ASSIGNMENT

NAME: HAMAD ALI

STUDENT REGISTRATION NUMBER (ID): 14270

SUBJECT: Risk and Disaster Management in Construction

Answer 1):

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.

Threat is anything that might exploit a vulnerability. Any potential cause of an incident can be considered a threat. Closely related to hazard. A threat is a hazard, but a hazard need not be a threat.

Types of Hazard:

- Biological.
- Chemical
- Physical.
- Safety.
- Ergonomic.
- Psychosocial.

Type of Thread:

- General
- Specific

A hazard in safety management is a condition that poses danger to your organization, and can lead to an accident, incident, or other mishap if not mitigates.

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.

A hazard is something that can cause harm, e.g. electricity, chemicals, working up a ladder, noise, a keyboard, a bully at work, stress, etc.

Answer 2):

Risk:

Risk is the possibility or chance of loss, danger or injury.

Risk is the possibility of something bad happening. Risk involves uncertainty about the effects/implications of an activity with respect to something that human's value, often focusing on negative, undesirable consequences.

A probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action.

Classification based on geographic distribution:

As soon as someone steps outside his own environment, he meets a new set of risks, which may include situations over which he has no control. Risks involving new culture, customs, materials, methods, different politics and varying rates of exchange fall under this type of classification.

Classification based on the size and complexity of the project

As a construction project increases in size, the risks inherent in its planning, design and execution do not simply multiply in conformity with the increase in size. Instead, new and peculiar risks emerge which need to be identified and taken care of prior to the commencement of design.
The size of projects measured in monetary values has escalated dramatically in recent years.
New names had to be conceived such as Jumbo, Giant and more recently Pharaonic. An example of the last description is the US$18 billion Itaipu Hydroelectric plant located on the
Parana River between Brazil and Paraguay. See page 390 under the heading of 'Adequacy of finance'.

Classification based on legal concepts

In general, the legal concepts accepted in the jurisdiction where the project is constructed produce a certain pattern of risks. Therefore, one may classify risks in accordance with law applicable to that jurisdiction, resulting in four areas of concern: contract; tort; equity or custom (depending on the part of the world being considered); and legislation in the form of statutes.

Classification based on the effect produced by the risk eventuating

As described earlier, the effect produced by a particular risk eventuating can be measured through the severity and the probability of occurrence. A classification may be carried out on the basis of the magnitude of either of these dimensions. There are recognized scales for each of the two dimensions giving a set grading, which starts at zero and ends at a certain value describing the highest anticipated magnitude of that dimension.

The effect, however, can be expressed in terms of monetary loss, property damage, personal injury, or a combination of any or all. The grading for probability of occurrence shown in

Classification based on chronology

Risks may be classified in accordance with the chronological staging of a construction project.

Thus, risks are divided into those occurring during the feasibility stage, followed by the design stage and so on including the stage when the project has been taken over in part or wholly by the owner and used. The classification brings together a spectrum of risks in an extensive matrix. In the following Chapter, the expected risks in a construction project are arranged in a succeeding order beginning with the brief and ending with the actual use of the project, i.e. beginning

Classification in construction contracts

This is the method used in most standard forms of construction contracts where specific risks are allocated to one party and all the other risks are allocated to the other party in the contract.

In general terms, the risks are classified and allocated to the respective parties on the basis of the criteria of control of the risks and their consequences, if and when they eventuate. Some of the consequences are then insured whilst others, although insurable, are not required to be insured. There remains a set of un-insurable risks that cannot be insured because in one way or another they do not conform to the concept and principles of insurance. These uninsurable risks must therefore be allocated to one of the parties in the contract on the basis of the benefit realized from being involved in the project.

Answer 3):

Introduction:

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. Dhaka, one of the fastest-growing megacities of the world with rapid urbanization, requires an efficient urban public transportation system to run the city functions well and to serve the demand of its inhabitants.

Performance Evaluation:

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.

