The Measurement of Operational Risk of China's Commercial Banks under the Background of Internet of Things Technology

Ruimin Song [a], Chao Wang [b]

School of Business, Guilin University of Electronic Technology, Guilin 541004, China.

[a]1240389358@qq.com, [b]982307237@qq.com

Abstract. With the rapid development of Internet of Things technology, it brings new ideas to the operational risk management of commercial banks in China. This paper collects the loss data of various types of operational risks of China's commercial banks from 2010 to 2017, and empirically analyzes the operational risks by constructing a POT peaks over threshold model, and compares the operational risks of commercial banks based on Internet of Things technology and the operation of traditional commercial banks. The ES value of the risk indicates that the former can effectively reduce the operational risk. Therefore, commercial banks should vigorously promote the deployment and application of the Internet of Things technology. At the end of the article, the proposed operational risk management of commercial banks based on Internet of Things technology is proposed.

Keywords: Internet of Things; commercial bank; operational risk; extreme value theory.

1. Introduction

With the rapid development of Internet of Things technology and its wide application on a global scale, the Internet of Things will promote the transformation and development of the financial industry. Shao Ping (2015) believes that the development of Internet of Things technology will not only bring huge investment and financing needs to banks, but also promote the bank's credit system from subjective credit to objective credit model, which will bring new development opportunities to banks [1]. Lu Minfeng (2017) believes that IoT banks refer to the traditional use of IoT thinking and technology to integrate the information flow, logistics, capital flow and commodity flow generated by users in economic activities such as life and production. Providing users with financial services such as deposits, loans, and remittances, resulting in a new type of IoT financial organization model [2].

The rapid development of Internet of Things technology not only brings mobile finance, IoT movable financing system and traceability system to commercial banks, but also brings new ideas to commercial banks' operational risk management. Based on the perspective of Internet of Things technology, this paper The extreme value theory super-threshold model quantitatively analyzes the operational risk of commercial banks in China, and uses the control variable method to compare the ES value of traditional commercial banks' operational risk with the ES value of commercial bank operational risk based on Internet of Things technology. The operational risks of commercial banks have been significantly reduced, and corresponding operational risk management recommendations have been proposed.

2. Operational Risk Analysis of Commercial Banks based on Internet of Things Technology

2.1 Traditional Bank Operation Risk Status

Due to the late development of operational risk management of commercial banks in China and the imperfect information disclosure system of domestic commercial banks, the complete operational risk loss database has not yet been created in China. This paper collects 281 cases of operational risk loss from commercial banks in China from 2010 to 2017. Through analysis, it is found that the operational risks of commercial banks in China are mainly concentrated in internal fraud and external fraud incidents, in which the frequency of internal fraud incidents reaches 40.57%, the amount of losses caused up to 52.318 billion yuan, the frequency of external fraud incidents is second only to internal fraud, accounting for 31.67%, resulting in losses of 35.095 billion yuan.

2.2 The Impact of Internet of Things on Bank Operational Risk Management

2.2.1 Reconstruction of Internet of Things in Bank Operational Risk Management

The pain points of commercial banks for operational risk management mainly lie in the lack of identification and monitoring of operational risks, the high cost of operational risk management and the low efficiency of operational risk management. With the development of the Internet of Things technology, banks can carry out transformation and upgrading through the means of Internet of Things technology, replacing the commercial bank's past management of human beings and human beings with the material management and physical management logic of property management. The "human management" thinking logic makes the risk control monitoring more objective, transparent and timely. In addition, the bank can comprehensively grasp the information of the financing enterprise from procurement to sales through the Internet of Things technology, breaking through the "information" that is common in existing information systems. The problem of "island", real-time and objective investigation and financing of financing companies, which will effectively reduce the occurrence of operational risk events such as internal fraud and external fraud.

