Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2016 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

Summer 6-27-2016

RISK FACTORS OF ENTERPRISE INTERNAL CONTROL: GOVERNANCE REFERS TO INTERNET OF THINGS (IOT) ENVIRONMENT

She-I Chang
National Chung Cheng University, actsic@ccu.edu.tw

Albert Huang
University of the Pacific, ahuang@pacific.edu

Li-Min Chang
National Chung Cheng University, changclm@gmail.com

Jhan-Cyun Liao
National Chung Cheng University, crazybearb@gmail.com

RISK FACTORS OF ENTERPRISE INTERNAL CONTROL: GOVERNANCE REFERS TO INTERNET OF THINGS (IOT) ENVIRONMENT

She-I Chang, Department of Accounting and Information Technology, National Chung Cheng University, Chiayi, Taiwan, actsic@ccu.edu.tw

Albert Huang, Eberhardt School of Business, University of the Pacific, USA, ahuang@pacific.edu

Li-Min Chang, Department of Accounting and Information Technology, National Chung Cheng University, Chiayi, Taiwan, changclm@gmail.com

Jhan-Cyun Liao, Department of Accounting and Information Technology, National Chung Cheng University, Chiayi, Taiwan, crazybearb@gmail.com

Abstract

This study aims to investigate enterprise risk factors for governing the risk of Internet of Things (IoT) environment. Under the guidance of Gowin's Vee knowledge map strategy, this study reviewed the related literature and used Delphi expert questionnaire to construct and revise the defined risk factors. Two rounds of expert survey were conducted. A total of 24 experts from the fields of information technology, audit management, and risk management were selected to conduct the questionnaire survey. Eighty-three question items were obtained and categorized into various types of risk factors including environment, process, decision-making, operation, authority, data processing and information, moral, and finance. These factors were categorized according to the consistent opinion of experts. Program SPSS 12.0 was adopted to analyze feedback information from expert questionnaire by conducting statistical analyses and validity testing. All risk factors were integrated and designed carefully, supplemented by verification through statistical value of mean, inter-quartile range, and content validity ratio (CVR). The results of this research can be used as reference in the study of risk factors under IoT governance, and to enhance the development of knowledge on qualitative research. Further, in the new generation of IoT governance practice, the related factors of enterprise risk management can be regarded as key measurement items in internal control and auditing.

Keywords: Risk factors, Enterprise internal control, IT governance, Internet of Things, Qualitative research

1 INTRODUCTION

With the rapid development of Information and Communication Technologies (ICTs), Internet of Things (IoT) has resulted in numerous applications of new generation IT and serving as an important bridge between people and people, things and things, and people and things worldwide (Gubbi et al. 2013; Madakam et al. 2015). Gartner, an international research and advisory body, has reported that in 2015, the number of networked objects under the environment of Internet of Things (IoT) continued to grow daily by 5.50 million. In 2016, the number of global networked things will reach 6.4 billion, representing an increase of 30% from the number in 2015. By 2020, this number is predicted to increase by 20.8 billion. In terms of economic efficiency, the amount of service expenditure driven by IoT in 2016 will be 235 billion US dollars, representing an increase of 22% compared with that in 2015 (Gartner 2015). It is foreseen that enterprises will transmit a large amount of business information through wired network, wireless network, tooth, cloud services, and Internet under the environment of IoT. Enterprise information system will also generate and collect business transaction data through the operation of an intelligent device, to promote the processing, analysis, and application of Big Data (Barnaghi et al. 2013; Perera et al. 2014).

As noted, when this innovative technology is widely adopted, new information security problems will also occur, including business transactions without authorization, high-level executives hiding the information on losses of companies, unsaved transaction records, hackers attacking IoT device/information system, and other problems that will raise new threats to the modern enterprises (Boyd & Crawford 2012; Madakam et al. 2015). Particularly, potential new threats and risk factors in IoT environment differ significantly from that in the past. If enterprises still carry out internal control by using existing audit mechanism or information security architecture, enterprises would fail to obtain existing results; business operations with many potential risks will have an influence on IT governance and operating performance of enterprises (Gubbi et et al. 2013; Weber 2010). However, in the increasingly complex environment of IoT, performing tasks effectively in IoT governance may not only assist enterprises in responding to the changes and challenges from emerging technologies, but also reducing operational risks and enhancing the physical fitness of an enterprise to improve its competitiveness in the peer settings (Debreceny & Gray 2013; Weill & Ross 2004). For risk factors that may occur in IoT, distinguishing, analyzing, and designing an appropriate audit mechanism become urgent and practical, in response to IT governance of enterprises under IoT. Thus, based on academic and practical needs, this study aims to enhance IT governance through an in-depth investigation of risk factors under IoT governance. Specifically, this study aims to achieve the following objectives: (1) define and classify the key risk factors that influence the performance of enterprises under IoT governance; (2) verify the effectiveness and feasibility of risk factors under IoT governance.

