

# Scaling of Values of Multiplicative Method for Risk Evaluation

INFIGO-MD-2007-02

2007-06-01

Ivana Marijanović  
[Ivana.Marijanovic@infigo.hr](mailto:Ivana.Marijanovic@infigo.hr)

Hrvoje Šegudović  
[Hrvoje.Segudovic@infigo.hr](mailto:Hrvoje.Segudovic@infigo.hr)



This paper was originally published at MIPRO 2007 conference within ISS track.

Paper is intended for public use and may be used, referred to or quoted only in its original form and source referral.

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



## TABLE OF CONTENTS

<b>1. SUMMARY</b>	<b>4</b>
<b>2. INTRODUCTION</b>	<b>5</b>
<b>3. CASE 1 – LINEAR QUANTIFICATION OF ALL PARAMETERS</b>	<b>7</b>
<b>4. CASE 2 - LINEAR QUANTIFICATION OF TWO PARAMETERS WITH GEOMETRIC QUANTIFICATION OF THE THIRD PARAMETER</b>	<b>8</b>
<b>5. CASE 3 - LINEAR QUANTIFICATION OF ONE PARAMETER WITH GEOMETRIC QUANTIFICATION OF THE OTHER TWO PARAMETERS</b>	<b>10</b>
<b>6. CASE 4 – GEOMETRIC QUANTIFICATION OF ALL PARAMETERS</b>	<b>11</b>
<b>7. MULTIPLICATIVE METHOD WITH SCALES WITH THREE VALUES AND FIVE VALUES</b>	<b>12</b>
7.1. SCALES WITH THREE VALUES	12
7.2. SCALES WITH FIVE VALUES	13
<b>8. CONCLUSION</b>	<b>14</b>
<b>9. LITERATURE</b>	<b>15</b>

# 1. SUMMARY

According to the multiplicative method of risk evaluation, risk is assessed as the product of resource values - AV (asset value), PT (threat probability) and IT (threat impact). This method allows arbitrary, independent value scales which all variables (AV, P, I) can assume, but the most common scales used in practice are identical, linear scales.

The objects of this study are the possibilities of using nonlinear independent value scales for risk evaluation and their applicability in various practical situations. This paper will analyze the influence of nonlinear value scales in borderline cases when threat probability is considerably different than the threat impact.

## 2. INTRODUCTION

Risk evaluation is crucial in the process of information security management. This process justifies decision making and resource distribution to ensure confidentiality, integrity, the availability of information and business processes continuity. Since the resources are always limited, the application of security controls is required on the most critical resources, i.e. on the resources which represent the biggest risk for organization's business. In these conditions, it is highly important that risk evaluation results match actual business needs.

Risk evaluation results depend on the procedure of risk evaluation, i.e. on the methodology used. The object of this analysis is the multiplicative method of risk evaluation, described in [2], but some other methods listed in [1] were also considered.

The multiplicative method of risk evaluation is based on the following assumptions:

- every resource has its value – AV (asset value),
- vulnerability of each resource either exists or not – V (vulnerability),
- if the system vulnerability exists, there is at least one threat which can use the vulnerability (the threat and the vulnerability are interdependent),
- the threat has a realization probability, which depends on the circumstances – PT (threat probability),
- the threat has potential consequences and their severity depends on the circumstances – IT (threat impact).

Risk evaluation can be described as (1).

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

It can be seen that all function parameters have no more than one variable, which ensures uniformity and simplicity of interpretation.

Multiplication (2) is used in order to make risk evaluation more sensitive for the differences in size of each parameter and thus to enable more flexibility in the risk management process.

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

The range of values which each of the parameters can assume is arbitrary.

Since the qualitative risk evaluation is based on human evaluation, it is not recommended to use a scale with more than 5 values due to the nature of human perception. Scales with two values (binary scales) do not enable prioritization and symmetrical scales (3 and 5 values), again due to human perception, include inherent risk of averaging.

