The Risk Management Strategy of Applying Cloud Computing

Chiang Ku Fan
Department of Risk Management and Insurance
Shih Chien University.
No.70, Dazhi St., Zhongshan Dist., Taipei City 104,
Taiwan (R.O.C.)

Tien-Chun Chen
Department of Risk Management and Insurance
Shih Chien University.
No.70, Dazhi St., Zhongshan Dist., Taipei City 104,
Taiwan (R.O.C.)

Abstract— **It is inevitable that Cloud Computing will trigger off some loss exposures. Unfortunately, not much of scientific and objective researches had been focused on the identification and evaluation of loss exposures stemming from applications of Cloud Computing. In order to fill this research gap, this study attempts to identify and analyze loss exposures of Cloud Computing by scientific and objective methods which provide the necessary information to administrators in support of decisions of risk management. In conclusion, this study has identified "Social Engineering", "Cross-Cloud Compatibility" and "Mistakes are made by employees intentionally or accidentally" are high priority risks to be treated. The findings also revealed that people who work in the field of information or Cloud Computing are somehow ignorant of where the risks in Cloud Computing lie due to its novelty and complication.**

Keywords- Cloud Computing; Risk Assessment; Risk Management; Insurance.

I. INTRODUCTION

Since 1980's, the functions of Personal Computer (PC) have indicated that their capabilities have been widely developed to serve human beings with all kinds of daily works. After that, networks have reached every single corner on this planet. During the Past decade, there are more than 2 billion network users now around the world, 5 times of the number of year 2000. The quality and quantity of PC fall behind the pace of fast growing network and PC users. This was the reason why traditional functionality of computer could no longer satisfy PC users and scientists. As a result, engineers strived to devise new technologies to meet different needs all over the world.

Fortunately, Cloud Computing system, a revolutionary architecture of computer system, has been emerged in recent years. Statistics data shows that 66% of USB sticks are lost and around 60% of those lost contain commercial data. Feigenbaum said [1], the enterprise security director of Google, stated that data is typically lost when laptops and Universal Serial Bus(USB) flash drives are lost or stolen, however, local storage is no longer necessary if a company uses cloud-based apps.

This new development has brought computer users' interests back to the information technology. Thanks to the rapidly increased popularity, Cloud Computing services are destined to be the next generation of information technology. Cloud computing providers offer individuals, enterprises and government agencies a variety of services that allow users to apply Cloud Computing for saving and sharing information, database management, data mining as well as their far-reaching web services ranging from mega datasets processing for complex scientific problems to utilizing clouds to administrate and supply access to certain records [2]. In other words, Cloud Computing, which yields highly scalable computing application, storage and platforms, is playing more and more important role through-out business information technology strategy [3]. The computing utility, like all other four existing utilities: water, gas, telephony, and electricity, will provide the basic level of computing service that is considered essential to meet the everyday needs of the general community [4].

While it is true that Cloud Computing services are a modern trend and around 75% of companies and public sectors intend to reallocate or increase their budgets to finance secure Cloud Computing and "Software as a Service" (SaaS) according to some surveys conducted within 2010, however, certain concerns about Cloud Computing and services do exist nowadays. For example, International Data Corporation's (IDC) report shows that 30% of respondents were seeking data security and non-stop support from their cloud providers. Moreover, issues regarding reliability, security, availability, privacy, performance and the management of service level agreements of software services are deeply concerned by the users in the cloud [5][6][7]. In addition, the Chief Information Security officers (CISOs) pointed out that their particular concerns are about the lack of standards for working in the cloud, SaaS, and the secure internet access. Because lack of standards not only makes companies unable to back up their data from one Cloud Computing service providers to another, but also makes it difficult to handle the service interruption of Cloud providers .

We are never short of stories about Cloud Computing service interruptions. For example, Amazon put their users out of service for six hours in February 2008 while their Simple Storage Service (S3) and Elastic Compute Cloud (EC2) suffered a three hours outage. In July, the same year, an eight hours outage was again caused by Amazon's S3 [8]. Google's Webmail service "Gmail" went down for three hours in early 2009, thus prevented its 113 million users from accessing their emails or documents they stored online as "Google Docs" [9].

Base on the discussion above, taking the advantages of Cloud Computing may obviously an ideal solution that leads to both cost-efficiency and flexibility. However, it is inevitable that Cloud Computing will trigger off some loss exposures need to be treated. Unfortunately, there were rare scientific and objective researches focused on identifying and evaluating the loss exposures from applications of Cloud Computing. Insurers or enterprises have only limited information to refer to when they attempt to plan an appropriate risk management program. In order to fill the blank with regard to the research on loss exposures identification and evaluation in Cloud Computing services, the purposes of this study are:

1) to identify loss exposures of Cloud Computing services by scientific and objective methods;

2) to measure and analyze the loss exposures with regard to application of Cloud Computing;

3) to provide the necessary information to administrators in support of decision making risk management with regard to employment of Cloud Computing;

4) to support management's authorization of Cloud Computing based on objectively and scientifically risk-focused assessments; and

5) to recommend essential risk management strategies could be employed to control or reduced losses attributable to the application of Cloud Computing.

II. Literature Review

The major purposes of this research are to identify loss exposures of Cloud Computing services by scientific methods and evaluate the loss exposures with regard to application of Cloud Computing. Therefore, this study is going to review the prior literatures related to the definition of Cloud Computing, risk management, and risks of applying Cloud Computing service.

A. The Definition of Cloud Computing

Throughout scientific literatures, many different definitions of Cloud Computing can be found. Svantesson and Clarke [10] defined Cloud Computing as typically a technical arrangement under which users store their data on remote servers under the control of other parties, and rely on software applications stored and perhaps executed elsewhere, rather than on their own computers. In other words, the Cloud Computing appears to be a single point of access for all the Information Technology (IT) requests from consumers.

Based on the observations of Knorr & Gruman [11] and Ward & Sipior [12], the essence of Cloud Computing may be an updated version of utility computing which includes virtual servers delivered over internet; while a broader definition encompasses IT resources outside of the firewall including conventional outsourcing. To draw a conclusion from the above definitions, Cloud Computing, obviously, is not a new technology but a new concept and a new business model. Moreover, Cloud Computing is an evolving term that describes the development into something different. Meanwhile, many studies or reports described Cloud Computing. The most common descriptions are "agility", "scalability", "availability", "cost-efficiency" , "elasticity", "extensibility" [3][13][14][15].