2 LITERATURE REVIEW

2.1 IT Governance under IoT

The technology of Internet of things (IoT) has being broadly applied throughout the global service market. IoT technology aims to deliver real-time messages through a common platform, through either wired network, wireless network (e.g., blue tooth and RFID), GPS, or cloud computing method, with the aim of understanding, providing a warning, communicating, or monitoring case situations (Babar et al. 2010). Weber (2010) pointed out that IoT is widely applied especially in the global supply chain network. The IoT services provided are highly diverse, and the type of information technologies, the people, and matters involved are extremely complicated, thus, new problems regarding IoT network security and privacy that threaten the operations of enterprises have also occurred continually. IT governance aims to manage IT investments by achieving authority and control mechanism to enable the accomplishment of the mission entrusted by the organization. IT governance further aims to ensure the realization of the organization's business objectives through risk monitoring and control, efficiency

adjustment, and value adding. IT governance refers to an expected behavior to encourage IT applications by regarding clear decision-making authority and responsibility as the framework (Weill & Ross 2004). Therefore, the acquisition of maximum value from IT depends on the expected behavior toward IT applications. Expected behavior depends on whether an organization's beliefs and culture firmly demonstrate the needs of IT applications, including an outline of company values, mission, business rules, and agreed behavior and structure, to name but a few. Moreover, the implementation of IT governance strategy in the specific acts should be meaningful. To have an understanding of risk factors under IoT governance is the key to perform effective risk management (Babar et al. 2010; Beasley et al. 2005). Formulating a set of mechanisms through audit strategy and internal control action as a follow up is an important approach to implement risk management (Kober et al. 2007; Spira & Page 2003).

2.2 Risk Factors of Enterprise Internal Control and its Category

A good enterprise internal control should consider the various risks that an organization faces in different departments or operational stages, and provide an effective management mechanism to prevent the occurrence of risks in the science and technology environment. In addition, presenting a clear hierarchy to classify the risk factors can result in effective risk management (Beasley et al. 2005; Sutton et al. 2008). Thus, in order to understand the type of enterprise risk factors, this study broadly reviewed the manuals and literature in the fields of IS, economics, and governmental operations regarding the risk and crisis management to identify IoT-related influences. The result can be discussed from two aspects, namely, general enterprise risk factors and IT risk factors.

For general enterprise risk factors, the US Committee of Sponsoring Organization (COSO), issued an internal control and integration framework in 1992, and supplemented some contents in 1994. Since the release of the COSO framework, it has been approved gradually by formulation authorities of the world's internal control guidelines, and has become the international general internal control guidelines. COSO 2013 is a revised edition based on the 1992 framework. The component factors of internal control are divided into five control dimensions, namely, control environment, risk evaluation, information and communication, and supervision. In addition, the Centre for Economics and Business Research in the UK further provided eight types of intersecting risks including environment, process, decision-making, operation, authority, data processing and information, moral, and finance. The eight categories cover 73 indices, which can be used as an important reference for the study of risk management. Accordingly, the relevant categories provide an important insight for this study to construct the risk checklist for enterprise internal control. For IT risk factors, the development of IT has been an important strategy for obtaining business advantage in recent years. The investigation of risk factors under IoT governance has also become the focus of studies on computer audit and information security (Feng 2014; Barnaghi et al. 2013; Sood 2012). It is noted that the characteristics of IoT environment are having multiple agents connecting various users, services, and devices among different Networks. Having a multi-level security mechanism is needed to ensure the management of information flow. Kato et al. (2014) pointed that a multi-agent based infrastructure is vital to realize flexible cooperation and service composition among IoT devices, and is fundamental in performing the relevant request tasks in IoT environment. According to the European Telecommunications Standards Institute, IoT DCM has the following three levels: Device, Connection, and Management. The three layer communication architecture can provide security protection in managing the risk of Internet of Things in the Cloud and relevant Network. The DCM dimensions not only provide a simple and effective method to enhance risk management, but also promote IoT risk management for enterprise internal control.

