New Risk Analysis Method for Information System Security

Easter C. K. Huang
Ph.D. program in Taiwan Industrial Strategy and Development, in College of Management
Chaoyang University of Technology, Taichung, Taiwan
bestiso2000@yahoo.com

Chin Chung-Jen, Ed.D.
President of Chaoyang University of Technology, Taichung, Taiwan
pres@cyut.edu.tw

Abstract

This study used the Failure Mode Effect Analysis (FMEA) that is one of the most popular methods for risk analysis to explain the regulatory compliance rate with the information security risk analysis of the Taiwan universities. Using the regression analysis, the independent variables including violating times to Taiwanese laws, the self-detecting violating times to Taiwanese laws, the attacked times that detected by government and the non-conformities issued by third-party to the dependent variables that the risk priority number (RPN) that the multiplication of occurrence of violation (O), the Severity (S) and detecting ability (D). The multicollinearity is not obvious, and the result is significant correlation of the variables that independent variables could explain 68% to the dependent variable. In this study, the FMEA could explain the regulatory compliance that means the risk analysis could improve information security detective methods for the preventive purposes.

Index Terms: Personal Information Protection, information security, risk analysis, FMEA, ISO27001, certification.

I、INTRODUCTION

A. Background

The "Personal Information Protection Act" in Taiwan (hereinafter referred to as "TPIPA") was formally implemented on October 1, 2012. The previous name of this Act as "Computer Processing of Personal Data Protection Act" has been implemented from 1995; the main objective was to protect personal information. This modified act is a public prosecution criminal law that requests the enterprises shall take more responsibility to protect the information security and personal information. However, most organizations, including the universities did not well prepare to protect the personal information and information security. The purpose of this study is trying to find a risk analysis method for not only the Personal Information Protection Act but also the information security management systems (ISMS).

The universities and enterprises could use the prevent risk mode-FMEA from the mandatory certification standards- TS16949:2009 of the automotive industry to analyze the risk of the information security system.

B. ISO and system certification

International organization of Standardization (ISO) created the first certification standard ISO9000:1987--the "quality management system" from 1987, has been developed thousands different standards now [1]. In 2009, Mintzberg pointed out there are four kinds of business organizations; the first is manufacture, the second is the trade company also includes networks and banking, the third is non-profit organizations and the fourth is government. Different organizations have different targets and goals, the above first two are looking for the best benefits for the shareholders, the other two are increasing the welfare and reducing the Risk of the organizations [2].

As my paper in 2013 found that the enterprises get the different ISO certifications cannot achieve their business goals. Profit is not just simply equal to the revenue minus the costs [3]. In addition to the profit, there are several important factors including the leader's style, marketing share, life cycle, new products development ability, human resource and facility ability[3]. There are many business models and strategies to analyze the achieving goals for enterprises. As the ISO certifications do not fully explain the real profits, it successfully explains the cost of quality and the risk reducing [3]. This is the reason to use the system certification standard ISO27000 and FMEA to analyze the information system risk.

C. Taiwan TPIPA

The TPIPA extends its range to all organization that collected, processed and used personal information that including the computer processing people, the officers, natural persons, the non-government agencies and the organizations.

Lu pointed the following basic steps to protect the personal data in 2009 [7]:

(1) Risk analysis
(2) Set the personal data process;
(3) collection and processing the personal data
(4) set the protection and detection equipments and methods;
(5) audit the previous process
(6) review and modify the process

D. ISMS

The Taiwan government encourages all organizations that shall protect their information system security and must follow the TPIPA [4]. Conformity with ISO27001 is the first step in achieving this goal [3].

In 2013, Executive Yuan found that there are 460 organizations including some of the Universities got the ISMS certifications. There are four levels of government that separate based on the important and the employee's number. The grade A and B organizations are 90% getting the ISMS certifications and the grade C and D are only 10% getting the ISMS that due to lack of funds and personnel, which results in a serious problem for the ISMS [5].

There are around 30 certification bodies could issue the ISMS and personal information protecting certifications in Taiwan, including third parties such as: SGS, TUV, NQA and the government authorized organization such as the Tsinghai University.

