The Application Research of Information Security Risk Assessment Model Based on AHP Method

Meng Meng and Enping Liu*
Institute of Scientific and Technical Information, CATAS, Danzhou Hainan, China
Email: {mengmengsir, yjlep} @163.com

Abstract—**Information security risk assessment involves four basic elements, including information assets themselves, vulnerabilities of information assets, facing threats of information assets and possible risks of information assets. A key problem of risk assessment is the distribution of the weights among risk factors. Here we put forward the weight of risk factors which is calculated by using Analytic Hierarchy Process (AHP), obtain the weight of risk factors, sort in accordance with weight of risk factors, intuitively grasp the harm degree of various risks, and screen out the weights relatively larger risk factors for risk management. Our approach provides the scientific basis for information security risk management decisions.**

***Index Terms*—analytic hierarchy process, information security, risk assessment**

I. Introduction

With the rapid development of information technology and the extensive application of network, modern enterprises, government departments, financial institutions and commercial organizations increasingly rely on information. Information and the software and hardware resources of bearing information constitute a organic whole, are the fifth dimensional space outside of four dimensional spaces (length, width, height and time), has brought many conveniences to the people, and greatly promoted the development of human society. However, the information technology is a double-edged sword, "Pandora's box" in the field has more than once opened. In recent years, loss and impact of information security issues are growing, information security problem more and more get people's attention, and it has become an important factor influencing the development of the information technology [1]-[2].Therefore, to strengthen the enterprise information security risk management and formulate practical and feasible risk management measures is an important work to ensure enterprise information resources security, but the first step of information security risk management is information security risk assessment. Risk management appeared Harvard Business Review in 1956, at the time the so-called risk refers to the insurance company's financial risk [3]. Information security risk assessment is to stand in the perspective of risk management, uses the scientific method, in view of the threats to information systems and the existing vulnerabilities to conduct a comprehensive analysis, through the assessment of the possible harm and influence of information security incidents, puts forward effective countermeasures and effective protective measures, prevents and defuses the risk of information security, and then controls the risk in an acceptable range [4].

The research of information security risk assessment has a history of over 20 years abroad, IT developed countries such as America and Canada, have established information security risk assessment certification bodies and certification system in the 1970s and 80s, which are responsible for the research and development of assessment criteria, assessment methods and assessment technology [5]-[9]. The research of information security risk assessment has been started in recent years in China, at present the main work focuses on the establishment of the organizational structure and business system, the corresponding standard system and technical system are still in research stage.

However, whether foreign or domestic, security model research, standard selection, element extraction, assessment method research and assessment implementation process have been a research focus in information security risk assessment. After decades of research and development, the field of information security has more mature security models and assessment methods, such as P2DR model [10], APPDRR model [11] and ISO15408 model, etc. Assessment methods commonly used have Delphi [12], Fault Tree Analysis (FTA) [13], Analytical Hierarchy Process (AHP) [14], etc. The Delphi method is suitable for the huger data and the larger uncertainty situation, although can synthesize various experts and avoid the impact of subjective, but it is a kind of qualitative assessment methods, and hard to avoid the deficiency of qualitative methods. Although the FTA method can be used for qualitative, also can be used for quantitative, the analysis results are more systematic, accurate and predictable. However, the fault tree logical relationship is complicated and difficult to understand, has also a higher requirement for the analysts, and limit the promotion and popularization of the FTA method. At

Manuscript received July 1, 2015; revised September 1, 2015.

doi: 10.12720/jait.6.4.201-206

present, the AHP method is more widely used, and it realizes the combination of qualitative and quantitative, and suitable for solving the problem of difficult to complete quantitative analysis.

Based on this, This article uses T. L. Saaty Professor AHP (Analytic Hierarchy Process, AHP) to assess information security risk of S company, achieves a qualitative analysis to quantitative analysis of the transformation, obtains the weight of risk factors, sorts in accordance with weight of risk factors, intuitively grasps the harm degree of various risks, and screens out the weights relatively larger risk factors for risk management. Our approach makes information security risk management of S company more scientific, and draws up risk management measures of S company more targeted.

II. AHP Method

AHP [15] is a multi-objective decision analysis method which had been proposed by T. L. Saaty in the mid-1970s, and the method often is used for multiple optimal selections programs or risk assessment decision-making. AHP is an analysis method of the combination of qualitative and quantitative and the combination of subjective and objective, and the method possesses systematization and hierarchy.

