J Inf Process Syst, Vol.10, No.2, pp.240~255, June 2014
http://dx.doi.org/10.3745/JIPS.03.0004

pISSN 1976-913X
eISSN 2092-805X

Leveraged BMIS Model for Cloud Risk Control

YouJin Song* and Yasheng Pang**

Abstract—Cloud computing has increasingly been drawing attention these days. Each big company in IT hurries to get a chunk of meat that promises to be a whopping market in the future. At the same time, information is always associated with security and risk problems. Nowadays, the handling of these risks is no longer just a technology problem, with a good deal of literature focusing on risk or security management and framework in the information system. In this paper, we find the specific business meaning of the BMIS model and try to apply and leverage this model to cloud risk. Through a previous study, we select and determine the causal risk factors in cloud service, which are also known as CSFs (Critical Success Factors) in information management. Subsequently, we distribute all selected CSFs into the BMIS model by mapping with ten principles in cloud risk. Finally, by using the leverage points, we try to leverage the model factors and aim to make a resource-optimized, dynamic, general risk control business model for cloud service providers.

Keywords—Cloud risk, CSFs, BMIS, Risk control, Leverage point, Effective model

1. Introduction

“Cloud computing” has ceased to be unfamiliar vocabulary nowadays. The main advanced idea of cloud computing is to make better use of distributed resources and integrate various resources sufficiently to adapt to the changing client requirements. Nevertheless, it is still a newborn business model for IT service; cloud risk or security problem becomes a “hot potato” that hinders an enterprise’s adoption of cloud services to some degree. No wonder, delivering one’s data to a third-party provider that owns infrastructure or platform or software that is not within your grasp is worrisome enough.

Many research and literature on cloud security management have been published. Among these, some papers submit new management model or framework in cloud security [1,2], whereas some models try to connect on a business level [3-5]. Is it possible to combine the business purpose with an approved risk control model? Is it possible to make a simple yet effective business model to control all risk factors arising in cloud computing? We aim to answer this question in this paper.

Business Model for Information Security (BMIS) is a widely recognized and available model published by ISACA (Information Systems Audit and Control Association). This is a generalized, dynamic security model on a business level. To advance this model, Sembhi [6]

※ This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2013R1A1A2011581). This work was also supported by the Dongguk University Research Fund of 2013.
Manuscript received July 19, 2013; accepted September 26, 2013.

Corresponding Author : YouJin Song (song@dongguk.ac.kr)
* Dept. of Information Management, Dongguk University, Gyeongju, 780-714, Korea (song@dongguk.ac.kr)
** ElComTec Co. (pangpang7117@gmail.com)

suggested looking for a leverage point of this prominent model during an RSA conference in 2010. In that conference, however, he merely presented a suggestion, not a solution; until now, there are still no articles published to solve this problem. This paper focuses on cloud risk and presents an integrated cloud risk table. Aiming at these practical risks, it applies and leverages the published BMIS model by mapping with the recognized “twelve leverage points” [7] to the cloud service environment. Finally, we try to make a resource-optimized, effective, dynamic, general risk control business model in cloud computing focusing on cloud risk control at a business level.

The rest of this paper is organized as follows: Section 2 introduces related work, describing the basic concept of every related method; Section 3, which is the core part of this paper, tackles model building, which includes three steps – first, find out the essential causal factors for all existing cloud risks, and then connect them with the BMIS model by mapping with “Ten principles,” and finally, using the published “Twelve leverage points,” find the leverage points for all factors and leverage this model to apply to the cloud service environment; Section 4 presents the conclusions of this paper, describes the advantage and meaning of the entire work, and also points out the shortcomings of this paper.

2. Related Work

2.1 BMIS

The history of BMIS can be traced back to a project at the USC (University of Southern California) Marshall School of Business. ISACA then obtained the right to develop it in 2008 [8] and officially published this model in October 2010 [9]. There are four elements and six dynamic interconnections in the construction of this model. The four elements are organization, people, process, and technology; the six interconnections are governing, culture, enabling and support, emergence, human factors, and architecture. This model is illustrated in Fig. 1.

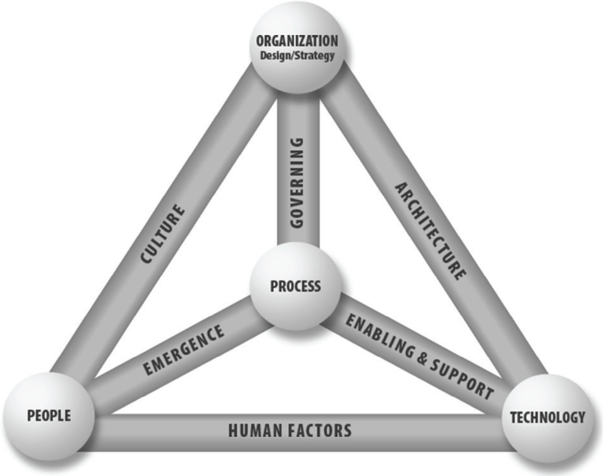

Fig. 1. Business model for information security [8]

In Figure 1, you may see a plain model and think that it is just a “process-centered” triangle. Note, however, that this is a three-dimensional, pyramid-shaped structure. According to ISACA, it is a model that can be predictive and proactive, not just concerning traditional information security but also includes privacy, linkage to risk, physical security, and compliance, which is what we need -- a dynamic, integrated, general risk control model.

