

# Skaliranje vrijednosti varijabli multiplikativne metode za procjenu rizika

INFIGO-MD-2007-02

2007-06-01

Ivana Marijanović  
Hrvoje Segudovic



Ovaj dokument originalno je objavljen kao referat u sklopu savjetovanja Sigurnost informacijskih sustava (ISS) na Mipro 2007.

Ovaj dokument namijenjen je javnoj objavi, a vlasništvo je Infigo IS. Svatko ga smije koristiti pozivati se na njega ili ga citirati, ali isključivo u izvornom obliku i uz obvezno navođenje izvora.

Korištenje dokumenata na bilo koji drugi način od gore navedenog, bez dozvole Infigo IS predstavlja povredu vlasništva i kao takvo podložno je zakonskoj odgovornosti koja je regulirana zakonima Republike Hrvatske ili drugom primjenjivom regulativom.

Infigo IS d.o.o.  
Horvatovac 20  
10000 Zagreb

tel. +385 1 4662 700  
fax. +385 1 4662 701  
info@infigo.hr  
www.infigo.hr



# SADRŽAJ

<b>1. UVOD</b>	<b>4</b>
<b>2. UVOD</b>	<b>5</b>
<b>3. SLUČAJ 1 – LINEARNA KVANTIFIKACIJA SVIH PARAMETARA</b>	<b>7</b>
<b>4. SLUČAJ 2 – LINEARNA KVANTIFIKACIJA DVA PARAMETRA UZ GEOMETRIJSKU KVANTIFIKACIJU TREĆEG PARAMETRA</b>	<b>8</b>
<b>5. SLUČAJ 3 – LINEARNA KVANTIFIKACIJA JEDNOG PARAMETRA UZ GEOMETRIJSKU KVANTIFIKACIJU PREOSTALA DVA</b>	<b>10</b>
<b>6. SLUČAJ 4 – GEOMETRIJSKA KVANTIFIKACIJA SVA TRI PARAMETRA</b>	<b>11</b>
<b>7. MULTIPLIKATIVNA METODA SA SKALAMA OD TRI VRIJEDNOSTI I PET VRIJEDNOSTI</b>	<b>13</b>
7.1. SKALE S TRI VRIJEDNOSTI	13
7.2. SKALE S PET VRIJEDNOSTI	13
<b>8. ZAKLJUČAK</b>	<b>14</b>
<b>9. LITERATURA</b>	<b>15</b>

# 1. UVOD

Prema multiplikativnoj metodi procjene rizika, rizik se procjenjuje kao umnožak vrijednosti resursa - AV (*engl. asset value*), vjerojatnosti ostvarenja prijetnje - PT (*engl. threat probability*) i posljedica ostvarenja prijetnje - IT (*engl. threat impact*). Metoda dozvoljava proizvoljne, nezavisne skale vrijednosti koje mogu poprimiti sve varijable (AV, P, I), no praksa pokazuje da se najčešće koriste identične, linearne skale.

Rad raspravlja mogućnosti korištenja nelinearnih, nezavisnih skala vrijednosti za procjenu rizika, te mogućnost primjene u različitim praktičnim situacijama. Istražuje se utjecaj nelinearnih skala vrijednosti u graničnim slučajevima kad se vjerojatnost ostvarenja prijetnje znatno razlikuje od negativnih posljedica ostvarenja iste.

## 2. UVOD

Procjena rizika ima temeljnu ulogu u procesu upravljanja informacijskom sigurnošću. To je proces koji opravdava donošenje odluka i raspodjelu resursa kako bi se osigurali povjerljivost, integritet i raspoloživost informacija i kontinuitet poslovanja organizacije. Budući su resursi uvijek ograničeni, postavlja se zahtjev primjene sigurnosnih kontrola na najkritičnije resurse, odnosno na resurse koji predstavljaju najveći rizik za poslovanje organizacije. U takvim uvjetima od velike je važnosti da rezultati procjene rizika odgovaraju stvarnim poslovnim potrebama.

Rezultati procjene rizika ovise o postupku procjene rizika odnosno o korištenoj metodologiji. U ovom radu, predmet analize je multiplikativna metoda procjene rizika, opisana u [2], ali u obzir su uzete i druge metode navedene u [1].

