Proposal of a Model Supporting Decision-Making on Information Security Risk Treatment

Ritsuko Kawasaki (Aiba), Takeshi Hiromatsu

Abstract—Management is required to understand all information security risks within an organization, and to make decisions on which information security risks should be treated in what level by allocating how much amount of cost. However, such decision-making is not usually easy, because various measures for risk treatment must be selected with the suitable application levels. In addition, some measures may have objectives conflicting with each other. It also makes the selection difficult. Therefore, this paper provides a model which supports the selection of measures by applying multi-objective analysis to find an optimal solution. Additionally, a list of measures is also provided to make the selection easier and more effective without any leakage of measures.

Keywords—Information security risk treatment, Selection of risk measures, Risk acceptance and Multi-objective optimization.

I. INTRODUCTION

This paper aims to support decision-making about risk treatment and risk acceptance for all information security risks within an organization.

In information security risk management, risk treatment and risk acceptance are the activities which particularly require decision-making by management. In other words, management is required to make decisions on which risks are treated in what level, and on which risks are accepted, among identified and evaluated risks in risk assessment processes. Here, a risk means an information security risk in this paper, though the term "risk" generally has broader meaning.

Risks are various, however management is required to understand all risks within an organization and to modify their values to the pre-defined "risk acceptance level" or less by distributing limited resources in the processes of risk treatment.

If a scope of risk management is quite limited, decision-making about risk treatment and risk acceptance may not be difficult very much, because in-depth risk assessment can be done and decision can be made based on detailed and specific information. On the other hand, if whole organization is a scope, applying detailed risk management is not realistic. It spends much time and cost, and its outcome is too much complicated to maintain and revise. Identification of risks and risk treatment plans in appropriate granularity is needed to make risk management pragmatic.

Risk treatment involves deciding the treating risks, selecting measures for them, and implementing measures. The levels of risks are modified to the risk acceptance level or less by implementing measures. For achieving the effective risk treatment, preparing the good list of candidates of measures is quite important.

The risks within an organization are various, so the measures are also various. Thus, the objective of each measure is also various. This means that risk treatment approach involves multi objectives and some objectives may conflict. For example, one of the measures is network access control. The objective of it is appropriately controlling network access. Application of this measure improves confidentiality, one of the aspects of information security; however, it may violate availability, another aspect of information security. Therefore, applying multi-objective optimization method is suitable to select measures, and the results are provided as Pareto optimal solutions.

For the reasons above, this paper provides a way to prepare a list of measures a way on how to quantify the relationship between each measure and each risk, a model providing one of the optimal solutions about the selection of measures, and the cost distribution for each measure.

The model uses goal programming for multi-objective optimization to find an optimal solution. The model is implemented by using solver add-in of Excel 2010. Thus, the model calculates one of the optimal solutions of selection of hedges and distribution of resources to each hedge selected.

II. LITERATURE REVIEW

The studies about risk treatment, which provide the ways on how to select measures to the risks identified, are limited. Among the few studies, the approaches by [1] and [2] are pragmatic as the approaches applying to an organization. They provide the ways modeling the relationship among assets, threats and measures, and logically find the optimal combinations of measures. The selection of measures is formulated as discrete optimization problems. However, they possess the following issues.

Firstly, the approaches assume identification and evaluation of assets and their threats. Setting these presuppositions is natural, because the previous international standard of ISO/IEC 27001:2005 [3] was required to identify and evaluate assets, threats and vulnerabilities to identify and evaluate risks within an organization. Previous international technical report of ISO/IEC TR 13335-3:1998 [4] also provide such guidance, and many users refer these documents. However, revised ISO/IEC 27001:2013 [5] does not include the requirements identifying assets, threats and vulnerabilities as activities of risk assessment. Only risks and their owners are required. When considering that ISO/IEC 27001:2005 [3] has broadly been
referred and new version of it will be referred from now on, the
method not to identify assets and threats will be needed.

Secondly, the studies do not provide detailed ways for the
preparation of a list of measures for the risks identified, though
it needs rich knowledge and experiences. The literature [1]
provides nothing about how to list up measures. The literature
[2] only describes: "measures are listed by referring [6], and the
measures achieving by organizational activities are omitted by
assuming that they are preferentially implemented." Thus, both
studies do not provide the ways how to make a list of measures.
As a result, the efficiency of the lists provided in these studies
cannot also be confirmed.

