2025
ASIA-PACIFIC
COMMUNITY
MEETING

A Maturity Framework for PCI DSS Compliance:

Quantifying Risks for Asia-Pacific Payment Security

PCI Security Standards Council

Sanket Sarkar

Hacker, Mathematics Geek, CRQ Researcher

Founder and CEO

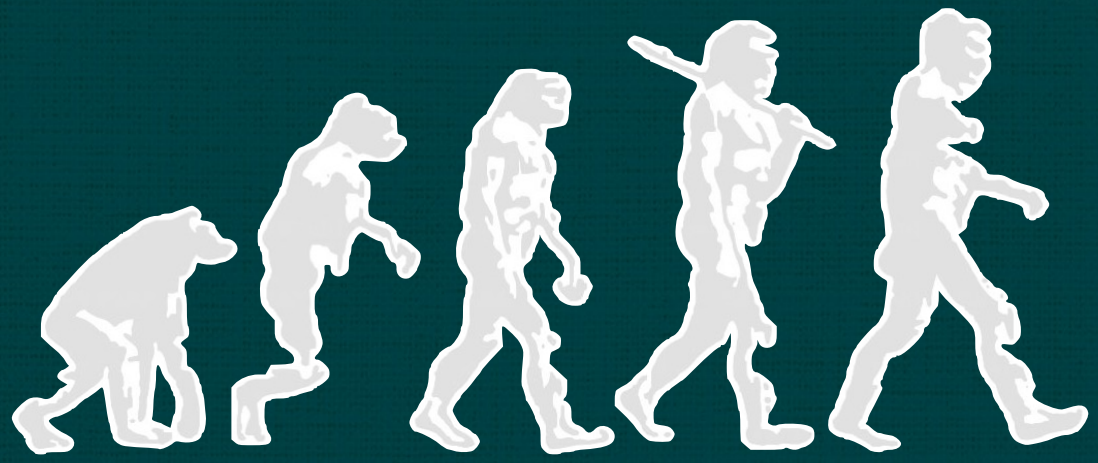
Zeron

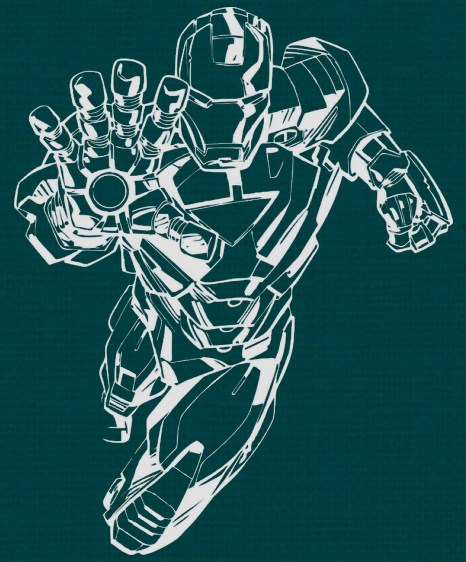
ZERON

PCI Security Standards Council

The PCI DSS Evolution.

How has PCI DSS Evolved over the years and what's the future?





Understand Guidelines

Grasp the PCI DSS framework and its requirements.

Identify Gaps

Recognise areas where current practices fall short of standards.

Implement Improvements

Take actions to address identified gaps and enhance security.

