Research on Security Risk Assessment Based on the Improved FAHP

Wenmin Li[1,*], **Ye Liang**[2], **Wenyu Wang**[1], **Xueqi Jin**[3], **Piaohong Kong**[3], **Zhengwei Jiang**[3] **and Lisong Shao**[2]

[1]State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China
[2]NARI Group Corporation, Nanjing 211106, China
[3]State Grid Zhejiang Electric Power Co. Ltd., Hangzhou 310007, China
*liwenmin02@outlook.com

Abstract. In order to reduce the subjectivity of information security risk assessment process and improve assessment efficiency, we propose a new method of information security risk assessment based on improved FAHP (Fuzzy Analytic Hierarchy Process) to analyse the information security-related standards for domestic and international risk assessment. We establish a Hierarchical Security Assessment Model and introduce refinement indicators and Intuitionistic Fuzzy Sets to reduce subjective judgment factors in the assessment of traditional risk. We then applied an e-commerce company in case analyse the security risk and the results are satisfactory and in line with the actual situation of the company. The indicator system of this method is more objective and comprehensive and the evaluation process is more efficient, which provide new ideas for risk assessment of existing information security companies.

1. Introduction

Network security threats such as APT and account fraud are increasing unabated and the scope of which is extending and threat every internet user. The threat posed by new technologies such as cloud computing and big data, which need to be solved, are making urgent security issues. In December 2017, Gartner predicted[1] that the total security expenditure of global enterprises will reach 96.3 billion dollars next year, an increase of 8% compared with 2017. In order to ensure the safety of the organization business, safety investment will be increased within five years. Besides, it is an inevitable trend to ensure the rationality, compliance and correctness of business security with the help of internal and external forces.

Information Security Risk Assessment is an assessment of the threat, vulnerability and hidden risk in an organization's information security management system, which runs through the organization, strategy, operation, technology, evaluation and other stages of the information security system [2].

Laarhoven et al. [3] first proposed the combination of AHP and Fuzzy theory in 1983. Bian et al. [4] combined AHP with fuzzy comprehensive evaluation by using AHP_FCE model, taking into account the complexity of relationship within the system and the fuzziness of value system. Gu et al. [5] combined with three evaluation technologies AHP-FAHP-FCE to build a model and solve the security situation evaluation from different perspectives. Zhao et al. [6] used AHP and Fuzzy Logic method to evaluate the risk of network security and wireless network security respectively. Yu et al. [7] analyzed the risk factors involved in the information system with the help of the Fuzzy Sets theory and gave the level description. However, these methods do not completely get rid of the subjective influence of experts' evaluation of the judgment matrix. At the same time, due to the high complexity of the evaluation method and the high industry barriers, the theoretical research is far from the practical application, and there is no real practical risk evaluation scheme.

In this paper, a Fuzzy Analytic Hierarchy Process (FAHP) based information security risk assessment scheme is proposed. The objective and perfect general index system is used to replace the subjective evaluation of experts in the traditional assessment process. A scientific hierarchical security assessment model is established from the five dimensions of risk analysis, risk prevention, risk control, risk treatment, monitoring and improvement, and the detailed index system and Intuitionistic Fuzzy Sets are combined, which makes complex theoretical research more practical.

2. Construction of Information Security Risk Assessment Scheme Index System

2.1. *Risk Assessment Related Definitions*

According to GB / T 20498-2007 [8], the function of assessing information security risk is as follows:

$$r=\varphi(w,v,t) \tag{1}$$

Where r, w, v and t respectively represent information security risk value, asset scope, vulnerability impact and consequences caused by threats. Security risk needs to consider the possibility and impact of risks. Vulnerability comes from organizational assets, and threats use vulnerability to cause risk impact on the organization. Therefore, a scientific and comprehensive risk assessment index system should cover w, v, t and related aspects, so as to make the most objective and real assessment of the complex information security management system.

2.2. *Index System Construction*

This paper divides the information security index system into target level, criterion level (primary indicator) and indicator level (secondary indicator) according to the hierarchical concept of AHP method, covering five aspects: strategy, organization, operation, technology and evaluation. The criterion level consists of five dimensions including risk analysis, risk prevention, risk control, risk treatment and monitoring and improvement, as shown in Table 1:

