Advances in Economics, Business and Management Research, volume 70

International Conference on Economy, Management and Entrepreneurship（ICOEME 2018）

Study on the Financial Information Security Governance Under Cloud Environment

Songyue Liu
School of Management
Wuhan University of Technology
Wuhan, China 430070

Lei Xia
School of Management
Wuhan University of Science and Technology
Wuhan, China 430081

***Abstract*—In the era of "Big Data, Intellectualization, Mobile Internet and Cloud Computing", enterprises successively establish the financial share centers. Financial cloud causes a revolution to the accounting industry. However, it is worthy of our attention on the risk of financial information security under cloud environment. Based on the analysis on IT audit and AIS internal controls under the financial cloud model, this paper attempts to prevent and mitigate the risks of financial information security under cloud environment.**

Keywords—financial cloud; IT audit; AIS internal controls

I. INTRODUCTION

The global economic situations change rapidly. The traditional accounting models can no longer meet the demands of enterprises and the management personnel are striving to gradually realize the transformation from centralized finance, financial synergy and financial share to the "financial cloud service" through continuous financial process reengineering. [1] Currently, many enterprises are constructing the financial shared service center. While the current trend is toward the cloud, such as ZTE financial cloud, accounting cloud of Yongyou, private cloud of Dahua Finance and mixed cloud of Changhong, etc.

"Internet plus" leads the society to step into the cloud era; bank-corporate interconnection and bank-corporate direct linkage connect the enterprise financial system, ERP system and bank accounts; the reform on aspects of tax affairs including on-line tax declaration, on-line bill authentication, on line invoice issuance and receiving, invoice electronization and paperless and the Electronic tax payment, etc have promoted the progress of financial cloud; it is stipulated in the new Measures for the Administration of Accounting Archives that the enterprises can utilize the information system to manage the accounting archives and the accounting archives can be filed in electronic form. Such new transformations promote the development of financial development. The financial cloud breaks through the field of enterprise information and connects the business layer (CRA/ERP/SCM/PLM/HRM), accounting layer (financial accounting system), management layer (budget management system, cost management system, performance management system and risk control system), decision-making level (operating decision support system) and connects the exterior and bank, customer, tax department and other third-party platform so as to gradually realize "business and finance integration" of enterprise. [2]

The risks in information security caused by financial cloud cannot be ignored. The studies related to financial information security governance under cloud environment can prevent such risks. IT audit is a link in the internal audit which is mainly used for banks, financial enterprises in the past but receives the attention of more and more experts and scholars with the continuous application of cloud computing. Some large enterprises start recruiting IT audit talents to prevent IT risks. This paper puts forward the IT audit and AIS internal control relations of financial cloud and attempts to find the solutions from the improvement of AIS internal control design and IT audit procedures of enterprises.

II. LITERATURE REVIEW

IT audit (Information Technology Audit) is a process of obtaining and assessing evidences to determine whether the computer system can guarantee assets safety, data integrity and whether the system can effectively utilize the resources of organization to realize the organizational objectives.

Cheng Ping and Bai Yi (2016)[3] pointed out that the financial information security risks caused by financial share service can be prevented and avoided by adopting IT audit; Cheng Ping and Fan Ke (2016)[4] referred to COBIT5.0 and constructed the IT audit system frame under cloud environment. Many scholars also pay attention to the problems in internal control of financial cloud. The AIS internal control means the internal control of Accounting Information System. Cheng Ping and Li Ning (2015)[5] analyzed the current situations and problems of AIS internal control of enterprises under cloud accounting environment and proposed corresponding improvement measures. Zheng Wei, Xu Mengmeng and Qi Guangwu (2014)[6] selected the data sample of 2012 annual A-share listed companies in Shanghai Stock Market and proved that there is the coupling relationship between enterprise internal audit and internal control and there is the positive correlation between internal control and internal audit quality. Therefore, as the branch of internal audit, the IT audit has certain coupling relationship with AIS internal control. And their mutual interaction can be favorable to lower the information system security risks under financial cloud environment.

