EMPLOYING THE GREY RELATIONAL ANALYSIS TO IDENTIFY AND EVALUATE CLOUD COMPUTING RISKS

Chiang Ku Fan [1] & Cong-Syuan An[2]
[1,2] Department of Risk Management and Insurance, Shih Chien University. No.70, Dazhi St., Zhongshan Dist., Taipei City 104, Taiwan (R.O.C.)

ABSTRACT
Cloud computing will provide the basic levels of computing services that are considered essential to meet the everyday needs of the general community, similar to water, gas, telephone, and electrical utilities, but it also inevitably triggers a certain degree of loss exposure. Unfortunately, there is little objective, scientific research focused on evaluating the loss exposure that results from cloud computing. In this study, a modified Delphi method and the grey relational analysis (GRA) were employed to identify and evaluate risks of cloud computing. Research findings show that the risks of Agreement or contract, Social engineering, Mistakes made by employees intentionally or accidentally, System vulnerability, and Cross-cloud compatibility are rated highly on severity and frequency. The risks of Privacy and Damaged or spoiled by employees intentionally or accidentally are perceived as being more severe risks but occur at lower frequencies. The risks of Jurisdiction, Burglary, Normal wear and tear or malfunction, and Natural disaster are rated lower on severity and frequency.

Keywords: *cloud computing; risk management; grey relational analysis.*

1. INTRODUCTION

Cloud computing has revolutionized the architecture of computer systems. Enterprises can lower costs, save energy, and automatically upgrade their systems by replacing traditional computer systems and facilities with cloud computing services. Because of its increasing popularity, cloud computing is surely the future of information technology. Eventually, cloud computing will provide the basic levels of computing services that are considered essential to meet the everyday needs of the general community, similar to water, gas, telephone, and electrical utilities〔1〕.

Cloud computing may lead to both cost-efficiency and flexibility, but it also inevitably triggers a certain degree of loss exposure. Unfortunately, there is little objective, scientific research focused on identifying and evaluating the loss exposure that results from cloud computing. Insurers and enterprises have limited information to aid them in creating an appropriate risk management program. This study has the following objectives:

1. Identify the loss exposure attributable to cloud computing services using scientific and objective methods;
2. Measure and analyze loss exposure from cloud computing;
3. Provide administrators with the information necessary to make risk management decisions with regard to cloud computing;
4. Provide support for management's authorization of cloud computing based on objective, scientific, risk-focused assessments; and.

2. LITERATURE REVIEW

2.1. Risk Assessment and Plotting the Risk Management Matrix

To determine the appropriate technique or techniques for handling losses, a matrix (see Figure 1) may be helpful to identify different types of loss exposure according to the frequency and severity of risks〔2〕.

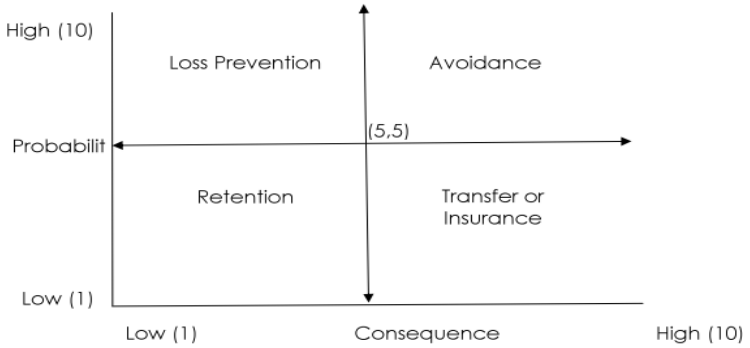

Figure 1. Risk Management Matrix

There is a widespread belief that the qualitative ranking provided by matrices reflects an underlying quantitative ranking. However, risk management matrices are constructed in an intuitive, often arbitrary, manner. Unfortunately, it is impossible to maintain perfect correspondence between qualitative matrices and quantitative rankings 〔3〕because it is not possible to represent quantitative rankings accurately on a rectangular grid〔4〕. Moreover, severity cannot be assessed objectively for uncertain outcomes. Risk matrix inputs (e.g., frequency and severity classifications) and their resulting outputs (e.g., risk ratings) require subjective interpretation, and different users may offer inconsistent ratings for the same quantitative risks. Therefore, the development of an appropriate risk assessment approach may enable risk managers to plot risks on matrices in a more logical manner. Fortunately, several studies provide a frame of reference for dealing with common problems related to quantitative risk assessment 〔5, 6, 7, 8〕. The common approach of these studies is to employ relative severity and frequency to assess risks, while utilizing information about the severity and frequency of risks from the literature and feedback from experts. In this study, an appropriate technique for the assessment of loss exposure is selected according to this approach.

