Q.1 What is the difference between hazards and threats? Provide examples.

Ans: A hazard is something that exists with the capacity to cause problems in the future. An earthquake fault under a city, a steeply inclined hillside with erosion patterns above a housing development, or a high voltage power line above a swimming pool are all hazards. They all have the potential to cause problems, but the problem has not manifested itself as an event. Whereas; threat is a communication with a promise to do a subset which is frequently a punishment judged by a human recipient to create fear. We are sometimes threatened by a boss with job loss, threatened with divorce by a spouse. Criminal threats are the violent threats.

Q.2 Define risk and provide classification of risk based on its sources. Provide an example for each risk source.

Ans: Any action or activity that leads to loss of any type can be termed as risk. There are different types of risks that can be faced and needs to overcome. Widely, risks can be classified into for types:

<u>Financial risk</u>: it is the downside risk, meaning the potential for financial loss and uncertainty about its extent.

<u>Compliance or regulatory risk</u>: it is the risk that a change in laws and regulations will materially impact a security, business, sector or market.

<u>Strategic risk</u>: it is the risk that failed business decisions may pose to a company. Strategic risk is often a major factor in determining a company's worth, particularly observable if the company experiences a sharp decline in a short period of time.

<u>Operational risk</u>: Operational risk is the prospect of loss resulting from inadequate or failed procedures, systems or policies. Employee errors. Systems failures. Fraud or other criminal activity. Any event that disrupt business processes

<u>Reputational risk</u>: it is the potential loss to financial capital, social capital and/or market share resulting from damage to a firm's reputation. This is often measured in lost revenue, increased operating, capital or regulatory costs, or destruction of shareholder value.

Q.3 How would you assess the performance of a transportation system of a city?

Ans: Performance Evaluation of Public Transport system is very much essential to understand the effectiveness of the plans in vogue as well as to devise plans for its improvement. Most of the major metropolitan cities of the world are presently witnessing rapid growth in industry, infrastructure, economic activities and population over the past few decades which makes them more attractive to job seekers, causing major increase in personalized modes. As a result, the cities are subjected to increase in traffic congestion resulting in huge delays and environmental pollution. To tackle the huge transportation demand and to provide a sustainable environment there is a need for the provision of better public transportation facilities. To fulfill the high demand for better public transport system, there is a need to establish attractive, safe and highly sophisticated public transport systems. In this regard, it is essential to conduct a thorough evaluation of public transport modes. This paper gives an overview and presents the possible ways to identify and measure the

performance of public transit system. It presents the definition and literature in respect of different measurement models towards the public transit performance assessment coupled with comparative study of different measurement models that can be used for performance evaluation.

Q.4 Define security vulnerabilities of a university campus

Ans: There are two schools of thought on computer security at institutions of higher education. One is that universities are lagging behind companies in their security efforts and need to embrace a more locked-down, corporate approach to security. The other holds that companies are, in fact, coming around to the academic institutions' perspective on security—with employees bringing their own devices to work, and an increasing emphasis on monitoring network activity rather than enforcing security by trying to keep out the outside world.