International Journal of Knowledge and Systems Science
Volume 7 • Issue 3 • July-September 2016

AHP-Driven Knowledge Leakage Risk Assessment Model: A Construct-Apply-Control Cycle Approach

Haley Wing Chi Tsang, Knowledge Management and Innovation Research Centre, The Hong Kong Polytechnic University, Hong Kong

Wing Bun Lee, Knowledge Management and Innovation Research Centre, The Hong Kong Polytechnic University, Hong Kong

Eric Tsui, Knowledge Management and Innovation Research Centre, The Hong Kong Polytechnic University, Hong Kong

ABSTRACT

Intellectual Capital (IC) is becoming more widely understood by the academic and business communities, especially its important role in value creation of an organization. However, few people are aware that IC, if not managed properly, may also pose threats, sometime serious, to an organization. Knowledge leakage from an organization, for example, may come about when an experienced employee leaves for another job. Knowledge leakage is pervasive throughout an organization but is seldom noticed until the consequence is felt. This intellectual capital risk has to be systematically and effectively identified, assessed and controlled in the whole value chain of an organization. An AHP (Analytic Hierarchy Process) based multi-dimensional decision making and assessment model is developed to determine knowledge leakage risk in an organization.

KEYWORDS

Analytical Hierarchy Process, Intellectual Capital Risk Management, Intellectual Capital Risk, Intellectual Capital, Knowledge Assets, Knowledge Loss, Knowledge Management, Risk Assessment

INTRODUCTION

In the globalized knowledge-intensive, technology-driven economy, the importance of knowledge to any sector in society or business has never been so critical. Intellectual capital (IC), a term often used interchangeably with knowledge assets, refers to the knowledge, skills and experiences of employees, and the knowledge embedded in business processes, management practice, company culture, client relationships etc. of an organization. Edvinsson (1997) stated that IC was knowledge that could be transformed into values (products or services) to generate revenues for an organization. For a long time since the term was coined, IC has been classified into three categories: human capital, structural capital and relational capital (Edvinsson & Kivikas, 2007). IC has also received growing attention by the public and business people, and a fair amount of research efforts by academics. The focus up to now has been on the value creation side of IC. This is expected. However, the downside of IC, or IC risks, is not on the radar of many professionals, including researchers, despite its potential disastrous impact on an organization in some instances of IC risks occurring in real life. IC risks include, for example, employee turnover (experienced staff leaving the organization) (Harvey & Lusch, 1999; Parise, Cross, & Davenport, 2006) and reputation damage (product safety has serious problems) (Harvey & Lusch, 1999).

DOI: 10.4018/IJKSS.2016070101

Among the typical IC risks in an organizations, knowledge leakage risk is by far one of the most pervasive and it can occur in different business functions or processes. By definition, knowledge leakage refers to the loss of knowledge to a third party which is owned by and resident in an organization for internal use only (Frishammar, Ericsson, & Patel, 2015). Knowledge leakage can take many forms and bring many disadvantages to an organization. For example, an organization may have developed a very effective sales/marketing software to streamline the sales process and reporting which is of great help in increasing the productivity of sales staff. If the design of the software is leaked to a competitor, the 'secret' of success may be replicated in a short time in the competitor's systems to enable it to enjoy the same benefits offered by the software. The organization's competitive advantage may be seriously affected, making the resulting costs of knowledge leakage quite obvious (DeLong, 2004). This example showed that the downside of knowledge leakage can threaten the survival of even a large corporation, but research in this type of common IC risk is still insignificant (Parker, 2012). In an attempt to fill this research gap, this study proposes a knowledge leakage assessment model driven by the Analytic Hierarchy Process (AHP). In the following sections, the building components of the model, methodology, benefits and examples of applying the model in the business world are discussed.

RISK ASSESSMENT AND ANALYTICAL HIERARCHY PROCESS

In enterprise risk management, there are a number of frameworks in use today and COSO (Committee of Sponsoring Organizations of the Treadway Commission) (Curtis & Carey, 2012) is the most widely adopted by organizations. Typically, risk management involves identifying, prioritizing, responding to, assessing, monitoring and reporting risks. The risks may include physical risks like fire and earthquake and financial risks like interest rate instability and payment default. However, there is also an important category of risks not specifically addressed by these common frameworks but related to IC of organizations which must be effectively managed to ensure competitiveness and sustainability. These risks, arising from IC not properly managed, are called IC risks. Examples are: knowledge leakage, intellectual property (IP) loss and employee turnover. In this paper, the focus is on risk assessment component of a framework as applied to one of the most important IC risks - knowledge leakage. As for risk assessment, it refers to activities carried out in establishing assessment criteria and scope, determining likelihood and impact of risks, and prioritizing them (Hallikas, Karvonen, Pulkkinen, Virolainen, &Tuominen, 2004). Common frameworks like COSO (Curtis & Carey, 2012) and CAS (Casualty Actuarial Society) (Casualty Actuarial Society, 2013) have similar risk assessment methodology. The determination of the level of risk is important in risk management, including IC risk management. According to Zhi (1995) and Williams (1993), risk is expressed mathematically as:

$$R = P \times I$$

where R is the level of risk, P is the probability for the risk to occur and I is the impact of the risk.

In the usual risk management of an organization, the management process consists of a number of sequential steps: identification, prioritization, aversion, mitigation, assessment, monitoring, reporting and review (Hallikas, Karvonen, Pulkkinen, Virolainen, & Tuominen, 2004). In this study, the focus is on the assessment step which is roughly at the middle of the process. In this step, the performance of the preceding steps is measured. The assessment results then become input to the following steps which depend on such inputs and other information to achieve the objectives of monitoring and review, for example. Therefore, a study of risk assessment will yield a high ROI (Return on Investment) and improve the whole risk management process significantly. However, the assessment of IC risks has been mainly qualitative and done on individual risks often in isolation from each other. What is lacking is unified empirical assessment not only at individual risk level but also at functional and organizational levels to obtain better overall management. To fill this gap, the current study will deal with the organization-wide empirical assessment of IC risks. Thus a common IC risk, knowledge leakage, which can occur in many functions, departments or projects, is chosen for the study. To carry out the empirical assessment of an IC risk with an organization-wide characteristic, Analytic Hierarchy Process (AHP) was selected. The suitability of AHP in this project would be explained as follows. The chosen knowledge leakage risk has many kinds and can occur in different functions at different management levels and their relationships would best be described by a hierarchy, as explained in the later section on knowledge leakage hierarchy construction. Since AHP is hierarchy-based, both are compatible and AHP can be applied to this hierarchy to assess risks.

