Advances in Economics, Business and Management Research, volume 156
2nd International Scientific and Practical Conference on Digital Economy (ISCDE 2020)

Internal Audit Strategies for Dealing With Digital Risk in the Digital Economy

Xiaofei Xie

Saint Petersburg State University, Saint Petersburg 198504, Russia
**Corresponding author. Email: xiexfei@yandex.ru*

ABSTRACT
With the advent of digital economy era, conforming to the development of digital economy has become a global consensus, and the global digital economy presents a situation of rapid development. From mobile Internet to artificial intelligence, blockchain to big data, digital technology has infinite potential. The digital characteristics of economic development are constantly enhanced, and enterprises are increasingly dependent on the digital, digital security has become a major risk. The management of digital risk has also become the key research object of enterprises. As the supervisor of enterprise risks, internal audit needs to identify, analyze and evaluate digital risks, and coordinate and deal with them. This paper describes the change of the definition of internal audit to the direction of risk prevention and control, and the affirmation of the role of risk management of internal audit by various risk management associations. Secondly, the definition and characteristics of digital risk are analyzed, and it is found that digital risk is characterized by universality, complexity and severe destructiveness in enterprises. Thirdly, it puts forward that internal audit, as an important risk prevention and control agent in digital economy, should be improved in terms of technological innovation, big data utilization, digitalization improvement and auditor quality improvement. It is hoped that these recommendations will contribute to internal audit efforts in controlling digital risks.
Keywords: *Digital economy, Digital risk, Digitization, Internal audit, Risk control, Improvement measures*

1. INTRODUCTION

The global economy is still in a relatively stable stage of recovery, and the real economy, represented by advanced manufacturing industry, will continue to be the main growth point. With the in-depth implementation of digital economy strategies in various countries and regions, the Internet, big data, artificial intelligence and other new-generation information technologies are widely used in the manufacturing industry. The United Nations conference on trade and development released the 2019 digital economy report pointed out that the global digital economy accounts for about 4.5% of GDP to 15.5%. Digital economy will promote all-round reforms and breakthroughs from production factors to innovation systems, business structure to organizational forms, and development concepts to business models. It will continue to give birth to new models such as personalized customization, intelligent production, networked collaboration, and service-oriented manufacturing.

2. THE HISTORY OF RISK-ORIENTATION FOR INTERNAL AUDITING

In June 1999, the International Association of Internal Auditors (IIA) [1] reviewed and adopted a new definition of risk-oriented internal audit, which adds value to an organization by assessing and improving risk management, control, and corporate governance. In 2001, the IIA's Practice Standards for Internal Audit [2] reaffirmed this goal, pointing out that "Internal audit is a systematic and standardized approach that helps achieve business objectives through the evaluation of enterprise risk management, control and governance processes. In 2004, COSO Committee [3] issued an announcement saying that the combination of internal control and risk management can better promote the development of enterprises, effectively promote the transformation of internal audit mode towards the risk-oriented, and make the risk-oriented audit method become the mainstream trend in the future. In 2010, the Association of Financial Risk Managers (GARP) and the International Association of Risk Managers (PRMIA) proposed that the discovery, analysis, management and supervision of material misstatement risks will be the focus of future internal audits. The latest edition of the International Professional Practice Framework for Internal Audit published by the IIA [4] in January 2011 clarifies a new definition of internal audit: Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. Many scholars found that the application of risk-oriented internal audit can bring positive effects to enterprises, and pay more attention to the effectiveness of

the application of risk-oriented internal audit in practice. Zhang Lijin and Chen Weiyu [5] pointed out that in terms of conventional risk management, the main role of internal audit is consultation and confirmation, while in terms of third-party risk management, supervision, Suggestions and confirmation are all extensions of the role of internal audit. Li Feng chu [6] found through research that risk management is an audit means reflecting the standardization and systematization of internal audit institutions, as well as an effective way to review and evaluate the appropriateness and effectiveness of the role of internal audit of enterprises.

3. DIGITAL RISK ANALYSIS

The digitization of enterprises has brought high efficiency and high profit to enterprises, which urges traditional enterprises to digitize one after another. Digital development has become the core development strategy of many enterprises. In the process of digitization, enterprises carry out business based on network, platform and other operational tools, which will inevitably lead to digitization risks. Digital risk is a term encompassing all digital enablement's that improve risk effectiveness and efficiency—especially process automation, decision automation, and digitized monitoring and early warning. The approach uses work-flow automation, optical-character recognition, advanced analytics (including machine learning and artificial intelligence), and new data sources, as well as the application of robotics to processes and interfaces. Essentially, digital risk implies a concerted adjustment of processes, data, analytics and IT, and the overall organizational setup, including talent and culture [7].

