane, a mogućnost realizacije pojedinih pretnji se može prikazati nivoom rizika.

Pri identifikovanju rizika veoma su bitne relevantne i ažurirane informacije. To se odnosi na odgovarajuće prethodne informacije o riziku ukoliko je do njih moguće doći. Oni koji imaju odgovarajuća znanja takođe bi trebalo da budu uključeni u identifikovanje rizika. Nakon identifikovanja onoga što bi moglo da se desi, neophodno je uzeti u razmatranje i uzroke i scenarije koji pokazuju do kakvih posledica može doći. Pri identifikovanju rizika takođe je važno uzeti u obzir i rizike u vezi s neiskorišćenim prilikama.

3.2. Analiza rizika

Analiza rizika pruža ulaznu informaciju za ocenu rizika i predstavlja uslov za odluku o tome da li je rizike potrebno tretirati, kao i koje su najprihvatljivije strategije za tretiranje rizika. Analiza rizika obuhvata razmatranje uzroka i izvora rizika, njihovih pozitivnih i negativnih posledica, kao i verovatnoću pojavljivanja tih posledica. Takođe je potrebno identifikovati činioce koji utiču na pojavu posledica i verovatnoću njihovog pojavljivanja. Prema mestu i pravcu delovanja, ti činioci se mogu podeliti na spoljne i unutrašnje.

Spoljni činioci predstavljaju aktivnosti različitih subjekata, događaja ili pojava, a fizički se ne nalaze u krugu ili u prostorijama organizacije. Spoljni faktori mogu biti:

a) makrolokacija;
b) mikrolokacija, i
v) konkurencija.

Unutrašnji činioci predstavljaju aktivnosti različitih subjekata, događaja ili pojava, a fizički se nalaze u krugu ili u prostorijama organizacije. Unutrašnji faktori mogu biti:

a) istorija negativnih događaja;
b) usklađenost organizacije s propisima;
v) veličina organizacije;
g) način organizovanja;
d) edukovanost zaposlenih;
đ) količina vrednosti u objektu – organizaciji;
e) dnevni broj stranaka, i
ž) postojeće obezbeđenje.

Rizik se analizira tako što se određuju posledice i verovatnoća njegovog nastanka, kao i ostale osobine rizika. Neki događaj može imati višestruke posledice i višestruko ugroziti ciljeve organizacije. Takođe, u razmatranje treba uzeti postojeće mere za kontrolu rizika i njihovu efikasnost.

Način na koji su verovatnoća nastanka rizika i njegove posledice izraženi i način na koji se oni kombinuju s ciljem ocenjivanja stepena rizika variraće u zavisnosti od tipa rizika i svrhe u koje će se izlazna informacija o proceni rizika koristiti. Svi oni moraju biti u skladu s kriterijumom rizika. Takođe je važno razmotriti međuzavisnost različitih rizika i njihovih izvora.

U analizi bi trebalo da budu razmotreni pouzdanost ocene rizika i njena osetljivost na stvarne uslove i pretpostavke, kao i njeno delotvorno prenošenje donosiocima odluka i ostalim zainteresovanim stranama ukoliko se tako zahteva. Činioci poput razmimoilaženja u mišljenjima stručnjaka ili ograničenja u modelima treba da budu jasno predočeni, pa čak i naglašeni.

Analizi rizika treba pristupiti s različitim stepenom detaljnosti, što zavisi od rizika, svrhe analize i dostupnih informacija, podataka i izvora. Analiza se može podeliti na kvalitativnu, polukvantitativnu i kvantitativnu, ili može predstavljati njihovu kombinaciju u zavisnosti od okolnosti. U praksi, kvalitativna analiza se često primenjuje kao prva da bi se došlo do opšte indikacije stepena rizika i otkrivanja najvećih rizika. Kad god je to moguće, trebalo bi izvršiti i određeniju, kvantitativnu analizu rizika kao sledeći korak.