2.2.2 Internet of Things System Risk

While reconstructing the operational risk management of traditional commercial banks, the Internet of Things technology has also generated various types of new operational risks. According to the logical structure of the Internet of Things, it can be classified into three categories [4]: Perceived layer risk: in the credit stage Risks such as inaccurate or incomplete data or information of related enterprises or platforms are collected; risks such as inspection equipment failure, inaccurate monitoring, and unresponsiveness occur during the cooperative loan phase; relevant market information may appear during the loan repayment period. The risks are not comprehensive enough and there is no timely tracking of related financing items. Network transport layer risks: information disclosure, delay, encryption and asymmetry risks, malicious interference risks, network instability risks, etc. Application layer risks: intellectual property protection risks, cooperation risks of various parties, data mining efficiency risks, and IoT management risks.

3. Construction of Operational Risk Measurement Model based on Extreme Value Theory

3.1 Extreme Value Theory

Extreme value theory is a statistical analysis of extreme events that occur at very low frequencies and that often have a significant impact. Extreme value theory mainly includes BMM model and POT model. The drawback of the BMM model is that it does not fully and effectively utilize the information provided by the data. The POT model can optimize this defect. The POT model determines a reasonable threshold from the sample data, and then constructs a sample data that exceeds the threshold into a new data set, and analyzes and models it.

3.2 Construction Risk Tail Loss POT Model Construction

Suppose X1, X2, ... Xn represent sample data of various types of loss events of commercial banks' operational risk, u is a reasonable threshold selected from X1, X2, ... Xn, then Xu is the excess, and Fu(y) is The conditional distribution function, F(x) is the population distribution function, and has the following relationship:

$$F_u(y) = P(X - u \le y | X > u), \quad y > 0 \tag{1}$$

Derived by the conditional probability formula:

$$F_u(y)=\frac{F(y+u)-F(u)}{1-F(u)},y>0 \tag{2}$$

The derivation conversion can be obtained:

$$F(x)=F_u(y)[1-F(u)]+F(u),\quad x>u \tag{3}$$

Assume that the sample data of the commercial bank operational risk loss sample data exceeding the threshold is y (y1, y2...yt). When the threshold u is large enough, Fu(y) will approximate the GPD distribution, and the expression is as follows:

$$F_u(y)\approx G_{\delta,\theta,u}(y)=\begin{cases}1+\left[1+\delta\frac{x-u}{\theta}\right]^{-\frac{1}{\delta}} & \delta\neq 0\\ 1-\exp\left(-\frac{x-u}{\theta}\right) & \delta=0\end{cases} \tag{4}$$

From y=x-u, substituting the above formula:

$$G_{\delta,\theta}(y)=\begin{cases}1+\left[1+\delta\frac{y}{\theta}\right]^{-\frac{1}{\delta}} & \delta\neq 0\\ 1-\exp\left(-\frac{y}{\theta}\right) & \delta=0\end{cases} \tag{5}$$

The first derivative of the GPD distribution function is obtained, and the probability density function is obtained as follows:

$$g_{\delta,\theta}(x)=\begin{cases}\frac{1}{\theta}\left(1+\frac{\delta}{\theta}x\right)^{-\left(1+\frac{1}{\delta}\right)} & \delta\neq 0\\ \frac{1}{\theta}e^{\frac{x}{\theta}} & \delta=0\end{cases} \tag{6}$$

Substituting y(y1, y2...yt) into the above equation yields a log-likelihood function expression as follows:

$$L(\delta,\theta|y)=\begin{cases}-n\ln\theta-\left(1+\frac{1}{\delta}\right)\sum_{i=1}^{n}\ln\left(1+\frac{\delta}{\theta}y_i\right) & \delta\neq 0\\ -n\ln\theta-\frac{1}{\theta}\sum_{i=1}^{n}y_i & \delta=0\end{cases} \tag{7}$$

