**Unit 2: Users, Assessment & the Risk Management Process**

**Objectives:**

* Review the Risk Management Process (RMP).
* Review the effects of different assessment types (Qualitative vs. Quantitative).
* Discuss potential changes to the RMP based on changes in user participation.

**Outcomes:**

* Discuss the differences between assessment approaches (Qualitative vs. Quantitative).
* Explain the importance of user participation in the risk management process.
* Discuss the implications of any recommended mitigations.

**Reflection**

It is claimed that at least half of all security breaches in information systems are the consequence of unauthorized system access by personnel already employed by the company (Gordon et. al., 2005). It may be possible to reduce the number of times that employees accidentally compromise information system security by failing to pay enough attention to the potential dangers that may crop up in the course of their normal job activities and responsibilities. Instead, it is generally believed that organizational efforts to manage information security (IS) concentrate on flaws in technological assets such as hardware, software, and networking at the expense of controlling other potential sources of vulnerabilities, such as people, policies, procedures, and culture. This view is supported by the fact that this is the prevalent perception (Halliday et. al., 1996; HU et. al., 2006; Jaher and Creamer et. al.,2005).

The qualitative risk assessment is one way that may be used to analyze risk. It involves categorizing the likely outcomes and probabilities of each risk using descriptive or quantitative rating methods. Alternative measurement approaches are semi-quantitative and quantitative risk assessment (Cranenburgh, et. al., 2019). An essential aspect of qualitative risk analysis is identifying the risks (or opportunities) that exist, their likelihood of materialization, and the potential implications of their occurrence. Usually, the results are presented as a Probability/Impact ranking matrix. This kind of research will also categorize dangers according to their causes or effects. (AS, et. al.,).

In contrast to quantitative risk analysis, which assigns numerical values and use independently verifiable data, qualitative risk analysis operates in a more expansive and "big picture"-oriented environment. In quantitative risk analysis, statistics are used to create a number that quantifies the acceptability of a risk occurrence.

The detailed difference between the qualitative and quantitative risk is shown in the below Table 1.

|  |  |
| --- | --- |
| **Qualitative Risk Analysis** | **Quantitative Risk Analysis** |
| It accounts for each, and every risk identified by the recognized risk method. | It only considers the hazards that have been indicated for additional examination because of qualitative risk analysis. |
| It does not do a quantitative examination of the risk to assess its likelihood and probability. | Conduct quantitative risk analysis using probability distributions to characterize the risk. The probability and repercussions. |
| Here, we assess individual risk by assigning a quantitative value of probability and consequence. This score runs from 0 to 1, with 1 signifying a very dangerous situation. | Using the cumulative effects of risk, it predicts the predicted outcome of the project in terms of cost or duration. |
| Almost all of our projects use the qualitative risk analysis approach we created. | We do not use this strategy for basic or moderately complex tasks, and you are unlikely to encounter it in software development projects. |

References:

Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Richardson, R., 2005. 2005 CSI/FBI computer crime and security survey. *Computer Security Journal*, *21*(3), p.1.

Halliday, S., Badenhorst, K. and Von Solms, R., 1996. A business approach to effective information technology risk analysis and management. *Information Management & Computer Security*.

Hu, Q., Hart, P. and Cooke, D., 2006, January. The role of external influences on organizational information security practices: An institutional perspective. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)* (Vol. 6, pp. 127a-127a). IEEE.

Jahner, S. and Krcmar, H., 2005. Beyond technical aspects of information security: Risk culture as a success factor for IT risk management. *AMCIS 2005 Proceedings*, p.462.

Cranenburgh, N. (2019). *Qualitative Risk Assessment*. [online] REBOK Community. Available at: <https://rebok.engineersaustralia.org.au/resources.html/tools-and-techniques/qualitativeriskassessmentr18/#:~:text=Qualitative%20risk%20assessment%20is%20one>.

AS, S.S.S. (n.d.). *An Introduction to Qualitative Risk Analysis | Safran*. [online] www.safran.com. Available at: https://www.safran.com/content/introduction-qualitative-risk-analysis#:~:text=Qualitative%20risk%20analysis%20involves%20identifying.