

# Qualitative risk analysis method comparison

INFIGO-MD-2006-06-01

05-06-2006

Hrvoje Segudovic  
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. RISK ASSESSMENT</b>	<b>6</b>
<b>4. QUANTITATIVE APPROACH</b>	<b>7</b>
<b>5. QUALITATIVE APPROACH</b>	<b>8</b>
<b>6. METHODS</b>	<b>9</b>
6.1. METHOD 1: PREDEFINED VALUE MATRIX	9
6.2. METHOD 2: THREAT RANKING BY RISK EVALUATION	10
6.3. METHOD 3: ASSESSMENT OF THE PROBABILITY OF A THREAT BEING REALIZED AND IT'S CONSEQUENCES	12
6.4. METHOD 4: ACCEPTABLE AND UNACCEPTABLE RISK SEPARATION	13
<b>7. QUALITATIVE RISK ASSESSMENT METHOD EVALUATION</b>	<b>14</b>
<b>8. A MODIFIED QUALITATIVE RISK ASSESSMENT METHOD</b>	<b>15</b>
8.1. ASSUMPTIONS	15
8.2. RISK ASSESSMENT	15
<b>9. CONCLUSION</b>	<b>17</b>

# 1. SUMMARY

Information security management is a business process part that is usually required by various regulatory laws.

Security controls are defined by the business to ensure an adequate security level that is validated by a process called risk management. The risk management process allows the definition of strategy and goals in an organization's information security.

The most important part of this process, which is usually prone to errors, is the first step - risk assessment. Literature classifies risk assessment as qualitative and quantitative. Qualitative risk assessment calculates the risk level using plain judgment and assessor's experience, while quantitative risk assessment depends on a numerical model (typically based on financial values).

Although, in theory, quantitative risk assessment allows for a more detailed risk assessment, in practice this approach is usually not adequate, as an information resource's value is based on its financial value (which does not show the true value of the information resource for a corporation). This is the main reason why a combination of qualitative and quantitative methods is preferred for risk assessment. As qualitative risk assessment is based on subjective judgment, it is prone to errors.

This paper analyzes some qualitative (quantitative-qualitative) risk assessment methods. Special attention is given to the influence of various elements on risk assessment result and reliability.

## 2. INTRODUCTION

Risk management is a process that validates security controls defined by business. Besides this validation, risk management also defines strategy and goals in the area of information security.

The most important and time consuming part of a risk management process is risk assessment or analysis [5]. Basically, there are two risk assessment approaches: quantitative and qualitative. Various papers and international standards ([6], [7]) that define information security management systems, and even practitioners, typically prefer quantitative approach.

This paper briefly describes the quantitative risk assessment approach with attention on its disadvantages when applied in information security. Four qualitative risk assessment methods are evaluated in more details. The evaluated methods are described in [1] and [2]. The evaluation consists of a method description and an assessment of its advantages and disadvantages.

This paper introduces a modified method that increases the reliability of risk assessment results, considering that other methods' disadvantages affect the reliability and further usability of their results. The modified method also allows additional flexibility in the risk management process, by using prioritization.

### 3. RISK ASSESSMENT

Generally, risk is represented as a combination of probability of an event and its impact or a (negative) consequence of the event when the threat was realized.

When discussing information security, an individual resource's risk (R) is assessed through its asset value (AV), its vulnerability (V), threats that can abuse these vulnerabilities (T), probability that the threats will happen (P) and consequences or impact (I) in the event when the threat has happened. Mathematically speaking, the risk is a function of the following variables (1).

$$R = f(AV, V, T, P, I) \quad (1)$$

In order to consider a risk assessment's results valid, the process has to satisfy the following criteria:

- uniqueness,
- objectiveness,
- reliability,
- repeatability.