By maximizing the above equation, the estimated values of the parameters θ and δ can be obtained. Substituting Fu(y) and F(u) into equation (3-6) yields a functional expression of F(x) as follows:

$$F(x)=\begin{cases}1-\frac{N_u}{n}\left(1+\frac{\delta}{\theta}(x-u)\right)^{-\frac{1}{\delta}} & \delta\neq 0\\ 1-\frac{N_u}{n}e^{-\frac{(x-u)}{\theta}} & \delta=0\end{cases} \tag{8}$$

In the above formula, Nu represents the number of sample data larger than the threshold u. When a confidence level α is given, the expression for calculating VaR can be obtained by reversing the above equation:

$$VaR_{\alpha}=\begin{cases}u+\frac{\theta}{\delta}\left\{\left[\frac{n}{N_u}(1-\alpha)\right]^{-\delta}-1\right\} & \delta\neq 0\\ u-\theta\ln\left[\frac{n}{N_u}(1-\alpha)\right] & \delta=0\end{cases} \tag{9}$$

In order to make up for the fact that VaR does not have sub-additiveness on the mathematical problem, and cannot calculate the specific value of the high loss, we introduce the expected loss value ES, which can effectively solve the measurement problem of the thick-tail distribution of the lost sample data. At a given confidence level α, the expression for calculating the ES value is as follows:

$$ES_{\alpha} = \frac{VaR_{\alpha}}{1-\delta} + \frac{\theta - u\delta}{1-\delta} \tag{10}$$

3.3 Threshold Selection and Parameter Estimation

In this paper, the threshold is selected by the method of excess mean function graph, and the mean value map of the excess function is observed. When there is a significant linear change, the corresponding u value of the point is the initially selected threshold, so the selected threshold will be subject to personal subjectivity. In view of this, this paper will use the excess function mean map to initially select three thresholds u1, u2, u3, and then perform maximum likelihood estimation on these three thresholds respectively, and then the θ and δ parameters corresponding to each threshold can be obtained. With regard to the determination of the optimal threshold of various types of loss events for operational risk, this paper adopts the χ2 goodness-of-fit test method to determine.

4. Empirical Analysis

4.1 Traditional Commercial Bank Operational Risk Measurement Analysis

4.1.1 Data Sources and Their Descriptive Statistical Analysis

At present, domestic banks have not yet created a complete operational risk loss database, so this paper mainly collects data from public channels, such as from authoritative media magazines, Sina, Netease and other portals, as well as the official websites of the People's Bank of China, the China Banking Regulatory Commission, and the Judgment Network. Data, obtained sample data of operational risk loss cases of China's commercial banks from 2010 to 2017, a total of 281 data were collected. The collected data were classified and descriptive statistical analysis was performed on the data. The analysis results are shown in Table 1.

Table 1. Descriptive statistical analysis of operational risk loss events of China's commercial banks in 2010-2017 (Unit: 10,000 yuan)

	Number of samples	Maximum	Minimum	Mean	Standard deviation	Skewness	Kurtosis
Internal fraud	114	1200000	3.00	45893.09	159148.83	5.119	29.397
External fraud	89	40164.80	1.70	2578.61	6557.99	4.134	18.141
Pledge lost or damaged	46	8200.00	10.82	1301.00	1664.14	2.477	6.860
Practitioner's operation error	32	6000.00	1.20	566.33	1167.32	3.719	15.675

According to the descriptive statistical analysis of the operational risk sample data in the above table, it can be found that the skewness of all types of operational risk loss events is greater than 0, and the kurtosis is greater than 3, which indicates the loss sample of various types of loss events of commercial banks in China. The data all show a thick tail distribution, and also shows the characteristics of low-frequency high-loss of operational risk events.

4.1.2 Based on POT Model, Commercial Bank Operation Risk Measurement

In order to further verify the accuracy of the sample data with thick tail distribution, this paper draws the Q-Q graph of each type of sample data by using Matlab software. As shown in Figure 1, it can be found that the data points in the graph are in an upward curved shape, so it can be shown that the data obeys the thick tail distribution.