Posledice se mogu odrediti izradom modela ishoda nekog događaja ili niza događaja, ekstrapolacijom iz eksperimentalnih studija ili dostupnih podataka. Posledice se mogu izraziti u vidu merljivih i nemerljivih uticaja. U nekim slučajevima, neophodno je raspolagati s više od jedne numeričke ili opisne vrednosti da bi se precizirale posledice za različito vreme, mesto, grupe ili situacije.

3.3. Ocena rizika

Cilj ocene rizika je pomoć u donošenju odluka na osnovu rezultata analize rizika o tome kojim se rizicima treba baviti i o prioritetima u tretiranja rizika.

Ocena rizika obuhvata poređenje stepena rizika dobijenog na osnovu analize i kriterijuma za rizike utvrđenim tokom razmatranja čitavog konteksta. Takođe, treba razmotriti ciljeve organizacije i okolnosti do kojih može doći. U situacijama kada treba napraviti izbor između opcija, on će zavisiti od konteksta organizacije. Prilikom odlučivanja treba uzeti u obzir širi kontekst rizika i toleranciju na rizike drugih organizacija od kojih organizacija ima koristi. Odluke takođe treba da uzmu u obzir zakonska ograničenja.

Ukoliko se stepen rizika ne može tolerisati s obzirom na postavljeni kriterijum za rizike, onda bi takav rizik trebalo tretirati, odnosno baviti se njime.

U nekim uslovima, ocena rizika može dovesti do odluke o nastavku dalje analize. Ocena rizika može takođe voditi i ka odluci o tome da se rizik dalje ne ublažava ni na koji drugi način osim realizacijom postojećih mera za tretiranje rizika. Ta odluka će zavisiti od odnosa organizacije prema riziku i kriterijuma za rizike koje je ona utvrdila.

4. Metodologija procene rizika

Da bi bilo uspešno i održivo, upravljanje rizicima bi trebalo da bude integrisano u organizaciju i da ima podršku menadžmenta. Koncept za upravljanje rizicima pomaže organizacijama da efikasno upravljaju rizicima pri-

menom procesa upravljanja rizicima na različitim nivoima i u okviru specifičnih područja organizacije. Takav koncept treba da omogući da se informacije o riziku, nastale u okviru tog procesa, adekvatno procesuiraju i koriste u donošenju odluka na relevantnim nivoima organizacije.

Aktivnom i sveobuhvatnom procenom rizika menadžment organizacije treba da:

1) artikuliše i odobri politiku upravljanja rizicima;
2) obavesti sve zainteresovane strane o prednostima upravljanja rizicima;
3) definiše indikatore performansi (uspeha) upravljanja rizicima koji odgovaraju organizacionim performansama;
4) osigura podudarnost ciljeva upravljanja rizicima s ciljevima i strategijom organizacije;
5) obezbedi zakonitost i saglasnost s pravnim aktima, i
6) obezbedi raspodelu potrebnih resursa za potrebe upravljanja rizicima.

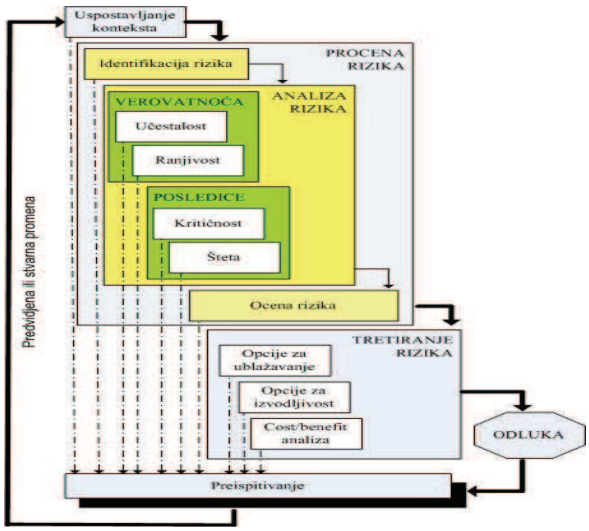
Radi definisanja kriterijuma za procenu rizika (poglavlje 5), metodologija procene rizika treba da obuhvati sledeće:

1) kako će biti definisana verovatnoća;
2) kako će biti utvrđen nivo rizika;
3) kakvi su priroda i tipovi posledica koji se mogu pojaviti i kako će se meriti;
4) nivo na kom rizik postaje podnošljiv/tolerancija rizika;
5) vremenski okvir verovatnoće i/ili posledice;
6) koji nivo rizika zahteva tretiranje, i
7) da li treba uzeti u obzir kombinaciju više rizika.