Table 1. Information security risk assessment index system

target level	criterion level	indicator level
Risk Assessment(A)	Risk Analysis(B_1)	Business Concept (C_1) , Risk Identification (C_2) Risk Classification (C_3)
	Risk Prevention(B_2)	Security Organizations (C_4), Training And Drill (C_5) Business Continuity (C_6)
	Risk Control(B_3)	Security Strategy And Procedures(C_7), Personnel Safety (C_8), Physical Environment Security (C_9), Network Partition (C_{10}) Access Control (C_{11})
	Risk Treatment (B_4)	Event Response (C_{12}), System Maintenance (C_{13}) Information And Document Management (C_{14})
	Monitoring and Improvement (B_5)	Consistency (C_{15}) Review of Improvement And Maintenance (C_{16})

Risk analysis consists of three secondary indicators: business concept, risk identification and risk classification. Risk prevention includes three secondary indicators: safety organization, training and drill, and business continuity. Risk control includes five secondary indicators: security strategies and regulations, personnel security, physical environment security, network partition and access control. Risk management consists of three secondary indicators: event response, system maintenance and information and document management. Monitoring and improvement are composed of two secondary indicators: consistency, review improvement and maintenance.

3. Information Security Risk Assessment based on FAHP

3.1. Overview of Intuitionistic Fuzzy Sets

The Fuzzy Analytic Hierarchy Process (FAHP) overcomes the limitations of the traditional analytic hierarchy process, such as the difficulty of matrix consistency, the complexity of adjusting the judgment matrix to meet the consistency [9], and increases the objectivity of the evaluation results.

Definition 1 [10-11] if x is a fixed non-empty set, $A = \{\langle x, \mu_A(x), \nu_A(x)\rangle | x \in X\}$, such triples are Intuitionistic Fuzzy Set, where $\mu_A(x), \nu_A(x)$ represent the membership and non-membership degree of the element x in X, and satisfy $\mu_A\colon \mathrm{X} \longrightarrow [0,1], \nu_A\colon \mathrm{X} \longrightarrow [0,1], 0 \le \mu_A(x) + \nu_A(x) \le 1, x \in X$.

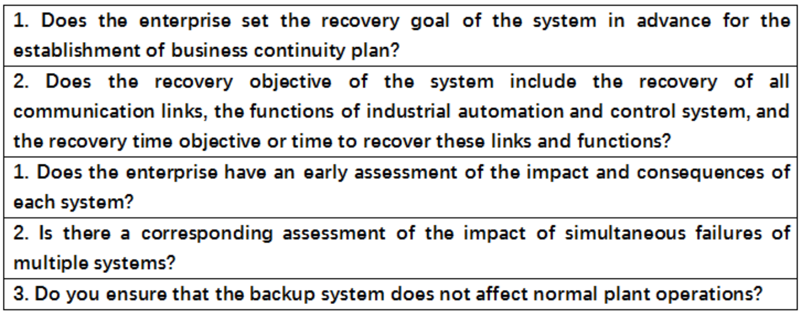
Definition 2 [10-11] In every Fuzzy Set of $\mathrm{X}, \pi_A(x) = 1 - \mu_A(x) - \nu_A(x)$ is the degree of hesitation that element x belongs to X, and $0 \le \pi_A(x) \le 1, x \in X$.

Intuitionistic Fuzzy Set in this paper is $\alpha = (\mu_\alpha, \nu_\alpha, \pi_\alpha)$, We describe the corresponding risk assessment index questionnaire. For example,$(\mu_\alpha, \nu_\alpha, \pi_\alpha) = (0.6, 0.3, 0.1)$, or$\mu_\alpha = 0.6, \nu_\alpha = 0.3, \pi_\alpha = 0.1$. The meaning is: suppose there are ten detailed questions in a secondary index of the index questionnaire, among which 6 questions are "Yes", 3 questions are "No", and 1 question is "Not Sure ".

3.2. Information Security Risk Assessment Process

3.2.1. Construction of information security risk assessment index system

According to the hierarchical concept of AHP method, the information security index system is divided into target layer, criterion layer and indicator layer. The criterion layer is composed of five dimensions, which are risk analysis, risk prevention, risk control, risk treatment, monitoring and improvement, as shown in table 1. An instance of the detailed questionnaire part of the indicator system is shown in Figure 1.



1. Does the enterprise set the recovery goal of the system in advance for the establishment of business continuity plan?
2. Does the recovery objective of the system include the recovery of all communication links, the functions of industrial automation and control system, and the recovery time objective or time to recover these links and functions?
1. Does the enterprise have an early assessment of the impact and consequences of each system?
2. Is there a corresponding assessment of the impact of simultaneous failures of multiple systems?
3. Do you ensure that the backup system does not affect normal plant operations?

Figure 1. Business continuity indicator refinement questionnaire

3.2.2. Construction of judgment matrix of Intuitionistic Fuzzy Sets

According to the importance preference degree of information security indicators, this paper defines the quantitative scale of importance evaluation [26], as shown in Table 2.