3 RESEARCH METHOD, DESIGN, AND DATA ANALYSIS

This study adopts a qualitative research method to explore enterprise risk factors in the IoT. In order to obtain a set of reasonable research procedures, Gowin's Vee knowledge map and Delphi method are

adopted as the foundation for research and development. Gowin's Vee knowledge map is a type of effective learning strategy and knowledge management tool, the core concept of which is to establish a knowledge system based on the problem (Gowin 1981; Novak & Gowin 1984; Novak 1990). Therefore, in the early stage of research and development, the collection of concepts and integration of theories can be based to construct static knowledge. The Delphi method is referred to as expert methodology and is commonly used in the collection of expert knowledge. This method aims to send the questions individually to seek urgent solutions from experts by communicating and consulting with them based on intuitive judgment of expert experience (Dalkey & Helmer 1963; Linstone & Turoff 1975). After obtaining expert comments, the method collects, organizes, and sorts out a comprehensive view that is used as basis for reversion.

This study initially sorted enterprise risk factors under IoT governance based on the Gowin's Vee knowledge map, and then revised the risk factors and questionnaire prototype by using the Delphi expert questionnaire. Questionnaire release procedure covered the following steps: (1) establishing an expert team; (2) designing an expert questionnaire; (3) releasing questionnaire to experts; (4) sorting and revising feedback opinions from experts; (5) confirming the validity of all question items using verification analysis; and (6) producing a report on enterprise risk factors under IoT governance. Two rounds of expert survey were conducted. The questionnaire survey in the first round aimed mainly to revise the inconsistent problems and supplementations on the original questionnaire opinions of experts. The questionnaire was administered from June 12 to 25, 2015. The expert questionnaire in the second round was intended to enable the experts to confirm the results from the first round. The second round of questionnaires were administered June 26 to July 3, 2015. In the survey on the number of people, many scholars emphasize the suitability of a small-scale expert team when conducting the Delphi operation, as it would be easier to achieve expert validity than when a large-scale expert team is used. The most suitable number of experts is between 10 and 50 (Hill & Fowles 1975; Linstone & Turoff 1975). Accordingly, based on the requirements of the survey, a total of 24 experts from information technology, audit management, and risk management were selected to conduct the questionnaire survey.

This research uses SPSS 12.0 to analyze feedback information from expert questionnaire by conducting data analysis and validity testing of various risk factors. For example, Average is used to observe the importance of risk factors; Quartile Deviation (IQR) is used to analyze the consistency of expert opinion; and Content Validity Ratio (CVR) is adopted to check the content validity of all question items to ensure its ability to detect the features and functions of IoT risk factors in all dimensions (Churchill 1979; Lawshe 1975; Hair et al. 2006; Hair et al. 2006). Twenty-four experts judged the risk factors, and hence, the CVR should greater than the threshold value (> 0.42) (Lawshe 1975). We further added the options of "Belonging" or "Not belonging" in the various items of the questionnaire in this paper to screen out inappropriate items. These options were used to enable experts to determine the appropriateness of the item. From the results of the data analysis, an item should be deleted if it fails to meet the principle of consistency. Based on the Delphi operation and statistical test, however, inappropriate items were deleted after two rounds of feedback and revision by the experts. Eighty-three question items were obtained from the various types of risk factors such as environmental, process, decision-making, operational, authority, data processing and information, moral, and financial risk; these factors were categorized through the consistent opinion of experts. Table 1 illustrates the recovery situation of expert questionnaire. Table 2 shows the analysis results of enterprise risk factors under IoT governance.

Questionnaire	Field of Experts	Number of experts in Round 1	Recovery ratio	Number of experts in Round 2	Recovery ratio
Enterprise risk factor under IoT governance	Information technology	12	50.0%	11	47.8%
	Auditing	7	29.2%	7	30.4%
	Risk management	5	20.8%	5	21.7%
	Total	24	100.0%	23	100.0%