2.2. Risks of Cloud Computing Services

In a traditional model of on-premises application deployment, the sensitive data of each enterprise resides within the enterprise itself and is subject to its physical, logistical, and personnel security control policies 〔9〕. However, in most cloud computing service models, enterprise data are stored externally. Because malicious users can exploit weaknesses in the data security model to gain unauthorized access to data, cloud computing vendors are urged to adopt additional security measures to prevent breaches. In other words, the use of cloud computing services implies system vulnerability associated with malicious employees 〔10〕. Unfortunately, not all security breaches in cloud computing are caused by cloud service providers. Employees' mistakes may also result in security breaches 〔11〕. One example is the use of weak security passwords or a standard company default password to log on to a network or e-mail platform〔10, 11〕.

Enterprises that use a cloud computing service may also have legal problems related to privacy, jurisdiction, and agreement or contract risks. The cloud infrastructure must address challenges beyond the traditional issues of remote access, data transfer, and intrusion detection and control through constant system monitoring 〔12〕. Cloud computing's unique schema for physical data storage may sufficiently store the data of multiple clients on one physical device. This shared physical server model requires the vendor to ensure that each customer's data are kept separate, so that no data bleeding occurs across virtual servers〔13〕. Furthermore, enterprises and individuals interested in using cloud computing services must be aware of the privacy risks associated with their use and take these risks into account when deciding to use cloud computing services 〔14〕. In many cases, vendor servers span multiple countries with different compliance and data privacy laws, making it unclear which legal entity has jurisdiction over the data 〔9, 12〕. Cloud computing also raises potential legal issues between cloud users and cloud providers 〔15, 13〕. The apportionment of liability in a cloud service contract may be unclear, or a user may get locked into a contractual arrangement that does not cater to the user's needs.

Cross-cloud compatibility is another risk that enterprises face when using a cloud computing service. An online storage service called "The Linkup" shut down on August 8, 2008, after losing access to as much as 45% of customer data. The Linkup's 20,000 users were told that the service was no longer available and were urged to use another storage site. Developing a new generalized usage model in which the same software infrastructure can be used across cloud service systems would mitigate these data lock-in concerns. Therefore, before developing interoperability technology and improving the portability of data and resources between different parts of the cloud, cloud computing services should first address the risk of cross-cloud compatibility because it creates significant uncertainty that will impact the efficiency of using a cloud computing service〔12〕.

To draw a conclusion from the prior literature review (a) Privacy, (b) Agreement or contract, (c) Jurisdiction, (d) Damaged or spoiled by employees intentionally or accidentally, (e) Burglary, (f) Normal wear and tear or malfunction, (g) Natural disaster, (h) System vulnerability, (i) Social engineering, (j) Mistakes made by employees intentionally or accidentally, and (k) Cross-cloud compatibility are eleven risks of cloud computing. This study also conducted a Delphi study and grey relational analysis (GRA) to identify the risks of using cloud services and the relative weights of each risk's frequency and severity.

3. METHODOLOGY

In this study, the estimation model is built in three phases (see Figure 2). In the first phase, the risks of applying cloud computing are identified using a modified Delphi method. In the second phase, the relative weights of the risk frequency and severity are calculated by employing grey relational analysis (GRA). In the third phase, measures to

mitigate the risks of cloud computing are proposed by using a frequency and severity matrix. The GRA adopted in this study is described as follows.

