Assignment for Risk and Disaster Management

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

Hazard is a source of potential harm or a condition, which may result from an external cause (e.g., earthquake, flood, or human agency) or an internal vulnerability, with the potential to initiate a failure mode. It is a situation with a potential to cause loss, that is, a risk source. Depending on the nature of a project and its geographical location, some of the following natural hazards should be included within the scope of risk studies: flooding due to rivers, extreme precipitation and monsoons, coastal waves, dam/levee failure, sea-level rise, tidal, cyclones, drought including bushfires or forest fires, extreme wind, tornado, landslide, mudslide, subsidence and sinkholes, volcano, earthquakes and potential tsunamis, and coastal/shoreline erosion.

For example, the hazard can be uncontrolled fire, water, radioactive material, and strong wind. In order for the hazard to cause harm, it must interact with persons or things in a harmful manner. The magnitude of the hazard is its amount or intensity that could cause harm, such as wind speed, flooding depth, ground acceleration in the case of an earthquake, and quantity of radioactive release. Potential hazards must be identified and considered perhaps using life cycle analyses or some other approach necessary for an orderly and structured enumeration.

The interaction between a person (or a system) and a hazard can be voluntary or involuntary. For example, exposing a marine vessel to a sea environment might lead to its interaction with extreme waves in an uncontrollable manner (i.e., an involuntary manner). The decision of a navigator of the vessel to go through a developing storm system can be viewed as a voluntary act and might be necessary to meet schedule constraints or other constraints, and the potential rewards of delivery of shipment or avoidance of delay charges offer an incentive that warrants such an interaction. Other examples would include individuals who interact with hazards for potential financial rewards, fame, self-fulfillment, and satisfaction, ranging from investments to climbing cliffs.

Threat is the potential intent to cause harm or damage on, with, or through a system by exploiting its vulnerabilities. Threats can be associated with intentional human actions as provided in Table 2.1 that lists examples under several threat types including chemical, biological, radiological, nuclear, explosive, sabotage, and cyber.

Assignment for Risk and Disaster Management
ID#15002

TABLE 2.1
Threat Types and Examples

Selected Threat Type	Example Delivery Mode	Example Weapon/Agent	Example Quantity/Quality
Chemical	Outdoor dispersal	Ricin	Potent
		Mustard gas	Potent
	Crop duster	VX nerve agent	Potent
		Chlorine gas	Potent
	Missile	Any of the above	Potent
	Postal mail	Ricin	Potent
Biological	Outdoor dispersal	Anthrax	Potent
		Severe acute respiratory syndrome (SARS)	Potent
	Postal mail	Anthrax	Potent
	Food buffets	Hepatitis	Potent
		Salmonella	Potent
	Missile	Any of the above	Potent
Radiological	Standard deployment	Dirty bomb	Strong
		Radiological release	Strong
Nuclear	Standard deployment	Improvised nuclear device	In kilotons
		Strategic nuclear weapon	In kilotons
Explosive	Standard deployment	Backpack bomb	In pounds of Trinitrotoluene (TNT)
		Missile	In tons
	Truck	Fertilizer bomb	In pounds
	Boat	Composition C4 explosives	In pounds
	Airplane	Jet fuel	In gallons
Sabotage	Physical	Cut power cable	Not applicable
		Cut bolts	Not applicable
		Improper operation or maintenance	Not applicable
	Cyber	Providing unauthorized access	Disruption of services
Cyber	Physical	Cut control cable	Not applicable
		Magnetic weapons	Power units
	Cyber	Worm virus	Disruption of services

Difference between Hazard and Threat

Sometimes, hazard and threat might be used interchangeably. Consider the example of a flock of birds flying close to an aircraft. This flock is both a hazard and a threat.
However, because the concept of a threat is vaguer than the concept of a hazard, a threat is not always a hazard. Consider the example of:
migrating birds, which are a hazardous source but not an actual hazard, or fatigue, which is a contributing factor.
The takeaway here is that a hazard occurs (is "actualized") when your operations interact with hazard sources. A threat is simply a generic way to describe danger, whether the danger has actualized or not.

