TARA INNOVA

PCI DSS Mapping Guide

How TARA INNOVA Maps to Payment Card Industry Data Security Standard v4.0

What Is PCI DSS

PCI DSS v4.0 is the global security standard for organizations that handle payment card data. It applies to merchants, processors, acquirers, issuers, and service providers. Version 4.0 (effective March 2025) introduces a customized approach alongside the traditional defined approach, with greater emphasis on continuous security and evidence of control effectiveness.

Key Requirements and TARA INNOVA Coverage

PCI DSS v4.0 Requirement	TARA INNOVA Coverage
Req. 1 — Install and maintain network security controls	Quicksand provides L4/L7 traffic inspection at network boundaries. Geo-enforcement, rate limiting, and IP reputation filtering. Policy-based access control per endpoint.
Req. 2 — Apply secure configurations	Quicksand Admin manages all security configurations with version history. Every change audited with user attribution and timestamp.
Req. 5 — Protect from malicious software	Quicksand blocks exploit attempts, injection patterns, and malicious payloads at the edge before they reach application servers.
Req. 6 — Develop and maintain secure systems	Quicksand protects web applications from OWASP Top 10 attacks. URL pattern detection, path traversal prevention, input validation at the edge.
Req. 7 — Restrict access by business need-to-know	Role-based access across the platform. Quicksand enforces per-tenant isolation. CRP documents access control evidence.
Req. 8 — Identify users and authenticate access	Quicksand enforces session integrity with device trust verification, PoW challenges, and configurable session policies. MFA support.
Req. 10 — Log and monitor all access	Immutable audit logs of all enforcement decisions. CRP provides centralized log analysis, dashboards, and scheduled compliance reports.
Req. 11 — Test security regularly	CRP documents continuous control effectiveness. Trend analysis across reporting periods. Evidence of ongoing security testing.
Req. 12 — Support information security with policies and programs	CRP generates policy compliance documentation. Maps enforcement evidence to organizational security policies.

PCI DSS v4.0 Customized Approach

PCI DSS v4.0 introduces the customized approach — allowing organizations to meet control objectives through alternative methods, provided they demonstrate equivalent security. TARA INNOVA supports this with:

- **Targeted risk analysis** — CRP provides data-driven risk analysis based on actual enforcement metrics, not theoretical assessments
- **Control effectiveness evidence** — Quantified protection rates, block rates, and response times demonstrate security outcomes
- **Continuous validation** — Real-time monitoring proves controls are operating effectively between QSA assessments

- **QSA-ready documentation** — Evidence packages formatted for assessor review with clear control-to-evidence mapping

Cardholder Data Environment Protection

Quicksand deploys at the boundary of your cardholder data environment. All traffic entering the CDE is inspected, validated, and logged before reaching payment systems. Enforcement happens at your edge — cardholder data never leaves your infrastructure. Combined with CRP's continuous evidence generation, this provides both the protection and the proof that PCI DSS demands.