International Journal of Engineering & Technology, 7 (4.31) (2018) 145-150

SPC

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



The Role of Employee in Information Security Risk Management

David Lau Keat Jin[1], Noor Hafizah Hassan[2], Nurazean Maarop[3], Ganthan Narayana Samy[4] and Rasimah Che Mohd Yusof [5]

Advanced Informatics Department, Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, Kuala Lumpur
**Corresponding author E-mail: noorhafizah.kl@utm.my*

Abstract

Information security risk management (ISRM) is become essential for establishing safe and reliable environment for online and e-transactional activities. With the coming Industrial Revolution 4.0, there is a huge interest of the organization for involving user in their risk management activity to minimize any security incidents. Limited research has been conducted in investigating involvement of user in ISRM. Therefore, this paper examines the involvement of user in ISRM in financial organization. Besides, this paper discusses the existing theories of risk management use in assessing ISRM. This paper investigates user participation in ISRM implemented in the organization using mixed-method approach. This study use questionnaire survey and follow-up with interview in one financial organization. Besides, Strength, Weakness, Opportunities and Threat (SWOT) analysis is presented based on the result found for the organisation to focus on their improvements needed. This study shows that a well-known procedure and standards must be implemented in the organisation to ensure that employee participate more in the ISRM process and activities.

Keywords: *Information Security Risk Management, Risk Assessment, Employee Risk, Information Security*

1. Introduction

Risk is the effect of uncertainty for an organization in achieving its objectives. Risk management is the series of activities to identify the causes, estimate the effects and formulate countermeasures to the risks. According to ISO 31000: 2009 Risk management–Principles and guidelines (2009), risk assessment process includes identification, analysis and evaluation of risk while risk management involve both risk assessment and risk treatment activities. Risk assessments can be conducted at all three tiers in the risk management hierarchy—including Tier 1 (organization level), Tier 2 (mission/business process level), and Tier 3 (information system level) [1].

Treatment to risk serves as countermeasure, safeguard or security control that would either reduce it, transfer it to another party, avoid it totally or to explicitly accept it. In reducing the risk, it may be possible to either reduces its likelihood of occurrences or the adverse impact when it occurs. Hence, safeguards will only lower risk to an acceptable level and not utterly eliminate it.

Information security is related in safeguarding critical information assets identify within the organization. Effective risk management in an organization will enable the acculturation of processes that would enable the organization to confidently and distinctly answer some of the aspects pertaining to risk items in the organization. It is important to look in holistic view of information security management that include risk management criteria as reported by [2]. Meanwhile, it has been suggested in [3], employee play an important role for implementing information security risk and policy management in an organization. In [4], their findings suggested that research on information security management system should focus on people, process, and business goals that support the technology. User participations in security risk management becomes a valuable and important criterion to ensure that awareness of security among users can better be aligned with organizational business goal [5]. Therefore, it is important for researcher to look into user involvement towards effective information security management. In this study, employee in the organization is identified as user to investigate their involvement in ISRM. A study from [6], have also use questionnaire from [5] to examine user participation in different context of organization.

This paper is aims to examine employee role in the organization towards practicing information security risk management. The first section of the paper will brief on ISRM and the related theory and methodologies use in ISRM. Next, the research method apply in this study is discussed. A quantitative and qualitative study use in this study were discussed in findings section. Finally, the paper concludes the findings with discussion, limitation and future work that related towards the study conducted.

2. Risk Management

There are different categories of risks such as business or operational, country, environmental, reputational, strategic and financial risk (Hopkin, 2017). Depending on the outcome of a risk, it can be classified into hazard, control or opportunity type of risk. Hence, segregation of risks may be done based on its causes, impact areas and outcome as illustrated in Table 1.