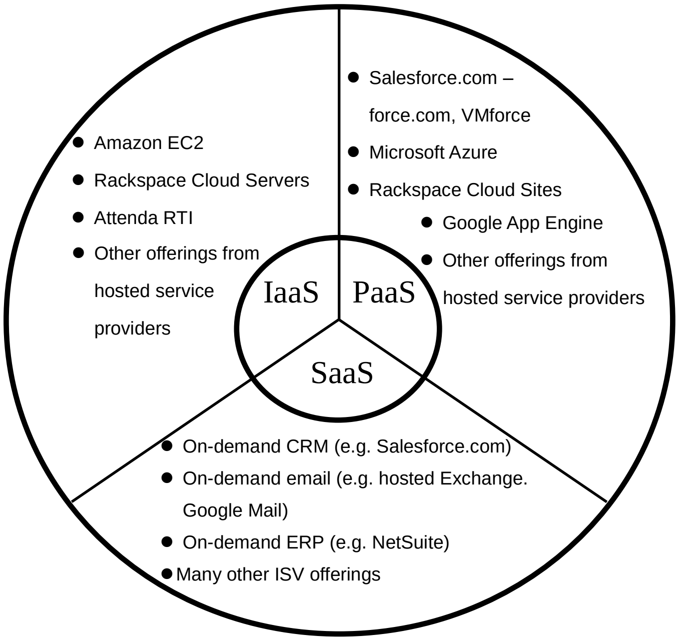
IaaS
PaaS
SaaS
Amazon EC2
Rackspace Cloud Servers
Attenda RTI
Other offerings from hosted service providers
Salesforce.com – force.com, VMforce
Microsoft Azure
Rackspace Cloud Sites
Google App Engine
Other offerings from hosted service providers
On-demand CRM (e.g. Salesforce.com)
On-demand email (e.g. hosted Exchange. Google Mail)
On-demand ERP (e.g. NetSuite)
Many other ISV offerings

Figure 1. Products in Different Cloud Computing Service Level. [16]

There is not much doubt that Cloud Computing improves a company's ability to flexibly scale services up and down. In detail, Cloud Computing can be classified into three services layers. The lowest level is Infrastructure as a Service (IaaS). This is where pre-configured hardware is provided via a virtualized interface or hypervisor.

There is no high level infrastructure software provided such as an operating system, this must be provided by the buyer embedded with their own virtual applications. Platform as a Service (PaaS) goes a stage further and includes the operating environment included the operating system and application services.

PaaS suits organizations that are committed to a given development environment for a given application but like the idea of someone else maintaining the deployment platform for them. Software as a Service (SaaS) offers fully functional applications on-demand to provide specific services such as email management, Customer Relationship Manage, Enterprise Resource Planning, web conferencing and an increasingly wide range of other applications [12][15][17]. Fig. 1, for examples, shows products of every Cloud Computing service level.

B. Risk Assessment and Plotting in Risk Management Matrix

In the research of Marshall and Alexander [18], participants were asked to think of the risks their businesses faced and list these risks. The participants were then asked to evaluate the probability and the consequence of the risks on a scale of 1 to 10, where 1 is low and 10 is high.

The consequence of the risks can be evaluated by terms of severity and cost to the business. Once the participants have rated the probability and consequence of all risks, it can be placed on the risk management matrix shown in Fig. 2.

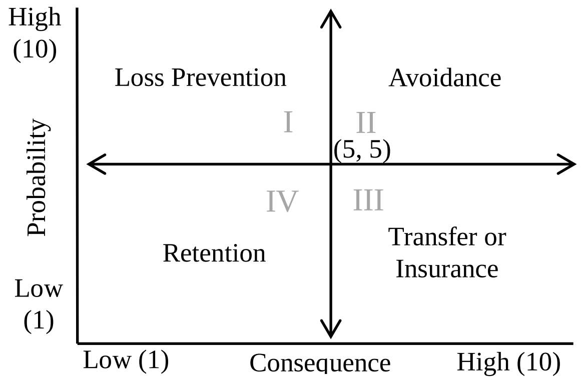

Figure 2. Risk Management Matrix

Many variations of above risk management matrix model are in use. Descriptions of consequence and probability along the two axes may vary [19][20], as many descriptions in particular cells, depending on the context and requirements of the organization using the model. Some versions incorporate references to the organization's decision-making structure [21]. This facilitates assessment of where a particular risk falls in terms of consequence and probability (many other axes such as "frequency" and "severity" or "likelihood" and "impact" are also used, but changing names does not affect the logic.) and helps establish the organizational response to manage the risk [22][23]. Based on the prior studies, the standard and major approach of assessing and characterizing risk is to use matrices which categorize risks by consequence and probability of occurrence. In other words, a two-dimensional risk matrix was usually used to analyze exposures (also see Fig. 2). The consequence (severity) is displayed on the horizontal axis, and the probability (frequency) is displayed on the vertical axis. The resulting four quadrants are with the risk characteristics of high frequency and high severity; high frequency and low severity; low frequency and high severity; and low frequency and low severity. In determining the appropriate technique or techniques for handling losses, a matrix can be used that classifies the various loss exposures according to frequency and severity [24].

There is a widespread belief that the qualitative ranking provided by matrices reflects an underlying quantitative ranking. Typically these matrices are constructed in an intuitive (but arbitrary) manner. Unfortunately, it is impossible to maintain perfect congruence between qualitative (matrix) and quantitative rankings [21].This is essentially due to the impossibility of representing quantitative rankings accurately on a rectangular grid [25]. Moreover, Categorizations of severity cannot be made objectively for uncertain consequences. Inputs to risk matrices (e.g., frequency and severity categorizations) and resulting outputs (e.g., risk ratings) require subjective interpretation, and different users may obtain opposite ratings of the same quantitative risks. Therefore developing an appropriate risk assessment approach may enable risk managers to plot risk on matrices in a more logically sound manner. Fortunately, some studies provided good references which may deal with the problems of tradition of quantitative risk assessment [26][27][28][29]. Their common approach is to employ relative severity and frequency to assess risks while severity and frequency information come from review of the literature and export elicitation.

C. *Risks of Cloud Computing Service*

The sensitive data of each enterprise, which is in a traditional on-premise application deployment model, continues to reside within the enterprise boundary and is subject to its physical logical and personnel security and access control policies [14]. However, the enterprise data is stored outside the enterprise in the most of Cloud Computing service model. Therefore, the Cloud Computing vendor is usually suggested to adopt additional security checks to prevent breaches. This is because malicious users can exploit weakness in the data security model to gain unauthorized access to data. In other words, applying Cloud Computing service has the risk of system vulnerability through malicious employees [30]. Unfortunately, not all security breaches in the Cloud Computing are the fault attributable to the Cloud Computing service provider. Mistakes made by employees intentionally or accidentally are the risk which results in breaches [31]. For example, the use of poor passwords or company's default password to log on to their network or e-mail platform [30][31].

Utilizing Cloud Computing service, enterprises may get into legal troubles which are caused by the risks of privacy, jurisdiction, and agreement or contract. The cloud infrastructure needs to suffer challengers beyond the traditional issues of remote access, data transfer, and intrusion detection and control through constant system monitoring [3]. The unique schema for physical data storage may well house multiple clients' data on one physical device. This shared physical server model requires the vendor to ensure that each separate customer's data remains segregated so that no data bleeding occurs across virtual servers [32]. Further, enterprises and individuals interested in applying Cloud Computing services must ensure they are aware of the privacy risk associated with using the product and take this risk into account when deciding whether to use it [33]. In many cases, vendors' servers span multiple countries, due to compliance and data privacy laws in various countries, whose jurisdiction the data falls under, when an investigation occurs [3][14]. There is also another law issue raised by applying Cloud Computing between cloud users and cloud provider [32][34]. Such as to sign an unclear delineation of liability in a Cloud Computing service contract, or to get locked into a contractual arrangement that does not cater for the user's needs.