The literatures [7] and [8] provide the way to select measures
by analyzing in details within limited scopes. The literature [7]
proposes an optimal security objectives (measures) decision
method which determines security objectives (measures)
quantitatively from the viewpoint of effectiveness and
efficiency. The method includes a derivation scheme of
security objective (measures) candidate sets for protection from
possible threats by applying minimal path set search algorithm
on the fault trees with respect to the threats. This method can be
applied only for a product or a system with limited functions,
because of the complexity of its processes. The literature [8]
limits the threats to illegal copying, and provides the method to
obtain the optimal combination of countermeasures for illegal
copying, based on combinatorial optimization technique and
fault tree analysis. Since this method is also complex, removing
the limitation of threats is difficult. Both studies are suitable to
apply to a quite limited scope and are not suitable to apply to an
organization.

The literatures [9] and [10] are focusing on a risk of potential
lawsuit. They separate measures to two groups: measures for
risks of potential lawsuit, and measures which prevent information
security incidents. This approach may suitable for
an organization which deals with personal information and/or
data, because such an organization generally possesses high
risks of lawsuit. However, on the other hand, it can be
considered lacking versatility.

The literature [11] provides the approach to select
information security measures. The groups of controls provided
by ISO/IEC 27002 [12] are used as the list of measures in these
studies, because of the comprehensiveness and versatility
above a certain level. The approach aims to apply to an
organization, and to evaluate and identify the most appropriate
controls based on organization specific criteria. However, it
does not assume risk assessment. That is to say risk are not
identified and evaluated when using this approach. Risk
assessment has become a general process in organizational
management not only in information security field but also any
other management areas. ISO 31000 [13] provides principals,
framework and processes of risk management, (risk
management includes risk assessment), and all risks are
included in its scope. The identical text commonly used by
ISO's all management systems standards also includes the
notion of risks. From these situations, risk management process
can be considered to be adopted by many organizations. Thus,
selection of controls also should follow general risk assessment

approach. The approach provided by [14] is similar to [11].It
also does not assume risk assessment. The scope of [14] is
limited to electronic commerce.

III. A Model

A. Overview of a Model

The objective of the model proposed in this paper is
supporting a decision-making by management about risk
treatment and risk acceptance. More concretely to say, the
model provides the way to find one of the optimal solutions
about which risks are treating to what level by applying which
measures.

The following are the elements of the model:
1) A comprehensive list of risks within an organization and a
value of each risk,
2) A comprehensive list of measures and each cost needed to
implement each measure,
3) A value of effect by each measure to each risk,
4) A risk acceptance level (a value of risk acceptance), and
5) A total cost for measures (an organization's budget). The
lists and values of (1)-(3) are dealt with as fixed. The
values of (4) and (5) are changed when applying the model to
find optimal solutions. The solutions consists the degrees of
implementation of the measures listed. How to prepare (1)-(5)
is introduced in the following chapters.

B. A List of Risks and the Values of the Risks

The number of risks dealt with this model should be limited
to the number that management can pragmatically understand
and modify them. In this paper, seven risks are identified (see
Table I).

In addition, the risks must be identified without any leakage,
because unrecognized risks cannot be treated and as a result it
causes security failure. To eliminate any leakage, two attributes
"risk sources" and "motive of risks" are set. The attribute "risk sources"
are classified to four: internal users, contracted users,
other users and other than persons. Another attribute "motive of
risks" is classified to two: intentional and accidental. By
combining these attribute, all risks are separated to seven
groups. For example, one of the groups includes risks by
internal user’s intentional actions. Finally, each group is
considered as a risk and a list of seven risks are prepared (see
Table I).

<table>
<thead>
<tr>
<th>Name of Risks</th>
<th>Attribute 1 Risk Source</th>
<th>Attribute 2 Motive</th>
<th>Value (ri)</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>Internal user</td>
<td>Intentional</td>
<td>7</td>
</tr>
<tr>
<td>R2</td>
<td>Internal users</td>
<td>Accidental</td>
<td>6</td>
</tr>
<tr>
<td>R3</td>
<td>Contracted users</td>
<td>Intentional</td>
<td>8</td>
</tr>
<tr>
<td>R4</td>
<td>Contracted users</td>
<td>Accidental</td>
<td>7</td>
</tr>
<tr>
<td>R5</td>
<td>Other users</td>
<td>Intentional</td>
<td>9</td>
</tr>
<tr>
<td>R6</td>
<td>Other users</td>
<td>Accidental</td>
<td>8</td>
</tr>
<tr>
<td>R7</td>
<td>Not due to human</td>
<td>Intentional</td>
<td>6</td>
</tr>
</tbody>
</table>

The values of risks (ri) are set by using a numeric scale from
0 to 9, like in Table I in this paper. The methods proposed in
ISO/IEC 27005 [15] and [16] are assumed to be referred in order to set these values in this paper. Here, note that the values of risks differ from organization to organization depending on their business and environmental situations, thus the values in Table I is just an example. These values are considered fixed values in the model.

