Understanding User Participation in Information Security Risk Management

Mohd Sharudin Mat Deli[a],Jarin Fathima Ahmad[a],
Noor Hafizah Hassan[a,*], Nurazean Maarop[a], Ganthan Narayana Samy[a], Mohd Shahidan Abdullah[a], Suraya Yaacob[a]

[a]*Advanced Informatics School, Universiti Teknologi Malaysia, Jalan Sultan Yahya Petra, 54100 Kuala Lumpur, Malaysia.*

Abstract

Risk management is the continuing process to control and manage the risk in organisation for identifying, accessing and controlling threats to an organisation’s capital and earning. The implementation of information security risk management (ISRM) helps to address the risks to information processed by an organisation that may help the organisation to manage the risk effectively. Involving the user throughout the process of ISRM is important to ensure that it provides an effective security risk management (SRM). There are limited evidence shows that user participation is important in ISRM. Therefore, the aim of this paper to investigate user participation in ISRM from user participation and access control constructs. A quantitative method is implemented by distributing a questionnaire to two different organisational backgrounds to 20 respondents. This paper presents the initial findings that user participation play a significant role towards ISRM by presenting the results from the two constructs. The findings contribute to the body of knowledge that understanding user participation in ISRM shows that the process of risk management is different between two organisational backgrounds.

Keywords: Information Security Risk Management, User Participation, ISRM

1. Introduction

Risk management will help top management in organisation to treat loss exposures and monitor risk control and financial resources, and then mitigate the adverse effects of loss [1]. Loss may result from the variety of sources including financial risks such as cost of claims and liability judgments, operational risks such as labour strikes, perimeter risks including natural disaster or political change and strategic risks including management changes or loss of reputation. Nowadays, the development of risk management plan broadens in many ways. It helps the organisations in identifying and controlling threats in protecting their digital assets such as in proprietary corporate data, a customer’s personally identifiable information and intellectual property.

* Corresponding author. *E-mail address*: noorhafizah.kl@utm.my

Risk management standards have been developed by several organisations, including the National Institute of Standards and Technology and the ISO. The ISO 31000 principles, for example, provide frameworks for risk management process improvements that can be used by companies, regardless of the organisation's size or target sector [2]. All risk management processes follow the same basic steps showing five risk management process steps which are i) identify, ii) analyse, evaluate and rank (iv) treat (v) monitor and review the risk [3].

Many organisations largely depend on existing security risk management (SRM) framework to support their risk management activity. In information technology project, it is known that user risk were found to reduce the positive influence of controls on process performance in ensuring good process performance [4]. Besides, in [5], it shows that user participation was found to add value to an organization’s SRM with the support of organisational awareness of security risks and control with alignment of SRM objectives, values and needs.

The purpose of this study is to understand how user participation in ISRM practices may contributes to the efficient of risk management in two different organisational background. This research use the constructs suggested in [5]. Therefore in this paper, the background of ISRM is review, covering well established standards and frameworks. Next, a methodology and result of data collected from the questionnaire survey is presented. Final section presented discussion and conclude the findings from the study conducted.

2. Information Security Risk Management (ISRM)

Information security risk management (ISRM) is known as the process of identifying, understanding, assessing and mitigating risk together with underlying vulnerabilities and the impact to information, information systems and the organisations that rely upon information for their operations [6]. In addition to identifying risks and risk mitigation actions, a risk management method and process will help to identify critical information assets - a risk management program can be extended to also identify critical people, business processes and technology [7].

The ISRM is a part of general risk management of an organisation, so it should be aligned with general, high-level risk management policy. The realization of the above-mentioned goal of information security is dependent on the information security risk management methodology; policy and procedures, process and stakeholders [8]. Threat, vulnerability, assets, outcome and impact are known as information security risk (ISR) components. The most important component in ISR is the assets [9]. Assets consist of information, process or technology that was affected by the risk. All components in ISR cannot be controlled except vulnerability [10].