## 4. QUANTITATIVE APPROACH

Quantitative approach to risk assessment is based on exact numerical values. In this case, function variables have precise values. The value of a resource is typically displayed in monetary units. Vulnerabilities, threats and impacts in an event of realization are displayed as an exposure factor (EF). The exposure factor represents percentage of loss of a resource's value, in case of a threat event [3]. The probability, which also depends on vulnerabilities and threats, is typically observed in a given time period, for which risk quantification will be valid (2).

$$R = AV * EF_{I,V,T} * P_{V,T} \quad (2)$$

For example, the risk for a resource that has the value of 1000\$, the exposure factor of 20% and the probability of 0.05% in a year can be easily calculated (3).

$$R = 1000\$ * 0,2 * 0,05 / year = 10\$ / year \quad (3)$$

Although the quantitative approach results in exact (absolute) risk values, when assessing information security risk this approach is not adequate for various reasons.

First, monetary value of a resource is typically based on a value provided by procurement or accounting office. This value does not have to represent the real value of the asset for a business process. For example, a critical database can be installed on an old server that has no real asset (monetary) value, while a completely new server can be used for less critical business processes. For the business, the value of the first server is much bigger than the second one, no matter what the current asset (monetary) value is.

Second problem when using quantitative risk assessment is establishment of an exposure factor. In most cases it is practically impossible to determine what the exposure factor is. Sometimes this can not even be done approximately.

Finally, the probability of a threat being realized is also difficult to determine. Even in cases where statistical data is available, it can cause additional errors in the risk assessment process. For example, a detailed statistical data about detected vulnerabilities in operating systems for the last couple of years is available. This data can indicate that operating system OS1 continuously had a lower number of security vulnerabilities than operating system OS2. A quantitative approach would, in this case, favor operating system OS1 and this does not need to be realistic.

Based on the above facts, it can be concluded that quantitative approach to risk assessment in information security systems is not appropriate because exact numerical values that this risk assessment methodology produces can not be trusted. The main reason for this is that values of variables used in the calculation can not be trusted.

For this reason, this paper will not discuss interpretation of results achieved through this methodology or its advantages and disadvantages [4].

## 5. QUALITATIVE APPROACH

Qualitative approach does not use absolute variable values, but instead it qualitatively evaluates influence of each variable on the risk. Experience, expertise and competence of a person conducting the risk assessment are the most important when taking a qualitative approach. The risk is assessed qualitatively; however, in order to interpret the results easier, variables, as well as the assessed risk, will be quantified. In contrast to qualitative risk assessments, in this case numeric values are not absolute, but relative.

Besides subjectivity, that is an inherent problem of the qualitative risk assessment method, an additional factor that can affect result reliability is how these, subjectively estimated parameters, are quantified. Risk quantification and repeated reinterpretation of these numerical values are all direct causes for result uncertainty.

Considering that qualitative variable values are estimated subjectively, in order to achieve repeatability, it is very important that the assessment process is unambiguous. In this case the same process can be repeated by different experts, and will produce same or similar results.

## 6. METHODS

There are various qualitative risk assessment methods available. This paper evaluates four qualitative risk assessment methods as described in [1] and [2].

Each of the methods uses some variables defined in formula (1). Methods are differentiated by variables they use and by how those variables were quantified.

### 6.1. METHOD 1: PREDEFINED VALUE MATRIX

This method uses three parameters to assess the risk: a resource value, threats and vulnerabilities. Each of these parameters is assessed relatively to possible threats, while the threats are assessed relatively to vulnerabilities (4). All values are quantified arbitrarily.

$$R = f(AV_I, V_{I,P}, T_{I,V,P}) \quad (4)$$

A variation of this method that is described in [1] and [2], uses numerical values ranging from 0 (low value) to 4 (high value) to determine resource value. For vulnerability and threat quantification the method uses values ranging from 0 (low level) to 2 (high level). Risk level is defined by a sum of parameters (5).

$$R = AV + V + T \quad (5)$$

Table 1 shows a matrix with predefined values.