Table 2. Quantitative scale of importance

Importance evaluation	Intuitionistic Fuzzy number
Factor i is much more important than factor j	(0.90,0.10,0.00)
Factor i is much more important than factor j	(0.80,0.15,0.05)
Factor i is more important than factor j	(0.70,0.20,0.10)
Factor i is more important than factor j	(0.60,0.25,0.15)
Factor i is as important as factor j	(0.50,0.30,0.20)
Factor j is more important than factor i	(0.40,0.45,0.15)
Factor j is more important than factor i	(0.30,0.60,0.10)
Factor j is much more important than factor i	(0.20,0.75,0.05)
Factor j is much more important than factor i	(0.10,0.90,0.00)

We construct the judgment matrix of Intuitionistic Fuzzy Sets. The judgment matrix of Intuitionistic Fuzzy Sets is $R = \left(r_{ij}\right)_{n\times n} (i, j = 1,2 \ldots n)$, i and j respectively represent the rows and columns of the matrix, where $r_{ij} = \left(\mu_{ij}, \nu_{ij}\right)$, μ_{ij} indicates the importance of index i relative to index j, γ_{ij} indicates the importance of index j relative to index I, and $0 \le \mu_{ij} + \nu_{ij} \le 1$. In order to convert the scoring results of the index questionnaire into the relative importance elements of the judgment matrix of Intuitionistic Fuzzy Sets, this paper considers the universality of the safety index and the rationality of the limit case, and defines the fuzzy mapping matrix $M = (m_{ij})_{n\times n}$ by combining the fitting function with the quantitative scale, where i and j respectively represent the rows and columns of the matrix, and m_{ij} represents two comparative indexes. The importance of index with score i compared with index with score j is m_{ij}. A complete judgment matrix of Intuitionistic Fuzzy Sets can be obtained by normalizing the reciprocal distance of the four vertices mapped to the matrix region as the weight. The pseudo code is given in algorithm 1.

algorithm **1:** Inverse distance normalized weighting

```
Input: Fuzzy mapping matrix $M$, 0-1 cut distance, list $A$ of Fuzzy Membership Degree of each index;
Output: Judgment matrix of Intuitionistic Fuzzy Sets $R = \left(r_{ij}\right)_{n\times n}$;
for $index = i$ in $A$ do
    for $index = j$ in $A$ do
        Solve the minimum rectangle position of $(A[i], A[j])$ in M, and get the four vertex coordinates $LU, LB, RU, RB$ of the rectangle.
        Calculate the distance between $(A[i], A[j])$ and the vertex of the rectangle, and get the values of D_LU,D_LB,D_RU,D_R.
        Normalized distance: Norm(D_LU, D_LB, D_RU, D_RB);
        Weighted weight: $M[i][j] = S[i][j] \times D\_LU + S[i+1][j] \times D\_RU + S[i][j+1] \times D\_LB + S[i+1][j+1] \times D\_RB$
    end for
end for
```

3.2.3. Construction consistency judgment matrix of Intuitionistic Fuzzy Sets

In this paper, $\mathrm{\bar{R}} = \left(\mathrm{\bar{r}_{ij}}\right)_{\mathrm{n\times n}}$, $\mathrm{\bar{r}_{ij}} = \left(\bar{\mu}_{\mathrm{ij}}, \bar{\nu}_{\mathrm{ij}}\right)$ is used to express the consistency judgment matrix of Intuitionistic Fuzzy Sets, which is based on the judgment matrix $\mathrm{R} = \left(\mathrm{r_{ij}}\right)_{\mathrm{n\times n}}$, $\mathrm{r_{ij}} = \left(\mu_{\mathrm{ij}}, \nu_{\mathrm{ij}}\right)$, The process is as follows [25]:

(1) When $\mathrm{j > i + 1}$:

$$\mu_1 = \sqrt[\mathrm{j-i-1}]{\prod_{\mathrm{t=i+1}}^{\mathrm{j-1}} \mu_{\mathrm{it}}\mu_{\mathrm{tj}}}, \mu_2 = \sqrt[\mathrm{j-i-1}]{\prod_{\mathrm{t=i+1}}^{\mathrm{j-1}} (1-\mu_{\mathrm{it}})(1-\mu_{\mathrm{tj}})}, \bar{\mu}_{\mathrm{ij}} = \frac{\mu_1}{\mu_1+\mu_2} \tag{2}$$

$$\nu_1 = \sqrt[j-i-1]{\prod_{t=i+1}^{j-1} \nu_{it}\nu_{tj}}, \nu_2 = \sqrt[j-i-1]{\prod_{t=i+1}^{j-1} (1-\nu_{it})(1-\nu_{tj})}, \bar{\nu}_{ij} = \frac{\nu_1}{\nu_1+\nu_2} \tag{3}$$