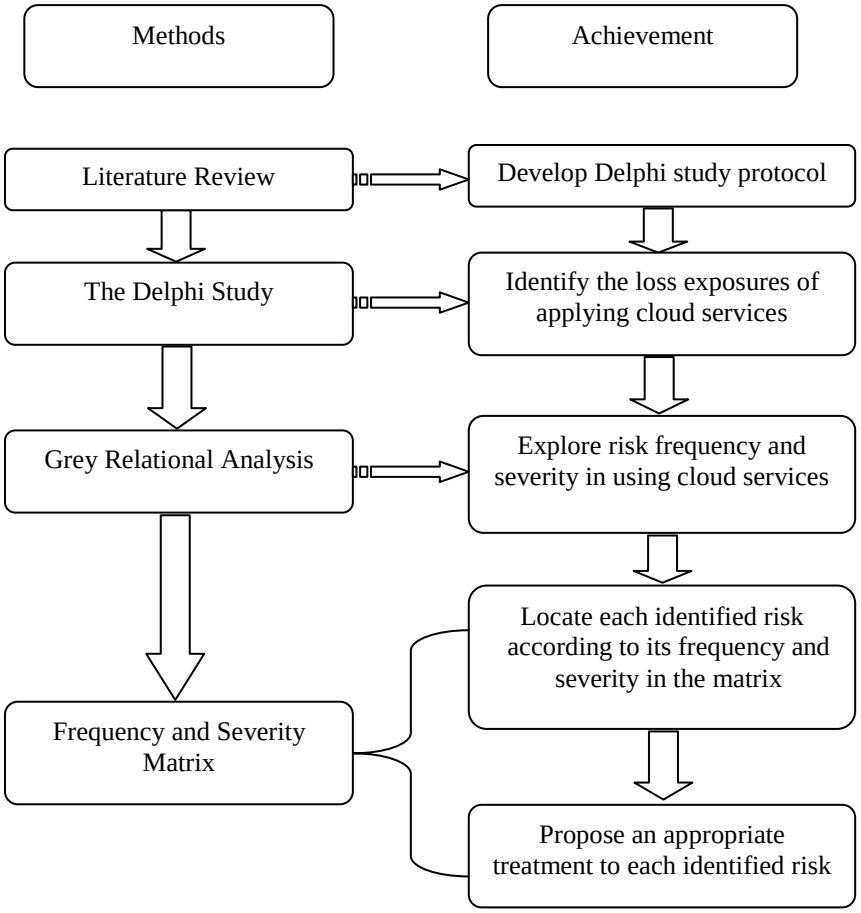

Figure 2.Theoretical Approach Adopted in This Study

The possible risks of cloud computing were derived first from the literature and experts' pinions and then were evaluated by 10 experts who were required to be in a management role at an information technology company and have knowledge of cloud computing. The 10 experts rated their five levels of frequency and severity toward risks of cloud computing. The grey relational analysis (GRA) initiated by Deng〔16, 17〕(1989; 1999) was conducted to rank the risks of cloud computing. The calculating procedure of GRA is discussed as following:

3.1. Calculate the Grey Relation Grade. Let X_0 be the referential series with k entities (or quality characteristics) of $X_1, X_2, \dots, X_i, \dots, X_N$ (or N detected candidate schemes)

$$X_0 = \{x_0(1), x_0(2), \cdots, x_0(j), \cdots, x_0(k)\},$$
$$\vdots$$
$$X_i = \{x_i(1), x_i(2), \cdots, x_i(j), \cdots, x_i(k)\},$$
$$\vdots$$
$$X_N = \{x_N(1), x_N(2), \cdots, x_N(j), \cdots, x_N(k)\}.$$

The grey relational coefficient between the compared series X_i and the referential series of X_0 at the j-th entity is defined as:

$$\gamma_{oi}(j) = \frac{\Delta_{\min} + \tau \Delta_{\max}}{\Delta_{0i}(j) + \tau \Delta_{\max}} \quad (1)$$

where $\tau = 0.5$ and $\Delta_{0i}(j)$ is the absolute value of difference between X_0 and X_i at the j-th entity, that is $\Delta_{0i}(j) = |x_0(j) - x_i(j)|$ and $\Delta_{\max} = \max_i \max_j \Delta_{0i}(j)$, $\Delta_{\min} = \min_i \min_j \Delta_{0i}(j)$. The grey relational grade (GRG) for series of X_i is given as:

$$\Gamma_{0i} = \frac{1}{k}\sum_{j=1}^{k} \gamma_{0i}(j) \tag{2}$$

3.2. Data Normalization (or Data Dimensionless).
Before calculating the grey relation coefficients, the data series can be treated based on the following three kinds of situation and the linearity of data normalization to avoid distorting the normalized data [25]. They are:

3.2.1. Upper-bound effectiveness measuring (i.e., larger-the-better)

$$x_i^*(j) = \frac{x_i(j) - \min_j x_i(j)}{\max_j x_i(j) - \min_j x_i(j)} \tag{3}$$

where $\max_j x_i(j)$ is the maximum value of entity *j* and $\min_j x_i(j)$ is the minimum value of entity *j*.

3.2.2. Lower-bound effectiveness measuring (i.e., smaller-the-better)

$$x_i^*(j) = \frac{\max_j x_i(j) - x_i(j)}{\max_j x_i(j) - \min_j x_i(j)} \tag{4}$$

3.2.3. Moderate effectiveness measuring (i.e., nominal-the-best)

$$x_i^*(j) = 1 - \frac{|x_i(j) - x_{ob}(j)|}{\max_j\{\max_j x_i(j) - x_{ob}(j), x_{ob}(j) - \min_j x_i(j)\}} \tag{5}$$

where $x_{ob}(j)$ is the objective value of entity *j*.

Thus, GRA method can detect the priority of the risks of cloud computing based upon ten experts' opinions. The procedures of detecting order of the priority are:

1. Sample ten experts and measure their quality characteristics for ten ranks.
2. Decide the referential series and the compared series.
3. Make data normalization for determining $x_i^*(j)$.
4. Compute $\Delta_{0i}(j)$.
5. Compute the relational coefficient, $\gamma_{0i}(j)$, of all compared series.
6. Compute the GRG, Γ_{0i} and can be to see the order for eleven ranks based upon the expert's opinion.

4. RESULTS

To identify the risks of applying cloud services, this study first used a purposive sampling technique to find participants for the Delphi study. This purposive sampling is applied to ten experts who match the characteristics shown in Table 1.

