Part-B

Question 6: What is software risk? Explain all type of software risk. (1+4)

Ans: Software risk refers to the potential problems or uncertainties that can arise during the development, deployment, and maintenance of software systems.

1. **Requirements Risk:** This type of risk occurs when there are inaccuracies, ambiguities, or incomplete requirements. It can lead to misunderstandings between stakeholders and developers, resulting in software that does not meet the desired functionality or user expectations.
2. **Schedule Risk:** Schedule risk refers to the possibility of project delays or missed deadlines.
3. **Technical Risk:** Technical risks are those that could affect the quality or performance of the software. For example, a technical risk could be a design flaw, a coding error, or a compatibility issue with hardware or software.
4. **Budget Risk:** Budget risk relates to the potential for exceeding the allocated budget for a software project.
5. **Business Risk:** are those that could affect the business case for the software project. For example, a business risk could be a change in the market, a competitor introducing a new product, or a change in government regulations.

Question 7: What is project scheduling? What are the basis principles of project scheduling? (1+4)

Ans: Project scheduling is the process of planning and managing the time, resources, and activities involved in a project.

1. **Define the scope of the project:** This includes identifying all of the tasks that need to be completed in order to deliver the project's final product or service.

2. **Break down the project into smaller tasks:** This makes it easier to estimate the time and resources required for each task, and it also helps to identify any dependencies between tasks.
3. **Estimate the time and resources required for each task**: This can be done by using historical data, expert judgment, or a combination of both.
4. **Identify any dependencies between tasks:** This means identifying which tasks must be completed before other tasks can begin.
5. Create a schedule that shows the order in which tasks will be completed. This schedule should also show the start and end dates for each task.

Question 8: What are the four components of risk? Explain RMMM plans? (1+4)

Ans: The four components of risk;

1. Risk Identification.
2. Risk Assessment.
3. Risk Mitigation.
4. Risk Monitoring and Management.

RMMM Plans:

1. Risk Mitigation: Risk mitigation is the process of reducing the likelihood or impact of a risk. There are a variety of risk mitigation techniques, such as avoidance, prevention, transference, and acceptance.
2. Risk Monitoring: This section focuses on how risks will be monitored and tracked throughout the project. It includes the methods, tools, and frequency of risk assessment and monitoring activities.
3. Risk Management: This section addresses the overall management of risks and encompasses ongoing risk assessment, mitigation, and response activities. It outlines the roles and responsibilities of project team members involved in risk management

Question 9: Define the goal of a system audit? Write down the types of system security you would like to implement in the system? (2+3)

Ans: The goal of a system audit in software engineering is to evaluate the effectiveness of the software development process and the quality of the software products.

1. Improve the cost-benefit ratio of information systems
2. Increase the satisfaction and security of the users of these computerized systems

Types of system security that I implemented in any system;

1. **Access control:** Access control is the process of restricting who has access to a system and what they can do with it. This can be implemented using passwords, user groups, and permissions.
2. **Data encryption:** Data encryption is the process of scrambling data so that it cannot be read without a key. This can be used to protect sensitive data, such as passwords and credit card numbers.
3. **Firewalls:** Firewalls are network security devices that monitor and control incoming and outgoing network traffic based on predetermined security rules.
4. **Patch management:** Patch management is the process of applying security patches to a system to protect it from known vulnerabilities.

Question 10: Follow the appropriate steps for developing an E-R diagram and create on for your university's course registration system. Make sure you indicate whether the relationship you depict is one-to-one, one-to-many, many-to-many, or many-to-one.

Ans:

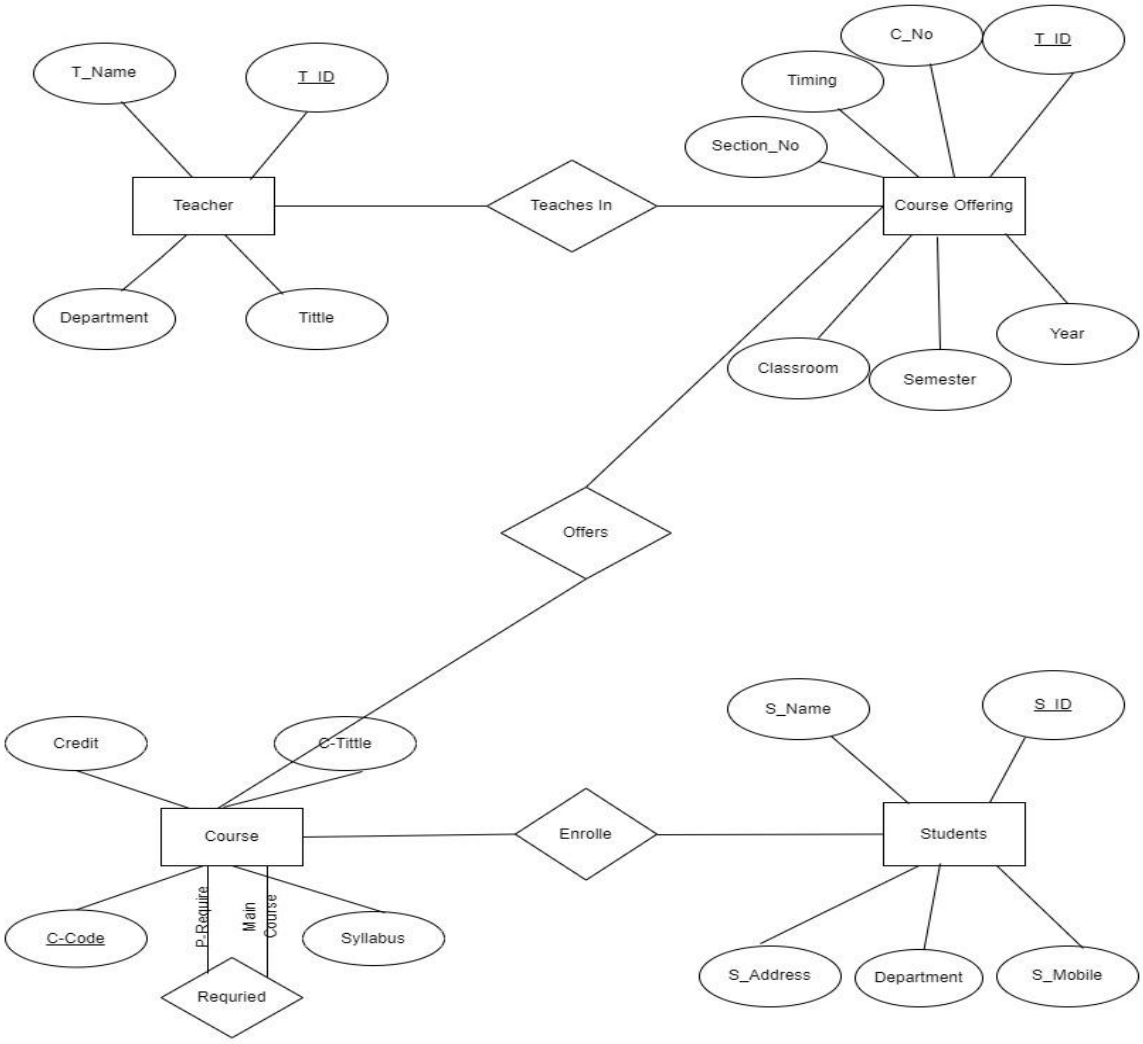

Fig: University Course Registration System