Project of Mohammad Aminul Islam

Name: Mohammad Aminul Islam
Project Title: Security Audit & Risk Management for Loreal Corner

Professional Summary:

My name is Mohammad Aminul Islam. I am skilled in programming, problem solving, and analytical thinking. I am committed to protecting organizations from cyber threats, particularly in cloud and **web security**. I am dedicated to ensuring the confidentiality, integrity, and availability of data and systems. My goal is to utilize my skills and knowledge to **help organizations strengthen their security posture** and protect sensitive information from evolving threats.

Objective:

Conducted a security audit for Loreal Corner, identifying critical vulnerabilities in asset management, data encryption, and regulatory compliance (PCI DSS, GDPR, SOC). Recommended improvements in access controls, disaster recovery, encryption, and intrusion detection systems to mitigate risks. The audit highlights my ability to assess security gaps and provide actionable solutions to enhance business security and ensure compliance.

Project Overview: Loreal Corner Security Audit

Scope and Goals of the Audit

Scope:
The audit covers the comprehensive security landscape of Loreal Corner,

encompassing assets such as employee equipment, internal networks, systems, and the management of critical business data. The focus is on evaluating their existing security controls, compliance practices, and protecting key business components like e-commerce and internal communication systems.

Goals:

- Assess the current security status and assets of Loreal Corner.
- Complete the controls and compliance checklist.
- Identify areas for improvement in data security, asset management, and regulatory compliance.
- Provide actionable steps for achieving compliance with standards such as PCI DSS, GDPR, and SOC, thereby minimizing the risk of data breaches and other security threats.

Key Findings and Risk Assessment

Assets Managed by IT:

- **On-premises Equipment:** Hardware used for office operations.
- **Employee Equipment:** Devices like desktops, laptops, smartphones, and accessories.
- **Storefront Products:** Inventory stored onsite and available for sale online.
- **Management of Systems:** Accounting, telecommunication, database, security, e-commerce, and inventory systems.
- **Data Retention:** Methods and protocols for data storage and retention.

- **Legacy Systems:** End-of-life systems requiring ongoing monitoring.

Risk Assessment:

- **Risk Score:** 8/10 (High Risk due to inadequate security controls and non-compliance practices).

Primary Risks Identified:

- Lack of proper asset management and access controls.
- Absence of encryption for sensitive customer data.
- No disaster recovery plans or backup systems in place.
- Non-compliance with industry standards like PCI DSS, GDPR, and SOC.

Control Categories and Types

Control Categories:

- **Administrative/Managerial Controls:** Policies and procedures for data management and employee responsibilities.
- **Technical Controls:** Firewalls, IDS/IPS, antivirus, encryption, and backup solutions.
- **Physical Controls:** Surveillance cameras, locks, and fire detection systems.

Control Types:

- **Preventative:** Controls designed to prevent security incidents.
- **Corrective:** Controls to restore data or assets after an incident.
- **Detective:** Controls to detect anomalies or attacks in progress.
- **Deterrent:** Controls aimed at discouraging potential threats before they occur.

Audit Findings – Controls Assessment

Control	Implemented	Needs Improvement
Least Privilege	No	Yes
Disaster Recovery Plans	No	Yes
Password Policies	No	Yes
Separation of Duties	No	Yes
Firewall	Yes	No
IDS/IPS	No	Yes
Backups	No	Yes
Antivirus Software	Yes	No
Legacy Systems Maintenance	No	Yes

Encryption	No	Yes
Password Management System	No	Yes
Physical Locks & CCTV	Yes	No
Fire Detection and Prevention	Yes	No

Compliance Checklists

PCI DSS Compliance:

- Lack of encryption for customer payment data.
- No segregation of duties; all employees have access to sensitive financial information.
- Inadequate password management policies.

GDPR Compliance:

- No encryption of personal data.
- Absence of regular data classification and inventory practices.
- Need for robust privacy policies and procedures.

SOC Compliance:

- Insufficient user access policies (all employees have access to critical data).
- No encryption for sensitive PII/SPII.
- Insufficient data integrity protocols.

<u>Recommendations to Improve Security Posture</u>

1. **Implement Access Controls:**
    - Restrict access to sensitive data using Least Privilege policies.
    - Define and enforce Separation of Duties to mitigate insider risks.
2. **Data Encryption:**
    - Implement encryption protocols for both at-rest and in-transit data, especially for customer payment and personal information.
3. **Disaster Recovery and Backup Plans:**
    - Establish and regularly test disaster recovery and backup systems to ensure business continuity in case of a breach or data loss.
4. **Intrusion Detection and Prevention Systems (IDS/IPS):**
    - Deploy an IDS/IPS system to detect and prevent anomalous activities on the network.
5. **Regular Legacy Systems Monitoring:**
    - Set up a regular schedule for maintaining and updating legacy systems to minimize vulnerability risks.

6. **Compliance with Regulatory Standards:**

   - Ensure full compliance with PCI DSS, GDPR, and SOC standards by implementing required security measures and policies.

7. **Password Management System:**

   - Implement a centralized password management system to enforce secure password practices.

Conclusion:

The audit revealed several critical security gaps within Loreal Corner's existing operations, including inadequate access management, a lack of encryption, and insufficient disaster recovery planning. By implementing the recommended controls, Loreal Corner can significantly reduce its security risks and enhance its compliance with essential industry standards.