(2)When $\mathrm{j < i}$, $\mathrm{\bar{r}_{ij}} = \left(\bar{\nu}_{\mathrm{ji}}, \bar{\mu}_{\mathrm{ji}}\right)$;

(3)When $\mathrm{j = i + 1}$, $\mathrm{\bar{r}_{ij}} = \left(\mu_{\mathrm{ij}}, \nu_{\mathrm{ij}}\right)$.

3.2.4. Consistency test

According to the distance measure between Fuzzy Sets [13][14], the consistency test process of the judgment matrix of Fuzzy Sets is as follows [13]:

$$\Delta_\mu = \sum_{i=1}^{n}\sum_{j=1}^{n}\left(\left|\bar{\mu}_{ij} - \mu_{ij}\right|\right), \Delta_\nu = \sum_{i=1}^{n}\sum_{j=1}^{n}\left(\left|\bar{\nu}_{ij} - \nu_{ij}\right|\right), \Delta_\pi = \sum_{i=1}^{n}\sum_{j=1}^{n}\left(\left|\bar{\pi}_{ij} - \pi_{ij}\right|\right),$$

$$d(\bar{R}, R) = \left(\Delta_\mu + \Delta_\nu + \Delta_\pi\right)/2(n-1)(n-2) \tag{4}$$

Where R is the judgment matrix of Intuitionistic Fuzzy Sets, $\bar{R}$ is the consistency judgment matrix of Intuitionistic Fuzzy Sets, $\mathrm{i},\mathrm{j} = 1,2 \ldots \mathrm{n}$. If $d(\bar{R},R) < 0.1$, then $\bar{R}$ passes the consistency test. If $d(\bar{R},R) \geq 0.1$, it needs to adjust the consistency.

3.2.5. *Consistency adjustment*

When $\bar{R}$does not meet the consistency, the iterative parameter σ needs to be introduced, and the value of σ needs to be reduced in a certain step to change the consistency judgment matrix of Intuitionistic Fuzzy Sets, so that it finally meets the consistency condition. In this paper, $\sigma = 1(\sigma > 0)$, and $\text{the step} - 0.01$ is used for iteration. The process is as follows [13]:

$$\tilde{\mu}_{ij} = \frac{(\mu_{ij})^{1-\sigma}(\bar{\mu}_{ij})^{\sigma}}{(\mu_{ij})^{1-\sigma}(\bar{\mu}_{ij})^{\sigma}+(1-\mu_{ij})^{1-\sigma}(1-\bar{\mu}_{ij})^{\sigma}} \quad \tilde{\nu}_{ij} = \frac{(\nu_{ij})^{1-\sigma}(\bar{\nu}_{ij})^{\sigma}}{(\nu_{ij})^{1-\sigma}(\bar{\nu}_{ij})^{\sigma}+(1-\nu_{ij})^{1-\sigma}(1-\bar{\nu}_{ij})^{\sigma}} \tag{5}$$

Where $\mathrm{i},\mathrm{j} = 1,2 \ldots \mathrm{n}$. Through the above formula, the consistency judgment matrix of the adjusted Intuitionistic Fuzzy Sets $\tilde{R} = \left(\widetilde{r_{ij}}\right)_{n\times n}, \widetilde{r_{ij}} = \left(\tilde{\mu}_{ij}, \tilde{\nu}_{ij}\right)$ is obtained, and the consistency is checked again by publicity (6). If it is satisfied, the consistency is checked. If it is not satisfied, step (5) is repeated until it passes the consistency test.

$$\Delta_{\mu}= \sum_{i=1}^{n}\sum_{j=1}^{n}\left(\left|\tilde{\mu}_{ij} - \mu_{ij}\right|\right), \Delta_{\nu}= \sum_{i=1}^{n}\sum_{j=1}^{n}\left(\left|\tilde{\nu}_{ij} - \nu_{ij}\right|\right), \Delta_{\pi}= \sum_{i=1}^{n}\sum_{j=1}^{n}\left(\left|\tilde{\pi}_{ij} - \pi_{ij}\right|\right),$$
$$d\left(\tilde{R},R\right) = \left(\Delta_{\mu} + \Delta_{\nu} + \Delta_{\pi}\right)/2(n-1)(n-2) \tag{6}$$