C. A List of Measures and the Costs Needed

The number of measures dealt with this model also should be limited to the pragmatic number. At the same time the list of measures must be comprehensive. In order to prepare such a list, ISO/IEC 27002:2013 [12] is referred in this mode, because it is widely used in information security field, and its lists of control objectives and controls are considered comprehensive at some level as generic lists. ISO/IEC 27002:2013[12] specifies 35 control objectives and 113 controls. Each control objective includes one or more controls, and control objectives are categorized to 14 clauses constructed by collecting similar control objectives. Thus, each clause includes one or more control objectives and controls under high level objectives.

A list of measures is set by using the structures of ISO/IEC 27002:2013 [12]. That is, 14 clauses are considered 14 measures. Here, the term “hedge” is used to indicate these 14 measures in order to distinguish from general measures, and controls in ISO/IEC 27002:2013 [12] (see Table II).

<table>
<thead>
<tr>
<th>Name of Hedge</th>
<th>Category</th>
<th>Cost (C)</th>
</tr>
</thead>
<tbody>
<tr>
<td>H₀</td>
<td>Security Policies (Clause 5)</td>
<td>500</td>
</tr>
<tr>
<td>H₁</td>
<td>Organization of Information Security (Clause 6)</td>
<td>1000</td>
</tr>
<tr>
<td>H₂</td>
<td>Human Resource Security (Clause 7)</td>
<td>1000</td>
</tr>
<tr>
<td>H₃</td>
<td>Asset Management (Clause 8)</td>
<td>1500</td>
</tr>
<tr>
<td>H₄</td>
<td>Access Control (Clause 9)</td>
<td>2500</td>
</tr>
<tr>
<td>H₅</td>
<td>Cryptography (Clause 10)</td>
<td>1000</td>
</tr>
<tr>
<td>H₆</td>
<td>Physical and Environmental Security (Clause 11)</td>
<td>5000</td>
</tr>
<tr>
<td>H₇</td>
<td>Operations Security (Clause 12)</td>
<td>1500</td>
</tr>
<tr>
<td>H₈</td>
<td>Communications Security (Clause 13)</td>
<td>1500</td>
</tr>
<tr>
<td>H₉</td>
<td>System Acquisition, Development and Maintenance (Clause 14)</td>
<td>2000</td>
</tr>
<tr>
<td>H₁₀</td>
<td>Supplier Security (Clause 15)</td>
<td>3000</td>
</tr>
<tr>
<td>H₁₁</td>
<td>Information Security Incident Management (Clause 16)</td>
<td>1500</td>
</tr>
<tr>
<td>H₁₂</td>
<td>Information Security Aspects of Business Continuity Management (Clause 17)</td>
<td>2000</td>
</tr>
<tr>
<td>H₁₃</td>
<td>Compliance (Clause 18)</td>
<td>1000</td>
</tr>
</tbody>
</table>

The characteristics that each hedge is consisted by one or more controls are used when quantifying an effect of each hedge to each risk as effect value (see next section).

In addition, the costs needed to implement the hedges (cᵢ) are required in the model. The values in Table II are set in this paper. The values of costs are assumed to be calculated by referring the descriptions of ISO/IEC 27002:2013[12] and the situation of an organization by using monetary value.

The hedges include a lot of controls, thus the notion of an implementation rate of a hedge is applied in this model, and a set of the rates is set as a solution of the model. Here, it is assumed that an effect of a hedge is directly proportional to a cost of a hedge, to simplify the model. By distributing organization’s total cost, the set of rates of implementation of hedges are decided automatically by applying this assumption (see Fig. 1).

D. Quantification of an Effect by Each Hedge to Each Risk

To find an optimal solution of a set of application rate of hedges, the relationship between hedges and risks are needed. In other words, an effect by each hedge to each risk is needed to be quantified. In order to quantify the effects, the characteristics of controls included in hedges are utilized.

