AUDITING MECHANISM FOR ENTERPRISE OPERATION MANAGEMENT UNDER IOT ENVIRONMENT

Jhan-Cyun Liao, Department of Accounting and Information Technology, National Chung Cheng University, Taiwan, 886-5-2720411, crazybearb@gmail.com
Li-Min Chang, Department of Accounting and Information Technology, National Chung Cheng University, Taiwan, 886-5-2720411, changclm@gmail.com
She-I Chang, Department of Accounting and Information Technology, National Chung Cheng University, Taiwan, 886-5-2720411, actsic@ccu.edu.tw

ABSTRACT

The aim of this study is to develop the auditing mechanism for enterprise operation management and internal control in the IoT environment. With the guidance of Gowin's Vee knowledge map strategy, we first reviewed relevant literature to identify the enterprise risk audit items in the IoT environment. Second, we utilized the Delphi questionnaire operation to correct defined audit items. Third, we designed the audit items into an operation management audit table suitable for the IoT environment based on the verification results, from which feasible audit standards and operation procedures were set. This research has three important outputs: audit items, tables, and procedures related to enterprise operation management. The outputs of this research could be used as the references in developing internal control audit documents and knowledge study related to the IoT environment.

Keyword: Internet of things (IoT), auditing mechanism, operation management, Delphi method

EXTENDED ABSTRACTS

IoT has become a major technology in promoting social and economic development [3][8]. The technology in the new era has led to global social reform as well as a wave of innovations and applications in the commercial mode. For example, IoT technology can be used to deliver real-time messages through a common platform, wired/wireless network, GPS, or cloud computing method, with the aim of providing a warning, or monitoring case situations [1]. Particularly, in the field of commerce, IoT has helped develop new modes of commerce and diversified technology applications that further promoted the development of various business activities [6][7][11]. The technological application of IoT in various aspects of business activities has become a key strategy, which allows enterprises to establish their competitive advantage.

IoT has created diverse business opportunities for enterprises. However, these enterprises also face many challenges because of the interconnected and complex characteristics of an IoT environment such as hackers attack the websites of enterprises by abusing the weaknesses of IoT and using cloud computation to launch a Distributed Denial of Service (DDoS) attack. In this situation, an enterprise information system can be used as the window of attack via malicious software resulting from loopholes in IoT that cannot be plugged in real time. However, issues regarding information security and internal control mechanisms under the IoT environment have exposed the enterprises' operations to high potential risks. Therefore, improving the supervision and control mechanism of the management system to reduce the risks of enterprises' operations has become an important research topic in the new economic environment [13][14][17].

Spira and Page (2003) emphasized internal control and risk management playing the significant effect of enterprise operation management and corporate governance. Managers could implement various measures and mechanisms of risk management and internal control to achieve the goal of ensuring effective corporate governance [2][12][16]. Relevant activities via internal audit can not only identify potential operational risks at an earlier stage but can also help in supervising and improving the security against existing risks, thus ensuring full control over various resources. Although enterprises have existing frameworks and relevant standards in implementing the audit of internal control, such as COSO, COBIT 5, ISO 31000, ISO 27001, and ISO 27005, IoT remains a new technology. Yet the application of emerging technologies in the Internet of Things, the potential threats and risk factors of business operations have been very different from the traditional environment. If the company still adopts an existing internal control framework or risk management audit mechanism, it may expose the enterprise to potential risks [7][17]. It is important to create an audit mechanism that is suitable for the IoT environment which can assist enterprises in operation control. The current study has three main objectives: to define the audit items of enterprise risks under the IoT environment; to design risk management audit tables suitable for the IoT environment and to establish the standard operating procedures for implementing audit activities.

To provide this study with a set of reasonable procedures to follow, we adopted Gowin's Vee knowledge map as the basis of research development. Gowin's Vee knowledge map is an association management tool used in qualitative research to explore the knowledge of a research subject, theory, or method [9]. Guided by the development strategy of Gowin’s Vee knowledge map, firstly, we explored the literature to better understand the general concepts, principles, rules, and theories of audit mechanism in the IoT environment from a theoretical perspective. From this, we constructed the questionnaire prototype including the audit items of internal control. Secondly, in the methodological aspect, we utilized Delphi for binary expert questionnaire investigation, with the aim of upgrading the content validity of various audit aspects and detailed items through the feedback and correction of the experts' opinions in various fields. The Delphi method is an expert investigation method that is frequently used for collecting practical knowledge [4][5][10].

We used two rounds of Delphi questionnaires and conduct expert group to correct and revise the developed internal control audit items. The first questionnaire testing aimed to gather the opinions of the expert group regarding the original questionnaire to rectify any problematic audit items. The questionnaire testing time started on 12 June and the recovery was completed on 25 June 2015. The second expert questionnaire was distributed to the respondents after the completion of the first questionnaire, and the revised version was delivered to expert groups for confirmation. The second questionnaire distribution lasted between 26 June and 3 July 2015. A total of 31 experts in the audit profession and risk management field were invited to participate in the initial investigation. We utilized statistical software SPSS 12.0 for the analysis and validity test of relevant data. The content included the following: to observe the importance of audit items with Average; to analyze the consistency of expert opinions with Quartile Deviation and to use Content Validity Ratio (CVR) values to test the content validity of the audit items. To understand the importance of audit items, the questionnaire used the five-point Likert-scale, the measurement range is from 5 to 1 points with 5 as “very important” and 1 as “very unimportant.” Thereby allowing experts to express their opinions on the importance of specific items. Finally, based on the Delphi method operation, the present research produced 66 internal control audit items.

