J Inf Process Syst, Vol.10, No.1, pp.132~144, March 2014
http://dx.doi.org/10.3745/JIPS.2014.10.1.132
pISSN 1976-913X
eISSN 2092-805X

How to Manage Cloud Risks Based on the BMIS Model

Youjin Song* and Yasheng Pang*

Abstract—Information always comes with security and risk problems. There is the saying that, "The tall tree catches much wind," and the risks from cloud services will absolutely be more varied and more severe. Nowadays, handling these risks is no longer just a technology problem. So far, a good deal of literature that focuses on risk or security management and frameworks in information systems has already been submitted. This paper analyzes the causal risk factors in cloud environments through critical success factors, from a business perspective. We then integrated these critical success factors into a business model for information security by mapping out 10 principles related to cloud risks. Thus, we were able to figure out which aspects should be given more consideration in the actual transactions of cloud services, and were able to make a business-level and general-risk control model for cloud computing.

Keywords—Cloud Risk, Risk Control, Cloud Computing, BMIS, CSFs

1. INTRODUCTION

Nowadays, ubiquitous (or pervasive) computing, including ambient intelligence, augmented reality, or proactive computing [1], is a hot topic in the information area. Cloud computing is a typical technology in this field. Meanwhile, the cloud risks or security problems have become "hot potato" issues that hinder an enterprise's adoption of cloud services to some degree. For many years, information security has been viewed as a technical issue just focused heavily on process and technology. Figure 1 is a survey conducted by PwC in 2010, the x-axes show the percentage of survey respondents who reported impacts that the current economic downturn has had on their companies' security functions.

Though this figure, we can see the reasons for, and the problems we need to face in, information security. Not only technical security, but also regulations and cost considerations at the business level should be taken into account.

Today, more and more people are becoming gradually aware of the importance of management in information security. The concept of the management information system (MIS) was first presented in a comptroller's handbook [2], which now is a set course in most business schools and is even conferred as a degree in Master's or PhD programs [3]. So far, a lot of research and literature has been published in the field of cloud security management. Among

※ This research was supported by 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 April 24, 2013; accepted December 11, 2013.
Corresponding Author: YouJin Song (song@dongguk.ac.kr)
* Dept. of Information Management, Dongguk University, Gyeongju, 780-714, Korea (song@dongguk.ac.kr, pangpang7117@gmail.com)

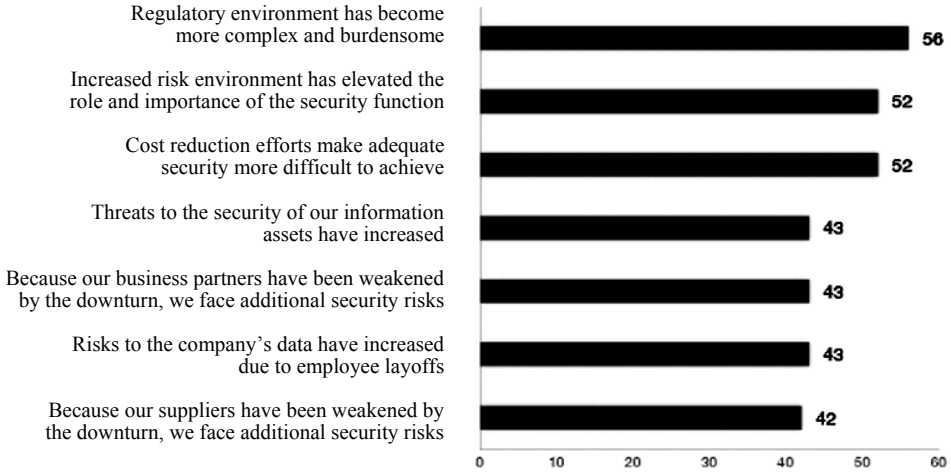

Fig.1. PwC 2010 the global state of information security [26]

these papers, including from works on the conceptual SLA framework [4], is a citation of a variety of classic standards (such as ISO 20000, ISO 27002, SOX, COBIT) [5,6,7]. Some other papers have submitted a new management model or framework in cloud security. Guo et al. [8] proposed a governance model for cloud computing based on the governance objectives in the cloud. However, this model is premised on a cloud service users perspective and is complicated to operate. Meanwhile, Zhao [7] put forward a holistic framework of security management based on a cloud service provider (CSP) position, and described an array of processes in security management. But what we need is a more integrated, or to some degree, more universal model for controlling cloud risks, especially one that can connect on a business level and contribute to benefitting an enterprise. In this regard, some models try to connect on a business level. For instance, Hwang et al. [9] suggested a business model that was adopted by at least two different CSPs and that can support encryption and decryption separately (see Figure 2 below).