Multiplikativna metoda za procjenu rizika temelji se na sljedećim pretpostavkama:

- svaki resurs ima svoju vrijednost – AV (*engl. asset value*),
- ranjivost pojedinog resursa postoji ili ne – V (*engl. vulnerability*),
- ukoliko ranjivost sustava postoji, postoji barem jedna prijetnja koja je može iskoristiti (prijetnja i ranjivosti su međusobno zavisne),
- prijetnja ima vjerojatnost ostvarenja koja ovisi o okolnostima – PT (*engl. threat probability*)
- prijetnja ima moguće posljedice čija veličina ovisi o okolnostima – IT (*engl. threat impact*).

Procjena rizika može se prikazati kao (1).

$$R = f(AV, P_T, I_T) = f(V), \quad (1)$$

Može se uočiti da su svi parametri funkcija najviše jedne varijable, što osigurava jednoznačnost i jednostavnost interpretacije.

Da bi procjenu rizika bilo moguće napraviti osjetljivijom na razlike u veličinama pojedinih parametara i na taj način omogućiti više fleksibilnosti u postupku upravljanja rizikom koristi se operacija množenja (2).

$$R = AV * P_T * I_T \quad (2)$$

Raspon vrijednosti koje svaki od parametara može poprimiti je proizvoljan.

Obzirom da se kvalitativna procjena rizika bazira na ljudskoj procjeni, zbog načina ljudske percepcije nije preporučljivo koristiti skale s više od 5 vrijednosti. Skale od dvije vrijednosti (binarne skale) ne omogućavaju prioritizaciju, a simetrične skale (3 i 5 vrijednosti), ponovno zbog ljudske percepcije, u sebi sadrže inherentni rizik od usrednjavanja.

Uzevši u obzir gore navedene razloge, ovaj rad prvenstveno analizira postupak procjene rizika i interpretira rezultate kod modela koji za svaki od parametara koristi (asimetričnu) skalu od četiri vrijednosti.

Kod tog modela pretpostavlja se da svaki od parametara (AV, P, I) koji se koristi za procjenu rizika može poprimiti četiri vrijednosti koje se kvalitativno mogu opisati kao niska (L), srednja (M), visoka (H) i vrlo visoka (VH).

U radu se analizira utjecaj korištenja različitih načina kvantifikacije kvalitativnih vrijednosti parametara na rezultat procjene rizika. Razmotreni su sljedeći načini kvantifikacije parametara:

- linearna kvantifikacija svih parametara,
- linearna kvantifikacija dva parametra, uz geometrijsku kvantifikaciju trećeg parametra,
- linearna kvantifikacija jednog parametra, uz geometrijsku kvantifikaciju preostala dva parametra,
- geometrijska kvantifikacija sva tri parametra.

Prilikom analize nije se manipuliralo definiranim rasponima procijenjenog rizika nego je korišten predefimirani raspon četiri razine rizika (*engl. risk levels*): L (*engl. Low*), M (*engl. Medium*), H (*engl. High*) i VH (*engl. Very High*). Rasponi pojedinih razina rizika definirani su geometrijskim nizom kako je prikazano u (3).

$$\begin{aligned} &Low[R_{MIN}, R_{MAX} / 8), \\ &Medium[R_{MAX} / 8, R_{MAX} / 4), \\ &High[R_{MAX} / 4, R_{MAX} / 2), \\ &VeryHigh[R_{MAX} / 2, R_{MAX} ] \end{aligned} \tag{3}$$

Također, sažeto je analiziran utjecaj opisanih načina kvantifikacije na modele sa (simetričnim) skalama od 3 i 5 vrijednosti.

### 3. SLUČAJ 1 – LINEARNA KVANTIFIKACIJA SVIH PARAMETARA

Matrica rizika multiplikativne metode s linearnom kvantifikacijom svih parametara prikazana je u sljedećoj tablici (Tablica 1).

