Ingénierie des Systèmes d'Information
Vol. 25, No. 4, August, 2020, pp. 475-480
Journal homepage: http://iieta.org/journals/isi

# Reliability Analysis of Risk Model Metrics Based on Business Approach in Information Security

Prajna Deshanta Ibnugraha[1*], Lukito Edi Nugroho[2], Paulus Insap Santosa[2]

[1] School of Applied Science, Telkom University, Bandung 40257, Indonesia
[2] Department of Electrical Engineering and Information Technology, Universitas Gadjah Mada, Yogyakarta 55281, Indonesia

Corresponding Author Email: prajna@telkomuniversity.ac.id

https://doi.org/10.18280/isi.250410

**Received:** 20 April 2020
**Accepted:** 16 July 2020

***Keywords:***
*reliability analysis, Cronbach's alpha, risk model, information security, business approach*

**ABSTRACT**

Threat of information security has impact to business of organization. Therefore, the development of information security risk model should consider business perspective. In order to develop new risk model, defining metrics is important process. It can be conducted by theoretical analysis, validity analysis and reliability analysis. Theoretical analysis and validity analysis had been performed in previous work. Furthermore, reliability analysis is performed in this paper. Cronbach's Alpha is required as method to measure reliability coefficient from five proposed metrics namely reputation, financial impact, critical level, business type of organization, and size of organization. Reliability analysis from proposed metrics results coefficient between 0.70-0.91. Based on previous researches, metric is reliable if it has coefficient greater than 0.65. Therefore, proposed metrics have adequate reliability to be used as metrics of risk model.

## 1. INTRODUCTION

Nowadays, information technology is main part from business of organization [1]. It is proven by implementation of information technology in all of business process from organization like human resource management, marketing, production, etc. Digital information becomes main component where it is processed by information technology. Digital information in organization can be employee information, transaction records, production asset, etc. It can be formed as confidential information or public information. Confidential information only can be accessed by authenticated users whereas public information can be accessed by general people. Incident of leakage data often happens in confidential information. In report from Security Industry Association (SIA), Equifax as large enterprise in credit agency ever experienced data leakage related personal information. 143 million confidential information from Americans had been exposed by hackers in 2017. Exposed information consists of Social Security Number (SSN), credit card number and other confidential information [2].

Based of Verizon's investigation, incidents of data leakage almost 75% were caused by outsiders that made impact for business organization [3]. Therefore, audit of information security becomes mandatory implementation to prevent incident and minimize risk. In implementation, audit of information security needs risk model. It gives reference related risk measurement and risk profiling [4]. Business aspects are perspective that must be considered as metrics of risk model because incidents of information security have business impact for organization [5-7]. However, existing risk model has limitation related business perspective. Mostly of risk model focus in technical aspects [8]. Therefore, development is needed to obtain risk model with business approach.

The development of risk model has to pass through several procedures i.e. identification of metrics, development of risk model and evaluation of risk model. Identification of metrics is performed by selecting business aspects. It was ever conducted by several studies where they identified metrics for new risk model. Early study related identifying metrics in risk model was shown by Ghani et al. where they conducted study related economic metrics to measure risk. Ghani et al. resulted potential damage and ex-post response costs as metrics of risk model [9]. Tamjidyamcholo et al. also built a risk model for information systems with the Fuzzy Set Theory method. Differences of characteristic and asset from organization became reason of risk model development. Metrics consisted of people, procedure, data, software, hardware and networking [10]. Furthermore, business unit and people were also developed by Alpcan et al. as metrics of risk model. It used Risk-Rank algorithm to determine risk [11]. Identification metrics of three models above is conducted by theoretical analysis. However, reliability analysis of metrics had not been performed by them. It leads problems such as inconsistent interpretation regarding to result of assessment [12]. Therefore, we involve reliability analysis as part of metrics development from our risk model.