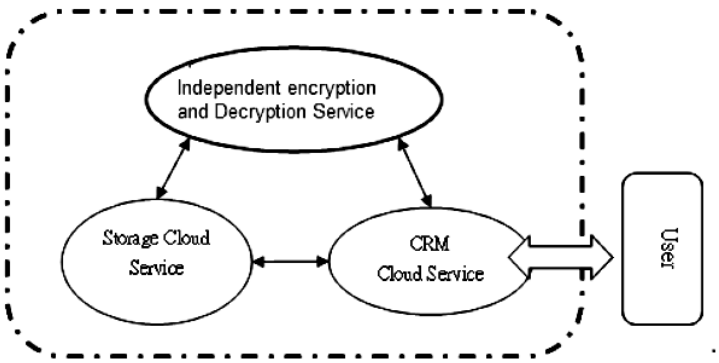

Fig. 2. Business model concept that integrates separate cloud services for data encryption/decryption, CRM, and storage [9]

The model in Figure 2 may be a fairly good method for decreasing security risks in cloud computing, but it increases the complexity of customer relationships and implicit costs, and it also lacks feasibility. Lo [10] also described a business model for information security, but the model itself seems complicated, and the elements in this model need to be much more systematic. Von Rössing [25] combined COBIT with the Business Model for Information Security (BMIS) and offered some recommendations for the daily operation of the BMIS. Some methods have tried to integrate the management paradigm with critical factors and other requirements in cloud security. Colella and Colombini [1] suggested the centrality of the human factor (other factors are organization and technical factors) and a dynamic approach to both external and internal threats. Ramgovind et al. [11] discussed information security requirements and control methods in cloud computing. The purpose of this paper is to make a simple and effective business model to control these integrated security factors in cloud computing.

BMIS was issued by the Information Systems Audit and Control Association (ISACA) in 2010 [12], which takes a business-oriented, holistic, and dynamic approach to managing information security [13]. Critical Success Factors (CSFs) which were defined by John F. Rockart [14], refer to vital elements that can help an organization accomplish its mission and determine its success. In our previous research, we proposed a cloud-risk table that integrated nearly all of the security problems and risks in cloud computing. In this paper, we will show how we figured out the integrated CSFs based on the integrated risk table, the security factors, and on the requirements mentioned in other literature [11,12,13,14] and try to combine them with the BMIS. Then we made a dynamic, effective, general and integrated business model that focuses on cloud risk control at the enterprise level.

The remainder of this paper is structured as follows: Section 2 gives a literature review and some details on every formational theory. Section 3 proposes the business model to achieve risk-control functions, which connect with selected critical factors. We suggest further work and give our conclusions in Section 4.

2. RELATED WORK

2.1 BMIS

The history of BMIS traces back to a project at the USC Marshall School of Business. ISACA then got the right to develop it in 2008 [13], and officially published this model in October 2010 [12]. There are four elements and six dynamic interconnections in the construction of this model. The four elements are: the organization, people, the process, and technology. The six interconnections are: governing, culture, enabling and support, emergence, human factors, and architecture. The shape of this model is shown in Figure 3 below.

In Figure 3, one may just think that the model is just a “process-centered” triangle. However, it is worth noting that this is a three-dimensional, pyramid-shaped structure. According to ISACA, it is a model that can be predictive and proactive, and that it is not just concerning traditional information security but includes issues related to privacy, linkage to risks, physical security, and compliance [13]. It is a dynamic, integrated and general risk control model for cloud computing, which is what we need.