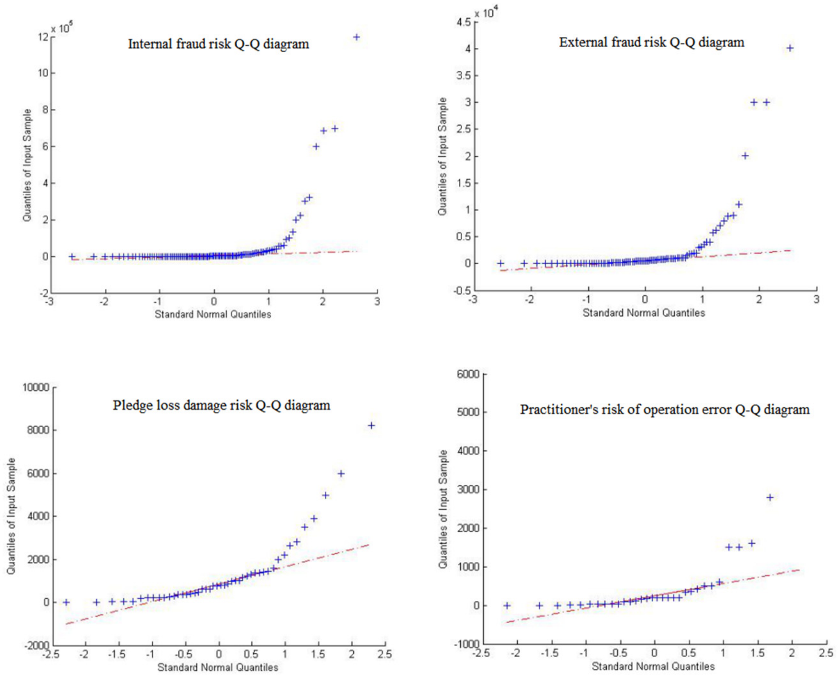

Figure 1. Q-Q diagram of various types of loss events

This paper uses Matlab software to draw the excess mean function graph of various types of loss events of commercial banks' operational risks, as shown in Figure 2. By observing the mean value map of the excess function, the thresholds u1, u2, and u3 of each type of loss event are preliminarily selected, and the maximum likelihood estimation is performed to obtain the parameters θ and δ corresponding to each threshold, and then the corresponding χ2 value is calculated, and the card is calculated. The square fitting goodness test is performed to select the optimal threshold.

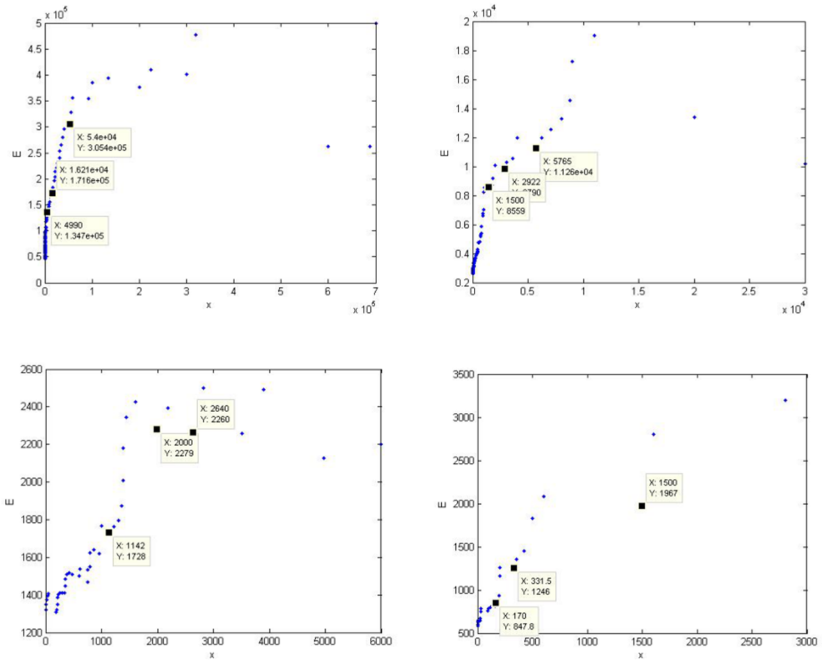

Figure 2. Operational risk type loss event average function mean value map

The specific results are shown in Table 2.