III. FEATURES OF IT AUDIT AND AIS INTERNAL CONTROL UNDER FINANCIAL CLOUD ENVIRONMENT

A. Differences Between IT Audit Based on Financial Cloud and Traditional IT Audit

Because the financial cloud involves external suppliers, the enterprise data and IT environment are all under the control of external suppliers. Therefore, the audit works will be more complex than regular works. David C. Chou (2015)[7] put forward two kinds of audit methods which separately are value added audit and risk-oriented audit. [10]Value-added audit is a new trend of IT audit and its objective is value creation which can help enterprises with the company governance. However, because the risk-oriented audit is more suitable for the practice of internal audit, this paper is based on the risk-oriented audit. As long as the financial cloud auditors follow the audit frame and select effective risk assessment methods, the financial cloud audit works will be just like regular IT audit works.

The IT audit environment becomes complex and dynamic due to the customized service based on demand of cloud computing. When carrying out the IT audit of financial cloud, all the audit risks under the condition without outsourcing and measures for dealing with such risks shall be taken into consideration. And the risks cannot be mitigated due to third-party outsourcing. For example, the external supplier may not grant you with direct access authority, therefore the audit on the configuration of specific server will become the guarantee on safety of external suppliers while the guarantee on the safety of external supplier is mainly realized through audit on service level agreement.

B. The Difference Between the AIS Internal Control Based on Financial Cloud and the Traditional AIS Internal Control

There are changes in the five factors of AIS internal control based on financial cloud including control environment, risk assessment, information and communication, control activities and monitoring. The data of financial cloud is stored on the cloud. The financial cloud relies on information system which enables it to possess high degree of automation. And the reform on organizational flow incurred by cloud services has caused large quantity of staff reduction and caused the control environment to become complex; the information system used in financial cloud will regularly and automatically update, maintain and upgrade. If relying on automatic control procedure, the management level will neglect risks. Currently, the financial cloud is still in initial stage and the management level lacks credible risk assessment procedures, therefore it is hard for the enterprises to assess the risk levels of the purchased cloud services; the data interconnection brought by financial cloud actually increases the paths for control activities and the data transmission process of each interface becomes the key point of control activity. How to guarantee the safety and correctness of data transmission process has become the new challenge of financial staff; the financial cloud model not only includes the internal system but also the communication among systems. The efficiency and effect of information and communication rely on the design and improvement of internal control; the financial cloud relies on system but not the artificial supervision. Because the system supervision possesses hysteretic nature, it will be difficult in solving the problems incurred. Therefore, the supervision of financial cloud shall combine with internal IT audit.

IV. RELATION BETWEEN AIS INTERNAL CONTROL AND IT AUDIT OF FINANCIAL CLOUD

The enterprises that implement financial cloud shall employ IT auditing personnel and design AIS internal control procedures in the cooperative operation mode. The information safety personnel shall design and implement various kinds of internal control procedures to guarantee the safety of information system; IT auditors shall regularly feedback the validity related to such control activities and provide improvement opinions. The feedback provided can be used to reduce the risks in information system safety of enterprises.

A. AIS Internal Control of Financial Cloud

Ransbotham and Mitra (2009) [9] divide the internal control on information system safety into three parts including configuration control, access control and monitoring control. The configuration control includes vulnerability scanning and patch management system, etc which can reduce the possibility where the system weaknesses may be identified; the access control includes firewall, intrusion prevention system, physical access control, authentication and authorized program, etc which can prevent the attackers from accessing system without authorization; the monitoring control includes document and log analysis and its functions are to monitor problems and provide remedy information. The monitoring control cannot directly lower the risks in information safety. For example, when changing the default configurations, using patch programs, deploying firewall and realizing other types of safety control, the suitable documents can lower the risks of ignoring key system problems. The log analysis can help to find out the reasons of events. The document and log analysis can help modify the internal control so as to reduce the possibility of reappearing of occurred information system risks. The model of Ransbotham and Mitra (2009) [9] potentially exists certain feedback relationship and the documents and log analysis for monitoring control can help collect information so as to provide the basis for altering configuration control and access control.