2.2 CSFs

Daniel [10] put forward the concept of “success factors” in 1961. Rockart [11] developed it as “Critical Success Factors” in one of his publications in 1979 and refined it in another paper in 1981 [12]. It was initially used for information system management and data analysis, which can ensure that the organization accomplishes its mission or the success of a strategy [13]. R.A.Caralli [14] aligned CSFs (Critical Success Factors) with enterprise security management and stated that CSFs have shown not only promise in helping organizations guide and direct themselves but also the order of action, which contributes to security strategies and security management at the enterprise level. R.A.Caralli [14] demonstrated the importance and definitiveness of CSFs in security management, whereas Wang and colleagues [15] hierarchized them through the FAHP (Fuzzy Analytic Hierarchy Process) method and used it in the cloud environment. Note, however, that this paper simply reviews information security management literature; it neither focuses on practical risks in the cloud nor takes into consideration all the risk types in a realistic cloud environment. Selecting CSFs focusing on integrated risks in the cloud and taking into consideration the requirements at the security or governance level will be vital to our business model building.

2.3 Ten principles of cloud computing

David Vohradsky [16], who has more than 25 years’ experience in information and security management, presented ten principles of cloud computing risk based on BMIS and demonstrated an assessment framework for cloud risk through a case study. In that publication, the author describes four guiding principles as a cloud assessment road map and ten detailed principles that connect with BMIS. We summarize them in Table 1 below.

The important thing is that we can map the critical cloud risk factors with both the four guiding principles and the ten detailed principles according to the definition of every principle.

Table 1. Ten principles and related concepts

Implication of each guiding principle	Guiding principles	Ten detailed principles	Connection with BMIS structure
What is the business vision, and who will own the initiative?	Vision	1. Executives must have oversight over the cloud.	Governing
		2. Management must own the risks in the cloud.	Organization
What needs to be done, and what are the risks?	Visibility	3. All necessary staff must have knowledge of the cloud.	Human factors
		4. Management must know who is using the cloud.	People
		5. Management must authorize what is put in the cloud.	Technology

Who is accountable, and to whom?	Accountability	6. Mature IT processes must be followed in the cloud.	Process
		7. Management must buy or build management and security in the cloud.	Architecture
		8. Management must ensure that cloud use is compliant.	Culture
How will it be monitored and measured?	Sustainability	9. Management must monitor risk in the cloud.	Enabling and support
		10. Best practices must be followed in the cloud.	Emergence

2.4 System leverage points

The concept of leverage is one of the most powerful in all of science. Archimedes proved the Law of the Lever and applied it to a variety of inventions. Historian John Tzetzes, writing in the 12th century, wrote that Archimedes said, "Give me a place to stand, and with a lever I will move the world" [17]. In systems, thinking of a leverage point is a place in a system's structure where a solution element can be applied. It is a low leverage point if a small amount of force causes a small change in system behavior. It is a high leverage point if a small amount of force causes a large change in system behavior[6].

An article titled “Leverage points to intervene in a system” was published in 1999 by Donella Meadows [7]. Meadows, who worked in the field of systems analysis, proposed a scale of places to intervene in a system. Awareness and manipulation of these levers are an aspect of self-organization, and they can lead to collective intelligence. In this paper, there are twelve leverage points:

① Power to transcend paradigms
② Mindset or paradigm out of which the system arises
③ Goal of the system
④ Power to add, change, evolve, or self-organize the system structure
⑤ Rules of the system (such as incentives, punishment, constraints)
⑥ Structure of information flow
⑦ Gain around driving positive feedback loops
⑧ Strength of negative feedback loops relative to the effect they are trying to correct
⑨ Length of delays relative to the rate of system changes
⑩ Structure of material stocks and flows (such as transport network, population age structures)
⑪ Size of buffers and other stabilizing stocks relative to their flows
⑫ Constants, parameters, numbers (such as subsidies, taxes, standards)

These twelve leverage points are listed in order of importance. Compared with the BMIS model, it also mentioned the elements structure, organization, and human factor, giving an ordinary sequence of these elements that you should pay attention to in a system. Definitely, there is a leverage point in every system; we can do resource optimization by using this leverage point. Regarding resource optimization, it aims to obtain maximum output with minimum input. This is just what we need to figure out and help us in risk governance on a business level.

3. Model Building

Excavation for the essentially formative factors of each specific cloud risk will certainly be a good way to define CSFs in cloud risk management. Consider the old Chinese proverb, "Know yourself and know your enemy; you will win every war." Similarly, find the reason for the problems, and then seek the solution to deal with them. The whole idea of leveraged BMIS model is to find the essential causal risk factors in the cloud environment, which can connect with the four elements of BMIS, and then seek the leverage point of each risk factor for more effective control. Thus, the overall visual you will see is a model that has four elements (organization, people, process, and technology) to keep macro-control and a series of selected CSFs to deal with micro-control in detail.

3.1 Selection of factors

In the previous research, we browsed many literature focusing on cloud risk [18-23] and, through analysis and comparison with other security requirments [14,24], filtered and sorted a suite of causal factors of cloud risk, which were selected as CSFs in our model building. (See Table 2.)