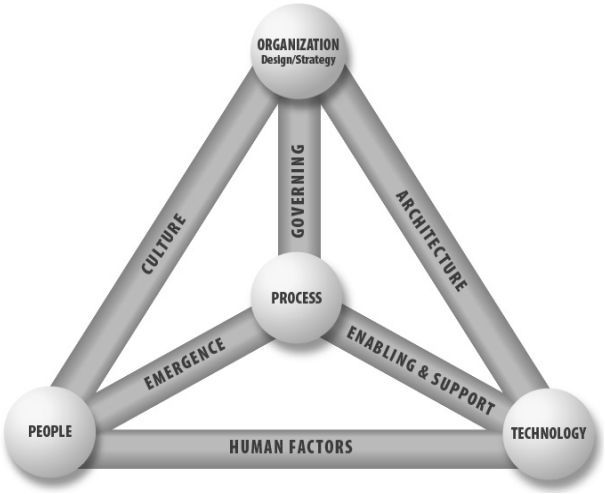

Fig.3. Business model for information security [14]

2.2 CSFs

Daniel put forward the concept of "success factors" in 1961 [16]. Rockart developed it as "critical success factors" in one of his publications in 1979 [17], and refined it in another paper in 1981 [18]. CSFs 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 [19]. Richard aligned CSFs with enterprise security management and stated that CSFs have shown promise in helping organizations not only guide and direct themselves but also doing what with the order of action, which contributes to security strategies and managing security at the enterprise level [20]. Richard demonstrated the importance and definitiveness of CSFs in security management, and Richard et al. hierarchized them through the FAHP (Fuzzy Analytic Hierarchy Process) and used it in the cloud environment [21]. But the CSFs in this paper just review the literature on information security management, but do not focus on practical risks in the cloud computing environment, and do not take into consideration all of the types of risks in a realistic cloud environment. CSF selection that focuses on integrated risks in the cloud computing environment and that takes into consideration requirements in the security or governance level, are vital for our business model building.

2.3 Ten principles for cloud computing

David Vohradsky, who has more than 25 years of experience in information and security management, presented 10 principles for cloud computing risks, based on the BMIS [22], and demonstrated an assessment framework for cloud risks through a case study. The publication [22] describes four guiding principles as a cloud assessment road map, and 10 detailed principles that connect with the BMIS. We have summarized them in Table 1 below.

Table 1. Ten principles and related concepts [22]

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 are they accountable?	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 risks in the cloud	Enabling and support
		10. Best practices must be followed in the cloud	Emergence

The significant point from Table 1 is that we can map the critical cloud risk factors with both the four guiding principles and the 10 detailed principles, according to the definition of every principle.

3. MODEL BUILDING

3.1 The selection of factors

In our previous research, we presented an integrated cloud risk table in another paper (see in Table 2), which classified the concrete cloud risks into five areas and twelve specific risks in detail. The CSA top threat's format [15], which is a document from CSA (Cloud Security Alliance), covers almost all risks or security problems in the practical cloud service transaction.

Table 2. Integrated cloud risks

Risk Classification	Specific Risk
Technology Problem	1. Insecure interfaces & APIs 2. Shared technology issues 3. Abuse/Nefarious use of cloud computing 4. Account or service hijacking
Trust Problem	5. Malicious insiders 6. Composite service's risk
Data Problem	7. Data leakage 8. Data loss: Temporary & Permanent 9. Lack of update / Patching
Compliance Problem	10. Inappropriate SLA/QoS & Lack of standards 11. The regional differences between different Laws & Regulations
Measurability Problem	12. Metering & Billing Errors

Consider the old Chinese proverb of, "Know yourself and know your enemy; you will win every war." Similarly, you must find the reason for the problems, and then find the solution to deal with them. There are five types of risks in the integrated cloud risk table, which are as follows: technology problems, trust problems, data problems, compliance problems, and measurability problems. We will present our analyzation of the causal factors based on the concrete risk. We also seriously considered other perspectives on issues, such as cloud security requirements and other factors in the cloud security area. For instance, Guo et al. [8] summarized four factors in the security management model and Ramgovind [11] concluded that there are six security requirements in cloud computing. Iankoulova and Daneva [23] took a systematic review of cloud security requirements based on Firesmith's Security Quality Factors [24], etc. The reason for requirements in factor selection is not just because of the causal factors, but because coincidence with security requirements is a good, integrated way to define our CSFs in cloud risks. Among all the reviews, Wang and et al. [21] and Firesmith [24] are more comprehensively analyzed, especially in terms of requirements and security factors. We chose their methods and in Table 3 we classified their methods into five areas to compare with our integrated causal risk factors.