		AV			
I <sub>r</sub>	P <sub>r</sub>	1	2	3	4
1	1	1	2	3	4
	2	2	4	6	8
	3	3	6	9	12
	4	4	8	12	16
2	1	2	4	6	8
	2	4	8	12	16
	3	6	12	18	24
	4	8	16	24	32
3	1	3	6	9	12
	2	6	12	18	24
	3	9	18	27	36
	4	12	24	36	48
4	1	4	8	12	16
	2	8	16	24	32
	3	12	24	36	48
	4	16	32	48	64

Tablica 1: Matrica rizika s linearnim skalama

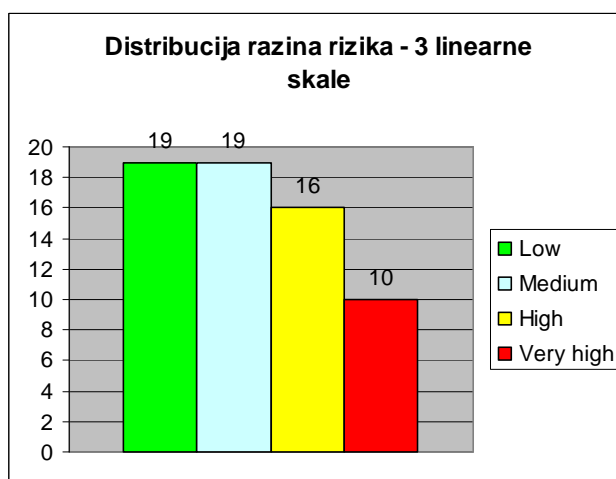
Na temelju (2) i predloženog raspona vrijednosti mogu se izračunati minimalne i maksimalne vrijednosti procijenjenog rizika (4).

$$R_{MIN} = AV_{MIN} * P_{MIN} * I_{MIN} = 1$$

$$R_{MAX} = AV_{MAX} * P_{MAX} * I_{MAX} = 64 \quad (4)$$

Distribucija rizika (Slika 1), uz definirani način procjene rizika (3) može se približno opisati kao logaritamska.

Matrica rizika definirana u Tablici 1 ima određene nedostatke. Naime, praksa je pokazala da ovako definirane skale vrijednosti u određenim situacijama daju nerealne rezultate. U graničnim slučajevima kad postoji velika razlika između vjerojatnosti ostvarenja prijetnje i utjecaja negativnih posljedica ostvarenja, korištenje linearne kvantifikacije svih parametara daje procjenu rizika koja ne odgovara stvarnosti. Npr. realni primjer nuklearne katastrofe, koja ima velike posljedice za svaki resurs, no vjerojatnost za njeno ostvarenje je vrlo niska, prema opisanoj metodi kvantificirao bi se kao: (AV, P, I) = (VH, L, VH), a procijenjeni rizik R bio bi visok (H). Realna procjena rizika takvog događaja može se pak smatrati niskom, što pokazuje nedostatak metode. Kod ovakvog načina kvantifikacije isti problem prisutan je u svim kombinacijama vrijednosti VH, H, L.



Slika 1: Distribucija rizika za linearne skale svih varijabli

#### 4. SLUČAJ 2 – LINEARNA KVANTIFIKACIJA DVA PARAMETRA UZ GEOMETRIJSKU KVANTIFIKACIJU TREĆEG PARAMETRA

Ukoliko se jedan parametar kvantificira geometrijski, on postaje utjecajnija veličina na procijenjeni rizik. Matrica rizika prikazana je tablicom (Tablica 2), uz geometrijsku kvantifikaciju vrijednosti resursa (AV).

		AV			
$I_T$	$P_T$	2	4	8	16
1	1	2	4	8	16
	2	4	8	16	32
	3	6	12	24	48
	4	8	16	32	64
2	1	4	8	16	32
	2	8	16	32	64
	3	12	24	48	96
	4	16	32	64	128
3	1	6	12	24	48
	2	12	24	48	96
	3	18	36	72	144
	4	24	48	96	192
4	1	8	16	32	64
	2	16	32	64	128
	3	24	48	96	192
	4	32	64	128	256

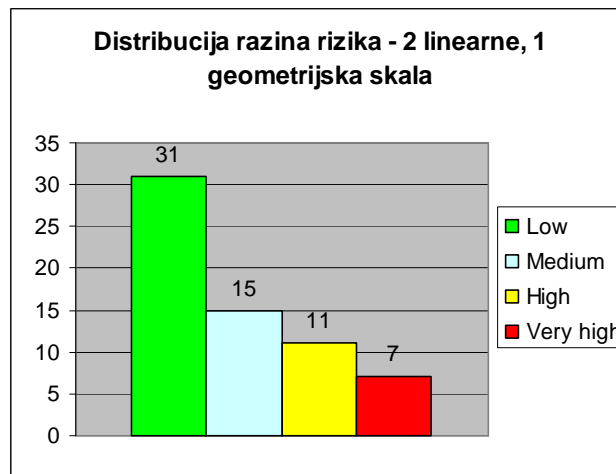
Tablica 2: Matrica rizika s dvije linearne i jednom geometrijskom skalom