Information security and personal information protecting certification standard include, ISO20000, ISO 27001, ISO29100, NIST SP800-122/53., and BS10012. However, the organization getting these voluntary certifications cannot reduce their legal responsibility [4].

The organization could develop their own information security control process according to their information security and the impact of the risk [3].

Huang suggested the following process to set the ISMS; provide ISMS commitments, risk assessment methodology policy, supply the resource, Internal Audit and the corrective and preventive actions, and achieve continuous improvement. The above is the basic mode of ISO27001. Another set of this standard are the mandatory control objectives and control measures including the following 137 items in the 11 areas : A.5 Information Security Policy, A.6 information security organization , A.7 Asset Management, A.8 Human resources security , A.9 Physical and Environmental security A.10 Communications and operations management, A.11 Access control , A.12 Information system acquisition, development and maintenance, A.13 Information security incident management, A.14 Business Continuity Management, A. 15 Compliance [3].

E. Risk analysis for information security

There are several risk analysis methods for the ISMS, usually separated for the product analysis and system analysis [3]. The most popular methods for products analysis are generalized fuzzy number [6] and proposed similarity measure for the software or the website [7]. These technology issues are excluded in this study.

Huang pointed that asset method is one of the most popular system risk analysis method for ISMS. However, the organizations need to check all assets include the software, AP, hardware, human resource, and the facility [3]. Due to the asset methods required a lot of resource and time, this study used the FMEA as the other new and useful risk analysis method to analyze the risk of the information security.

F. FMEA

Failure Mode Effect Analysis is a risk assessment model to prevent failure [8]. FMEA is created by NASA in 1950 to prevent the accident in the aerospace industry. The World Auto Union -IATF used the FMEA as the mandatory risk method for the global automotive industry from 1998. IATF pointed that the FMEA consists of the following eight steps: 1. Modify the production or service processes, 2 Verify the sub-processes, 3. Confirm each processes, 4. Organize the process map, 5. Develop FMEA processes list, 6. Analysis the FMEA risk, 7. Decide the accept RPN and identify the corrective action 8.Track results and continuously update the FMEA [8]. If the RPN had more than the acceptable risk value, it is necessary to improve. All variables are strictly defined; such as only changing the design processes can decrease the severity rating [9].

G. Using FMEA in ISMS

FMEA is one of the most comprehensive and professional guides for risk analysis. There are many papers research how the FMEA using in different industries and management systems. However, There are only few study such as Živković intended to demonstrate how the FMEA method can be used to analyze information security risks and design the ISMS [10]. However, his study is only address and introduces the FMEA that no any evidences to support the finding and result. Huang did three studies about the FMEA using in the ISMS that exactly provided the evidences that the FMEA could successful used in the ISMS to prevent the risk [1] [3] [13]. However, Huang found in 2014 that the organization getting the ISMS certifications cannot reduce or control the risk of the ISMS if the organization did not achieve their key performance index of the ISMS [13].

II、 Methodology

A. Hypotheses

ISMS risk analysis: Huang pointed that the risk of ISMS is often used the following categories based on the consequence and probability as the “transfer, avoid, reduce and accept” [1]. The processes of risk analysis in ISO/IEC TR13335-3:1998 as following Figure 1: 1.Set the scope, identify the assets value (A) include the HR, software, hardware, and facilities. 2. Identify the threats (T) and vulnerabilities (V). 3. Compare the risk value with the risk control methods and equipments. 4. Separate the level of the risk: high, middle and low. 5. Choice the acceptable risk level and do the corrective plan to reduce the risk until accept, transfer or avoid using these high risk assets. Figure 1 shows the processing flow of the ISMS risk analysis, which involves too much work and uncertain factors, such as different level Earthquake will affect the same assets with different threats and vulnerability. According to this model that human factor which maybe threats by lack of training, or missing attention in

the same time which will very difficultly to give a quantity number. So we need to find an easy and popular method for risk analysis.

Figure 2 shows the FMEA detection model This FEMA compares with the ISMS assets method (Figure 1) that is easier to understand and use. However, because the multicollinearity, both models cannot use the regression analysis [10].