2.1 Review of ISRM Standards

The ISRM frameworks are typically a bundle of processes and practices. The framework enables security managers to pinpoint where they are most vulnerable and, then, how to deal with those vulnerabilities. There are many details involved to realize an ISRMF. In this paper, 5 different frameworks is compared as shown in Table 1 which are Octave, Frap, Cobra, Risk Watch and ISRAM.

Table 1 : Comparison of ISRM framework

ISRM FRAMEWORK / **CRITERIA**	**OCTAVE**	**FRAP**	**COBRA**	**RISK WATCH**	**ISRAM**
Risk analysis approaches	Qualitative	Qualitative	Qualitative	Quantitative	Quantitative
Implementation based	Workshop based	Meeting based	Tools based - Risk Consultant & ISO Compliance	Tools based - expert knowledge database	Poll-based model / survey based
Compliance to IT standard	N/A	ISO 17799	ISO 17799	ISO 17799 US-NIST-800-26	NIST-SP-800-30 ISO 17799 ISO 13335
Skills needed	Standard	Standard	IT security, Operational risk, High level risk, e-security	Online help	Standard
Phase / Process	3 phases, 8 processes	3 phases	2 phases	3 steps	7 steps
Focus	Develop Protection Strategy	Threats, vulnerabilities, and results of data confidentiality, integrity, and availability	Gather the information about the types of assets, vulnerabilities, threats, and controls	Show ROI for various strategies	Produce well-defined risks
Impact value	Expected Value Matrix	Business impact analysis	Business impact analysis	Value of risk	Numeric value of Risk

3. Method

This study adopted research model proposed by [5] that has suggested five model constructs which are (i) User participation (ii) Organizational awareness (iii) Business-aligned SRM (iv) Control development (v) Control performance to describe the user participation in SRM. However, this study will only use two constructs which are (i) user participation and (ii) control performance as a descriptive understanding before adopting the holistic research model.

This research use quantitative method involving 20 respondents from two different organisations. The questionnaire was administered online, and consists of questions that have been divided into 3 sections, namely respondent's demographic background, user participation and control development. The first organisation known as ABC is a multinational corporation that specialise on the asset management with main services such as equity investment, fixed income investment, multi asset investment and absolute return funds. Only one staff is responsible for the risk management in the organisation, while 3 compliance officers are part of the total staff. As this organisation involved with the management of funds and assets, this organisation is strictly driven by risk matters for any decision made.

Second organisation known as XYZ is an IT department in an education organisation(university) that are responsible for the support unit that delivers ICT services for the university (staffs and students) especially in the ICT infrastructure, system development, and academic/administrative activities. Only one senior manager is responsible in ISRM in their department and organisation.

4. Findings

The results of the study are discussed in this section.

i. User participation (in SRM process)

Table 2 shows the above-mentioned risk management activities that contribute in managing risk towards information security in the organisation. In ABC organisation, it shows that implementation controls and ensuring key control exist to mitigate specific type of risk were rated as the highest. In XYZ, most respondent (N=7) responded that defining procedural controls, followed by documenting business process/transactions for risk evaluation, implementing controls and communicating any security policies.

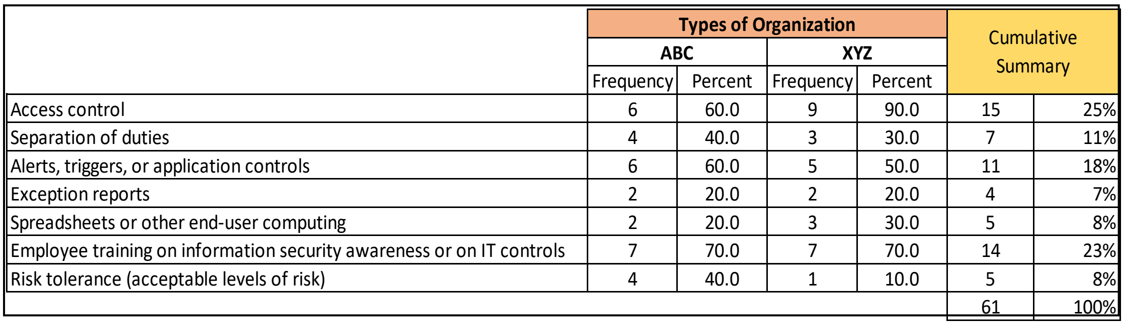
Table 2: User Participation in SRM Process