Minimalne i maksimalne vrijednosti rizika:

$$R_{MIN} = AV_{MIN} * P_{MIN} * I_{MIN} = 2$$

$$R_{MAX} = AV_{MAX} * P_{MAX} * I_{MAX} = 256 \quad (5)$$

Distribucija rizika definirana prema (3), prikazana na Slici 2, je približno eksponencijalna. Broj malih rizika je povećan, dok je broj ostalih rizika umanjen u odnosu na linearnu kvantifikaciju svih parametara.



**Slika 2:** Distribucija rizika za dvije linearne i jednu geometrijsku skalu

Usporedba tablica (Tablica 1 i Tablica 2) pokazuje da dolazi do općenitog umanjivanja procijenjenog rizika. Najveće umanjjenje se može uočiti kod linearno kvantificiranih parametara, odnosno tamo gdje ti parametri poprimaju visoke (H) i vrlo visoke (VH) vrijednosti.

U graničnim slučajevima ova metoda umanjuje procijenjeni rizik kod linearno procijenjenih parametara, dok se za geometrijski procijenjeni parametar procjena rizika ne mijenja (usporedi krajnji desni stupac Tablica 1 i Tablica 2).

## 5. SLUČAJ 3 – LINEARNA KVANTIFIKACIJA JEDNOG PARAMETRA UZ GEOMETRIJSKU KVANTIFIKACIJU PREOSTALA DVA

Geometrijska kvantifikacija dvaju parametara ima dodatni utjecaj na općenito umanjivanje procijenjenog rizika. Matrice rizika kod koje su geometrijski kvantificirane vrijednost resursa (AV) i posljedice (I), prikazana je u tablici (Tablica 3). Minimalne i maksimalne vrijednosti rizika su:

$$R_{MIN} = AV_{MIN} * P_{MIN} * I_{MIN} = 4$$

$$R_{MAX} = AV_{MAX} * P_{MAX} * I_{MAX} = 1024 \quad (6)$$

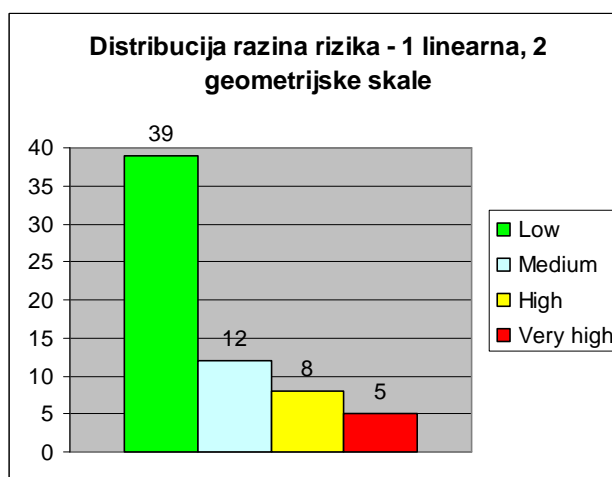
Razine rizika definirane su prema (3), što daje distribuciju rizika kako je pokazano na slici (Slika 3) koja ima eksponencijalni oblik.

Uočljivo je da se, primjenom dvije geometrijske i jedne linearne skale, u odnosu na prethodne slučajeve, dodatno umanjuju razine procijenjenog rizika (Slika 1, Slika 2)

U matrici rizika može se primijetiti da se procijenjeni rizik i u graničnim slučajevima umanjuje, izuzev kombinacije geometrijski kvantificiranih parametara.