A. Establish the Hierarchical Structure Model

In the analysis of the problems faced by the following, the factors are divided into different layers, including the target layer, criterion layer, program layer and so on. When a certain layer contains more factors (such as more than nine), the layer can be further divided into several sub-layers, as shown in Fig. 1.

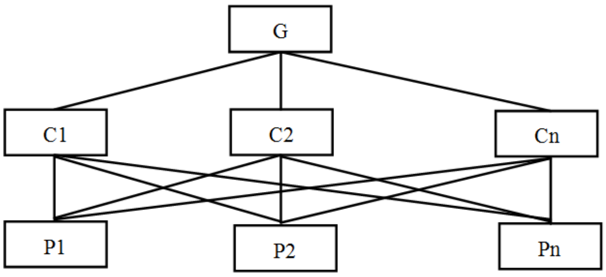

Figure 1. Hierarchical structure

B. Construct Comparison Matrixes

In the hierarchical model, the single taxis problem of the each layer elements relative to the upper layer corresponding element can be simplified to a series of judgment and comparison. That is to say, under the control of the upper element determined, the lower elements are compared, and get the comparison matrixes of the upper one element. On a certain goal or criterion, the lower two criterions or schemes always are compared, adopt Delphi method to obtain the judgment information [16], design and release the relevant information questionnaires, and please experts or professionals to fill in. According to 1-9 scale method, on the comparison of the different situations, and give the quantitative scale (Table I).

TABLE I. 1-9 Scale

Scale	Factor i and factor j compared
1	Equally important
3	Somewhat important
5	Important
7	Very important
9	Extremely important
2、4、6、8	Intermediate state

According to scaling theory [17], construct comparison matrixes, and the matrix is a square matrix: A=（a_{ij}）$_{n\times n}$, has the following properties: ① $a^{ij}>0$, ② $a^{ij}=1/a^{ji}$, ③$a^{ii}=a^{jj}=1$, which is called the positive reciprocal matrix.

$$A=\begin{pmatrix} a_{11} & K & a_{1n} \\ M & O & M \\ a_{n1} & L & a_{nn} \end{pmatrix}=\left(a_{ij}\right)_{ij}$$

C. Single Taxi Sand Consistency Test

① Calculate the result of multiplying the elements of each row Mi , See equation (1)

$$Mi=\prod_{j=1}^{n} a_{ij} \tag{1}$$

② Calculate the n-th root of Mi , see equation (2)

$$\overline{Wi}=\sqrt[n]{Mi} \tag{2}$$

③ Vector quantities Wi = （$\overline{W1}$，$\overline{W2}$，...，$\overline{Wn}$）^{T}, for normalized, see equation (3).

$$W_i=\frac{\overline{W_i}}{\sum_{i=1}^{n}\overline{Wi}} \tag{3}$$

Then W=（W^1，W^2，W^3，$\cdots$，W^n）^{T}, that is feature vector of the matrix.

④ Calculate the maximum Eigen value $\lambda_{\max}$ of the matrix, see equation (4).

$$\lambda_{\max}=\sum_{i=1}^{n}\frac{(AW)_i}{nW_i} \tag{4}$$

In the equation, $(AW)_i$ also shows the first *i* element of AW.

⑤ Consistency test

(a) Calculate the consistency index CI, see equation (5).

$$CI=\frac{\lambda_{\max-n}}{n-1} \tag{5}$$

In the equation, $\lambda_{\max}$ represents the maximum Eigen value of the matrix, and n represents the order of the matrix.

(b) According to the order n of the matrix, find out the average random consistency index RI, as shown in Table II.

TABLE II. AVERAGE RANDOM CONSISTENCY INDEX RI

	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
RI	0.00	0.00	0.58	0.90	1.21	1.24	1.32	1.41	1.45

(c) Calculate the consistency ratio CR, See equation (6).

$$CR = \frac{CI}{RI} \qquad (6)$$

If CR<0.1, the comparison matrix with satisfactory consistency, sort weights is acceptable.

D. Hierarchy Total Taxis and Consistency Test

Use all single taxis results of the same layer and it can calculate for the relative importance weights of all the elements of the layer in terms of the upper layer, which is a hierarchy total taxi. It needs be calculated in order from top to bottom by layer, for the second layer below the highest layer, single taxis is hierarchy total taxis.