Table 2. Operation risk threshold selection and parameter estimation

Operational risk loss category	u1	u2	u3	χ2 value	Number of super-threshold samples	Parameter δ estimator	Parameter θ estimator
Internal fraud	4990	16209	54000	0.926	27	0.3748	29662
External fraud	1500	2922	5765	0.818	10	0.1710	9462
Pledge lost or damaged	1142	2000	2640	0.034	17	0.4694	977
Practitioner's operation error	170	332	1500	1.212	10	0.6446	600

Note: The underlined data in the table is the corresponding optimal threshold.

Taking the confidence level α as 99.9%, and substituting the parameter estimates θ and δ into (3-9) and (3-10), the corresponding VaR and ES values can be calculated. The results are shown in Table 3.

Table 3. Operational risks VaR and ES of various types of loss events

Operational risk loss category	Internal fraud	External fraud	Pledge lost or damaged	Practitioner's operation error
VaR（99.9%）	551320	74494	32451	37162
ES（99.9%）	919560	100080	61990	105650

According to the results of Table 3, we can see that under the 99.9% confidence level, the numerical difference between the loss events of different types of operational risks of commercial banks in China is relatively large. From the table, it can be concluded that the total ES of operational risks of commercial banks in China is as high as 11.782.8 million yuan. Among them, the risk of external fraud and internal fraud risk is the biggest, so effectively preventing internal and external fraud losses is the focus of operational risk management.

4.2 Measurement and Analysis of Operational Risk of Commercial Banks based on Internet of Things Technology

4.2.1 Data Sources and Their Descriptive Statistical Analysis

This paper adopts the control variable method, which reduces the number of occurrences of various types of loss events of commercial banks in China, and increases the operational loss data caused by the risk of the Internet of Things system. Then, a descriptive statistical analysis is performed on the operational risk loss data of commercial banks based on the Internet of Things technology. The results are shown in Table 4.

Table 4. Descriptive Statistical Analysis of Operational Risk Loss Events of Commercial Banks Based on Internet of Things Technology in 2010-2017 (Unit: 10,000 yuan)

	Number of samples	Maximum	Minimum	Mean	Standard deviation	Skewness	Kurtosis
Internal fraud	96	1200000	20.00	40784.57	160231.37	5.590	33.934
External fraud	76	40164.80	7.00	2569.956	6339.188	4.354	21.080
Pledge lost or damaged	37	8200.00	10.82	1172.506	1610.868	2.916	10.042
Practitioner's operation error	26	2800.00	1.20	427.525	672.939	2.375	5.656
Internet of Things system risk	13	2450.00	820.00	1027.154	436.488	3.358	11.672

4.2.2 Commercial Bank Operational Risk Measurement based on Internet of Things Technology

As can be seen from Table 4, the risk loss data of the Internet of Things system has a kurtosis greater than 3, a skewness greater than 0, and the data points in the Q-Q graph are upwardly curved, so it can be determined that the sample data obeys the thick tail distribution.