In practice, AHP starts first with the construction of a hierarchy of criteria relevant to the context of the decision to be made. In this project, the criteria became the different kinds of knowledge leakage risks, the context was the knowledge leakage situation in an organization and the decision making was about finding the relative risk impacts. Then pair-wise comparison of two criteria in terms of relative importance is done before an algorithm is deployed to determine the weighting of each criterion (Partovi, Burton, & Banerjee, 1990). The weightings calculated make AHP especially useful in multi-criteria decision making and are thus similarly used in the assessment of knowledge leakage risks hierarchy, as shown in the sections below.

Going back in history, AHP was a process developed by Saaty (1977) for multi-criteria decision making. It was used for prioritization of tasks or allocation of resources (Saaty, 2008). Since then, AHP has been applied in various business areas, for example, in risk assessment, project risk assessment (Mustafa & Al-Bahar, 1991) and overseas construction project risk assessment (Zhi, 1995). Scholars have also used AHP to weigh the knowledge assets of a company (Carlucci & Schiuma, 2007); to select the best set of knowledge management (KM) tools (Grimaldi & Rippa, 2011); to evaluate KM strategies (Wu & Lee, 2007) and to explore KM enablers (Jandaghi, Jandaghi, Irani, Mousavi, & Davoodavabi, 2014). Other industries include supplier selection (Handfield, Walton, Sroufe, & Melnyk, 2002), weapon system evaluation (Cheng & Mon, 1994) and site selection (Saaty, 2008). Finally, organization examples are: Department of Defence in the U.S., British Airways and Federal Financial Institutions Examination Council (Saaty, 2008). The great number of varied applications of AHP since its inception shows that it is a strong, proven analytic tool with a wide range of usability. The AHP in knowledge leakage risk assessment represents only one of the recent novel research efforts.

KNOWLEDGE LEAKAGE RISK HIERARCHY

In any organization, knowledge is embedded in employees, business processes, systems, databases, marketing campaigns, design documents, patents, products, services and so on. During normal business activities, knowledge, sensitive or insensitive, public or confidential, is used to carry out daily tasks. It is probable that some or significant portion of the knowledge, intended for internal use only, may be exposed to external parties because of errors unintentionally or business necessities unavoidably (Ahmad, Bosua, & Scheepers, 2014). The worst happens when highly sensitive proprietary knowledge is in the hands of competitors or parties hostile to the organizations, causing potentially great damage like loss of competitive advantage (Frishammar et al., 2015). The above incidents are knowledge leakage and the undesirable effects are referred to as the negative side of knowledge leakage. On the other hand, there is the opposite side to knowledge leakage too. When knowledge is intentionally leaked or lost to selected outside parties beyond information sharing or business collaboration needs to achieve something advantageous to the organization, for example, better collaboration or business relationship, such benefits are known as the positive side of knowledge leakage (Jiang, Li, Gao, Bao, & Jiang, 2013; Mohamed et al., 2007). Normally, in the course of business, knowledge leakage is predominantly negative. Therefore, though both the positive and negative sides of knowledge leakage are under-researched (Mohamed et al., 2007), much more attention to the latter side is required (Frishammar et al., 2015) and the present study belongs to the latter.

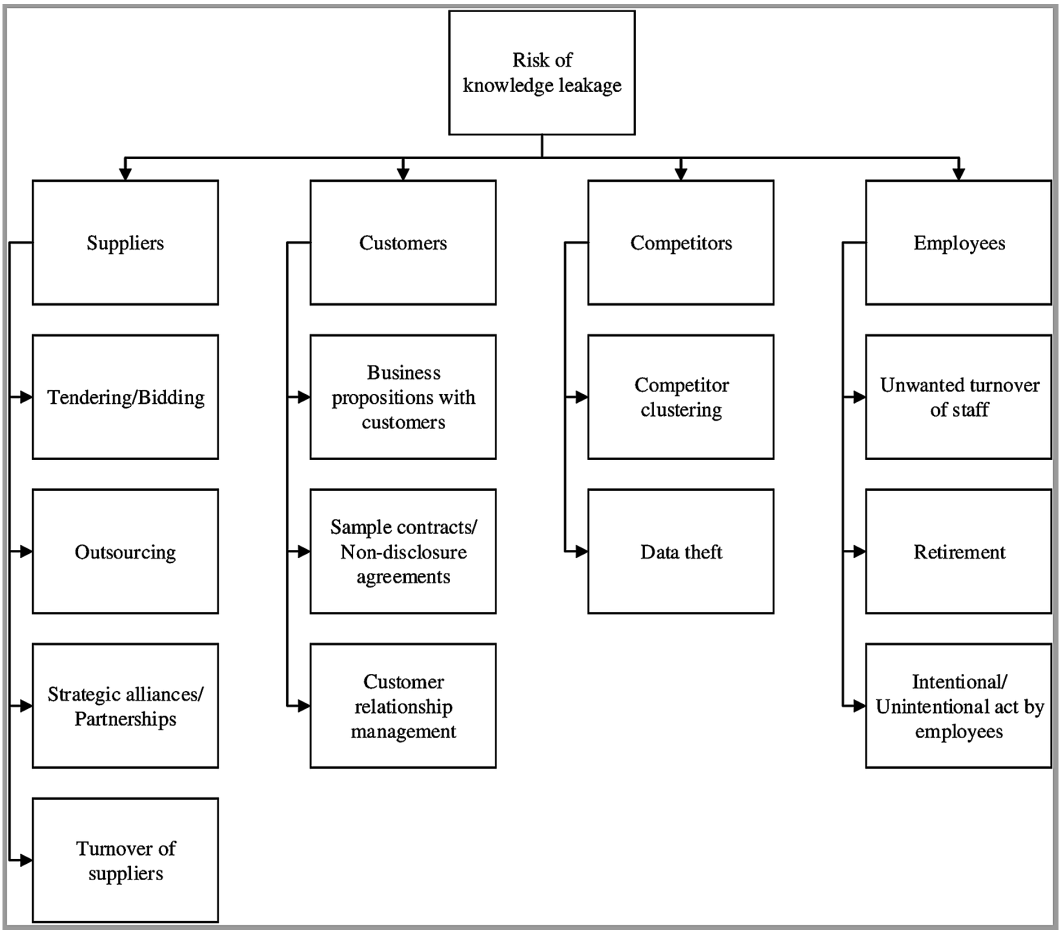
In nature, knowledge leakage risks have characteristics distinct from other common enterprise risks. Knowledge leakage can occur at any time in any place in an organization. Business processes, product designs and trade secrets may suffer from knowledge leakage from time to time. It is the pervasiveness of knowledge leakage which makes it different from other common risks such as stock price risks, payment default risks and country risks, which may be dealt with by some specific departments only. Knowledge leakage risks, because they can occur in many different functions, are rather being addressed by employees in many departments or groups. Then within a department, for example, marketing, there are also different kinds of knowledge leakage in areas like product sales data, promotional strategies, major customers list and pricing strategies. Going further, another sub-departmental level of knowledge leakage is possible. Considering the situation as a whole, a hierarchy becomes a natural choice to depict their relationships. Furthermore, as there are many properties common to different kinds of knowledge leakage, a multi-level hierarchy and its sub-hierarchies help group similar knowledge leakage risks together for more uniform and effective risk management at different levels of the hierarchy. It also follows that risk assessment can be done at different levels, depending on the needs.