Risk analysis seeks to discover the magnitude, acuteness or severity of risk. In many occasion, it is a function of either impact to the organization in the areas aforementioned or the probability of occurrence. Regardless of the risk analysis process that is being practised by an organization (whether it is BS7799, GMIT, CSE or others), the common outcome usually involves identifying the asset, ascertaining the risk, determining the vulnerability and im-

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

plement the corrective action or accepting the risk if the cost of treatment is deemed uneconomical. Treatment to risk serves as countermeasure, safeguard or security control that would either reduce it, transfer it to another party, avoid it totally or to explicitly accept it. In reducing the risk, it may be possible to either reduces its likelihood of occurrences or the adverse impact when it occurs. Hence, safeguards will only lower risk to an acceptable level and not utterly eliminate it.

Table 1: Risk Category

Risk Category			
RISK	**Sources**	**Impact Areas**	**Outcome**
	(i) Internal • Employees • Technology deployed • Operation • Physical (ii) External • Economy • Nature • Politics • Competitors • Emergent	(i)Business/ Operation (ii) Country (iii) Environment (iv) Reputation (v) Project/ Strategy (vi) Finance • Credit • Currency • Interest Rate • Liquidity • Funding	(i) Hazard/ Pure (ii) Control/ (iii) Uncertainty (iv) Opportunity/ Speculative

3. Information Security Risk Management Overview

Information security (IS) is the protection of an organization's valuable information from undesirable exposure, tampering or destruction [7]. Subsequently, information security program aims to maximise the output (products or services) of an organization while minimising the undesirable outcomes due to potential risks [8]. As part of the program, risk management endeavours to conduce confidence to all stakeholders by providing appropriate level of security for the information systems that support the organization's ongoing operations [1].

Due to a myriad of information security risk assessment methodologies, [9] attempted to classify those methodologies into qualitative, qualitative or hybrid categories. Five-dimensional view – strategy, technology, organization, people as well as environment and conceived STOPE – an IS risk management (ISRM) framework that can incorporate the common stages mentioned in the other methodologies to ensure a more complete and holistic coverage for risk analysis in [10]. However, there are no numerical result to validate its effectiveness. A framework to evaluate the completeness of the existing ISRM methodologies so that organizations may utilize a systematic approach to evaluate the suitability of those methodologies for their own organization has been proposed in [11]. Few ISRM frameworks has been use such as OCTAVE Allegro, Facilitated Risk Analysis Process (FRAP), A ISO/IEC 27005:2011; Community Based Resilient Assessment (COBRA) and Information Security Risk Assessment (ISRAM) that has been use in many organization will be summarize.

3.1 OCTAVE Allegro

The operationally critical threat, asset and vulnerability evaluation (OCTAVE) method was created by CERT Survivable Enterprise Management team to enable organizations to perform information security risk assessments in line with the operational and strategic drivers that their respective organizations rely on to achieve their mission [12].

3.2 Facilitated Risk Analysis Process (FRAP)

Developed by Tom Peltier in 1999, the Facilitated Risk Analysis Process (FRAP) is an efficient and disciplined process for ensuring that information security-related risks to business operations are considered and documented [13]. It is a risk analysis process that is driven by the business managers, take only days to implement, cost effective, uses in-house experts and can be conducted by someone with limited knowledge of particular system or business process but with good facilitation skills.

3.3 ISO/IEC 27005:2011

ISO27005 is a sequential method that comes with extensive appendices that supports the user scoping, asset, threat and vulnerability assessment (ISO, 2011). The other key standards published by the same organization that provide additional references in the implementation of this method include ISO Guide 73:2009 (Risk management-Vocabulary), ISO/IEC 27001:2013(Information technology-Security techniques-Information security management systems-Requirements), ISO/IEC 27002:2013 (Information technology-Security Techniques-Code of practice for information security controls), and ISO 31000:2009 (Risk management-Principles and guidelines). This framework provides guidelines for information security risk management in an organization, supporting in particular the requirements of an information security management (ISMS) according to ISO/IEC 27001.

3.4 Community Based Resilient Assessment (COBRA)

Community Based Resilient Assessment (COBRA) framework are famously use for assessment and analysis on risk related to environment and community [14]. It is widely use around the world to assess problems and issue related to environment such as natural disaster, natural crisis such as floods, hurricanes, tornadoes, volcanic eruptions, earthquakes, tsunamis, and other geologic processes. COBRA framework is used for only qualitative research and it cannot be used for quantitative methodology since natural disaster measurement is not static.

