Cybersecurity Risk Assessment & Treatment Plan for E-Commerce Company

I was engaged as a cybersecurity consultant for a mid-sized e-commerce company that handled a significant volume of customer transactions and stored sensitive financial data. The organization sought to strengthen its security posture by addressing risks to the confidentiality, integrity, and availability of its information assets.

1. Conducted a Risk Assessment Using ISO 27001 Guidelines

Objective: Identify risks to information assets affecting confidentiality, integrity, and availability (CIA).

Approach:

- **Establish the context**: Understand the organization's structure, processes, data flow, IT systems, and regulatory requirements.
- **Define the scope**: Limit assessment to systems handling sensitive customer and financial data.
- **Asset identification**: Inventory of information assets—databases, web servers, payment systems, etc.

2. Identified and Document ed Threats, Vulnerabilities, and Impacts

Examples of threats and vulnerabilities:

Asset	Threat	Vulnerability	Impact
Payment system	Malware	Outdated antivirus	Financial fraud, data breach
Web server	DDos attack	Lack of WAF	Website downtime
Customer DB	Insider threat	Excessive user permissions	Data leak, regulatory fines

3. Assessed the Likelihood and Impact of Each Risk

Risk Matrix (qualitative or quantitative method):

Risk	Likehood (L)	Impact (I)	Risk level (L x I)
Data breach via phishing	High	High	High
DDoS attack	Medium	Medium	Medium
SQL injection	Medium	High	High

4. Developed a Risk Treatment Plan

Treatment options:

- **Avoidance**: Stop risky activity (e.g., discontinue insecure 3rd-party integrations).
- **Mitigation**: Apply controls to reduce risk (e.g., patch management, MFA)
- **Transfer**: Cyber insurance or outsourcing to secure cloud services.
- **Acceptance**: For low-priority risks with minimal impact.

Sample entry from plan:

Risk	Treatment	Responsible	Deadline
Data breach	Implement email filtering, staff training	IT security lead	Q2 2025

5. Prioritized and Recommended Security Controls

Based on ISO 27001 Annex A controls (2022 revision):

Control Area	Recommended Control	Rationale
A.5 Policies	Information Security Policy	Aligns staff behaviour with security practices
A.9 Access Control	Role-Based Access Control (RBAC)	Minimize insider threats
A.12 Operations Security	Patch Management Program	Reduce vulnerability to know exploits
A.18 Compliance	Regular audits & monitoring	Ensure regulatory adherence (PCI DSS,

		GDPR)