In the proposed model, a similar knowledge leakage hierarchy of an organization is used in the risk assessment. To do this, a simple hierarchy is constructed first by making use of the key knowledge leakage drivers and a subset of sub-drivers extracted from the corresponding full set of a larger scope appeared in a study by Mohamed et al. (2007). The purpose is to illustrate some of the steps, factors and considerations involved in the construction process and therefore, only general business and risk knowledge of a typical organization of today is used here to arrive at several common sub-drivers examples for each key driver. This hierarchy is also developed to illustrate how AHP can be applied in the assessment of knowledge leakage as in the later sections. The description and explanation is not intended to modify or replace any of the original arguments presented. In practice, the key staff of the organization will take part in the process as well. It details the factors and considerations involved in building this three-level hierarchy. The top level is the ‘Risk of knowledge leakage’ with four children (key drivers) at the level below being respectively ‘Suppliers’, ‘Customers’, ‘Competitors’ and ‘Employees’, from left to right in the figure. Each has several sub-drivers at the next lower level (third level). Refer to Figure 1 for all the elements of the hierarchy.

The ‘Supplier’ key driver is at the leftmost of the second level. In any business, suppliers of products or services are essential. However, during the course of conducting business transactions with them, knowledge leakage can happen. For example, in the purchase or tendering process, an organization provides specifications for products/services to be purchased from suppliers, which at least indirectly lets the suppliers know some part of the future sales plan or future products in design/manufacture, when such information is generally regarded as trade secrets. In another instance, the organization may outsource internal IT services to an outsourcing provider, and the risk of leakage of sensitive business information to suppliers is high and must be managed properly. In an organization which relies on an excellent supply chain to produce products, it has excellent relationships with suppliers, and if necessary, may transfer proprietary knowledge/skills to them so that their product/services can meet the requirements of the supply chain. These suppliers effectively become business partners. However, this situation makes the relationship with them riskier than with ordinary suppliers because more specialized proprietary knowledge is released to a third party who may pass it to the organization’s competitors especially when these suppliers cease doing business with the organization and turn to its competitors instead. The stakes are high with such supplier partnerships for the organization. The four sources of knowledge leakage identified become four sub-drivers of the key driver ‘Supplier’: ‘Tendering/Bidding’, ‘Outsourcing’, ‘Strategic alliances/Partnerships’ and ‘Turnover of suppliers’.

The second key driver is ‘Customers’. Customers, a critically important asset of an organization, can be a driver for knowledge leakage. During the sales process, presentations and proposals are made to sell proposed solutions to a potential/existing customer business problem. These proposed solutions are the output of applying the knowledge of the organization to a sales situation and might be leaked. The potential/existing customers may take the ideas in the proposed solution and develop them further for their own purposes. Similar kinds of leakage occur in sample contracts or non-

Figure 1. The knowledge leakage risk hierarchy adapted from Mohamed et al. (2007)


Risk of knowledge leakage
Suppliers
Customers
Competitors
Employees
Tendering/Bidding
Outsourcing
Strategic alliances/ Partnerships
Turnover of suppliers
Business propositions with customers
Sample contracts/ Non-disclosure agreements
Customer relationship management
Competitor clustering
Data theft
Unwanted turnover of staff
Retirement
Intentional/ Unintentional act by employees

disclosure agreements. At another sales step, customer relationship building, a sales manager may reluctantly or unintentionally disclose some sensitive business information to a customer when being asked in order to make the customer satisfied. In light of these considerations, four sub-drivers under ‘Customer’ are identified: ‘Business propositions with customers’, ‘Sample contracts/non-disclosure agreements’ and ‘Customer relationship management’.Besides ‘Customers’, ‘Competitors’ can become a key driver of knowledge leakage as well. It is very common in many industries for participants in the same industry, who are competitors, to attend trade shows, exhibitions, seminars, workshops, meetings or conferences together. During these occasions, they share news, trends and developments or exchange information. If participants do not take sufficient precautionary measures, it is easy for them to disclose unintentionally some confidential company business information to other participants who are competitors, and will take advantage of this unintentional knowledge leakage. At other times, there are people who are very knowledgeable in computer security and attempt to access the database of their competitors to gain unauthorized copy of trade secret information. These considerations give rise to two sub-drivers for ‘Competitors’: ‘Competitor clustering’ and ‘Data theft.’

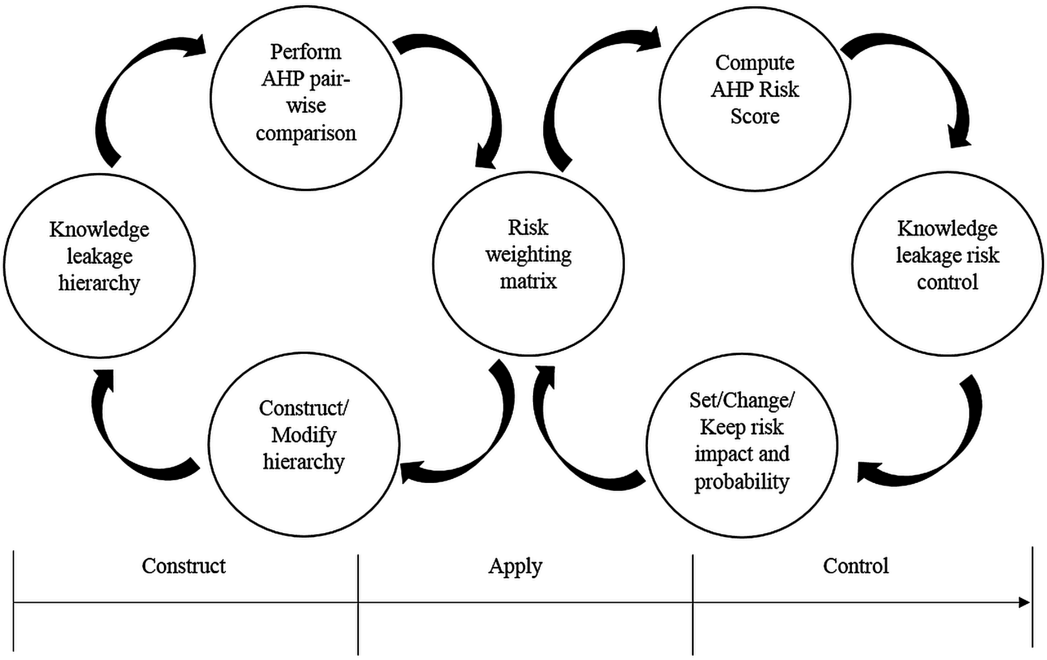
The last key driver of knowledge leakage is ‘Employees’. People are regarded as the most important asset in an organization because any successful running of a business depends greatly on the knowledge, skills and experience of its employees. Therefore, if employees leave an organization, very often this also means loss of knowledge as far as the organization is concerned. An organization would try to minimise the loss of key staff and their associated knowledge to avoid the undesirable effects on the organization's daily operation and growth. At the same time, an organization must get prepared for the retirement of staff so that the knowledge and skills of retired staff can be transferred to other employees in a timely and orderly manner. In other situations, some employee may leak company information to people outside the organization unintentionally or by mistake, or intentionally for benefits, because of dissatisfaction with the organization or other factors. Proper employee training in data security measures and ethics may reduce such knowledge leakage. What have been considered leads to three sub-drivers identified for 'Employees': 'Unwanted turnover', 'Retirement' and 'Intentional/unintentional act by employees'.

