**Assignment:** Identifying and Evaluating Risks & Quantitative vs. Qualitative Risk Assessment

**Scenario:** Imagine you are the IT security officer for a mid-sized financial services company. Your organization handles sensitive customer information, including payment card details, social security numbers, and personal financial data. Your company has recently implemented a new online banking system and several cloud-based services for data storage. However, management has concerns about potential security risks.

**Part 1: Identifying and Evaluating Risks**

* **Risk:** Data Breach through Phishing Attacks Targeting Customers.
  + **Risk Category:** Operational Risk
  + **Risk Description:** Once the customer provides their bank information, they can access customer accounts, steal funds, or compromise additional sensitive data.
  + **Threats:** attackers often use highly convincing messages with branding and wording that imitate legitimate company communications.
  + **Vulnerabilities:** Lack of Customer Awareness
  + **Potential Impact:** This can lead to account takeovers, identity theft, and significant reputational damage to your organization.
  + **Likelihood:** High
* **Risk:** Insider Threats from Employees or Contractors
  + **Risk Category:** Operational Risk
  + **Risk Description:** Potential for harm and loss due to the unauthorized or negligent actions of insiders, which could compromise sensitive data or disrupt operations.
  + **Threats:** The specific action or behavior by an insider (e.g. stealing, leaking, or mishandling data) that exploits vulnerabilities within the organization.
  + **Vulnerabilities:** Lack of employee training
  + **Potential Impact:** exposure of sensitive customer information, leading to financial loss, reputational damage, and loss of customer trust
  + **Likelihood:** Medium
* **Risk:** Malware Infections on Customer Devices
  + **Risk Category:** Technical Risk
  + **Risk Description:** Data loss due to malware infections on customer devices, which can compromise sensitive information and disrupt service usage.
  + **Threats:** The specific types of malwares (e.g., ransomware) that target customer devices to steal credentials, financial data, or disrupt operations.
  + **Vulnerabilities:** outdated security software, unpatched systems, insecure network connections, and risky downloads.
  + **Potential Impact:** financial loss, identity theft, and disruption of customer services.
  + **Likelihood:** High
* **Risk:** Absence of Multi-Factor Authentication (MFA)
  + **Risk Category:** Technical Risk
  + **Risk Description:** Some customer may not finish to set up their MFA or failed to comply the required information for the MFA.
  + **Threats:** Attackers can immediately access their accounts, if customers unknowingly share their login credentials. Since MFA acts as an additional security layer that helps mitigate the damage of stolen credentials by requiring a second form of verification
  + **Vulnerabilities:** Weak password, Single Factor Authentication
  + **Potential Impact:** Data breaches and potential financial losses from fraudulent transactions.
  + **Likelihood:** High
* **Risk:** Data Loss or Corruption
  + **Risk Category:** Operational Risk
  + **Risk Description:** Happens when cloud-stored data is accidentally deleted or becomes corrupted due to system errors or failures.
  + **Threats:** potential for data to be accidentally or maliciously deleted, altered, or rendered inaccessible, resulting from system failures, human errors, or cyber-attacks.
  + **Vulnerabilities:** System Failures, Human error, Inadequate Backup Procedures, Lack of Data Integrity Checks.
  + **Potential Impact:** loss access to critical data, which can disrupt operations, lead to business continuity issues, and result in significant recovery costs.
  + **Likelihood:** High

**Part 2: Quantitative vs. Qualitative Risk Assessment (20 points)**

1. Quantitative Risk Assessment

* **Risk:** Application Vulnerabilities
  + Likelihood: 10 times per year
  + Impact: $100,000 to $2 million, depending on the severity of the vulnerability, the impact on users, and the costs associated with fixing the issues, including potential regulatory fines and legal costs.
  + ALE = $250,000 (SLE) x 10 (ARO) *= 2,500,000*
* **Risk:** Unpatched Software Vulnerabilities
  + Likelihood: 5 times per year
  + Impact: $250,000 to $3 million, depending on the severity of the exploitation, the impact on the app's users, and the costs associated with patching, remediation, and any potential legal or regulatory consequences.
  + ALE = $500,000 (SLE) x 5 (ARO) *= 2,500,000*

1. Qualitative Risk Assessment

* **Risk:** Application Vulnerabilities
  + Likelihood: High. Vulnerabilities such as those found in software code, insecure data storage, or insufficient input validation are frequently discovered in mobile apps, often resulting in multiple incidents per year across the industry.
  + Impact: frequently high, exploited by attackers and can have significant impacts on security, leading to data breaches, financial loss, and reputational damage.
* **Risk:** Application Vulnerabilities
  + Likelihood: Medium to High. Unpatched vulnerabilities are commonly exploited by attackers and can lead to security incidents multiple times per year.
  + Impact: Mid to high since its risk level depends on the nature and severity of the unpatched vulnerabilities. They can be exploited by attackers, leading to security incidents, but the frequency and impact may vary based on the specific context and patch management practices.

1. Compare the Two Approaches
   * In **quantitative approach** one of the main advantages of this is that you can exactly measures how often the risk occur per year and how much exactly is the cost of that risk if ever that happens. You can get the right value by using this numbers, like for example above getting the Annualized Loss Expectancy (ALE), for us to know how much did we lost per year which is the effect of the risk. It will provide numerical data on risk likelihood and impact, allowing for more objective and consistent assessments, which will enable clear prioritization of risks based on their potential financial impact, aiding in decision-making. While the disadvantage of it is that numerical data are dependent so it requires accurate data and statistical models, which may not always be available or reliable. It is also more complex and time consuming compared to qualitative and has limited context since it may not capture qualitative factors like organizational culture or human behavior, which can be critical in risk assessment.
   * In **qualitative approach** the advantage of it compared to quantitative is it provides a broader understanding of risks by considering qualitative factors like organizational culture, human behavior, and situational context. Which means it is easier to implement and adapt, especially in environments with limited data or where data is difficult to quantify. One of the main disadvantages of it is that the risk assessments may be influenced by personal biases and opinions, leading to less objective results. It is harder to prioritize and quantify the impact of risks, since it does not provide specific numerical values. May lead to varying conclusions based on different assessors’ perspectives, reducing consistency and comparability that will give us inconsistent result.