Research on Internal Control Risks and Prevention in Artificial Intelligence Environment

Mingwei Sun[a], Quangen Gu[b, *], Dongxia Huang[c]

Suzhou Institute of Trade and Commerce, Suzhou 215009, China

[a]2542492528@qq.com, [b]362341397@qq.com, [c]383524190@qq.com

*Corresponding author

Keywords: artificial intelligence, internal control, control risk, preventive measures

Abstract: With the advent of the artificial intelligence era, information technology brings efficiency and convenience to the internal control of enterprises, but also triggers potential control risks. Based on the analysis of internal control risk in artificial intelligence environment, this paper puts forward some preventive measures for enterprise internal control risk in artificial intelligence era, which has certain reference value for the reponse to internal control risks in artificial intelligence era.

1. The research background

Artificial Intelligence (AI) is a modern science and technology. It is a branch of computer science and is used in many fields such as image recognition and speech recognition. Artificial intelligence includes techniques in psychology, philosophy, computer technology, mathematics, information technology, etc., which can simplify human work to the greatest extent, especially in the field of data processing, which not only greatly simplifies the workload, but also reduces human errors. Internal control is a series of control systems adopted for enterprises to achieve their established business objectives. It can ensure the security of enterprise resources, the legality of business activities, the reliability of accounting information, and improve the overall operational efficiency of enterprises. Artificial intelligence technology is widely used in enterprise internal control, and it also raises higher requirements for prevention of internal control risks.

In 1987, the American AICPA published an article “Introduction to Artificial Intelligence and Expert System", pointing out the role of artificial intelligence systems in the field of accounting, revealing the relationship between artificial intelligence systems and financial accounting. In July 2007, the State Council issued the "New Generation Artificial Intelligence Development Plan", and proposed the guiding ideology, strategic objectives, key tasks and safeguard measures for the development of China's new generation of artificial intelligence in 2030, emphasizing the deployment and construction of China's artificial intelligence development. In March 2016, Deloitte partnered with Kira Systems to create the Deloitte Financial Robot, which can replace the manual labour and quickly read contracts and documents and extract useful information from them. In August 2016, Beijing Jiahuihun Technology Co., Ltd. launched a fully automatic and intelligent financial system of “Yundou Accounting”, which took only 1 minute and 20 seconds to complete the whole process from scanning and uploading bills to checkout, subverting the public's perception of bookkeeping.

The development of artificial intelligence technology has a major impact on internal control. Jon Raphael (2015) proposed to use artificial intelligence to solve the difficulty between information transmission speed and its cost, so that auditors can be freed from tedious manual labor, focus on audit quality and improve internal quality. Wang Jing et al. (2017) believed that the emergence of artificial intelligence can help financial personnel to distinguish useful and useless information, make financial decisions in a timely, convenient and scientific manner, which is essential for the internal control of enterprises. Yu Yingmin et al. (2018) pointed out that financial robots have the advantages

of deep learning, precision and reliability, high efficiency, low consumption and rapid response. Their emergence will further simplify the management process of enterprises and reduce management costs, but it also brings great challenges to the accounting industry. Basic-level accounting will face the pressure of unemployment or re-employment. Traditional financial theory will be challenged and internal control will face new challenges. The development of artificial intelligence technology will bring many risks while promoting the optimization of internal control of enterprises. Therefore, it is necessary to analyze the application in the field of enterprise internal control and the risks that may be implied, and explore the methods of risk aversion in order to help the development of the enterprise.

2. The application of artificial intelligence in internal control

2.1 Cloud computing platform

With the advent of the artificial intelligence era, all enterprises need to change the traditional view, transform to data analysis enterprises, build an accounting big data analysis platform, and use data in a whole process, all-round, and full-time. The foundation of building an accounting cloud platform is to build a big data analysis platform, which requires enterprises to improve the internal control system, coordinate the relationship between various departments, and form a flexible, scalable, extensible, and manageable cloud computing platform.

2.2 hierarchical data processing

Artificial intelligence can be divided into three levels of internal control: for the first level, the main management department conducts consistency and compliance checks, such as the use of artificial intelligence programs to automatically extract financial data. For the second level, the data is simply summarized and analyzed to complete the filtering of the data. For the third level, artificial intelligence is used to realize the processing of isomerized massive data, and automatically generates an analysis report after data analysis.

2.3 Intelligent robot

Financial artificial intelligence can effectively solve a lot of cumbersome and mechanized financial work, decompose complex financial information into sub-information, and solve with financial artificial intelligence system. For example, Deloitte, PricewaterhouseCoopers, Ernst & Young, and KPMG are gradually introducing financial robots suitable for their businesses.