The Asia-Pacific region has witnessed rapid population growth and urbanization. In 2016, half of the world's 4 billion urban dwellers lived in the region, and today 19 of the world's 31 megacities are in the region. According to recent projections, by 2030 urban population in the region will reach 2.7 billion (56 per cent of total population), and by 2050 this number will reach 3.2 billion (63 per cent urban share)

The provision of sustainable urban transport is becoming a major issue due to rapid urbanization worldwide, including in the Asia-Pacific region.

The performance of a transportation system is affected by several factors such as human factors, vehicle factors, acceleration characteristics, braking performance etc. These factors greatly influence the geometric design as well as design of control facilities. Variant nature of the driver, vehicle, and roadway characteristics should be given importance for the smooth, safe, and efficient performance of traffic in the road.

Transportation system in a city performs depends both on public investment and policy, and on millions of decisions made daily by consumer-travelers about whether, where, how and when to travel. Understanding how people make travel choices is key to understanding urban transportation problems and potential solutions.

Travelers aim for value:

Most urban trips do not occur because people enjoy the travel. They occur because people want to enjoy the benefits of being in different places, engaging in different activities and having choices available to get the best value. In that sense, travel is a means to other ends: the real consumer demand is for jobs (the better the transportation, the greater the opportunities and potential economic rewards), shopping (more choices and lower prices), entertainment, recreation, education, social interaction and so on.

Travelers consider the benefits:

The main benefits that travelers consider are safety, speed, reliability, convenience and comfort. Other characteristics can be more important to some travelers than others: for example, environmental sensitivity.

Travelers consider the costs:

The main costs that dominate travelers' decision-making are the ones that affect them directly: out-of-pocket costs for vehicles, fuel, maintenance, parking, tolls and travel time. Some travelers may also give some consideration to costs to society (e.g., the costs of vehicle emissions, which contribute to health hazards and to greenhouse gases)

Performance evaluation of public transport system requires to understand the terms on behalf of performance of the system to be evaluated. The evaluation can be done in two ways based on present perception of users about the service delivered based on the feedback provided by experienced evaluation team. Performance evaluation is defined as the technique to evaluate how well or bad is the performance of a transit service is under the prevailing operating condition. The performance

of transit system can be enumerated based on two distinct dimensions i.e., Service and Service quality. Service is described as “the business transaction that take place between a donor (Service provider) and Receiver Whereas, Service quality gives the measure of how well the service level delivered to the commuter’s as per their expectation.

Performance Evaluation Models:

SERVQUAL Model:

Parasuraman (1985) suggested a model for measuring service quality by measuring the gap between the service delivered and service received. It is mostly used by market researchers to identify customer satisfaction on behalf of service delivered. This model represents the service quality in terms of 10 dimensions namely, Reliability, Responsiveness, Competence, Access, Courtesy, Communication, Credibility, Security, understandability and Tangibles.

Impact Score Technique (IST):

Federal Administration of the U.S (1999) developed a simple and effective measurement method to evaluate customer satisfaction for transit services termed as Impact Score Technique. The IST approach determines the relative impact of attributes on user satisfaction by measuring relative decrease in user satisfaction when there is a problem with the attributes.

Important Performance Analysis (IPA):

IPA was first introduced by Martilla (1977). IPA is also known as quadrant analysis which is used in many areas due to its ease of identification of different quality parameter that can lead to the improvement in Service quality.

Customer Satisfaction Index (CSI)

Customer Satisfaction Index is a method to determine the level of satisfaction that has been achieved with respect to the service delivered. CSI was proposed by Supranto (1997). CSI can be computed by using the average value of the level of expectation and the performance of each service item.

Ordered Logit Model:

The ordered logit models are regression models for ordinal dependent variables and the genesis behind using this model is to understand how well that output can be predicted by the responses to other questions.

Structural Equation Modeling (SEM):

Structural Equation Modeling (SEM) methodology is a powerful multivariate analysis technique in which a set of relationships between observed and unobserved variables are established. It is relatively new method which began in the 1970s (Fornell, 1981), it has been widely applied in various domain of research, including psychology, education, social science, economics, statistics, etc.