Table 1. Recovery situation of expert questionnaire

Risk categories	IoT DCM Levels	No.	Risk factors	Belonging to IoT environment			Importance					
				Round 1	Round 2	Belonging	Round 1			Round 2		
				CVR	CVR		Mean	IQR	Mode	Mean	IQR	Mode
Environ-mental risk	C: Network	1.C.1	Loophole of sharing technology	1.00	-	Y	4.38	0.50	4	-	-	-
		1.C.2	Difficulties in compliance	0.58	-	Y	3.42	0.50	4	-	-	-
		1.C.3	Supply chain failure	0.42	0.74	Y	3.04	2.50	4	3.83	0	4
		1.C.4	Performing a malicious detection or scan	0.92	-	Y	4.25	0.50	5	-	-	-
		1.C.5	Risk changes from legal impact	0.83	-	Y	3.71	0.25	4	-	-	-
		1.C.6	Attack of social engineering	0.75	-	Y	3.46	0.63	4	-	-	-
		1.C.7	Unsafe wireless communication channel	0.92	-	Y	4.58	0.50	5	-	-	-
		1.C.8	Natural disasters	0.33	0.91	Y	2.67	1.63	0	3.43	0.5	3
		1.C.9	Complexity of virtual machine management	0.50	-	Y	3.17	0.50	4	-	-	-
		1.C.10	Definition of communication standard/specifications	0.67	-	Y	3.38	0.75	4	-	-	-
	D:Perception	1.D.1	Power consumption of node equipment	0.33	0.65	Y	2.63	1.25	4	3.17	0.5	3
		1.D.2	Personnel health problems	**-0.17**	**-0.57**	**N**	**1.88**	**2.00**	**0**	**1.13**	**1.5**	**0**
Process risk	M: Application	2.M.1	Invasion of privacy	1.00	-	Y	4.67	0.50	5	-	-	-
		2.M.2	Lack of integration	0.92	-	Y	4.54	0.13	5	-	-	-
	D: Perception	2.D.1	Invasion of privacy (location privacy)	0.92	-	Y	4.58	0.13	5	-	-	-
		2.D.2	Message eavesdropping	1.00	-	Y	4.67	0.50	5	-	-	-
		2.D.3	Betrayal of secrets	0.75	-	Y	3.75	0.50	4	-	-	-
Decision-making risk	C: Network	3.C.1	Problems concerning auditing and searching	0.83	-	Y	4.00	0.50	5	-	-	-
		3.C.2	Long-term and permanent outage	0.58	-	Y	3.38	1.00	5	-	-	-
Operational risk	M: Application	4.M.1	Emergency management strategy for fault	0.67	-	Y	3.83	0.50	5	-	-	-
	C:Network	4.C.1	Lack of governance mechanism	0.58	-	Y	3.54	1.00	4	-	-	-
		4.C.2	The behavior of the other tenants causing the company to suffer damage.	0.75	-	Y	3.87	0.00	4	-	-	-
		4.C.3	Insufficient resources	0.67	-	Y	3.58	0.63	4	-	-	-
		4.C.4	Economic interruption service	0.75	-	Y	3.88	1.00	5	-	-	-
		4.C.5	Conflict between customer's Solidification Procedure (Rigorous Procedure) and Cloud environment	0.92	-	Y	4.17	0.50	4	-	-	-
		4.C.6	The lack of trust between the data provider and the data user	0.58	-	Y	3.38	0.50	4	-	-	-
	D: Perception	4.D.1	False label	0.75	-	Y	3.67	0.63	4	-	-	-
		4.D.2	Equipment update/ version control	1.00	-	Y	4.38	0.50	4	-	-	-
Authority risk	M: Application	5.M.1	Access control	0.92	-	Y	4.08	0.50	5	-	-	-
		5.M.2	Data ownership	0.83	-	Y	3.58	0.50	4	-	-	-
		5.M.3	Data sharing with third party groups	0.50	-	Y	3.04	0.88	4	-	-	-
	C:Network	5.C.1	Termination or failure of cloud services	1.00	-	Y	4.71	0.13	5	-	-	-
		5.C.2	Cloud service providers are merged	1.00	-	Y	4.50	0.50	5	-	-	-
		5.C.3	Privilege escalation	0.83	-	Y	4.25	0.50	5	-	-	-
Data processing and information risk	M: Application	6.M.1	Denial of service	1.00	-	Y	4.63	0.50	5	-	-	-
		6.M.2	Identity authentication	1.00	-	Y	4.58	0.50	5	-	-	-
		6.M.3	Software vulnerability and protection mechanism	1.00	-	Y	4.67	0.50	5	-	-	-
		6.M.4	Need new professional skills	1.00	-	Y	4.75	0.13	5	-	-	-
		6.M.5	Robust system easy to use	0.83	-	Y	4.17	0.50	5	-	-	-
		6.M.6	Processing, filtering, and mining of massive data	0.92	-	Y	4.58	0.50	5	-	-	-
	C: Network	6.C.1	Data leakage	0.83	-	Y	4.21	0.50	5	-	-	-
		6.C.2	Data loss	0.25	0.91	Y	2.38	2.00	4	3.61	0.5	4