	Threat	0			1			2		
	Vulnerability	0	1	2	0	1	2	0	1	2
Resource value	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

**Table 1:** Predefined values matrix

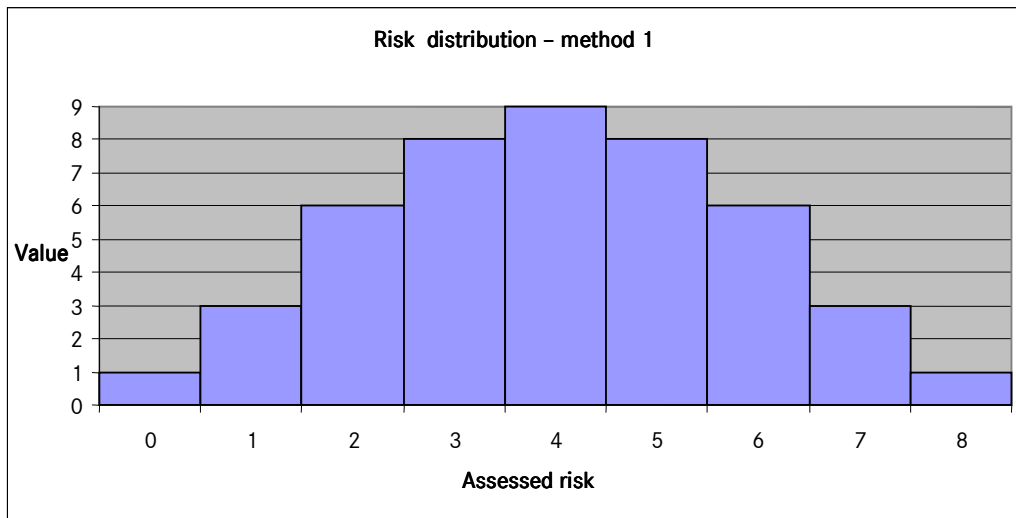
Based on (5) and parameter ranges defined in [1] and [2], minimum and maximum assessed risk values can be calculated (6).

$$\begin{aligned} R_{MIN} &= AV_{MIN} + V_{MIN} + T_{MIN} = 0 \\ R_{MAX} &= AV_{MAX} + V_{MAX} + T_{MAX} = 8 \end{aligned} \quad (6)$$

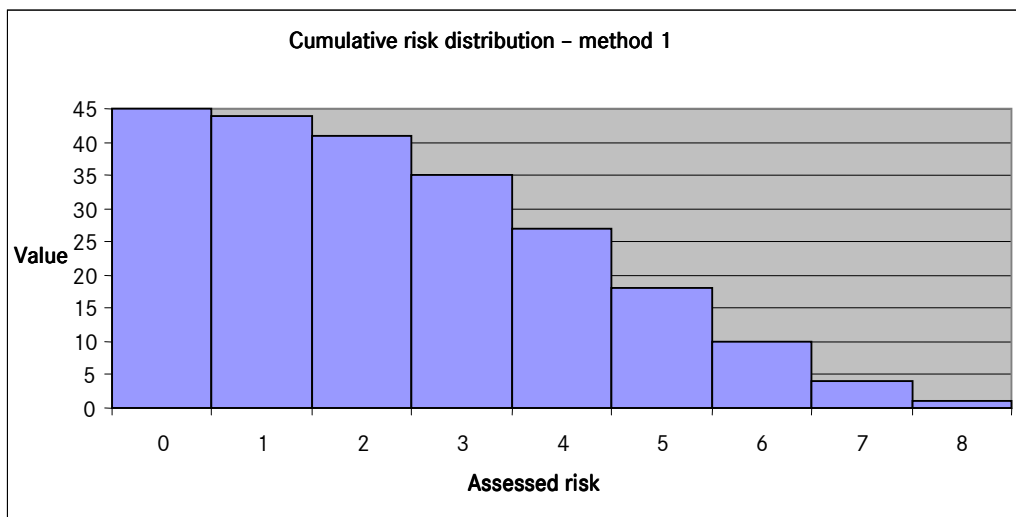
The assessed risk can be any integer value between and including  $R_{MIN}$  and  $R_{MAX}$ .