3.2.6. *Determine the weight*

Finally, the weight of each index is calculated by the consistency judgment matrix of Intuitionistic Fuzzy Sets through consistency test, as formula (7), where $i,j = 1,2 \ldots n$.

$$\omega_i = \left(\frac{\sum_{j=1}^{n}\bar{\mu}_{ij}}{\sum_{i=1}^{n}\sum_{j=1}^{n}(1-\bar{\nu}_{ij})}, 1 - \frac{\sum_{j=1}^{n}(1-\bar{\nu}_{ij})}{\sum_{i=1}^{n}\sum_{j=1}^{n}\bar{\mu}_{ij}}\right) \tag{7}$$

3.2.7. *Final evaluation results*

According to the operation rule of Intuitionistic Fuzzy Sets[15], the weights of each secondary index and its corresponding primary index are weighted and carried out set operation, and the process is as follows [13]:

$$\omega_1 \otimes \omega_2 = \left(\mu_{\omega1}\mu_{\omega2}, \nu_{\omega1}+\nu_{\omega2} - \nu_{\omega1}\nu_{\omega2}\right), \omega_1 \oplus \omega_2 = \left(\mu_{\omega1} + \mu_{\omega2} - \mu_{\omega1}\mu_{\omega2}, \nu_{\omega1}\nu_{\omega2}\right) \tag{8}$$

Calculate the weight of indicators at all levels as formula (9), refer to the index system in this paper, $n = 16, j = 5$. Calculate total weight as formula (10). In order to facilitate the rating of the organization's security status, this paper defines the scoring function of information security risk assessment according to the actual situation as formula (11).

$$\omega(C_i) = \omega_{B_j} \otimes \omega_{C_i}, i = 1,2 \ldots n, j = 1,2 \ldots m \tag{9}$$

$$W = \oplus_{i=1}^{n}\omega(C_i) \; = 1,2 \ldots n \tag{10}$$

$$h(W) = 1 - 0.5(1 - \mu_W)(1 + \pi_W) \tag{11}$$

3.2.8. *Maturity level division*

In this paper, CMMI [16] is used as the basis for the classification of information security level. Combined with the final evaluation results, the model is divided into five levels (initial level, spontaneous management level, process definition level, quantitative control level and optimal level) by using interval division method, which marks the five levels of maturity of enterprise information security capability, as shown in Table 3.

Table 3. Enterprise information security maturity classification

Maturity level	Grade standards	Interval
Initial Level 1	The importance and necessity of this safety control measure have been realized, but no standardized process or mode has been formed, and the implementation and management of the control measure are unorganized.	(0,0.2)
Spontaneous Management Level 2	It has started to follow some conventional process or mode, but it lacks of documented and standardized system support, and there is no education, training and responsibility definition related to it.	(0.2,0.4)
Process Definition Level 3	It has been supported by standardized and documented systems, as well as related education, training and responsibility definitions, but it is difficult to find problems in the implementation process due to the lack of monitoring and quantitative management.	(0.4,0.6)
Quantitative Control Level 4	Comprehensive monitoring and quantitative management have been implemented to ensure that the implementation process is carried out in strict accordance with the system requirements, and automation tools are also applied to this control measure.	(0.6,0.8)
Optimal Level 5	It has reached or exceeded the level of best practice, and made continuous improvement according to the implementation effect or reference benchmark level.	(0.8,1)

4. Case Analysis-an E-Commerce Company

4.1. Information Security Risk Assessment of

Taking an e-commerce company A as an example, this paper makes a risk assessment on the current situation of information security of the e-commerce company by using the improved FAHP scheme. The company has 11 departments, including management, business travel business department and credit business department, and 11 people participate in filling in the information security index questionnaire. Due to the length, this paper only shows the process of evaluating the results of one of the questionnaires.

4.2. Construction of judgment matrix of Intuitionistic Fuzzy Sets

5 primary indicators and 16 Secondary indicators of the questionnaire are as S_B, S_C : After normalization and algorithm 1 processing, the Intuitionistic Fuzzy Sets judgment matrix R_B of the primary indicators is obtained:

$$S_B=\left\{\begin{matrix} & (33,10,9) & (39,12,5) & \\ (102,13,23) & (52,9,12) & (26,4,8) \end{matrix}\right\} S_C=\left\{\begin{matrix} (2,0,3) & (12,5,3) & (19,5,3) & (9,5,0) \\ (18,4,1) & (12,3,4) & (12,1,4) & (14,3,3) \\ (20,1,5) & (6,0,3) & (50,8,8) & (20,1,5) \\ (21,4,4) & (11,4,3) & (11,2,4) & (15,2,4) \end{matrix}\right\}$$