Data is normally collected from focus group discussion, interview and disaster measurement method [15]. By identifying disaster resilience for the target community, authorities may help in improvement of the situation for community. Resilience is a transformative process of strengthening the capacity of women and men, communities, institutions, and countries to anticipate, prevent, recover, adapt and/ or transform from shocks, stresses, and improve or change.

3.5 Information Security Risk Assessment (ISRAM)

By the name itself it can be define that Information Security Risk Assessment Methodology (ISRAM) is a risk assessment methodology used for information system security risk[16]. ISRAM methodology is proposed from [16] National Research Institute of Electronics and Cryptology and the Gebze Institute of Technology year 2014. They mentioned that ISRAM produce a consistent result during their research. However, ISRAM does not implement techniques such as single occurrence losses (SOL) or annual loss expectancy (ALE) [17]. In general, the advantages and disadvantages of ISRM methodologies or frameworks grouped into qualitative and quantitative categories as described in Table 2. In [18], they have proposed a more comprehensive taxonomy for classification of information security risk assessment framework.

In Malaysia, the Malaysian Cabinet on February 24th, 2010 mandated that each agency identified as operating within the domain of CNII must obtain certification of Information Security Management Systems (ISMS) Standard or ISO/IEC 27001:2007 within three years [19]. Prior to that, the Malaysian Administrative Modernisation and Management Planning Unit (MAMPU) published The Malaysian Public Sector Information Security Risk Assessment Methodology (MyRAM) Handbook as guidance to all government offices in safeguarding assets of information [20]. ISMS commenced in the 1990s with the Department of Trade Industry,

UK initiated an effort to increase awareness regarding IS and proposed security controls for information protection. It began with Code of Practice in 1993 and subsequently became British Standard (BS7799-1) in 1995. It then progresses from ISO/IEC 27001:2005 to become ISO/IEC 27001:2007 and finally ISO/IEC 27001:2013 which is used by all Malaysian Government Agencies.

Table 2: Information Security Risk Analysis Category

	Category of IS Risk Analysis	
	Qualitative	**Quantitative**
Advantage	• Calculations are simple. Not necessary to determine monetary value of asset. • Easier to involve non-security and non-technical staff. • Provides flexibility in process and reporting.	• The results are based. substantially on objective processes and metrics. Great effort is put into asset valuation and risk mitigation. • Cost/benefit assessment effort is essential. Results can be expressed in management-specific language.
Disadvantages	•Very subjective in nature. •Limited effort to develop monetary value for targeted assets which would aid in determining the worth of an asset. •Devoid of information for cost/benefit analysis of risk mitigation.	• Calculations are complex. • Historically only works well with a recognized automated tool and associated knowledge base. • Large amount of preliminary work. • Not presented on a personnel level. • Difficult to change directions. • Difficult to address 'out-of-scope' issues
Example	OCTAVE, CORAS, CRAMM, FRAP & COBRA	ISRAM, COBRA, IS, RiskWatch

4 Research Method

This research is adopting the Sequential Explanatory Design approach (mixed methods research design) which begins with a quantitative approach to get a sample data to verify the risk management practices of the organizations involved [21]. This is followed by a qualitative approach to identify the various risk management models, their applicability and completeness in some organizations. Our methods and analysis are used to illicit the information related to our research questions as listed in Table 3.

The respondents for this study is chosen based on their experience involved with any ISRM activities. For quantitative approach, an online survey was conducted through Google Forms to a targeted group of respondents from the studied organizations. For questionnaire survey, a set of question adopted from [5] is used to understand user participations in ISRM.

Table 3: Questions, Methods, and Analysis

Research Question	Research Methods, Data Sources and Analysis
What are some of the risk management model used by existing organizations?	• Obtain articles, journals and standard-related documents from Internet. • Identify the primary methodologies of each model • Review each model's category from information security risk assessment perspective.
What are the issues faced by the organizations in practicing risk management?	• Conduct survey to targeted through online Google questionnaires. • Carry out guided interviews with personnel in those organizations that has working knowledge of risk management. • Analyse and report the results obtained from survey and interview.
How can the identified organizations improve their risk management practices?	• Summarise the results obtained respondents. • Implement SWOT (strength, weaknesses, opportunity and threat) analysis.

