Inherent Risk Analysis

An identified risk fails to achieve control objective and must be evaluated based on the operational, financial, and regulatory impact and likelihood on objective. Each identified risk is categorized and mapped to an entity in an assessment to evaluate and prioritize risks prior to response creation and control deployment.

For example, a company's power and communication cables carrying data has a potential risk of impairment due to the excavation at the maintenance site or any other illegal dig-ups without formal notice. As a security user, you need to analyze each of the likelihood and impact category based on the external factors (frequency of dig-ups and lack of skill personnel at the excavation site and disruption of vendor's business operations) and internal factors (infrastructure and technical personnel availability in case of emergency execution).