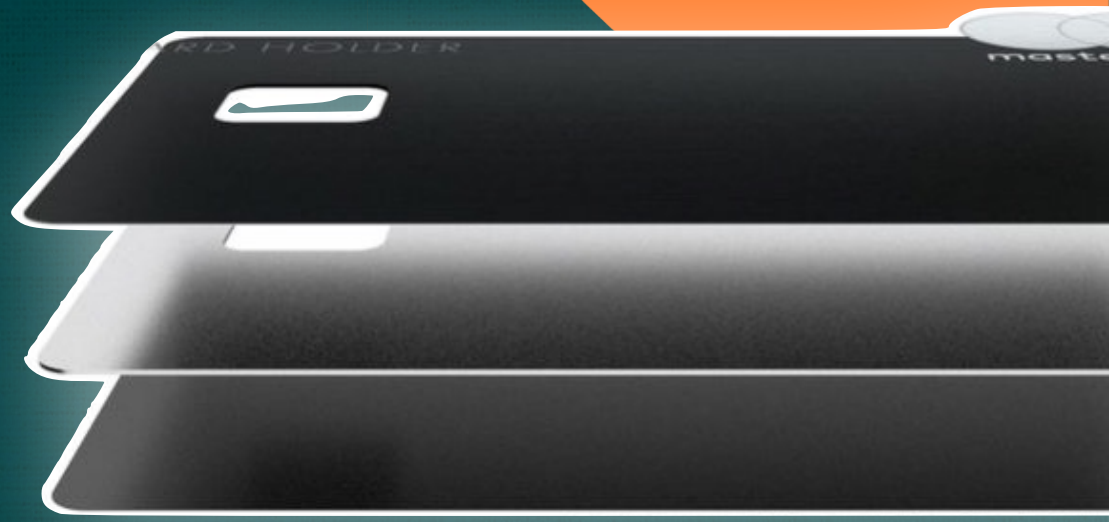
Measure & Track Security Posture

Continuously monitor and update security measures to stay compliant.

PCI Security Standards Council®

Introducing

An Enhanced Maturity Framework for PCI DSS v4.0.1 Compliance



A data-efficient, rigorous framework for objective and repeatable compliance evaluation.

PCI Security Standards Council

Methodology.

1. **Define** scope and collect data (CDE, regional risks).

2. **Assess** maturity across 12 PCI DSS requirements.

3. **Identify** and map risks to TEL impacts.

4. **Quantify** risks using MCMC simulations.

5. **Prioritise** controls to close gaps.

6. **Monitor** and reassess dynamically.

PCI Security Standards Council®

Methodology.

Dona always ignores quality potato menus.

1. **Define** scope and collect data (CDE, regional risks).
2. **Assess** maturity across 12 PCI DSS requirements.
3. **Identify** and map risks to TEL impacts.
4. **Quantify** risks using MCMC simulations.
5. **Prioritise** controls to close gaps.
6. **Monitor** and reassess dynamically.

PCI Security Standards Council®

Maturity Levels

$$S_t = (\Sigma_{i=1}^{12} w_i * C_i/12) * 100, C_i \in 0,1,2,3,4$$

Levels	Range	Maturity Metric
Initial	0-20	Ad-hoc, minimal compliance
Developing	21-40	Basic, inconsistent controls
Defined	41-60	Standardised, documented process
Managed	61-80	Proactive Monitoring, minor gaps
Optimised	81-100	Fully compliant, advanced technology.

PCI Security Standards Council®

Scoring Metrics

Req.	Numerator	Denominator	Ratio
1	Firewalls/IDS entry points	Total entry points	% Coverage
2	Hardened systems	Total CDE systems	% Coverage
3	Encrypted/masked systems	Systems storing data	% Coverage
4	Secure channels (TLS 1.2+)	Total channels	% Coverage
5	Anti-malware systems	Total CDE systems	% Coverage
6	Patched systems (≤30 days)	Total systems	% Coverage
7	RBAC users/systems	Total users/systems	% Coverage
8	MFA users	Total users	% Coverage
9	Controlled locations	Total locations	% Coverage
10	Monitored systems	Total CDE systems	% Coverage
11	Tested systems	Total CDE systems	% Coverage
12	(Training % + Policy %) / 2	100%	% Average

Scoring Weights

Req.	Description	Default Weight	UPI Fraud Weight	Cross-Border Weight	SME Weight	Rationale
1	Network security controls	0.10	0.10	0.10	0.10	Essential for CDE protection; consistent importance across contexts.
2	Secure system configurations	0.10	0.10	0.10	0.10	Critical for system hardening; steady weight due to universal need.
3	Protect stored account data	0.10	0.15	0.12	0.10	Higher in UPI fraud context due to phishing risks; slightly elevated for cross-border data protection.
4	Secure data transmission	0.10	0.10	0.15	0.10	Increased for cross-border due to PDPA/DPDP compliance needs.
5	Anti-malware protection	0.10	0.15	0.10	0.10	Higher in UPI fraud context to address phishing and malware threats.
6	Secure system development	0.10	0.08	0.08	0.15	Elevated for SMEs due to reliance on patching and cloud solutions.
7	Restrict data access	0.10	0.08	0.10	0.08	Moderate importance; slightly lower in UPI and SME contexts to balance weights.
8	User authentication	0.10	0.10	0.15	0.08	Increased for cross-border to ensure secure access across jurisdictions.
9	Physical access controls	0.08	0.07	0.07	0.07	Lower weight due to less direct impact on digital risks; consistent across contexts.
10	Monitor network access	0.10	0.15	0.10	0.10	Higher in UPI fraud context for real-time fraud detection.
11	Regular security testing	0.08	0.07	0.08	0.15	Elevated for SMEs to address vulnerability management constraints.
12	Security policies	0.04	0.05	0.05	0.07	Lower weight as foundational; slightly higher for SMEs to emphasize training.