Besides law issues, cross cloud compatibility is another risk need to be concerned as utilizing Cloud Computing service. An online storage service called The Linkup shut down on August 8, 2008 after losing access as much as 45% of customer data. The Linkup's 20,000 users were told the service was no longer available and were urged to try out another storage site. In addition to mitigating data lock-in concerns, developing a new generalized usage model in which the same software infrastructure can be used in cross-cloud. Therefore, before developing interoperability technology and improving portability of data and resources between parts of the cloud, the risk of cross cloud compatibility actually is a significant uncertainty that will impact the efficiency of utilizing Cloud Computing service [3].

In practice, there is no specialized policy designed to cover Cloud Computing risks. However, the traditional policies (e.g. Cyber Security Liability Insurance, Cyber breach Insurance, Privacy-Data Breach Insurance, and Network Security and Privacy Insurance) provide partial coverage regard to the risks of applying Cloud Computing such as information, cyber or internet security. Thus, by reviewing coverage or exclusion noted in the policies, some risks related to utilizing Cloud Computing service could be recognized. The risks covered and excluded by policies can be classified into six categories, including legality, system vulnerability, social engineering, administrative or operational mistakes, damage cause by rogue employee, and damage cause by natural disaster.

III. METHODOLOGY

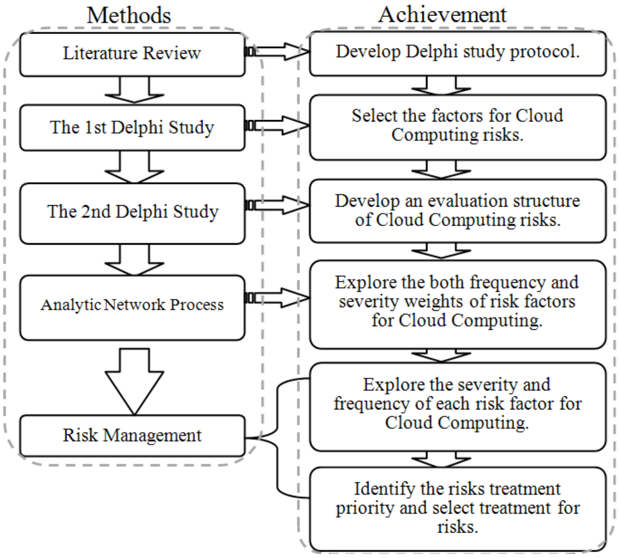
Methods
Achievement
Literature Review
Develop Delphi study protocol.
The 1st Delphi Study
Select the factors for Cloud Computing risks.
The 2nd Delphi Study
Develop an evaluation structure of Cloud Computing risks.
Analytic Network Process
Explore the both frequency and severity weights of risk factors for Cloud Computing.
Explore the severity and frequency of each risk factor for Cloud Computing.
Risk Management
Identify the risks treatment priority and select treatment for risks.

Figure 3. Theoretical Approach Adopted in This Study

The purpose of this paper is to identify and analyze the Cloud Computing related risks. More importantly, combine risk management matrix and ANP's result to provide practical implication. In order to achieve the objectives of this study, the estimation model in this study consists of three phases. In the first phase, the key success factors for Cloud Computing and hierarchical structure of evaluation are identified by using the modified Delphi method. In the second phase, risks' weights of frequency and severity of Cloud Computing are also used as the evaluation criteria and are calculated effectively by employing the "Analytic Network Process" (ANP). In the third phase, the gaps between risks' weights of Cloud Computing and the risk treatment priorities are recognized by using the "Risk Management Matrix". Theoretical approaches adopted herein are described as Fig. 3.

A. *Analytic Network Process*

After Delphi study, this paper adapts ANP methodology is adapted herein for the propose of identifying risks related to Cloud Computing due to its suitability in offering solutions in a complex multi-criteria decision environment since ANP uses a network without a need to specify levels in hierarchy. This study integrate the process of ANP comprises four major steps [35][36]. But we are not attempt to select the best alternatives in this study.

1) Step 1: Model construction and problem structuring.

The configuration decision problem needs to be stated clearly and structured into its important components. In this case, the relevant criteria is structured in the form of a control hierarchy where the higher the component level. A control hierarchy is simply a hierarchy of criteria and sub-criteria where priorities are derived with respect to the overall goal of the system being analyzed [35]. The highest elements are decomposed into sub-components and attributes. The model development will require the determination of attributes at each level and a definition of their relationships. The model can be obtained by seeking the opinions of the decision makers through brainstorming or other appropriate methods. In this study, the ultimate objective is to determine risks of Cloud Computing.

2) Step 2: Pairwise comparisons matrices between component levels

In this step, elicitation of the decision maker's priorities is completed. The decision maker is asked to respond to a series of pairwise comparisons. In ANP, like AHP, decision elements at each component are compared pairwise with respect to their importance for their control criterion, and the components themselves are also compared pairwise with respect to their contribution to the goal. In the case of interdependencies, components within the same level may be viewed as controlling components for each other, or levels may be interdependent on each other. We leave the interdependencies' evaluation until Step 3.

Saaty [36] has suggested a scale of 1 to 9 when comparing two components. A score of 1 represents the criteria have same importance or indifference where a score of 9 indicates complete dominance to the comparison criteria in a pairwise comparison matrix. If criteria have some level of weaker impact than its comparison criteria the range of the scores will be from 1 to 1/9, where 1 indicates indifference and 1/9 represents an extreme importance by one criterion (row component in the matrix) compared to the other criteria (column component in the matrix). Thus, the value a_{12} for=2, whereas a_{21}=1/2.When scoring is conducted for a pair, a reciprocal value is automatically assigned to the reverse comparison within the matrix. That is, a_{ij} is a matrix value assigned to the relationship of ith element to jth element, then denotes $a_{ij} = 1/a_{ji}$, Once all the pairwise comparisons are complete, the relative importance weight for each component is determined (these results are shown in Table 6 and Table 7). Given that A is the pairwise comparison matrix; the weights can be determined by expression (1).

$$A \bullet w = \lambda_{max} \qquad (1)$$

Where A is the matrix of pairwise comparison, w is the eigenvector or priority vector, and λ_{max} is the largest eigenvalue of A. Saaty [36] provides several algorithms for approximating w. In this study a two-stage algorithm to solve for the largest eigenvalue: the first one is the construction of the network (step 3), and the second one is the calculation of the priorities of the elements (step 4). In order to construct the structure of the problem, all of the interactions among the elements should be considered. This procedure is referred to as the process of averaging over normalized columns. The procedure may be algebraically represented as follows (Formula 2):

$$w_i = \frac{\sum_{i=1}^{I}\left(\frac{a_{ij}}{\sum_{j=1}^{J} a_{ij}}\right)}{I} \qquad (2)$$

where

w_i = the weighted priority for component i,

J = index number of columns (components),

I = index number of rows (components).