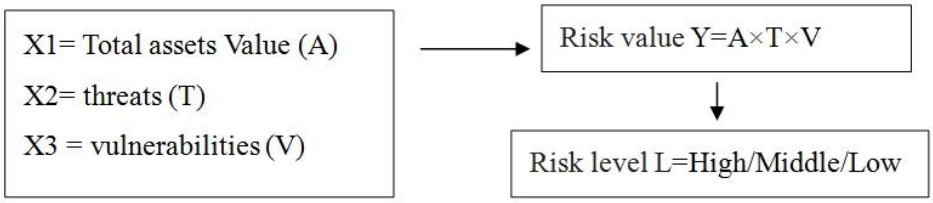

Figure 1: The ISMS risk analysis model.

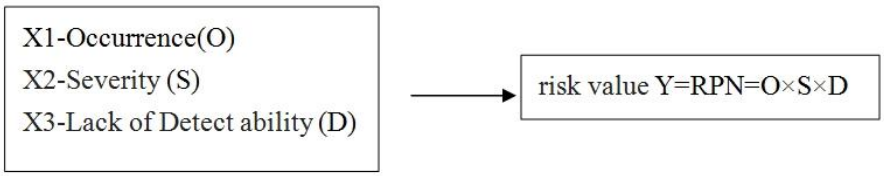

Figure 2: FMEA risk analysis model

B. Research organization chart

To avoid the weakness for the above two models, this study designs a new method as the Figure 3 for risk analysis of the information security.

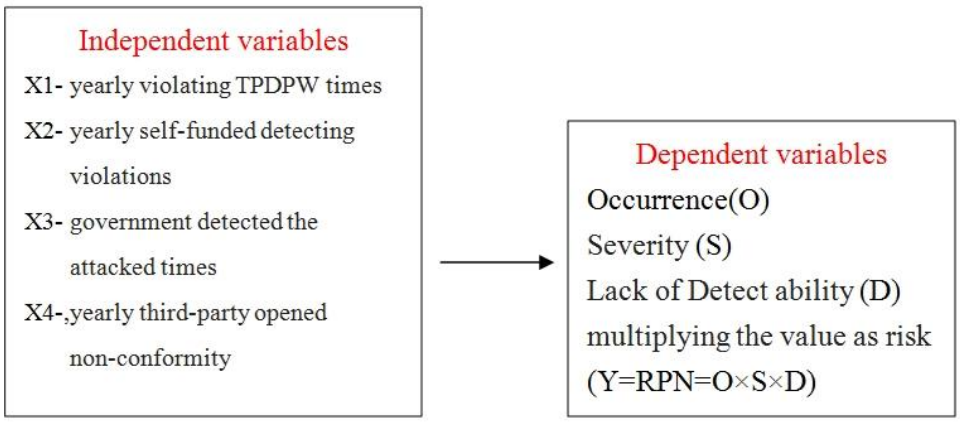

Figure 3: Risk analysis model

Figure 3 shows the detection model to analyze the information security risk for this study. The regression is a useful method of data analysis whenever quantitative variables (the

dependent or criterion variables) are to be examined in relationship to any other factors (expressed as independent or predictor variables) [11].

There are four independent variables in this study. X1: the yearly violating TPIPA times, X2: the yearly self-detecting violations times, X3: the government detected number of attacked and X4: the yearly third-party issued non-conformity. All above data could get from the organization. However, the only way to get the X is after the events happened that cannot avoid the risk. The study tries to find a useful way to avoid the risk not only for the Personal Information Protection Act but also for the Information security management systems. We use the FMEA to design a model as following Figure 4. According to the dependence variable RNP of the University and the independent variables are quantity and could use the regression analysis.

