Seminar 2 Preparation: Estimating Tools and Risk Assessment

Activity 1

*Review the **NIST Privacy tools**. How do these fit with the risk assessment methods and tools described in last week's lecturecast?*

The NIST privacy framework supports an organisation wanting to ensure due diligence with regards to the risks associated with individuals' data, whilst developing systems, products, and services. Therefore, it would be an additional framework used to aid the overall Enterprise Risk Management process covered by the frameworks mentioned in the lecturecast.

Activity 2

Also, read the articles by Verner et al (2014) and Anton & Nucu (2020) and then answer the following questions:

1. *What are the main risks that the authors identify?*

   Verner et al. (2014) show us that at a high level common risks fall into the areas of project management and human resources. Furthermore, the sub-area with the most risks is communication and collaboration. Reading Anton & Nucu's (2020) work one gathers that for a comprehensive risk management strategy an Enterprise Risk Management approach may be required.

2. *Which of the frameworks discussed in the Unit 3 lecturecast would you use to capture and categorise the risks?*

   There are various frameworks that one can choose from, each with their pros and cons. However, if I were forced to select one, I would use the Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) Allegro framework as it is lightweight and highly adaptable (Caralli, 2007). Furthermore, the supporting documentation is much more readily available and easier to use than the other larger frameworks (Caralli, 2007).

3. *Add a risk and a suggested mitigation to the module forum.*

   - One risk may be the failure to find an error in the system design or implementation before it is deployed in production (Lehtinen, 2014).
   - The mitigation would be to perform various levels of testing. In the case of a software development project Test Driven Development (TDD) could be adopted.

References

Anton, G. & Nucu, A. (2020). Enterprise Risk Management: A Literature Review and Agenda for Future Research. *Journal of Risk and Financial Management* 13(11): 281.

Caralli, R., Stevens, J., Young, L., Wilson, W. (2007) *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*. Carnegie Mellon University.

Lehtinen, A., Mäntylä, V., Vanhanen, J., Itkonen, J. & Lassenius, C. (2014) Perceived causes of software project failures – An analysis of their relationships. *Information and Software Technology* 56(6): 623–643

Verner, M., Brereton, P., Kitchenham, A., Turner, M. & Niazi, M. (2014) Risks and risk mitigation in global software development: A tertiary study. *Information and Software Technology* 56(1):54–78.