Table 2. Selected and sorted CSFs

Technology	Trust	Data	Compliance	Measurability
1. Encryption 2. VM technology 3. Identification 4. Authentication 5. Authorization	6. Staff reliability 7. Human resource 8. Service model 9. Outsourcing level 10. Scale & Structure 11. Fault control 12. Feedback loops	13. Data update 14. Physical loss 15. Disaster recovery 16. Business continuity	17. Contract (SLA) 18 Internal security policy & Regulation 19. External standards & laws	20. Auditing (business, data traffic, security)

In this table, we integrate all possible factors mentioned in the reviewed literature, dig out the essential causal factors, and ensure that there are no overlaps among them. To confirm the concept of each factor and to facilitate the explaination of factor connection in the next paragraph, based on the previous research, we give descriptions of the twenty CSFs as follows:

a.Encryption: Weak or outdated encryption algorithm may give rise to a risk in cloud computing.

b.Authorization: Insufficient authorization may give rise to a risk in cloud computing.

c.Authentication: Insufficient authentication may give rise to a risk in cloud computing.

d.Identification: Insufficient identification may give rise to a risk in cloud computing.

e.VM technology: A character of cloud technology is multi-tenant architecture. Isolation and access between the guest and the operating system may give rise to a risk in cloud computing.

f.Staff reliability: Internal staff always hold the first-hand information; the possibility of insider leak (including data, client info), even physical theft will pose a risk in cloud.

g.Human resource: Since cloud computing is advanced technology, the occasional lack of talented person of every aspect may give rise to a risk to the cloud company.

h.Service model: Traditional cloud service includes 3 kinds of service model (SaaS, PaaS, IaaS); depending on the service model, different physical structures pose different risks in cloud service.

i.Outsourcing level: Cloud nesting problem; a SaaS service may use another third-party PaaS service as supplier, and the asymmetry of information flowing between the two poses a risk in cloud computing.

j.Scale & Structure: Physical equipment scale; is it capable enough for normal operation when there is high business volume? The capacity of business is a potential menace in cloud service.

k.Fault control: When daily routine deviates from the business goal, the lack of capacity for system correction poses a risk in cloud service.

l.Feedback loops: The lack of monitoring, regular checking, and feedback information will pose a risk in cloud service.

m.Data update: It is reinforcement for system. The lack of patching and software upgrading process will pose a risk in cloud computing.

n.Physical loss: The effect of physical loss risk varies. Risks like data loss, data leak, temporary service interruption, etc., may all arise from physical loss in cloud service.

o.Disaster recovery: In emergency circumstances, the slow response time, lack of sensitivity, and backup resource will pose a risk in cloud service.

p.Business continuity: The company's long-term goal, i.e., sustainable development; the lack of capacity for "going concern" poses a risk (like bankruptcy) in the cloud company

q.Contract (SLA): Contractual liability; SLA (Service Level Agreement) specific to cloud service is still non-standard, contract disputes may give rise to a risk in cloud service

r.Internal security policy & regulation: Half-baked or incomplete internal rules, punishments will give rise to a risk in cloud enterprise.

s.External standards & laws: The lack of uniform international standards and laws may give rise to a risk in cloud computing.

t.Auditing (business, data traffic, security): Wrong or inaccurate bill auditing, data traffic auditing, and security auditing may give rise to a risk in cloud service.

3.2 Connection of factors

Making the connections with the BMIS model would be a challenge in the course of model building. To ensure the accuracy of connections, we will perform this work in light of David's "10 principles," which we introduced in related work (see Table 1). As mentioned before, this research seeks to find the essential causal risk factors that can connect with the four elements of BMIS, so we first need to pick out only the items that are relevant to the four elements from the ten principles, and then do deep reading to dig out the keywords of principle requirements and list them in Table 3.

According to the concept of each factor we described in the previous section, the factor concepts coinciding with the principle requirement should be connected with the relevant element.

"Service Model" and "Outsourcing Level" initially own a risk; "Fault Control" needs continued monitoring."Business Continuity" is the long-term goal that sets the direction of a cloud company, whereas "Scale & Structure" need physical establishment. "Contract (SLA)" and "Internal Security Policy & Regulation" require textual establishment. These factors all match the principle of "organization" element.

Table 3. Description of the four elements' relevant principles

BMIS elements	Relevant principles	Relevant principle requirements

Organization (design/strategy)	Management must own the risks in the cloud.	Own the risk;
		Establishment;
		Direction;
		Monitoring

People	Management must know who is using the cloud.	Who is using it; Human resource; Recruitment; Transfers; Terminations

Process	Mature IT processes must be followed in the cloud.	Align with policy;
		Meet business requirements;
		Communication;
		Appropriate resource

Technology	Management must authorize what is put in the cloud.	What is put in; Match the requirement of CIA (confidentiality, integrity, availability)

"Feedback Loops" emphasize the symmetry of information flow, which needs sufficient communication between different groups; "Data Update" ensures that the appropriate resource can be obtained in the system. "External Standards & Laws" are the policy we should conform to and align with, whereas "Auditing (business, data traffic, security)" is intended to ensure that there are no mistakes in bill auditing, data traffic measurement, and security assessment, which are also the business requirements in corporate operation. These factors all match the principle of "process" element.

"Human Resource" is a keyword in the "people" element principle; "Staff Reliability" strictly demands passing the recruitment, transfer, and termination process. These two factors meet the principle of "people" element.

"Encryption," "Authentication," "Authorization," and "Identification" are a series of approaches to ensure the confidentiality and integrity of data; "VM Technology" essentially deals with encryption and identification problems and also involves data confidentiality and integrity. "Disaster Recovery" concerns data availability, whereas "Physical Loss" is related to "what is put in" in a system. These factors all match the principle of "technology" element.