Risk categories	IoT DCM Levels	No.	Risk factors	Belonging to IoT environment			Importance					
				Round 1	Round 2	Belonging	Round 1			Round 2		
				CVR	CVR		Mean	IQR	Mode	Mean	IQR	Mode
		6.C.3	Account or service is invaded	0.67	-	Y	3.92	0.50	5	-	-	-
		6.C.4	Unsafe interface and application program interface (API)	0.92	-	Y	4.46	0.50	5	-	-	-
		6.C.5	DoS (denial of service), DDoS (discrete denial of service)	0.92	-	Y	4.42	0.50	5	-	-	-
		6.C.6	Data access control security and data separation	0.83	-	Y	4.00	0.50	5	-	-	-
		6.C.7	Data recovery and reliability	1.00	-	Y	4.71	0.50	5	-	-	-
		6.C.8	Be confined to the same platform	0.75	-	Y	3.79	0.50	5	-	-	-
		6.C.9	Isolation measures failure	0.67	-	Y	3.67	0.63	5	-	-	-
		6.C.10	Interception of data during transmission	1.00	-	Y	4.50	0.50	5	-	-	-
		6.C.11	Data leakage during loading/unloading	0.92	-	Y	4.42	0.50	5	-	-	-
		6.C.12	Deletion of unsafe or invalid data	0.75	-	Y	3.83	0.63	5	-	-	-
		6.C.13	Encryption key is lost	0.83	-	Y	3.92	0.63	5	-	-	-
		6.C.14	Compromise service engine	0.50	-	Y	3.00	0.50	4	-	-	-
		6.C.15	Summons and electronic search	0.75	-	Y	3.54	0.63	4	-	-	-
		6.C.16	Data protection risk	0.75	-	Y	3.63	0.25	4	-	-	-
		6.C.17	Document risk	1.00	-	Y	4.67	0.50	5	-	-	-
		6.C.18	Network outage	1.00	-	Y	4.79	0.00	5	-	-	-
		6.C.19	Network management	0.92	-	Y	4.00	0.63	5	-	-	-
		6.C.20	Modify network traffic	0.92	-	Y	4.42	0.50	5	-	-	-
		6.C.21	The compromise of lost or operating logs	1.00	-	Y	4.63	0.50	5	-	-	-
		6.C.22	The compromise of lost or security logs	0.67	-	Y	3.46	0.50	4	-	-	-
		6.C.23	Backup is lost or stolen	1.00	-	Y	4.21	0.50	4	-	-	-
		6.C.24	Unauthorized access	0.92	-	Y	4.50	0.50	5	-	-	-
		6.C.25	Data storage location	0.75	-	Y	3.46	0.63	4	-	-	-
		6.C.26	Virtual network protection	0.92	-	Y	4.21	0.50	5	-	-	-
		6.C.27	Client protection	0.83	-	Y	3.88	0.50	4	-	-	-
		6.C.28	Temporary failure	0.92	-	Y	4.21	0.50	4	-	-	-
		6.C.29	Processing and storage of large amounts of data	0.92	-	Y	4.50	0.50	5	-	-	-
	D: Perception	6.D.1	DoS attack	0.92	-	Y	4.38	0.50	4	-	-	-
		6.D.2	Communication flow analysis	0.67	-	Y	3.58	0.63	4	-	-	-
		6.D.3	Key security data packet loss	1.00	-	Y	4.21	0.50	5	-	-	-
		6.D.4	The use of well-known protection mechanism	0.92	-	Y	4.08	0.50	4	-	-	-
Moral risk	M: Application	7.M.1	Data leakage	0.67	-	Y	3.96	0.50	5	-	-	-
		7.M.2	Malicious internal staff	0.83	-	Y	4.17	0.50	5	-	-	-
	C: Network	7.C.1	Malicious internal staff	0.67	-	Y	3.54	0.63	4	-	-	-
		7.C.2	Malicious concealment of cloud service providers	1.00	-	Y	4.58	0.50	5	-	-	-
		7.C.3	Management interface compromise	1.00	-	Y	4.50	0.50	5	-	-	-
Financial risk	C: Network	8.C.1	Abuse of cloud service	0.67	-	Y	3.46	0.50	4	-	-	-
		8.C.2	Not doing enough service survey	0.83	-	Y	3.25	0.50	4	-	-	-
		8.C.3	Maintenance cost for equipment and network	0.50	-	Y	3.33	0.63	4	-	-	-
	D: Perception	8.D.1	Physical attack	0.83	-	Y	3.88	0.50	4	-	-	-
		8.D.2	Maintenance cost for equipment	0.75	-	Y	3.54	0.50	4	-	-	-
		8.D.3	Equipment is stolen	0.92	-	Y	4.13	0.50	5	-	-	-

Table 2. Risk factors under IoT governance

4 CONCLUSIONS

This study aims to investigate enterprise risk factors under IoT governance. Under the guidance of Gowin's Vee knowledge map strategy, review of related literature and Delphi expert questionnaire are used to construct and revise the defined risk factors. All risk factors are integrated and designed carefully, supplemented by verification through statistical software (e.g., mean, inter-quartile range, CVR). Data analysis results had high reliability and validity. The results of this research can be used as reference in the study of risk factors under IoT governance, and to enhance the development of knowledge on qualitative research. Further, in the new generation of IoT governance practice, the related factors of enterprise risk management can be regarded as a key measurement items in internal control and auditing.