KNOWLEDGE LEAKAGE RISK ASSESSMENT MODEL

In the model proposed in this paper, AHP plays two important roles. The first role is to make use of AHP algorithms to create the weighting matrix for a given hierarchy. The second is to multiply the matrix with necessary risk impact and probability data from real-life risk practice to obtain the risk score, which reflects the result of the current risk controls adopted. Therefore, there are two cycles in the model as shown in Figure 2, corresponding to the two roles.

In the first cycle, shown on the left in the figure, is the sub-cycle and is known as the hierarchy cycle. The knowledge leakage hierarchy is constructed according to the current business context. Then pair-wise comparison is performed for each pair of risks in the hierarchy according to AHP, producing the weighting matrix for all the concerned risks. Usually the hierarchy and pair-wise comparison remain stable over a relatively long period of time. However, if the business context changes in the future, the hierarchy is updated or the pair-wise comparisons are done all over again to produce an updated weighting matrix for use in AHP. Therefore, there is the step at the bottom of the cycle for this. The second cycle, shown on the right in the figure, is the main cycle and is known as the control cycle. It makes use of the weighting matrix, which is the common part of the two cycles, to compute the risk score of the hierarchy based on the current risk impact and probability data. Risk control is

Figure 2. The knowledge leakage risk assessment model


Perform AHP pair-wise comparison
Compute AHP Risk Score
Knowledge leakage hierarchy
Risk weighting matrix
Knowledge leakage risk control
Construct/ Modify hierarchy
Set/Change/ Keep risk impact and probability
Construct
Apply
Control

carried out in this cycle with the use of the weightings for task prioritization and other risk control measures like risk mitigation. As soon as the risk controls or changes in business context affect the impact or probability of a risk, such data are updated and then combined with the weighting matrix to produce a new risk score for evaluation and monitoring. Usually, as time progresses, this cycle repeats itself as often as required, depending on the changes in risks or business context. Therefore, these parts are much more active and dynamic than the other parts in the left cycle and assume a greater role in the model. It explains why the right cycle is the main cycle whereas the left is the sub-cycle. As can be seen in Figure 2, AHP is driving the two cycles, making the elements and actions depicted by the model interact in constant motion in the context of the bigger Construct (Hierarchy) – Apply (AHP) – Control (Risk) cycle.

METHODOLOGY OF THE MODEL

The methodology of the model involves a process of three phases during which AHP is applied to the knowledge leakage risk hierarchy constructed, as shown in Figure 3. The first phase is the construction of a hierarchy for the knowledge leakage risks of an organization while the second and third phases are the assessment of the knowledge leakage risks in the hierarchy using AHP.

Phase 1 – Construction of a hierarchy of knowledge leakage risk

In this phase, a hierarchy of knowledge leakage risks of an organization is constructed based on studies carried out for the organization. The number of levels and the kinds of leakage risks to be dealt with are identified to reflect the business context, the nature of risks and the depth of assessment. The procedures involved are best explained with an example. Refer to the section on ‘Knowledge Leakage Risk Hierarchy’ for details.

Phase 2 – Setup of an AHP environment

AHP is applied to the knowledge leakage hierarchy to assess the knowledge leakage risk. To do this, risks are measured in terms of their importance to the organization, and a weighting factor is assigned to a risk accordingly. The greater the importance is, the higher the weighting is. Starting with the four key drivers of knowledge leakage risks, a pair-wise comparison is performed for each driver with each of the other three drivers using Saaty’s scale (Saaty, 2008) for pairwise comparison as in Table l. In this section, a hypothetical organization is used and the data chosen reflects business parameters close to real world organizations. To illustrate, referring to the second, third and fourth entry in the first row in Table 2 (the first entry is for self-comparison), the importance of knowledge leakage through suppliers is considered as three times more than that through customers, three times less than

Figure 3. The 3 phases in the methodology

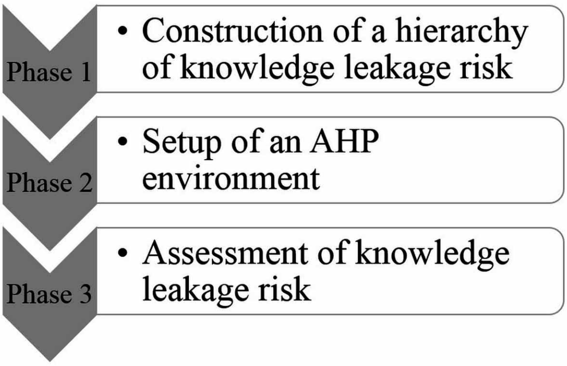

Phase 1
• Construction of a hierarchy of knowledge leakage risk
Phase 2
• Setup of an AHP environment
Phase 3
• Assessment of knowledge leakage risk

Table 1. Scale for pair-wise comparison by Saaty (2008)

Intensity of Importance	Definition	Explanation
1	Equal importance	Two activities contribute equally to the objective
3	Moderate importance	Experience and judgement slightly favour one activity over another
5	Strong importance	Experience and judgement strongly favour one activity over another
7	Very strong or demonstrated importance	An activity is favoured very strongly over another; its dominance demonstrated in practice
9	Extreme importance	The evidence favouring one activity over another is of the highest possible order of affirmation
2,4,6,8	Intermediate values	
Reciprocals of above	If activity *i* has one of the above non-zero numbers assigned to it when compared with activity *j*, then *j* has the reciprocal value when compared with *i*	

that through competitors and seven times less than that through employees. The same comparison procedure is then applied to the set of sub-drivers of each of the key drivers and the results are given in Table 3 to 6.