B. IT Audit of Financial Cloud

According to the study of Hassan Rasheed (2014) [8], this paper analyzes the IT audit of financial cloud through three aspects including infrastructure audit, data audit and the safety audit of service provider.

1) Infrastructure audit: The two important standards most widely applied in safety audit for enterprise infrastructure include Information Security Management of ISO (ISO 27001) and the Payment Card Industry Data Security Standard (PCI DSS). The audit items of safety audit for infrastructure include service level agreement (SLA), IT governance, cost saving, data storage, risk and safety and disaster protection, etc.

2) Data audit: Because the data of financial cloud may be stored out of the enterprise, we need to pay special attention to the safety and privacy of data. If the enterprises choose outsourcing mode, the data will be stored in the system of

service provider and the enterprise data may be stored with the data of other enterprises. If the data is not effectively insulated, it will cause many risks. If one part is under attack, other customers will also face data crisis. We also need to pay attention to the problems including Hackers and virus, etc. Therefore, the enterprises which adopt financial cloud shall audit the data encryption method to guarantee data security; require the service provider to provide third-party interface information; review how the staff of service provider access the system and whether the enterprise data has been controlled; adopt intrusion detection and prevention method to audit and assess the control measures applied for prevention, detection and response of attacks.

3) The security audit of service provider: The first task for adopting financial cloud model is to select proper service provider. Therefore, the assessment on the compliance and security is the most important part. (1) the service providers shall provide the authentication report on internal control from third party (SAS 70 report or SSAE 16 report); (2) obtain ISO 27001 and website security certificate and audit the assessment results of service provider to guarantee the assessment to be carried out by independent third party and determine the period of assessment; (3) review the contract contents and define related responsibilities. The contracts include performance assessment measure, service level agreement (SLA), implementation of requirements of specific control framework (such as COBIT 5.0), the requirements of third-party assessment, requirements of data storage measures, requirements of access authority, disaster recovery flow and data maintenance, data storage and destruction modes, etc. Define the contract details related to security responsibilities. The contract stipulates the fines for violation or delay in performance and the conditions for termination of agreements in case of not achieving performance indicator; obtain the guarantee of supplier to guarantee that the data can be obtained in stipulated form upon demands; forbid the supplier data from being used for other purposes in contract; the contract contains confidentiality clauses to prevent suppliers from disclosing company information; provide evidences to prove that the contract has gone through the audit of related department.

C. *Relation Between AIS Internal Control and IT Audit of Financial Cloud*

The model of Ransbotham and Mitra (2009) [9] potentially assume to exist a feedback process. This feedback process sues the information collected from monitoring control to modify the configuration control and access control. The monitoring control is an important part for effective monitoring control. Regular detection and organization of information security control can lower the risk of enterprise information security. Although the detection of information security can be and is usually accomplished through internal control, the feedback of internal audit can improve the effectiveness and efficiency of information security process and the audit results obtained from detection can provide correction measures and suggestions for the personnel responsible for security function. Therefore, the AIS internal control of enterprise supervises the enterprise information system security process and the IT audit provides the feedback information about whether the controlled operations are effective. Both of them can mutually complement, permeate and supervise to jointly prevent the risks in information system security.

V. CONCLUSION

A. *Enterprises Shall Establish AIS Internal Control and IT Audit Procedures to Convert IT Audit from Risk-oriented Audit into Value Added Audit*

The data security problem of financial cloud is the most noteworthy. Thereinto, the biggest problem is the data security problem caused by third-party interface. The sophisticated AIS internal control and IT audit procedures can help enterprises control risks. Cloud computing is a relatively new field which possesses certain technical defects. IT auditors need to adopt a series of audit procedures to timely find such defects; the risks in financial cloud mainly are non-technical risks which are related to contract. Enterprises shall formulate sophisticated service level agreement (SLA) to prevent contract disputes and clarify responsibilities. Therefore, SLA is one of the key points of IT audit including performance assessment, security articles, service charge and measurement method as well as termination of contract, etc.