Have calculated assuming the assembled power vector of the first K-1 layer's elements relative to the overall goal:

$$a^{k-1} = \left(a1^{k-1}, a2^{k-1}, ..., an^{k-1}\right)^T$$

Sort weight vector of the following elements of the first j element as a criterion of the first K layer to the first K-1 layer:

$$b_j^{\ k} = \left(b_{11}^{\ k}, b_{21}^{\ k}, ..., b_{m1}^{\ k}\right)^T$$

And form the matrix:

$$B^k = \left(b_1^{\ k}, b_2^{\ k}, ..., b_n^{\ k}\right)$$

The sort weight vector combined of the n elements of the first K layer relative to the overall goal calculated by the following formula, see equation (7).

$$a^k = B^k a^{k-1} \qquad (7)$$

For the Consistency test of the total sort weight, and also need to calculate the CI layer by layer. If you were to get the results CI^{k-1} of calculations of the first layer of K-1 layer and table look-up results RI^{k-1}, the corresponding index of the first K layer,see equation (8) And equation (9).

$$CI^k = \left(CI_1^{\ k-1}, CI_2^{\ K-1}, ..., CI_n^{\ k-1}\right)a^{k-1} \qquad (8)$$

$$RI^k = \left(RI_1^{\ k-1}, RI_2^{\ k-1}, ..., RI_n^{\ k-1}\right)a^{k-1} \qquad (9)$$

Consistency ratio of the total order of the first K layer, see equation (10).

$$CR^k = \frac{CI^k}{RI^k} \qquad (10)$$

III. THE SELECTION AND ASSESSMENT OF INFORMATION SECURITY RISK ASSESSMENT FACTORS

A. The Selection of Information Security Risk

Assessment Factors: Information security risk assessment involves four basic elements of the information assets, the vulnerabilities of information assets, the facing threats of information assets and the existent possibility risks of information assets. Information security risk assessment was launched around these basic elements, through the analysis of the vulnerabilities of assets to determine the threat may use which weaknesses to undermine its security [18].

Through the main information asset classification and value recognition of S company, according to the main information assets environment, conditions and previously threatened damage, and determine they may face the risks and their own vulnerabilities which combine with these threats, and form information security risk assessment factors list of S company [19], as shown in Table III.

TABLE III. LIST OF INFORMATION SECURITY RISK ASSESSMENT FACTORS OF S COMPANY

Criterion layer(C)	Index layer (P)
Physical Security(C1)	Equipment Security(P1) Environment Security(P2)
Platform Security(C2)	Network structure Security(P3) Operating System Security(P4) System software Security(P5)
Operation Security(C3)	Network Maintenance Security(P6) Operating System Maintenance Security(P7) Database maintenance Security(P8)
Backup Security(C4)	Database Backup Operation Security(P9) Database Backup Media Security(P10) Database Backup Protection Security(P11)
Management Security(C5)	System Strategy Security(P12) Human Resources Security(P13) Access Control Security(P14)

B. The Assessment of Information Security Risk

Assessment Factors: (1) Establish the hierarchy model of information security risk assessment of S company

According to the information security risk assessment element list of S company in Table III, and establish the hierarchy model of information security risk assessment of S company, as shown in Fig. 2.

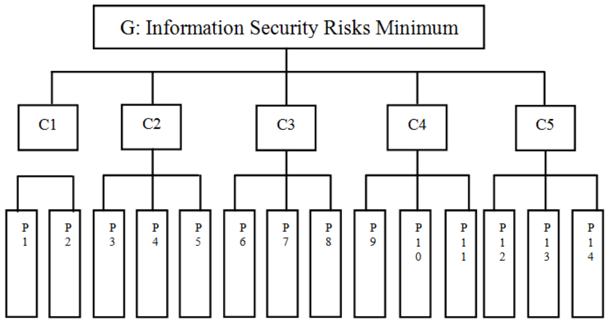

Figure 2. The hierarchy model of information security risk assessment of S company

(2) Construct the judgment matrixes of information security risk assessment of S company

According to the assessment factors and their mutual relations of the hierarchy model of information security risk assessment of S company in Fig. 2, construct the judgment matrixes, combine with the actual situation of information construction of S company, design questionnaire (slightly), and adopt Delphi method to obtain the judgment information. According to Table I, score the questionnaires, calculate them by the geometric mean, and finally convert to the values of the matrixes. Then according to equation (3) and equation (4), calculate the W value and the $\lambda_{\max}$ value of each judgment matrix.

For each matrix, according to equation (6), carry out the consistency test of the single layer. Did not pass the consistency test, further communication with the staff questionnaires, the appropriate changes and adjustments for the values, and finally pass the consistency test of the single layer until all the judgment matrixes.