Given an initial determinant of risks control hierarchy network, pairwise comparisons need to be made between the applicable attributes within a given risks dimension cluster.

3) Step 3: Pairwise comparisons matrices of interdependencies

To reflect the interdependencies which occur in the network, pairwise comparisons need to be created among all the risk factors of Cloud Computing. We have not included the influence of risks on itself yet. When the elements of a component Y depend on another component X, represent this relation with an arrow from component X to Y. All of these relations are evaluated by pairwise comparisons and a super-matrix, which is a matrix of influence among the elements, is obtained by these priority vectors. The super-matrix is raised to limiting powers to calculate the overall priorities, and thus the cumulative influence of each element on every other element with which it interacts is obtained [37]. If self-controlling linkages are allowed, the graphical representation (which would show in Fig. 7 and Fig. 8) would be a loop from the controlling attribute to itself. The example question asked of the decision maker for evaluating the interdependencies is “When considering risks of Cloud Computing, with regards to increasing robustness, what is the relative impact of criteria A when compared to criteria B?” For example, “When considering risks of Cloud Computing, with regards to improving robustness, what is the relative impact of Hardware when compared to Legality?” For the criteria cluster, this procedure is repeated three times to account for all the applicable risk factors as shown in Fig. 4.

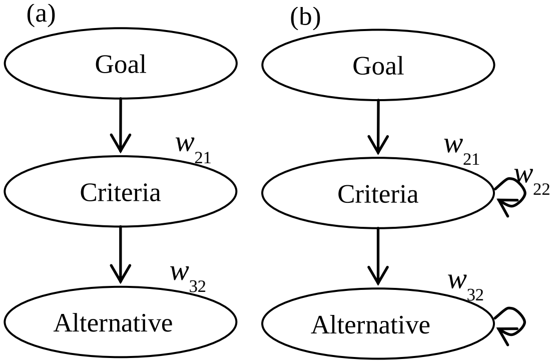

Figure 4. A hierarchy. (b) A nonlinear network.

To obtain global priorities in a system with interdependent influences, the local priority vectors are entered in the appropriate columns of a matrix known as a super-matrix. A super-matrix is actually a partitioned matrix, where each matrix segment represents a relationship between two nodes (components or clusters) in a system [36]. Let the components of a decision system be C_k, k = 1,2,3,…,n and let each component k have m_k elements, denoted by $e_{k1}, e_{k2}, \ldots, e_{kn}$.The local priority vectors obtained in Step 2 are grouped and located in appropriate positions in a super-matrix based on the flow of influence from a component to another component, or from a component to itself, as in the loop. A standard form of a super-matrix is shown in formula (3) [35].

$$W = \begin{array}{cc|ccccc} & & C_1 & \cdots & C_k & \cdots & C_n \\ & & e_{11}\cdots e_{1m_1} & \cdots & e_{k1}\cdots e_{km_k} & \cdots & e_{n1}\cdots e_{nm_n} \\ \hline C_1 & \begin{matrix} e_{11} \\ \vdots \\ e_{1m_1} \end{matrix} & \boldsymbol{w}_{11} & \cdots & \boldsymbol{w}_{1k} & \cdots & \boldsymbol{w}_{1n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ C_k & \begin{matrix} e_{k1} \\ \vdots \\ e_{km_k} \end{matrix} & \boldsymbol{w}_{k1} & \cdots & \boldsymbol{w}_{kk} & \cdots & \boldsymbol{w}_{kn} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ C_n & \begin{matrix} e_{n1} \\ \vdots \\ e_{nm_n} \end{matrix} & \boldsymbol{w}_{n1} & \cdots & \boldsymbol{w}_{nk} & \cdots & \boldsymbol{w}_{nn} \end{array} \qquad (3)$$

For example, the super-matrix representation of a hierarchy with three levels is as shown in Fig. 4(a) is as follows (Formula 4) [32]:

$$W_h = \begin{bmatrix} 0 & 0 & 0 \\ w_{21} & 0 & 0 \\ 0 & w_{32} & I \end{bmatrix} \qquad (4)$$

Where w_{21} is a vector that represents the impact of the goal on the criteria; w_{32} is a matrix that represents the impact of criteria on each of the alternatives; I is the identity matrix; and entries of zero correspond to those elements that have no influence. For the above example, if the criteria are interrelated among themselves, the hierarchy is replaced by a network, as shown in Fig. 4(b). The (2, 2) entry of w_n given by w_{22} would indicate the interdependency, and the super-matrix would be as follows (Formula 5):

$$W_n = \begin{bmatrix} 0 & 0 & 0 \\ w_{21} & w_{22} & 0 \\ 0 & w_{32} & I \end{bmatrix} \qquad (5)$$

Note that any zero in the super-matrix can be replaced by a matrix if there is an interrelationship of the elements in a component or between two components. Since there usually is interdependence among clusters in a network, the columns of a super-matrix usually sum to more than 1. The super-matrix must first be transformed to make it stochastic; that is, each column of the matrix sums to unity. An approach recommended by Saaty [34] is to determine the relative importance of the clusters in the super-matrix with the column cluster (block) as the controlling component [33]. That is, the row components with nonzero entries for their blocks in that column block are compared according to their impact on the component of that column block [32]. Through pairwise comparison of the row components with respect to the column component, an eigenvector can be obtained for each column block. For each column block, the first entry of the respective eigenvector is multiplied by all the elements in the first block of that column, the second by all the elements in the second block of that column, and so on. In this way, the block in each column of the super-matrix is weighted. The result is known as the weighted super-matrix, which is stochastic. Raising a matrix to powers gives the long-term relative influences of the elements on each other.

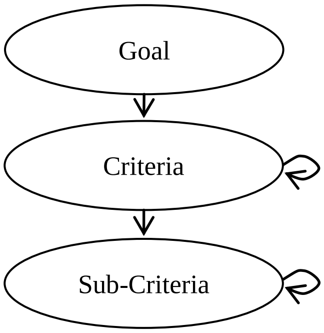

Figure 5. Network form for this paper.

To achieve convergence on the importance weights, the weighted super-matrix is raised to the power of 2*k*+ 1, where *k* is an arbitrarily large number. This new matrix, called the limit super-matrix [32], has the same form as the weighted super-matrix, but all the columns are the same. By normalizing each block of the super-matrix, the final priorities of all the elements in the matrix can be obtained. The network model of this study is described in Fig. 5.

B. Combine ANP Results with Risk Management Matrix

This study use ANP method that combines traditional technique of risks treatment and risk management matrix (Frequency/Severity matrix) to measure and understand the big picture of Cloud Computing related risks. First step, obtain relative weight of Cloud Computing risks' frequency and severity separately by running ANP method twice. Second step, put relative weight of risks' frequency and relative weight of risks' severity on the risk management matrix.