3.3 Leveraging of CSFs for the BMIS model

3.3.1 Leverage points mapping with the factors of each element

As we mentioned before, Meadows [7] published "twelve leverage points" to intervene in a system in 1999. Actually, these leverage points mentioned in this paper form an effectiveness rank ordering. To map selected CSFs with leverage points, first, we need better understanding of the meaning of every leverage point. We read the "twelve leverage points" in depth and conclude the key concept of every leverage point as follows (see Table 4):

Leverage point mapping with CSFs should be a vital process in the entire work. According to the concept description of every CSF (see 3.1) and the keyword description of each leverage point (see Table 4), we map all cloud risk factors (twenty CSFs) with "twelve leverage points" one by one. By this process, we found the leverage point of each subordinate factor for the relevant element of the BMIS model.

Table 4. Keyword description of twelve leverage points

Leverage Points	Concept and Keyword Description
1. Power to transcend paradigms	Stay flexible. • Keep oneself unattached in a paradigm. • No paradigm; you can choose whichever will help achieve your purpose
2. Mindset or paradigm out of which the system arises	Paradigm change • Keep pointing at failures in the old paradigm. • Keep getting greater assurance from the new one. • Insert people with the new paradigm in place of public visibility and power.
3. Goal of the system	• Whole system goal (Physical, stocks, flows, feedback loops, information flows, and self-organizing behavior will be twisted to conform to that goal.) • To grow, to increase market share, to bring the world more and more under the control of the corporation
4. Power to add, change, evolve, or self-organize the system structure	System education • Adding completely new physical structures, such as brains or wings or computers • Adding new negative or positive loops • Making new rules
5. Rules of the system	• The rules of the system define its scope, its boundaries, and its degree of freedom. • Contracts need to be honored. • System with rules designed by corporations, run by corporations, for the benefit of corporations
6. Structure of information flow	• Information feedback • Comprehensive, timely market information flow delivering information to a place where it was not going before; thus causing people to behave differently
7. Gain around driving positive feedback loops	Self-reinforcing • The more it works, the more it gains power to work some more • Controlling the growth rate
8. Strength of negative feedback loops relative to the effect they are trying to correct	Self-correcting (information and control part) • Keep the appointed stock at or near its goal. • Accuracy and rapidity of monitoring • Quickness and power of response
9. Length of delays relative to the rate of system changes	Timely information, timely response • Delay, too short time causes overreaction, too long time causes loss of interest • It is critical relative to the rates of change in system state that the feedback loop is trying to control
10. Structure of material stocks and flows	• Plumbing structure, stock, and flows and their physical arrangement • Physical building/structure
11. Size of buffers and other stabilizing stocks relative to their flows	• Stabilizing power • Moderate buffer • Constant inventory to face occasional fluctuations
12. Constants, parameters, number (such as subsidies, taxes, standards)	• System constants or parameters • E.g., interest rate, act of firing people and hiring new ones

In the organization aspect, there are seven CSFs subordinate to it. “Service Model” risk is related to the different level of physical structure, matching leverage point 10, which refers to physical arrangement; “Outsourcing Level” risk is related to the asymmetric information flow between different cloud service providers, matching leverage point 6, which emphasizes comprehensive, timely information flow. “Scale & Structure” risk is related to business capacity whether the physical scale is enough or not to meet high business volume; it matches leverage point 11, which mentions moderate buffers and constant inventory to face fluctuations. “Fault Control” risk is related to error-correcting capability, matching leverage point 8, which means self-correcting capacity. “Business Continuity” risk is related to sustainable development ability, with business continuity as a company long-term goal; it matches leverage point 3, which refers to the entire system goal of growth and development. “Contract (SLA)” and “Internal Security Policy & Regulation” are terms and rules established by the company itself, and their risk is related to half-baked or disputed rules; both of them match leverage point 5, which mentions the system rules and contract compliance.

In the process aspect, there are four CSFs subordinate to it. “Feedback Loops” risk is related to the lack of monitoring and feedback information, matching leverage point 6, which also means information feedback. “Data Update” risk is related to the lack of reinforcement of system; it means patching or software updating process, matching leverage point 7, which refers to self-reinforcing. “Auditing (business, data traffic, security)” risk is related to wrong or inaccurate auditing, matching leverage point 8, which mentions self-correcting and accuracy of monitoring; “External Standards & Laws” risk is related to the lack of constant and uniform standards, matching leverage point 12, which describes the effectiveness regarding constants and parameters.

In the people aspect, there are two CSFs subordinate to it. “Human Resource” risk is related to the lack of talented persons, matching leverage point 4, which refers to system education and brains addition; “Staff Reliability” risk is related to malicious insider, and it is related to staff recruitment and termination. This matches leverage point 12, which also mentions the act of firing people and hiring new ones.

In the technology aspect, there are seven CSFs subordinate to it. “Encryption,” “Authentication,” “Authorization,” “Identification,” and “VM Technology” are an array of technical tools. Upon scrutiny of all leverage points, there is actually no direct description of technology terms; according to the definition of technology [25], however, it involves the making, knowledge of tools, machines, and methods of organization used to solve a problem. In this regard, these technical factors all match leverage point 4, which explains the need for adding new brains or wings or computers and for system education. “Disaster Recovery” risk is related to the lack of backup resource and delayed response, matching leverage point 11, which means timely response and appropriate length of delays. “Physical Loss” can result in many kinds of risk (such as data leak and data loss), and it is a factor that destroys the physical structure; this matches leverage point 10, which defines the effectiveness of the physical structure.