In our previous work, metrics development had passed through theoretical analysis and validity analysis [13]. Theoretical analysis aims to select metrics from business aspects based on theory literature. Furthermore, output of theoretical analysis is processed in validity analysis. It consists of two steps, i.e. correlation analysis and significance analysis. Correlation analysis aims to assess direction and strength of relationship between metrics and risk profile while significance analysis aims to measure significance impact of metrics in building risk profile. In our previous work, we resulted five metrics namely reputation, financial impact, critical level, size of organization and type of business from

organization. However, consistency of metrics needs to be assessed through reliability analysis. Therefore, objective of this study is to perform reliability analysis to five metrics where these metrics is outputs from our previous study. In contribution, we propose new reliable metrics to develop risk model in information security. In order to reach objective, we define two sections in this study. Research method is section that reveals proper method for this study. It consists of two subsections, i.e. data collection and reliability analysis method. Next section is results and discussion. In this section, we elaborate some results from previous study to underlie reliability analysis process. Analysis of results is also carried on this section.

## 2. RESEARCH METHOD

### 2.1 Data collection

Questionnaire is used to obtain data for internal reliability measurement. Respondents involved in data collection have formal education in subject of information communication and technology (ICT). Most of respondents have work experience more than five years. Some of them also have experience in managerial position. Table 1 describes profile of respondents in data collection.

**Table 1.** Profiles of respondents

| Variables | Categories | Number of respondents |
|---|---|---|
| Gender | Male | 83.3% |
| | Female | 15.7% |
| Education | Diploma | 3.3% |
| | Bachelor | 20.0% |
| | Master | 36.7% |
| | Doctoral | 40.0% |
| Job | Lecturer | 46.7% |
| | System Analyst | 16.7% |
| | Programmer | 20.0% |
| | Network and System Administrator | 10.0% |
| | Telecommunication Engineer | 6.7% |
| Working Experience | < 5 years | 23.3% |
| | 5 years and more | 76.7% |
| Managerial Position | None | 20.0% |
| | Managerial | 80.0% |
| Company/ Institution Size of Respondents | Small | 3.4% |
| | Medium | 13.3% |
| | Large | 83.3% |
| Business Types of Company/ Institution from Respondents | Education | 57.7% |
| | ICT company | 20.0% |
| | Government | 6.7% |
| | Health | 6.7% |
| | Financial/Banking | 3.3% |
| | Others | 6.7% |

According to profile of respondents, we can assume that majority of respondents understand content of questionnaire because they have background knowledge and working experience about it. Various perceptions of respondents based on organization background are expected to be accommodated from profile of company/ institution size and company/ institution business type. Meanwhile, development of questionnaire refers to Table 2. Questionnaire is generated in items where each item is classified into suitable metrics.

**Table 2.** Items of metrics

| Metric | Items | References |
|---|---|---|
| Financial Impact (FI) | Cost of mitigation and recovery<br>Loss of revenue<br>Loss of financial | [7, 9, 14, 15] |
| Reputation (RE) | Reputation damage<br>Loss of trust<br>Negative sentiment<br>Loss of customers loyalty | [7] |
| Critical Level (CL) | Loss of safety<br>Fatal injury<br>Economic damage or bankrupt<br>Security damage | [16, 17] |
| Organization Size (OS) | Number of employees<br>Number of assets<br>Number of computers | [5, 6, 18] |
| Type of Business from Organization (TB) | Financial<br>Non-Financial | [19] |

Metrics and items in Table 2 have relationship with risk profile variable where it can be illustrated in Figure 1.