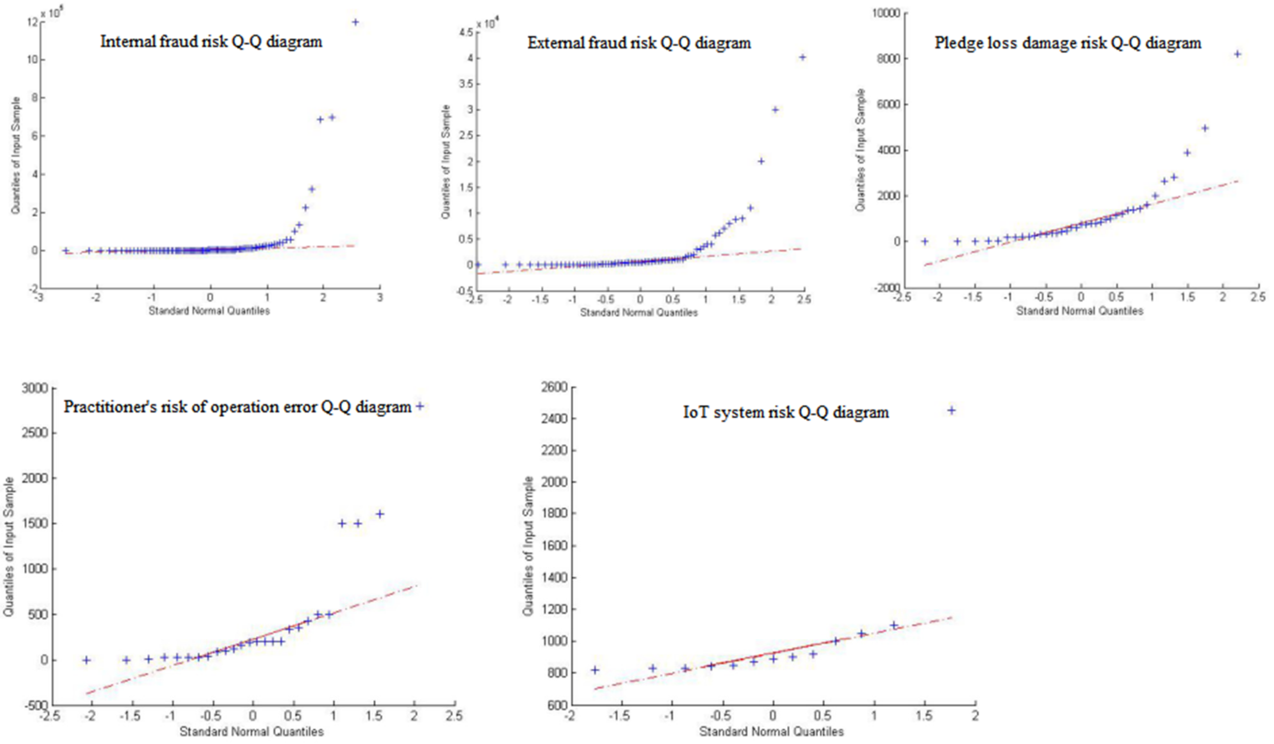

Figure 3. Q-Q diagram of various types of loss events

This paper uses Matlab software to draw the excess mean function graph of various types of loss events of commercial banks under the Internet of Things technology, as shown in Figure 4.