2.4 Risk management

Artificial intelligence can make internal control deep into all aspects of business operations, improve internal control efficiency, and can carry out early warning processing of different internal control risks, so as to prevent problems in advance, in the event and afterwards, and deal with problems in a timely and accurate manner.

3. The risk of internal control in artificial intelligence environment

While artificial intelligence technology brings efficiency and convenience to enterprises, it also raises potential internal control risks. There are major risks in data acquisition, information disclosure, fraud, emerging technologies, and lack of personnel.

3.1 Risk of data acquisition

The business of the system or platform is to display the processing results in some form in a given business process. However, in the era of big data and artificial intelligence, these normal data acquisition business processes are extremely prone to data insecurity. The presentation of data acquisition results often leads to the problem of intellectual property security. For example, the first-level search engine obtains data, and then the secondary value behind the data is explored by

multi-level companies. The secondary value is referenced by the first-level search engine, and the data have intellectual property issues.

3.2 Risk of information disclosure

At present, information leakage incidents occur frequently, and the resulting property rights of data has become the focus. All professions and trades involve a large amount of data interaction. Any disclosure of enterprise information will not only pose a serious threat to the user's property, but may even endanger the development of the entire social economy, politics, humanities, etc. Therefore, enterprises must strictly carry out internal control and avoid corporate information disclosure.

3.3 Risk of fraud

The application of artificial intelligence requires the interoperability of all links, which inevitably has the problem of controlling the risk of fraud. For example, the recent frequent exposure of customer information in China's express delivery industry is caused by internal employees suspected of stealing user information.

3.4 Emerging technology risks

Emerging technologies are inherently flawed and problematic due to the immaturity of the project, as well as network failures, infrastructure, system solutions, personnel operations, etc., which can have serious consequences. The more the enterprise relies on information, the greater the loss after the system has problems. For example, in May 2017, the Windows operating system broke out of the Wanna Cry infection incident worldwide, which caused the deletion of encrypted files of users in more than 100 countries around the world, and many industries suffered.

3.5 Risk of talent shortage

The wide application of big data and artificial intelligence has accelerated the development of various industries, and at the same time there has been a shortage of talents. Enterprises are making every effort to tap the top talents in the industry to meet the needs of enterprise development. According to current statistics, at present, the gap between big data analysis and processing talents is about 20 million. It is necessary to open artificial intelligence related disciplines in various universities and to train applicable talents as soon as possible.

4. Internal control risk prevention under artificial intelligence environment

In the era of artificial intelligence, internal control of enterprises faces important opportunities and challenges in terms of technology, systems and talents. Therefore, the construction of the internal control system of the enterprise must be based on technological development, system construction and personnel training, expand the advantages of internal control, prevent and control the risk of internal control, and enable enterprises to develpe smoothly and efficiently in the information technology era.

4.1 Strengthen government supervision

The government uses big data for supervision and management, both in terms of hierarchy and system. First, at the level, the government must take the lead in leading the way. Government departments have a large amount of data, but the data released to the public are very little, and the value of most of the data has not been explored. The government should mobilize the enthusiasm of enterprises, units, and individuals, jointly design big data systems, and establish a trinity of big data, Internet of things, and platforms to explore the deep value. Second, in terms of systems, the government must lead the system of regulation construction. In order to further improve the credibility of the data, the government must lead the establishment of a sound legal system to ensure

the accuracy of the use of big data in the process of obtaining, collecting, analyzing, organizing, storing, publishing, making decisions, implementing and supervising data to promote development of big data.

The large size, strong timeliness, and high density determine that the big data preprocessing will be complicated. Therefore, the government must promote the integration of big data information platforms, and strive to promote the collection and summary system of data. It is necessary to take enterprises as the main body and increase the key technology research and development, industrial development and personnel training systems for big data. At the same time, the government should pre-process public data without compromising the quality of information, taking into account the issue of citizen privacy.

4.2 Focus on corporate governance

The company's internal control system should focus on the governance of information technology risks from a global perspective and maximize the use of resources. Keeping a sense of risk management and control at all times requires not only technical safety, but also safety management. The company should establish a long-term strategic target system, and quantify it into a medium- and short-term specific implementation plan, establish an information security system from top to bottom, ensure the integrity, continuity and stability of the entire system, rationally use artificial intelligence technology resources, and properly control risks. Flatten corporate governance organizations, assign responsibilities to specific departments, and develop risk prevention and control protection level mechanisms to maximize economic efficiency.

