TOPCERTIFIER

Governance, Risk & Compliance Consultants

PCI DSS GAP ANALYSIS TEMPLATE

INTRODUCTION:

TopCertifier presents a Simplified PCI DSS Gap Analysis Checklist to help you identify areas where your organization may need improvements to comply with PCI DSS (Payment Card Industry Data Security Standard) requirements. This checklist offers a fundamental framework for evaluating your alignment with PCI DSS and serves as an initial step in assessing your compliance.

SECTION 1: DATA SECURITY

- ☐ Is payment card data properly encrypted during transmission and storage?
- ☐ Are sensitive authentication data, such as CVV numbers, not stored post-authorization?
- ☐ Is there a policy for securing cardholder data and sensitive authentication data?

SECTION 2: NETWORK AND FIREWALL SECURITY

- ☐ Are network configurations and firewall rules regularly reviewed and updated?
- ☐ Is there a network diagram illustrating the flow of cardholder data?
- ☐ Are security policies and procedures in place for securing network infrastructure?

SECTION 3: ACCESS CONTROL

- ☐ Are user access privileges restricted based on business need-to-know?
- ☐ Is multi-factor authentication implemented for remote access to the network?
- ☐ Are user accounts promptly deactivated upon termination or role changes?

SECTION 4: VULNERABILITY MANAGEMENT

- ☐ Are security patches applied promptly to address vulnerabilities?
- ☐ Is there a process for vulnerability scanning and penetration testing?
- ☐ Are critical security patches reviewed and prioritized based on risk??

SECTION 5: SECURITY POLICIES AND PROCEDURES

- ☐ Are comprehensive security policies and procedures documented and disseminated?
- ☐ Is there a security awareness training program for employees?
- ☐ Are security policies reviewed and updated as needed?

SECTION 6: MONITORING AND LOGGING

- ☐ Are security events and logs regularly reviewed and monitored?
- ☐ Is there a process for conducting real-time alerting for suspicious activities?
- ☐ Are incident response and reporting procedures established?

SECTION 7: INCIDENT RESPONSE

- ☐ Is there an incident response plan outlining steps for addressing security incidents?
- ☐ Are employees trained on how to recognize and report security incidents?
- ☐ Is there a documented process for post-incident analysis and improvement?

SECTION 8: PHYSICAL SECURITY

- ☐ Are physical access controls in place to prevent unauthorized access to cardholder data?
- ☐ Is access to secure areas restricted and monitored?
- ☐ Are video surveillance and visitor logs maintained for sensitive areas?

SECTION 9: THIRD-PARTY SERVICE PROVIDERS

- ☐ Are third-party vendors assessed for PCI DSS compliance?
- ☐ Are written agreements with service providers in place to ensure cardholder data protection?
- ☐ Is there a process for monitoring and evaluating third-party security practices?

Please note that this checklist provides a high-level overview, and it's essential to perform a thorough analysis specific to your organization's processes and context. Additionally, it's recommended to engage with PCI DSS experts or consultants to conduct a comprehensive gap analysis for your organization.