Week 1 Assignment

[Author Name]

[Institutional Affiliation(s)]

Week 1 Assignment

Quantitative risk assessment consists of five steps process that includes assigning a monetary value to an asset, input the value of an asset for each value after that producing SLE value that is single loss expectancy-value, determining the ARO (annual rate of occurrence) and ALE (annual loss expectancy). The methods used in the quantitative risk assessments are ALE, Courtney’s and Fisher method and ISRAm model. The basic correlation that is applied for the assessment of IT risk assessment is as follows: R=P x W where P=F x V. here r stands for risk factor, p for probability of number of incidents that cause loss, W= value of the assets lost, F= frequency of threats while V is susceptibility of the system. In the ALE method, the annual loss expectancy can be measured by the formula ALE= SLE\*ARO (Irfandhi, 2016).

Qualitative risk assessment consists of the following phases. The first is selecting a system that is to be evaluated then identifying potential threats on the system, identifying the system's susceptibility, analyzing the applied methods, determining the impact of the applied method on the system and determining risk level with the help of matrix. The matrix consists of the probabilities of the incidence that occurred and the strength of the incident (Laudon & Laudon, 2015).

The vulnerability is defined as the system's weak points or weakness that makes it unsafe and prone to get security problems. The threat is defined as an incident or thing that could potentially damage the system or an asset. It can be due to natural disasters such as floods or intentional threats that include malicious software. The threat agent is an entity responsible for carrying an attack that could damage an asset. Risk can be described as the loss or damaged done when an asset’s vulnerability is exploited by the threat. Exposure and control are the two terms that are connected in a sense of control provide security and technical protection to the system that is exposed to any threat or risk (Munteanu, 2006). The three types of security control that focus on risk management. The security policy is an example of management control. The second type is operational control. These are the controls that are both implemented and executed by people for example steps such as not opening spam emails to protect the system from phishing attacks. The third control is technical control that is executed using hardware and software. For instance, firewalls are used that do not allow any external attacks or malicious data to pass through the wall.

The four ways to manage the risk are as follows:

**Risk mitigation**

It is important to first avoid the risk by safeguarding the system and work on to improve the vulnerabilities of the system to avoid future attacks and threats. Also if the system is damaged then there is a need to find an effective way such as countermeasures to reduce the risk.

**Risk acceptance**

It is important to accept the risk and start analyzing the cost-effective safeguards that are the countermeasure to stop the threat.

**Risk assignment**

The assigning of risk or transferring of risk referred to the placement of the cost of losing a risk that represents another entity. Generally, risks are conferred to insurance companies however during risk assignment some of the risks are still left (Rot, 2008).

**Risk rejection**

Risk rejection can be described as to deny that the potential risk has occurred by considering the risk as invalid. This could be disastrous for any organization as mostly IT assets are vulnerable and to protect the asset it is necessary to acknowledge them.

**References**

Irfandhi, K. (2016). Risk Management in Information Technology Project: An Empirical Study. *ComTech: Computer, Mathematics and Engineering Applications*, *7*(3), 191-199.

Laudon, K. C., & Laudon, J. P. (2015). *Management Information Systems: Managing the Digital Firm Plus MyMISLab with Pearson eText--Access Card Package*. Prentice Hall Press.

Munteanu, A. (2006, June). Information security risk assessment: The qualitative versus quantitative dilemma. In *Managing Information in the Digital Economy: Issues & Solutions-Proceedings of the 6th International Business Information Management Association (IBIMA) Conference* (pp. 227-232).

Rot, A. (2008). IT risk assessment: Quantitative and qualitative approach. *Resource*, *283*, 284.