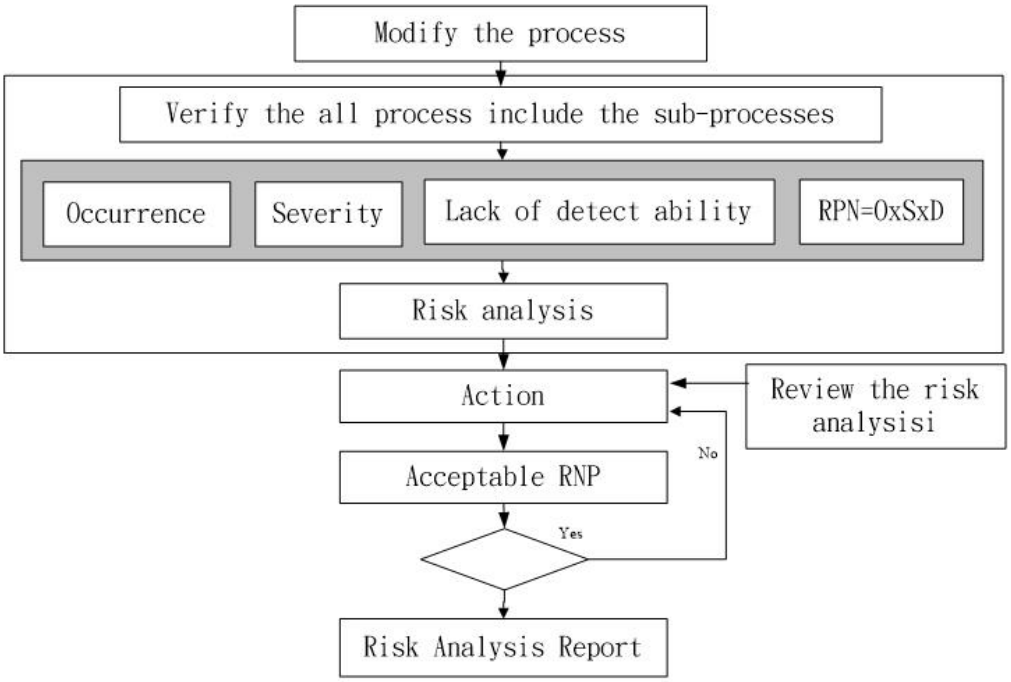

Figure 4: FMEA-ISMS risk analysis process

C. Sample selection

There are more than hundred industries and million organizations in Taiwan; however there are only 460 organizations which is 0.5% get the ISO27001 certificates. We choice the Universities as the sample because that there is more that 36% (61 of 167) Universities in Taiwan that got the ISO27001 certifications. We sent the questionnaires to get the dependent variable and the independent variables. The sampling list and data is based on the international Certification Bodies such as the NQA, the TUV-NORD, SGS, and BSI.

D. Research design

The risk analysis method is the value multiplying as the risk (Y = RPN = O × S × D). For the university, modify the FMEA method O, S, D to be set as the following quantitative criteria from 1-5.

(1) Occurrence (O):

We calculated the probability for the particular cause in the previous year as the occurrence. Please see the following Table 1.

Table 1: Occurrence Quantitative

Quantitative	Occurrence
5	More than 365 per year
4	55 to 365 per year
3	13 to 54 per year
2	1 to 12 times per year
1	Zero

(2) Severity(S):

According to National Information and Communication Security, the severity is the biggest resulting from the following five different failure modes as shown in Table 2.

Table 2: Severity Quantitative

	Organizational reputation	Operation	Casualties	Privacy loss	Property damage
5	Top news	Full stop	People died	1001-	1million
4	News	one major	serious disability	501-1000	500K-1million
3	Local news	Some minor	serious Injuries	101-500	100k-500K
2	Inside news	Few	Injuries	1-100	10K-100K
1	Rumor	False alarm	False alarm	0	Under 10kNT

(3) Lack of Detectability (D):

The methods of the failure probability will not be detected.

Table 3: Lack of Detectability Quantitative

Quantitative	Standard
5	No any detective control methods
4	No fixed plan, random by human detective
3	Using the human or machine auto detective at least monthly
2	Using the human and machine auto detective at least weekly
1	Using the human and machine auto detective at least daily

(4) Risk Priority Number (RPN) = O × S × D that means the Frequency× Severity ×Probability. The RNP value is from one to 125. The university should decide the acceptable risk value, and improve all the unacceptable process until it's could be accepted.