4.1 Implications for Academia

Qualitative research method is a commonly used research method in the field of social science and education. Qualitative research has many advantages, including exploration through nature, inductive analysis, comprehensive view, use of qualitative data, individual contact and in-depth understanding, typical and particular cases used as orientation of the study, and an elastic research design (Cooper & Schindler 2001; Roche et al. 2014). Compared with quantitative research, qualitative research offers additional focus through the survey of small-size sample. Hence, qualitative research can not only provide in-depth individual observations of the study, but also assist further in generating information or knowledge of an individual case. However, qualitative research also has certain disadvantages, particularly when personal information and the method of understanding of researchers are insufficient, or when researchers fail to put forward effective analysis data. This research method has frequently been viewed as being subjective, thereby reducing the effectiveness of the research results. Therefore, proposing effective research strategies would be useful in improving the quality of the qualitative research (Seawright & Gerring 2008).

This study uses Gowin's Vee knowledge map as a research strategy to compensate for the limitations of qualitative research. Under the systematic guidance of this method, an in-depth investigation was conducted, starting from the formulation of a theoretical framework. A prototype version of the questionnaire is developed sequentially from the overall concept of literature, theory, principle and concept (Fox 2007; Gowin 1981; Novak & Gowin 1984). The Delphi method is used repeatedly to test, provide feedback, and revise the questionnaire (Dalkey & Helmer 1963; Hanafin 2004). SPSS statistical software is further used to analyze and interpret various risk factors (Ledesma & Valero-Mora 2007) as well as to complete the arrangement of enterprise risk factors under IoT governance. In this research, massive data to support the detection results of the statistical measurement and the reported materials were not found. Nevertheless, through strict qualitative strategy, method, and design of the method of investigation, the obtained IoT enterprise risk factors and research process constructed in this research can be used as reference for studies in related fields.

4.2 Implications for IoT Governance

IT governance of enterprises has focused mostly on risk management and the implementation of internal control audit system. In an increasingly complex IoT environment, the applications of related technologies (e.g., cloud computing, mobile instruments, RFID, and wireless network) have grown rapidly in the global service market. In the face of rapid change and technical innovations of the IoT environment, enterprises should not only establish their own competitive business information mode, but also construct a risk-oriented security protection mechanism necessary to guarantee their digital future (Babar et al. 2010; Debreceny & Gray 2013; Xue et al. 2008; Yoo 2010).

In this research, a group of experts (i.e., experts in information technology and risk management) suggest that IoT-related activities should transmit and connect networking materials in a series through technical connections among all segments. Therefore, process risk management is extremely important

for an enterprise to maintain the control of its safety in the IoT environment. Moreover, moral risk management cannot be ignored. Steps should be taken to prevent internal staff from committing fraud, such as buying and selling out, creating fake accounts, conducting illegal practices, seeking illegal interests, and infringing on the interests of investors and shareholders. Furthermore, internal staff with malicious intentions could also leak data or hide operational events through application-level or network-level cloud services. These malicious acts are important moral risk management items that need to be addressed. Accordingly, this paper suggests that enterprises enhance moral risk management, in addition to focusing extra attention to risk control of the flow of data transmission and receipt. In this manner, the performance of enterprises in internal control and auditing can be enhanced.

The applications of IoT-related technologies result in operational efficiency and convenience for enterprises. However, the question of whether subsequently expected enterprise risk can be controlled effectively under existing policies requires further study. No standard or audit mechanism can provide an enterprise with the necessary auditing. Under such a demand, this paper identifies eight categories of enterprise risk factors based on a literature review (e.g., environment, process, decision, operation, authority, information processing and technology, moral risk, and financial risk), and classifies these risk factors based on three levels of framework of IoT DCM (e.g., network, perception, and application), to constitute the reference for enterprises to execute internal control. These results could assist enterprises in discovering possible potential risks in an IoT environment as well as in performing effective safety supervision of internal control.

4.3 Limitations and Future Research

This study strives to achieve precision and objectivity of the research process during the development of enterprise risk factors under IoT governance. However, the lack of time, manpower, as well as financial and other factors contribute to several limitations.