Note that there is neither overlap nor vagueness among the twelve leverage points’ concepts nor umbrella term among the selected CSFs. Every selected CSF is very specific; thus, there is no one-to-many mapping connection in this process. Through the analysis above, we made the leverage points table of CSFs for the BMIS model. Table 5 clearly shows the leverage point for each subordinate factor.

Table 5. Leverage point mapping for the BMIS model's subordinate factors

	Elements	Subordinate CSFs	Mapping Leverage Point
BMIS Model	Organization (design/strategy)	1. Business Continuity	**3**
		2. Contract (SLA)	**5**
		3. Internal Security Policy & Regulation	**5**
		4. Outsourcing Level	**6**
		5. Fault Control	**8**
		6. Service Model	**10**
		7. Scale & Structure	**11**
	Process	1. Feedback Loops	**6**
		2. Data Update	**7**
		3. Auditing (business, data traffic, security)	**8**
		4. External Standard & Laws	**12**
	People	1. Human Resource	**4**
		2. Staff Reliability	**12**
	Technology	1. Encryption	**4**
		2. Authentication	**4**
		3. Authorization	**4**
		4. Identification	**4**
		5. VM Technology	**4**
		6. Disaster Recovery	**9**
		7. Physical Loss	**10**

3.3.2 Final model confirmation

After leverage point mapping, the cloud-applied, integrated, leveraged BMIS model comes into view. Fig. 2 presents the subordinate CSFs of every element, with the leverage points shown behind each factor.

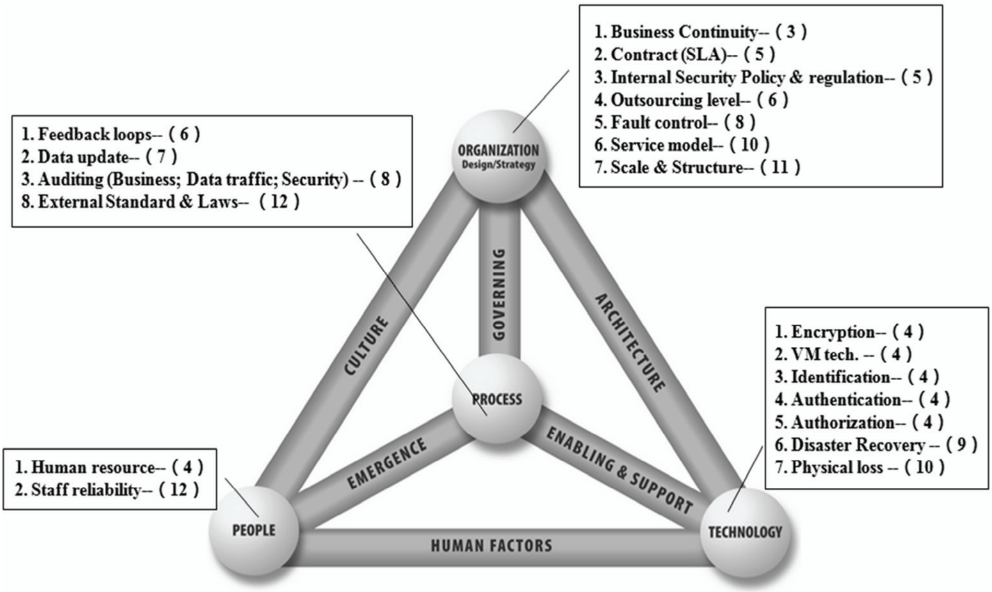
1. Business Continuity-- (3)
2. Contract (SLA)-- (5)
3. Internal Security Policy & regulation-- (5)
4. Outsourcing level-- (6)
5. Fault control-- (8)
6. Service model-- (10)
7. Scale & Structure-- (11)
1. Feedback loops-- (6)
2. Data update-- (7)
3. Auditing (Business; Data traffic; Security) -- (8)
8. External Standard & Laws-- (12)
ORGANIZATION
Design/Strategy
GOVERNING
CULTURE
ARCHITECTURE
1. Encryption-- (4)
2. VM tech. -- (4)
3. Identification-- (4)
4. Authentication-- (4)
5. Authorization-- (4)
6. Disaster Recovery -- (9)
7. Physical loss -- (10)
PROCESS
EMERGENCE
ENABLING & SUPPORT
1. Human resource-- (4)
2. Staff reliability-- (12)
PEOPLE
HUMAN FACTORS
TECHNOLOGY

Fig. 2. Leveraged BMIS model-controlled area in cloud service activity

The figure above shows a risk control model at the business level in the cloud environment. Based on the original BMIS model, considering the cloud environment, we found the Critical Success Factors (CSFs) of each component.

For the organization aspect, there are seven subordinate CSFs attached to it. In this aspect, “Business Continuity” requires the most attention, matching the practical role of the organization character since all efforts and governance by organization are geared toward maintaining the stability and development of a system. Second, “Contract (SLA)” and “Internal Security Policy” will require your equal attention, which means paperwork is relatively effective in this aspect. Then, “Outsourcing Level,” “Fault Control,” “Service Model,” and “Scale & Structure” come into the list in that order.