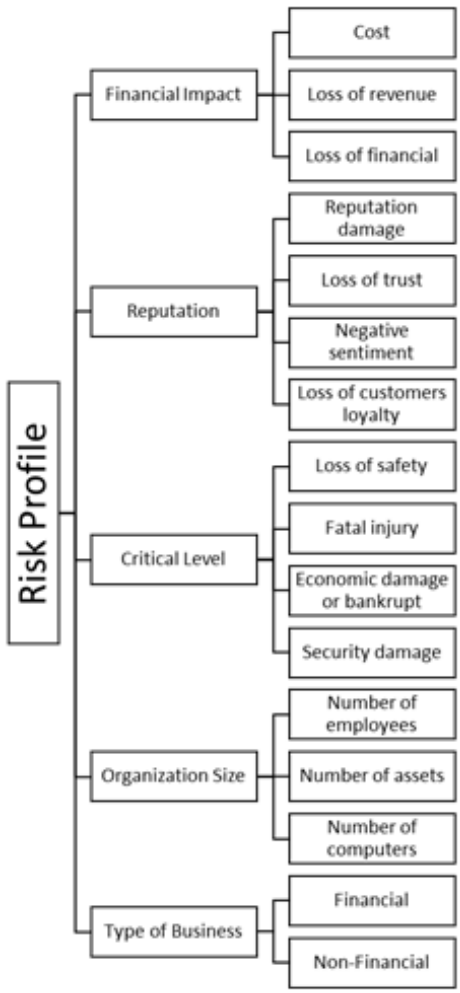


**Figure 1.** Relation between risk profile, metrics and items

In order to obtain data with questionnaire, Likert scale is used to represent response from respondents with gradations:
(1) strongly disagree

(2) disagree,
(3) neither agree nor disagree,
(4) agree,
(5) strongly agree.

All responses from questionnaire is treated as data source to compute internal reliability coefficient. Generally, Likert scale uses 5 or 7 point of ordinal scale [20] and we determine to use 5 scale to simplify the responses. Furthermore, the selected method of reliability analysis must be considered output of ordinal data from questionnaire.

### 2.2 Reliability analysis method

Business aspects can be used as metrics of risk model after it is processed in validity analysis. However, reliability analysis is still needed for defining consistency of business aspects as metrics. Generally, reliability analysis can be performed using two procedures. First procedure is external reliability analysis. It uses repeated testing and makes comparison for output. Data for testing is collected from same individuals in group on different times (Figure 2). In order to determining reliability, these procedure uses coefficients of correlation and variance of error [21].

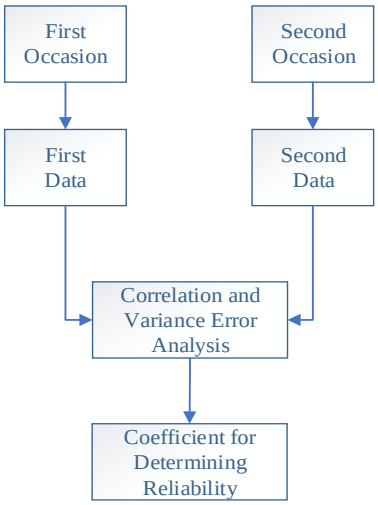


**Figure 2.** Process of repeated testing for reliability analysis

Second procedure is internal reliability analysis. It uses once collecting data for reliability analysis. This procedure involves multiple items in analysis process. Reliability coefficient is measured by testing consistency between items. Generally, internal reliability analysis uses methods such as split-half Spearman-Brown and Cronbach's Alpha.

Even though Split-half Spearman-Brown and Cronbach's Alpha are similar method for internal reliability analysis, Split-half Spearman-Brown and Cronbach's Alpha have different approach. Cronbach's Alpha uses variances of data so it is possible to handle heterogeneous data. Moreover, Split-half Spearman-Brown has different result when it uses different splitting condition. It leads potential for bias [12].

