UNIT 2: User's Participation, Assessment and Risk Management Process.

Introduction:

Here we reviewed the two different approaches of risk management assessment (Qualitative &Quantitative assessment) method in the context of regulatory compliance. An article on user's participation in information system development by Spears & Barki (2010) was used to illustrate benefit of user participation in Information System Design (ISD), implementation and control. The two assessments approaches above facilitate data gathering, processing and result prioritizing for security risk management (SRM) identification, implementation, monitoring and mitigation. (Alberts and Dorofee 2003)

- One of the formative Weekly activities is to read the Spears & Barki (2010) article on user participation in information system security risk management in MIS Quarterly and answer the following questions:

Q1. How did the authors use both Qualitative and Quantitative assessment approaches? What benefits did each approach yield?

Response: One of the ways the author used the above assessment approaches is under multi-method research design where it illustrated that the use of qualitative exploratory study informed a subsequent confirmatory study by quantitative method.

Some of the benefits of the adopted approaches such as qualitative method is that it provides rich understanding of activities, behaviours and assignment that defines user participation in the context of Security Risk Management for regulatory compliance. It also allows process model to be constructed by applying the three user participation theories as a framework for analysis (Markus and Mao 2004). The process model is based on narrative explanation of a sequence of events that contribute to a specific outcome (Tsohou et al.2008, P.275)

Q2. What do the authors list as the advantages of involving users in the risk management process?

Response are as follows:

1. it influences the degree of success in implementation of the Information System Development (ISD). Using the author's Buy-in theory of user participation to illustrate the point, it involves the user participating in the planning and designing of Information System Development and this gives the user the sense of ownership and it triggers positive attitudes towards adoption of the ISD (Barki and Hartwick 2001).

2. It increases the users' awareness of security risk of a system.

3. It encourages information exchange and knowledge transfers (Latham et al, 1994, Locke et al 1997). Involving the users to participate in ISD planning, designing and implementation, gives the Risk management team the opportunity to understand users' business dynamics and identifies the possible threats and vulnerabilities. Likewise, the users having the privilege to the underlying principles behind certain risk control measures and the possible effect on the asset.

4. It improves system quality. As indicated in the system quality theory, the developers become more informed about the business needs when the users are appropriately engaged, and it results to a higher quality and more successful system (Markus and Mao 2004).

5. It aids adaptability of the users with the system. The participation creates the opportunity for the users to have relationship with the system which result in higher usage of the system.

6. User participation helps to increase the risk control measures.

Q3. Based on the findings of the research,

i. How will the lack of user access affect the risk assessment you will carry out as part of your assessment?

Response: This will contribute to inadequate risk identification, evaluation and implementation of appropriate measures or risk assessment techniques. Allowing user participate in the risk management process of ISD will assist the analyst to identify the critical risk areas to deploy appropriate risk control as there is full engagement in understanding the user's task process and feedbacks on asset usage experience .

ii. Will it affect the choice of Qualitative vs. Quantitative assessment methods you utilise?

Response: The articles explained factors that drive the assessment method to be used in evaluating security risk of ISD using Sarbanes-Oxley Act in the context of organization compliance .

S/N	Variables	Qualitative Assessment Approach	Quantitative Assessment Approach
1.	Value of the asset	The asset has lower value ie the asset sensitivity is very low	Asset value is high as any successful cyberattack has a great implication.
3	Personnel skill	Used by untrained or unskilful staff.	This approach is usual use by professionals like Compliance risk assessment officer, Risk

			Audit staff, & Management consultant etc,
	Data Collection	Subjective risk evaluation method like response from questionnaires	It uses statistic or historical data
4	Threat/Vulnerabilities Ranking	The risks are categorized as High, Medium & Low	The risks are ranked on weight of the probability outcome

iii. How might you mitigate any issues encountered?

Response: The mitigation mechanisms can be categorized as listed below

1. Physical Control: This is where physical control such as CCTV, Alarms system and Security guards etc. are deployed.

2. Procedural Control: It can be induction or annual training on new process or new roles

3. Technical control: This is where organisation deploy and improve on network security system such as firewalls, Access control, Security Information & Event Management (SIEM) etc.

The above mitigations can be used for preventative control like blocking and removal of threats and vulnerabilities, Detective control as detect and report unauthorized personal, corrective control in terms of response and fix incident or improve on user's participation feedback. The above can also be used to directive control where staff are been informed of their duties and responsibilities.

Reference:

Spears, J. & Barki, H. (2010) User Participation in Information Systems Security Risk Management. *MIS Quarterly* 34(3): 503.Avaliable from: https://www-jstor-org.uniessexlib.idm.oclc.org/stable/25750689[Accessed 18 August 2023]

University Essex Lecture Cast unit 1. Risk & The Risk Management Process**,**Available from :https://www.my-course.co.uk/Computing/Cyber%20Security/SRM/SRM%20Lecturecast%201/content/index.html#/ [Accessed on 15 August 2023]