The first step of the quantification is setting new aspects for controls to find the relationship between controls and hedges. The list of aspects in Table III is used. These aspects may be considered that they are duplicated to the categories applied in ISO/IEC 27002:2013 [12]. It is true; however, applying these aspects again for each control has a meaning. The controls set under a control objective in ISO/IEC 27002:2013 [12] are still high level. That is to say, a control includes a lot of concrete measures. For instance, a control “9.4.2 Secure log-on procedures” includes not only technical measures, such as applying a function for authentication and a function not disclosing sensitive information, but also operational measure, such as checking logs and making policy for log-on procedure. Thus, the aspect in Table III is set in order to analyze controls. The aspects are set by referring [17].
### TABLE III
ASPECTS APPLYING TO EACH CONTROL FOR QUANTIFICATION OF THE EFFECT VALUES

<table>
<thead>
<tr>
<th>Aspect</th>
<th>Measures included in the aspect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td>- Installation of appropriate equipment for protection from interference, damage, not allowed entry, etc.</td>
</tr>
<tr>
<td></td>
<td>- Access control to buildings and rooms</td>
</tr>
<tr>
<td></td>
<td>- Anti-theft for PC, mobile devices, etc.</td>
</tr>
<tr>
<td></td>
<td>- Administration of network and computer systems</td>
</tr>
<tr>
<td></td>
<td>- Access control on network and computer systems</td>
</tr>
<tr>
<td></td>
<td>- Development, implementation and maintenance of systems</td>
</tr>
<tr>
<td>Technical</td>
<td>- Anti-virus</td>
</tr>
<tr>
<td></td>
<td>- Collection of security information</td>
</tr>
<tr>
<td></td>
<td>- Monitoring</td>
</tr>
<tr>
<td></td>
<td>- Checking compliance</td>
</tr>
<tr>
<td></td>
<td>- Considerations to operations management</td>
</tr>
<tr>
<td></td>
<td>- Agreement for outsourcing</td>
</tr>
<tr>
<td></td>
<td>- Development of rules</td>
</tr>
<tr>
<td></td>
<td>- Setting roles and responsibilities</td>
</tr>
<tr>
<td></td>
<td>- Education and training</td>
</tr>
<tr>
<td></td>
<td>- Reporting scheme for incidents/accidents</td>
</tr>
<tr>
<td></td>
<td>- Password administration</td>
</tr>
<tr>
<td></td>
<td>- Contraction of temporary and part-time workers</td>
</tr>
</tbody>
</table>

### TABLE IV
AN EXAMPLE OF A CALCULATION OF AN EFFECT VALUE (A CASE OF H3)

<table>
<thead>
<tr>
<th>Control</th>
<th>Aspect</th>
<th>R1</th>
<th>R2</th>
<th>R3</th>
<th>R4</th>
<th>R5</th>
<th>R6</th>
<th>R7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clause 7</td>
<td>Human Resource Security</td>
<td>7.1 Prior to employment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Technical</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Operational</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Human Resource</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

| Clause 7 | Human Resource Security | 7.2 During employment |
| Physical | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Technical | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Operational | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| Human Resource | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

| Clause 7 | Human Resource Security | 7.3 Termination and change of employment |
| Physical | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Technical | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Operational | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| Human Resource | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |

| Sum | 9 | 7 | 0 | 4 | 4 | 0 | 0 |
| Effect value (Sum/234) | 0.04 | 0.03 | 0 | 0.02 | 0.02 | 0 | 0 |