Following AHP procedures, the elements C_{ij} in each pair-wise comparison matrix A, as below, are translated into absolute values (weightings) with a consistency ratio (CR) for each set of matrix.

Table 2. Pair-wise comparison matrix for the four main drivers of knowledge leakage

Main drivers	Suppliers	Customers	Competitors	Employees
Suppliers	1/1	3/1	1/3	1/7
Customers	1/3	1/1	1/5	1/7
Competitors	3/1	5/1	1/1	1/5
Employees	7/1	7/1	5/1	1/1

Table 3. Pair-wise comparison matrix for sub-drivers under ‘Suppliers’

Sub-drivers	Tendering/ Bidding	Outsourcing	Strategic alliances/ Partnerships	Turnover of suppliers
Tendering/ Bidding	1/1	1/3	1/9	1/5
Outsourcing	3/1	1/1	1/7	1/3
Strategic alliances/ Partnerships	9/1	7/1	1/1	3/1
Turnover of suppliers	5/1	3/1	1/3	1/1

Table 4. Pair-wise comparison matrix for sub-drivers under 'Customers'

Sub-drivers	Business propositions with customers	Sample contracts/ Non-disclosure agreements	Customer relationship management
Business propositions with customers	1/1	1/1	5/1
Sample contracts/ Non-disclosure agreements	1/1	1/1	5/1
Customer relationship management	1/5	1/5	1/1

Table 5. Pair-wise comparison matrix for sub-drivers under 'Competitors'

Sub-drivers	Competitor clustering	Data theft
Competitor clustering	1/1	1/9
Data theft	9/1	1/1

Table 6. Pair-wise comparison matrix for sub-drivers under 'Employees'

Sub-drivers	Unwanted turnover	Retirement	Intentional/ unintentional act by employees
Unwanted turnover	1/1	3/1	1/4
Retirement	1/3	1/1	1/9
Intentional/ unintentional act by employees	4/1	9/1	1/1

$$A = \begin{pmatrix} C_{11} & \cdots & C_{1j} \\ \vdots & \ddots & \vdots \\ C_{i1} & \cdots & C_{ij} \end{pmatrix}$$

The consistency ratio is calculated as below:

$$A\omega = \lambda_{\max}\omega$$

where ω is the principal Eigen vector of the matrix.

$$CR = \frac{CI}{RI}$$

$$CI = \frac{\lambda_{\max} - n}{n - 1}$$

where *CI* is the consistency index and *RI* is the random consistency index in Table 7 and *n* is the

A web-based AHP software application developed by Dr. Klaus D. Goepel (http://bpmsg.com/academic/ahp.php) was selected to perform the AHP calculations to obtain the required weightings. There are a number of professional commercial software packages available for AHP (Al-Harbi, 2001; Alidi, 1996), e.g. Expert Choice, Criterium. Dr. Klaus D. Goepel's version was chosen because its features and capabilities are sufficient to support the non-complex AHP processing needs of this paper to illustrate the use of AHP in the knowledge leakage context, making the commercial grade software with sophisticated features unnecessary. Furthermore, the chosen is free and easy to use over the web with no local software installation required.

The weightings of the four key drivers and the consistency ratio are presented in Table 8. Subsequently, for each of the sub-driver pair-wise comparison matrices, the final weightings w'_{ij} are obtained by multiplying the weighting w_i *(i = 1,…,D)* of the respective main driver d_i *(i = 1,…,D)* with the initial weighting w_{ij} *(i = 1,…,D ; j = 1,…,S)* of the respective sub-driver s_{ij} *(i = 1,…D ; j = 1,…,S)* as below:

$$w'_{ij} = w_i \times w_{ij}$$

where w_i is the weighting of the main driver d_i and w_{ij} is the initial weighting of the sub driver s_{ij}

In this way, the final weightings of each sub driver are normalized with:

$$\sum_{j=1}^{s} w'_{ij} \leq 1, i = 1,\ldots,D$$

For example, the final weighting w'_{ij} for 'Tendering/Bidding= 0.0048 is obtained by multiplying the weighting of 'Suppliers' = 0.097 by the initial weighting of 'Tendering/Bidding' = 0.049. The

Table 7. Sample Random consistency index RI as in Patil and Kant (2014)

Size (n)	1	2	3	4	5	6	7	8
RI	0	0	0.52	0.89	1.11	1.25	1.35	1.40

Table 8. The weightings/prioritised ratings for the four main drivers

	Suppliers	Customers	Competitors	Employees	CR
w_i	0.097	0.051	0.209	0.643	0.088

final weightings with the consistency ratios are presented in Table 9. All the consistency ratios are less than 0.1, indicating that the results are sufficiently accurate (Partovi et al., 1990).

Phase 3 – Assessment of knowledge leakage risk

The impact and probability are then assessed for each sub driver after risk control actions have been performed. The more effective the risk control measures are, the more risk these measures can control and the less risk remains. The impact scale is a 1-10 scale, with 1 as the least impact and 10 as the most severe impact, while the probability scale is a 1-10 scale with 1 as the least possible and 10 as the most possible. The final risk score is capped at 100 and is calculated as:

$$Score = \sum_{j=1}^{S} w'_{ij} \times I_{ij} \times P_{ij}, i = 1, \ldots, D$$

where w'_{ij} is the final weighting of the sub-driver s_{ij}, I_{ij} is the impact score of the sub-driver s_{ij} and P_{ij} is the probability score of the sub-driver s_{ij}

Table 9. The initial and final weightings/prioritised ratings for the sub-drivers

Sub-drivers	w_{ij}				w'_{ij}	CR
	Suppliers	Customers	Competitors	Employees		
Tendering/ Bidding	0.049	-	-	-	0.005	0.032
Outsourcing	0.101	-	-	-	0.010	
Strategic alliances/ partnerships	0.607	-	-	-	0.059	
Turnover of suppliers	0.243	-	-	-	0.024	
Business propositions with customers	-	0.455	-	-	0.023	0.000
Sample contracts/ Non-disclosure agreement	-	0.455	-	-	0.023	
Customer relationship management	-	0.091	-	-	0.005	
Competitors clustering	-	-	0.100	-	0.021	0.000
Data theft	-	-	0.900	-	0.188	
Unwanted turnover	-	-	-	0.200	0.129	0.010
Retirement	-	-	-	0.073	0.047	
Intentional/ unintentional act by employees	-	-	-	0.727	0.467	

As illustrated in Table 10, the final risk score for the hypothetical organization is 33.8. The risk score can be used as an indicator of the level of risk in the organization as well as for monitoring the effectiveness of risk control measures taken. Basically, the higher the final risk score (the closer it is to 100), the higher the risk of knowledge leakage in the organization.