Soft Computing Techniques:

At present soft computing techniques are also being used by researchers for performance appraisal of different transit system. Among different soft computing techniques Artificial Neural Network (ANN), Fuzzy logic and Genetic algorithm now a days quite popular.

Answer 4):

Security Vulnerability:

An unintended flaw in software code or a system that leaves it open to the potential for exploitation in the form of unauthorized access or malicious behavior such as viruses, worms, Trojan horses and other forms of malware.

security vulnerabilities can result from software bugs, weak passwords or software that's already been infected by a computer virus or script code injection, and these security vulnerabilities require patches, or fixes, in order to prevent the potential for compromised integrity by hackers or malware.

In cyber security, a vulnerability is a weakness which can be exploited by a cyber-attack to gain unauthorized access to or perform unauthorized actions on a computer system. Vulnerabilities can allow attackers to run code, access a system's memory, install malware, and steal, destroy or modify sensitive data.

To exploit a vulnerability an attacker must be able to connect to the computer system. Vulnerabilities can be exploited by a variety of methods including SQL injection, buffer overflows, cross-site scripting (XSS) and open source exploit kits that look for known vulnerabilities and security weaknesses in web applications.

Security Vulnerability of University:

The large and open networks of Universities are particularly vulnerable because they often have multiple overlapping public and private networks. The staff, faculty members or students with

infected devices might connect with the Universities networks. Many labs also have devices into their networks that were never intended to be there, which opens up new avenues of attack.

Securing large network has been always an issue to IT managers and security analyst. There are large similarities between securing a large network and university network but each one has its own issues and challenges. Pointing fingers at students is an easy option- a large number of suspects transiting inside the network. Current education pays more attention to IT technology to improve their students learning experience. Creating a convenient and secure network system in an educational environment is a challenging task. University tends to have a weak centralize policies. This means that they have tendency toward decentralization. This could be due to the way universities have been operated long time before computer systems was born. In some universities different departments will have it is own IT department, staff and budget ,the central IT group only provide bandwidth and high level services. Having decentralized IT group raises a challenge when it comes to policy making and policy enforcement.

When does a vulnerability of University become an exploitable?

A vulnerability with at least one known, working attack vector is classified as an exploitable vulnerability. The window of vulnerability is the time from when the vulnerability was introduced to when it is patched.

If you have strong security practices, then many vulnerabilities are not exploitable for your organization.

For example, if you have properly configured S3 security then the probability of leaking data is lowered. Check your S3 permissions or someone else will.

Likewise, you can reduce third-party risk and fourth-party risk with third-party risk management and vendor risk management strategies.

What causes vulnerabilities?

There are many causes of vulnerabilities including:

Complexity: Complex systems increase the probability of a flaw, misconfiguration or unintended access.

Familiarity: Common code, software, operating systems and hardware increase the probability that an attacker can find or has information about known vulnerabilities.

Connectivity: The more connected a device is the higher the chance of a vulnerability.

Poor password management: Weak passwords can be broken with brute force and reusing passwords can result in one data breach becoming many.

Operating system flaws: Like any software, operating systems can have flaws. Operating systems that are insecure by default and give all users full access can allow viruses and malware to execute commands.

Internet usage: The Internet is full of spyware and adware that can be installed automatically on computers.

Software bugs: Programmers can accidentally or deliberately leave an exploitable bug in software.

Unchecked user input: If your website or software assume all input is safe it may execute unintended SQL commands.

People: The biggest vulnerability in any organization is the human at the end of the system. Social engineering is the biggest threat to the majority of organizations.

Phishing and Social Engineering Attack

One of the biggest challenges with university cybersecurity is the sheer amount of hacking that goes on in these environments. Schools 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.

The IT Crunch:

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.

Regulatory Burdens:

Another part of this challenging cybersecurity environment is that schools and universities have big compliance burdens under many different types of applicable regulation.

System malware:

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.

There is a reasonable expectation that manufacturers will make adequate security available, but this doesn't absolve the University of having to look for security loopholes and close them. This means evaluating architectures — for example, can hackers get host names, IP addresses and other information from devices like printers?

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 school itself.