First, only 24 experts were involved in this study. Although these experts have the necessary professional backgrounds and practical experiences, and thus can assist us in defining risk factors, the limited number of samples result in a weak extrapolation of the research results. To address this deficiency, future studies could use these results as basis for expanding the implementation of a case study or in conducting a multi-round industry survey, thereby refining and creating additional IoT risk factors from the study results.

Second, this study does not create a case study of a multinational group or company and the risk factors investigated. Therefore, risk evaluation does not apply to foreign enterprises. Hence, future studies could conduct in-depth investigations on the risk factors of a multinational company under IoT governance to supplement the deficiencies of this study.

Third, this paper only investigated risk factors, but does not raise a feasible plan for enterprises to execute auditing mechanism or control method. Accordingly, further studies is recommended for the establishment of internal control and auditing system against risk management, resulting in the effect of the auditing mechanism being able to play out fully.

References

Babar, S., Mahalle, P., Stango, A., Prasad, N. and Prasad, R. (2010). Proposed security model and threat taxonomy for the internet of things. In Recent Trends in Network Security and Applications (pp. 420-429). Springer Berlin Heidelberg.

Barnaghi, P., Sheth, A. and Henson, C. (2013). From Data to Actionable Knowledge: Big Data Challenges in the Web of Things. Intelligent Systems, IEEE, 28 (6), 6-11.

Beasley, M.S., Clune, R. and Hermanson, D.R. (2005). Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. Journal of Accounting and Public Policy, 24 (6), 521-531.

Boyd, D. and Crawford, K. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. Information, communication & society, 15 (5), 662-679.
Churchill, G.A. (1979). A Paradigm for Developing Better Measures of Marketing Constructs. Journal of Marketing Research, 16 (1), 64-73.
Cloninger, D.O. (1983). Moral and systematic risk: a rationale for unfair business practice. Journal of Behavioral Economics, 11 (2), 33-49.
Cooper, D.R. and Schindler, P.S. (2001). Business research methods (7th ed.). McGraw-Hill Higher Education.
Dalkey, N. and Helmer, O. (1963). An experimental application of the Delphi method to the use of experts. Management science, 9 (3), 458-467.
Debreceny, R.S. and G.L. Gray. (2013). IT governance and process maturity: A multinational field study. Journal of Information Systems, 27 (1), 157-188.
Feng, N., Wang, H.J., and Li, M. (2014). A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. Information sciences, 256, 57-73.
Galliers, R.D. and Leidner, D.E. (2014). Strategic information management: challenges and strategies in managing information systems. Routledge.
Gartner (2015). Gartner Says 6.4 Billion Connected "Things" Will Be in Used in 2016, Up 30 Percent From 2015. Retrieved from http://www.gartner.com/newsroom/id/3165317
Gaynor, M., and Gertler, P. (1995). Moral hazard and risk spreading in partnerships. The RAND Journal of Economics, 591-613.
Gowin, D.B. (1981). Educating. New York: Cornell University Press.
Grabski, S., Leech, S.A., and Lu, B. (2001). Risks and controls in the implementation of ERP systems. The International Journal of Digital Accounting Research, 1 (1), 47-68.
Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M. (2013). Internet of Things: A vision, architectural elements, and future directions. Future Generation Computer Systems, 29 (7), 1645-1660.
Hair, J.F., Black, B., Babin, B., Anderson, R.E. and Tatham, R. L. (2006). Multivariate data analysis (6th ed.). Upper Saddle River, NJ: Pearson/Prentice Hall.
Hanafin, S. (2004). Review of literature on the Delphi Technique. Dublin: National Children's Office.
Hill, K. Q. and Fowles, J. (1975). The methodological worth of the Delphi forecasting technique. Technological Forecasting and Social Change, 7 (2), 179-192.
Holden, M.C., and Wedman, J.F. (1993). Future issues of computer-mediated communication: The results of a Delphi study. Educational technology research and development, 4 1(4), 5-24.
International Organization for Standardization. (2013). ISO/IEC 27001 - Information security management. Retrieved from http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
Kato, T., Chiba, R., Takahashi, H., Sasai, K., Kitagata, G., and Kinoshita, T. (2014, October). Multiagent-based cooperation infrastructure for IoT devices. In Consumer Electronics (GCCE), 2014 IEEE 3rd Global Conference on (pp. 571-572). IEEE.
Kober, R., Ng, J., and Paul, B. J. (2007). The interrelationship between management control mechanisms and strategy. Management Accounting Research, 18 (4), 425-452.
Krishnan, J. (2005). Audit committee quality and internal control: An empirical analysis. The accounting review, 80 (2), 649-675.
Lawshe, C. H. (1975). A quantitative approach to content validity1. Personnel psychology, 28 (4), 563-575.
Ledesma, R.D. and Valero-Mora, P. (2007). Determining the number of factors to retain in EFA: An easy-to-use computer program for carrying out parallel analysis. Practical assessment, research & evaluation, 12 (2), 1-11.
Linstone, H.A. and Turoff, M. (Eds.). (1975). The Delphi method: Techniques and applications (Vol. 29). Reading, M Gartner A: Addison-Wesley.
Madakam, S., Ramaswamy, R. and Tripathi, S. (2015). Internet of Things (IoT): A Literature Review. Journal of Computer and Communications, 3 (5), 164-173.

