Lab Activity
Risk Assessment Projects

ACTIVITY 01: RISK IDENTIFICATION IN ORION ENTERPRISES' CUSTOMER DATA PROCESSING SYSTEM

Objective:

Identify potential risks associated with the customer data processing system at Orion Enterprises, focusing on security, compliance, and operational efficiency.

Materials Needed:

- Brief on Orion Enterprises and its customer data processing system.
- Template for documenting identified risks.

Step-by-Step Guide:

1. **Understand the Business Process:**
    - Review the provided brief on Orion Enterprises, focusing on how the customer data processing system operates.
    - Note the flow of customer data, from collection through processing to storage.
2. **Identify Potential Risks:**
    - Consider areas where things could go wrong, such as unauthorized access to data, data corruption, system downtime, and non-compliance with data protection laws.
    - Use the template to list identified risks, describing each risk briefly.
3. **Document Each Risk:**
    - For each identified risk, fill out the template with the following details:
        - Risk Description: A brief explanation of the risk.
        - Potential Causes: What might cause this risk to materialize.
        - Potential Impact: The consequences of the risk occurring.
4. **Review and Refine:**
    - Go through your list of identified risks, ensuring each is clearly described and justified based on the business process overview.

Business Process

Orion Enterprises, a technology firm established in 2015, focuses on cloud storage and data analytics, catering to a global market. they prioritize innovative solutions and data security. Their operations include a customer data processing system that collects and analyzes client data for improved services and marketing strategies. However, they face challenges like data security, system reliability, regulatory compliance, and third-party integration complexity.

The goal is to reinforce security, system infrastructure, and integration efficiency while maintaining compliance with data protection laws. The task is identifying risks related to their data processing system, considering security, compliance, and operational efficiency. It involves reviewing their business process, recognizing potential risks, and documenting each with its cause and potential impact.

Potential Risks:

Unauthorized Access to Data

Data Corruption

System Downtime

Non-compliance with Data Protection Laws

Integration complexity

Document Each Risk:

1. ***Unauthorized Access to Data:***

   Risk description: Unauthorized entities or bad actors gaining access to sensitive customer data through illegal means.

   Potential Causes: Weak security measures, weak passwords, phishing attacks, lack of encryption.

   Potential Impact: Data breaches, loss of stakeholder's trust, legal consequences, and financial losses.

2. ***Data Corruption:***

   Risk Description: This simply is the corruption, infection, or loss of stakeholder data during processing or storage.

   Potential Causes: Hardware failure, cyber-attacks, software bugs and malfunctions and system errors.

   Potential Impact: Loss of valuable data, damage to the company's reputation, financial losses, and disruption of service.

3. ***System downtime:***

Risk Description: This can be described as any unplanned downtime to the data processing system.

Potential Causes: Software failures, hardware failures, power outages, natural disasters, and cyber-attacks.

Potential Impact:: Any disruption of service, financial losses, and reputational damage to the company.

4. ***Non-compliance with Data Protection Laws:***

   Risk Description: This is the failure by organizations to comply with necessary laws such as GDPR or CCPA.

   Potential Causes: Inadequate data protection measures, failure to update policies per changes in laws, and the lack of knowledge about relevant industry laws.

   Potential Impact:: Legal penalties, loss of customer trust, and damage to company reputation.

5. ***Integration Complexity:***

   Risk Description: This can be described as any issues arising from the integration of third-party services.

   Potential Causes: Inconsistencies between systems, Lack of technical expertise, third-party system failures

   Potential Impact:: Increased operational cost, disruption of services, and data breaches.