### TABLE V
EFFECT VALUES OF ALL HEDGES TO EVERY RISK

<table>
<thead>
<tr>
<th>Risk Hedge</th>
<th>R1</th>
<th>R2</th>
<th>R3</th>
<th>R4</th>
<th>R5</th>
<th>R6</th>
<th>R7</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1</td>
<td>0.01</td>
<td>0.01</td>
<td>0.01</td>
<td>0.01</td>
<td>0.01</td>
<td>0.01</td>
<td>0.01</td>
</tr>
<tr>
<td>H2</td>
<td>0.06</td>
<td>0.06</td>
<td>0.06</td>
<td>0.06</td>
<td>0.06</td>
<td>0.05</td>
<td>0.02</td>
</tr>
<tr>
<td>H3</td>
<td>0.04</td>
<td>0.03</td>
<td>0.00</td>
<td>0.02</td>
<td>0.02</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>H4</td>
<td>0.10</td>
<td>0.10</td>
<td>0.09</td>
<td>0.10</td>
<td>0.10</td>
<td>0.09</td>
<td>0.04</td>
</tr>
<tr>
<td>H5</td>
<td>0.13</td>
<td>0.13</td>
<td>0.12</td>
<td>0.12</td>
<td>0.12</td>
<td>0.11</td>
<td>0.00</td>
</tr>
<tr>
<td>H6</td>
<td>0.02</td>
<td>0.02</td>
<td>0.02</td>
<td>0.02</td>
<td>0.02</td>
<td>0.02</td>
<td>0.00</td>
</tr>
<tr>
<td>H7</td>
<td>0.13</td>
<td>0.13</td>
<td>0.12</td>
<td>0.13</td>
<td>0.13</td>
<td>0.10</td>
<td>0.07</td>
</tr>
<tr>
<td>H8</td>
<td>0.11</td>
<td>0.11</td>
<td>0.08</td>
<td>0.11</td>
<td>0.11</td>
<td>0.07</td>
<td>0.03</td>
</tr>
<tr>
<td>H9</td>
<td>0.06</td>
<td>0.06</td>
<td>0.06</td>
<td>0.06</td>
<td>0.06</td>
<td>0.06</td>
<td>0.06</td>
</tr>
<tr>
<td>H10</td>
<td>0.11</td>
<td>0.12</td>
<td>0.10</td>
<td>0.10</td>
<td>0.11</td>
<td>0.10</td>
<td>0.08</td>
</tr>
<tr>
<td>H11</td>
<td>0.02</td>
<td>0.03</td>
<td>0.02</td>
<td>0.02</td>
<td>0.03</td>
<td>0.02</td>
<td>0.02</td>
</tr>
<tr>
<td>H12</td>
<td>0.05</td>
<td>0.05</td>
<td>0.05</td>
<td>0.05</td>
<td>0.05</td>
<td>0.05</td>
<td>0.05</td>
</tr>
<tr>
<td>H13</td>
<td>0.04</td>
<td>0.04</td>
<td>0.04</td>
<td>0.04</td>
<td>0.04</td>
<td>0.04</td>
<td>0.04</td>
</tr>
<tr>
<td>H14</td>
<td>0.06</td>
<td>0.06</td>
<td>0.04</td>
<td>0.06</td>
<td>0.06</td>
<td>0.04</td>
<td>0.04</td>
</tr>
</tbody>
</table>

### E. Other Components of a Model

A risk acceptance level and a total cost of for hedges are needed in the model. The risk acceptance level (R accept) is the
value that an organization aims to modify all-risks’ values ($r_i$, $i=1, 2, \ldots, 7$) to it or less. The total cost for hedges (B) means a budget for risk treatment of an organization. The sum of each cost implementing each hedge at some level cannot exceed the budget. These values are considered constraints in the model.

**F. Formula of a Model**

The model handles a set of application rates of hedges ($x_1, x_2, \ldots, x_{14}$) as a set of variables in the model. Where, $x_i$ is an application rate by percentage of $H_i$. Finding an optimal solution of the set of variables is an objective of the model. An optimal solution is defined which meets the following conditions in this model:

- the value of risks are modified to the pre-determined risk acceptance level or less,
- sum of the costs to be used to hedges is organization’s budget or less, and
- the difference between modified risks and risk acceptance level are minimize.

The first and second conditions are by the constraints, and the third condition is based on the thought that big difference between modified risks and the risk acceptance level means excessive use of cost. These conditions are converted to the following formulas.

For the original values of risks ($r_j$), the value after modification ($r_j'$) is calculated by (1), where $e_{ij}$ is an effect value of $H_i$ to $R_j$, and $R_{accept}$ is an risk acceptance level.

$$r_j' = r_j \times \left(1 - \frac{\sum_{i=1}^{14} e_{ij} \times x_i}{\sum_{i=1}^{14} e_{ij}} \times \frac{1}{100}\right) \leq R_{accept} \quad (1)$$

The formula of the second condition about cost is (2), where $c_i$ is the cost needed to implement $H_i$ completely, and B is the total cost for hedges (organization’s budget).

$$\sum_{i=1}^{14} c_i \times x_i \leq B \quad (2)$$

The formula of the third condition is (3), and this is the objective function of the model.

$$\text{Min. } \{f(x_i) = \sum_{j=1}^{7} (R_{accept} - r_j')\} \quad (3)$$

The model was implemented by using solver add-in, on Excel 2010 in this paper.