McGregor, C. and Schiefer, J. (2004). A Web-Service based framework for analyzing and measuring business performance. Information Systems and E-Business Management, 2 (1), 89-110.
Murry Jr, J.W., and Hammons, J.O. (1995). Delphi: A Versatile Methodology for Conducting Qualitative Research. Review of Higher Education, 18 (4), 423-36.
Novak, J. (2002). Meaningful learning: The essential factor for conceptual change in limited or inappropriate prepositional hierarchies leading to empowerment of learners. Science Education, 86 (4), 548-571.
Novak, J.D. (1990). Concept maps and Vee diagrams: Two metacognitive tools to facilitate meaningful learning. Instructional science, 19 (1), 29-52.
Novak, J.D. (1998). Learning, Creating, and Using Knowledge: Concept Maps as Facilitative Tools in Schools and Corporations. Mahwah, NJ: Lawrence Erlbaum Associates Press.
Novak, J.D. and Gowin, D.B. (1984). Learning how to Learn. England: Cambridge University Press.
Ordanini, A. and Rubera, G. (2010). How does the application of an IT service innovation affect firm performance? A theoretical framework and empirical analysis on e-commerce. Information & Management, 47 (1), 60-67.
Perera, C., Zaslavsky, A., Christen, P. and Boyd Georgakopoulos, D. (2014). Context aware computing for the internet of things: A survey. Communications Surveys & Tutorials, IEEE, 16 (1), 414-454.
Reason, J.T., and Reason, J.T. (1997). Managing the risks of organizational accidents (Vol. 6). Aldershot: Ashgate.
Roche, N., Reddel, H., Martin, R., Brusselle, G., Papi, A., Thomas, M. and Price, D. (2014). Quality standards for real-world research. Focus on observational database studies of comparative effectiveness. Annals of the American Thoracic Society, 11 (2), 99-104.
Rudner, L.M. and Schaefer, W.D. (2000). Practical Assessment, Research and Evaluation, Practical Assessment, Research and Evaluation, 1 (10), 2002-2003.
Seawright, J. and Gerring, J. (2008). Case selection techniques in case study research a menu of qualitative and quantitative options. Political Research Quarterly, 61 (2), 294-308.
Sood, S. K. (2012). A combined approach to ensure data security in cloud computing. Journal of Network and Computer Applications, 35 (6), 1831-1838.
Spira, L. F. and Page, M. (2003). Risk management: The reinvention of internal control and the changing role of internal audit. Accounting, Auditing & Accountability Journal, 16 (4), 640-661.
Sutton, S.G., Khazanchi, D., Hampton, C. and Arnold, V. (2008). Risk analysis in extended enterprise environments: Identification of critical risk factors in B2B e-commerce relationships. Journal of the Association for Information Systems, 9 (3-4), 151-174.
The Institute of Internal Auditors (2013). The Three Lines of Defense in Effective Risk Management and Control: Is Your Organization Positioned for Success? Retrieved from https://na.theiia.org/news/Pages/The-Three-Lines-of-Defense-in-Effective-Risk-Management-and-Control-Is-Your-Organization-Positioned-for-Success.aspx
Weber, R.H. (2010). Internet of Things–New security and privacy challenges. Computer Law & Security Review, 26 (1), 23-30.
Weill, P. and Ross, J.W. (2004). IT governance: How top performers manage IT decision rights for superior results. Harvard Business Press.
Whitman, N.I. (1990). The Committee Meeting Alternative: Using the Delphi Technique. Journal of Nursing Administration, 20 (7-8), 30-36.
Xue, Y., Liang, H. and Boulton, W.R. (2008). Information technology governance in information technology investment decision processes: The impact of investment characteristics, external environment, and internal context. MIS Quarterly, 32 (1), 67-96.
Yoo, Y. (2010). Computing in Everyday Life: A Call for Research on Experiential Computing. MIS Quarterly, 34 (2), 213-231.