Table 1. Experts' Backgrounds

Expert	Employer	Years of Working Experience in Information Technology	Title
NO. 1	Model company A	12	Vice President.
NO. 2	Model company B	18	C. E. O.
NO. 3	Model company C	14	Senior Manager
NO. 4	Model company D	11	Vice Assistant President
NO. 5	Model company E	10	Senior Manager
NO. 6	Model company F	12	Vice President
NO.7	Model company G	10	Senior Engineer
NO.8	Model company H	11	Senior Manager
NO.9	Model company I	10	C. E. O.
NO.10	Model company J	15	Senior Engineer

4.1. Results from the Delphi Study

The aim of the Delphi study was to identify the risks of using cloud services. The Delphi respondents answered the interview questions and rated their level of agreement with risks, ranging from strongly agree (5) to strongly disagree (1). The interview protocol was developed based on a literature review. The interview more fully explored the perceptions of the experts regarding the risks of using cloud services. These qualitative responses helped explain quantitative responses to the standardized questions and qualitative themes that were representative of opinions expressed by a large majority of the Delphi respondents.

Descriptive statistics about the respondents' attitudes toward each risk are listed in Table 2. In the final round, ten Delphi respondents strongly agreed that "Privacy," "Agreement or contract," "Damaged or spoiled by employees intentionally or accidentally," "Natural disaster," "Social engineering," "Mistakes made by employees intentionally or accidentally," "Cross-cloud compatibility," and "Normal wear and tear or malfunction" were risks of using cloud services. Moreover, nine Delphi respondents strongly agreed that "Jurisdiction," "Burglary," and "System vulnerability" were risks of using cloud services. No respondents said they were undecided, disagreed, or strongly disagreed that these factors were risks faced by users of cloud services in round 3.

*Table 2. Descriptive Statistics for Attitudes toward Each Risk in Interview Rounds 2 and 3.*Attitudes toward Risks: Strongly Agree (SA), Agree (A) Undecided (UD), Disagree (D), and Strongly Disagree (SD).*

Risks	Attitude toward Risks※									
	SA		A		UD		D		SD	
	R2	R3	R2	R3	R2	R3	R2	R3	R2	R3
Privacy	9	10	0	0	0	0	0	0	0	0
Agreement or contract	9	10	0	0	0	0	0	0	0	0
Jurisdiction	8	9	1	1	1	0	0	0	0	0
Damaged or spoiled by employees intentionally or accidentally	8	10	1	0	0	0	0	0	0	0
Burglary	8	9	1	1	1	0	0	0	0	0
Normal wear and tear or malfunction	9	10	1	1	0	0	0	0	0	0
Natural disaster	10	10	0	0	0	0	0	0	0	0
System vulnerability	8	9	1	1	1	0	0	0	0	0
Social engineering	8	10	2	0	0	0	0	0	0	0
Mistakes made by employees intentionally or accidentally	10	10	0	0	0	0	0	0	0	0
Cross-cloud compatibility	9	10	1	0	0	0	0	0	0	0

Based on the results of a Kendall's Coefficient of Concordance Test, there were no significant attitude differences toward each risk among the seven Delphi experts. Thus, the 11 items proposed by this study should be identified as risks associated with the use of cloud services.

4.2. The Relative Weight of Each Identified Risk's Severity

The numerical illustration follows the procedures previously discussed.

4.2.1. Sample eleven ranks and their multiple quality characteristics are graded based upon ten Delphi panelists' opinions (see Table 3)

Table 3. Measured Multiple Quality Characteristics for Eleven Ranks

Risks of Cloud Computing	Quality Characteristics									
	Delphi Expert1	Delphi Expert2	Delphi Expert3	Delphi Expert4	Delphi Expert5	Delphi Expert6	Delphi Expert7	Delphi Expert8	Delphi Expert9	Delphi Expert10
Privacy	5.0000	5.0000	4.0000	4.0000	4.0000	4.0000	4.0000	4.0000	4.0000	4.0000
Agreement or contract	5.0000	4.0000	4.0000	4.0000	4.0000	5.0000	4.0000	5.0000	5.0000	4.0000
Jurisdiction	4.0000	4.0000	3.0000	4.0000	3.0000	4.0000	4.0000	3.0000	4.0000	3.0000
Damaged or spoiled by employees intentionally or accidentally	5.0000	4.0000	4.0000	4.0000	4.0000	5.0000	5.0000	5.0000	5.0000	4.0000
Burglary	4.0000	4.0000	4.0000	3.0000	4.0000	3.0000	3.0000	3.0000	3.0000	3.0000
Normal wear and tear or malfunction	4.0000	4.0000	3.0000	3.0000	3.0000	3.0000	3.0000	3.0000	3.0000	2.0000
Natural disaster	3.0000	3.0000	3.0000	3.0000	3.0000	4.0000	2.0000	3.0000	2.0000	3.0000
System vulnerability	5.0000	4.0000	4.0000	4.0000	4.0000	4.0000	4.0000	4.0000	4.0000	3.0000
Social engineering	4.0000	4.0000	4.0000	5.0000	4.0000	4.0000	4.0000	4.0000	4.0000	5.0000
Mistakes made by employees intentionally or accidentally	4.0000	4.0000	4.0000	4.0000	4.0000	4.0000	4.0000	4.0000	4.0000	5.0000
Cross-cloud compatibility	5.0000	4.0000	5.0000	5.0000	4.0000	5.0000	4.0000	4.0000	4.0000	3.0000

4.2.2. According to literatures reviewing, eleven risks of cloud computing are important equally. Moreover, the quality characteristic is a nominal-the-best response. Therefore, the referential series can be X_0=(5,5,5,5,5,5,5,5,5,5,5) and the quality characteristics of compared series are X_1, X_2, X_3, X_4, X_5, X_6, X_7, X_8, X_9, X_{10}, and X_{11}.