Figures 1 and 2 show distribution and cumulative distribution of the above risk assessment function.

It can be noticed that the risk assessment function distribution has averaging values (Figure 1), while the cumulative risk distribution function values are concave ().



**Figure 1:** Risk assessment function distribution - method 1



**Figure 2:** Cumulative risk assessment function distribution - method 1

By using a matrix with predefined values, one can arbitrarily rank the risk by its value during the risk treatment and management processes afterwards. Because of the distribution function, higher risks will not be prioritized.

A disadvantage of this method is that risk assessment explicitly does not use possible consequences and probabilities of threat realizations. The consequences are implicitly used to assess values of all parameters, while the probabilities of threat realizations should match probabilities of realization of individual occurrences.

Also, it is difficult to neutrally assess threats and vulnerabilities in the real world, so assessment of values for both parameters is pretty difficult.

## 6.2. METHOD 2: THREAT RANKING BY RISK EVALUATION

This risk assessment method formally uses only two parameters: impact on a resource (resource value) and probability of a threat being realized. It is implicitly assumed that the impact on a resource is equivalent to the resource value, while the threats are observed relatively to adequate vulnerabilities. This way assessed risk becomes a function of multiple parameters (7).

$$R = f(I_{AV,T}, P_{V,T}) \quad (7)$$

A variation of this method, which is explicitly described in [1] and [2], uses the same range of values for impact (the resource value) and probability of a threat realization. Possible values are ranging from 1 (low) to 5 (high). Risk level is calculated by multiplying these two parameters (8).

$$R = I * P \quad (8)$$

Table 2 shows a risk assessment matrix containing values resulting from the above formula. Threats also have values associated by the range defined above.

	Impact (value)	Realization probability	Risk	Threat ranges
Threat A	5	2	10	2
Threat B	2	4	8	3
Threat C	3	5	15	1
Threat D	1	3	3	5
Threat E	4	1	4	4
Threat F	2	4	8	3

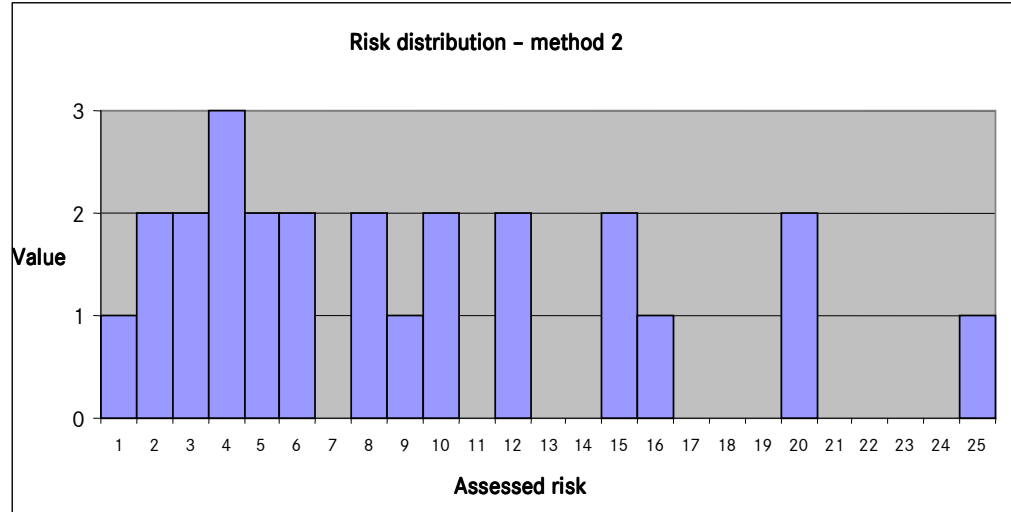
**Table 2:** Threat ranking by assessed risk

Based on (8) and value ranges defined in [1] and [2], minimal and maximal values of the assessed risk can be calculated (9).