Table 3. Comparison of key factors and security requirements [16][21][24]

	Causal Factors [16]	**Security Quality Factors [24]**	**Key Factors [21]**
Technology Problem	1. Encryption technology 2. VM technology 3. Access control 4. ID management 5. Authentication 6. Authorization	1. Access control (identification; authentication; authorization) 2. Attack/ Harm detection 3. Non-repudiation 4. Integrity (data integrity) 7. Privacy (anonymity)	11. Technical capability 12. Interface 14. Infrastructure 15. Encryption 17. Authentication
Trust Problem	1. Staff reliability 2. Human resources 3. Contract (cloud nesting) 4. Organization 5. Governance 6. Visibility & Transparency	4. Integrity (personnel)	5. Resource 6. Scale & structure 9. Service model 10. Strategies 13. Outsourcing level 18. Fault control 20. Training plan 21. MIS staffing 22. Feedback loops
Data Problem	1. Data leakage 2. Data update 3. Physical loss 4. DR (Disaster Recovery) 5. BC (Business Continuity)	4. Integrity (hardware) 4. Integrity (software) 6. Physical protection 7. Privacy (confidentiality) 8. Recovery	16. Data recovery 19.Disclosure prevention
Compliance Problem	1. Contract (SLA) 2. Internal security policy & regulations 3. External standards & laws		1. Regulation 2. Standards & protocols 8. Security policy
Measurability Problem	1. Business auditing 2. Data auditing	5. Security auditing	23. Auditing
Others		9. Prosecution	3. Competitor 4. Customer 7. Cost

Through comparison and analysis, we ultimately chose 20 items to constitute the critical success factors in our model, as seen in Table 4.

Table 4. CSFs' selection based on Table 3

Technology	Trust	Data	Compliance	Measurability
1. Encryption 2. VM technology 3. Identification 4. Authentication 5. Authorization	6. Staff reliability 7. Human resources 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, and security)

In this table, we integrated all of the possible factors from Table 2, removed the essential causal factors, and ensured that there were no overlaps. For instance, "access control" or "interface" is referred to in a lot of the literature on security, but if we examine these problems they are all about "identification," "authentication," "authorization," and "non-repudiation," as mentioned by Firesmith [24], which can actually be covered by encryption using the digital signature technique. Some of the items are very conceptual, such as "visibility & transparency," "organization," and "governance." We define them as more concrete factors under "contract (cloud nesting)." "Visibility & transparency" can be under the "service model;" "outsourcing level" and "organization" can be under "scale & structure;" and "governance" can be under "fault control" and "feedback loops."

3.2 The connections between factors

Making the connections is the most crucial part and is also a challenge in the process of model building. Because most of the factors are not absolutely independent, every factor possibly has an intricate connection with every other factor. For example, the concept of "governing" is an umbrella term, and almost every factor can more or less connect with it. Thus there may well be some overlapping factors in the finished classification model.

BMIS is actually comprised of just 4 elements and the other 6 dynamic interconnections are relationship links. To avoid duplication in the model, we designed it as follows: first, according to the 10 principles, we classified all 20 CSFs into four elements individually. (See Table 5.)

According to the concept of each factor, the factor concepts that coincide with the principle requirements should be connected with the relevant element. We thoroughly read the principles in detail, selected the keywords for each relevant principle and listed them in Table 5.

"Service model" and "outsourcing level" initially posses risks. "Fault control" needs to keep monitoring; "business continuity" is the long-term goal, which creates the direction for a cloud company; "scale & structure" need a physical establishment, while "contract (SLA)" and "internal security policy & regulation" need a textual establishment. These factors all match the principle of an "organization" element.

