

PCI SSF

Compliance Checklist



1. Define Your Assessment Scope

☐ List all in-scope payment software products and version numbers.

☐ Determine applicable standards:

- PCI SSS – Individual payment software validation.
- PCI SLC – Vendor-wide software development lifecycle validation (if applicable).

☐ Clarify software purpose: payment acceptance, facilitation, or other PCI-defined uses

☐ Identify the applicable modules under PCI SSS:

- Account Data Protection
- Terminal Software Requirements
- Web Software Requirements

- ☐ Document platforms, third-party components, and deployment environments
- ☒ Select a PCI SSC-qualified Secure Software Assessor (e.g., VISTA InfoSec)

2. Strengthen Organizational Security

- ☐ Maintain approved, documented security policies shared with all teams
- ☐ Clearly define roles for software development, security, and support
- ☐ Train developers in secure coding practices (initial + annual updates)
- ☐ Track and manage open-source/third-party component risks.
- ☐ Monitor security threats continuously (e.g., CVEs, vendor advisories)

3. Design Software with Security Built-In

- ☐ Maintain approved, documented security policies shared with all teams
- ☐ Clearly define roles for software development, security, and support
- ☐ Train developers in secure coding practices (initial + annual updates)
- ☐ Track and manage open-source/third-party component risks.
- ☐ Monitor security threats continuously (e.g., CVEs, vendor advisories)

4. Develop Software Securely

- ☐ Follow secure coding standards (e.g., OWASP Top 10, CWE Top 25)
- ☐ Perform static and dynamic testing before software release
- ☐ Eliminate hard-coded secrets (e.g., passwords, test keys).
- ☐ Use validated cryptographic libraries (PCI-approved or FIPS 140-2).
- ☐ Enforce strong key management and secure cryptographic protocols (TLS 1.2+, SHA-256+).

5. Test Software for Security and Functionality

- ☐ Prepare and document security and functional test plans.
- ☐ Conduct independent peer code reviews.
- ☐ Perform penetration testing (network + application layers).
- ☐ Run vulnerability scans and validate all findings.
- ☐ Address and re-test all critical/high-severity issues before release.



VISTA INFOSEC®
TRUSTED ADVISORS, ASSURED COMPLIANCE™

6. Release Software Securely

- ☐ Apply code signing and integrity checks (e.g., digital signatures).
- ☐ Distribute software over secure channels (HTTPS, authenticated downloads).
- ☐ Provide version control, changelogs, and patch tracking
- ☐ Include secure configuration guides with every release.
- ☐ Offer timely vulnerability patches (with defined SLAs).

7. Maintain a Secure Software Lifecycle (PCI SLC Only)

- ☐ Enforce secure practices across SDLC: design development release
- ☐ Manage change with security risk assessments
- ☐ Implement an incident response and disclosure process.
- ☐ Monitor third-party risks (e.g., supply chain vulnerabilities).
- ☐ Schedule regular security reviews and control updates.
- ☐ Plan for secure EOL and decommissioning.

8. Prepare Your Documentation & Evidence

- ☐ Gather supporting evidence: policies, test reports, threat models, etc
- ☐ Map internal controls to PCI SSF requirements
- ☐ Perform an internal gap assessment before validation.
- ☐ Retain logs and test results for at least 12 months.
- ☐ Schedule a pre-assessment review with your assessor (e.g., VISTA InfoSec).

Have any questions regarding PCI SSF compliance?

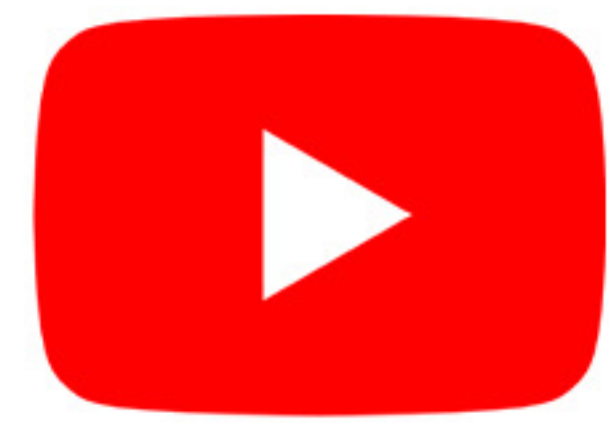
**Schedule a free consultation with our certified
PCI SSF compliance assessor today!**

Contact Us

Visit Us: <https://vistainfosec.com/>



<https://www.linkedin.com/company/vistainfosec/>



www.youtube.com/@Vistainfosecofficial



twitter.com/vistainfosec



facebook.com/vistainfosec

Contact Us: [sales\(at\)vistainfosec.com](mailto:sales(at)vistainfosec.com)

USA: +1-415-513-5261 Singapore: +65-3129-0397

India: +91 998724469 UK: +442081333131