4.2.3. Data normalization are obtained by using Eqs. (3). The results are tabulated in Table 4.

Table 4. Summary of Data Normalization

Risks of Cloud Computing	Quality Characteristics									
	Delphi Expert1	Delphi Expert2	Delphi Expert3	Delphi Expert4	Delphi Expert5	Delphi Expert6	Delphi Expert7	Delphi Expert8	Delphi Expert9	Delphi Expert10
Privacy	1.0000	1.0000	0.5000	0.5000	1.0000	0.5000	0.6667	0.5000	0.6667	0.6667
Agreement or contract	1.0000	0.5000	0.5000	0.5000	1.0000	1.0000	0.6667	1.0000	1.0000	0.6667
Jurisdiction	0.5000	0.5000	0.0000	0.5000	0.0000	0.5000	0.6667	0.0000	0.6667	0.3333
Damaged or spoiled by employees intentionally or accidentally	1.0000	0.5000	0.5000	0.5000	1.0000	1.0000	1.0000	1.0000	1.0000	0.6667
Burglary	0.5000	0.5000	0.5000	0.0000	1.0000	0.0000	0.3333	0.0000	0.3333	0.3333
Normal wear and tear or malfunction	0.5000	0.5000	0.0000	0.0000	0.0000	0.0000	0.3333	0.0000	0.3333	0.0000
Natural disaster	0.0000	0.0000	0.0000	0.0000	0.0000	0.5000	0.0000	0.0000	0.0000	0.3333
System vulnerability	1.0000	0.5000	0.5000	0.5000	1.0000	0.5000	0.6667	0.5000	0.6667	0.3333
Social engineering	0.5000	0.5000	0.5000	1.0000	1.0000	0.5000	0.6667	0.5000	0.6667	1.0000
Mistakes made by employees intentionally or accidentally	0.5000	0.5000	0.5000	0.5000	1.0000	0.5000	0.6667	0.5000	0.6667	1.0000
Cross-cloud compatibility	1.0000	0.5000	1.0000	1.0000	1.0000	1.0000	0.6667	0.5000	0.6667	0.3333

4.2.4. Compute $\Delta_{0i}(j)$. The results are tabulated in Table 5.

Table 5. The Result of $\Delta_{0i}(j)$

Risks of Cloud Computing	Quality Characteristics									
	Delphi Expert1	Delphi Expert2	Delphi Expert3	Delphi Expert4	Delphi Expert5	Delphi Expert6	Delphi Expert7	Delphi Expert8	Delphi Expert9	Delphi Expert10
Privacy	0.0000	0.0000	0.5000	0.5000	0.0000	0.5000	0.3333	0.5000	0.3333	0.3333
Agreement or contract	0.0000	0.5000	0.5000	0.5000	0.0000	0.0000	0.3333	0.0000	0.0000	0.3333
Jurisdiction	0.5000	0.5000	1.0000	0.5000	1.0000	0.5000	0.3333	1.0000	0.3333	0.6667
Damaged or spoiled by employees intentionally or accidentally	0.0000	0.5000	0.5000	0.5000	0.0000	0.0000	0.0000	0.0000	0.0000	0.3333
Burglary	0.5000	0.5000	0.5000	1.0000	0.0000	1.0000	0.6667	1.0000	0.6667	0.6667
Normal wear and tear or malfunction	0.5000	0.5000	1.0000	1.0000	1.0000	1.0000	0.6667	1.0000	0.6667	1.0000
Natural disaster	1.0000	1.0000	1.0000	1.0000	1.0000	0.5000	1.0000	1.0000	1.0000	0.6667
System vulnerability	0.0000	0.5000	0.5000	0.5000	0.0000	0.5000	0.3333	0.5000	0.3333	0.6667
Social engineering	0.5000	0.5000	0.5000	0.0000	0.0000	0.5000	0.3333	0.5000	0.3333	0.0000
Mistakes made by employees intentionally or accidentally	0.5000	0.5000	0.5000	0.5000	0.0000	0.5000	0.3333	0.5000	0.3333	0.0000
Cross-cloud compatibility	0.0000	0.5000	0.0000	0.0000	0.0000	0.0000	0.3333	0.5000	0.3333	0.6667

4.2.5. Compute the relational coefficient, $\gamma_{0i}(j)$ of compared series by using Eq. (1) and the results are tabulated in Table 6.