IV. Results

A. Result of Delphi method

The goal of the first Delphi study is to identify the risk factors for Cloud Computing. Delphi panelists were asked to justify their answers to interview questions and rate their level of agreement toward risk factors, ranging from strongly agree (SA) (5) to strongly disagree (SD) (1).

The interview protocol was developed based on the literature review. The interview explored more fully the perceptions of experts about the risk factors for Cloud Computing. These qualitative responses helped to elaborate the quantitative responses to the standardized questions, and qualitative themes were indicative of opinions raised by a large majority of the Delphi panelists.

Descriptive statistics of attitude toward each key factor at interview were showed as Table 1. In the final round (3rd round), 6 Delphi panelists strongly agreed that "Normal Wear and Tear or Malfunction", "Natural Disaster", "System Vulnerability", and "Social Engineering" are risk factors for Cloud Computing. Moreover 5 Delphi panelists strongly agreed that "Privacy", "Agreement or Contract", "Burglary", and "Cross-Cloud Compatibility" are risk factors for Cloud Computing. There were no undecided (UD) (3), disagree (D) (2) and strongly disagree (SD) (1) answers for key factor item at round 3.

TABLE 1: DESCRIPTIVE STATISTICS OF ATTITUDE TOWARD EACH KEY FACTOR AT INTERVIEW ROUND 2 AND ROUND 3

Key factors of risk	Attitude toward key factors of risk									
	SA		***A***		***UD***		***D***		***SD***	
	R2	***R3***	***R2***	***R3***	***R2***	***R3***	***R2***	***R3***	***R2***	***R3***
Agreement or Contract	5	5	1	1	0	0	0	0	0	0
Privacy	4	5	2	1	0	0	0	0	0	0
Jurisdiction	4	4	1	2	1	0	0	0	0	0
Burglary	4	5	2	1	0	0	0	0	0	0
Damaged or spoiled by employees result from intention or accidental	3	5	2	1	1	0	0	0	0	0
Natural Disaster	5	6	1	0	0	0	0	0	0	0
Normal Wear and Tear or Malfunction	4	6	1	0	1	0	0	0	0	0
System Vulnerability	5	6	0	0	1	0	0	0	0	0
Social Engineering	5	6	1	0	0	0	0	0	0	0
Mistakes are made by employees intentionally or accidentally	3	4	3	2	0	0	0	0	0	0
Cross-Cloud Compatibility	3	5	2	1	1	0	0	0	0	0

*Five Attitudes toward Necessary Competencies: Strongly Agree (SA), Agree (A) Undecided (UD), Disagree (D), and Strongly Disagree (SD).

TABLE 2: COMPARISON OF INTERVIEW ROUND 2 AND ROUND 3

Delphi Panelist Attitude toward Each Risk Factor Between R2 and R3	**Z**	**Sig.(2-tailed) (α=0.05)**
Agreement or Contract	0.000	1.000
Privacy	-1.000	0.317
Jurisdiction	-1.000	0.317
Burglary	-1.000	0.317
Damaged or spoiled by employees result from intention or accidental	-1.732	0.083
Natural Disaster	-1.000	0.317
Normal Wear and Tear or Malfunction	-1.342	0.180
System Vulnerability	-1.000	0.317
Social Engineering	-1.000	0.317
Mistakes are made by employees intentionally or accidentally	-1.000	0.317
Cross-Cloud Compatibility	-1.732	0.083

As stated in the methodology chapter, the issues of divergence and convergence of opinion are fundamental to a Delphi study. Based on the result of a Wilcoxon Signed Rank test, no significant attitude difference toward each key success factor was found between R2 and R3. Thus, the 10 items proposed by this study can be identified as risk factors for Cloud Computing.

TABLE 3: DESCRIPTIVE STATISTICS OF THE 3RD ROUND INTERVIEW

Risk Factor	N	Max	Min	Mean	Std. Dev.
Agreement or Contract	6	5	4	4.8	0.4
Privacy	6	5	4	4.8	0.4
Jurisdiction	6	5	4	4.7	0.5
Burglary	6	5	4	4.8	0.4
Damaged or spoiled by employees result from intention or accidental	6	5	4	4.8	0.4
Natural Disaster	6	5	5	5.0	0.0
Normal Wear and Tear or Malfunction	6	5	5	5.0	0.0
System Vulnerability	6	5	5	5.0	0.0
Social Engineering	6	5	5	5.0	0.0
Mistakes are made by employees intentionally or accidentally	6	5	4	4.7	0.5
Cross-Cloud Compatibility	6	5	4	4.8	0.4

As a result, according to Table 2 and 3, all items proposed by this study in first round of Delphi method can be identified as risk factors for Cloud Computing.

The goal of the second Delphi study was to develop an evaluation hierarchical structure for risks of Cloud Computing. Delphi panelists were asked to justify their answers to interview questions and rate their level of agreement toward hierarchical evaluation structure developed by this research (see Fig. 6). These qualitative responses helped to elaborate the quantitative responses to the standardized questions, and qualitative themes were indicative of opinions raised by a large majority of the Delphi panelists.

B. Result of ANP method

The ANP questionnaire was developed based on the result of the second Delphi study and distributed to 6 experts same as the panelists in Delphi studies. The following is general sub-Matrix notation for the risk analysis of Cloud Computing:

$$W= \begin{array}{r} \\ Goal(G) \\ Criteria(C) \\ Sub\text{-}criteria(S) \end{array} \begin{array}{c} \begin{array}{ccc} G & C & S \end{array} \\ \begin{bmatrix} 0 & 0 & 0 \\ w_{21} & w_{22} & 0 \\ 0 & w_{32} & w_{33} \end{bmatrix} \end{array}$$

This study asked experts to figure the relations among criterion as well as sub-criterion. Table 4 represents pairwise comparison and eigenvectors (e-Vector) of the criteria.

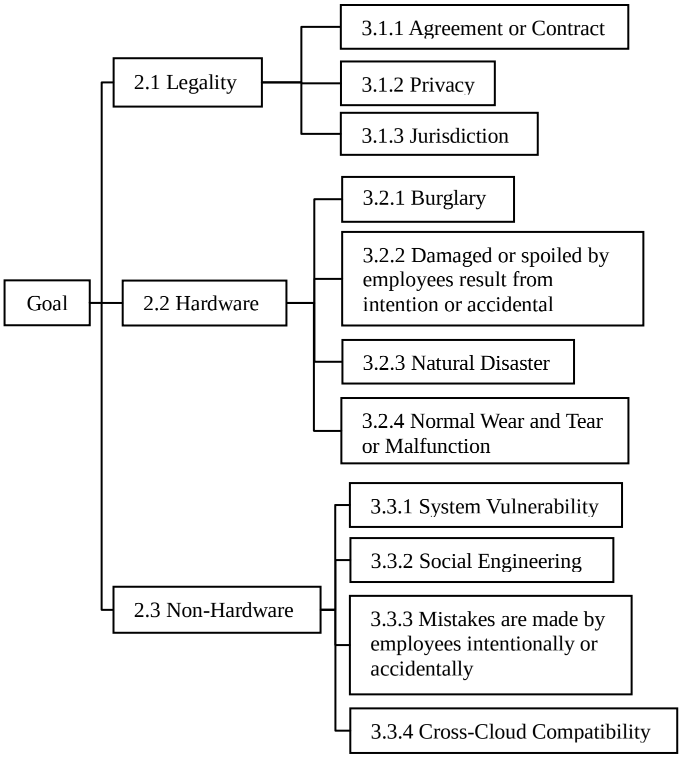
Goal
2.1 Legality
3.1.1 Agreement or Contract
3.1.2 Privacy
3.1.3 Jurisdiction
2.2 Hardware
3.2.1 Burglary
3.2.2 Damaged or spoiled by employees result from intention or accidental
3.2.3 Natural Disaster
3.2.4 Normal Wear and Tear or Malfunction
2.3 Non-Hardware
3.3.1 System Vulnerability
3.3.2 Social Engineering
3.3.3 Mistakes are made by employees intentionally or accidentally
3.3.4 Cross-Cloud Compatibility