4.3 Strictly control technical risks

In the era of artificial intelligence, internal control organizations often rely too much on machine management and control, while ignoring the factors of technical departments, there are technical security and risk issues. To control technical risks, the following aspects should be done: First, the right to deal with risks is appropriately granted. The contact and communication between the safety control personnel and the internal control department should be strengthened, and they should be given certain rights to deal with risks, so that they can control the overall risk in a timely and effective manner and avoid the risk loss of the enterprise. Second, the reliability of the technology should be ensured. Enterprises must ensure the reliability and feasibility of technology, repair vulnerabilities in a timely manner, and avoid risk caused by customer information leakage. Third, investment in technology should be incresed. In order to stay in front of technology, intelligent enterprises must establish a dedicated technical team. This is inseparable from the support of funds. The internal control department should fully measure the ratio of cost input to revenue. Fourth, the awareness of internal control risks should be improved. Internal security personnel should improve risk early warning and prevention capabilities, use advanced data processing systems and systems at home and abroad, and use the latest data analysis software to timely repair and check database vulnerabilities.

4.4 Control key links

The internal control department shall jointly conduct internal audit, finance, sales, investment, production and other departments to strictly review the relevant software and hardware of artificial intelligence technology, and run the server, client, review equipment, software and hardware configuration, patch management system, etc. Perform real-time monitoring and conduct regular safety tests. Strict control and auditing of every aspect may cause security problems to ensure stable, continuous and safe operation of the system. The responsibility of the internal control department is not only monitoring and supervision, but also fully communicating with professionals such as information system development, operation, and maintenance departments to jointly conduct safety management.

4.5 Cultivate risk awareness

Under the risk control framework, enterprises should establish a risk control system that is led by internal control agencies and coordinated by various departments. The internal control department shall set up special regulations and exception handling procedures. Each front-line personnel shall conduct specialized training and adequate training, have a consistent understanding of the enterprise risk management and control mechanism and operational objectives, and actively use risk control measures to control risks. When there is an unknown risk, the frontline personnel should respond to the risk in a timely, effective and calm manner, without having to report it at different levels. On the basis of solving the known risks of quantification, emerging technologies are likely to bring about unknown risks. The prevention of unknown risks cannot be solved by robots. It is necessary to rely on excellent risk management and control personnel, predict risks in advance, and formulate reasonable and flexible risks. Risk management and decision-making mechanism to minimize risk loss.

4.6 Strengthen security cooperation

In the era of artificial intelligence, each company needs to build an open information communication mechanism, use its own superior resources, communicate with external personnel in a timely and effective manner, understand the industry environment in real time, discover the opportunities and challenges of enterprises at any time, and accurately collect internal and external. Information and feedback from personnel to grasp the needs of the public. The Internet connects the entire planet, and any enterprise is placed in a rapidly changing environment. No company can exist independently. In particular, large enterprises must establish a security emergency internal control response center to conduct security tests with external related companies, discover data vulnerabilities in a timely manner, and manage risks in a low-cost and efficient manner.

5. Conclusion

The emergence and application of artificial intelligence technology is the product of scientific and technological progress, and it also brings new opportunities and challenges for the development of internal control. While enjoying the advantages of its high-efficiency service, enterprises should also be alert to the risks they may bring to the enterprise. It is necessary to establish a risk management and control plan for artificial intelligence systems in advance, so as to promote artificial intelligence for internal control services and enhance enterprises. Comprehensive economic benefits.

References

[1] Zhang Xiangzhi, Dai Wentao, Research on Internal Control Evaluation System of Chinese Enterprises [J], Audit Research, 2011(1): 69-78

[2] Xu Jinye, accounting cloud computing: "brain intelligence" in the Internet of Things system [J], Friends of Accounting, 2012 (24): 90-91

[3] Wang Xuelian, the construction of the internal control system of the People's Bank of China based on the new framework of COSO [J], Accounting Research, 2017(3): 62-68

[4] Ma Wei, Lu Ying, Liu Yueyue, Method of Financial Risk Deviation under Big Data Conditions [J], Statistics and Decision, 2015(9): 84-87

[5] Pan Shangyong, on the transformation and upgrading of accounting under the new technology and future development [J], Friends of Accounting, 2016 (23): 18-20

[6] Jon Raphael, see how artificial intelligence improves audit quality [N], China Accounting, 2015-06-26 (008)

[7] Wang Jing, Liang Wenqiao, Breakthrough of Accounting Personnel under Artificial Intelligence [J], Hebei Enterprise, 2017(7): 51-52

[8] Yu Yingmin, Wang Cailin, the impact of financial robots on the accounting industry and its coping strategies [J], Friends of Accounting, 2018 (7): 54-56

[9] Wang Haibing, Dong Qian, Yang Yu, Research on Informatization Risk and Coping Strategies of Enterprise Internal Control Audit [J], Friends of Accounting, 2015(9): 57-61