Table 6. The Result of Relational Coefficients $\gamma_{0i}(j)$

Risks of Cloud Computing	Quality Characteristics									
	Delphi Expert1	Delphi Expert2	Delphi Expert3	Delphi Expert4	Delphi Expert5	Delphi Expert6	Delphi Expert7	Delphi Expert8	Delphi Expert9	Delphi Expert10
Privacy	1.0000	1.0000	0.6667	0.6667	1.0000	0.6667	0.7500	0.6667	0.7500	0.7500
Agreement or contract	1.0000	0.6667	0.6667	0.6667	1.0000	1.0000	0.7500	1.0000	1.0000	0.7500
Jurisdiction	0.6667	0.6667	0.5000	0.6667	0.5000	0.6667	0.7500	0.5000	0.7500	0.6000
Damaged or spoiled by employees intentionally or accidentally	1.0000	0.6667	0.6667	0.6667	1.0000	1.0000	1.0000	1.0000	1.0000	0.7500
Burglary	0.6667	0.6667	0.6667	0.5000	1.0000	0.5000	0.6000	0.5000	0.6000	0.6000
Normal wear and tear or malfunction	0.6667	0.6667	0.5000	0.5000	0.5000	0.5000	0.6000	0.5000	0.6000	0.5000
Natural disaster	0.5000	0.5000	0.5000	0.5000	0.5000	0.6667	0.5000	0.5000	0.5000	0.6000
System vulnerability	1.0000	0.6667	0.6667	0.6667	1.0000	0.6667	0.7500	0.6667	0.7500	0.6000
Social engineering	0.6667	0.6667	0.6667	1.0000	1.0000	0.6667	0.7500	0.6667	0.7500	1.0000
Mistakes made by employees intentionally or accidentally	0.6667	0.6667	0.6667	0.6667	1.0000	0.6667	0.7500	0.6667	0.7500	1.0000
Cross-cloud compatibility	1.0000	0.6667	1.0000	1.0000	1.0000	1.0000	0.7500	0.6667	0.7500	0.6000

4.2.6. Compute the related grade, Γ_{0i}, by using Eq(2) to determine the rank grade. The result reported in Table 7.

Table 7. Summary of the GRG Γ_{0i}

	Privacy	Agreement or contract	Jurisdiction	Damaged or spoiled by employees intentionally or accidentally	Burglary	Normal wear and tear or malfunction	Natural disaster	System vulnerability	Social engineering	Mistakes made by employees intentionally or accidentally	Cross-cloud compatibility
Γ_{0i}	0.7917	0.8500	0.6267	0.8750	0.6300	0.5533	0.5267	0.7433	0.7833	0.7500	0.8433
Rank	4	2	9	1	8	10	11	7	5	6	3

From Table 6, this study decided the grey relation was following:
$\gamma(\chi_0, \chi_4) > \gamma(\chi_0, \chi_2) > \gamma(\chi_0, \chi_{11}) > \gamma(\chi_0, \chi_1) > \gamma(\chi_0, \chi_9) > \gamma(\chi_0, \chi_{10}) > \gamma(\chi_0, \chi_8) > \gamma(\chi_0, \chi_5) > \gamma(\chi_0, \chi_3) > \gamma(\chi_0, \chi_6) > \gamma(\chi_0, \chi_7)$

In other words, after conducting the grey relational analysis, this research showed the rank of eleven risks of cloud computing from the most severity to the least severity, but still crucial, risks are showed as followings (see Table 8): (1) Damaged or spoiled by employees intentionally or accidentally, (2) Agreement or contract, (3) Cross-cloud compatibility, (4) Privacy, (5) Social engineering, (6) Mistakes made by employees intentionally or accidentally, (7) System vulnerability, (8) Burglary, (9) Jurisdiction, (10) Normal wear and tear or malfunction, and (11) Natural disaster.

Table 8. The Results from the Grey (Severity)

Risks	GRG
Privacy	0.7917
Agreement or contract	0.8500
Jurisdiction	0.6267
Damaged or spoiled by employees intentionally or accidentally	0.8750
Burglary	0.6300
Normal wear and tear or malfunction	0.5533
Natural disaster	0.5267
System vulnerability	0.7433
Social engineering	0.7833
Mistakes made by employees intentionally or accidentally	0.7500
Cross-cloud compatibility	0.8433

4.3. The Relative Weight of Each Identified Risk's Frequency

The relative weight for each identified risk's frequency, presented in Table 10, was obtained by repeating the same evaluation procedures as in the previous section. The GRG (frequency) are also presented in Table 9. The ranking is Agreement or contract > Cross-cloud compatibility > Mistakes made by employees intentionally or accidentally > System vulnerability > Social engineering > Burglary > Damaged or spoiled intentionally or accidentally by employees > Privacy = Jurisdiction > Normal wear and tear or malfunction > Natural disaster.

