**TASK 2: project Charter**

**Project Purpose/Justification:**

With increasing threats to online platforms, cybersecurity is crucial for maintaining trust, protecting data, and ensuring business continuity. This project focuses on conducting a comprehensive cybersecurity risk assessment and implementing mitigation strategies for a modern e-commerce platform to prevent data breaches, fraud, and downtime.

**Objectives:**

* Identify and assess key cybersecurity risks on the e-commerce platform.
* Design and implement mitigation strategies using industry best practices.
* Ensure compliance with legal, regulatory, and security standards (e.g., ISO 27001, GDPR).
* Enhance system resilience, user data protection, and operational security.

**Scope:**

In Scope:

* Cyber risk identification (internal & external threats)
* Vulnerability assessment
* Implementation of security controls (firewalls, encryption, access control)
* Policy development
* Staff awareness training
* Monitoring tools setup

Out of Scope:

* Physical security infrastructure
* Third-party vendor risk management outside platform
* Post-deployment maintenance

**Key Stakeholders:**

|  |  |
| --- | --- |
| Role | Name / Group |
| Project Sponsor | E-Commerce Platform Owner |
| Project Manager | [Your Name] |
| Cybersecurity Team | Internal IT Security Team |
| External Consultant | (if applicable) |
| Customers | E-Commerce Users |
| Regulatory Bodies | PCI DSS, GDPR Authorities |

**Deliverables:**

* Risk Assessment Report
* Mitigation Plan
* Implementation of Security Controls
* Incident Response Plan
* Final Project Report

**Milestones:**

|  |  |
| --- | --- |
| Milestone | Target Date |
| Project Initiation | [Date] |
| Risk Assessment Completed | [Date] |
| Mitigation Strategy Finalized | [Date] |
| Security Controls Implemented | [Date] |
| Project Closure | [Date] |

**Risks and Constraints:**

Risks:

* Budget limitations
* Unexpected technical vulnerabilities
* Limited time for testing
* Lack of security training for staff

Constraints:

* Strict deadline
* Limited access to some system components
* Compliance requirements