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

The concept of risk can be linked to uncertainties associated with events. Within the context of projects, risk is commonly associated with an uncertain event or condition that, if it occurs, has a positive or a negative effect on the objectives of a project. Risk originates from the Latin term risicum, which means the challenge presented by a barrier reef to a sailor. The Oxford Dictionary defines risk as the chance of hazard, bad consequence, loss, and so on, or risk can be defined as the chance of a negative outcome.

Risk should be associated with a system and commonly defined as the potential loss resulting from an uncertain exposure to a hazard or resulting from an uncertain event that exploits the system's vulnerability. Risk should be based on identified risk events or event scenarios.

In 2009, the ISO provided a broadly applicable definition of risk in its standard (ISO 2009a) as the "effect of uncertainty on objectives" in order to cover the following considerations as noted in the standard:

- An effect is a deviation from the expected that can be positive and/or negative effect.
- Objectives can have different aspects, such as financial, health and safety, and environmental goals, and can apply at different levels, such as strategic, organization-wide, project, product, and process.
- Risk is often expressed in terms of a combination of the consequences of an event, including changes in circumstances, and the associated likelihood of occurrence as provided in the commonly used definition.

Classification of Risk based on its sources:

Below are few sources of risk that can be available in a Project. They are:
Schedule: Whether you get the hardware or software out on time, just like planned.

Scope: It is always a risk; whether you have covered all the work required. It will cost you if you have missed any important requirement.

Resource: This is also an aspect that is unpredictable; you can’t expect availability of resources as planned. The planned resources can be used for some other projects as well, in that case you need to get someone new thus creating a problem in both schedule and cost. Sometimes in quality also, in case of inexperience.

Quality: The deliverable can be of poor quality due to some other imposed factors, making it a huge risk.

Cost: Estimation of cost can be a risk in a project; if there is something you have planned to purchase and if it is not available, it can prove costly, as you have to wait for this particular item for a longer period.

Apart from above, sources of risk can be organized into categories such as customer risk, technical (product) risk, and delivery risk. Within each category, specific sources of risk can be identified, and risk reduction techniques can be applied.

Material and equipment risks:

- Required hardware will not be delivered on time.
- Access to the development environment will be restricted.
- Equipment will fail.

Customer risks:

Customer risk is related to the customer's key success factors for the project. A project is not successful if the customer is not successful with the process. It can be sub-divided as follows:

- Customer resources will not be made available as required.
- Customer staff will not reach decisions in a timely manner.
- Deliverables will not be reviewed according to the schedule.
- Knowledgeable customer staff will be replaced with those less qualified.
- Conflict within the customer organization about the desirability or feasibility of the project will threaten it.

Scope risks:

- A lack of clarity in the scope definition will result in numerous scope creep.
- A lack of clarity in the scope definition will result in conflict in the customer about the scope.
- A lack of clearly defined acceptance criteria will cause delays in acceptance and sign-off.

Technological risks:

Technical risk arises from the capability of the technical solution to support the requirements of the customer. It can be categorized as follows as well:

- The technology will have technical or performance limitations that endanger the project.
- Technology components will not be easily integrated.
- The technology is unproved and will fail to meet customer and project requirements.
- The technology is new and poorly understood by the project team and will introduce delays.

Delivery Risks:

Delivery risk is related to the ability of the complete team to deliver against the plan at the cost and schedules estimated, like;

- System response time will not be adequate.
- System capacity requirements will exceed available capacity.
- The system will fail to meet functional requirements.

Unpredictable risks:

- The office will be damaged by fire, flood, or other methods.
- A computer virus will infect the development environment or operational system.

Project management risks:

- The inexperience of the project manager will result in budget or schedule slippages.
- Management will deem this project to have a lower priority for resources and attention.

Resource risks:

- Main staff may not be available.
- Key skill sets will not be available when needed.
- Key staff will be lost during the project.
- Subcontractors or vendors will below-perform and fail to meet the milestones.