Table 9. The Results from the Grey (Frequency)

Risks	GRG
Privacy	0.6450
Agreement or contract	0.9083
Jurisdiction	0.6450
Damaged or spoiled by employees intentionally or accidentally	0.6633
Burglary	0.6800
Normal wear and tear or malfunction	0.6033
Natural disaster	0.5100
System vulnerability	0.8100
Social engineering	0.7600
Mistakes made by employees intentionally or accidentally	0.8167
Cross-cloud compatibility	0.9017

4.4. The Relative Weights of Severity and Frequency of Each Identified Risk

The relative weights of severity and frequency for each identified risk are presented in Table 10.

Table 10. The Relative Weights of Severity and Frequency for Each Identified Risk

Identified Risk	Frequency	Severity	Location
Privacy	0.6450	0.7917	II
Agreement or contract	0.9083	0.8500	I
Jurisdiction	0.6450	0.6267	III
Damaged or spoiled by employees intentionally or accidentally	0.6633	0.8750	II
Burglary	0.6800	0.6300	III
Normal wear and tear or malfunction	0.6033	0.5533	III
Natural disaster	0.5100	0.5267	III
System vulnerability	0.8100	0.7433	I
Social engineering	0.7600	0.7833	I
Mistakes made by employees intentionally or accidentally	0.8167	0.7500	I
Cross-cloud compatibility	0.9017	0.8433	I
Mean	0.7221	0.7248	Origin

4.5. The Customized Risk Management Matrix

The risk management matrix gives risk managers an overview of the relationship between risk factors and the frequency and severity of risks so that risk managers can develop strategies to mitigate risks. This study places frequency on the X axis and severity on the Y axis. The point where the two axes intersect is called the origin. The origin consists of two variables that are defined as the means of risks' relative frequencies and relative severities assessed in the GRA (see Table 10 and Figure 3).

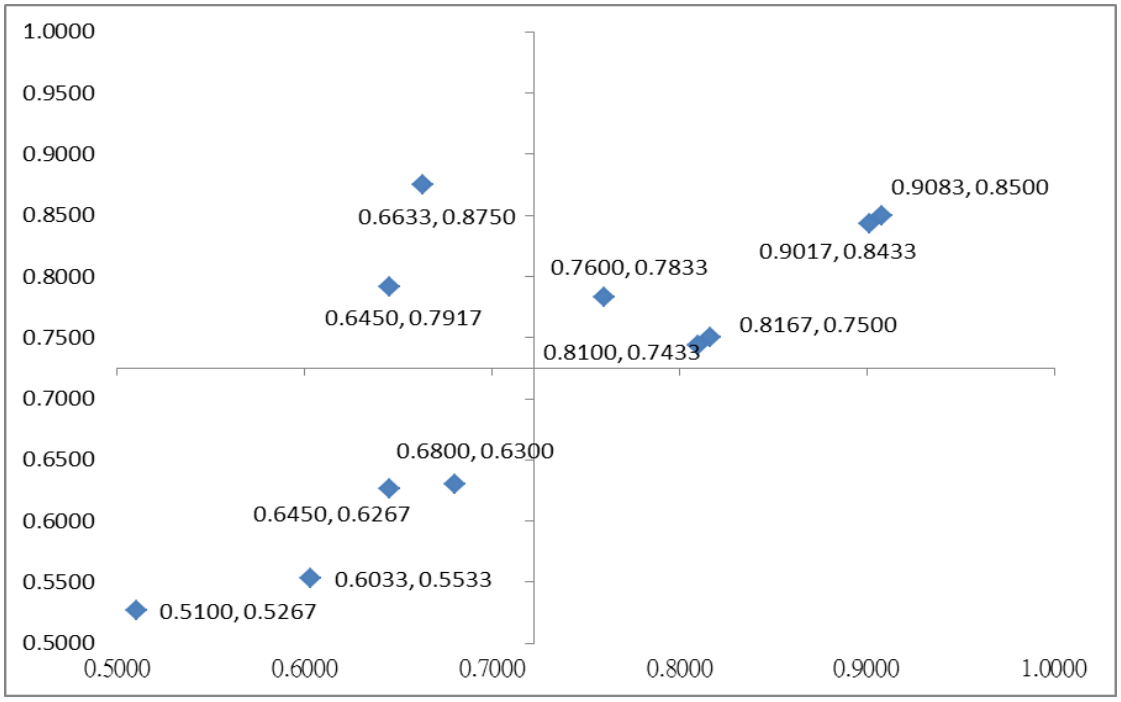

Figure 3. Risk Management Matrix

Figure 3 shows that the risks of Agreement or contract, Social engineering, Mistakes made by employees intentionally or accidentally, System vulnerability, and Cross-cloud compatibility are located in quadrant (I) because they are rated highly on severity and frequency. The risks of Privacy and Damaged or spoiled by employees intentionally or accidentally fall into quadrant (II) because they are perceived as being more severe risks that occur at lower frequencies. The risks of Jurisdiction, Burglary, Normal wear and tear or malfunction, and Natural disaster are located in quadrant (III) because they are rated lower on severity and frequency. No risks are present in quadrant (IV).

5. CONCLUSIONS AND IMPLICATIONS

Loss exposure attributable to Jurisdiction, Burglary, Normal wear and tear or malfunction, and Natural disaster located in quadrant (III) are characterized by low frequency as well as relatively low severity. If losses occur regularly and are predictable, a retention technique, such as self-funding, is recommended.