In order to make the constructed auditing mechanism play an effective and substantial role, this study refers to the three lines of defense of the International Internal Auditing Association (IIA) to design a set of internal control auditing procedure and evaluation method that can be followed for reference in future audits. The auditing procedure for this study is divided into six steps: planning, execution, problem communication, reporting, problem tracking, and closing. Detailed operations are included in the developed audit manual. In terms of the audit evaluation, to make the development of the IoT auditing mechanism have a sound foundation, this study designed an evaluation method in accordance with the framework of the three-line defense of IIA (i.e., risk classification, internal control, organization self-evaluation), as a basis for internal control audit under the environment Internet of Things. In addition, the weight ratios of the first and second layers are the default values for the assessment based on the classification of enterprise risks and the average of the five internal control audit facets of COSO 2013. The weight ratio of the third layer is set by the audited organization according to the pre-set value provided by adding or subtracting ±5%.

In sum, this research explores the enterprise internal control audit mechanism in the IoT environment. With the guidance of Gowin's Vee knowledge map strategy, we first reviewed relevant literature to identify the enterprise risk audit items under the IoT environment. Second, we utilized the Delphi questionnaire operation to correct various defined audit items. Third, we used a statistics software for data verification (i.e., average, quartile deviation, and CVR value). Finally, we designed the audit items into a risk management audit table suitable for the IoT environment. The design was based on the verification results, from which feasible audit standards and operation procedures were set. This research has three important outputs: audit items, tables, and procedures related to enterprise internal control. The outputs of this research could be used as the reference for the academic world in developing internal control audit documents and knowledge study related to the IoT environment. The results could also be regarded as an important benchmark for enterprises to implement internal control and establish an audit system in implementing operation management related to the IoT environment.

REFERENCES

[1] Babar, S., Mahalle, P., Stango, A., Prasad, N. & Prasad, R. Proposed security model and threat taxonomy for the internet of things. In Editor (Ed.). Recent trends in network security and applications (pp. 420-429). Berlin Heidelberg: Springer, 2010.

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

[3] Chan, H. C. Internet of things business models. *Journal of Service Science and Management,* 2015, 8 (4), 552-568.

[4] Chang, S. I. An alternative methodology for Delphi-type research in IS key issues studies. *International Journal of Management and Enterprise Development*, 2005, *3* (1-2), 147-168.

[5] De Haes, S. & Van Grembergen, W. An exploratory study into the design of an IT governance minimum baseline through Delphi research. *Communications of the Association for Information Systems*, 2008, 22 (24), 443-458.

[6] Galliers, R. D. & Leidner, D. E. Strategic information management: challenges and strategies in managing information systems. Routledge, 2014.

[7] Gubbi, J., Buyya, R., Marusic, S. & Palaniswami, M. Internet of things: A vision, architectural elements, and future directions. *Future Generation Computer Systems,* 2013, 29 (7), 1645-1660.

[8] Madakam, S., Ramaswamy, R. & Tripathi, S. Internet of things (IoT): A literature review. *Journal of Computer and Communications,* 2015, 3 (5), 164-173.

[9] Novak, J. & Gowin, D. B. Learning how to learn. Cambridge, England: Cambridge University Press, 1984.

[10] Okoli, C. & Pawlowski, S. D. The Delphi method as a research tool: An example, design considerations and applications. *Information & Management,* 2004, 42 (1), 15-29.

[11] Ordanini, A. & Rubera, G. How does the application of an IT service innovation affect firm performance? A theoretical framework and empirical analysis on e-commerce. *Information & Management,* 2010, 47 (1), 60-67.

[12] Pathak, J. Risk management, internal controls and organizational vulnerabilities. *Managerial Auditing Journal,* 2005, 20 (6), 569-577.

[13] Posey, C., Roberts, T. L. & Lowry, P. B. The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems,* 2015, 32 (4), 179-214.

[14] Roman, R., Zhou, J. & Lopez, J. On the features and challenges of security and privacy in distributed internet of things. *Computer Networks,* 2013, 57 (10), 2266-2279.

[15] Spira, L. F. & Page, M. Risk management: The reinvention of internal control and the changing role of internal audit. *Accounting, Auditing & Accountability Journal,* 2003, 16 (4), 640-661.

[16] Sutton, S. G., Khazanchi, D., Hampton, C. & Arnold, V. Risk analysis in extended enterprise environments: Identification of critical risk factors in B2B e-commerce relationships. *Journal of the Association for Information Systems,* 2008, 9 (3-4), 151-174.

[17] Weber, R. H. Internet of things: New security and privacy challenges. *Computer Law & Security Review,* 2010, 26 (1), 23-30.