For the process aspect, there are four subordinate CSFs included. “Feedback Loops” rank first in this aspect, which means regular monitoring of information flow is relatively important in process governance. “Data Update” and “Auditing” process subsequently come into the list. The one requiring least investment in this aspect is “External Standard & Law,” which will not cause a big change in running a system.

For the people aspect, there are only two CSFs under this component: “Human Resource” and “Staff Reliability.” It is important to note that “Human Resource” is deemed much more significant than “Staff Reliability,” which further illustrates that the sufficiency of talented persons is more effective in keeping the system stable and securing value-added.

For the technology aspect, there are seven CSFs under this component. “Encryption,” “Authentication,” “Authorization,” “Identification,” and “VM Technology” are ranked in the first level of this aspect. This is reasonable because “Encryption,” “Authentication,” “Authorization,” and “Identification” are actually a set of processes carried out at the same time, with the “VM Technology” risk closely bound with them. “Physical Loss” is ranked in the second level, and “Disaster Recovery” is last on this list, which means that, compared with the response time and backup data, more attention needs to be paid to physical materials or devices.

After the separate analysis of the model components, we will look at them on a global level. There are actually twenty CSFs subordinate to this model, following a holistic approach to the statistics.

All in all, there are twenty CSFs in charge of cloud risk in our leveraged model. Through statistics, these twenty CSFs are labeled in ten different levels.

“Business Continuity” is ranked at the top among all CSFs. The mapping leverage point is 3, which again proves that the goal of controlling other risks is control of business continuity risk.

“Human Resource,” “Encryption,” “Authentication,” “Authorization,” “Identification,” and “VM Technology” are ranked at the second level. The corresponding mapping leverage point is 4. It make sense that human resource is always side by side with the technology factor, so we need to invest equal energy and time in these aspects.

“Contract (SLA)” and “Internal Security Policy & Regulation” are at the third level. The corresponding mapping leverage point here is 5.

“Feedback Loops” and “Outsourcing Level” are ranked at the fourth level. The corresponding mapping leverage point here is 6.

“Data Update” is at the fifth level. The corresponding mapping leverage point here is 7.

“Auditing (business, data traffic, security)” and “Fault Control” are ranked at the sixth level. The corresponding mapping leverage point here is 8.

“Disaster Recovery” is at the seventh level. The corresponding mapping leverage point here is 9.

“Physical Loss” and “Service Model” are ranked at the eighth level. The corresponding mapping leverage point here is 10.

“Scale & Structure” are at the ninth level. The corresponding mapping leverage point here is 11.

“External Standard & Laws” and “Staff Reliability” are ranked at the tenth level. The corresponding mapping leverage point here is 12.

To give a snapshot of the aforesaid contents, Table 6 lists CSFs’ leverage points ranking as follows:

Table 6. Subordinate CSFs ranking from a holistic approach

Subordinate CSF Ranking	Mapping Leverage Point
1. Business Continuity	**3**
2. Human Resource 2. Encryption 2. Authentication 2. Authorization 2. Identification 2. VM Technology	**4**
3. Contract (SLA) 3. Internal Security Policy & Regulation	**5**
4. Feedback Loops 4. Outsourcing Level	**6**
5. Data Update	**7**
6. Auditing (business, data traffic, security) 6. Fault Control	**8**
7. Disaster Recovery	**9**
8. Physical Loss 8. Service Model	**10**
9. Scale & Structure	**11**
10. Staff Reliability 10. External Standard & Laws	**12**

Note that there is no subordinate factor mapping with leverage points 1 and 2. This is fair and reasonable because all CSFs are under the charge of four elements (organization, process, people, and technology) of the BMIS model. CSFs are at the management level, which is concretely in charge of specific risk by macro-control. In comparison, the four elements are at the governance level, which is responsible for micro-control. Thus, the effectiveness of CSFs may be lower than the elements, meaning leverage points 1 and 2 may fall off the leverage points mapping list. For instance, the element “organization” can map with leverage point 1 due to its power to transcend the paradigm.

Unlike other cloud risk control models [1,2], this approach utilizes the approved BMIS model. Compared with other risk control methods, this business model enjoys more recognition and acceptability. Unlike the traditional risk model, it always isolates the security responsibility and business targets. The BMIS model is labeled as the combination of information security program and business goals.

Furthermore, it innovatively uses the leverage points to improve business effectiveness. This approach describes in detail the specific reason for leverage point mapping with each factor and element. Meanwhile, based on previous research, this model digs up the essential cloud risk factors in practical cloud service; thus, risk control is directly focused on the realistic problems in cloud computing.

In actual business administration, there is always interaction between macro-control and micro-control; thus, the discovered essential risk factors and the model element can be flexibly used in actual business admisitration.

Compared with Microsoft's internal cloud layer control, we described the practical significance of our presented model. The relation between CSFs and elements and the practical implication will be illustrated in the next section.

From a practical perspective, Fig. 3 is an internal control mechanism of cloud layers in Microsoft [26]. The business object is the three cloud layers (SaaS, PaaS, IaaS) and data foundation; the periphery is macro-control by policies, standards, and procedures. In the middle are the control objectives, with the final layer distributing control activities for these cloud layers.