In previous research, Cronbach's Alpha was also able to be applied for measuring internal reliability of factors in several subjects. In education, Cronbach's Alpha was ever used to measure reliability and stability of factors that represent capability of students in facing job challenge after their graduation [22]. Identified factors was used as evaluation parameter that accommodated differences of characteristic and capability from students. Identified factors become reliable as measurement parameter if factors have Cronbach's Alpha coefficient more than 0.80. Moreover, reliability analysis using Cronbach's Alpha was ever conducted in Objective Structural Clinical Examination (OSCE) environment. OSCE is a multisystem course in medical area and it needs Cronbach's Alpha to ensure reliability of exam and fairness among all participants [23]. Cronbach's Alpha in OSCE study is based on data of 80 multiple-choice questions from medical students. Meanwhile, in subject of information security, Cronbach' Alpha was used to determine reliability of factors for reducing insider threats [24].

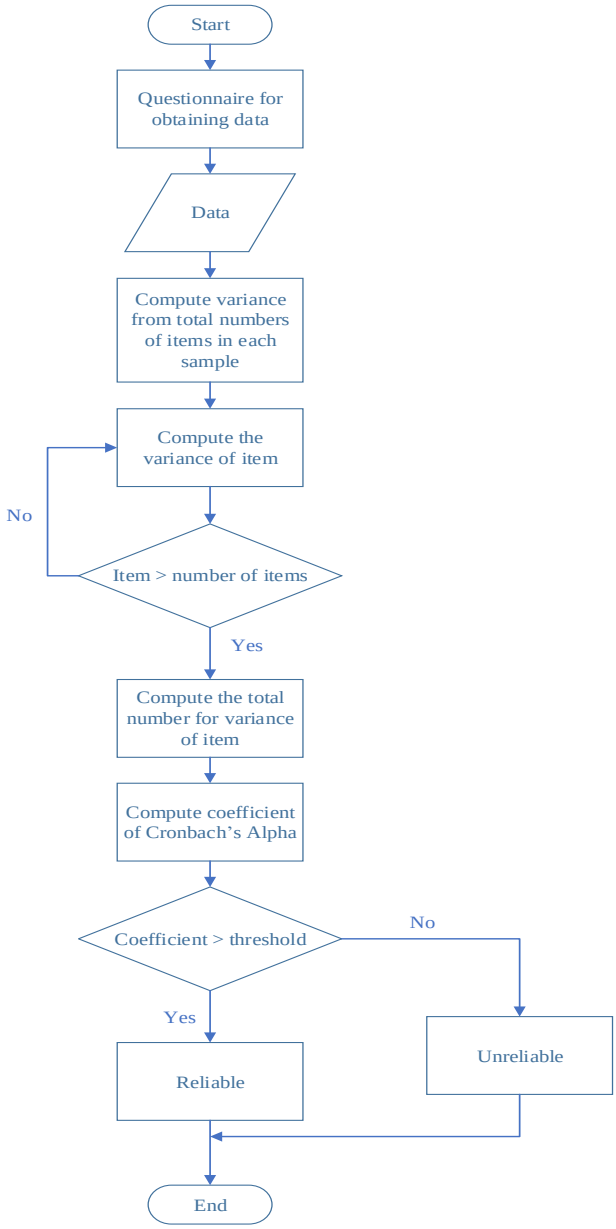


**Figure 3.** Flowchart for reliability analysis

If we conclude from illustration above, Cronbach's Alpha has characteristics such as able to handle heterogenous data, able to reduce bias and able to be implemented in measuring factors reliability. Therefore, this study uses Cronbach's Alpha as method for internal reliability analysis. This method generally has formula that shown in Eq. (1) [25]. Result of calculation in Eq. (1) is reliability coefficient that has value from zero up to one.

$$\alpha = \frac{n}{n-1}\left[1 - \frac{\sum_{i=1}^{n} var_i}{var_t}\right] \quad (1)$$

$n$ is number of items. $var_i$ is total numbers of variance in each item while $var_t$ is the variance from total number of items in each sample. In order to compute variance, we use formula in Eq. (2).

$$var = \frac{\sum_{k=1}^{N}(x_k)^2 - \frac{(\sum_{k=1}^{N} x_k)^2}{N}}{N-1} \quad (2)$$

$x_k$ is data of item $k$, whereas $N$ is number of samples in internal reliability analysis. Meanwhile, the process of reliability analysis in this study can be described in flowchart Figure 3.