To obtain a clearer view of matters regarding the issues faced by the organization in managing risk, guided interviews were also conducted with employee that directly involve in risk management. Meanwhile for qualitative study, interview was conducted based on the following constructed question.

i. What is your working definition of risk?
ii. How important is risk management in your organization today and why?
iii. How do you identify and assess risk in your IS organization?
iv. Do you use a formal risk management methodology? If so, how does it work? When do you use it?
v. What effective or ineffective risk management practices have you implemented?
vi. Do you address risk management issues with users? Why or why not?
vii. What are the risks of not doing risk management and/or the benefits of doing risk management?
viii. Do you agree that risk assessment should be a primary management tool in IS?
ix. State the most reported risk incidents in your organization?
x. Do you take reactive or proactive actions?

Only one financial organisation is selected as a guided case study was used in this research as preliminary investigation. This study will help to identify the method and mechanism they are using currently to handle threats and attacks (incidents) in their organization. Some of the factors that contribute to information security risk will be discussed further and mechanism to improve these issues will also be identified and discussed in the findings section of this paper. The qualitative study may help in understanding more about the organisation risk definition and type of risk management they are using rather than quantitative study.

5 Results

The following section will brief describe the results from the method conducted based on quantitative study (survey) and qualitative study (interview).

5.5 Results from Quantitative Study

Online survey was conducted from 16 till 31 October 2017. A total of 18 respondents from Information Management Division has given their responses with 15 respondents from IT personnel and the other 3 respondents with designations with accounting background. Half of the respondents served in the organisation for more than 10 years while 6 of them have 5 to 10 years of experience. Only 3 of them worked or less than 5 years. Hence, their responses are valid based on their job scope and years of service.

In quantitative study, nine constructs were adopted from previous study [5], which are (i) user participation in the risk management process, (ii) user participation in security control; (iii) user participation via accountability; (iv) awareness; (v) demonstrated ownership; (vi) user business perspective; (vii) Business-based IS security strategy; (viii) perceived improvement in control development; (ix) increased efficiencies. The result is presented in tabular format. With only one financial organization involved in this study, there is limited respondents that must fulfil the criteria needed which the respondents need to be involved in risk management activities.

(i) User participation in the risk management process

Figure 1 demonstrated the documenting business processes or transactions for risk evaluation is highest (100%) while remediating defective controls and communicating any security policies are the lowest (50%).

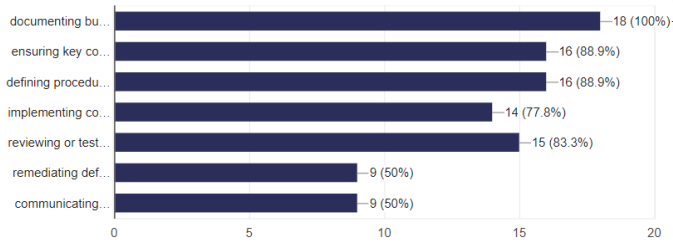

Fig. 1: User Participation in the Risk Management Process

(ii) User participation in security controls

Usage of access control is highest (100%) while application of spreadsheets or other end-user computing is lowest (38.9%) as depicted in Figure 2.

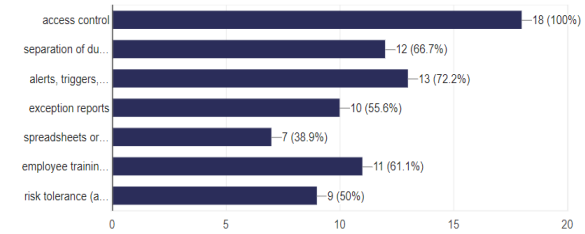

Fig. 2: User Participation in Security Controls

(iii) User participation via accountability

In figure 3, individual roles and responsibilities defined and participation documented (or reviewed/ revised) shared the highest ranking with information security policies communicated accountability to all employees and contractors (77.8%) with 14 respondents agreed that these two activities occurred in their organization. Senior management reviews information security policy and executive business management's support demonstrated for information security ranked lowest (50%) in user participation via accountability

