(858) 999-3030 • www.rsisecurity.com • info@rsisecurity.com

PCI DSS 4.0 Compliance Checklist

Streamline your PCI DSS 4.0 Compliance

Scope Review

- Review and confirm scope every 12 months (Service Providers: Every 6 months)
- Review and confirm scope upon significant changes

Network and Data Security

- Review network security configurations (NSCs) every 6 months
- Review stored data retention and disposal every 3 months
- Test, detect, and identify unauthorized wireless access points every 3 months
- Perform internal and external vulnerability scans at least every 3 months.
- Perform internal and external penetration testing at least annually.

Cryptography and Software Development

- Document and review cryptographic cipher suites at least once every 12 months
- Provide secure software development training to the development team every 12 months
- Apply high and critical security patches within 1 month of release

User Account and Security Policy

- Perform user accounts review every 6 months
- Review and update information security policy at least annually.
- Review critical software and hardware at least annually.
- For all requirements to be performed periodically, perform targeted risk analysis (TRA) or review the TRA that was performed previously, at least annually.
- For each requirement met using a customized approach, perform targeted risk analysis (TRA) at least annually.

Service Providers

- Perform quarterly reviews of the security and compliance tasks per the security policies and procedures.

(858) 999-3030 • www.rsisecurity.com • info@rsisecurity.com

PCI DSS 4.0 Compliance Checklist

☑ **Streamline your PCI DSS 4.0 Compliance**

☐

Security Awareness and Incident Response

- Review security awareness programs at least annually.
- Monitor and review the compliance status of TPSPs at least annually.
- Review and update the incident response plan at least annually.
- Perform incident response plan testing at least annually.
- Provide incident response training at least annually.

☐

Management

- Formally assign information security to a security officer or other security-knowledgeable executive management team member.