Risk Register Development for E-Commerce Startup

Prepared by: Rameen Mughal
Assigned by: Cybrox – GRC Internship
Date: November 21, 2025

I. Company Overview

The company operates as an E-Commerce startup, managing online sales, customer data, cloud-based operations, and digital payment systems. Maintaining business continuity, data security, and regulatory compliance is critical for the organization.

II. Purpose of the Risk Register

The risk register is used to systematically identify, assess, and manage potential risks across all business operations and IT infrastructure. It provides a structured framework to prioritize risk mitigation efforts and ensure operational resilience.

III. Key Components

1. Asset Identification

Critical assets are identified, including customer data, cloud servers, employee devices, payment gateways, and company reputation.

2. Threat and Vulnerability Assessment

Potential threats (such as data breaches, phishing attacks, or DDoS attacks) and vulnerabilities that could expose assets are evaluated.

3. Inherent Risk

The raw risk (likelihood × impact) is assessed before applying any controls.

4. Existing Controls and Control Effectiveness

Current measures in place to mitigate risks are documented, and their effectiveness is rated as High, Medium, or Low.

5. Residual Risk

The remaining risk after considering existing controls is determined to highlight areas that need further mitigation.

6. Proposed Controls

Additional mitigation measures are recommended to further reduce residual risk.

7. Ownership and Review

Each risk is assigned an owner, and review intervals are specified to ensure continuous monitoring.

IV. Attached Documents

An **Excel sheet** containing the full risk register is attached for reference. This document serves as a practical tool for the company to identify risks, implement controls, and monitor risk mitigation over time.