"Human resource" is a keyword in the "people" element principle and "staff reliability" demands a recruitment, transfer, and termination process. These two factors meet the principle of the "people" element.

"Feedback loops" emphasize the symmetry of information flow, which needs sufficient communication between different groups. "Data update" ensure process can get the appropriate

Table 5. Connection with BMIS elements

BMIS Elements	Keywords Mentioned in Each Relevant Principle Requirement	Connected CSFs
Organization (design/strategy)	Own the risk Establishment Direction Monitoring	8. Service model 9. Outsourcing level 10. Scale & structure 11. Fault control 16. Business continuity 17. Contract (SLA) 18. Internal security policy & regulation
People	Who is using it Human resources Recruitment Transfers Terminations	6. Staff reliability 7. Human resources
Process	Align with the policy Meet business requirements Communication Appropriate resources	12. Feedback loops 13. Data update 19. External standards & laws 20. Auditing (Business; Data traffic; Security)
Technology	What is put in CIA (confidentiality, integrity, and availability)	1. Encryption 2. VM technology 3. Identification 4. Authentication 5. Authorization 14. Physical loss 15. Disaster recovery

resources in the system. “External standards & laws” is the policy we should conform and align with. “Auditing (business, data traffic, and security)” is done in order to ensure that there are no mistakes in bill auditing, data traffic measurements, and security assessments, which businesses also require in their corporate operations. These factors all match the principle of the “process” element.

“Encryption, authentication, authorization and identification” are a series of approaches to ensure the confidentiality and integrity of data. “Disaster recovery” concerns data availability and “physical loss” is right related to “what’s put in” in a system. These factors all match with the principle of the “technology” element. That means CSFs in the two neighboring elements automatically become interconnection factors. In order to keep the typicality and normalization of every dynamic interconnection, and in light of the 10 principles, we again chose the closest factors in the two neighboring elements to make up the dynamic interconnections. (See Table 6.)

First, “governing” connects the “organization” and “process” elements, so the factors involved in these two elements should be take into consideration. From among these factors, “fault control” and “feedback loops” require oversight and continuous monitoring. “Contract (SLA),” “internal security policy & regulations,” “external standards & laws,” and “auditing” require compliance with the laws, policies, and regulations. These factors match the “governing” interconnection principle.

Second, “human factors” connect the “people” and “technology” elements. The factors that are involved in these two elements should be taken into consideration when doing connection. From among the factors that are involved in connection, just “human resources” matches the commensurate knowledge and accountability requirements, which is the principle of the “human

factors" interconnection.

Table 6. Connection with BMIS interconnections

BMIS Dynamic Interconnection	Keywords Mentioned in Each Relevant Principle Requirement	Connected CSFs
Governing	Oversight Continuous monitoring Compliance with laws, policies, regulations	11. Fault control 12. Feedback loops 17. Contract (SLA) 18. Internal security policy & regulations 19. External standards & laws 20. Auditing
Human factors	Commensurate knowledge Accountability	7. Human resources
Architecture	Security management building Cloud investments	10. Scale & structure 14. Physical loss 15. Disaster recovery
Culture	Compliance Appropriate use Client commitment	6. Staff reliability 17. Contract (SLA) 18. Internal security policy & regulations 19. External standards & laws
Enabling and support	Monitoring Information risk reporting Escalation process	13. Data update 20. Auditing (Business; Data traffic; Security)
Emergence	Practices System development Address information risks	7. Human resources 12. Feedback loops 13. Data update

Third, "architecture" combines the "organization" and "technology" elements. From among the factors that are involved in these two elements, "scale & structure" and "physical loss" can impact the "building" and "cloud investment factor. "Disaster recovery" should be a part of "security management." These factors match the "architecture" interconnection principle.

Fourth, "culture" combines the "organization" and "people" elements. From among the factors that are involved in these two elements, "staff reliability" refers to appropriate use requirement, "contract(SLA)" refers to client commitment requirements, and "internal security policy & regulation" and "external standards & laws" refer to compliance requirements. These match the "culture" interconnection principle.