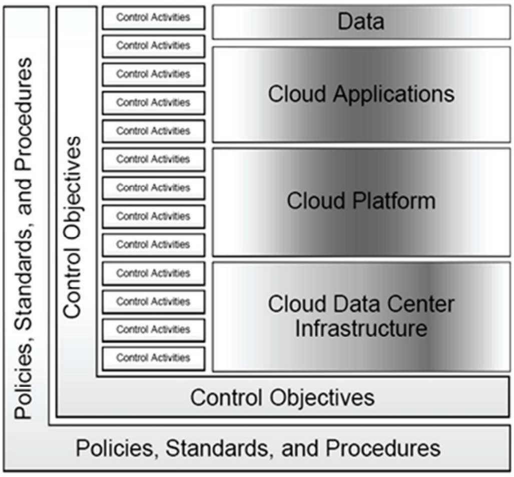
Policies, Standards, and Procedures
Control Objectives
Control Activities
Data
Cloud Applications
Cloud Platform
Cloud Data Center Infrastructure
Control Objectives
Policies, Standards, and Procedures

Fig. 3. Internal control mechanism of cloud layers in Microsoft [26]

For reference, Microsoft gives us a good guide to cloud controlling. Combining the leveraged BMIS model we presented, we can design a cloud risk control model as shown in Fig. 4 below.

In Fig. 4, the first peripheral is the BMIS model; the leveraged BMIS model as micro-control includes policies, standards, and procedures. The second peripheral is the four elements of the BMIS model, which can be regarded as the control objectives. We then insert the twenty cloud risk factors that we summarized in this paper in the third peripheral. As cloud risk management factors, the twenty factors can take effect on micro-control. Finally, we can distribute the specific control activities on different cloud layers.

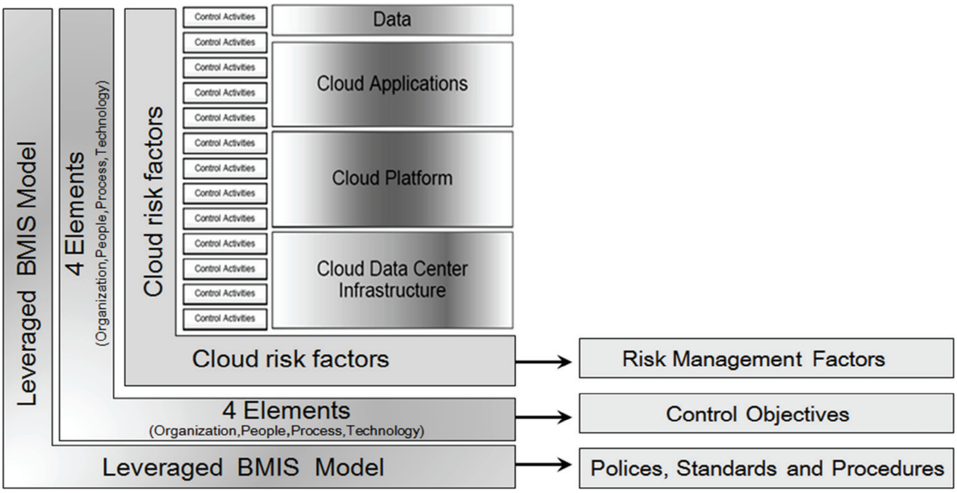

Fig. 4. Leveraged BMIS model execution in a practical case

In the cloud service industry, the risk always points to bi-direction, and both cloud service providers and cloud service clients can be subject to damage. Traditional security models tend to incorporate the in-house environment, regard outsourcing or third party as a business issue that is only addressed at the contractual or legal level. The leveraged BMIS model is highly applicable to the cloud environment; it is an interactive, dynamic model that can act on both internal and external sides. Thus, both cloud service providers and client enterprises can use this model to manage and reduce the risk. More and more types of service will gradually move to the cloud -- cloud broadcasting, for example – and the leveraged BMIS model can be applied to more different cloud enterprises in practice.

4. Conclusion and Future Work

Security problems always coincide with economic and business problems. The risks will certainly be more severe in a cloud environment. After a study on several risk control models, we found the specific meaning of the existing BMIS model in information security governance: it is a perfect combination of information security and business value developed by ISACA. In this paper, first, through review and study on the existing literature, we have reclassified the risks based on the described key factors, and then explored and selected CSFs (Critical Success factors) from the summarized cloud risk and connected them with the BMIS model. Finally, we found the leverage point for each of them by mapping with the well-known “twelve leverage points” by Meadows. The main purpose of this paper is to control and prevent the existing cloud risks by using the leveraged BMIS model. According to our previous research, there is hardly any article that applies the BMIS model to cloud computing. This leveraged BMIS model, which stands at a business level, makes every effort to optimize the allocation of resources in cloud computing by using leverage points. It carries out the policy of putting prevention first and combining prevention with control at the same time; every aspect in this model interacts with each other, and anyone changing or mishandling it will break the balance of this model.

The significance of this paper lies in the fact that we applied and leveraged the BMIS model to the cloud service environment.

Nonetheless, this paper has some shortcomings and insufficiency. First of all, to target making a model focusing on cloud risk, understanding how many kinds of existing or potential cloud risks there are is very important. Since the cloud computing area is still in a growth stage, there are probably still some areas we have not tackled. Lever accuracy is the second problem. The research method of this paper is mapping relation, which can only describe qualitatively the CSFs' leverage point ranking. To advance this model, qualitative description and quantitative analysis need to be part of the agenda. Every risk control effort or management aims at business profit and continuity in the end. Every quantitative decision-making method can be taken into account, such as AHP and Delphi method [27].

In future work, we will try to use a quantitative method such as AHP to enhance the utilization rate of this model and strive to get a more precise hierarchical BMIS model for the cloud service environment.