**IV. SAMPLE DATA APPLICATION TO A MODEL**

**A. The Objective of the Application of Sample Data**

In order to verify the effectiveness of the model, sample data is applied. Applying actual data to the model is desirable, however actual data of which amount of cost is spent to each hedge is not generally disclosed by organizations. Thus, sample data is prepared in this paper.

By applying such sample data to the model, the validation of solutions and the effectiveness of the model are analyzed.

**B. A Solution of a Model**

A solution of the model consists of the set of application rates by percentages of all hedges, and the sum of cost to be spent for the selected hedges’ implementation. The model needs the input of constraints. Table VI shows an example of a set of constraints, and the results for the inputs.

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Acceptance Level</td>
<td>5</td>
</tr>
<tr>
<td>Total Cost (Organization’s Budget)</td>
<td>12000</td>
</tr>
<tr>
<td>The Sum of Cost to be Spent</td>
<td>10756.94</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application level (%)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$H_1$</td>
<td>0</td>
</tr>
<tr>
<td>$H_2$</td>
<td>100</td>
</tr>
<tr>
<td>$H_3$</td>
<td>100</td>
</tr>
<tr>
<td>$H_4$</td>
<td>0</td>
</tr>
<tr>
<td>$H_5$</td>
<td>100</td>
</tr>
<tr>
<td>$H_6$</td>
<td>100</td>
</tr>
<tr>
<td>$H_7$</td>
<td>0</td>
</tr>
<tr>
<td>$H_8$</td>
<td>100</td>
</tr>
<tr>
<td>$H_9$</td>
<td>0</td>
</tr>
<tr>
<td>$H_{10}$</td>
<td>0</td>
</tr>
<tr>
<td>$H_{11}$</td>
<td>100</td>
</tr>
<tr>
<td>$H_{12}$</td>
<td>0</td>
</tr>
<tr>
<td>$H_{13}$</td>
<td>0</td>
</tr>
<tr>
<td>$H_{14}$</td>
<td>75.69</td>
</tr>
</tbody>
</table>

**C. Application of Basic Data to a Model**

Firstly, considering the case that $R_{accept}$ of 9 and total cost of 25000 are inputted. The model provides the result in Table VII in this case.

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Acceptance Level</td>
<td>9</td>
</tr>
<tr>
<td>Total Cost (Organization’s Budget)</td>
<td>25000</td>
</tr>
<tr>
<td>The Sum of Cost to be Spent</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application level (%)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$H_1$</td>
<td>0</td>
</tr>
<tr>
<td>$H_2$</td>
<td>0</td>
</tr>
<tr>
<td>$H_3$</td>
<td>0</td>
</tr>
<tr>
<td>$H_4$</td>
<td>0</td>
</tr>
<tr>
<td>$H_5$</td>
<td>0</td>
</tr>
<tr>
<td>$H_6$</td>
<td>0</td>
</tr>
<tr>
<td>$H_7$</td>
<td>0</td>
</tr>
<tr>
<td>$H_8$</td>
<td>0</td>
</tr>
<tr>
<td>$H_9$</td>
<td>0</td>
</tr>
<tr>
<td>$H_{10}$</td>
<td>0</td>
</tr>
<tr>
<td>$H_{11}$</td>
<td>0</td>
</tr>
<tr>
<td>$H_{12}$</td>
<td>0</td>
</tr>
<tr>
<td>$H_{13}$</td>
<td>0</td>
</tr>
<tr>
<td>$H_{14}$</td>
<td>0</td>
</tr>
</tbody>
</table>

Where, 25000 is the sum of $c_i$ and 9 is the highest value of risks. Thus, the inputs do not act as constraints in this case. The result means no hedge is implemented because all values of risks are under $R_{accept}$. Thus, this result is reasonable.
Next, considering the case that \( R_{\text{accept}} \) of 0 and total cost of 25000 are inputted. For the inputs, the model provides the result in Table VIII.