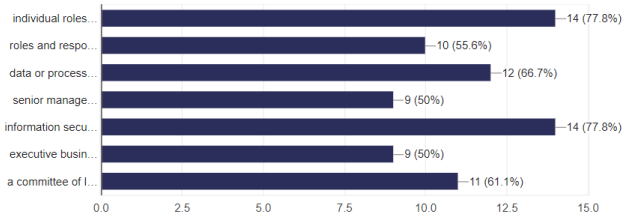

Fig. 3: User Participation via Accountability

(iv) Awareness

Figure 4 shows that results of internal employees are considered aware of policies, procedures and the need for integrity of financial reporting since a total of 11 respondents mildly agreed to strongly agreed to the statement.

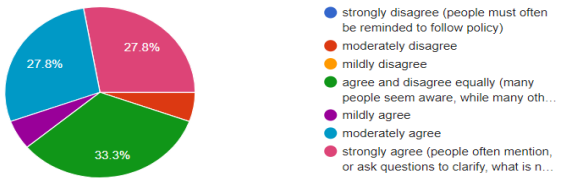

Fig. 4: Awareness

(v) Demonstrated ownership

Generally, business users are not seen as actively contributing to IS risk to financial reporting and/or financial information systems since 27.8% of respondents concurred that there are no contribution from business users with another 38.9% agreed that they contributed their perspective but not routinely as shown in Figure 5.

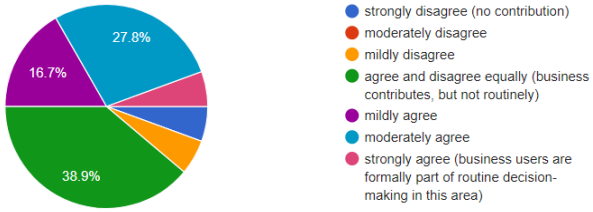

Fig. 5: Demonstrated Ownership

(vi) User business perspectives

Strategic decisions on IS policies and solutions are largely business-driven, given that 33.3% of the respondents agree with this proposition with the other 33.3% agree and disagree equally as presented in Figure 6.

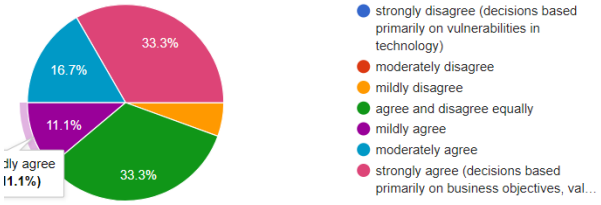

Fig. 6 : User Business Perspectives

(vii) Business-based IS security strategy

Majority agreed (>50%) that there were improvements in business-based IS security strategy in the area of access control (figure 7), segregation of duties for system users (Figure 8) and information security policy (Figure 9).