## 3. RESULTS AND DISCUSSION

In our previous study, validity analysis had been conducted using correlation and significance analysis process [13]. Correlation between metrics and risk profile had been computed using Spearman-Rank method and produced coefficients in Table 3.

**Table 3.** Coefficient of correlation

| Relation | Coefficient |
|---|---|
| FI-RP | 0.692 |
| RE-RP | 0.460 |
| CL-RP | 0.259 |
| OS-RP | 0.341 |
| TB-RP | 0.425 |

According to Table 3, financial impact (FI) has strong correlation with risk profile (RP). Reputation (RE), organization size (OS) and type of business from organization (TB) have moderate correlation with risk profile. Weak correlation is only resulted by relation between critical level (CL) and risk profile. Significance analysis is performed by involving correlation coefficient and t-test method. Financial impact, reputation and business type have significance effect in generating risk profiles, while critical level and organization size have less effect.

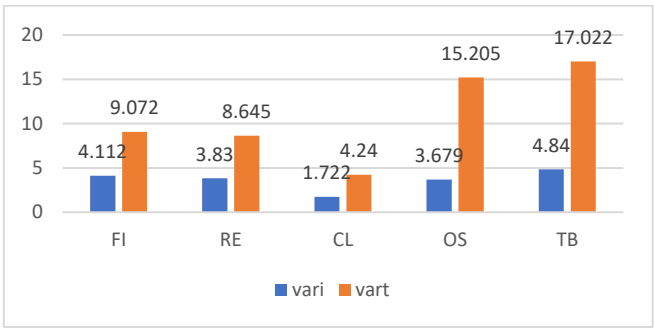


**Figure 4.** Values of variances

Furthermore, reliability analysis is performed in this study to determine consistency of metrics. It is conducted using equal data from validity analysis. Cronbach's Alpha formula is used to compute reliability coefficient. It needs two main variables, i.e. variance from total numbers of each items ($var_i$) and variance from total numbers of items in each sample ($var_t$). As illustrated in Figure 4, variance in each metrics have values from 1.722 up to 17.022. Highest value of variance is owned by metric of business type while the lowest value is in critical level metric.

Values of variances is and number of items are considered to generate reliability coefficients for each metrics. It can be computed using Eq. (1) and produces outputs like on Table 4.

**Table 4.** Result of reliability coefficient

| Metrics | Reliability Coefficient |
|---|---|
| Financial Impact (FI) | 0.73 |
| Reputation (RE) | 0.70 |
| Critical Level (CL) | 0.79 |
| Organization Size (OS) | 0.91 |
| Type of Business from organization (TB) | 0.82 |

Several studies stated that variable with coefficient reliability greater than 0.65 was able to be accepted as reliable variable. Rosaroso states that Cronbach's alpha with values greater than 0.80 has high reliability [26]. However, Cronbach's alpha with value greater than 0.60 is accepted as reliable coefficient. Ary also uses value greater than 0.60 as threshold for reliable coefficient [27]. Cortina, DeVellis, Nunnally, Bernstein and Vaske state in different papers that Cronbach's alpha with value 0.65 is lower limit of reliable coefficient [25].

Table 4 shows that reliability coefficients of metrics are from 0.70 up to 0.91. These results fill requirement for minimum value of reliability. It indicates that proposed metrics are adequate to be used as measurement variables. According to result of our previous and current study, proposed metrics have passed from validity testing and reliability testing. It shows that proposed metrics have relationship in generating risk profiles and have stability as measurement variables. It concludes that proposed metrics are ready to be used in risk model development. Therefore, our future work is to develop risk model in information security based on resulted metrics in this study.