Have been determined the matrixes of each layer, and according to equation (7), calculate combination weights of the layer. Then, according to equation (10), carry out the consistency test of the total layer, and get through.

The final results of the Judgment matrixes are shown in Table IV shown in Table XI(Table IV, Table V, Table VI, Table VII, Table VIII, Table IX, Table X and Table XI).

TABLE IV. THE MATRIX OF THE CRITERION LAYER C RELATIVE TO THE TARGET LAYER G

Relative to the G	C1	C2	C3	C4	C5	*Single layer weights*	*Combination weight*
C1	1	2/5	1/3	2/7	1	0.0928	0.0928
C2	5/2	1	5/8	2/5	8/5	0.1784	0.1784
C3	3	8/5	1	8/7	10/3	0.3191	0.3191
C4	7/2	5/2	7/8	1	14/9	0.2928	0.2928
C5	1	5/8	3/10	9/14	1	0.1169	0.1169

TABLE V. THE MATRIXES OF THE INDEX LAYER RELATIVE TO THE CRITERION LAYER C1

Relative to the C1	P1	p2	*Single-layer weights*	*Combination weight*
P1	1	10/3	0.7692	0.0714
P2	3/10	1	0.2308	0.0214

TABLE VI. THE MATRIXES OF THE INDEX LAYER RELATIVE TO THE CRITERION LAYER C2

Relative to the C2	P3	p4	p5	*Single-layer weights*	*Combination weight*
P3	1	3/8	3/8	0.1554	0.0277
P4	8/3	1	9/5	0.5040	0.0899
P5	8/3	5/9	1	0.3406	0.0608

TABLE VII. THE MATRIXES OF THE INDEX LAYER RELATIVE TO THE CRITERION LAYER C3

Relative to the C3	P6	p7	p8	*Single-layer weights*	*Combination weight*
P6	1	3/7	3/7	0.1761	0.0562
P7	7/3	1	4/5	0.3814	0.1217
P8	7/3	5/4	1	0.4425	0.1412

TABLE VIII. THE MATRIXES OF THE INDEX LAYER RELATIVE TO THE CRITERION LAYER C4

Relative to the C4	P9	p10	p11	*Single-layer weights*	*Combination weight*
P9	1	21/8	29/8	0.5939	0.1739
P10	8/21	1	16/7	0.2676	0.0784
P11	8/29	7/16	1	0.1385	0.0406

TABLE IX. THE MATRIXES OF THE INDEX LAYER RELATIVE TO THE CRITERION LAYER C5

Relative to the C5	P12	p13	p14	*Single-layer weights*	*Combination weight*
P12	1	3/8	16/7	0.2691	0.0315
P13	8/3	1	10/3	0.5869	0.0686
P14	7/16	3/10	1	0.1440	0.0168

TABLE X. THE CONSISTENCY TEST RESULTS OF THE EACH MATRIX

The matrixes	$\lambda_{\max}$	*CI*	*RI*	*CR*	*The test results of Consistency*
G	5.1242	0.0311	1.2100	0.0257	CR <0.1, Through the consistency test.
C1	2.0000	0.0000	0.0000		C1 is a positive reciprocal matrix, CI = 0 meet the test.
C2	3.0685	0.0193	0.5800	0.0332	CR <0.1, Through the consistency test.
C3	3.0056	0.0028	0.5800	0.0048	CR <0.1, Through the consistency test.
C4	3.0282	0.0141	0.5800	0.0243	CR <0.1, Through the consistency test.
C5	3.0406	0.0203	0.5800	0.0350	CR <0.1, Through the consistency test.

TABLE XI. THE CONSISTENCY TEST RESULTS OF THE TOTAL INDEX LAYER

CI	a	$CI \times a$	RI	a	$RI \times a$
0.0000	0.0928	0.0000	0.0000	0.0928	0.0000
0.0193	0.1784	0.0034	0.5800	0.1784	0.1035
0.0028	0.3191	0.0009	0.5800	0.3191	0.1851
0.0141	0.2928	0.0041	0.5800	0.2928	0.1698
0.0203	0.1169	0.0024	0.5800	0.1169	0.0678
$CI(p) = \sum CI \times a = 0.0108$			$RI(p) = \sum RI \times a = 0.5262$		

$$CR(p) = \frac{CI(p)}{RI(p)} = 0.0205 < 0.1’$$

Through the consistency test.

