**Project Charter: Cybersecurity Risk Assessment and Mitigation Strategy Implementation for an E-Commerce Platform**

**Background**

**Because cyber-attacks on e-commerce platforms are increasing rapidly, it is increasingly important to act on cybersecurity. E-commerce businesses have access to personal information, credit card numbers and previous purchases, so attackers are interested in them. Lately, numerous security failures in retail have revealed that insufficient controls can destroy consumer trust, face legal penalties and result in losses.**

**This project started to assess the cybersecurity risks facing the e-commerce infrastructure and come up with a clear strategy to address them. Thanks to this plan, the platform would be more protected from cyberattacks, in accordance with regulations like PCI DSS and GDPR and adopt a culture that prioritizes security.**

**Goals**

**1. Make sure all IT equipment, ways of communicating and places where data is kept are included in your cybersecurity audit.**

**2. Rely on industry-accepted metrics such as CVSS, to spot out the most dangerous and common vulnerabilities and threats.**

**3. Design, implement and document actions that will address the unacceptable and high risks identified.**

**4. Install live monitoring systems, SIEM tools and set up a specific way of responding to cyber threats.**

**5. Adjust your platform’s security architecture to follow well-known standards like ISO 27001, the NIST Cybersecurity Framework and OWASP’s list of the top 10 risks.**

**Scope**

**In Scope:**

* **Making a list and sorting of digital assets such as web servers, APIs and databases**
* **Designing threat models and scenario of risks**
* **The execution of system audits by running Nessus, OpenVAS and Burp Suite**
* **The front-end and back-end systems require penetration testing.**
* **Firewalls, IDS/IPS, multi-factor authentication (MFA) and encryption are all secure methods that organizations can use.**
* **Automating log gathering and analysis with help of SIEM platforms such as Splunk and Wazuh**
* **Tracking code versions with GitHub and using Jira for handling all team tasks**

**Out of Scope:**

**• either fully changing the IT setup or switching to a different cloud supplier**

**• Always check outside vendors and third-parties that integrate with the primary application**

**• Carrying out legal analysis or forensic work after simply reporting the incident**

**Key Stakeholders**

**Client: SecureCart Pty Ltd  
Sponsor: Priyanshi Patel, Chief Information Officer (CIO), SecureCart Pty Ltd  
Project Manager: Aayush Patel  
Project Team Members: Aayush Patel, Samriti Jaswal, Hasti Zalavadiya,**

**Project Milestones**

* **Beginning the Project and Requirement Gathering: On 29 May 2025**
* **On 5 June 2025, we completed the Asset Discovery and Risk Identification Phase.**
* **Vulnerability Assessment and Testing will be completed on 12 June 2025.**
* **19 June 2025 is the date for designing and setting up the mitigation strategy.**
* **From 24 June 2025, security tools were installed and real-time monitoring was set up.**
* **System validation, documenting and review will be completed on 28 June 2025**
* **Group presentation and final report are due by 3 July 2025.**

**Project Budget**

**Non-Recurring Costs:**

* **Burp Suite Pro and Nessus Licenses: $1,200**
* **This service covers Consultant Fees for Understanding Risks and Mapping to ISO/NIST at $2,000**
* **A yearly budget for cybersecurity toolkits includes threat intelligence feeds and SIEM tools for $1,500.**

**Monthly Recurring Costs:**

* **You will additionally need access to Cloud Security Monitoring and Alert Services for $300.**
* **Services for Encrypting Your Backup and Archived Data: $200**

**Constraints, Assumptions, Risks and Dependencies**

**Constraints:**

* **Testing is not done on production systems, as there might be important business results.**
* **Because of strict submission dates, the time available for the project is set**
* **The number of resources might change each semester because of my efforts in other college courses.**

**Assumptions:**

* **Members will quickly be able to get access to test systems, relevant records and required accounts**
* **The team will work following the timeline and make sure their quality is as planned.**
* **At least one review session will be available with people outside the organization**

**Risks and Dependencies:**

* **A possible hold-up due to incorrect systems or missing testing permission**
* **The need for the availability of security software and for network access**
* **When the documentation from the client is inaccurate or missing important details, vulnerability analysis suffers**
* **A security issue during assessment or scanning may result in service interruptions and unhappy customers**

**Approval Signatures**

**Priyanshi Patel, Project Client**

**Priyanshi Patel, Project Sponsor**

**Aayush Patel, Project Manager**