Loss exposures attributable to Privacy and Damaged or spoiled by employees intentionally or accidentally can be addressed through insurance. Insurance is not only most appropriate for mitigating these risks but also economically feasible for risks that seldom occur but result in severe losses. It is recommended that risk managers also adopt a combination of insurance and retention techniques to mitigate these risk exposures.

Risks generated through Agreement or contract, Social engineering, Mistakes made by employees intentionally or accidentally, System vulnerability, and Cross-cloud compatibility located in quadrant (I) are characterized by both high frequency and severity. This type of exposure is best handled by avoidance. But as a practical matter, not all risks can or even should be avoided. Therefore, to mitigate legal risks involving contracts or agreements, it is necessary to hire a contract lawyer to review agreements and help companies solve issues related to breaches of contract or disputes over agreements. To minimize the risk of cross-cloud compatibility, a company can propose a cross-cloud application management platform to administrate applications among heterogeneous clouds to control the application's compatibility so that applications can run under heterogeneous cloud platforms. Although protecting against reverse social engineering is probably the most difficult challenge, it is recommended that risk managers design a defense against social engineering threats for the staff in a company. To reduce the risks of mistakes made by employees, it is important to provide more effective, task-related training to involved employees. However, all of the above solutions can only reduce the risks of recurrence (risk frequency) but not eliminate recurrences. In other words, risk is inevitable, but risks with severe consequences may be heavy burdens. Purchasing insurance, if possible, is also strongly recommended.

6. REFERENCES

[1]. R. Buyya, M. Parashar, User requirements for cloud computing architecture, Proc. 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing, Melbourne, Australia. 17-20 May, 625-630 (2010).

[2]. G.E. Rejda, Principles of Risk Management and Insurance, 11th Edition, Prentice Hall, New Jersey (2011).

[3]. K. Awati, Cox's Risk Matrix Theorem and Its Implications for Project Risk Management', http://eight2late.wordpress.com/2009/07/01/cox%E2%80%99s-risk-matrix-theorem-and-its-implications-for-project-risk-management/, accessed 18 Dec 2011 (2009).

[4]. L.A. Cox, What's Wrong with Risk Matrices? Risk Analysis. 28(2), 497-515 (2008).

[5]. S.H. Lim, Risks in the North Korean Special Economic Zone: Context, Identification, and Assessment, Emerging Markets Finance & Trade. 47(1), 50-66 (2011).

[6]. F. Picado, G. Barmen, G. Bengtsson, S. Cuadra, K. Jakobsson, A. Mendoza, Ecological, Groundwater, and Human Health Risk Assessment in a Mining Region of Nicaragua, Risk Analysis: An International Journal. 30(6), 916-933 (2010).

[7]. K.D.M. Pintar, D.F. Charron, A. Fazil, S.A. McEwen, F. Pollari, D. Waltner-Toews, A Risk Assessment Model to Evaluate the Role of Fecal Contamination in Recreational Water on the Incidence of Cryptosporidiosis at the Community Level in Ontario, Risk Analysis: An International Journal. 30(1), 49-64 (2010).

[8]. T. Aven, O. Renn, The Role of Quantitative Risk Assessments for Characterizing Risk and Uncertainty and Delineating Appropriate Risk Management Options, with Special Emphasis on Terrorism Risk, Risk Analysis: An International Journal. 29(4), 587-600 (2009).

[9]. S. Subashini, V. Kavitha, A Survey on Security Issues in Service Delivery Models of Cloud Computing, Journal of Network and Computer Applications. 34, 1-11 (2011).

[10]. J. Casale, Social Networking, Cloud Computing Bring New Risk Exposures, Business Insurance. 44(38), 17 (2010).

[11]. E. Bublitz, Catching The Cloud: Managing Risk When Utilizing Cloud Computing, National Underwriter P & C. 114(39), 12-16 (2010).

[12]. S. Paquette, P.T. Jaeger, S.C. Wilson, Identifying the Security Risks Associated with Governmental Use of Cloud Computing', Government Information Quarterly. 27, 245-53 (2010).

[13]. P.T. Jaeger, J.M. Grimes, J. Lin, S.N. Simmons, Where Is the Cloud? Geography, Economics, Environment, and Jurisdiction in Cloud Computing. 14(5), 4-15 (2009).

[14]. D. Svantesson, R. Clarke, Privacy and Consumer Risks in Cloud Computing, Computer Law & Security Review. 26, 391-397 (2010).

[15]. M. Armburst, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, *et al*. Above the Clouds: A Berkley View of Cloud Computing', http://radlab.cs.berkekey.edu/, accessed 5 Dec 2011 (2009).

[16]. J. Deng, Introduction to Grey System, Journal of Grey System. 1(1), 1-24 (1989).

[17]. J. Deng, Grey System Theory and Applications, Kao-Li, Taiwan, (1999).