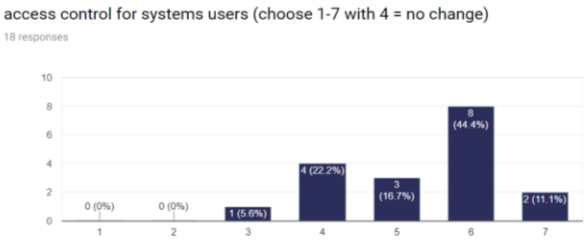

Fig. 7: Access Control

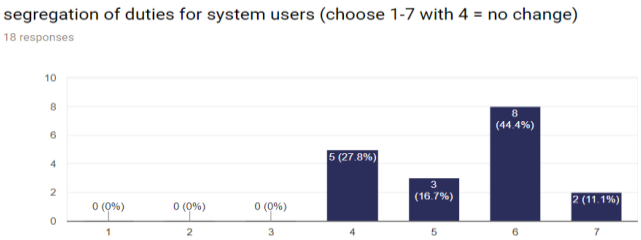

Fig. 8: Segregation of Duties

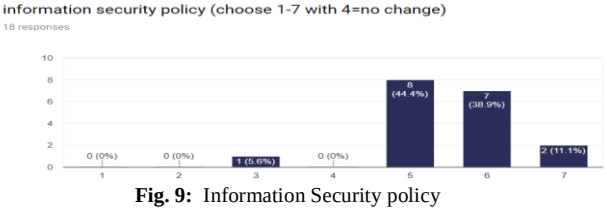

Fig. 9: Information Security policy

(viii) Perceived improvement in control development

Majority agreed (>50%) that there were strong accountability regarding the assignment of risk controls in their organization from perceived improvement perspectives as depicted in Figure 10.



Fig. 10: Perceived Improvement

(ix) Increased efficiencies

Figure 11 shows that majority of respondents agreed (>50%) that there have been efficiency improvements made (or are in-progress) to the system of controls.



Fig. 11: Increased Efficiencies

5.6 Results from Qualitative Study

The guided interviews were conducted with 4 personnel identified as having the working knowledge regarding risk management in the organisation. Besides, they also involve in information security with at least one year experience working in that area. Table 4 are a consolidated response from all four of the respondents. The table shows the summary of answer from the respondents. A total of ten questions were asked during interview session that last almost one hour. The summary shows that the organisation has already implemented a proper planning in their risk management. The involvement of the employee was also part of their risk management activities.

Table 4: Summary of Qualitative Study

Criteria	Consolidated Answers from Interviewees
Risk definition	Risk is an undesirable event that can occur which would disrupt the organization core business and operations. It is something that must be prepared for because it occurs has effect on the objective.
Importance of risk management	Risk management is very important that a systematic and agreed upon measures to be taken to manage it, such that if an identified risk occur, the organisation are able to respond to it rather than react to it. If the department defines objectives without taking the risks into consideration, chances are that we will lose direction once any of these risks hit home.
Method of risk identification and assessment	The organization is ISMS certified. The steps required by the standard is diligently applied in risk identification and assessment process. Risk identification on the assets related to the core business, ascertain/decide the associated risk that occur based on each asset's vulnerability and threat, assess the risks and take action, make a record of the findings and then evaluate/review the risk based on impact and probability of occurrence. Business Continuity Management (BCM) policy stated in the organization review Business Continuity Plan (BCP) Documentation at least once every 12 months together with the risk.
Risk management methodology used	This organisation has a 5-year ICT Strategic Plan based on its 5-year Business Strategic Plan. Under this plan, security initiatives are identified. Other than ISO/IEC 27001:2013 standard, The Malaysian Public Sector Information Security High- level Risk Assessment (HiLRA) Guides and subsequently apply MyRAM (Malaysian Public Sector Information Security Risk Assessment Methodology) are implemented. In considering the magnitude of risk, the threat, vulnerability and the valuation of assets are evaluated.
Effectiveness of risk management practices	The cycle of plan, do, check and act in the risk management cycle is implemented. Disaster recovery site ready in case the primary site is disrupted due to one reason or another. Challenges in updating all of system to the latest patches as pointed out in penetration testing report are identified.
Addressing risk management issues with users	Latest ICT Security Policy issue were address together with risk management. The risk related to social engineering and human errors become the main concern. Risk management must always be based on awareness of the capacity for the service user's risk level to change over time, and a recognition that each service user requires a consistent and individualized approach.
Criteria	**Consolidated Answers from Interviewees**
Benefits of risk management	Risk of not performing risk management include non-compliance with MAMPU's directive. Also, the organization use and generate a lot of financial information which is vital to the Federal Government. Hence, confidentiality, integrity and availability of information is crucial for the organization's success.
Risk assessment as management tool in IS	Risk management tool is necessary but its benefits must commensurate with the expenses. This also applies to the control mechanism we put in place to manage risk.
Most reported risk incidents	Most reported risk incidents would be external DDOS attack on the public website which enable the users to download their monthly pay slip. There also instance that IT personnel cannot perform payroll process because typo error like wrong amount in their remunerations and wrong charge line are mostly committed by new system users.
Reactive vs Proactive actions	Proactive actions such as equipping the data centres with firefighting system, UPS, water leak detection system, as well as monitoring system is implemented. The employees are screened before placed in their respective positions. Apart from that, revoking the access rights for any employee that has left the organization is one of the priority in minimising the risk. Risk on security is reduced significantly as the critical systems are monitored round-the-clock by Security Operations Centre (SOC). Training and re-training is also applied and meeting with the user's management is being done monthly.