Figure 6. Structure of criteria and sub-criteria.

TABLE 4: CRITERIA PAIRWISE COMPARISON MATRIX OF FREQUENCY OF RISK FACTORS

Goal	Legality	Hardware	Non-Hardware	Weights (e-Vector)
Legality	1	1/2	1/3	0.0938
Hardware	2	1	1/4	0.1666
Non-Hardware	3	4	1	0.7396

$$\text{Thus, in Frequency, } W_{21} = \begin{bmatrix} 0.0938 \\ 0.1666 \\ 0.7396 \end{bmatrix}$$

The respective of the three evaluative criteria in frequency (F) are “Legality” (F=0.0938), “Hardware” (F=0.1666) and “Non-Hardware” (F=0.7396). Then, same as criteria’s procedure, this study obtained sub-criteria’s e-Vector shown as table 5.

TABLE 5: PAIRWISE COMPARISON WEIGHTS (E-VECTOR) FOR SUB-CRITERIA

Sub-Criteria	Frequency
Agreement or Contract	0.4934
Privacy	0.3108
Jurisdiction	0.1958
Burglary	0.1936
Damaged or spoiled by employees result from intention or accidental	0.3564
Natural Disaster	0.1243
Normal Wear and Tear or Malfunction	0.3257
System Vulnerability	0.1906
Social Engineering	0.4182
Mistakes are made by employees intentionally or accidentally	0.1205
Cross -Cloud Compatibility	0.2707

The e-Vector for "Legality" ($W_{32\ (Column\ 1)}$), "Hardware" ($W_{32\ (Column\ 2)}$) and "Non-Hardware" ($W_{32\ (Column\ 3)}$) are organized into matrix W_{32}. W_{32} represents the relative importance of sub-criteria with respect to criteria in frequency and severity as follows:

$$\text{In frequency, } W_{32}= \begin{array}{c} \\ 3.1.1 \\ 3.1.2 \\ 3.1.3 \\ 3.2.1 \\ 3.2.2 \\ 3.2.3 \\ 3.2.4 \\ 3.3.1 \\ 3.3.2 \\ 3.3.3 \\ 3.3.4 \end{array} \begin{array}{c} \begin{array}{ccc} \text{Legality} & \text{Hardware} & \text{Non-Hardwa} \end{array} \\ \begin{bmatrix} 0.4934 & 0 & 0 \\ 0.3108 & 0 & 0 \\ 0.1958 & 0 & 0 \\ 0 & 0.1936 & 0 \\ 0 & 0.3564 & 0 \\ 0 & 0.1243 & 0 \\ 0 & 0.3257 & 0 \\ 0 & 0 & 0.1906 \\ 0 & 0 & 0.4182 \\ 0 & 0 & 0.1205 \\ 0 & 0 & 0.2707 \end{bmatrix} \end{array}$$

The inner dependence network maps of criteria and sub-criteria were illustrated by experts as follows. (see Fig. 7 and Fig. 8)

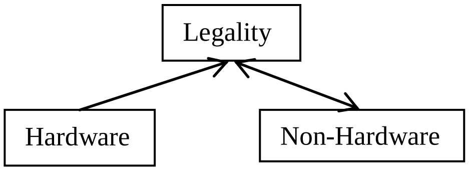

Figure 7. Inner dependence among criteria.

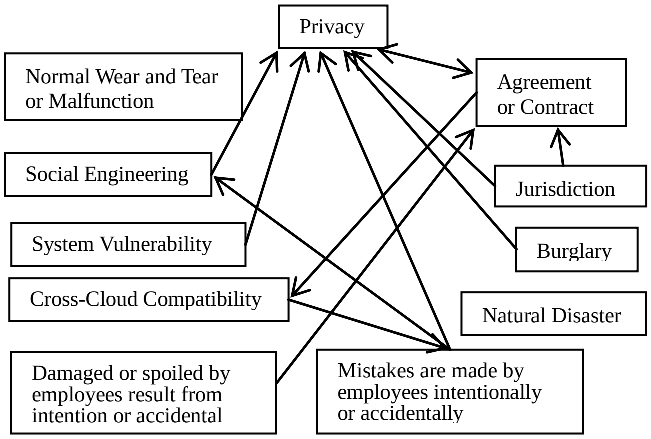
Privacy
Normal Wear and Tear or Malfunction
Agreement or Contract
Social Engineering
Jurisdiction
System Vulnerability
Burglary
Cross-Cloud Compatibility
Natural Disaster
Damaged or spoiled by employees result from intention or accidental
Mistakes are made by employees intentionally or accidentally

Figure 8. Inner dependence among sub-criteria.

After data collection, the weights of risks of Cloud Computing were obtained by ANP. According to the results on Table 6, the highest weight of the criteria, both frequency (F) and severity (S), is "Non-Hardware" (Weight: F=0.60355, S=0.53099). The 2nd is "Legality" (Weight: F=0.25, S=0.40702) and the least important criteria is "Hardware" (Weight: F=0.14645, S=0.06199). Among the criteria of "Legality", "Hardware" and "Non-Hardware", the most important sub-criterion of frequency are: 1st "Cross-Cloud Compatibility" (Weight=0.24803), 2nd "Social Engineering" (Weight=0.17236), 3rd "Mistakes are made by employees intentionally or accidentally" (Weight=0.14337) respectively. The least important sub-criterion of frequency are "Natural Disaster" (Weight=0.01007, Rank=11th), 10th is "Normal Wear and Tear or Malfunction" (Weight=0.0264) and 9th is "Burglary" (Weight=0.04295). Moreover, the most important sub-criterion of severity are "Cross-Cloud Compatibility" (Weight=0.25841), "Mistakes are made by employees intentionally or accidentally" (Weight=0.19201) and "Social Engineering" (Weight=0.09754). The lowest sub-criterion of severity are "Normal Wear and Tear or Malfunction" (Weight=0.00405, Rank=11th), 10th is "Natural Disaster" (Weight=0.01246) and 9th is "Burglary" (Weight=0.03061). (see table 7).