3.1. Digital risk exists in all aspects of an enterprise's business

The digitalization process can include new components that will bring additional risks to it [8]. Modern enterprises basically use information tools to carry out all kinds of business, such as procurement, production, sales, management, finance and so on, which causes the spread of risks in the enterprise chain. More interconnectivity also increases network complexity, and thus favors the rapid spread of cyber-attacks within the information network [9]. Any business and Internet connection of an enterprise will create external digital risk. At the same time, in the internal operation process of an enterprise, it is also possible to generate internal digital risks based on systematic errors or human factors. Risk will be transmitted through the business chain, causing risk accidents of the whole enterprise, so the enterprise needs to carry out risk prevention and control in all aspects. The difference between traditional risk and digital risk is that if the enterprise does not carry out relevant business, this risk will not be generated and there is no need to prevent this risk. Therefore, as long as an enterprise has begun to change its digital mode, it will inevitably encounter digital risks at the strategic and various specific business levels.

3.2. Digital risk prevention and control is difficult

Digital risk is an extremely complex risk. Different enterprises and industries will have different digital risks due to different application technologies. But in the enterprise interior, the digital risk penetrates in the enterprise each kind of different business, and produces the digital risk the factor is many. Therefore, to prevent and control such a complex risk, managers need to have knowledge and skills in multiple fields [10], as well as comprehensive strategic thinking and strong communication skills. So, whether based on the risk itself or risk management personnel, there is greater difficulty and complexity.

3.3. Digital risks have serious consequences

The influence of traditional risks is limited, which generally has a large unilateral influence on the enterprise, and the overall influence on the enterprise can be controlled. Digital risks, on the other hand, are more widespread than traditional ones, and the losses are more severe. In the application of technology by enterprises, data leakage, network security and technology infringement are all possible [11]. These problems can cause a heavy blow to enterprises in a very short time. For example, Facebook has been hit with a $5 billion fine for data breaches. So digital risk cannot be viewed in a traditional light.

4. CHANGES IN INTERNAL AUDITING IN THE DIGITAL ECONOMY

In the trend of digital economy, how to effectively control digital risk is the main problem faced by modern enterprises. As an important force of risk control, internal audit should play a more important role. Due to the development of digital economy, the innovation and reform of internal audit cannot keep pace with the development of digital economy. Internal audit needs to change and adapt to the characteristics of the digital economy and digital risk.

4.1. Internal audit should accelerate the innovation of technology application

With the rapid development of cloud computing, Internet of Things, mobile Internet, intelligence and big data, various innovative auditing technologies are constantly emerging. For example, the implementation of networked audit, cloud platform audit, system intelligent audit, virtual reality audit and blockchain independent audit. Technological advances are indispensable for the establishment of an effective

digital auditing system [12]. Both application-level and feature-level audit analytics usage have positive impacts on performance of internal audit [13]. Networked audit provides internal auditors with more comprehensive and specific audit data, which expands the scope of audit in an unprecedented way, promotes the establishment of audit early warning mechanism, and advances the audit threshold. Cloud platform audit is an audit platform built on the basis of the Internet, big data and cloud computing. It realizes digitalization of various audit information to promote the exchange and sharing of information and fully optimize the utilization of audit resources. System intelligent audit is to use quantitative decision support model to assist auditors to make decisions and simulate expert thinking to solve non-structural problems. Virtual reality auditing is the use of virtual reality technology to simulate internal control and risk. Blockchain independent audit is the use of blockchain distributed ledger technology to achieve data authenticity, transparency and integrity, and through the consensus mechanism to ensure that all parties in the system recognize the content recorded in the ledger. Given that it features elements such as decentralization and transparency, blockchain certainly has the potential to improve information and accounting quality [14]. These features will be widely used in audit, and the application of blockchain technology will promote the reduction of audit costs.

4.2. Internal audit should leverage big data to improve predictive power

Big data technical analysis is to analyze the operation and financial status of an enterprise through mining and collecting the basic data of the company [15]. Using big data technology, internal audit can analyze customer payment behavior, evaluate customer credit rating, predict customer credit risk, predict the impact of credit limit on revenue, etc. Internal auditors can discover high-risk areas through big data technology, which is conducive to an in-depth understanding of the audited entity, so as to help the audited entity improve its risk management level. In addition, large amounts of unstructured and semi-structured data can also be obtained through big data technology, and timely updating the database is conducive to improving the accuracy and pertinence of internal audit.

4.3. Internal audit should be more digital

The trend towards the widespread use of digital technology and the increase in mobile devices has led to significant changes in the working environment of internal audit. Based on the degree of digitalization, internal audit will no longer be limited by time and space. Digital technologies provide internal audit with unlocking resources, such as information systems, mobile offices, and web links, which enable auditors to work efficiently and seamlessly wherever and whenever they want. Modern audit tools and techniques must be used so that internal control processes will be appropriate for an ES [16]. Internal audit should ensure that data collection meets stringent information standards to facilitate the establishment of data systems for use across devices and platforms.