$$R_B=\begin{bmatrix} (0.50,0.30) & (0.45,0.30) & (0.45,0.27) \\ (0.60,0.30) & (0.50,0.30) & (0.50,0.27) \\ (0.60,0.35) & (0.50,0.35) & (0.50,0.30) \\ (0.55,0.35) & (0.50,0.35) & (0.70,0.30) \\ (0.60,0.35) & (0.50,0.35) & (0.60,0.30) \\ & (0.45,0.27) & (0.45,0.27) \\ & (0.50,0.27) & (0.50,0.27) \\ & (0.55,0.30) & (0.60,0.30) \\ & (0.50,0.30) & (0.70,0.30) \\ & (0.60,0.35) & (0.50,0.30) \end{bmatrix}$$

4.3. Consistency Test

First, the consistency judgment matrix $\bar{R}_B$ of Intuitionistic Fuzzy Sets of the primary indicators is obtained by formula (2) and (3) , and then $d(\bar{R}_B,R_B) \approx 0.4335>0.1$ is obtained by formula (4), which does not meet the consistency condition. Using the same method, the consistency judgment matrix of Intuitionistic Fuzzy Sets of secondary indicators, $\bar{R}_{C_1}, \bar{R}_{C_2}, \bar{R}_{C_3}, \bar{R}_{C_4}, \bar{R}_{C_5}$, is obtained.

$$\bar{R}_B = \begin{bmatrix} (0.50,0.50) & (0.45,0.30) & (0.45,0.14) \\ (0.30,0.45) & (0.50,0.50) & (0.50,0.27) \\ (0.14,0.45) & (0.27,0.50) & (0.50,0.50) \\ (0.14,0.45) & (0.14,0.50) & (0.30,0.50) \\ (0.14,0.45) & (0.14,0.50) & (0.16,0.50) \\ & (0.45,0.14) & (0.45,0.14) \\ & (0.50,0.14) & (0.50,0.14) \\ & (0.55,0.30) & (0.50,0.16) \\ & (0.50,0.50) & (0.70,0.30) \\ & (0.30,0.50) & (0.50,0.50) \end{bmatrix} \bar{R}_{C_3} = \begin{bmatrix} (0.50,0.50) & (0.50,0.30) & (0.60,0.16) \\ (0.30,0.50) & (0.50,0.50) & (0.60,0.30) \\ (0.16,0.65) & (0.30,0.60) & (0.50,0.50) \\ (0.16,0.65) & (0.16,0.78) & (0.30,0.70) \\ (0.16,0.60) & (0.16,0.60) & (0.16,0.78) \\ & (0.65,0.16) & (0.60,0.16) \\ & (0.78,0.16) & (0.60,0.16) \\ & (0.70,0.30) & (0.78,0.16) \\ & (0.50,0.50) & (0.60,0.30) \\ & (0.30,0.60) & (0.50,0.50) \end{bmatrix}$$

$$\bar{R}_{C_1} = \begin{bmatrix} (0.50,0.50) & (0.40,0.45) & (0.35,0.23) \\ (0.45,0.40) & (0.50,0.50) & (0.45,0.27) \\ (0.33,0.28) & (0.56,0.36) & (0.50,0.50) \end{bmatrix} \bar{R}_{C_4} = \begin{bmatrix} (0.50,0.50) & (0.70,0.30) & (0.78,0.19) \\ (0.30,0.70) & (0.50,0.50) & (0.60,0.35) \\ (0.19,0.78) & (0.35,0.60) & (0.50,0.50) \end{bmatrix}$$

$$\bar{R}_{C_2} = \begin{bmatrix} (0.50,0.50) & (0.55,0.25) & (0.60,0.13) \\ (0.25,0.55) & (0.50,0.50) & (0.55,0.30) \\ (0.13,0.60) & (0.30,0.55) & (0.50,0.50) \end{bmatrix} \bar{R}_{C_5} = \begin{bmatrix} (0.50,0.50) & (0.45,0.30) \\ (0.30,0.45) & (0.50,0.50) \end{bmatrix}$$