Case Study I

Organisational Context

A small e-commerce startup in Mumbai processes 20,000 UPI transactions monthly (average value $20), generating $1M annual revenue with 30 employees. The startup faces frequent UPI fraud (e.g., phishing attacks), leading to 150 fraud incidents last year, costing $80K in losses and $30K in customer reimbursements. Weak encryption and lack of monitoring exacerbate vulnerabilities, risking customer trust and regulatory penalties under India's DPDP Act.

Req.	Description	Weight (UPI Fraud)	Before Ratio	Before C_i	After Ratio	After C_i
1	Network security controls	0.10	20% (10/50 entry points)	1	20% (10/50 entry points)	1
2	Secure system configurations	0.10	0% (0/100 systems)	0	20% (20/100 systems)	1
3	Protect stored account data	0.15	0% (0/20 systems)	0	75% (15/20 systems)	3
4	Secure data transmission	0.10	25% (5/20 channels)	1	25% (5/20 channels)	1
5	Anti-malware protection	0.15	0% (0/100 systems)	0	70% (70/100 systems)	3
6	Secure system development	0.08	0% (0/100 systems)	0	10% (10/100 systems)	1
7	Restrict data access	0.08	0% (0/30 users)	0	0% (0/30 users)	0
8	User authentication	0.10	0% (0/30 users)	0	0% (0/30 users)	0
9	Physical access controls	0.07	33% (1/3 locations)	1	33% (1/3 locations)	1
10	Monitor network access	0.15	0% (0/100 systems)	0	60% (60/100 systems)	3
11	Regular security testing	0.07	0% (0/100 systems)	0	0% (0/100 systems)	0
12	Security policies	0.05	20% ((20% training + 20% policies)/2)	1	70% ((80% training + 60% policies)/2)	3

Before Maturity Score and Level

$$S_t = \frac{0.32}{12} \times 100 \approx 8(Initial)$$

After Maturity Score and Level

$$S_t = \frac{1.35}{12} \times 100 \approx 28(Developing)$$

PCI Security Standards Council

Case Study II

Organisational Context

A Singapore payment processor with 15,000 cross-border transactions monthly (Singapore-Malaysia, $50 average value, $3M annual revenue, 80 employees) faces $200K fine risk and $80K churn due to inconsistent encryption and authentication. Interventions: TLS 1.3, MFA, policies/training ($50K total cost).

Req.	Description	Weight (Cross-Border)	Before Ratio	Before C_i	After Ratio	After C_i
1	Network security controls	0.10	60% (30/50 entry points)	2	60% (30/50 entry points)	2
2	Secure system configurations	0.10	20% (20/100 systems)	1	20% (20/100 systems)	1
3	Protect stored account data	0.12	25% (5/20 systems)	1	25% (5/20 systems)	1
4	Secure data transmission	0.15	33% (10/30 channels)	1	93% (28/30 channels)	4
5	Anti-malware protection	0.10	30% (30/100 systems)	1	30% (30/100 systems)	1
6	Secure system development	0.08	0% (0/100 systems)	0	10% (10/100 systems)	1
7	Restrict data access	0.10	62.5% (50/80 users)	2	62.5% (50/80 users)	2
8	User authentication	0.15	25% (20/80 users)	1	93.75% (75/80 users)	4
9	Physical access controls	0.07	40% (2/5 locations)	1	40% (2/5 locations)	1
10	Monitor network access	0.10	20% (20/100 systems)	1	20% (20/100 systems)	1
11	Regular security testing	0.08	0% (0/100 systems)	0	0% (0/100 systems)	0
12	Security policies	0.05	30% ((30% training + 30% policies)/2)	1	85% ((90% training + 80% policies)/2)	4

Before Maturity Score and Level

$$S_t = \frac{0.96}{12} \times 100 = 20(Initial)$$

After Maturity Score and Level

$$S_t = \frac{2.17}{12} \times 100 \approx 45(Defined)$$

PCI Security Standards Council

MATURITY

Your maturity level at present is in Defined Stage

ZERON

PCI SCORE

52.3

MOST MATURED CONTROL

Anti-malware systems

The Anti-Malware Systems show optimised maturity level with a score of 92%

LEAST MATURED CONTROL

User Authentication

With 7% score, the user authentication control shows initial level of maturity

ACTION PLANS

1. Implement IAM 60%
2. Employee Training 20%
3. Encrypt Systems 90%

Network security controls	DEFINED	27TH JULY 2025
Restrict Data Access	OPTIMISED	26TH JULY 2025

Thank You

LinkedIn

PCI Security Standards Council