Fifth, "enabling and support" combines the "process" and "technology" elements. From among the factors that are involved in these two elements, only "data update" and "auditing (business, data traffic, and security)" match the information risk reporting and escalation process of the related principle of requirements.

Lastly, "emergence" combines the "process" and "people" elements. From among the factors that are involved in these two elements, "human resources" are critical to system development and "feedback loops" and "data update" keep the practice going and reduce the address information risks. These match the "emergence" interconnection principle.

3.3 Cloud risk model implementation based on BMIS

After considering the factor connections, the integrated, dynamic, and effective risk control model at the business level in the cloud environment comes into view. The control area for the elements and the interconnection control objects are shown in Figures 4 and 5.

Figure 4 is the graphic embodiment of Table 5. The specific instructions for CSFs' mapping reasons have already been discussed in the previous paragraph. The CSFs' "service model," "outsourcing level," "scale & structure," "fault control," "business continuity," "contract

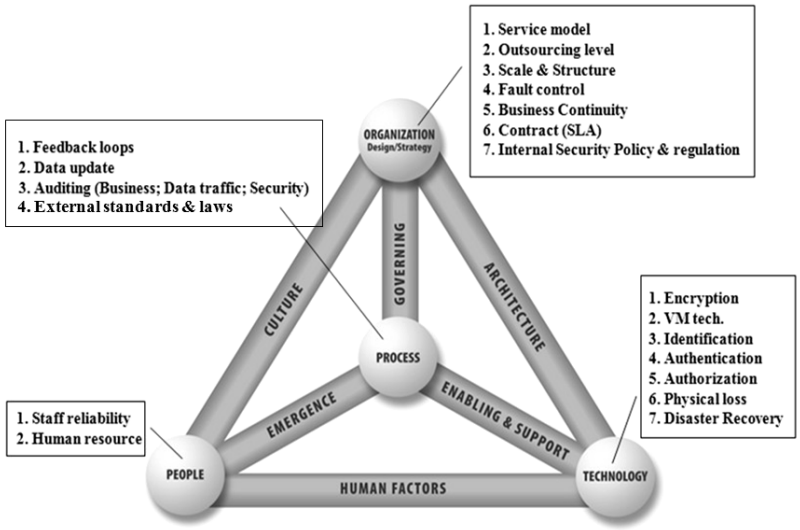

Fig. 4. The BMIS control area for the elements in a cloud environment

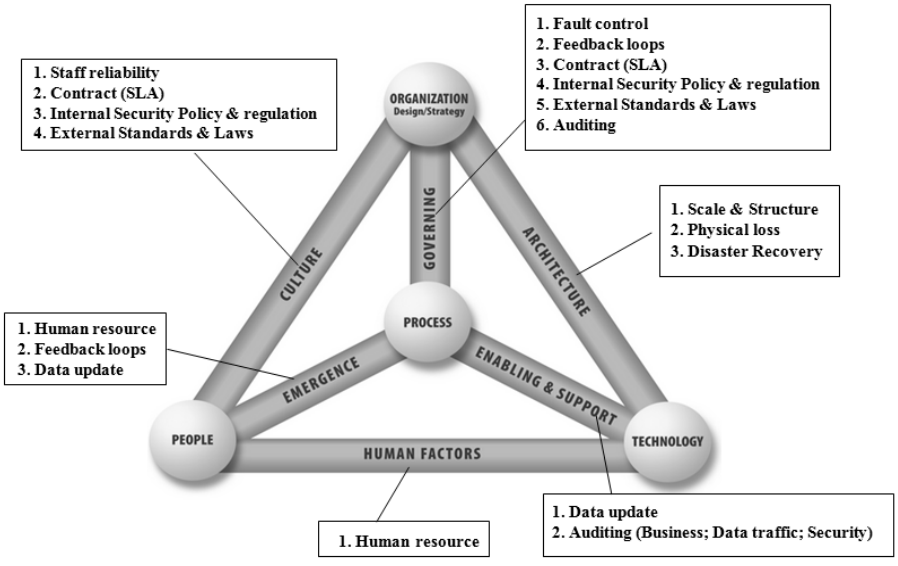

Fig. 5. The BMIS interconnection control objects in a cloud environment

(SLA)," and "internal security policy & regulations" belong to the "organization" element. The CSFs' "encryption," "VM technology," "identification," "authentication," "authorization," "physical loss," and "disaster recovery" belong to the "technology" element. The CSFs' "feedback loops," "data update," "external standards & laws," and "auditing (business, data traffic, and security)" belong to the "process" element. The CSFs' "staff reliability" and "human resources" belong to the "people" element.