If we take the above mentioned reasons into consideration, this study primarily analyzes the risk evaluation procedure in models which use a (asymmetrical) 4-value scale for each of the parameters. This model presupposes that each of the parameters (AV, P, I) used for risk evaluation can assume four values, whose quality can be described as low (L), medium (M), high (H) and very high (VH).

The study analyzes how a different usage of quantification of the qualitative values of parameters influences the result of risk evaluation. The following methods of parameter quantification were considered:

- linear quantification of all parameters,
- linear quantification of two parameters, with geometric quantification of the third parameter,

- linear quantification of one parameter, with geometric quantification of the other two parameters,
- geometric quantification of all three parameters.

During the analysis there was no manipulation of the defined ranges of the evaluated risk. Instead, we used the predefined range of four risk levels: L (low), M (medium), H (high) and VH (very high). The range of each risk level is defined by geometric series shown in (3).

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

Moreover, we briefly analyzed the influence of the described methods of quantification on models with (symmetrical) scales with 3 and 5 values.

### 3. CASE 1 – LINEAR QUANTIFICATION OF ALL PARAMETERS

Risk matrix of multiplicative method with linear quantification is shown in the following table (Table 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

**Table 1:** Risk matrix with linear scales

Minimal and maximal value of the evaluated risk (4) can be calculated based upon (2) and the suggested value range.

$$\begin{aligned}
 R_{MIN} &= AV_{MIN} * P_{MIN} * I_{MIN} = 1 \\
 R_{MAX} &= AV_{MAX} * P_{MAX} * I_{MAX} = 64
 \end{aligned}
 \tag{4}$$

Risk distribution (Picture 1), with the defined way of risk evaluation (3), can approximately be described as logarithmic.

The risk matrix defined in Table I has certain flaws. It has been proven that value scales defined in this way give unreal results in some situations. In borderline cases when there is a big difference between threat probability and threat impact, linear quantification of all parameters gives risk evaluation which does not match the actual situation. For example, following the described method, a real example of a nuclear disaster, which has impact on every resource, but a very low probability level, would be quantified as: (AV, P, I) = (VH, L, VH), and the evaluated risk R would be high (H). Real risk evaluation of such an incident can be considered low, which proves the flaw of this method. When using this method of quantification, the same problem is present in the combinations of all values VH, H, L.

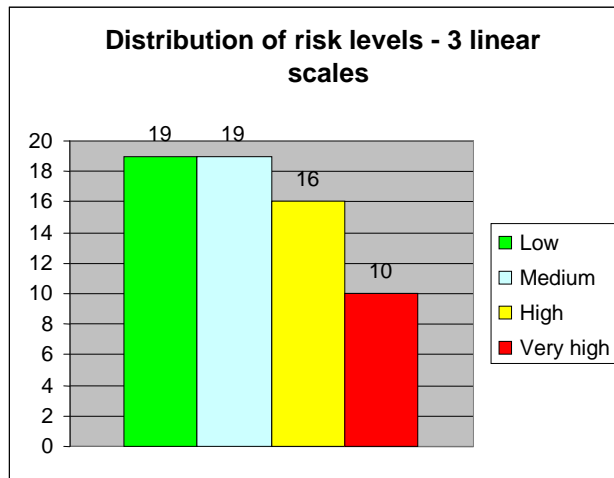


Figure 1: Risk distribution for linear scales of all variables

#### 4. CASE 2 – LINEAR QUANTIFICATION OF TWO PARAMETERS WITH GEOMETRIC QUANTIFICATION OF THE THIRD PARAMETER

If one parameter is quantified geometrically, it becomes a magnitude with more influence on the evaluated risk. Risk matrix is shown in Table 2, with geometric quantification of resource value (AV).