REFERENCES

[1] G. Zhao, "Holistic framework of security management for cloud service providers," in *Proceedings of the 10th IEEE International Conference on Industrial Informatics*, Beijing, China, 2012, pp. 852-856.

[2] Z. Guo, M. Song, and J. Song, "A governance model for cloud computing," in *Proceedings of the International Conference on Management and Service Science*, Wuhan, China, 2010, pp. 1-6.

[3] J. J. Hwang, H. K. Chuang, Y. C. Hsu, and C. H. Wu, "A business model for cloud computing based on a separate encryption and decryption service," in *Proceedings of the International Conference on Information Science and Applications*, Jeju, Korea, 2011, pp. 1-7.

[4] C. C. Lo, *Information Security and Its Impact on Business*. Hsinchu, Taiwan: National Chiao-Tung University, 2006.

[5] R. von Rössing, "Applying BMIS to cloud security," *in ISSE 2010 Securing Electronic Business Processes*, N. Pohlmann, H. Reimer, and W. Schneider, Eds. Berlin, Germany: Vieweg+Teubner Verlag, 2011, pp. 101-112.

[6] S. Sembhi, "The business model for information security," in *RSA Conference Europe*, London, UK, 2010.

[7] D. Meadows (1999). *Leverage points: places to intervene in a system* [Online]. Available: http://www.donellameadows.org/archives/leverage-points-places-to-intervene-in-a-system/

[8] Information Systems Audit and Control Association (ISACA) (2010). *An introduction to the business model for information security* [Online]. Available: http://www.isaca.org/Knowledge-Center/Research/Documents/Introduction-to-the-Business-Model-for-Information-Security_res_Eng_0109.pdf

[9] Information Systems Audit and Control Association (ISACA) (2010). *ISACA issues new comprehensive business model for information security* [Online]. Available: http://www.isaca.org/About-ISACA/Press-room/News-Releases/2010/Pages/ISACA-Issues-New-Comprehensive-Business-Model-for-Information-Security.aspx

[10] R. D. Daniel, "Management information crisis," *Harvard Business Review*, vol. 39, no. 5, pp. 111-121, 1961.

[11] J. F. Rockart, "Chief executives define their own data needs," *Harvard Business Review*, vol. 57, no. 2, pp. 81-93, 1979.

[12] C. V. Bullen and J. F. Rockart, "A primer on critical success factors," Alfred P. Sloan School of Management, Center for Information Systems Research, Working Paper No. 69, 1981.

[13] Wikipedia. *Critical* Success *Factor* [Online]. Available: http://en.wikipedia.org/wiki/Critical_success_factor#cite_note-4

[14] R. A. Caralli, "The critical success factor method: establishing a foundation for enterprise security

management," Carnegie Mellon University, Pittsburgh, PA, Technical Report CMU/SEI-2004-TR-010, 2004.

[15] J. S. Wang, C. H. Liu, and G. T. R. Lin, "How to manage information security in cloud computing," in *IEEE International Conference on Systems, Man, and Cybernetics*, Anchorage, AK, 2011, pp. 1405-1410.

[16] D. Vohradsky, "Cloud risk: 10 principles and a framework for assessment," *ISACA Journal*, vol. 5, pp. 31-41, 2012.

[17] Wikipedia. *Lever* [Online]. Available: http://en.wikipedia.org/wiki/Lever#cite_note-1

[18] Cloud Security Alliance (CSA) (2010). *Top Threats to Cloud Computing V1.0* [Online]. Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[19] V. Mukhin and A. Volokyta, "Notice of violation of IEEE publication principles security risk analysis for cloud computing systems," in *Proceedings of the IEEE 6th International Conference on Intelligent Data Acquisition and Advanced Computing Systems*, Prague, Czech Republic, 2011, pp. 737-742.

[20] W. A. Jansen, "Cloud hooks: security and privacy issues in cloud computing," in *Proceeding of the 44th Hawaii International Conference on System Sciences*, Kauai, HI, 2011, pp. 1-10.

[21] Y. Kadam, "Security issues in cloud computing: a transparent view," *International Journal of Computer Science & Emerging Technologies*, vol. 2, no. 5, pp. 316-322, 2011.

[22] J. Brodkin, "Gartner: seven cloud-computing security risks," *InfoWorld News* [Online]. Available: http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853

[23] S. K. B. Tammaiah, "Cloud computing data security internet and web system2-term paper," unpublished.

[24] D. Firesmith, "Specifying reusable security requirements," *Journal of Object Technology*, vol. 3, no. 1, pp, 61-75, 2004.

[25] Wikipedia. *Technology* [Online]. Available: http://en.wikipedia.org/wiki/Technology

[26] Y. Li, "Security & standards in the Cloud: building trust through openness and interoperability in the Cloud," unpublished.

[27] P. Saripalli and B. Walters, "QUIRC: a quantitative impact and risk assessment framework for cloud security," in *Proceedings of the IEEE 3rd International Conference on Cloud Computing*, Miami, FL, 2010, pp. 280-288.

YouJin Song

He received a Ph.D. degree in Information Security from Tokyo Institute of Technology, Japan in 1995. He has been a professor at Dongguk Univ. since 1996. His research interests include privacy protection, secret sharing, cloud security and its application, multimedia security.

Yasheng Pang

She received a master degree in Electronic Commerce Technology from Dongguk University, Korea in 2013. Her research interests include cloud security, risk management, data mining and cloud broadcasting.