To je moguće postići razumevanjem organizacije i njenih odnosa sa spoljašnjim i unutrašnjim subjektima.

Procena rizika obuhvata:

− izračunavanje verovatnoće realizacije pretnje, i
− izračunavanje verovatnoće posledica negativnog događaja.



Slika 2 − *Grafički prikaz metodologije procene rizika*

Nivo rizika je u direktnoj zavisnosti od učestalosti ponavljanja događaja, ranjivosti sistema, odnosno postojećeg stanja zaštite u sistemu i posledica za sistem ako rizik preraste u negativan događaj. Nivo rizika se izračunava prema sledećem obrascu:

$$\mathbf{NR = V \times P}$$

$$\mathbf{V = U \# R}$$

P= Š # K, gde su:

NR – izračunati (određeni) nivo rizika,

V – verovatnoća da određeni rizik rezultira negativnim događajem,

P – posledice ili efekat koji negativan događaj ostavlja na vrednosti organizacije,

U – učestalost ili frekvencija dešavanja (pojavljivanja),

R – ranjivost ili osetljivost organizacije na mogućnost realizacije pretnji i pretvaranja u negativan događaj,

Š – šteta, vrednost (veličina) oštećenja štićene vrednosti na koju je negativan događaj ostavio posledice,

K – kritičnost, vrednost ili važnost štićene vrednosti za organizaciju na koju je negativan događaj ostavio posledice.

Učestalost se odnosi na ponavljanje određene pretnje u određenom periodu. Može se stepenovati na sledeći način: 1 − vrlo retko, 2 − povremeno, 3 − često, 4 − pretežno i 5 − veoma često.

Na primer: Organizacija je banka. U proteklom periodu je bila tri puta napadnuta. Učestalost je 2 – povremeno.

Ranjivost predstavlja postojeće stanje zaštite organizacije, odnosno osetljivost organizacije na pretnje. Može se stepenovati na sledeći način: 1 − vrlo velika, 2 − velika, 3 − srednja, 4 − mala i 5 − vrlo mala.

Na primer: Organizacija je banka. Ima samo fizičko obezbeđenje. Ranjivost je 2 – velika.

Verovatnoća predstavlja kombinaciju učestalosti dešavanja određene pretnje i ranjivosti organizacije u odnosu na datu pretnju. Može se stepenovati na sledeći način: 1 − retko, 2 − malo verovatno, 3 − umereno verovatno, 4 − verovatno i 5 − skoro sigurno.

Na primer: Organizacija je banka U proteklom periodu je bila tri puta napadnuta. Ima samo fizičko obezbeđenje. Učestalost je 2 – povremeno. Ranjivost je 2 – velika. Verovatnoća je 3 – umereno verovatno.

RANJIVOST / UČESTALOST		vrlo velika	velika	srednja	mala	vrlo mala
		1	2	3	4	5
vrlo retko	1	3	2	1	1	1
povremeno	2	4	3	2	2	1
često	3	5	4	3	2	2
pretežno	4	5	4	3	3	3
stalno	5	5	5	4	3	3

Šteta je mera oštećenja vrednosti i može biti izražena različitim stepenima: 1 − vrlo mala, 2 – mala, 3 – srednja, 4 − velika i 5 − vrlo velika.

Na primer: Organizacija je mala fabrika. Izvršen je fizički napad. Napadom je nastala šteta u vrednosti od 1 000 dinara lomom stakala na kućici čuvara. Šteta je 1 − vrlo mala.

Kritičnost je mera vrednosti, odnosno važnosti štićene vrednosti za organizaciju. Može se stepenovati prema sledećem: 1 − vrlo velika, 2 – velika, 3 – srednja, 4 − mala i 5 − vrlo mala.