## 4. CONCLUSION

The identification business aspects as metrics of information security risk model must be performed for accommodating business impact. These identification process involves validity analysis and reliability analysis. In previous result, validity analysis has produced five proposed metrics, namely financial impact, reputation, critical level, size of organization, and type of business. Further, the output of validity analysis must be through reliability analysis to produce consistent metrics. This study uses Cronbach's Alpha as reliability analysis method because it has advantages such as able to handle heterogenous data, able to reduce bias and able to compute factors reliability. Based on reliability measurement, proposed metrics have coefficients of Cronbach's Alpha between 0.70-0.91. These coefficients have value greater than 0.65 where it means that the proposed metrics have acceptable reliability. Hence, the proposed metrics are feasible to be risk model metrics. However, the threshold of acceptable reliability has different perspective for researchers where it is the limitation of these method in determining feasibility of variables. In future, the metrics will be a part in information security risk model development.

## REFERENCES


[1] Gunawan, T.S., Lim, M.K., Zulkurnain, N.F., Kartiwi, M. (2018). On the review and setup of security audit using Kali Linux. Indonesian Journal of Electrical Engineering and Computer Science, 11(1): 51-59. https://doi.org/10.11591/ijeecs.v11.i1.pp51-59

[2] Security Industry Association. (2018). Data Privacy and Security Trends for 2018. https://www.securityindustry.org/wp-content/uploads/2018/01/SIA_DATA_PRIVACY_WHITEPAPER_WEB.pdf.

[3] The Council of Economic Advisers. (2018). The Cost of Malicious Cyber Activity to the U.S. Economy. https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

[4] He, M., An, X. (2016). Information security risk assessment based on analytic hierarchy process. Indonesian Journal of Electrical Engineering and Computer Science, 1(3): 656-664. https://doi.org/10.11591/ijeecs.v1.i3.pp656-664

[5] Kaspersky Lab ZAO. (2013). Global Corporate IT Security Risks: 2013. Kaspersky. https://media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf.

[6] PWC. (2014). US Cybercrime: Rising Key Findings from the 2014 US State of Cybercrime Survey. PWC, (July), 21. https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=269621.

[7] Jekot, M., Niemiec, M. (2016). IT risk assessment and penetration test: Comparative analysis of IT controls verification techniques. In IDT 2016 - Proceedings of the International Conference on Information and Digital Technologies, Rzeszow, Poland, pp. 118-126. https://doi.org/10.1109/DT.2016.7557160

[8] Suhartana, M., Pardamean, B., Soewito, B. (2014). Modeling of risk factors in determining network security level. International Journal of Security and Its Applications, 8(3): 193-208. https://doi.org/10.14257/ijsia.2014.8.3.21

[9] Ghani, H., Luna, J., Suri, N. (2013). Quantitative assessment of software vulnerabilities based on economic-driven security metrics. In 2013 International Conference on Risks and Security of Internet and Systems (CRiSIS), pp. 1-8. https://doi.org/10.1109/CRiSIS.2013.6766361

[10] Tamjidyamcholo, A., Yamchello, H. T., Bin, M. S., Gholipour, R. (2013). Application of fuzzy set theory to evaluate the rate of aggregative risk in information security. In 2013 International Conference on Research and Innovation in Information Systems (ICRIIS), 2013: 410-415. https://doi.org/10.1109/ICRIIS.2013.6716745

[11] Shameli-Sendi, A., Aghababaei-Barzegar, R., Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). Computers & Security, 57: 14-30. https://doi.org/10.1016/j.cose.2015.11.001

[12] Bardhoshi, G., Erford, B.T. (2017). Processes and procedures for estimating score reliability and precision. Measurement and Evaluation in Counseling and Development, 50(4): 256-263. https://doi.org/10.1080/07481756.2017.1388680

