SEMINAR 2 PREPARATION GROUP 1

User Participation in the Risk Management Process

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

A lack of user access could mean…

Design, implementation and performance for security control development

- Inferior knowledge of user operation
- No consideration to user feedback
- Potentially lower performance as users can support the level of risk exposure understanding
- Risk assessment may not be directly relevant for effective use

Business objectives

- Challenge to align security measures to business objectives
- Business outcomes may be lower
- Lack of organisational awareness with business processes

Expertise

- Lack of user expertise to identify mitigation needs
- Limitation of the expression of expertise to the business-oriented goals
- Lack of empowerment for the users

Amrit, C., Hillegersberg, J. & Diest, B. (2013) Involving End Users to Mitigate Risk in IS Development Projects. Journal of Organizational and End User Computing 2013 Vol. 25. United States. Available from: DOI: 10.4018/joeuc.2013070105 Accessed 16 March 2022].

Spears, J. & Barki, H. (2010) User Participation in Information Systems Security Risk Management. Management Information Systems Research Center, University of Minnesota. Available from: https://www.jstor.org/stable/25750689 [Accessed 16 March 2022].

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

- Quantitative method uses numerical and statistical techniques to calculate the likelihood and impact of risk
- Quantitative method is data-driven and produces statistically reliable results
- Given the high degree of uncertainty and insufficient knowledge to deduce user participation, a quantitative method will not yield a satisfactory result.
- It is not easy to collect data on every process.
- Reliable historical data may not be available for analysis to quantify risk.
- The cost of quantitative analysis is usually higher than qualitative analysis
- Qualitative analysis often reflects inputs of business units more accurately than quantitative analysis, and it also captures “soft” risk such as morale or reputation.

Considering the above, we would use the qualitative assessment method for risk assessment.

Information Systems Audit And Control Association (2013). CRISC review manual 2014. Rolling Meadows, Ill.: Isaca.
Spears, J. & Barki, H. (2010) User Participation in Information Systems Security Risk Management. Management Information Systems Research Center, University of Minnesota. Available from: https://www.jstor.org/stable/25750689 [Accessed 14 March 2022].

How might you mitigate any issues encountered?

Issues	Mitigation
Subjective Assessment Qualitative assessment does not yield measurements, it is based on the perspective of the individual doing the research instead	A qualitative risk analysis should involve numerous persons to reduce subjectivity. The accuracy and depth of the analysis are determined by the team's past expertise.
Noisy data Meaningless data might produce during the assessment when users resist the change or focus on self-interest.	According to the research, it could be robust to noise with regression like Partial Least Squares (PLS), developed from the principal component regression, which helps in building models predicting more than one dependent variable (Lorber et al., 1987).

Lorber et al., (1987) A theoretical foundation for the PLS algorithm. Journal of Chemometrics. Available from: https://analyticalsciencejournals.onlinelibrary.wiley.com/doi/10.1002/cem.1180010105 [Accessed 16 March 2022].

References

Amrit, C., Hillegersberg, J. & Diest, B. (2013) Involving End Users to Mitigate Risk in IS Development Projects. Journal of Organizational and End User Computing 2013 Vol. 25. United States. Available from: DOI: 10.4018/joeuc.2013070105 Accessed 16 March 2022].

Information Systems Audit And Control Association (2013). CRISC review manual 2014. Rolling Meadows, Ill.: Isaca.

Spears, J. & Barki, H. (2010) User Participation in Information Systems Security Risk Management. Management Information Systems Research Center, University of Minnesota. Available from: https://www.jstor.org/stable/25750689 [Accessed 14 March 2022].

Lorber et al., (1987) A theoretical foundation for the PLS algorithm. Journal of Chemometrics. Available from: https://analyticalsciencejournals.onlinelibrary.wiley.com/doi/10.1002/cem.1180010105 [Accessed 16 March 2022].

Spears, J. & Barki, H. (2010) User Participation in Information Systems Security Risk Management. Management Information Systems Research Center, University of Minnesota. Available from: https://www.jstor.org/stable/25750689 [Accessed 16 March 2022].