Then, by formula (5), we take σ=1 and iterate with step size − 0.01, so that it finally meets the consistency constraint condition. Finally, when σ=0.19, we get the adjusted consistency judgment matrix $\tilde{R}_B$ of Intuitionistic Fuzzy Sets. After the test by formula (8), $d(\tilde{R}_B,R_B) \approx 0.0977<0.1$, the consistency test is passed. The same process is used to deal with the secondary index layer. After iteration, $d(\tilde{R}_{C_1},R_{C_1}) \approx 0.0958$, $d(\tilde{R}_{C_2},R_{C_2}) \approx 0.0972$, $d(\tilde{R}_{C_2},R_{C_2}) \approx 0.0999$, $d(\tilde{R}_{C_2},R_{C_2}) \approx 0.0959$, σ are 0.13, 0.11, 0.18, 0.10 respectively, and the adjusted judgment matrices of consistency of Intuitionistic Fuzzy Sets are $\tilde{R}_{C_1}, \tilde{R}_{C_2}, \tilde{R}_{C_3}, \tilde{R}_{C_4}, \tilde{R}_{C_5}$, as follows:

$$\tilde{R}_{C_2} = \begin{bmatrix} (0.50,0.32) & (0.55,0.25) & (0.51,0.23) \\ (0.51,0.46) & (0.50,0.32) & (0.55,0.30) \\ (0.45,0.47) & (0.52,0.32) & (0.50,0.32) \end{bmatrix} \tilde{R}_{C_5} = \begin{bmatrix} (0.50,0.50) & (0.45,0.30) \\ (0.30,0.45) & (0.50,0.50) \end{bmatrix}$$

$$\tilde{R}_{C_1} = \begin{bmatrix} (0.32,0.32) & (0.40,0.45) & (0.35,0.33) \\ (0.58,0.27) & (0.50,0.32) & (0.45,0.27) \\ (0.33,0.28) & (0.56,0.36) & (0.50,0.32) \end{bmatrix} \tilde{R}_{C_4} = \begin{bmatrix} (0.50,0.31) & (0.70,0.30) & (0.58,0.33) \\ (0.57,0.37) & (0.50,0.32) & (0.60,0.35) \\ (0.50,0.32) & (0.44,0.30) & (0.50,0.32) \end{bmatrix}$$

$$\tilde{R}_B = \begin{bmatrix} (0.50,0.33) & (0.45,0.30) & (0.45,0.24) \\ (0.54,0.33) & (0.50,0.34) & (0.50,0.27) \\ (0.49,0.37) & (0.45,0.38) & (0.50,0.34) \\ (0.49,0.37) & (0.41,0.38) & (0.46,0.34) \\ (0.49,0.37) & (0.41,0.38) & (0.42,0.34) \\ & (0.45,0.24) & (0.45,0.24) \\ & (0.50,0.24) & (0.50,0.24) \\ & (0.50,0.30) & (0.50,0.27) \\ & (0.50,0.34) & (0.50,0.30) \\ & (0.46,0.34) & (0.50,0.34) \end{bmatrix} \tilde{R}_{C_3} = \begin{bmatrix} (0.50,0.33) & (0.46,0.33) & (0.60,0.35) \\ (0.50,0.30) & (0.50,0.33) & (0.63,0.35) \\ (0.60,0.27) & (0.60,0.30) & (0.50,0.33) \\ (0.53,0.27) & (0.56,0.27) & (0.70,0.30) \\ (0.60,0.27) & (0.60,0.27) & (0.56,0.27) \\ & (0.42,0.36) & (0.59,0.5) \\ & (0.42,0.39) & (0.60,0.35) \\ & (0.55,0.37) & (0.42,0.38) \\ & (0.50,0.33) & (0.63,0.35) \\ & (0.56,0.27) & (0.50,0.33) \end{bmatrix}$$

4.4. Evaluation Results

Take the $\tilde{R}_B$ passing the consistency test into formula (7) to get the weight of each primary indicator, and use the same method to calculate the secondary indicators $\tilde{R}_{C_1}, \tilde{R}_{C_2}, \tilde{R}_{C_3}, \tilde{R}_{C_4}, \tilde{R}_{C_5}$ of consistency test to get the final weight information, as shown in Table 4:

Table 4. Final weight information of all levels of indicators

Primary indicators (ω_{B_i})	Secondary indicators(ω_{C_i})
(0.1344, 0.6935)	(0.1770, 0.5260), (0.2524, 0.4644), (0.2289, 0.4907)
(0.1484, 0.6985)	(0.2599, 0.5216), (0.2605, 0.5822),(0.2445, 0.5888)
(0.1426, 0.7186)	(0.1610, 0.7396), (0.1603, 0.7443), (0.1761, 0.7514) (0.1471, 0.7619), (0.1622, 0.7635)
(0.1377, 0.7246)	(0.2905, 0.5809), (0.2731, 0.5923), (0.2369, 0.5776)
(0.1328, 0.7277)	(0.4222, 0.3143), (0.3556, 0.4000)

Finally, weight aggregation is carried out by formula (9)~(10), the total weight $W=(0.4174, 0.1299)$ can be obtained, and the final risk assessment score $h(W)=1-0.5(1-0.4174)(1+0.1299)=0.5989$ can be obtained by formula (11). According to the information security maturity rating table, this questionnaire shows that company a is at Level 3 (process definition level).