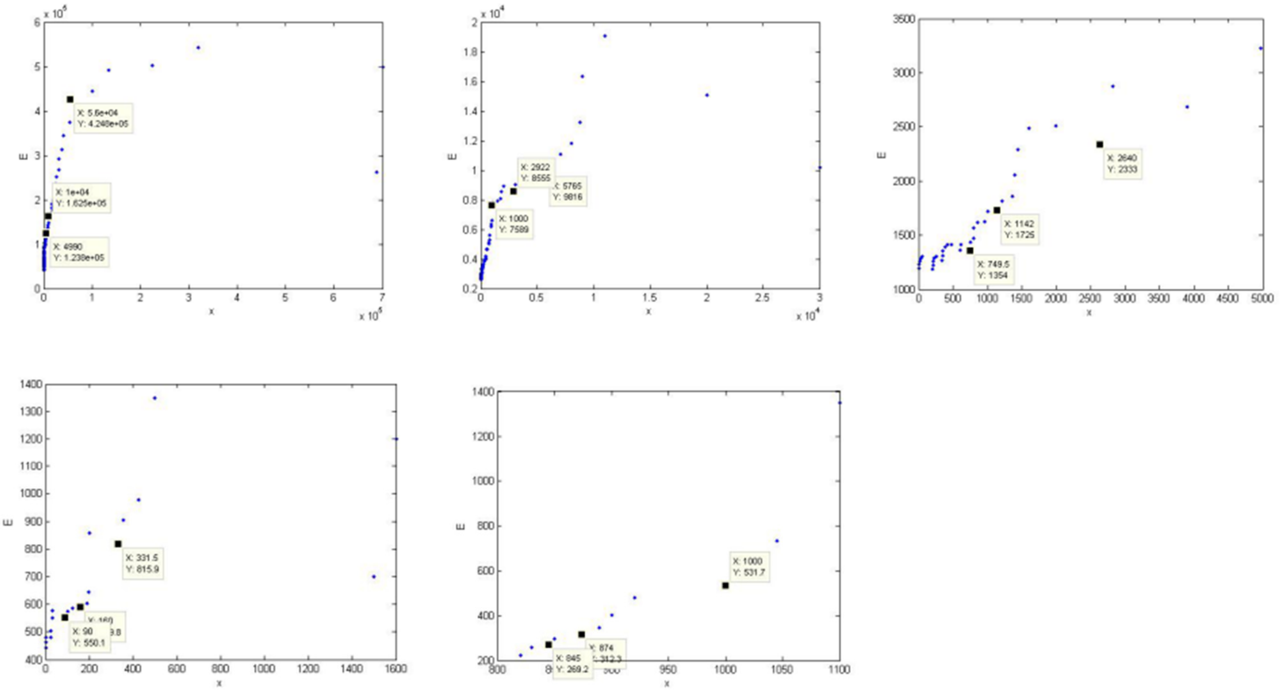

Figure 4. Operational risk type loss event average function mean value map

By observing the mean value map of the excess function, the thresholds u1, u2, and u3 of each type of loss event are preliminarily selected, and the maximum likelihood estimation is performed to obtain the parameters θ and δ corresponding to each threshold, and then the corresponding χ2 value is calculated, and the card is calculated. The square fitting goodness test is performed to select the optimal threshold. The specific results are shown in Table 5.

Table 5. Operation risk threshold selection and parameter estimation

Operational risk loss category	u1	u2	u3	χ2 value	Number of super-threshold samples	Parameter δ estimator	Parameter θ estimator
Internal fraud	4990	10000	56000	0.933	30	0.2298	18862
External fraud	1000	2922	5765	0.857	15	0.5343	4328
Pledge lost or damaged	750	1142	2640	0.246	12	0.5944	814
Practitioner's operation error	90	160	332	1.147	8	0.0615	867
IoT system risk	845	874	1000	0.014	9	0.7195	100

Note: The underlined data in the table is the corresponding optimal threshold.

Taking the confidence level α as 99.9%, and substituting the parameter estimates θ and δ into (3-9) and (3-10), the corresponding VaR and ES values can be calculated. The results are shown in Table 6.

Table 6. Operational risks VaR and ES of various types of loss events

Operational risk loss category	Internal fraud	External fraud	Pledge lost or damaged	Practitioner's operation error	IoT system risk
VaR（99.9%）	230200	132210	42339	6287	16072
ES（99.9%）	321880	289840	104720	7601	55487

From the results of Table 6, we can see that under the 99.9% confidence level, the total ES value of commercial bank operation risk based on IoT technology is 779.528 million yuan, which is lower than the total ES value of traditional commercial bank operation risk. Ten thousand yuan, this shows that commercial banks have effectively reduced operational risks under the transformation of Internet of Things technology.

