Rodrigo Brasil 11/2023

1. **Consider a bank ATM that allows users to access bank account balances. What measures can the ATM incorporate to cover the principles of the CIA triad?**
   1. The CIA triad stands for Confidentiality, Integrity, and Availability, which are three core principles of information security.
   2. For confidentiality we can use encrypted communication to ensure that all communication between the ATM and the bank's servers is encrypted. This prevents unauthorized access to sensitive information during data transmission.
   3. For integrity we can use transaction logging to keep detailed logs of all transactions. This helps in identifying and tracking any suspicious or unauthorized activities, ensuring the integrity of the transaction history.
   4. For availability we can do regular maintenance. Schedule regular maintenance and updates to prevent system failures due to outdated software or hardware. This ensures that the ATM is consistently available for customer use.
2. **Name three best practices that support the CIA triad.**
   1. **Role-Based Access Control** is a best practice that helps enforce the principle of confidentiality. It ensures that individuals have access only to the resources and information necessary for their roles within an organization.
   2. **Data Encryption** is a fundamental practice for maintaining the confidentiality and integrity of data. It involves converting data into a coded format that can only be deciphered with the appropriate key.
   3. **Regular Data Backups** are crucial for ensuring the availability of information. In the event of data loss, system failures, or security incidents, having up-to-date backups allows for the restoration of data and services.
3. **What are the three stages of the risk management lifecycle? What is each stage’s main goal or objective?**
   1. **Risk Assessment/Identification:** The goal of this stage is to identify and assess potential risks that could affect an organization's objectives, assets, or projects. This involves systematically recognizing and documenting risks that may arise from internal or external sources.
   2. **Risk Mitigation/Analysis:** Once risks have been identified and assessed, the next stage focuses on developing strategies to mitigate or manage these risks. The goal is to reduce the likelihood and impact of identified risks to an acceptable level.
   3. **Risk Monitoring and Review:** The final stage involves continuous monitoring and review of the risk management process. The goal is to ensure that the implemented risk mitigation strategies are effective and that the risk landscape remains under control.