DISCUSSION

As can be seen in the model and methodology sections, the assessment of the knowledge leakage risks of the whole organization is facilitated with the application of AHP in the risk management process. The weightings help the prioritization of risks, or in better allocation of resources to tackle the knowledge risk. The two cycles, the hierarchy cycle and the control cycle, operate inter-dependently and co-operatively, though assuming different roles and fulfilling different needs in knowledge leakage assessment. The end result is that a risk score can be obtained as often as the business context demands for more effective assessment and quicker response across business entities or across different time periods in an organization, large or small. Though the risk score has to be interpreted together with other business performance indicators, it is still usable in monitoring. It indicates how AHP drives better risk management of knowledge leakage.

In fact, the hierarchy in the example can be replaced by another knowledge leakage hierarchy to suit a new business demand, where the top level becomes Sales/Marketing, Customer Service, Inventory Operations, Hardware Support, Software Support, Manufacturing and R&D, for example. Below the top level, each top level element is furthered composed of a number of knowledge leakage sub-risks specific to the top-level element. Almost immediately, another Construct-Apply-Control cycle can be carried out to assess the knowledge leakage risks from another perspective. This shows the flexibility of the present approach. To develop a usable hierarchy requires the cooperation of internal managerial staff and external specialists, where applicable. The hierarchy construction process can make use of

Table 10. Risk scores for sub drivers

Risk of Knowledge Leakage	Weighting w'_{ij}	Impact I_{ij}	Probability P_{ij}	Risk Score
Tendering/Bidding	0.005	3	7	0.100
Outsourcing	0.010	3	7	0.206
Strategic alliances/partnerships	0.059	7	4	1.649
Turnover of suppliers	0.024	5	2	0.236
Business propositions with customers	0.023	3	5	0.348
Sample contracts/Non-disclosure agreements	0.023	6	3	0.418
Customer relationship management	0.005	5	5	0.116
Competitors clustering	0.021	7	4	0.585
Data theft	0.188	9	2	3.386
Unwanted turnover	0.129	7	6	5.401
Retirement	0.047	8	7	2.629
Intentional/unintentional act by employees	0.467	8	5	18.698
Total				**33.8**

the Delphi method (Sun, Srivastava, & Mock, 2006), a managed procedure to brainstorm alternatives and choose the different options available. One added benefit of the hierarchy construction process is that it enables the managing staff concerned to think systematically of the knowledge leakage risk they face every day without ever having a chance or time to think them through in a more organized way in order to discover what they do not already know or ignore most of the time. The knowledge leakage risks will be better attended to and managed.

Application I: Applying the Model across Organizational Structure

Except for small organizations, there are usually more than one business entities inside the same organization. In addition to constructing the knowledge leakage hierarchy for the whole, known as the main hierarchy, individual hierarchies, known as sub-hierarchies, can also be constructed for different business entities, and an independent AHP can be done for risk control of a particular entity. In other words, depending on the business needs, the model can be used for any structural or functional part of the whole organization as long as it makes business sense, from the corporate risk management perspective. In fact, the model can be deployed as one of the management tools for a specialized project of a definite duration. As a result of this flexibility, more cost-effective and detailed risk assessments can be carried out to meet current or anticipated needs.

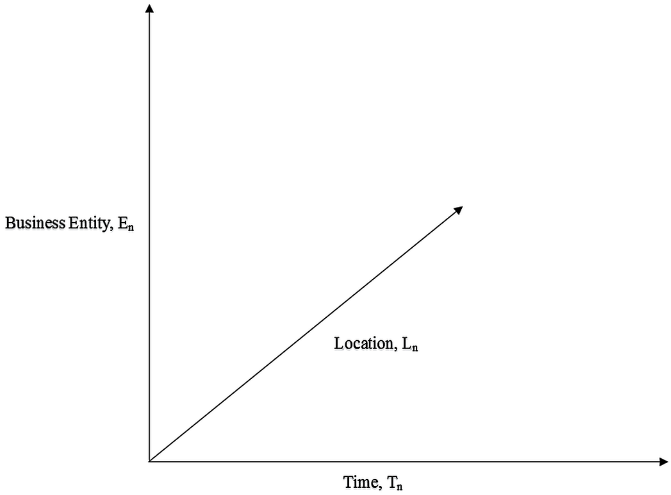
To implement this flexibility in practice, there are three main directions for applying the model across different business entities, as shown by the three axes in Figure 4. First, for the x-axis, the axis of time, if the hierarchy and weightings are the same or stable over a period of time, a line graph constructed along this axis can show the risk score trend of the same business entity for different times. For the y-axis, the axis of business entity, if a number of business entities in the same organization location (e.g. a plant) are of similar business nature (e.g. product groups with each working on a different product in the same manufacturing campus) and thus share the same hierarchy and same weighting matrix, a line graph can be drawn along this axis to show the variation of risk scores for different entities in the same time period. Then for the z-axis, or the axis of business location, if a business entity of the same nature (e.g. web page design project group) exists in different business locations (e.g different districts in the same city or different cities in the same country) and they share the same hierarchy and weighting matrix, a line graph drawn along the z-axis can show the risk scores of entities in the same period in different locations for risk control results comparison. For a multi-national company with subsidiaries around the world operating in the same business and sharing the same management structure and practice, the AHP can be applied to offer tangible data for monitoring and comparison of the same or different business entities over time or space.

Application II: Using the Model in Credit Risk Analysis

The AHP-driven knowledge leakage risk assessment model can be used in an organization to manage the concerned risk. At the same time, external parties can also take advantage of the usefulness of this model and one of them is the credit risk analyst of a financial institution which lends money to companies for running their businesses. At present, the credit risk analyst adopts the established practice for the credit risk assessment of loan applicants by mainly making use of the financial reports (Iazzolino, Migliano, & Gregorace, 2013). However, any knowledge leakage can potentially affect the competitive advantage significantly, putting its earning capacity in doubt. Therefore, it is advisable to include knowledge leakage risk assessment in the credit risk analysis of the applicant.

The financial institution can ask the applicant to submit knowledge leakage risk control reports which show their objectives, planning and review of what they have done in this domain of risk management. Further, the analyst can visit the applicant's office and hold meetings/interviews with the concerned staff to have on-site information gathering and observation. If the applicant uses the AHP-driven model, the analyst can do a better job in credit risk analysis in several ways. First, the risk hierarchy constructed for the model enables the applicant to have a critical systematic analysis and review of the current knowledge leakage risks faced. This action results in better planning and

Figure 4. Risk Scores comparison along time, business entity and location axes



prioritization for the leakage risks to increase the ability to eliminate or reduce losses, especially those affecting the repayment of loans. Thus the hierarchy work provides documented evidence to support what the applicant claims in the loan repayment schedules. The quality of the documents at least reflects to a certain extent how well the applicant manages the risk.