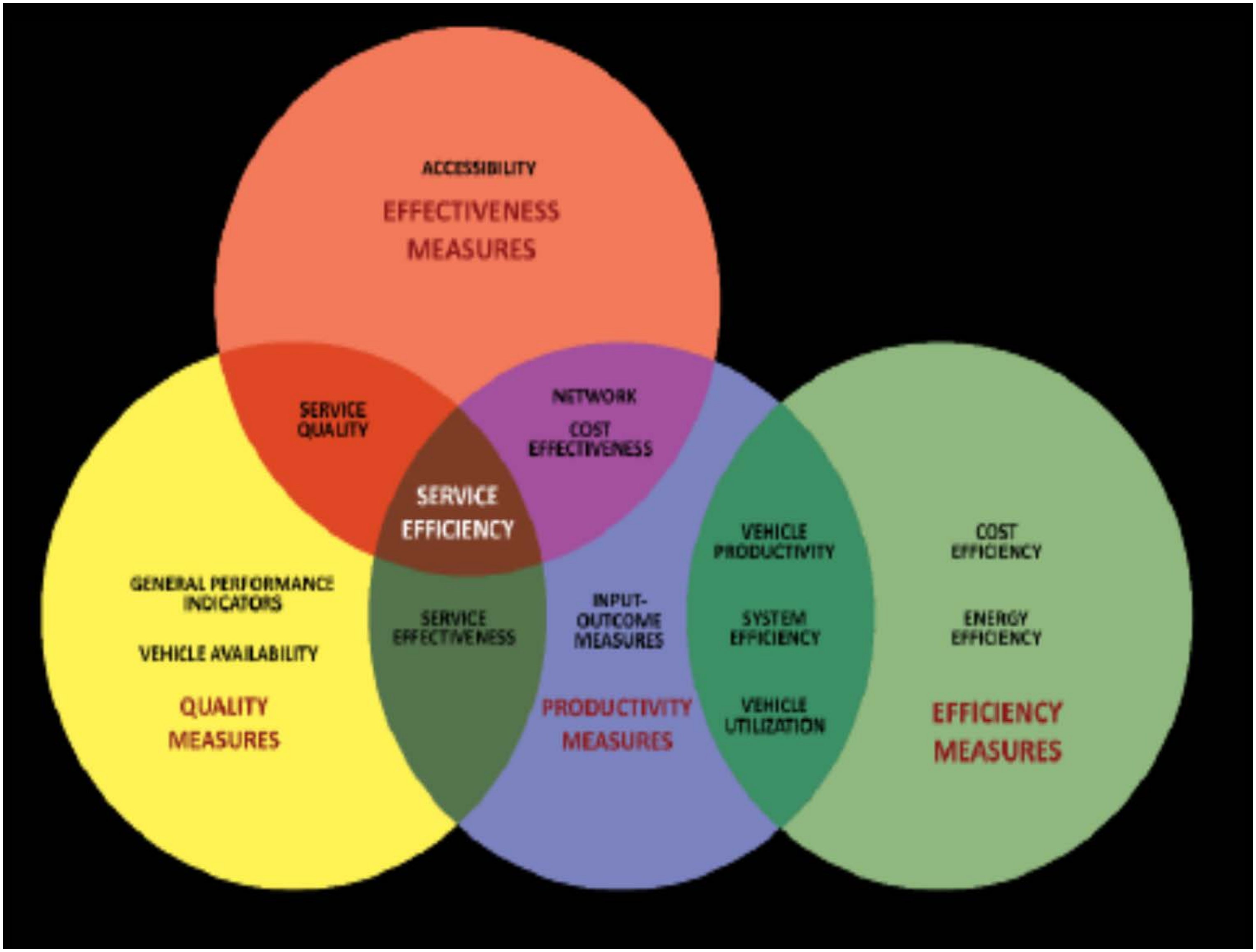
3. How would you assess the performance of a transportation system of a city?