The value-added IT audit can help enterprises understand the value of financial cloud, know the advantages and disadvantages of financial cloud, help the senior management of enterprises find the solutions for overcoming the shortcomings, enhance the overall business process management. Therefore, the future trend is to convert the risk-oriented IT audit into value-added IT audit so as to truly realize the value adding of IT audit.

B. *The State Shall Establish IT Audit Quality Framework and Improve the Legislation of Data Security*

There are many organizations in the world establishing IT audit quality framework, such as Internal Control- Integrated Framework and Enterprise Risk Management- Integrated Framework of America; the maturity model of IT internal control; ITIL of Britain; ISO 2700l, ISO 17799 and BS 7799 standards; Information Security Assessment Method of National Security Agency (NSA IAM); COBIT framework, etc. China releases the Auditing Standards for Chinese Certified Public Accountant No.1241- Consideration on the Service Agencies Applied by Unit under Auditing to conduct auditing guidance to the enterprises outsourcing the information technology to service providers. The various kinds of IT audit standards and frameworks (COBIT, ITIL and lSO2700l), laws and regulations and articles (Sarbanes—Oxley, HIPPA and PCI), etc explain contents related to IT audit risk assessment and management. China shall also pay attention to the studies on this aspect and refer to the international experience to optimize the IT audit process.

Currently, the identity information theft cases take place frequently. The data security and privacy is the issue needing urgent consideration of legislators. There is a lot of legislation on the aspects of data security and privacy, such as the

American Sarbanes-Oxley Act, Financial Services Modernization Act, SB 1386 Act of California, EU European Individual Data Protection Directive, Personal Information Protection and Electronic Documents Act, Michigan Social Security Number Privacy Act, American HIPPAA Act, New Basel Capital Accord, Payment Card Industry Data Security Standard (PCI DSS), etc. China shall also pay attention to the data security legislation to guarantee the data security of cloud computation.

C. Enhancing the Financial Cloud Knowledge and Cultivating the IT Audit Talents in Cloud Computation

The application of cloud computation makes the current audit environment more complex and the traditional IT audit personnel cannot meet demands. The IT audit personnel must learn the knowledge related to risk management and master the IT audit method of cloud computation; in the future, there is a large shortage in the IT audit personnel of cloud computation. The higher education in school shall open related courses, cultivate the IT audit talents in cloud computation; the internal audit and external audit shall all well prepare to face to reforms.

REFERENCES

[1] He Ying. Path and Orientation for Financial Process Reengineering of Enterprise Group based on Cloud Computation[J]. Management World, 2013, (04): 182-183.

[2] Chen Huzhu. Finance is IT- Enterprise Financial Information System[M]. Beijing: China Financial & Economic Publishing House. 2017: 46-55.

[3] Cheng Ping, Bai Yi. IT Audit based on Financial Shared Service Model in Big Data Era[J]. Friends of Accounting. 2016, (24): 128-131.

[4] Cheng Ping, Fan Ke. IT Audit System based on COBIT 5.0 Framework under Cloud Accounting[J]. Friends of Accounting, 2016, (18): 128-132

[5] Cheng Ping, Li Ning. Discussion and Analysis on the AIS Internal Control Problems under the Cloud Accounting Environment[J]. The Chinese Certified Public Accountant, 2015 (04): 78-81.

[6] Zheng Wei, Xu Mengmeng, Qi Guangwu. Study on the Internal Audit Quality and Validity of Control Activity- Based on the coupling relationship between Internal Audit and Internal Control and the Experimental Evidences of Listing Firms of Shanghai Market[J]. Auditing Research, 2014 (06): 100-107.

[7] David C. Chou. Cloud computing risk and audit issues[J]. Computer Standards & Interfaces,2015,42:137-142

[8] Hassan Rasheed. Data and infrastructure security auditing in cloud computing environments[J]. International Journal of Information Management,2014,34(3):364-368

[9] Ransbotham S, Mitra S. Choice and chance: a conceptual model of paths to information security compromise. Inf Syst Res 2009;20:121-39