III、 Result

A. Sampling information

There are total 167 Universities and we chose 61 that got the ISO27001 certifications to send the questionnaires. We recovered 52 copies (recovery rate 85.24%) that is 31.14% of total 167. We excluded uncompleted two questionnaires and the effective recovery of the samples is 50 copies. There are 22 National (Public) University (44%) and 28 private schools (56%); 23 University (46%), and 27 University of Technology (54%); the average year was established 17.8 years; the average student number is 8672.The above information showed that the samples were reasonable and acceptable.

(1) the different between public and private University:

Table 4: The Differences between Public and Private University

	Average	National	Private
X1, the yearly violating TPIPA times	0.14	0.136	0.142
X2,the yearly self-detecting violations time	12.86	15.6	10.65
X3,the government detected number of attacked	9.26	10.56	8.29
X4,the yearly non-conformities issued by third-party	1.34	1.13	1.49
Risk Priority Number (RPN)	15	20.7	10.1

Table 4 showed the X1 the yearly violating TPIPA times is not a significant different, the X2 internal inspection number of public school is 46.48% more than the private school that may be the public schools have more man power and the equipments to detect the violation the security events. X3, the attacked times by government detected showed that the public school is more easy attracted that maybe the public school open their web 24 hours for free using. The X4, non-conformity issued by third-party showed the private school is 32% more than public school that maybe the public school is more care for their reputation and try to request the auditor do not opened the finding or downgraded the minor non-conformity to the observation. The interesting result is the RPN showed the public school is actually higher risk than the private school that maybe the media is more interesting for the public school and the private school had more good relation with the media.

(2) The different between University and University of Technology:

Table 5: The Differences between University and Technology

	Average	University	University of Technology
X1, the yearly violating TPIPA times	0.14	0.22	0.07
X2,the yearly self-detecting violations time	12.86	15.40	10.70
X3,the government detected number of attacked	9.26	10.34	8.34
X4,the yearly non-conformities issued by third-party	1.34	1.51	1.20
Risk Priority Number (RPN)	15	21.2	9.72

Table 5 showed the university had more serious ISMS problems then university of technology in the legal issue, internal detective result, attracted number and Non-conformity that maybe the university had more detected equipments then the University of Technology and could find the ISMS problem. X2 internal inspection number, X3 the attacked times by government detected, and X4 third-party issued non-conformity yearly showed that the University has more risk than University of Technology. Especially the legal issue and RPN are that means that the university has 200% more risk than the University of Technology. This finding could do more research in the future to know that really risk or only the detected equipments reason.

(3) Established Years

Table 6: The Analysis for the Establish Years

	Average	Under18	More than 18
Average Year	17.8	20	30
X1, the yearly violating TPIPA times	0.14	0.11	0.16
X2,the yearly self-detecting violations time	12.86	13.46	12.46
X3,the government detected number of attacked	9.26	3.17	13.32
X4,the yearly non-conformities issued by third-party	1.34	1.22	1.42
Risk Priority Number (RPN)	15	10.5	18

Table 4 showed X1, X2 and X4 are no obvious different. X3 showed that senior schools were 420% more attracted than the younger schools that maybe too many new Universities and change their names very often that reduce the possibility to be attached. Furthermore, the reason maybe those younger schools have more equipments and human resource to protect their information security that need to do more research. The result of RPN showed that the older schools have higher risk than the younger school.

(4) Students' number

Table 7: Students Number Analysis

	Average	Under8672	More than8672
Average	8672	16	34
X1, the yearly violating TPIPA times	0.14	0.15	0.14
X2,the yearly self-detecting violations time	12.86	18.79	10.06
X3,the government detected number of attacked	9.26	16.11	6.07
X4,the yearly non-conformities issued by third-party	1.34	1.42	1.30
Risk Priority Number (RPN)	15	25	10.29

Table 4 showed the X1 and X4 has no obvious different. X2 internal inspection numbers of less-students school is more 86.748% risk than the more-students school that maybe the less-students schools had fewer man power and the equipments to detect the violation of the security events. X3, the attacked times by government detected showed that the less-students school is 265% easier attracted which is the same result from the less money or resource in man power and equipments. The RPN result showed the less-students numbers University had more 243% risk than the more-students schools. The student's number is one of the important factories for the information risk and the safety.