		AV			
I <sub>r</sub>	P <sub>r</sub>	2	4	8	16
2	1	4	8	16	32
	2	8	16	32	64
	3	12	24	48	96
	4	16	32	64	128
4	1	8	16	32	64
	2	16	32	64	128
	3	24	48	96	192
	4	32	64	128	256
8	1	16	32	64	128
	2	32	64	128	256
	3	48	96	192	384
	4	64	128	256	512
16	1	32	64	128	256
	2	64	128	256	512
	3	96	192	384	768
	4	128	256	512	1024

Tablica 3: Matrica rizika s jednom linearnom i dvije geometrijske skalom



Slika 3: Distribucija rizika za jednu linearnu i dvije geometrijske skale.

## 6. SLUČAJ 4 – GEOMETRIJSKA KVANTIFIKACIJA SVA TRI PARAMETRA

Posljednji razmatrani slučaj predstavlja geometrijska kvantifikacija svih parametara za procjenu rizika. U tom slučaju dobiva se matrica rizika prikazana u Tablici 4.

Minimalne i maksimalne vrijednosti rizika su:

$$R_{MIN} = AV_{MIN} * P_{MIN} * I_{MIN} = 8$$

$$R_{MAX} = AV_{MAX} * P_{MAX} * I_{MAX} = 4096 \quad (7)$$

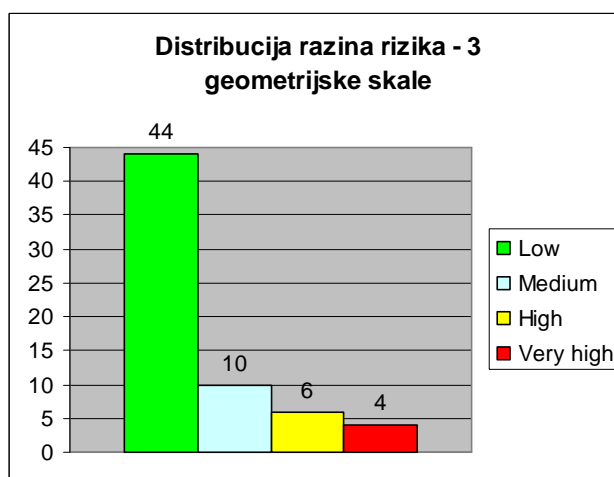
Uz razine rizika definirane prema (3) dobiva se izrazito eksponencijalna distribucija rizika što je uočljivo iz slike (Slika 4).

Može se uočiti da korištenjem geometrijske kvantifikacije svih parametara, općenito dolazi do izrazitog umanjenja procijenjenog rizika.

Također, u graničnim slučajevima procijenjeni rizik je jednoliko umanjen, što je i za očekivati zbog korištenja simetričnih skala.

		AV			
$I_T$	$P_T$	2	4	8	16
2	2	8	16	32	64
	4	16	32	64	128
	8	32	64	128	256
	16	64	128	256	512
4	2	16	32	64	128
	4	32	64	128	256
	8	64	128	256	512
	16	128	256	512	1024
8	2	32	64	128	256
	4	64	128	256	512
	8	128	256	512	1024
	16	256	512	1024	2048
16	2	64	128	256	512
	4	128	256	512	1024
	8	256	512	1024	2048
	16	512	1024	2048	4096

Tablica 4: Matrica rizika s geometrijskim skalama



**Slika 4:** Distribucija rizika za geometrijske skale svih varijabli

Ovako definirane skale daju prikladnije rezultate u graničnim slučajevima jer za nisku vjerojatnost pojave neželjenog događaja ili male posljedice neželjenog događaja daju nizak rizik. Zbog velikog broja niskih rizika ovako definirana metodologija je prikladna za sustave s velikim brojem prihvatljivih rizika.

## 7. MULTIPLIKATIVNA METODA SA SKALAMA OD TRI VRIJEDNOSTI I PET VRIJEDNOSTI

### 7.1. SKALE S TRI VRIJEDNOSTI

Ponašanje distribucije rizika multiplikativne metode u slučaju kad se koriste skale od 3 vrijednosti razlikuje se od ponašanja distribucije rizika s četiri skale vrijednosti. Razine rizika L (engl. Low), M (engl. Medium) i H (engl. High) su definirane na sljedeći način:

$$\begin{aligned} &Low[R_{MIN}, \lfloor R_{MAX} / 4 \rfloor], \\ &Medium[\lfloor R_{MAX} / 4 \rfloor, \lfloor R_{MAX} / 2 \rfloor], \\ &High[\lfloor R_{MAX} / 2 \rfloor, R_{MAX}] \end{aligned} \tag{8}$$

Ukoliko se svi parametri kvantificiraju linearno, metoda teži usrednjavanju vrijednosti.