The average of 11 results was taken, and the final total score was 0.5867, which was at the level of process definition. Last year, the company obtained 0.54 points through other risk assessment schemes, indicating that the company is at the third level of maturity. The scheme proposed in this paper shows that the company's score is higher, because the company has made supplementary improvements in safety planning and other aspects after last year's assessment. Although it has been supported by standardized and documented systems, it is difficult to find problems in the implementation process due to the lack of monitoring and quantitative management, so it is still at the third level. This scheme is more efficient and less time-consuming, and because the index system is designed according to the five aspects of strategy, organization, operation, technology and evaluation, the evaluation results can clearly reflect the gap between the company and the target level. In addition, compared with the scheme of [25], the scheme proposed in this paper is better in dealing with the limit case (the questionnaire scores are all ' Yes ' or ' No ').

5. Conclusion

In order to solve the problems in traditional information security risk assessment, this paper proposes an information security risk assessment scheme based on improved FAHP, and establishes a five-dimensional detailed index system. Taking an e-commerce company as an example, this scheme is used to evaluate the information security risk of it. The results show that the evaluation results of the scheme are consistent with the actual situation, and the evaluation process is efficient.

6. Acknowledgement

This research was funded by the Science and Technology Project Funding of State Grid Corporation of China (Research and Application of Network Security Situation Awareness Technology in Power Monitoring System in 2018-2019, Contract no.: 521104180028).

7. References

[1] *Forecast: Information Security*, Worldwide, 2015-2021, 3Q17 Update
[2] Li Z, Jianfen P, Yuge D U, et al. Information security risk assessment survey[J]. *Journal of Tsinghua University(Science and Technology)*, 2012, 25(1): 1578-1584.
[3] Laarhoven P J M V, Pedrycz W. A fuzzy extension of Saaty's priority theory[J]. *Fuzzy Sets & Systems*, 1983, 11(1): 199-227.
[4] Bian N, Wang X, Li M. Network security situational assessment model based on improved

AHP_FCE[C]//*International Conference on Advanced Computational Intelligence*. 2013.

[5] Zhao-Jun G U, Rui-Li W. A security situation assessment model of information system based on improved fuzzy analytical hierarchy process[J]. *Computer Engineering & Science*, 2016.

[6] Zhao D M, Wang J H, Ma J F. Fuzzy Risk Assessment of the Network Security[C]// *International Conference on Machine Learning & Cybernetics*. 2009.

[7] Yu Fu, Xiaoping Wu, Qing Ye, et al. Study on security risk assessment of information system based on Fuzzy Set and Entropy Weight Theory [J]. Journal of Electronics, 2010, 38(7): 1489-1494.

[8] GB/T 20984-2007, Code for risk assessment of information security [S]. Beijing: China Standards Press.

[9] Jijun Zhang. Fuzzy Analytic Hierarchy Process (FAHP)[J]. Fuzzy system and Mathematics, 2000, 14(2): 80-88.

[10] Atanassov K, Pasi G, Yager R. Intuitionistic fuzzy interpretations of multi-person multi-criteria decision making[C]// *Intelligent Systems, First International IEEE Symposium*. 2002.

[11] Atanassov K T. *On Intuitionistic Fuzzy Sets Theory*[M]. 2012.

[12] Xu Z, Liao H. Intuitionistic Fuzzy Analytic Hierarchy Process[J]. *IEEE Transactions on Fuzzy Systems*, 2014, 22(4): 749-761.

[13] Fahmi A, Derakhshan A, Kahraman C . Human resources management using interval valued intuitionistic fuzzy analytic hierarchy process[C]// *IEEE International Conference on Fuzzy Systems. IEEE*, 2015.

[14] Szmidt E, Kacprzyk J. Amount of Information and Its Reliability in the Ranking of Atanassov's Intuitionistic Fuzzy Alternatives[M]// Recent Advances in Decision Making. *Springer Berlin Heidelberg*, 2009.

[15] Xia M, Xu Z, Zhu B. Some issues on intuitionistic fuzzy aggregation operators based on Archimedean t-conorm and t-norm[J]. *Knowledge-Based Systems*, 2012, 31(none): 78-88.

[16] Chrissis M B, Konrad M, Shrum S. CMMI Guidlines for Process Integration and Product Improvement[M]. 2003.