B. All in methods of regression

Secondly, this study used the all in methods for the all independent variables with the RPN value to do the regression. It can be important to determine whether a multiple regression coefficient is statistically significant. The results show the F =24.97, R^2 =0.68, so our finding is statistically significant that means the four independent variables X1, X2, X3 and X4 at 95% reliability significant relationship can be explained 68.94% of the dependent variable of the variance Y = RPN.

Table 8: The Multiple Regression of RPN of X1, X2, X3 and X4

Multiple coefficient of correlation	0.830305
R^2	0.689407
Adjusted R^2	0.661798
Standard error	8.183562
Number of observations	50

The ANOVA

	DF	SS	MS	F	P-value
regression	4	6689.299	1672.325	24.971	6.2E-11
residual	45	3013.681	66.97068		
SUM	49	9702.98			

We obtained the Regression equation:

$Y=-2.50+23.15\ X1+0.45\ X2+1.15\ X3+1.65\ X4$

C. Multicollinearity

We did the following multicollinearity test with all possible regression analysis in order to determine their different combinations of variables.

The multicollinearity test results of the four independent variables of significance matrix are acceptable. The maximum value is 0.4194 that less than 0.8 and the multicollinearity of the independent variables is not obvious. These four independent variables can be used to force in the method. The biggest of Independent variable X and the dependent variable Y is the X1 0.695946, the X2 is 0.47 and the X3 is 0.44 that means the independent variables and the dependent variables are significantly relations.

Table 9: Multicollinearity Test

	X1	X2	X3	X4	Y
X 1	1				
X 2	0.296669	1			
X 3	0.054644	0.419112	1		
X 4	0.262312	0.296797	-0.05926	1	
Y	0.695946	0.474784	0.444337	0.041903	1

D. All possible subsets methods

Even though, these four X could explain dependent variable 68% of the variance. This study was a pilot study that used all possible subsets methods to check the all relation of the X of Y.

(1) Choice of the three independent variables X:

As the Table 10, showed that Y of X1, X2 and X3, F = 30.35, R^2 =0.66, P = 5.63E-11, 66% of the predicted variance in the social sciences can be considered quite high [11].

Table 10: Regression of RPN of X1,X2 and X3

Multiple coefficient of correlation		0.815103			
R^2		0.664393			
Adjusted R^2		0.642505			
Standard error		8.413743			
Number of observations		50			
ANOVA					
	DF	SS	MS	F	P-value
regression	3	6446.591	2148.864	30.35501	5.63E-11
residual	46	3256.389	70.79107		
SUM	49	9702.98			

According to Table11, Choice the X1, X3 and X4, that F value =30.18, R^2 value= 0.64, and P value =6.12E-11 that means it could explain 66% for Y.

Table 11: Regression PRN of X1, X3 and X4

Multiple coefficient of correlation	0.814339
R^2	0.663148
Adjusted R^2	0.641179
Standard error	8.429333
Number of observations	50

ANOVA

	DF	SS	MS	F	P-value
regression	3	6434.512	2144.837	30.18616	6.12E-11
residual	46	3268.468	71.05366		
SUM	49	9702.98			

According to Table 12, selected X1, X2 and X4 regression F value ＝30.18, R^2 value＝0.64, and P value ＝6.12E-11 that means it could explain 61% for Y.

Table 12: Regression X1, X2 and X4 of RPN

Multiple coefficient of correlation	0.781761
R^2	0.61115
Adjusted R^2	0.585791
Standard error	9.056587
Number of observations	50

ANOVA

	DF	SS	MS	F	P-value
regression	3	5929.979	1976.66	24.09921	1.6E-09
residual	46	3773.001	82.02176		
SUM	49	9702.98			

Table 13: Regression X1, X2 and X3 of RPN

Multiple coefficient of correlation		0.548362			
R^2		0.300701			
Adjusted R^2		0.255095			
Standard error		12.14521			
Number of observations		50			
ANOVA					
	DF	SS	MS	F	P-value
regression	3	2917.696	972.5653	6.593387	0.000844
residual	46	6785.284	147.5062		
SUM	49	9702.98			

According to Table 13, selected X2, X3 and X4 regression F value ＝6.59, R^2 value＝ 0.30, and P value ＝0.008 that means it could explain 30% for Y. The above 4 tables showed that the three Xs could explain less than the four Xs. However, the X1, X3 and X4 already could explain the 66.3% to Y.