Second, the weighting matrix, as a product of applying AHP to the hierarchy show the relative importance of the leakage risks in the applicant portfolio of the knowledge leakage risks. Detailed study by a credit risk analyst may reveal useful information, notably about the company's risk distribution but also the most important risks being faced, which may affect the organization's earnings in the future.

Third, the risk score, a numeric figure provided by the model, is very useful. The figure, when combined with other risk-related information, will inform the analyst about the quality of risk management in the organization. As this data can be provided regularly, like other financial data, the risk score can be used for the monitoring of risk management performance by comparing the figures in different periods.

Finally, this important numeric risk score can be fed into the credit risk analysis system of the lending company as part of the regular input data, making it a strong candidate to be one of the independent variable with the potential to enhance the credit risk analysis results. Earlier work by Iazzolino et al. (2013) showed that the use of intellectual capital related data (knowledge leakage is in this category) can benefit credit risk analysis. Further modelling work on the credit risk analysis software is required to realise this perceived advantage of the model.

LIMITATIONS AND FUTURE RESEARCH

The application of AHP to knowledge leakage risks of an organization is a novel approach conceptually and the empirical results after assessing a hierarchy of risks instead of individual risks are not commonly found in existing AHP applications nor in other risks assessment methods which are largely qualitative. The novel approach comes with limitations which are anticipated however. First, if the hierarchy consists of many kinds of knowledge leakage risks, to do all the pair-wise comparisons becomes a lengthy and cumbersome process (Belton, 1986), making some comparisons not be done accurately. This undesirable situation may occur especially when the model deals with a large hierarchy or a hierarchy which changes its structure and components quite frequently. More fundamentally, it may be argued that the translation of assessor understanding, perception or evaluation in the pair-wise comparisons into numbers may be inaccurate though the assessor may think otherwise (Deng, 1999). Associated with this translation concern and as it is usual the case with other empirical methods which rely on the assignment of numbers to a set of related qualitative measurements, the analysis results (the risk scores in the assessment model) can be difficult to interpret for practical use. This limitation is magnified when the risk scores of the same hierarchy are compared for two or more different periods and then interpreted.

In view of the above, more research needs be done to address them. One probable route to take is to use a fuzzy scale in the model to overcome the undesirable uncertainty or inaccuracy associated with pair-wise comparisons (Mikhailov & Tsvetinov, 2004). Also, efforts should be made in finding other empirical methods to augment the AHP in the model so that the new numeric results can be interpreted on stronger theoretical grounds. Finally, as with any novel theoretical considerations, the proposed model should be put to test in small or large organizations in order to get field feedback from practitioners as well and increase the model's strength. Since both the positive and negative sides of knowledge leakage risk are under-researched (Mohamed et al., 2007), testing the model for the positive side can be one of the next logical steps of future work.

CONCLUSION

How AHP can be applied to the knowledge leakage hierarchy constructed for an organization in the risk assessment cycle is demonstrated and how the AHP-generated weighting matrix can be used in risk control effectiveness comparison and monitoring across time and business entities at various levels of the organization locations is also discussed. Such work done and demonstrated in this paper is built on strong, solid theoretical and risk management grounds with significant implications.

It is the nature of knowledge leakage that it can occur in any business entity and any point in the value chain, implying that there are quite many kinds of knowledge leakage faced by an organization. This makes using a hierarchy to visualize them and show their inter-relationships, either functionally or structurally, a logical first step to take in any risk control effort of knowledge leakage. Therefore, hierarchy-based AHP and the knowledge leakage hierarchy come naturally together in determining the weightings of risks in the hierarchy. It is easy to understand and do the pair-wise comparisons across the risks at the higher level horizontally and across those risks one level immediately below vertically. The readily available AHP software in the public domain then creates the important weighting matrix for the hierarchy, giving at a glance a total picture of the relative importance of all knowledge leakage risks of the whole organization. This indicates the power of AHP combined with the organizational leakage hierarchy.

Conceptually, AHP has been developed for a long time and is theoretically a sound solid methodology in multi-criteria decision making and a hierarchy of knowledge leakage risks is also a theoretically sound representation of knowledge leakage risks in business because it reflects the nature of such risks in an the real world. From a theoretical standpoint, the application of AHP to knowledge leakage is valid and similar to many past usage examples of AHP much mentioned in the literature. What is unique is that this paper argues the conceptual combination of the two theoretical approaches and put forward the theoretical construct-apply-control approach in the risk assessment literature. Notably, it is the first time when the AHP theory is deployed to a new area of IC risks with revealing results when IC risk itself up to now is an under-researched topic for many years (Mohamed et al., 2007; Frishammar et al., 2015).

From the standpoint of management practice, the total organizational picture of knowledge leakages not only helps the allocation and prioritization of resources to combat leakages but also serves to monitor the risk control effectiveness across time or business entities, all being critical components in any risk management. The flexibility and robustness of AHP in knowledge leakage control become evident and crucial when IC, IC risks and knowledge leakage risks may change quickly, and new or emerging ones may come in great numbers without any pre-warning in the globalized knowledge-intensive economy. When even primitive tools let alone empirical ones of any sort are difficult to find in a research field as new as IC risk, the ease of using AHP makes it an attractive, effective tool to use in the initial control set up and following mitigation and monitoring to meet the fast changing uncharted IC risk waters. Compared against many existing risk management frameworks or systems, a systematic empirical means of risks assessment across time or business entities in an organization provided by the paper's model is conspicuously absent in them.

As said above, an AHP-driven risk assessment model is well-suited to knowledge leakage, as well as IC risks in general. The model can be further refined and developed to enlarge its scope of applicability and has the potential to use with other innovative empirical tools to provide risk assessment measures not seen at present in any risk management systems. As what it is now and will continue for some considerable time in the future, the robustness of this AHP model will make it a growing contributor in the empirical IC risk landscape and enterprise risk management landscape as well.

ACKNOWLEDGMENT

The authors would like to thank the Research Committee and the Department of Industrial and Systems Engineering of The Hong Kong Polytechnic University for the financial support of the research study (Account Code: RU8Q) and two anonymous reviewers for their valuable feedback.

REFERENCES

Ahmad, A., Bosua, R., & Scheepers, R. (2014). Protecting organizational competitive advantage: A knowledge leakage perspective. *Computers & Security*, *42*, 27–39.

Al-Harbi, K. M. A.-S. (2001). Application of the AHP in project management. *International Journal of Project Management*, *19*(1), 19–27.

Alidi, A. S. (1996). Use of the analytic hierarchy process to measure the initial viability of industrial projects. *International Journal of Project Management*, *14*(4), 205–208.

Belton, V. (1986). A comparison of the analytic hierarchy process and a simple multi-attribute value function. *European Journal of Operational Research*, *26*(1), 7–21.