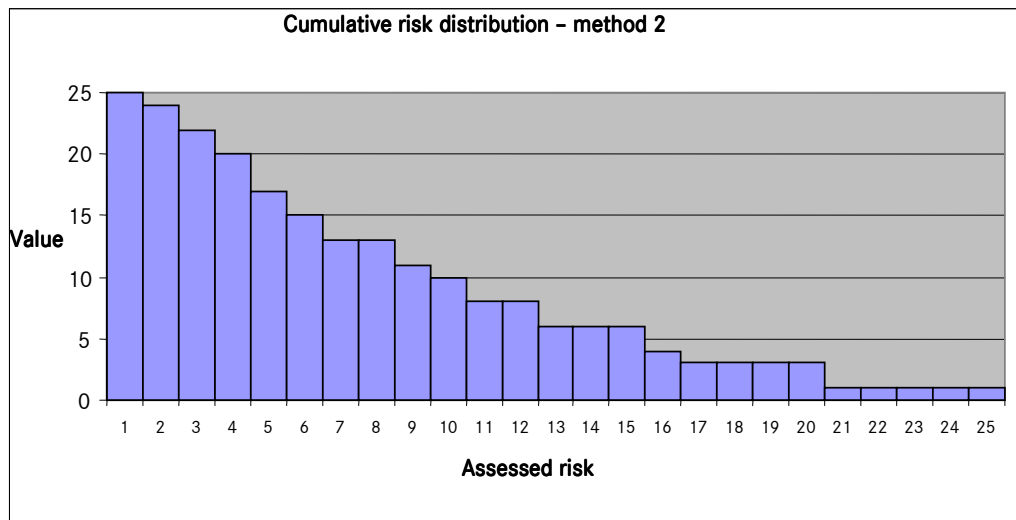
$$\begin{aligned} R_{MIN} &= I_{MIN} + P_{MIN} = 1 \\ R_{MAX} &= I_{MAX} + P_{MAX} = 25 \end{aligned} \quad (9)$$

Assessed risk can be any integer between and including  $R_{MIN}$  and  $R_{MAX}$ . Prime numbers outside this range are excluded, as well as their multiples.

Figures show distribution and cumulative distribution of the risk assessment function defined above.



**Figure 3:** Risk assessment function (method 2) distribution



**Figure 4:** Risk assessment function (method 2) cumulative distribution

From the figures above it is obvious that the risk assessment function group's lower values, while higher values are emphasized (Figure 3). The cumulative distribution graph is convex (Figure 4).

Threat ranking by risk assessment allows them to be prioritized during the following treatment (risk assessment) process.

A disadvantage of this method is that risk is explicitly assessed by only two parameters that are implicit functions of more variables. This method also equals a resource's value and the possibility of the resource being impacted; this approach is not correct in all cases.

### 6.3. METHOD 3: ASSESSMENT OF THE PROBABILITY OF A THREAT BEING REALIZED AND IT'S CONSEQUENCES

This method's risk assessment process is more complex than the previous two, and is conducted in two steps. First a resource's value, which is based on potential consequences of a threat being realized has to be defined. After this the probability of realization is calculated. This probability is based on threats and vulnerabilities (10).

$$P = f(V, T) \quad (10)$$

Finally, the risk is assessed as a combination of the resource's value and the probability of the threat being realized (11).

$$R = f(P_{V,T}, AV_{I,T}) \quad (11)$$

A variation of this method, explicitly described in [1] and [2], uses a range (0 - low, 4 - very high) to define a resource's value. A range between 0 (low) and 2 (high) is used to define how critical a vulnerability and threat is. The probability of realization (the frequency) can be calculated as a sum of assessed vulnerability and threat values (12).

$$P = V + T \quad (12)$$

The total risk is defines as a sum of the resource's value and the probability of the threat being realized (13).

$$R = AV + P = AV + V + T \quad (13)$$

Table 3 shows a probability of realization matrix.

With a probability of realization and the resource's value, it is possible to assess the risk by using a matrix defined in Table 4.