Figure 5 is the graphic embodiment of Table 6. The CSFs' "fault control," "feedback loops," "contract (SLA)," "internal security policy & regulations," "external standards & laws," and "auditing" are under the control of the "organization" interconnection. The CSFs' "human resources" is under the control of the "human factor" interconnection. The CSFs' "scale & structure," "physical loss," and "disaster recovery" are under the control of the "architecture" interconnection. The CSFs' "staff reliability," "contract (SLA)," "internal security policy & regulations," and "external standards & laws" are under the control of the "culture" interconnection. The CSFs' "data update" and "auditing (business, data traffic, and security)" are under the control of the "enabling and support" interconnection. The CSFs' "feedback loops," "data update," and "human resources" are under the control of the "emergence" interconnection.

Every element and interconnection requires more consideration and focus to be given to their subordinate CSFs in the cloud service environment. For example, "People" includes the two critical factors of staff reliability and human resources. Thus, we must pay more attention to recruitment and background checks, MIS staff development skills, training plans, etc. In this case, BMIS' orientation puts prevention first and combines prevention with control in managing existing cloud risks. Every aspect in this model interacts with the other elements. If anyone changes or mishandles BMIS interconnection, it will break the balance of this model. The proper function of this proactive, risk-predictive, and dynamic model requires us to control the model and to keep it in balance at every moment.

4. CONCLUSION AND FUTURE WORK

Security problems always coincide with economic and business problems. The risks certainly will be more severe in a cloud environment. In this paper, we presented measures to prevent and control risks in cloud computing by using the BMIS model. We explored and integrated the crucially casual factors that lead to risks in the cloud computing environment and connect them with BMIS elements. We carries out the policy of putting prevention first and combining prevention with control at the same time, and we built up a dynamic and risk-aware model that can be used in a cloud environment.

In the future, solutions and risk control should not just remain at the question of how to solve these risks. The business level needs to be addressed in terms of how we can obtain the maximum achievements by using the minimum amount of resource investments, which is a very important issue. Every risk control effort by security management aims at business profit and continuity in the end. Every decision-making method, such as the AHP (Analytic Hierarchy Process) and Delphi methods [21][27], can be considered. For future work, we will try to figure out a leverage point to enhance the utilization of this model.

REFERENCES

[1] Antonio Colella, Clara Colombini, "Security Paradigm in Ubiquitous Computing", 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp 634-638, available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6296928

[2] Office of the Comptroller of the Currency, "Management Information Systems", 1995, available at: http://www.occ.gov/publications/publications-by-type/comptrollers-handbook/mis.pdf

[3] Wikipedia, available at: http://en.wikipedia.org/wiki/Management_information_system

[4] Mohammed Alhamad, Tharam Dillon, Elizabeth Chang, "Conceptual SLA Framework for Cloud Computing", 4th IEEE International Conference on Digital Ecosystems and Technologies, 2010, pp 606-610, available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5610586

[5] Zhitao Huang, Pavol Zavarsky, Ron Ruhl, "An Efficient Framework for IT Controls of Bill 198 (Canada Sarbanes-Oxley) Compliance by Aligning COBIT 4.1, ITIL v3 and ISO/IEC 27002", International Conference on Computational Science and Engineering, 2009, pp 386-391, available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5283287

[6] Shamsul Sahibudin, Mohammad Sharifi, Masarat Ayat, "Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations", Second Asia International Conference on Modelling & Simulatio, 2008, pp 749-753, available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4530569