Carlucci, D., & Schiuma, G. (2007). Knowledge assets value creation map: Assessing knowledge assets value drivers using AHP. *Expert Systems with Applications*, *32*(3), 814–821. doi:10.1016/j.eswa.2006.01.046

Casualty Actuarial Society. (2003). *Overview of Enterprise Risk Management*. Retrieved from https://www.casact.org/area/erm/overview.pdf

Cheng, C.-H., & Mon, D.-L. (1994). Evaluating weapon system by analytical hierarchy process based on fuzzy scales. *Fuzzy Sets and Systems*, *63*(1), 1–10. doi:10.1016/0165-0114(94)90140-6

Curtis, P., & Carey, M. (2012). *Risk Assessment in Practice*. Retrieved from http://www.coso.org/documents/COSOAnncsOnlineSurvy2GainInpt4Updt2IntrnlCntrlIntgratdFrmwrk%20-%20for%20merge_files/COSO-ERM%20Risk%20Assessment%20inPractice%20Thought%20Paper%20OCtober%202012.pdf

DeLong, D. W. (2004). *Lost knowledge: Confronting the threat of an aging workforce*. New York: Oxford University Press. doi:10.1093/acprof:oso/9780195170979.001.0001

Deng, H. (1999). *Multicriteria analysis with fuzzy pairwise comparison.* Paper presented at the Fuzzy Systems Conference Proceedings, 1999. FUZZ-IEEE'99. 1999 IEEE International.

Edvinsson, L. (1997). Developing intellectual capital at Skandia. *Long Range Planning*, *30*(3), 320–373. doi:10.1016/S0024-6301(97)00016-2

Edvinsson, L., & Kivikas, M. (2007). Intellectual capital (IC) or Wissensbilanz process: Some German experiences. *Journal of Intellectual Capital*, *8*(3), 376–385. doi:10.1108/14691930710774821

Frishammar, J., Ericsson, K., & Patel, P. C. (2015). The dark side of knowledge transfer: Exploring knowledge leakage in joint R&D projects. *Technovation*, *41*, 75–88.

Grimaldi, M., & Rippa, P. (2011). An AHP-based framework for selecting knowledge management tools to sustain innovation process. *Knowledge and Process Management*, *18*(1), 45–55. doi:10.1002/kpm.365

Halawi, L., Aronson, J., & McCarthy, R. (2005). Resource-based view of knowledge management for competitive advantage. *Electronic Journal of Knowledge Management*, *3*(2), 75–86.

Hallikas, J., Karvonen, I., Pulkkinen, U., Virolainen, V.-M., & Tuominen, M. (2004). Risk management processes in supplier networks. *International Journal of Production Economics*, *90*(1), 47–58. doi:10.1016/j.ijpe.2004.02.007

Handfield, R., Walton, S. V., Sroufe, R., & Melnyk, S. A. (2002). Applying environmental criteria to supplier assessment: A study in the application of the Analytical Hierarchy Process. *European Journal of Operational Research*, *141*(1), 70–87. doi:10.1016/S0377-2217(01)00261-2

Harvey, M. G., & Lusch, R. F. (1999). Balancing the intellectual capital books: Intangible liabilities. *European Management Journal*, *17*(1), 85–92.

Iazzolino, G., Migliano, G., & Gregorace, E. (2013). Evaluating intellectual capital for supporting credit risk assessment: An empirical study. *Investment Management and Financial Innovations*, *10*(2), 44–54.

Jandaghi, E., Jandaghi, G., Irani, H. R., Mousavi, Z. S., & Davoodavabi, M. (2014). Ranking the knowledge management enablers based on University Academic Members, Staff and Students using AHP Method. *International Letters of Social and Humanistic Sciences,* 15, 7-13.

Jiang, X., Li, M., Gao, S., Bao, Y., & Jiang, F. (2013). Managing knowledge leakage in strategic alliances: The effects of trust and formal contracts. *Industrial Marketing Management*, *42*(6), 983–991.

Khan, R. A. (2014). Sustainable Competitive Advantage through Knowledge Management. *International Journal of Advanced Research in Computer & Technology*, *3*(4).

Mikhailov, L., & Tsvetinov, P. (2004). Evaluation of services using a fuzzy analytic hierarchy process. *Applied Soft Computing*, *5*(1), 23–33.

Mohamed, S., Mynors, D., Grantham, A., Chan, P., Coles, R., & Walsh, K. (2007). Unearthing key drivers of knowledge leakage. *International Journal of Knowledge Management Studies*, *1*(3-4), 456–470. doi:10.1504/IJKMS.2007.012535

Mustafa, M. A., & Al-Bahar, J. F. (1991). Project risk assessment using the analytic hierarchy process. *IEEE Transactions on Engineering Management*, *38*(1), 46–52.

Parise, S., Cross, R., & Davenport, T. H. (2006). Preventing a knowledge-loss crisis. *MIT Sloan Management Review*, *47*(4), 31.

Parker, H. (2012). Knowledge acquisition and leakage in inter-firm relationships involving new technology-based firms. *Management Decision*, *50*(9), 1618–1633. doi:10.1108/00251741211266714

Partovi, F. Y., Burton, J., & Banerjee, A. (1990). Application of analytical hierarchy process in operations management. *International Journal of Operations & Production Management*, *10*(3), 5–19. doi:10.1108/01443579010134945

Patil, S. K., & Kant, R. (2014). Ranking the barriers of knowledge management adoption in supply chain using fuzzy AHP method. *International Journal of Business Innovation and Research*, *8*(1), 52–75. doi:10.1504/IJBIR.2014.058047

Pfeffer, J. (1994). Competitive advantage through people. *California Management Review*, *36*(2), 9–28. doi:10.2307/41165742

Saaty, T. L. (1977). A scaling method for priorities in hierarchical structures. *Journal of Mathematical Psychology*, *15*(3), 234–281. doi:10.1016/0022-2496(77)90033-5

Saaty, T. L. (2008). Decision making with the analytic hierarchy process. *International journal of services sciences*, 1(1), 83-98.

Sun, L., Srivastava, R. P., & Mock, T. J. (2006). An information systems security risk assessment model under the Dempster-Shafer theory of belief functions. *Journal of Management Information Systems*, *22*(4), 109–142. doi:10.2753/MIS0742-1222220405

Williams, T. (1993). Risk-management infrastructures. *International Journal of Project Management*, *11*(1), 5–10. doi:10.1016/0263-7863(93)90003-6

Wu, W.-W., & Lee, Y.-T. (2007). Selecting knowledge management strategies by using the analytic network process. *Expert Systems with Applications*, *32*(3), 841–847. doi:10.1016/j.eswa.2006.01.029

Zhi, H. (1995). Risk management for overseas construction projects. *International Journal of Project Management*, *13*(4), 231–237. doi:10.1016/0263-7863(95)00015-I