	Types of Organization				Cumulative Summary	
	ABC		XYZ			
	Frequency	Percent	Frequency	Percent		
Documenting business processes or transactions for risk evaluation	9	90.0	6	60.0	15	17%
Ensuring key controls exist to mitigate specific types of risks	10	100.0	5	50.0	15	17%
Defining procedural controls (for example, rules for access control)	8	80.0	7	70.0	15	17%
Implementing controls	10	100.0	6	60.0	16	18%
Reviewing or testing controls	7	70.0	3	30.0	10	11%
Remediating defective controls	4	40.0	1	10.0	5	6%
Communicating any security policies	5	50.0	6	60.0	11	13%
					87	100%

ii. User participation (in controls)

Table 3 shows the types of security control that has been actively participate by business users through defining, reviewing or approving any of the listed types of control. Respondent from organisation ABC (60%) and XYZ (90%) rated that access control, employee training in information security awareness on IT controls, and alerts, triggers or application controls are the types of security control implemented.

Table 3: User participation (in controls)

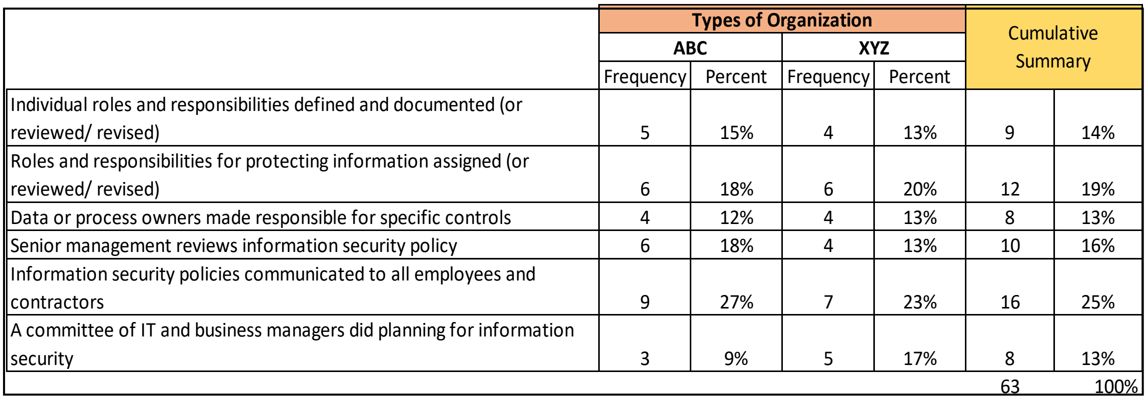


	Types of Organization				Cumulative Summary	
	ABC		XYZ			
	Frequency	Percent	Frequency	Percent		
Access control	6	60.0	9	90.0	15	25%
Separation of duties	4	40.0	3	30.0	7	11%
Alerts, triggers, or application controls	6	60.0	5	50.0	11	18%
Exception reports	2	20.0	2	20.0	4	7%
Spreadsheets or other end-user computing	2	20.0	3	30.0	5	8%
Employee training on information security awareness or on IT controls	7	70.0	7	70.0	14	23%
Risk tolerance (acceptable levels of risk)	4	40.0	1	10.0	5	8%
					61	100%

iii. User participation (via accountability)

Table 4 shows the list of actions that can be conducted to provide management accountability of information security. Both organisations, responded that information securities policies has been communicated to all employees and contractors (25%).