Geometrijskom kvantifikacijom jednog parametra, pojavljuje se eksponencijalna distribucija rizika, no za razliku od skale s četiri vrijednosti, povećanjem broja parametara s geometrijskom kvantifikacijom ne dolazi do promjena u distribuciji rizika.

### 7.2. SKALE S PET VRIJEDNOSTI

Razine rizika VL (engl. Very Low), L (engl. Low), M (engl. Medium), H (engl. High) i VH (engl. Very High) su definirane na sljedeći način:

$$\begin{aligned} &VeryLow[R_{MIN}, \lfloor R_{MAX} / 16 \rfloor], \\ &Low[\lfloor R_{MAX} / 16 \rfloor, \lfloor R_{MAX} / 8 \rfloor], \\ &Medium[\lfloor R_{MAX} / 8 \rfloor, \lfloor R_{MAX} / 4 \rfloor], \\ &High[\lfloor R_{MAX} / 4 \rfloor, \lfloor R_{MAX} / 2 \rfloor], \\ &VeryHigh[\lfloor R_{MAX} / 2 \rfloor, R_{MAX}] \end{aligned} \tag{9}$$

Skale s 5 vrijednosti se ponašaju slično kao i skale s četiri vrijednosti. Ukoliko su sve skale linearne, distribucija teži usrednjavanju rizika. Uvođenjem geometrijskih skala, povećava se broj niskih rizika.

## 8. ZAKLJUČAK

Analizom utjecaja korištenja linearnih i geometrijskih skala za procjenu vrijednosti parametara prilikom procjene rizika, uz identičnu skalu procjene rizika uočene su dvije bitne činjenice.

Kao prvo, uvođenjem geometrijskih skala, distribucija rizika ima tendenciju poprimanja eksponencijalnog oblika, gdje broj niskih (L) rizika raste, dok brojevi srednjih (M), visokih (H) i vrlo visokih (VH) rizika padaju.

Iz toga se može zaključiti da je korištenje geometrijskih skala prikladnije u sustavima koji su tolerantniji na rizik. Za sustave kod kojih ne postoji tolerancija na rizik, korištenje geometrijske kvantifikacije parametara nije preporučljivo, zbog izrazite tendencije umanjivanja rizika.

Druga bitna činjenica se odnosi na ponašanje u graničnim slučajevima, odnosno na veličinu procijenjenog rizika ukoliko dva parametra poprimaju maksimalne vrijednosti, dok jedan parametar poprima minimalnu vrijednost.

U većini realnih situacija, rizik takvih događaja je nizak, dok multiplikativna metoda u različitim situacijama pokazuje veće ili manje odstupanje od realne situacije. Najveće odstupanje pri tom je u slučaju korištenja linearne kvantifikacije svih parametara, dok se povećanjem broja geometrijski kvantificiranih parametara to odstupanje smanjuje, no ne poprima idealnu vrijednost.

U odnosu na skale gdje su parametri kvantificirani s tri vrijednosti, skala s četiri vrijednosti pokazuje bolje ponašanje u graničnim slučajevima, a također omogućava bolju manipulaciju distribucije rizika manipulacijom načina kvantifikacije parametara.

Ponašanje u slučaju skala gdje su parametri kvantificirani s pet vrijednosti može se ocijeniti vrlo sličnim.

## 9. LITERATURA

- [1] ISO/IEC TR 13335-3 Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security, 1st edition, 1998.
- [2] H.Šegudović, "Prednosti i nedostaci metoda za kvalitativnu analizu rizika", MIPRO 2006.
- [3] ISO/IEC 27001, Information technology – Security techniques – Information security management systems – Requirements, 1st edition, 2005.
- [4] ISO/IEC 17799, Information technology – Security techniques – Code of practice for Information security management, 2nd edition, 2005.
- [5] C.Alberts and A. Dorofee, "Managing Information Security Risks, The OCTAVE Approach", 1st edition, 2002.
- [6] D.Wenk, "Risk Management and Business Continuity, Overview and Perspectives", 2005.
- [7] An ioMosanic Corporation Whitepaper, "Designing an Effective Risk Matrix", 2002.