**TABLE VIII**

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>Total Cost (Organization's Budget) 25000</td>
</tr>
<tr>
<td></td>
<td>The Sum of Cost to be Spent 100</td>
</tr>
<tr>
<td></td>
<td>Application level (%)</td>
</tr>
<tr>
<td></td>
<td>H1 100</td>
</tr>
<tr>
<td></td>
<td>H2 100</td>
</tr>
<tr>
<td></td>
<td>H3 100</td>
</tr>
<tr>
<td></td>
<td>H4 100</td>
</tr>
<tr>
<td></td>
<td>H5 100</td>
</tr>
<tr>
<td></td>
<td>H6 100</td>
</tr>
<tr>
<td></td>
<td>H7 100</td>
</tr>
<tr>
<td></td>
<td>H8 100</td>
</tr>
<tr>
<td></td>
<td>H9 100</td>
</tr>
<tr>
<td></td>
<td>H10 100</td>
</tr>
<tr>
<td></td>
<td>H11 100</td>
</tr>
<tr>
<td></td>
<td>H12 100</td>
</tr>
<tr>
<td></td>
<td>H13 100</td>
</tr>
<tr>
<td></td>
<td>H14 100</td>
</tr>
</tbody>
</table>

The result means that all hedges are implemented under the sufficient budget to reduce values of all risks to zero. This result is reasonable.

**D. The Minimum Total Cost for a Given \( R_{\text{accept}} \)**

The minimum total cost can be found for a given \( R_{\text{accept}} \), by changing the value of total cost and applying the model. For example, for the total cost of 8000 and \( R_{\text{accept}} \) of 5, there is an optimal solution. For the total cost of 7000 and \( R_{\text{accept}} \) of 5, there is an optimal solution too. However, for the total cost of 6000 and \( R_{\text{accept}} \) of 5, there is no optimal solution (see Table IX). This means that the total cost of 8000 and 7000 are enough to achieve \( R_{\text{accept}} \) of 5; however, the total cost of 6000 is too small to achieve that. Thus, the minimum total cost for \( R_{\text{accept}} \) of 5 is more than 6000 and less than 7000.

**TABLE IX**

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>Risk Acceptance Level 8000 7000 6000</td>
</tr>
<tr>
<td></td>
<td>Total Cost 5 5 5</td>
</tr>
<tr>
<td></td>
<td>The Sum of Cost to be Spent 8000 7000 -</td>
</tr>
<tr>
<td></td>
<td>Application level (%)</td>
</tr>
<tr>
<td></td>
<td>H1 0</td>
</tr>
<tr>
<td></td>
<td>H2 100</td>
</tr>
<tr>
<td></td>
<td>H3 100</td>
</tr>
<tr>
<td></td>
<td>H4 27.22</td>
</tr>
<tr>
<td></td>
<td>H5 100</td>
</tr>
<tr>
<td></td>
<td>H6 0</td>
</tr>
<tr>
<td></td>
<td>H7 0</td>
</tr>
<tr>
<td></td>
<td>H8 100</td>
</tr>
<tr>
<td></td>
<td>H9 100</td>
</tr>
<tr>
<td></td>
<td>H10 0</td>
</tr>
<tr>
<td></td>
<td>H11 19.72</td>
</tr>
<tr>
<td></td>
<td>H12 0</td>
</tr>
<tr>
<td></td>
<td>H13 0</td>
</tr>
<tr>
<td></td>
<td>H14 100</td>
</tr>
</tbody>
</table>

Continuously, for the \( R_{\text{accept}} \) of 5, total cost of 6400 and 6300 are set. When total cost is 6400, a solution can be found. However, when total cost is 6400, there is not any solution. The approximate minimum total cost can be found for a given \( R_{\text{accept}} \) by changing total costs and apply them to the model.

**E. The Minimum \( R_{\text{accept}} \) for a Given Total Cost**

Next, in opposite to the previous section, the minimum \( R_{\text{accept}} \) can be found for a given total cost, by changing \( R_{\text{accept}} \) and applying them to the model. For example, for the total cost of 12000 and \( R_{\text{accept}} \) of 4, there is an optimal solution. For the total cost of 12000 and \( R_{\text{accept}} \) of 3, there is an optimal solution too. However, for the total cost of 12000 and \( R_{\text{accept}} \) of 2, there is no optimal solution (see Table XI). This means that the total cost of 12000 is insufficient to achieve \( R_{\text{accept}} \) of 2. Thus, \( R_{\text{accept}} \) of 3 is the smallest value achieved for the given total cost of 12000.