		AV			
I <sub>r</sub>	P <sub>r</sub>	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

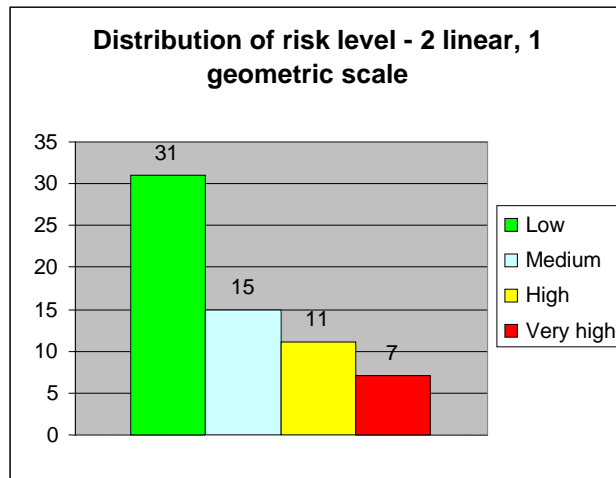
Table 2: Risk matrix with two linear and one geometric scale

Minimal and maximal risk values:

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

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

The distribution of risk defined in (3) shown in Picture 2 is approximately exponential. The number of low risks is higher, while the number of other risks is lower in relation to the linear quantification of all parameters.



**Figure 2:** Risk distribution for two linear and one geometric scale

The comparison of the tables (Table 1 and Table 2) shows that there is a general decrease of the evaluated risk. The biggest decrease can be seen in linearly quantified parameters, i.e. in situations where those parameters assume high (H) and very high (VH) values.

In borderline cases, this method decreases the evaluated risk in linearly evaluated parameters, while the risk evaluation for the geometrically evaluated parameter remains the same (compare far right column of Table 1 and Table 2).

## 5. CASE 3 – LINEAR QUANTIFICATION OF ONE PARAMETER WITH GEOMETRIC QUANTIFICATION OF THE OTHER TWO PARAMETERS

Geometric quantification of two parameters has an additional influence on general decrease of the evaluated risk. Risk matrices with geometrically quantified resource values (AV) and impact (I) is shown in table (Table 3). Minimal and maximal risk values are:

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

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

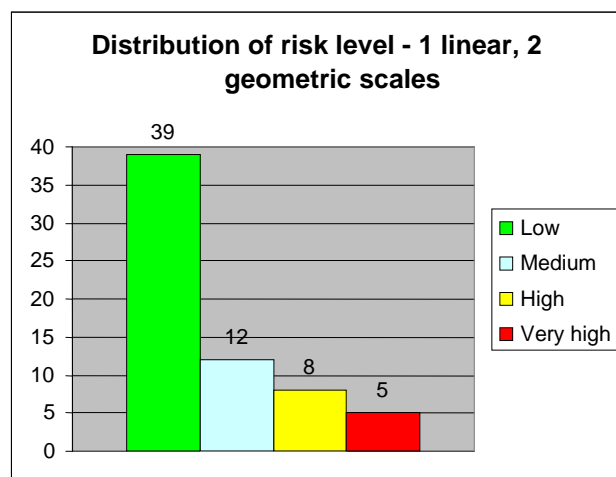
Risk levels are defined according to (3), which results in risk distribution shown in picture (Picture 3), with an exponential shape.


It can be seen that the usage of two geometric and one linear scale, unlike in the previous cases, additionally decreases the evaluated risk levels. (Picture 1, Picture 2)

The risk matrix shows that the evaluated risk is also decreased in borderline cases, except the combination of geometrically quantified parameters.

		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

Table 3: Matrix with one linear and two geometric scales





**Figure 3:** Risk distribution for one linear and two geometric scales.

## 6. CASE 4 – GEOMETRIC QUANTIFICATION OF ALL PARAMETERS

The last analyzed case is geometric quantification of all parameters for risk evaluation. This case produces risk matrix shown in Table 4.

Minimal and maximal risk values are:

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

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

With risk levels defined in (3), the risk distribution is very exponential, as can be seen in picture (Picture 4).