[7] Gang Zhao, "Holistic Framework of Security Management for Cloud Service Providers", 10th IEEE International Conference, 2012, pp 852-856, available at: http://ieeexplore.ieee.org/ stamp/stamp.jsp?tp=&arnumber=6301237

[8] Zhiyun Guo, Meina Song, Junde Song, "A Governance Model for Cloud Computing", Management and Service Science (MASS), 2010 International Conference, available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5576281

[9] Jing-Jang Hwang, Hung-Kai Chuang, Yi-Chang Hsu, Chien-Hsing Wu, "A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service", Information Science and Applications (ICISA), 2011 International Conference, available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5772349

[10] Chiao-chun Lo, "Information Security and Its Impact on Business", 2006, available at: http://www.iim.ncku.edu.tw/download.php?filename=180_acdf887c.ppt&dir=news&title=%E6%AA%94%E6%A1%88%E4%B8%8B%E8%BC%89

[11] Ramgovind S, Eloff MM, Smith E, "The Management of Security in Cloud Computing", 2010, available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5588290

[12] ISACA, 2010, available at: http://www.isaca.org/About-ISACA/Press-room/News- Releases/2010/Pages/ISACA-Issues-New-Comprehensive-Business-Model-for-Information-Security.aspx

[13] ISACA, "An Introduction to the Business Model for Information Security", available at: http://www.isaca.org/Knowledge-Center/BMIS/Documents/IntrotoBMIS.pdf

[14] Wikipedia, available at: http://en.wikipedia.org/wiki/Critical_success_factor#cite_note-4

[15] CSA, "Top Threats to Cloud Computing V1.0", 2010, available at: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[16] Daniel, D. Ronald, "Management Information Crisis," Harvard Business Review, Sept.-Oct., 1961.

[17] Rockart, John F. "Chief Executives Define their Own Data Needs", published in "Harvard Business Review", March 1979, available at: http://www.ope.co.kr/nbuilder/include/download.php?name=%C3%D6%B0%ED%B0%E6%BF%B5%C0%DA%B0%A1+%BF%F8%C7%CF%B4%C2+%C1%A4%BA%B8.pdf&key=53&dir=board_data/tb_ib_2541&mode=DOWN

[18] Rockart, John F. "A Primer on Critical Success Factors", published by the Center for Information Systems Research, 1981, available at: http://mit.dspace.org/bitstream/handle/1721.1/1988/SWP-1220-08368993-CISR-069.pdf?sequence=1

[19] Wikipedia, available at: http://en.wikipedia.org/wiki/Critical_success_factor#cite_note-4

[20] Richard A. Caralli , "The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management", published by Carnegie Mellon University, 2004, available at: http://www.sei.cmu.edu/reports/04tr010.pdf

[21] JenSheng Wang, CheHung Liu, Grace TR Lin, "How to Manage Information Security in Cloud Computing", Systems, Man, and Cybernetics (SMC), 2011 IEEE International Conference, pp 1405-1410, available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6083866
[22] David Vohradsky, "Cloud Risk—10 Principles and a Framework for Assessment", ISACA JOURNAL VOLUME 5, 2012, pp. 31-41, available at: http://www.candorsolutions.co.za/wp-content/uploads/2012/09/12v5-Cloud-Risk-10-Principles.pdf
[23] Iliana Iankoulova, Maya Daneva, "Cloud Computing Security Requirements:a Systematic Review", Research Challenges in Information Science (RCIS), 2012 Sixth International Conference, available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6240421
[24] Donald Firesmith, "Specifying Reusable Security Requirements", JOURNAL OF OBJECT TECHNOLOGY, Vol.3, No.1, 2004, pp. 61-75.
[25] Rolf Von Rössing, "Applying BMIS to Cloud Security", ISSE 2010 Securing Electronic Business Processes, 2011, pp. 101-112, available at: http://link.springer.com/chapter/10.1007%2F978-3-8348-9788-6_10
[26] PwC, "2010 Global state of information security", available at: http://www.pwc.com/us/en/view/issue-12/securing-information-downturn.jhtml
[27] Prasad Saripalli, Ben Walters, "QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security", 2010 IEEE 3rd International Conference on Cloud Computing, 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.