TABLE 6: CRITERION'S RELATIVE WEIGHT OF FREQUENCY AND SEVERITY

Criteria	Frequency (Rank)	Severity (Rank)
2.1 Legality	0.25 (2)	0.40702 (2)
2.2Hardware	0.14645 (3)	0.06199 (3)
2.3 Non-Hardware	0.60355 (1)	0.53099 (1)
Geometric mean	**0.280617152**	**0.237505995**

TABLE 7: SUB-CRITERION'S RELATIVE WEIGHT OF FREQUENCY AND SEVERITY

Sub-Criteria	Frequency (Rank)	Severity (Rank)
3.1.1 Agreement or Contract	0.06947 (7)	0.07497 (7)
3.1.2 Privacy	0.07854 (4)	0.09689 (4)
3.1.3 Jurisdiction	0.06377 (8)	0.09575 (5)
3.2.1 Burglary	0.04295 (9)	0.03061 (9)
3.2.2 Damaged or spoiled by employees result from intention or accidental	0.0723 (6)	0.04421 (8)
3.2.3 Natural Disaster	0.01007 (11)	0.01246 (10)
3.2.4 Normal Wear and Tear or Malfunction	0.0264 (10)	0.00405 (11)
3.3.1 System Vulnerability	0.07274 (5)	0.09311 (6)
3.3.2 Social Engineering	0.17236 (2)	0.09754 (3)
3.3.3 Mistakes are made by employees intentionally or accidentally	0.14337 (3)	0.19201 (2)
Geometric mean	**0.067289379**	**0.057189441**

V. RESULT OF RISK MANAGEMENT

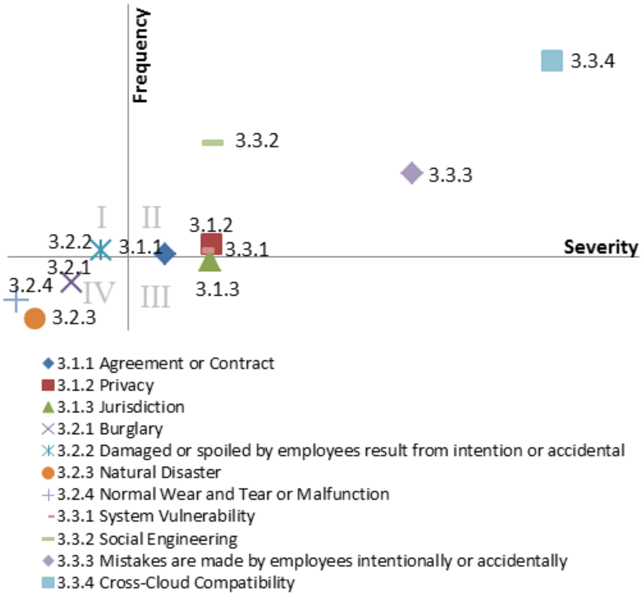

Figure 9. Sub-Criteria Risk Management Matrix

Fig. 9 represents a risk management matrix that illustrates a clear priority of risk management. In Fig. 9, the highest frequency of risk among all the eleven risks is "Cross-Cloud Compatibility" (3.3.4), the second highest frequency is "Social Engineering" (3.3.2), while the third one is "Mistakes are made by employees intentionally or accidentally" (3.3.3). In addition to the above-mentioned risks, "Privacy" (3.1.2), "System Vulnerability" (3.3.1), "Damaged or spoiled by employees result from intention or accidental" (3.2.2) and "agreement or Contract" (3.1.1) are merely greater than the geometric mean. The frequencies of the rest four risks are below geometric mean .From the aspect of severity, however, the sequence of the top three risks is contrary to that of frequency. The top severity is "Cross-Cloud Compatibility" (3.3.4), followed by "Mistakes are made by employees intentionally or accidentally" (3.3.3), then "Social Engineering" (3.3.2). As a result, "agreement or Contract" (3.1.1), "Privacy" (3.1.2), "System Vulnerability" (3.3.1), "Social Engineering" (3.3.2), "Mistakes are made by employees intentionally or accidentally" (3.3.3) and "Cross-Cloud Compatibility" (3.3.4) all fall within quadrant II. It is noteworthy that the severity of "Mistakes are made by employees intentionally or accidentally" (3.3.3) following "Cross-Cloud Compatibility" (3.3.4) by a very insignificant difference. Additionally, risks such as "System Vulnerability" (3.3.1), "Privacy" (3.1.2), "Damaged or spoiled by employees result from intention or accidental" (3.2.2) are all above geometric mean, but only "Damaged or spoiled by employees result from intention or accidental" (3.2.2) in quadrant II. Thus, "Jurisdiction" (3.1.3) fall within quadrant III. "Natural Disaster" (3.2.3), "Burglary" (3.2.1) and "Normal wear and tear or Malfunction" (3.2.4) represent relatively low risks on severity and frequency that lie on quadrant IV.

VI. CONCLUSION AND MANAGEMENT IMPLICATION

The major contribution of this paper lies in the identification and verification of Cloud Computing services' risk factors in which no research has ever been conducted before. ANP method is capable of solving complicated problems. Implementation of ANP method enables decision-makers to visualize the impact of various criteria in the final result as well as measure the severity and frequency of risk of Cloud Computing services. Apply ANP method to evaluate relative weight separately. Then put weight into risk management matrix, a general technique for measuring risk, and proceed to prioritize risks.

As the results of risk management matrix illustrated in Fig. 9 that seven of the criteria, "Agreement or Contract", "Privacy", "System Vulnerability", "Social Engineering", "Mistakes are made by employees intentionally or accidentally" and "Cross-Cloud Compatibility", located in the quadrant II needs to be handled with extra caution. Generally speaking, it is recommended to avoid the risk located in quadrant II. However, neither Cloud Computing users nor providers can escape risk such as "Cross-Cloud Compatibility" or "Social Engineering" in Fig. 9. In this situation, one may try to lower its frequency (which means loss prevention) so that it can be handled by insurance or transfer. This study suggests companies who plan to apply Cloud Computing technique or Cloud Computing service provider treat risk that falls within quadrant II as their first priority. Same reason, criterion in quadrant I, like "Damaged or spoiled by employees result from intention or accidental", requires extra caution as well to prevent loss. But it should be prioritized after quadrant II. Generally, risks in quadrant III can be covered by insurance or transfer, because risks in quadrant III occur higher loss than frequency. Likewise, the same coverage applies to the risk in quadrant III identified in this study (namely "Jurisdiction"). In term of quadrant IV, it is supposed to be the least priority that does not even deserve further processing. All that we need to do is monitor and trace the risk in quadrant IV then respond to any frequency and severity changing/unchanging. This study also found interesting implication that people who work in the information field tend to underestimate some risks. For example, this questionnaire shows that most experts outweighed "Legality" over "Privacy" and "Jurisdiction".