Minimum and maximum values of the assessed risk can be calculated as in (6), so they can be any integer value between and including  $R_{MIN}$  and  $R_{MAX}$ .

Distribution and cumulative distribution functions are same as in method 1 (Figure 1 and Figure 2).

Threat	0			1			2		
Vulnerability	0	1	2	0	1	2	0	1	2
Realization probability	0	1	2	1	2	3	2	3	4

**Table 3:** Realization probability matrix

Vrijednost resursa Vjerojatnost ostvarenja	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

**Table 4:** Risk assessment matrix

By assessing the realization probability and possible consequences (impact) it is possible to range risk by the assessed value, similarly to a matrix with predefined values.

Formulas that are used to assess risk in method 1 (predefined values matrix) (5) and in this method (13) are completely the same. However, method 1 implicitly reflects realization probability (frequency) during the vulnerability and threat assessment process, while this method assesses the realization probability based on assessed vulnerabilities and threats.

A disadvantage of this method is again independent assessment of threat levels and vulnerabilities.

#### 6.4. METHOD 4: ACCEPTABLE AND UNACCEPTABLE RISK SEPARATION

This method assesses the risk by using binary values. Risk can be acceptable (0) and unacceptable (1).

Risk assessment methodology can be same as described for the previous method (method 3). The only difference is that the assessed value risk matrix is binary (), as well as the value range (14).

Resource's value Realization probability	0	1	2	3	4
0	0	0	0	0	1
1	0	0	0	1	1
2	0	0	1	1	1
3	0	1	1	1	1
4	1	1	1	1	1

**Table 5:** Acceptable and unacceptable risk separation matrix

$$\begin{aligned} R_{MIN} &= 0 \\ R_{MAX} &= 1 \end{aligned} \quad (14)$$

This method is in fact a variation of method 3 (assessment of realization probability and possible consequences) or method 1 (predefined values matrix), so it shares their advantages and disadvantages.

## 7. QUALITATIVE RISK ASSESSMENT METHOD EVALUATION

Nonexistent financial values that are used for risk assessment can, but do not have to be a disadvantage when using a qualitative risk assessment method. A financial analysis can, in this case, be conducted later during the risk treatment (management) process.

The biggest disadvantage of any qualitative risk assessment method is subjectivity during a resource's value assessment, as these values are used as parameters later in the risk assessment process.

If a lower number of parameters that have to be assessed subjectively proportionally lowers unreliability of the result, the method 2 (threat ranging by risk assessment) that assesses the risk based on only two explicit values could be considered the most reliable.

However, as parameters for risk assessments are related (they are implicit functions of other parameters), they are actually introducing even more unreliability in the final result, especially when these functions depend on multiple parameters. Also, subjectivity while using functions with multiple implicit parameters can influence the risk assessment process repeatability, if the process is conducted independently by multiple persons in different time intervals.

In method 2, both parameters are implicit functions of multiple parameters and this influences the result reliability. An advantage of this method is that the risk is assessed as a multiplication of parameters. This allows a suitable value distribution and a precise definition of acceptable and unacceptable risk thresholds which results in a clean prioritization in the risk management process.

Method 4 presents a variation of methods 1 or 3 and will not be further discussed in this paper.

Methods 1 and 3 formally produce same risk assessment results. The fact that the realization probability in method 3 is assessed based on vulnerabilities and threats can be considered an advantage when comparing it to method 1, which implicitly includes this in the vulnerability and threat level assessment.

Both methods assess level of vulnerabilities and threats independently and this has been noted as a problem before as a reliable assessment of these values is very difficult in practice.

Finally, a smaller range of assessed risk values, caused by using a sum instead of a multiplication, can limit the risk assessment process later.

## 8. A MODIFIED QUALITATIVE RISK ASSESSMENT METHOD

Previously described methods have various disadvantages that can cause unreliable risk assessment results. In some cases the interval between assessed risk values can even be the limiting factor later when the risk is being managed.