C. The Combination Weight Sort of the Criterion Layer and Index Layer

According to Table IV and Table IX, calculating criterion layer weights and index layer combination weights, collecting and descending order, in order to manage the risk factors which have larger relative coefficient and larger effect, as shown in Table XII.

TABLE XII. THE COMBINATION WEIGHTS IN DESCENDING ORDER

The criterion layer C		*The index layer P*	
C3	0.3191	P9	0.1739
C4	0.2928	P8	0.1412
C2	0.1784	P7	0.1217
C5	0.1169	P4	0.0899
C1	0.0928	P10	0.0784
		P1	0.0714
		P13	0.0686
		P5	0.0608
		P6	0.0562
		P11	0.0406
		P12	0.0315
		P3	0.0277
		P2	0.0214
		P14	0.0168

D. The Criterion Layer Weight Sorting Figure and the Index Layer Weight Sorting Figure

According to Table XII, using Excel to generate the criterion layer weight sorting figure and the index layer weight sorting figure, as shown in Fig. 3 and Fig. 4.

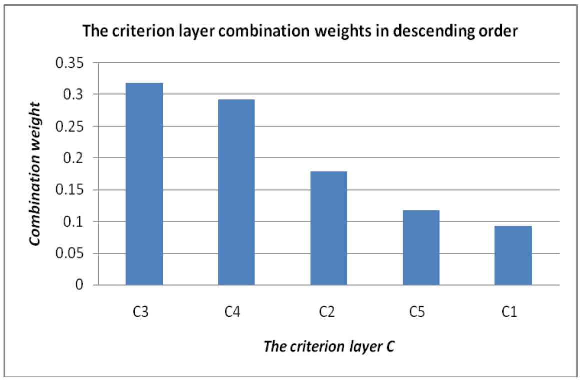

Figure 3. The criterion layer combination weights in descending order

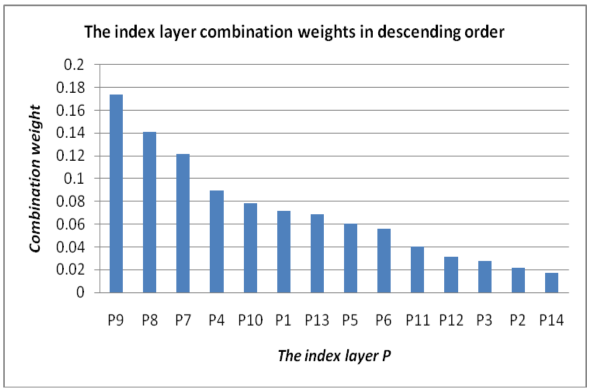

Figure 4. The index layer combination weights in descending order

IV. CONCLUSION

In order to ensure the risk factors' management measures formulated are more targeted, we set the criterion layer weight > 0.15 and the index layer weight > 0.05, and then manage the risk factors. According to Table XII, Fig. 3 and Fig. 4, Platform Security (C2), Operation Security (C3) and Backup Security (C4) are the three major risk factors of the criterion layer in the hierarchy model of information security risk assessment of S company. The key risk factors of the index layer associated with the three major risk factors (C2,C3,C4) of the criterion layer: (a) Operating System Security(P4) and System software Security(P5)belong to Platform Security(C2); (b) Network Maintenance Security(P6), Operating System Maintenance Security(P7) and Database maintenance Security(P8) belong to Operation Security(C3); (c) Database Backup Operation Security(P9) and Database Backup Media Security(P10) belong to Backup Security(C4); (d) and Equipment Security(P1) which belongs to Physical Security(C1) and Human Resources Security(P13) which belongs to Management Security(C5) also be the key risk factors we should pay attention to.

Through the above analysis, in order to ensure the information resources' security of S company, the information security management of S company should do the following aspects in the future:

(a) to strengthen the management work of Platform Security(C2), and ensure Operating System Security(P4) and System software Security(P5).

(b) to strengthen the management work of strengthen Operation Security(C3), and achieve real-time monitoring, scanning and detection system vulnerabilities and viruses, find vulnerabilities in time to install the system patch, and discover the virus and timely update antivirus software and virus check, kill, or physical isolation.

(c) to strengthen the management work of Backup Security(C4), and do a database backup using specialist, timing backup and high quality backup medium, and not regularly check the effectiveness and availability of the backup data.

(d) to strengthen the management work of Equipment Security(P1) and Human Resources Security(P13),and recommend the use of implementation guides on the equipment security and human resource security management in the ISO/IEC27001 standard for management [20].