Na primer: Organizacija je mala fabrika. Izvršen je fizički napad. Napadnuta je i oštećena kućica čuvara. Kritičnost je 5 − vrlo mala.

Posledice predstavljaju efekat negativnog događaja na vrednosti organizacije, a manifestuju se kao veličina gubitka (šteta) u odnosu na kritičnost štićene vrednosti. Posledica se može stepenovati prema sledećem: 1 − vrlo laka, 2 – laka, 3 − srednje teška, 4 − teška i 5 − izrazito teška.

Na primer: Organizacija je mala fabrika. Izvršen je fizički napad. Napadom je nastao gubitak u vrednosti od 1 000 dinara lomom stakala na kućici čuvara. Napadnuta je i oštećena kućica čuvara. Šteta je 1 − vrlo mala. Kritičnost je 5 − vrlo mala. Posledica je 1 – vrlo mala.

KRITIČNOST / ŠTETA		vrlo velika	velika	srednja	mala	vrlo mala
		1	2	3	4	5
vrlo mala	1	3	2	1	1	1
mala	2	4	3	2	2	1
srednja	3	5	4	3	2	2
velika	4	5	4	3	3	3
vrlo velika	5	5	5	4	3	3

Prema nivou rizika svi procenjeni rizici se mogu svrstati u sledeće kategorije:

1. vrlo mali rizik, zanemarljiv (NR = 1 i 2);
2. mali rizik (NR = 3, 4 i 5);
3. umereno veliki rizik (NR = 6, 8 i 9);
4. veliki rizik (NR = 10, 12, 15 i 16), i
5. izrazito veliki rizik (NR = 20 i 25).

POSLEDICA / VEROVATNOĆA		vrlo laka	laka	srednje teška	teška	izrazito teška
		1	2	3	4	5
retko	1	1	2	3	4	5
malo verovatno	2	2	4	6	8	10
umereno verovatno	3	3	6	9	12	15
verovatno	4	4	8	12	16	20
skoro sigurno	5	5	10	15	20	25

Procenjeni rizici se prema datoj kategorizaciji mogu svrstati u:

1) PRIHVATLJIVE (NR = 1, 2, 3, 4 i 5) i
2) NEPRIHVATLJIVE (NR = 6, 8, 9, 10, 12, 15, 16, 20 i 25).

Posle završenog procesa procene rizika sledi proces tretiranja rizika. Izbor odgovarajuće opcije za tretiranje rizika obuhvata balansiranje troškova i napora u primeni opcije i koristi koja se može iz toga izvući.

Veliki broj opcija za tretiranje rizika može biti razmatran i primenjen pojedinačno ili u kombinaciji. Organizacija može imati koristi od usvajanja kombinacije opcija za tretiranje rizika.

Odluke treba da uzmu u obzir retke ali ozbiljne rizike koji mogu opravdati akcije tretiranja rizika koje nisu opravdane (dozvoljene) prema strogo ekonomskim pravilima.

Radi delotvornog tretiranja rizika, a na osnovu izvršene procene, potrebno je definisati:

- opcije za ublažavanje rizika,
- opcije za izvodljivost primenjenih strategija, i
- analizu odnosa cene i koristi.

4.1. Opcije za ublažavanje

Na osnovu stepena prihvatljivosti rizika, potrebno je odrediti strategije kojima se tretira rizik. Mogu se primeniti sledeće strategije:

1. Izbegavanje rizika tako što se neće početi ili nastaviti s aktivnošću koja može dovesti do pojave rizika.
2. Traženje mogućnosti tako što će se početi ili nastaviti s aktivnošću koja može dovesti do manjeg rizika ili ga održati.
3. Uticaj na verovatnoću.
4. Uticaj na posledice.
5. Podela rizika s još jednom ili više strana.
6. Zadržavanje rizika, svesnim izborom ili nesvesno.