[13] Deshanta Ibnugraha, P., Nugroho, L.E., Santosa, P.I. (2018). Metrics analysis of risk profile: A perspective on business aspects. In 2018 International Conference on Information and Communications Technology (ICOIACT), pp. 275-279. https://doi.org/10.1109/ICOIACT.2018.8350675

[14] Bojanc, R. (2013). Quantitative model for information security risk. Engineering Management Journal, 25(2): 25-37. https://doi.org/http://dx.doi.org/10.1080/10429247.2013.11431972

[15] Aouf, S. El. (2011). Information Security Economics. The Stationery Office (TSO). https://tsoshop.co.uk/bookstore.asp?AF=A10075&Action=Book&ProductID=9780117068728.

[16] ENISA. (2015). Critical Information Infrastructures Protection Approaches in EU. ENISA. https://resilience.enisa.europa.eu/enisas-ncss-project/CIIPApproachesNCSS.pdf.

[17] El-attar, N.E., Awad, W.A., Omara, F.A. (2016). Empirical assessment for security risk and availability in public cloud frameworks. In 11th International Conference on Computer Engineering & Systems (ICCES), pp. 17-25. https://doi.org/10.1109/ICCES.2016.7821969

[18] Abdulsaleh, A.M., Worthington, A.C. (2013). Small and medium-sized enterprises financing: A review of literature. International Journal of Business and Management, 8(14): 36-54. https://doi.org/10.5539/ijbm.v8n14p36

[19] Clark, A., Tan, T.T., Barbee, C., Donker, J., Palmer, A., Skramstad, E. (2014). Threats to the financial services sector: Financial services sector analysis of PwC's 2014 global economic crime survey. Pwc. Retrieved from https://www.pwc.com/en_GX/gx/financial-services/publications/assets/pwc-gecs-2014-threats-to-the-financial-services-sector.pdf.

[20] Sullivan, G.M., Artino, A.R. (2013). Analyzing and interpreting data from likert-type scales. Journal of Graduate Medical Education, 5(4): 541-542. https://doi.org/10.4300/JGME-5-4-18

[21] Shirali, G., Shekari, M., Angali, K.A. (2017). Assessing reliability and validity of an instrument for measuring resilience safety culture in sociotechnical systems. Safety and Health at Work. https://doi.org/10.1016/j.shaw.2017.07.010

[22] Yan, H., Yibing, L. (2010). The research on index system optimization of graduation design based on Cronbach coefficient. In 2010 5th International Conference on Computer Science & Education, Hefei, China, pp. 1843-1845. https://doi.org/10.1109/ICCSE.2010.5593808

[23] Al-Osail, A.M., Al-Sheikh, M.H., Al-Osail, E.M., Al-Ghamdi, M.A., Al-Hawas, A.M., Al-Bahussain, A.S., Al-Dajani, A.A. (2015). Is Cronbach's alpha sufficient for assessing the reliability of the OSCE for an internal medicine course? BMC Research Notes, 8(1): 4-9. https://doi.org/10.1186/s13104-015-1533-x

[24] Safa, N.S., Maple, C., Watson, T., Von Solms, R. (2018). Motivation and opportunity based model to reduce information security insider threats in organisations. Journal of Information Security and Applications, 40: 1-11. https://doi.org/10.1016/j.jisa.2017.11.001

[25] Vaske, J.J., Beaman, J., Sponarski, C.C. (2017). Rethinking internal consistency in Cronbach's Alpha.

Leisure Sciences, 39(2): 163-173. https://doi.org/10.1080/01490400.2015.1127189
[26] Rosaroso, R.C. (2015). Using reliability measures in test validation. European Scientific Journal, 11(18): 1857-7881. https://eujournal.org/index.php/esj/article/viewFile/5847/5662
[27] Ary, D., Jacobs, L.C., Sorensen, C.K., Walker, D.A. (2010). Introduction to Research in Education (8th ed.). Belmont, USA: Wadsworth Cengage Learning.