Therefore, a modified qualitative risk assessment method described below is recommended.

### 8.1. ASSUMPTIONS

The modified qualitative risk assessment method is based on the following assumptions:

- Every resource has its value,
- Each resource is either vulnerable or it's not,
- If a system is vulnerable, there is at least one threat that can be realized (threats and vulnerabilities depend on each other),
- A threat has a certain probability of being realized, depending on circumstances,
- A threat has certain consequences that depend on circumstances.

### 8.2. RISK ASSESSMENT

Based on the assumptions above, risk assessment can be calculated with the following function (15).

$$R = f(AV, P_T, I_T), T = f(V) \quad (15)$$

All parameters are function of at most one variable – this ensures uniqueness and simplicity of interpretation.

Instead of adding parameters, as it was the case in methods 1 and 3, this modified method multiplies them in order to make the risk assessment method more dependable on parameters' values (16).

$$R = AV * P_T * I_T \quad (16)$$

Each parameter's values are arbitrary. In order to compare this method with method 1, resource values are on a scale from 1 to 5, while the threat probability and consequence values are on a scale from 1 to 3. Values start from 1 so the value of 0 is excluded.

The following table shows a modified risk assessment matrix.

Threat	Probability	1			2			3		
	Consequence	1	2	3	1	2	3	1	2	3
Resource value	1	1	2	3	2	4	6	3	6	9
	2	2	4	6	4	8	12	6	12	18
	3	3	6	9	6	12	18	9	18	27
	4	4	8	12	8	16	24	12	24	36
	5	5	10	15	10	20	30	15	30	45

**Table 6:** Modified risk assessment matrix

A matrix defined like the one above can be compared to the matrix shown in Table 1.

Based on (16) and on the recommended value scale, one can calculate minimal and maximal values of the assessed risk (17).

$$\begin{aligned} R_{MIN} &= AV_{MIN} * V_{MIN} * T_{MIN} = 1 \\ R_{MAX} &= AV_{MAX} * V_{MAX} * T_{MAX} = 45 \end{aligned} \quad (17)$$

Assessed risk can be any integer between  $R_{MIN}$  and  $R_{MAX}$ , excluding the prime numbers outside the parameter value scale and their multipliers.

Figures below show distribution and cumulative distribution of the risk assessment function defined above.

Similarly to method 2, the risk assessment function is grouping lower values, while higher values are emphasized (). The cumulative distribution graph is convex ().