4.2. Opcije izvodljvosti

Svaka opcija za tretiranje rizika treba da bude uzeta u obzir prema etapama procene rizika. Analiza svake opcije mora uzeti u obzir i cenu koštanja izmene procedura ili proizvoda u skladu s merama za tretiranje rizika.

Na primer: Postoji realna opasnost od krađa u prodavnicama maloprodaje. Moguća strategija kojom se eliminiše rizik je zatvaranje prodavnica i onemogućavanje ulaska lopova. Predložena strategija nije dobra zato što zatvaranjem prodavnica onemogućavamo ulazak redovnih mušterija i time ugrožavamo posao.

Dakle, potrebno je pronaći strategiju koja će omogućiti normalno funkcionisanje s jedne strane, a sprečiti ili svesti na minimum mogućnost krađa s druge strane.

4.3. Analiza cena/korist

Analiza cena/korist je poslednji korak u sprovođenju procene rizika s obzirom na preduzete strategije za tretiranje rizika. Potrebno je utvrditi kolika je stvarna cena koštanja primene predloženih opcija za tretiranje rizika i odrediti veličinu finansijskih i drugih troškova koji nastaju primenom predloženih mera.

Na primer: Nema smisla potrošiti 100 000 dinara za sigurnosnu opremu za sprečavanje krađe robe vredne 1 000 dinara, naročito ako se rizik od krađe može preneti na osiguravajuću kuću.

5. Kriterijumi za procenu rizika

U tabeli 1 su prikazani kriterijumi za kategorisanje rizika, proračunavanjem rizika na osnovu vrednosti verovatnoće nastupanja događaja i vrednosti mogućih opasnih posledica događaja.

Tabela 1 − *Kriterijumi za kategorisanje rizika*

1.1. KRITERIJUMI ZA PRORAČUN RIZIKA					
Verovatnoća		**Posledica**		**Rizik**	
Učestalost	Vrednost	Ozbiljnost	Vrednost	Kategorija	Ocena
Retko	0,1	Materijalna šteta koja ne prelazi iznos od **100 000 dinara**, ili izazivanje opasnosti za zdravlje ljudi ili za imovinu malog obima.	1	**Optimalan – rizik je prihvatljiv, redovno pratiti stanje.**	**0−2**
Malo verovatno	0,3	Materijalna šteta koja prelazi iznos od **100 000 dinara,** ili izazivanje opasnosti za zdravlje ili telo ljudi ili za imovinu manjeg obima.	2	**Srednji − rizik smanjiti na razumnu meru.**	**3–4**
Umereno verovatno	0,5	Materijalna šteta koja prelazi iznos od **450 000 dinara,** ili izazivanje opasnosti za život ili telo ljudi ili za imovinu srednjeg obima, ili narušavanje poslovnog ugleda ili kreditne sposobnosti, ili odavanje poslovne tajne.	3	**Visok − pre daljeg rada se mora smanjiti rizik.**	**>4**
Verovatno	0,8	Materijalna šteta koja prelazi **1 500 000 dinara,** ili izazivanje opasnosti za život ili telo ljudi ili za imovinu većeg obima, ili odavanje poslovne tajne iz koristoljublja.	4	**Stepen rizika se dobija množenjem brojčanih vrednosti verovatnoće nastupanja opasnosti i posledice, i to za svaku stavku iz Liste rizika organizacije.**	
Skoro izvesno	1,0	Materijalna šteta koja prelazi iznos od **5 000 000 dinara,** ili izazivanje opasnosti za život ili telo ljudi ili za imovinu većeg obima, ili odavanje poslovne tajne iz koristoljublja ili u pogledu naročito poverljivih podataka.	5		

6. Integralno upravljanje rizikom

Otkada je središte procene rizika pomereno s rizika koji potiču iz jednog izvora (npr., ispuštanje toksičnih materija iz industrijskog postrojenja s velikim lokalnim posledicama) ka višestrukim izvorima rizika (kao što je ispu-

štanje karbon-dioksida s globalnim posledicama za životnu sredinu), porastao je značaj interdisciplinarnog pristupa. Konvencionalni pristup upravljanju rizicima, koji je uglavnom vezan za disciplinarnu podvojenost, zamenjen je holističkim i integrisanim pristupom. Eliminisanje jednog izvora opasnosti može generisati drugu opasnost. Daglas daje primer azbesta, čiji je pronalazak praćen velikim publicitetom kao sredstvom prevencije od požara (Douglas, 1985). Mnogo godina kasnije, otkrivena su štetna dejstva azbestnih vlakana kao izvora plućnih bolesti.

