Securing Payment Systems: PCI DSS Compliance Assessment

I conducted a comprehensive review of the systems that handle customer payment data. The goal was to evaluate how closely operations align with the PCI DSS 4.0 standard, which is essential for protecting sensitive cardholder information and maintaining customer trust.

Key Observations

- The web platform processes payments via an external payment gateway, but cardholder data (including full PANs) is stored in the internal database for refunds.
- Admin and support staff access sensitive data through an internal portal, but MFA is not enforced.
- TLS is in place for web transactions, but older versions (e.g., TLS 1.0) are still supported in some areas.
- Software development practices currently do not include formal code reviews or security testing.

2. PCI DSS Compliance Assessment Summary

Control Area	PCI DSS Requirement	Your current status
Data Encryption	3.4, 4.1 - encrypt PAN in storage/transit	PAN found unencrypted in backups
Access Controls	7.8- role based access & MFA	Shared logins, MFA missing on admin apps
Secure Development	6.3 - secure coding, testing, code reviews	No structured secure SDLC in place
Logging & Monitoring	10 - review access logs, alerts	Logs collected but not actively reviewed
Incident Response	12.10 - Formal IR plan required	No documented incident response policy

3. Key Risk Areas

- Unencrypted Storage of Cardholder Data

- PAN data was found in plain text within daily database backups.
- This exposes the company to serious risks of data breach penalties and customer loss.

- Weak Internal Access Controls

Shared admin credentials and the absence of MFA make internal misuse or breaches easier.

- Missing Secure Development Lifecycle (SDLC)

Without secure coding practices, there's an increased risk of introducing exploitable vulnerabilities.

- Insufficient Monitoring & Logging

No alerts on unauthorized access could delay breach detection and response.

- No Formal Incident Response Procedure

In the event of a breach, there is no tested plan for quick containment or regulatory notification.

4. Remediation Plan

Issue	**Recommended Action**	**Owner**	**Target Date**
Unencrypted cardholder data	Encrypt all stored PANs (AES-256), review backup strategy	IT security	May 15
TLS version outdated	Disable TLS 1.0/1.1, enforce TLS 1.2+ on all external interfaces	Network admin	May 8
Shared accounts / no MFA	Implement unique logins and enable MFA across all admin systems	IAM team	May 22
No secure coding process	Train dev team on OWASP top 10,	Development manager	May 30

	introduce code reviews and test protocols		
Lack of active log monitoring	Implement centralized SIEM and log review SOP	Security operations	May 25
No incident response plan	Create, test and document IR plan, assign roles	Compliance manager	May 18