(2) Choice of the two Xs

There are 6 possible choices for the two independent variables. According to Table 14 that X1, X3, F value ＝ 43.62, R^2 value ＝ 0.649, P value ＝ 1.94E-11, 65% of the predicted variance is the best choice for the two Xs.

Table 14: Regression X1and X3 of RPN

Multiple coefficient of correlation		0.806176			
R^2		0.64992			
Adjusted R^2		0.635023			
Standard error		8.501333			
Number of observations		50			
ANOVA					
	DF	SS	MS	F	P-value
regression	2	6306.165	3153.082	43.62759	1.94E-11
residual	47	3396.815	72.27266		
SUM	49	9702.98			

(3) Choice of the one X:

There are 4 possible choices to choice one independent variable. According to Table 15 that X1, F value = 45.08, R^2 value = 0.48, P value = 2.02E-08, 48% of the predicted variance is the best choice for the one X.

Table 15: Regression X1 of RPN

Multiple coefficient of correlation		0.695946			
R^2		0.48434			
Adjusted R^2		0.473597			
Standard error		10.20971			
Number of observations		50			
ANOVA					
	DF	SS	MS	F	P-value
regression	1	4699.544	4699.544	45.08463	2.02E-08
residual	48	5003.436	104.2383		
SUM	49	9702.98			

According to Table 16, the X4, F= 45.08, R^2 value = 0.002, P value = 0.77, that showed not significant.

Table 16: Regression X4 of RPN

Multiple coefficient of correlation		0.041903			
R^2		0.001756			
Adjusted R^2		-0.01904			
Standard error		14.2053			
Number of observations		50			
ANOVA					
	DF	SS	MS	F	P-value
regression	1	17.0374	17.0374	0.084431	0.772632
residual	48	9685.943	201.7905		
SUM	49	9702.98			

The X4 is negative coefficient and the certification body auditor might base on humanity reason that does not yield the nonconformity or just open few amounts [1]. This issue could do more research in the future.

(4) All possible subsets result

The result of combining of all possible showed in the following Table 17.

Table 17: The Result for All Possible Subsets Method

independent	F	R^2	P
X1	45	0.48	2.02E-08
X2	13.96	0.22	0.000494
X3	9.96	0.29	0.000241
X4	0.08	0.081	0.772
X1+X2	30.31	0.56	3.51E-09
X1+X3	43.62	0.649	1.94E-11
X1+X4	24.03	0.56	6.47E-08
X2+X3	27.32	0.537	1.34E-08
X2+X4	22.31	0.42	3.25E-06
X3+X5	5.95	0.20	0.0049
X1+X2+X3	30.35501	0.663	5.63E-11
X1+X2+X4	24.09	0.61	1.6E-09
X1+X3+X4	30.18	0.664	6.12E-11
X2+X3+X4	6.59	0.30	0.0008
X1+X2+X3+X4	24.97	0.68	6.2E-11

All above showed that select more independent variable X1+X2+X3+X4 is the best choice to explain the Y. However, Choice the X1+X3+X4 almost have the same effective as the choice the 4X. This is an interesting issue to find the other independent variables such as the equipments numbers, student numbers or other factories in the future.

IV、 CONCLUSION

This paper used the FMEA model to detect the law compliance for universities. Most organization did not well do the risk analysis for the information system due to the ability of equipments and the manpower. This study offers an easy and useful way to do the risk analysis of the ISMS based on checking the exact result for the probability of Occurrence (O), Severity (S), the Lack of Detect ability (D) to determine the result of regulatory compliance and preventive management system and find the weakness to do the action to reduce and avoid the risk.

The independent variable in this study ,X1-yearly violating TPIPA times, X2-yearly self-detecting violations, X3-government detected the attacked times, and X4-yearly

third-party opened non-conformity were used for the regression analysis. The result shows a significant relation. Based on statistical analysis, in 95% reliability when X1, X2, X3, and X4 can be explain the dependent variable 68% of the variance. The multicollinearity is not obvious; therefore, the result can be accepted.