L. Drenan i A. Makonel uočavaju da, koliko god da su precizne procene rizika, ne može se zanemariti činjenica da su prihvatljivost i tolerantnost na pojedinačne opasnosti u krajnjem određeni ljudskim činiocem. S druge strane, industrijski i društveni razvoj podrazumevaju da se rizici neprestano menjaju. Pomenuti primeri imaju veliki uticaj na razvoj metodologije procene rizika. Nastupanjem internih i eksternih događaja kontekst i znanje se menjaju, pristupa se monitoringu i reviziji, neki rizici se pojačavaju i izbijaju na površinu, dok se drugi umanjuju. Organizacija bi morala da obezbedi proces upravljanja rizicima koji će moći da kontinuirano detektuje i odgovara na promene.

Kao rezultat prethodnog uviđanja, potrebno je sve rizike predstaviti na integralnoj mapi rizika, što je izvanredan alat koji omogućava veću preglednost i sistematičnost rizika i opasnosti, a naročito bolju komunikaciju s drugim linijama i nivoima menadžmenta. Što je još važnije, mape rizika omogućavaju da se lakše uoče veze između rizika i opasnosti, a time i interdisciplinaran uvid u carstvo rizika, s naglaskom na kontinuirani razvoj metoda procene rizika.

7. Zaključak

Sve aktivnosti organizacije uključuju rizike kojima se mora upravljati. Proces upravljanja rizicima doprinosi odlučivanju tako što uzima u obzir neizvesnost i mogućnost pojave budućih događaja i okolnosti i njihov uticaj na prihvaćene ciljeve. Iako je praksa upravljanja rizicima razvijana tokom vremena i u domenu različitih sektora kako bi zadovoljila različite potrebe, njen opšti okvir, sastavljen od osnovnih elemenata, može doprineti deletvornom i koherentnom upravljanju rizicima u organizaciji.

Pristup upravljanju rizicima opisan u ovom radu može biti upotrebljen u okviru širokog spektra različitih konteksta, kao što su projekti, funkcije, imovina, proizvod ili aktivnost. Izbor odgovarajućeg pristupa upravljanju rizicima podržaće i ojačati veze između određenih proizvoda, aktivnosti ili funkcija i opštih ciljeva organizacije. To znači da su razumevanje i pozna-

vanje neke organizacije, njenih procesa, ciljeva, kulture i konteksta u kome deluje uslov za upravljanje rizicima.

Ni najbolja metodologija procene rizika ne donosi sama po sebi rezultate. Upravljanje rizikom mora biti prihvaćeno kao deo rutinskih poslova organizacije i obaveza svakog pojedinca i poslovne funkcije. Upravo to ovaj posao razlikuje od ostalih, kao što su upravljanja ljudskim resursima, finansijama, marketingom i slično, gde je preciziran delokrug rada.

8. Literatura

ASIS INTERNATIONAL: General security risk assessment guideline.

Douglas, M. (1985). *Risk acceptability According to the Social Sciences*. New York: Russel Sage Foundation.

Drennan, L., & McConnell, A. (2007). *Risk and Crisis Management in the Public Sector*. London and New York: Routledge.

ISO TC 223/SC: Upravljanje rizicima − Uputstvo o principima i implementaciji upravljanja rizicima.

APPROACH TO RISK ASSESSMENT METHODOLOGY

Summary

All single organization has to provide risk management process to enable continuosly detection and response to changes in dynamical environment. This paper describes common risk assessment metodology and can be apply to any activity, decision and operation of public, private and societal enteprises, assossiations, group or person. However, applying this metodology includes certain precondition this paper presents as well.