# Collaborative Discussion One

Question

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

Answer

The author used Qualitative approach to provide an understanding of the user participation is the security risk management and to create a process model too, but this was only exploratory as it was not based on a pre defines data so a quantitative method was required too. The quantitative method was used after this to test the process model. A variance model was also created after this to further investigate the user participation. Benefits of Qualitative approach in this case was that prior to this there was unsureity about the user participation in I SRM to be able to quantitively measure it. Another benefit is that performing risk assessments is relatively an easier and quicker task to do compared to the Quantitative approach. (Wooldridge, 2007) But using both methods together provided supplied the study with a rich background as well as testability. (Kaplan and Duchon, 1988) Furthermore it strengthened the results as two various sources of data were used.

Question

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

Answer

The involvement helped increase awareness of the security risks as well as the awareness for the financial information system. They understood all about the details of the security risks and the reasoning’s behind the management of the risks

Question

Based on the findings of the research,

* + how will the lack of user access affect the risk assessment you will carry out as part of your assessment?
  + will it affect the choice of Qualitative vs. Quantitative assessment methods you utilise?
  + how might you mitigate any issues encountered?

Answer

The lack of user involvement could mean that the vulnerabilities detected would be a difficult task as users are vital part for risk assessments. Most likely for this assessment we would need to make a choice between using either qualitative or the quantitative methodology. I believe the qualitative methodology would be appropriate as we would need to make assumptions on behalf of the users.

References

Wooldridge, M., (2007). Qualitative risk assessment. Microbial risk analysis of foods, pp.1-28.

Kaplan, B. and Duchon, D., (1988). Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study. *MIS Quarterly*, 12(4), p.571.

Spears, J. & Barki, H. (2010) User Participation in the Risk Management Process. MIS Quarterly Vol. 34 No. 3:503-522. Available from:https://eds.b.ebscohost.com/eds/pdfviewer/pdfviewer?vid=2&sid=63261005-d8f1-47b7-aaa8-4e4b8626cc47%40sessionmgr102 [Accessed 14 August 2021].

Summary

After reading posts of peers, it can be analysed that using both Quantitative and qualitative methodology is a useful and essential aspects when carrying out Risk assessments. Furthermore, as Faruque (2021) has explained user involvement is necessary and we should not rely on only the technical driven analysis as this can lead to bias producing inaccurate results.

References

Faruque, N. (2021) Initial Post. Available from: <https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=271404> [Accessed 12 September 2021]

## Collaborative Discussion Two

Question

Top 5 overall causes of risks

Answer

Roy et al (2015) mentions 5 causes of risks which are:

1) Incorrectly estimating the resources

2) Incorrectly designing systems

3) Ambiguity from users and customers

4) Development of the systems which can cause the risk

5) insufficient requirements of system

Question

List the mitigation actions of the above risk

Answer

Solutions from group

As mentioned by my group member Luvaha (2021) It has been defined by Ross et al (2016) some mitigations for the above risks

During the system development life cycle the security principles shoykd be applied, to claim that the system is free from risks there should be solid evidence, furthermore security requirements should be analysed and defined as well and identifying the vulnerabilities which can cause threats to systems.

Further corrected by our tutor Faruque, (2021) “*An overall reliance of trust based concept should be established so that the subjective and contradictory needs of the stakeholders get addressed and only then the targeted cause of the risk factors could be eliminated*.”

References

Luvaha, D. (2021) Initial Post. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=273855 [Accessed 10/09/2021]

Ross, R., McEvilley, M. & Oren, J. (2016) Systems security engineering: considerations for a multidisciplinary approach in the engineering of trustworthy secure systems, volume 1.

Available from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf

[10/09/2021].

 Roy, B., Dasgupta, R. & Chaki, N. (2015) A Study on Software Risk Management Strategies and Mapping with SDLC. *Advances in Intelligent Systems and Computing* 1(1): 121-138. DOI: [**https://doi.org/10.1007/978-81-322-2653-6\_9**](https://doi.org/10.1007/978-81-322-2653-6_9). Available from: https://www.researchgate.net/publication/283713387\_A\_Study\_on\_Software\_Risk\_Management\_Strategies\_and\_Mapping\_with\_SDLC [Accessed 10 September 2021].

Faruque, N. (2021) Initial Post. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=273855 [Accessed 10 September 2021]