One can notice that the usage of geometric quantification of all parameters leads to general decrease of the evaluated risk.

Furthermore, the evaluated risk is evenly reduced in borderline cases, as can be expected due to the usage of symmetrical scales.

		AV			
I <sub>r</sub>	P <sub>r</sub>	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

Table 4: Risk matrix with geometric scales

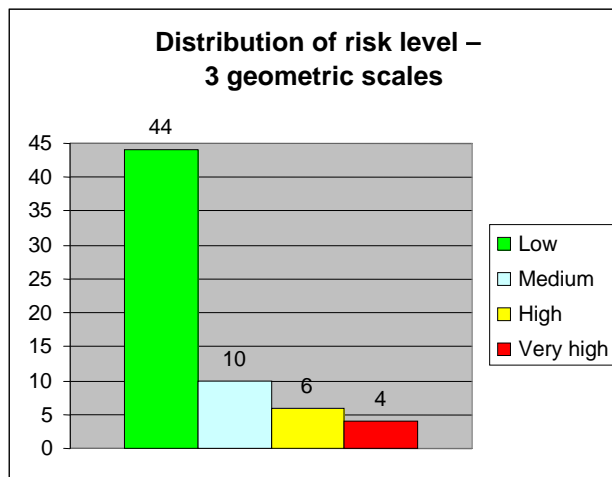


Figure 4: Risk distribution for geometric scales of all variables

Scales defined in this way give more appropriate results in borderline cases because they give low risk for low probability of an unwanted incident or small impact of an unwanted incident.

Due to a high number of low risks this kind of methodology is suitable for systems with a high number of acceptable risks.

## 7. MULTIPLICATIVE METHOD WITH SCALES WITH THREE VALUES AND FIVE VALUES

### 7.1. SCALES WITH THREE VALUES

The behavior of risk distribution of the multiplicative method in case when scales with 3 values are used is different than the behavior of risk distribution with four value scales. Risk levels L (low), M (medium) and H (high) are defined as follows:

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

If all parameters are linearly quantified, this method aims at the averaging of values.

Geometric quantification of one parameter creates exponential risk distribution, but unlike the scale with four values, the increase in the number of parameters with geometric quantification does not result in changes in risk distribution.

## 7.2. SCALES WITH FIVE VALUES

Risk levels VL (very low), L (low), M (medium), H (high) and VH (very high) are defined as follows:

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

Scales with 5 values behave in a similar manner as the scales with four values. If all scales are linear, distribution tends to average the risk. The introduction of geometric scales increases the number of low risks.

## 8. CONCLUSION

Two important facts are discovered in the analysis of the influence of using linear and geometric scales for the evaluation of parameter values during risk evaluation, with identical scale of risk evaluation.

In the first place, when geometric scales are introduced, risk distribution has a tendency to assume exponential shapes, with the increase of low (L) risks, and the decrease of the number of medium (M), high (H) and very high (VH) risks.

The conclusion is that the usage of geometric scales is more appropriate in systems which have higher risk tolerance. For systems with no risk tolerance, the usage of geometric quantification of parameters is not recommended, due to a strong tendency towards risk reduction.

The other important fact is related to the behavior in borderline cases or to the amount of the evaluated risk if two parameters assume maximal values, while one parameter assumes the minimal value.

In most real situations, the risk of such occurrences is low, while the multiplicative method in various situations shows a bigger or smaller deviation from the real situation. The biggest deviation can occur when using linear quantification of all parameters, while the increase in the number of geometrically quantified parameters decreases this deviation, but it does not assume the ideal value.

In comparison to scales where the parameters are quantified with three values, the scale with four values shows functions better in borderline cases, and it also enables better manipulation of risk distribution over the manipulation of parameter quantification.

Behavior is very similar in cases when scales have parameters quantified with five values.

## 9. LITERATURE

- [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.