4.4. Internal auditors should enhance their professional competence

In the face of new industries and business models brought about by the digital economy. A need for advanced it-audit techniques in debugging the internal audit function, thereby increasing IT audit skill demands on generalist internal auditors [17]. Enterprise audit committees should strengthen the continuing education and training of internal auditors. Internal auditor competence is positively associated with the effectiveness of internal control over compliance [18]. Enhance the professional competence of the internal auditor. Internal auditors need to keep abreast of developments in network information technology and innovate existing workflow. Improve the application of information technology in the timely detection of problems, and accurate judgment, timely response.

5. CONCLUSION

With the acceleration of technological change in the world, economic forms have also become more complex. As a powerful booster of the world economy, digital economy has a far-reaching impact on the world economy. Digital security in the digital economy has become a global issue, and building a more secure defense system has become an important task for all countries. More research is needed to develop more effective control and prevention methods for digital risks. This puts forward higher requirements on the internal audit of enterprises, which needs to keep pace with the development speed of the digital economy, so as to timely discover various risks and provide reliable and valuable Suggestions for the decision makers of enterprises.

REFERENCES

[1] IIA. Internal Audit Practices Framework, 1999(6).

[2] IIA. International Standards for the Professional Practice of Internal Audit. 2001(1)

[3] COSO. Enterprise Risk Management — Integrated Framework. 2004(9)

[4] IIA. International Internal Audit Professional Practice Framework. 2011(1)

[5] W.Y. Chen, L.J. Zhang. Research on the Expansion of Internal Auditing Functions: Third Party Management. Friends of Accounting, 2017(2):116-118.

[6] F. C. Li. Thoughts on Several Issues Concerning Deepening the Work of Internal Audit. China Audit Report, 008th edition.

[7] S. Ganguly, H. Harreis, B. Margolis, K. Rowshankish. Digital risk: Transforming risk management for the 2020 s. McKinsey & Company.

[8] V.G. Khalin, G.V. Chernova, Digitalization and Its Impact on the Russian Economy and Society: Advantages, Challenges, Threats and Risks. Administrative Consulting. (10) (2018) 46-63. DOI: 10.22394/1726-1139-2018-10-46-63

[9] O. Citizens, B. Haeckel, P. Karnebogen, J. Toppel. Estimating the impact of IT security incidents in digitized production environments. Decision Support Systems. Volume 127, December 2019, 113144 https://doi.org/10.1016/j.dss.2019.113144

[10] T. Ritter, C. L. Pedersen. Digitization capability and the digitalization of business models in business-to-business firms: Past, present, and future. Industrial Marketing Management, 86 (2020) 180-190. DOI: 10.1016/j.indmarman.2019.11.019

[11] X.H. Xie, China internet insurance in the era of digital economy. CITISE, (2) (2020) 406-418. DOI: 10.15350/2409-7616.2020.2.37

[12] P. Lois, G. Drogalas, A. Karagiorgos, K. Tsikalakis. "Internal audits in the digital era: opportunities risks and challenges", Euro Med Journal of Business, 15 (2) (2020) 205-217. DOI: 10.1108/EMJB-07-2019-0097

[13] H. Li, J. Dai, T. Gershberg, M. A. Vasarhelyi. Understanding usage and value of audit analytics for internal auditors: An organizational approach. Int.J. of Accounting Information Systems, 28 (2018) 59-76. DOI: 10.1016/j.accinf.2017.12.005

[14] E. Benson. M. Bedrove. "Blockchain and its implications for accounting and auditing", Meditari Accountancy Research, 27(5) (2019) 725-740. DOI: 10.1108/MEDAR-11-2018-0406

[15] X. H. Xie, X. F. Xie. Analysis and Transformation of Financial Management in the Digital Economy, in: High-tech and scientific innovation: Collection of selected articles of the International Scientific Conference, Nacrazvitie Press, Saint Petersburg, 2020, pp. 185-191.

[16] A. Kanellou, C. Spathis. "Auditing in enterprise system environment: a synthesis", Journal of Enterprise Information Management, 24(6) (2011) 494-519. https://doi.org/10.1108/17410391111166549

[17] A. Kotb, A Sangster, D. Henderson, E-business internal audit: the elephant is still in the room!, Journal of Applied Accounting Research, 15(1) (2014) 43-63. https://doi.org/10.1108/JAAR-10-2012-0072

[18] Y-T Chang, H.C. Chen, R. K. Cheng, W.C. Chi. The impact of internal audit attributes on the effectiveness of internal control over operations and compliance. Journal of Contemporary Accounting & Economics, 15(1) (2019) 1-19. DOI: 10.1016/j.jcae.2018.11.002