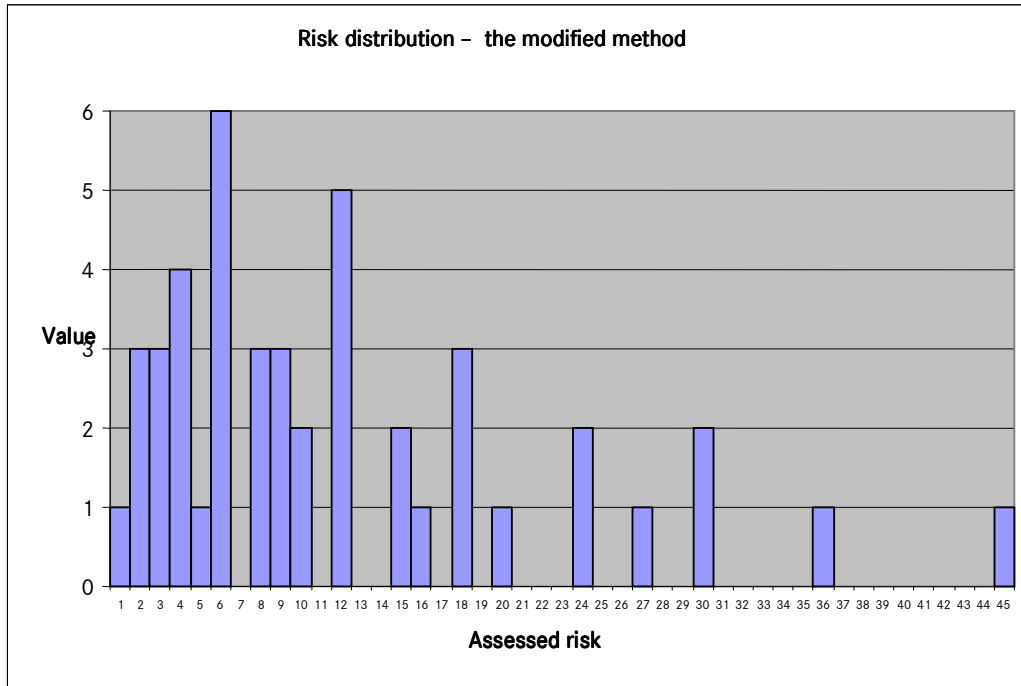


Figure 5: Risk assessment distribution function – the modified method

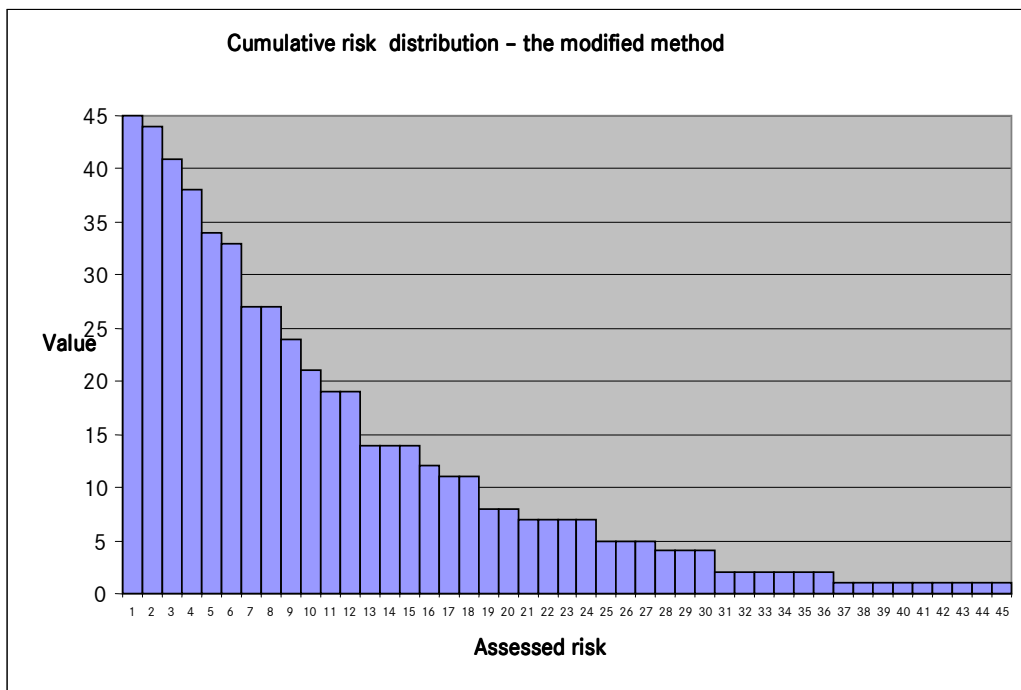


Figure 6: Cumulative risk assessment distribution function – the modified method

By emphasizing higher risks this distribution function allows better flexibility when the risk is being managed, comparing to method 1.

## 9. CONCLUSION

Quantitative risk assessment is the basis for risk management in information security management systems.

However, it is typically problematic to ensure that qualitative risk assessments are unique, reliable, objective and repeatable. Existing standards recommend various risk assessment methods that have certain disadvantages so they do not fulfill all risk assessment requirements.

This paper describes a modification of the described methods. The modification ensures that the risk can be assessed systematically and uniquely, without implicit parameters and functions. Values of the assessed risk are in an interval that allows more flexibility during the risk management phase. This can be an advantage, especially in big environments with a huge number of resources, as it allows efficient prioritization of critical elements.