Public transport usually refers to all available transportation modes which are envisioned to serve the public, regardless of the ownership or possession, provides mobility to all users, relieves congestion in the streets, and helps in creating and maintaining livable communities and environments.

Transportation system performance can be defined using the passenger, agency, and community's point-of-view. Passenger's viewpoint reflects the passenger's perception of the service. The agency's view reflects transport performance from the perspective of the transport agency like a business. The community's point-of-view measures transport's role in meeting broad community objectives.

The below table define the performance indicators required for any transportation system in a city. The transportation system can be judged by these indicators.

Assignment for Risk and Disaster Management
ID#15002



Measures of performance evaluation of public transportation

Assignment for Risk and Disaster Management
ID#15002

Category	Description	Indicators
System Efficiency	System efficiency measures the input-output ratio of consumption in the transportation process. It depends on several factors like network, finance factors, labor and utilization efficiency	• Mobility • Productivity • Passenger • Vehicle-km • Quality • Affordability • Infrastructure quality • Availability
Network Efficiency	Network efficiency measures the ability and capacity of the network to support direct services between areas, coverage of the total route, short distance flexibility	• Continuity between roads • Balancing of routes • Spatial coverage of the network • Route Overlapping • Network density • Average bus stop spacing • Service Coverage
Service Efficiency	Service efficiency indicators are used to measure the performance of the service delivered from the passenger's perspective	• Reliability • Availability • Service capacity • Accessibility • Distance • Vehicle availability • Service coverage
Utilization Efficiency	Utilization efficiency measures the rate of resource utilization by the existing system	• Fuel consumption per km • Vehicle capacity utilization • Vehicle utilization and break down • Vehicle per km • Passenger per km
Cost Efficiency	Cost efficiency measures and compares the amount of investment required/gained to/from the service	• Operating cost/vehicle-km • Operating cost/passenger-trip • Revenue/vehicle-km • Revenue/passenger-trip • Total revenue/total operating cost

4. Define security vulnerabilities of a university campus.

Security vulnerability is the inherent state of a security system that can be exploited by an adversary to undermine its effectiveness. Sometimes it seems like the security challenges facing by universities are never-ending. Students and others share user information. Campus visitors pop USB sticks into networked machines. Hackers find their way into an internal network through carelessly discarded information from an open screen or from an infected workstation.

Here are some of the things that keep university security people up at night, and big challenges that universities should address to make themselves more resistant to cyber threats.

Phishing and Social Engineering Attacks

One of the biggest challenges with university cybersecurity is the sheer amount of hacking that goes on in these environments. Universities have to deal with a unique mix of user levels, including students who are often young, and relatively trusting, and are not employees of the organization — so they're less controlled.

For example, research shows a full 90% of malware attacks originate through e-mail. Various types of spoofing and spear-phishing campaigns entice students and others to click on illegitimate links that can usher in a Trojan Horse to do damage to a network system, or compromise the security of information

The IT Crunch: Limited Resources

The challenge of limited resources and funding for university cybersecurity generally speaks for itself. The above kinds of network monitoring and cybersecurity engineering have significant costs attached to them, and many universities simply find it difficult allocate the manpower or the funding to address cybersecurity issues.

System Malware — Zero Day Vulnerabilities and More

Universities and colleges also have to anticipate situations where hackers may exploit existing system vulnerabilities. They have to look at continuing support for operating systems and other technologies.

Protecting Personally Identifiable Information

At the heart of many of these cybersecurity efforts is the daunting struggle to protect all sorts of personally identifiable information, from simple student identifiers to financial data and medical data, from grades to Social Security numbers and items that identity thieves might use. The above-mentioned regulations are part of the drive to secure this type of data, along with more general standards and best practices for enterprise. Simply put, data breaches cost money, both in damage control, and in the reputation of the universities itself.

End-User Awareness and Training

Another way for universities to increase safety is for them to conduct vibrant types of end-user awareness campaigns.

This starts with educating end-users on how malware gets into a system — asking them not to click on suspicious e-mails or use inbound links, but instead to always do online banking and perform other transactions through a secure website.