Compliance Gap Assessment for MegaMart: E-Commerce & Logistics

Prepared by: Rameen Mughal
Date: November 22, 2025

I. Company Overview

MegaMart is a mid-sized eCommerce company that sells consumer products through its online marketplace. The platform supports customer browsing, order placement, payment processing, seller onboarding, and digital product uploads. MegaMart also relies on several third-party service providers for SMS OTP delivery, CDN protection, cloud hosting, and marketing operations.

The business handles a significant amount of customer personal data, payment information (PCI), and seller-uploaded content. As the company scales, security, privacy compliance, and operational resilience have become critical to protect customer trust and ensure uninterrupted business operations.

II. Purpose of Gap Assessment

The purpose of this Gap Assessment is to:

- Identify security weaknesses in MegaMart’s current processes, systems, and controls.
- Compare the current state against industry best practices and compliance requirements.
- Highlight risks that could impact customer data, system availability, or regulatory compliance.
- Assign ownership for remediation actions and recommend timelines.
- Provide a clear roadmap for improving MegaMart’s security posture.

The assessment focuses on high-risk areas relevant to MegaMart’s operations, including server security, device patching, file upload security, payment data handling, backup practices, vendor management, and data retention processes.

III. Short Evidence Request List

To verify the current state of MegaMart and support the findings in the gap assessment, the following evidence was collected or requested:

1. **Device & Server Security**
   - Device inventory and OS version report
   - Patch management logs
   - Vulnerability scan reports
   - Server OS version (Ubuntu 18.04) and hardening configuration
   - Firewall configuration screenshots

2. **Application & Web Security**

- Cloudflare/WAF configuration
- Bot protection settings
- File upload logs and antivirus reports
- Web application logging configuration

3. **Data Protection & Privacy**
   - Data retention reports
   - Customer data storage logs from the data lake
   - Access control logs (for payment data)
   - Trello board exports showing exposed customer info

4. **Vendor & Third-Party Security**
   - SMS OTP vendor contract / SLA documents
   - Any existing data processing agreements

5. **Backup & Continuity**
   - AWS backup configuration
   - IAM roles for backup access
   - Disaster Recovery (DR) or backup test records

IV. Attached Documents

The following documents are attached to support this report:

- **Gap Assessment Excel Sheet**: Contains the full MegaMart Gap Assessment table, including current state, best practices, identified gaps, risk levels, and recommended actions.
- **Evidence Request List**: Current document containing a concise list of required evidence (e.g., policies, configurations, logs, system reports) used to validate the current state of MegaMart's security controls.

These attachments provide detailed references and supporting information for all findings discussed in this document.

V. References

[1] OWASP, "File Upload - OWASP Cheat Sheet Series," *cheatsheetseries.owasp.org*, 2024. https://cheatsheetseries.owasp.org/cheatsheets/File_Upload_Cheat_Sheet.html

[2] OWASP, "OWASP Top 10: 2021," *OWASP*, 2021. https://owasp.org/Top10/

[3] GDPR, "General Data Protection Regulation (GDPR)," *GDPR*, 2018. https://gdpr-info.eu/

[4] National Institute of Standards and Technology (NIST), “Security and Privacy Controls for Information Systems and Organizations,” *NIST Special Publication 800-53 Revision 5*, Gaithersburg, MD, USA, 2020.

[5] Center for Internet Security (CIS), **“**CIS Critical Security Controls Version 8,” *CIS*, East Greenbush, NY, USA, 2021.