The information analysis shows that

(1) Public school had more ISMS risk than the private school.

(2) University has more ISMS risk than the University of Technology.

(3) Senior schools had more ISMS risk than younger schools.

(4) The less-students' University had more ISMS risk than the more-students' University.

Based on FMEA and regresses analysis, decrease the O, S, D of the ISMS will reduce the risk. The following are the conclusions and directions for research in the future:

(1) Failure mode can be used in different organization for ISMS.

(2) Organization may purchase the appropriate information security detection equipments and facilities to reduce risk. (Reduce D and O)

(3) Increase training and detecting manpower could reduce risk. (Reduce D and O)

(4) Only design change could reduce the S that must use change the processes such as the software or hardware to reduce the S.

This study limited the timely to do the post study and limited to study the leadership, the relationship between the staffs, the profit, the marketing share (students' amount) and the cost issues. The research can be extended in the future.

[Acknowledgment]

This work was supported by Taiwan Information Security Advisory Group, technical service centers, international Certification Bodies such as the NQA, TUV-NORD, SGS, and BSI.

References

[1] Easter C. K. Huang and C. Chung-Jen, "The affection between the certification strategy and the quality cost," in *2013 Conference on Theory and Practice of Business Management & Accounting Information*, Taichung, June 2013.

[2] H. Mintzberg, J. Lampel and B. Ahlstrand, *Strategy Safari: A Guided Tour Through The Wilds of Strategic Management*, Free Press, 2005.

[3] Easter C. K. Huang and C. Chung-Jen, "The using of Eyes contact Video conferencing system in the information security" in *Electro-optics and Communications Conference*, Taipei May 2013.

[4] Executive Yuan, "The development programs of national information security, 2009~2012," *National Information and Communication Security*, 2009.
[5] Information Security Certification Center educational institutions of National Tsing Hua University, "ISMS Certifications list," 2011.
[6] W. Jiang, X. Fan, D. Duanmu and Y. Deng, "A new security risk assessment method of website based on generalized fuzzy numbers," *Journal of Computers*, vol 8, no 1, pp. 136-145, 2013.
[7] X. Lu, C. Zhong and L. Yang, "Security risk assessment method of website based on threat analysis," *Journal of Computer Applications*, vol. 29, pp. 94-96, 2009.
[8] International Automotive Task Force-IATF, "Failure Mode Effect Analysis," 2008, Fourth Edition.
[9] International Automotive Task Force-IATF, "Advanced Product quality planning," 2009.
[10] Slobodan Živković1, *An illustration of Failure Mode Effect Analysis* (*FMEA*), Techniques to the analysis of information risk, 2005.
[11] C. Chen, B. Cherng, X. Chen, Z. Liu, *multivariate analysis*, Wunan, Rev. 5, 2009.
[12] J. Cohen, P. Cohen, S. G. West and L. S. Aiken, *Applied multiple regression/correlation analysis for the behavioral sciences*, 3rd Ed., Mahwah, N.J.: Lawrence Erlbaum Associates, 2003.
[13] Easter C. K. Huang, *The Effectiveness of the Certification Strategies to the GDP and to the Enterprises' Risk and Quality Cost: The Nature of Certification*, Thesis for the Degree of Doctor. Ph.D. program in Taiwan Industrial Strategy and Development, Chaoyang University of Technology, 2014.

Authors introduce

Easter C. K. Huang was born in 1965 in Kaohsiung. Taiwan, He had more than 20 years working experience in the Computer security area, especially, in the risk control and the product and system certification area. He is the senior ISMS consultant for Taiwan government including FDA, MOTC, Taiwan Water Corp. and MOI, and training and teaching the TQM and ISMS in University in USA, China, Japan, Korean and Taiwan.

Chin Chung-Jen was born in Taiwan and is the Professor and President of Chaoyang University of Technology from 2005 to now and was the President of Yu Da University in 2003~2005, he is the Ph.D. in Education, National Chengchi University, Taipei, Taiwan. His research interests are in the areas of education Administration, Educational Psychology, Social Psychology and Interpersonal Relations and Communication.