6. Findings

To further analyse the results, this paper summarize the findings listed in the Strength , Weakness, Opportunities, and Threats (SWOT) compartments for the organisation in Table 5. This may help the organisation to investigate the level of employee involvement in their ISRM.

Table 5: SWOT analysis

Strength	Weakness
Controls: The organisation implemented standard controls based on available guidelines and standards. **Clarity of Objectives:** The organisation has clear vision and missions that are translated to job assignments of internal employees.	**Management and Business Users** **Role:** The management and business users did not contribute significantly to timely update of IS policies and procedures. **User Competence:** New users in key positions would require training and inculcation of IS awareness.
Opportunities	**Threats**
External Expertise: The organisation can leverage on expertise and experience of other departments in implementation of risk management.	**Policy Changes:** Changes in political leadership may warrant new project implementations and requirements.

6 Discussion

The study shows that most of the employee understand the importance of ISRM in the organisation. It can be summarized that as the organisation chosen is financial area, they have implemented an appropriate ISRM in the organisation. Most risk management

activities were implemented in the organisation. They also emphasize on risk awareness program by identifying related risk that occurs yearly together with auditing process. SWOT analysis presented shows that the organizational level to determine how closely a business is aligned with its growth trajectories and success benchmarks in risk management, and also be used to ascertain how well information security risk management is performing according to initial projections.

A survey conducted shows that majority of respondents are highly participate in documenting business processes or transactions for risk evaluation and access control. In term of security awareness, the respondents are aware of security policy in their organisation. However, in terms of demonstrating the ownership, business users in the organisation as low contributions to IS risk in the financial activities. This shows that there is a need from management to increase or motivate the employee in terms of the ownership. However, in terms of security improvements, most of them agree that a lot of improvements have been done by the management that shows that it increase efficiency in system control.

Meanwhile, from the interview conducted, it can be concluded that they have a proper risk management process according to the standard implement in their organisation. The organisation adopts respond approach compared to reactive approach to minimize the risk happened. This results on the reported-on risk incident majority is on external attack instead of internally. This demonstrates that the employee plays a very important role towards their information security activities.

This study shows that with the involvement of employee in information security risk management activities, it will minimize the incidents occur. However, the study should involve different types of organisation for better understanding of employee involvement.

7 Conclusion

Almost all types of organization are facing risk in their everyday business and services. Many standards are designed and created by private bodies to adhere in organization for their risk management processes. Implementing risk management system in organization especially large organization is a daunting journey, and often overlooked. Organizations typically chose specific standards for their risk or quality management but not many can claim success to implementing a risk management system. Often, organizations tend to manage risk in departmental level rather than looking it as an entire organizational need. Risk Management system basically facilitates the identification, analysis, monitoring, review and treatment of both existing and potential hazards and risks throughout organization. Identifying and applying appropriate treatments will secure companies vital assets such as information, hardware, people and environment. Typical risk management functions in organizations are documented as Business Continuations Process (BCP) and Disaster Recovery Process (DRP) which are sometimes overlooked and not updated regularly by authorities. Generally, actions are taken once the risk occurs which sometimes cause enormous damages to organisation assets.

Acknowledgement

We would like to thank Universiti Teknologi Malaysia, Ministry of Education and Vote 14J99.