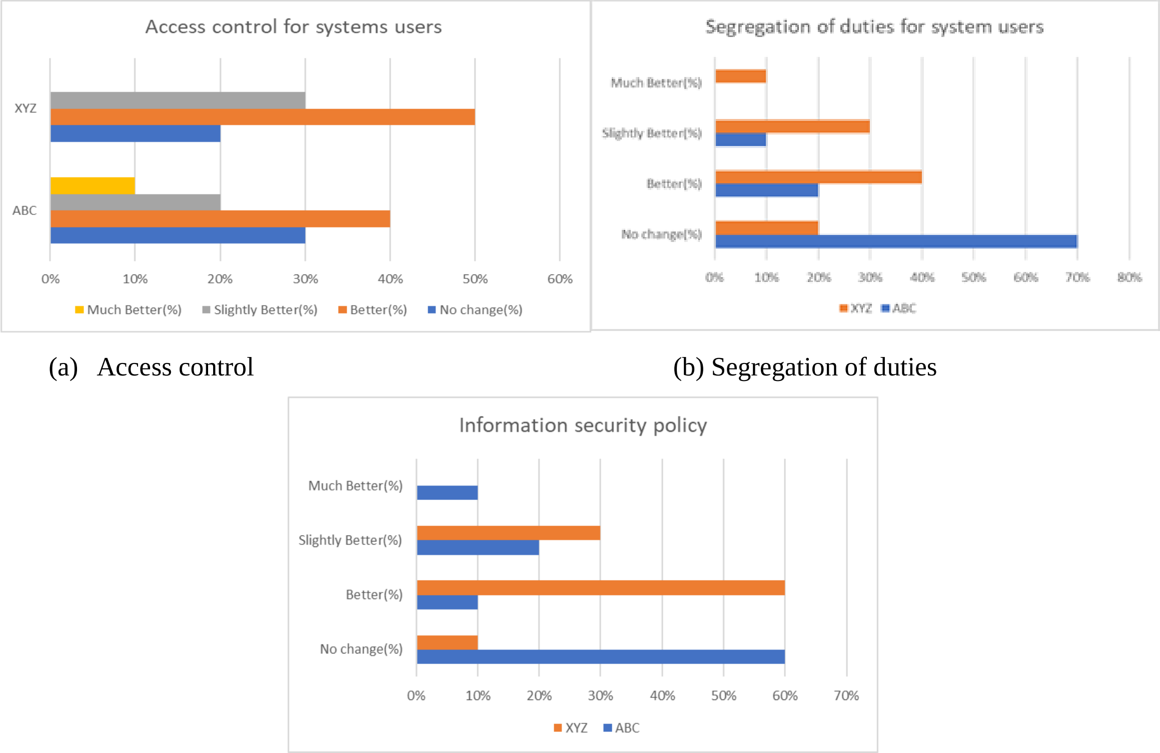
Table 4 : User Participation (via accountability)



	Types of Organization				Cumulative Summary	
	ABC		XYZ			
	Frequency	Percent	Frequency	Percent		
Individual roles and responsibilities defined and documented (or reviewed/ revised)	5	15%	4	13%	9	14%
Roles and responsibilities for protecting information assigned (or reviewed/ revised)	6	18%	6	20%	12	19%
Data or process owners made responsible for specific controls	4	12%	4	13%	8	13%
Senior management reviews information security policy	6	18%	4	13%	10	16%
Information security policies communicated to all employees and contractors	9	27%	7	23%	16	25%
A committee of IT and business managers did planning for information security	3	9%	5	17%	8	13%
					63	100%

iv. Control development

This section describes the improvement, if any, or implementation of each of the types of control, namely access controls for system users, segregation of duties for system users and information security policy.



(a) Access control

(b) Segregation of duties

(c) Information security policy

Figure 1 : Control Development

v. Control development (access control)

Figure 1(a) shows that 40% of the respondent from organisation ABC responded that access control has been better. 20% responded slightly better, and 10% responded much better, while 30% responded no change. For XYZ, the improvement on the access controls for the system are better (50%), 30% responded slightly better, 20% responded no change.

vi. Control development (segregation of duties)

Figure 1 (b) above shows the segregation of duties for system users. 70% of the respondent from organisation ABC says no change on this type of control, while 20% responded better, and 10% responded slightly better. 40% respondent from organisation XYZ says ‘better; for the improvement of control for segregations of duties for system users. 30% responded slightly better, 10% better and 20% responded change.

vii. Control development (information security policy)

Figure 1 (c) shows the respondent feedback on any improvement of information security policy in their organisation. 60% respondent from organisation ABC says that there was no change on the information security policy, while 10% says better, 20 % (slightly better) and 10% responded much better. For organisation XYZ, 60% of the respondents say information security policy has been better, 30% responded slightly better and 10% responded no change.