Furthermore, “Privacy” becomes the most severe and frequent risk among all risks in questionnaire. However, after adjust weight of criterion by ANP method base on connections drew in the questionnaire, the consequence reflects differently: “Privacy” becomes minor and “Cross-Cloud compatibility” becomes more important. That is the contribution of this study and also the reason why this study applies ANP method.

This study suggests further researches that focus on specific field or industry such as bank applying Cloud Computing service or insurance company applying Cloud Computing service, to acquire more certain, practical and clearer result.

REFERENCES

[1] Ashford, W. (2009), Cloud computing more secure than traditional IT, says Google. Computer Weekly. Retrieved on Sep. 13, 2011 from http://www.computerweekly.com/Articles/2009/07/21/236982/cloud-computing-more-secure-than-traditional-it-says.htm

[2] Hand, J. D. (2007), Principles of Data Mining, Adis Data Information BV.

[3] Paquette, S.; Jaeger, P. T. and Wilson, S. C. (2010), Identifying the security risks associated with governmental use of Cloud Computing, Government Information Quarterly 27 , p.p. 245-53.

[4] Buyya R. and Parashar M. (2010), User requirements for cloud computing architecture, Proc. 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing, Melbourne, Australia, 17-20 May 2010, p.p. 625-30.

[5] Sultan, N. (2011), Reaching for the “cloud”: How SMEs can manage, International Journal of Information Management, 31, p.p.272-8

[6] Stinchcombe, N. (2009), Cloud computing in the spotlight, Retrieved on Nov. 8, 2011 from http://www.infosecurity-magazine.com/view/4755/cloud-computing-in-the-spotlight/

[7] Chow, R.; Golle, P.; Jakobsson, M.; Masuoka, R.; Molina, J.; Shi, E. and Staddon, J. (2009), Controlling data in the Cloud: Outsourcing computation without outsourcing control, CCSW’09, November 13, 2009.

[8] Leavitt, N. (2009), Is Cloud Computing really ready for prime time? Computer, 42(1),p.p.15–20.

[9] Naughton, J. (2009), There's a silver lining to Google's Cloud Computing glitch, Retrieved on Aug. 15, 2011 from http://www.guardian.co.uk/technology/2009/mar/01/gmail-outage-cloud-computing

[10] Svantesson, D. and Clarke, R. (2010), Privacy and consumer risks in Cloud Computing, Computer Law & Security Review, 26, p.p. 391-7.

[11] Knorr, E. and Gruman, G. (2011), What cloud computing really means. Retrieved on Dec. 5, 2011 from http://www.infoworld.com/d/cloud-computing/wht-cloud-computing-really-means-031

[12] Ward, B. T. and Sipior, J. C. (2010), The internet jurisdiction risk of cloud computing, Information Systems Management, 27, p.p. 334-9.

[13] Tisnovsky, R. (2010), Risk versus value in outsourced Cloud computing, Financial Executive, November, p.p. 64-5.

[14] Subashini, S. and Kavitha, V. (2011), A survey on security issues in service delivery models of Cloud computing, Journal of Network and Computer Applications, 34, p.p. 1-11.

[15] Zissis, D. and Lekkas, D. (2011), Addressing cloud computing security issues, Future Generation Computer Systems, 28, p.p. 583-92.

[16] Tarzey, B. (2011), The cloud and the channel, Retrieved on Oct. 5, 2011 from http://www.quocirca.com/media/presentations/032011/572/Quo%20-%20cloud%20for%20CL%20-%20March%204th%202011%20V3.pdf

[17] Lackermair, G. (2010), Hybrid cloud architectures for the online commerce, Procedia Computer Science, 3, p.p.550-5.

[18] Marshall, M. I., & Alexander, C. (2006), Using a contingency plan to combat human resource risk, Journal of Extension , 44(2) Article 2IAW 1. Retrieved on Sep. 22, 2011 from

http://www.joe.org/joe/2006april/iw1.shtml

[19] Federal Aviation Administration (2009), Risk Management Handbook, Retrieved on Dec. 3, 2011 from http://www.faa.gov/library/manuals/aviation/media/FAA-H-8083-2.pdf

[20] GAIA R&D Limited (2010), Project Governance Seminars Workshops & Training, Retrieved on Dec. 20, 2011 from http://www.gaiainvent.com/services.html

[21] Awati, K. (2009), Cox’s risk matrix theorem and its implications for project risk management. Retrieved on Dec 18, 2011 from http://eight2late.wordpress.com/2009/07/01/cox%E2%80%99s-risk-matrix-theorem-and-its-implications-for-project-risk-management/

[22] Sinha, P. R.; Malzahn, D. and Whitman, L. E. (2004), Methodology to mitigate supplier risk in an aerospace supply china, Supply Chain Management: An International Journal, 9 (2), p.p. 154-68.

[23] Mac Crimmon K. R. and Wehrung, D. A. (1986), Taking risks: The management of uncertainty, Free Press, New York.

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

[25] Cox, L. A. (2008), What’s wrong with risk Matrices? Risk Analysis, 28(2), p.p.497-515.

[26] Lim, S.H. (2011), Risks in the north korean special economic zone: Context, identification, and assessment, Emerging Markets Finance & Trade, 47(1), p.p.50-66.

[27] Picado, F.; Barmen, G.; Bengtsson, G. Cuadra, S.; Jakobsson, K.; and Mendoza, A. (2010), Ecological, Groundwater, and Human Health risk assessment in a mining region of nicaragua, Risk Analysis: An International Journal, 30(6), p.p.916-33.

[28] Pintar, K. D. M.; Charron, D. F.;Fazil, A.; McEwen, S. A.; Pollari, F.; Waltner-Toews, D. (2010), 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, Jan2010, 30(1), p.p.49-64.

[29] Aven, T. and Renn, O. (2009), 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), p.p.587-600.

[30] Casale, J. (2010), Social networking, cloud computing bring new risk exposures, Business Insurance, 9/27/2010, 44(38), p.17.

[31] Bublitz, E. (2010),Catching the Cloud: Managing risk when utilizing Cloud Computing, National Underwriter Property & Casualty November 8, 2010, p.12, p.13, p.16 .

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

[33] Armburst, M.; Fox, A.; Griffith, R.; Joseph, A. D.; Katz, R. and Konwinski, A. et al. (2009), Above the clouds: a Berkley view of Cloud Computing. Retrieved on Dec. 5, 2011 from http://radlab.cs.berkekey.edu/

[34] Saaty T. L. (1996), Decision making with dependence and feedback: The analytic network process, RWS Publications, Pittsburgh.

[35] Meade, L. M. and Sarkis, J. (1999), Analyzing organizational project alternatives for agile manufacturing processes-An analytical network approach, International J. Prod. Res., 37(2), p.p.241-61.

[36] Saaty T. L. (1980), The Analytic Hierarchy Process, McGraw Hill Publications.

[37] Saaty, T. L. and Vargas, L. G. (1998), Diagnosis with dependent symptoms: Bayes theorem and the analytic hierarchy process. Operations Research, 46(4), p.p.491–502.