References

[1] Stoneburner, A., Goguen, A. and Feringa, A, "Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology", NIST Special Publication., (2002), available online: https://www.archives.gov/files/era/recompete/sp800-30.pdf, last visit: 20.06.2018

[2] Zahoor Ahmed Soomro, Mahmood Hussain Shah; Javed Ahmed, "Information Security Management Needs More Holistic Approach: A Literature Review", International Journal of Information Management, Vol. 36, No. 1, (2016), pp. 215–225, available online: https://www.sciencedirect.com/science/article/pii/S0268401215001103, last visit: 20.07.2018

[3] Safa, Nader Sohrabi, et al. "Information security conscious care behaviour formation in organizations", Computers & Security, Vol. 53 (2015), pp. 65-78, available online: http://www.mihantarjomeh.com/wp-content/uploads/2016/02/Information-security-management-needs___sder85t2d3gf0gg0g.pdf, last visit: 19.06.208.

[4] S Dzazali, Suhazimah, Ainin Sulaiman, and Ali Hussein Zolait. "Information security landscape and maturity level: Case study of Malaysian Public Service (MPS) organizations." Government Information Quarterly, Vol. 26, No. 4, (2009), pp. 584-593.

[5] Spears, Janine L., and Henri Barki. "User participation in information systems security risk management." MIS quarterly, Vol. 34, No. 3, (2010), pp. 503-522.

[6] Deli, M. S. M., Ahmad, J. F., Hassan, N. H., Maarop, N., Samy, G. N., Abdullah, M. S., & Yaacob, S. (2018). Understanding User Participation in Information Security Risk Management. Open International Journal of Informatics, vol. 5, No. 1, (2017), pp 1-8, available online: http://publication.ais.utm.my/ojs/index.php/oiji/article/view/35, last visit: 1.07.2018.

[7] Sadowsky, G., Dempsey, J. X., Greenberg, A., Mack, B. J., & Schwartz, A., Information technology security handbook. Washington, DC: World Bank. G (2003).

[8] Wheeler, E. Security risk management: Building an information security risk management program from the Ground Up. Elsevier, (2011).

[9] Behnia, A., Rashid, R. A., & Chaudhry, J. A.. "A survey of information security risk analysis methods", SmartCR, Vol. 2, No. 1, (2012), pp. 79–94.

[10] Salleh, K. A., Janczewski, L. J., & Beltran, F.. "SEC-TOE Framework: Exploring Security Determinants in Big Data Solutions Adoption", Proceedings of The Pacific Asia Conference on Information Systems, 2015.

[11] Wangen, G., Hallstensen, C., & Snekkenes, E."A framework for estimating information security risk assessment method completeness". International Journal of Information Security, (2016), pp. 1–19.

[12] Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R.. Introducing octave allegro: Improving the information security risk assessment process (No. CMU/SEI-2007-TR-012). CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST (2007).

[13] Peltier, Thomas R. "Facilitated risk analysis process (FRAP)." Auerbach Publication, CRC Press LLC (2000).

[14] United Nations Development Programme, "Community Based Resilience Assessment (CoBRA) Conceptual Framework and Methodology," (2013).

[15] Francis O., "Community Based Resilience Analysis (COBRA) Assessment", (2013), available online : https://www.researchgate.net/publication/279534526_Community_Based_Resilience_CoBRA_Assessment, last visit: 1.07.2018

[16] Karabacak, B., and Ibrahim S., "ISRAM: information security risk analysis method", Computers & Security, Vol. 24, No. 2 (2005), pp. 147-159.

[17] Chandrashekhar, A. M., Yadunandan Huded, and HS Sachin Kumar. "Advances in Information security risk practices." International Journal of Advanced Research in data mining and Cloud computing (IJARDC), Vol. 3, No. 5, (2015).

[18] Shameli-Sendi, A. , Rouzbeh Aghababaei-Barzegar, and Mohamed Cheriet. "Taxonomy of information security risk assessment (ISRA)." Computers & Security,Vol. 57, (2016), pp. 14-30.

[19] MAMPU, "Panduan Keperluan Dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 Dalam Sektor Awam," 2010.

[20] MAMPU, "The Malaysian Public Sector Information Security Risk Assessment Methodology (MyRAM) Handbook," 2005.

[21] Creswell J. and Plano Clark, V., Designing and Conducting Mixed Methods Research, SAGE publication, (2017).