5. Result and Discussion

In this paper, the objective was to gather deeper insights of user participation of ISRM in the context of the education and financial company background. The major implications garnered from the findings are shown in Table 5. It shows that ABC organisation that their major operation on managing fund shows higher percentage of user participation and not many improvements have been done in control development compared to XYZ organisation. Therefore, it can be conclude that the background of organisation may determine the participation of user in ISRM.

Table 5: Summary of Findings

Security Risk Management Requirements	**Percentage Company ABC**	**Percentage Company XYZ**
User participation in security risk management	Higher	Lower
User participation (in control)	Higher	Lower
User participation via accountability	Lower	Higher
Control development (access control)	Better	Better
Control development (segregation of duties)	No Change	Better
Control development (security policy)	No Change	Better

6. Conclusion

Many organisations recognize that their employees, who are often considered the weakest link in information security become the greatest assets in the effort to reduce risk related to information security to be included in ISRM framework. Understanding user participation is important to ensure that they comply and adhere to security rules and regulations in the organisation in the ISRM process implementation. This research identifies the current practice of risk management in information security for two organisations, and our results show that basically the information security risk management for both organisations may improve the company culture by increasing the aspect of user participation and control development. However, this research still infancy. This research only focused on two organisations with limited number of respondents and only presented on two independent construct that should be further evaluating the relationship in the research model. Besides, it did not test the holistic research model proposed that will be further evaluated with bigger sample and more organisation.

References

[1] C. Lindholm and M. Host, Introducing usability testing in the risk management process in software development, in *2013 5th International Workshop on Software Engineering in Health Care, SEHC 2013 - Proceedings*, 2013, pp. 5–11.

[2] D. Proença, J. Estevens, R. Vieira, and J. Borbinha, Risk Management - A Maturity Model Based on ISO 31000, in *19th Conference on Business Informatics*, 2017, pp. 99–108.

[3] G. P. Gasca-Hurtado, V. V Zepeda, J. A. Echeverri-Arias, and T. S. Feliu, “Symilarity of standards and models according to risk management process for software development, in *7th Iberian Conference on Information Systems and Technologies (CISTI 2012)*, 2012, pp. 1–6.

[4] M. Keil, A. Rai, and S. Liu, How user risk and requirements risk moderate the effects of formal and informal control on the process performance of IT projects, *Eur. J. Inf. Syst.*, vol. 22, no. 6, pp. 650–672, 2013.

[5] J. L. Spears and H. Barki, User Participation in Information Systems Security Risk Management, *MIS Q.*, vol. 34, no. 4, pp. 503–522, 2010.

[6] P. Sullivan, Information security risk management: Understanding the components, 2017. http:// http://searchsecurity.techtarget.com/tip/Information-security-risk-management-Understanding-the-components (accessed 15th December 2017)

[7] W. Al-Ahmad and B. Mohammed, A code of practice for effective information security risk management using COBIT 5, in *InfoSec*, 2016, pp. 145–151.

[8] J. Zarei and F. Sadoughi, Information security risk management for computerized health information systems in hospitals: A case study of Iran, *Risk Manag. Healthc. Policy*, vol. 9, pp. 75–85, 2016.

[9] U. Maneerattanasak and N. Wongpinunwatana, A proposed framework: An appropriation for principle and practice in information technology risk management, in *The Institute of Electrical and Electronics Engineers, Inc. (IEEE) Conference Proceedings*, 2017, pp. 1–6.

[10] S. Fenz and A. Ekelhart, Verification, Validation, and Evaluation in Information Security Risk Management, *Secur. Privacy, IEEE*, vol. 9, no. 2, pp. 58–65, 2011.