**Unit 2 – Seminar (User Participation in the Risk Management Process)**

The authors determined that a high level of uncertainty surrounded the study – implying inadequate information regarding user participation in the context of security risk management (SRM) for quantitative measurement. In adopting the qualitative assessment approach, the authors used a process model applying the three user participation theories described by Markus and Mao (2004) which are the buy-in theory, the system quality theory, and the emergent interactions. This process model is a sequence of events that contribute to a specific outcome Tsohou et al., (2008). This approach provided a rich understanding of the behaviour, activities, and assignments that define user participation in the context of SRM for regulatory compliance (Spears & Barki, 2010).

Quantitative assessment approach included the testing of theoretical model derived from the qualitative study, and then hypothesis generated from the qualitative study to determine a variance model for examining the degree to user participation in pre-specific outcome variables (Tsohou et al., 2008). The qualitative and quantitative approach combined provides a rich context, which strengthened the results through triangulation – whereby cross validation of both kinds of sources were congruent.

The major advantages to having users participate in the risk management process as described by the authors are:

* User Awareness of Risks: Those who handle information on their day to day business once aware of the risks, take extra precaution in ensuring things are done right. Engaging users through awareness enhances the risk management process.
* Aligning security controls with business objectives. Involving users in the risk management process will assist align business objectives, provide needed business knowledge, and further improve security measures.

Lack of users would make the risk assessment process not rich with user behaviour pattern and activities. This will skew the assessment to mere probability or guessing. A mitigation strategy would be to profile users, and have a decision criteria/reality check was set as input into control designs.

**Reference**

Spears, J.L. and Barki, H., 2010. User participation in information systems security risk management. *MIS quarterly*, pp.503-522.

Tsohou, A., Kokolakis, S., Karyda, M., and Kiountouzis, E. 2008. "Process-Variance Models in Information Security Awareness Research," Information Management & Computer Security (16:3), pp. 271-287