In summary, by using the analytic hierarchy process (AHP) to assess information security risk factors of S company, we can intuitively grasp the harm degree of various risks and more pertinently develop measures to control the information security risk assess. At the same time, the article also provides reference for small- and medium-sized enterprise information security risk management at home and abroad.

ACKNOWLEDGMENT

The work is supported by Hainan Social Science Fund (Project Number: HNSK （YB）15-31) and the Fund of People's Government of Wanning City, Hainan Province (Project Number: 20130121).

REFERENCES

[1] Y. Liu and W. D. Gu, "Survey of information security risk assessment research," *Journal of Qingdao University(E&T)*, vol. 23, no. 2, pp. 37-43, June 2008.

[2] D. G. Feng, Y. Zhang, and Y. Q. Zhang, "Survey of information security risk assessment," *Journal of China Institute of Communications*, vol. 25, no. 7, pp. 10-18, July 2004.

[3] R. Gallagher, "Risk management: A new phase of cost control," *The Harvard Business Review*, 1993.

[4] P. Y. Li, *Research on the Quantitative Methods of Information Security Risk Assessment Based on AHP*, Nanchang: Jiangxi University of Finance & Economics, 2012.

[5] National Institute of Standards and Technology, "Special Publications 800-30, Risk Management Guide (DRAFT)," June 2001.

[6] United States General Accounting Office, Accounting and Information Management Division, "Information Security Risk Assessment," August 1999.

[7] S. A. Butler and P. Fischbeck, "Multi-attribute risk assessment," *Technical Report CMD-CS-01-169*, December 2001.

[8] T. R. Peltier, "Information security risk assessment," *Rothstein Associates Inc*, 2001.

[9] S. A. Butler, "Security attribute evaluation method: A cost-benefit approach," *Computer Science Department*, 2001.

[10] P. P. Sun, *Research and Development of Information Security Risk Assessment System*, Beijing: Beijing Jiaotong University, 2004.

[11] T. Li, *Network Security Generality-- Security Technology Series*, Beijing: Publishing House of Electronics Industry, 2004, pp. 44-45.

[12] Y. K. Wang, "Evaluation model of scientific research project based on the principle of Delphi and AHP," *Journal of Shanxi Finace and Economics University*, vol. 23, pp. 148-149, December 2001.

[13] H. T. Li, Y. Liu, and D. Q. He, "Review on study of risk evaluation for IT system security," *China Safety Science Journal*, vol. 16, no. 1, pp. 108-113, January 2006.

[14] F. S. Liu, *Research and Design of Information Security Risk Assessment System Based on AHP*, Tianjing: Nankai University, 2006.

[15] S. B. Xu, *AHP Principle*, *Tianjin University Press*, 1993.

[16] W. Chen, T. J. Fang, and Y. J. Ma, "Research on group decision and application based on Delphi method and AHP method," *Computer Engineering*, vol. 29, pp. 18-20, April 2003.

[17] T. P. He and L. Cheng, "The application of AHP in safety assessment chemical industrial park," *Journal of Safety Science and Technology*, vol. 8, pp. 81-84, August 2008.

[18] S. Zhang and Y. H. Chen, "The theoretical research of information security risk assessment," *Journal of Shanxi Finance and Economics University*, vol. 30, pp. 193-195, April 2008.

[19] H. Luo, "Research and application of information security evaluation method," *Beihang University Degree Thesis*, *Wanfang Data*, pp. 43-49, July 2004.

[20] Information Technology-Security Techniques-Code of Practice for Information Security Management, ISO/IEC27001-2005.

Meng Meng, male, born in December 1977, master degree, assistant researcher, certified information system auditor. Since July 2008, in Institute of Scientific and Technical Information, Chinese Academy of Tropical Agricultural Sciences, mainly engaged in tropical agricultural products quality safety traceability research, information security risk assessment and management research, etc. In recent years, presided over or participated in 7 research projects of the provincial and ministerial, published more than 12 papers, 1 article has indexed by EI and 1 article has indexed by ISTP. Have Science and Technology Progress Awards of Hainan. Have 9 software copyrights.

Enping Liu, corresponding author, male, born in March 1965, professor, Master degree Supervisor, mainly engaged in tropical agricultural economy, tropical agricultural industry information monitoring and early warning. In recent years, presided over 10 research projects of the provincial and ministerial, published more than 30 papers, 1 article has indexed by SCI and edited books. Have Science and Technology Progress Awards of Hainan. Have 3 software copyrights.