**TABLE X**

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>Risk Acceptance Level 6400 6300</td>
</tr>
<tr>
<td></td>
<td>Total Cost 5 5</td>
</tr>
<tr>
<td></td>
<td>The Sum of Cost to be Spent 6400 -</td>
</tr>
<tr>
<td></td>
<td>Application level (%)</td>
</tr>
<tr>
<td></td>
<td>H1 0</td>
</tr>
<tr>
<td></td>
<td>H2 100</td>
</tr>
<tr>
<td></td>
<td>H3 0</td>
</tr>
<tr>
<td></td>
<td>H4 12.22</td>
</tr>
<tr>
<td></td>
<td>H5 0</td>
</tr>
<tr>
<td></td>
<td>H6 0</td>
</tr>
<tr>
<td></td>
<td>H7 0</td>
</tr>
<tr>
<td></td>
<td>H8 100</td>
</tr>
<tr>
<td></td>
<td>H9 0</td>
</tr>
<tr>
<td></td>
<td>H10 54.72</td>
</tr>
<tr>
<td></td>
<td>H11 0</td>
</tr>
<tr>
<td></td>
<td>H12 0</td>
</tr>
<tr>
<td></td>
<td>H13 0</td>
</tr>
<tr>
<td></td>
<td>H14 0</td>
</tr>
</tbody>
</table>

Continuously, for the \( R_{\text{accept}} \) of 5, total cost of 6400 and 6300 are set. When total cost is 6500, a solution can be found. However, when total cost is 6400, there is not any solution. The approximate minimum total cost can be found for a given \( R_{\text{accept}} \) by changing total costs and apply them to the model.

**TABLE XI**

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>Risk Acceptance Level 12000 12000 12000</td>
</tr>
<tr>
<td></td>
<td>Total Cost 4 3 2</td>
</tr>
<tr>
<td></td>
<td>The Sum of Cost to be Spent 12000 12000 -</td>
</tr>
<tr>
<td></td>
<td>Application level (%)</td>
</tr>
<tr>
<td></td>
<td>H1 0</td>
</tr>
<tr>
<td></td>
<td>H2 100</td>
</tr>
<tr>
<td></td>
<td>H3 100</td>
</tr>
<tr>
<td></td>
<td>H4 48.54</td>
</tr>
<tr>
<td></td>
<td>H5 0</td>
</tr>
<tr>
<td></td>
<td>H6 98.98</td>
</tr>
<tr>
<td></td>
<td>H7 100</td>
</tr>
<tr>
<td></td>
<td>H8 0</td>
</tr>
<tr>
<td></td>
<td>H9 100</td>
</tr>
<tr>
<td></td>
<td>H10 0</td>
</tr>
<tr>
<td></td>
<td>H11 0</td>
</tr>
<tr>
<td></td>
<td>H12 22.86</td>
</tr>
<tr>
<td></td>
<td>H13 0</td>
</tr>
<tr>
<td></td>
<td>H14 0</td>
</tr>
</tbody>
</table>

Continuously, for the \( R_{\text{accept}} \) of 5, total cost of 6400 and 6300 are set. When total cost is 6500, a solution can be found. However, when total cost is 6400, there is not any solution. The approximate minimum total cost can be found for a given \( R_{\text{accept}} \) by changing total costs and apply them to the model.
In sum, the model can be used not only to find an optimal solution but also to find the minimum total cost for a given $R_{accept}$ and the minimum $R_{accept}$ for a given total cost.

V. CONCLUSIONS

A model to find an optimal solution which provides selected risk hedges with their application levels, under the constraints of the total cost of risk hedges and the risk acceptance level was proposed. This model can also be used to find the suitable risk acceptance level for a given total cost, and the appropriate total cost for a given risk acceptance level.

In this model, a generic list of measures was also provided as candidates of selection in risk treatment process. This list was prepared by referring ISO/IEC 27002:2013[12] in order to make it comprehensive, and the measures included in the list were called the hedges. The hedges are defined in large particle size, thus, the application level was defined in direct proportion to the cost in this model.

Finally, the way to quantify the effect by a hedge to a risk was proposed and it was called the effect value of a hedge to a risk.

VI. FUTURE TASKS

In order to show the effectiveness of the model, applying this model to a real case is needed as a future task. The problem is that the data about risk treatment and resource distribution is usually not disclosed. Finding raw data is difficult, thus expanding the target of data applying to the model, such as statistical data, is also needed to consider.

REFERENCES