5. Conclusions and Recommendations

Commercial banks should vigorously promote the deployment and application of Internet of Things technology. With the new business form of Internet of Things, combined with the actual situation of the bank, the number of occurrences of operational risk loss events can be minimized and the losses of banks can be reduced. According to the development status of China's Internet of Things and the actual situation of the bank, the author puts forward the following operational risk management recommendations:

5.1 Internal Fraud Risk Management Recommendation based on Internet of Things Technology

At present, there are problems in the internal bank fraud risk management in China: insufficient risk awareness, single risk identification means, asymmetric risk information, lack of quantitative assessment indicators, insufficient disciplinary measures, etc. In order to solve the above problems, banks must strengthen their occupations for employees. In addition to moral education and fixed-term responsibilities, we should make full use of the three major advantages of IoT information technology, namely information acquisition, information transmission and information intelligent processing, and establish a scientific and perfect information system and internal control system for banks to reduce internal bank fraud. risk.

5.2 External Fraud Risk Management Recommendations based on Iot Technology

At present, the problems existing in the external fraud risk management of commercial banks in China mainly include anti-fraud management process and risk management system to be optimized, insufficient internal bank security management and insufficient risk management system. For the risk of external fraud, first, the bank can comprehensively grasp the whole process of procurement, production and sales of the financing enterprise production scenario through the Internet of Things technology, so that the pre-lending investigation, loan approval and post-loan management can be carried out in real time and objectively, and the bank can be upgraded. The risk identification and risk monitoring level; Second, banks can use the Internet of Things technology to actively promote the formation of unique and exclusive IoT warehouse receipts.

5.3 Proposal for Collateral Management based on Internet of Things Technology

Commercial banks can use the Internet of Things technology to upgrade the Internet of Things in the warehouse. For example, using sensors, RFID, cameras and other technologies to change “movable property” into “real estate”. Through intelligent and standardized operations, banks can grasp the status of pledges in real time. Effectively reduces the probability of collateral damage.

5.4 Risk Management Suggestion for Occupational Errors of Employees based on Internet of Things Technology

Commercial banks can optimize and upgrade banking business processes through Internet of Things technologies. For example, banks can introduce real-time sensing and tracking of important documents such as bank seals, invoices, and vouchers by introducing RFID and sensor covers and intelligent monitoring systems. As far as possible, avoid the mistakes of the practitioners.

Acknowledgments

This research was financially supported by the Innovation Project of GUET Graduate Education (2018YJCX109).

References

[1]. Shao Ping. Internet of Things Finance and Banking Development [J]. China Finance, 2015 (18) 16-18.

[2]. Lu Minfeng, Wang Zugang. Research on the Development Strategy of “Internet of Things + Banking” [J]. Contemporary Economic Management, 2017, 39(12): 76-82.

[3]. Chen Yujie. Internet of Things Financial Innovation Helps the Transformation of Commercial Banks [J]. Modern Commercial Bank, 2019 (05): 74-79.

[4]. Feng Xiaotong, Wang Chengfu, Yan Lei. Identification and Control of Supply Chain Financing Risk under the Internet of Things Financial Model[J].Commercial Economic Research, 2016 (03): 180-182.

[5]. McNeil A, Frey R. Estimation of tail-related risk measures for heteroscedastic financial time series: an extreme value approach [J]. Journal of Empirical Finance, 2000,(7):271-300.

[6]. Wang Q J. The POT Model Described by the Generalized Pareto Distribution with Poisson Arrival Rate [J]. Journal of Hydrology, 1991,129 (1): 263-280.

[7]. Acerbi C,Tasche D. Expected shortfall: A Natural Coherent Alternative to Value at Risk [J]. Economic Notes,2002, 31 (2): 379-388.

[8]. Conti J P. The Internet of things[J]. Communications Engineer, 2006, 4(6):20-25.

[9]. Shepherd C, Petitcolas F A P, Akram R N, et al. An Exploratory Analysis of the Security Risks of the Internet of Things in Finance[C]// International Conference on Trust & Privacy in Digital Business. 2017.