Haumaru Whānau
SECURING TRUST. PROTECTING DATA. ENABLING GROWTH.

VOLUME 1
AUGUST 2026

PCI FRIDAY | NEWSLETTER

PCI DSS
BEYOND THE AUDIT

WHAT WE'VE LEARNED SO FAR FROM PCI FRIDAY

Six practical lessons on scope, segmentation, governance, assurance, and sustainable PCI DSS compliance.

1. Protecting Trust
2. Segmentation
3. Costly Mistakes
4. Myths vs Reality
5. PCI DSS Scope
6. Requirement 12

CREST
Accredited

PCI QSA
Qualified Security Assessor

ISO/IEC 27001
Certified

UAE DESC
Accredited

Strong security builds confidence. Continuous assurance earns trust.

VOLUME 1

What PCI Friday Has Covered So Far

When we started **PCI Friday**, we did not want to create another series that simply walks through PCI DSS one requirement at a time. The standard already tells organizations what is expected. The harder part is making it work in a real environment: understanding scope, keeping ownership clear, collecting evidence, managing change, and ensuring controls continue to operate long after the assessment ends. Our first six PCI Friday editions explored those practical challenges from different angles. This volume brings the lessons together in one place.

Inside this volume

LESSON 01

An assessment matters, but it should never become the sole purpose of a PCI DSS programme.

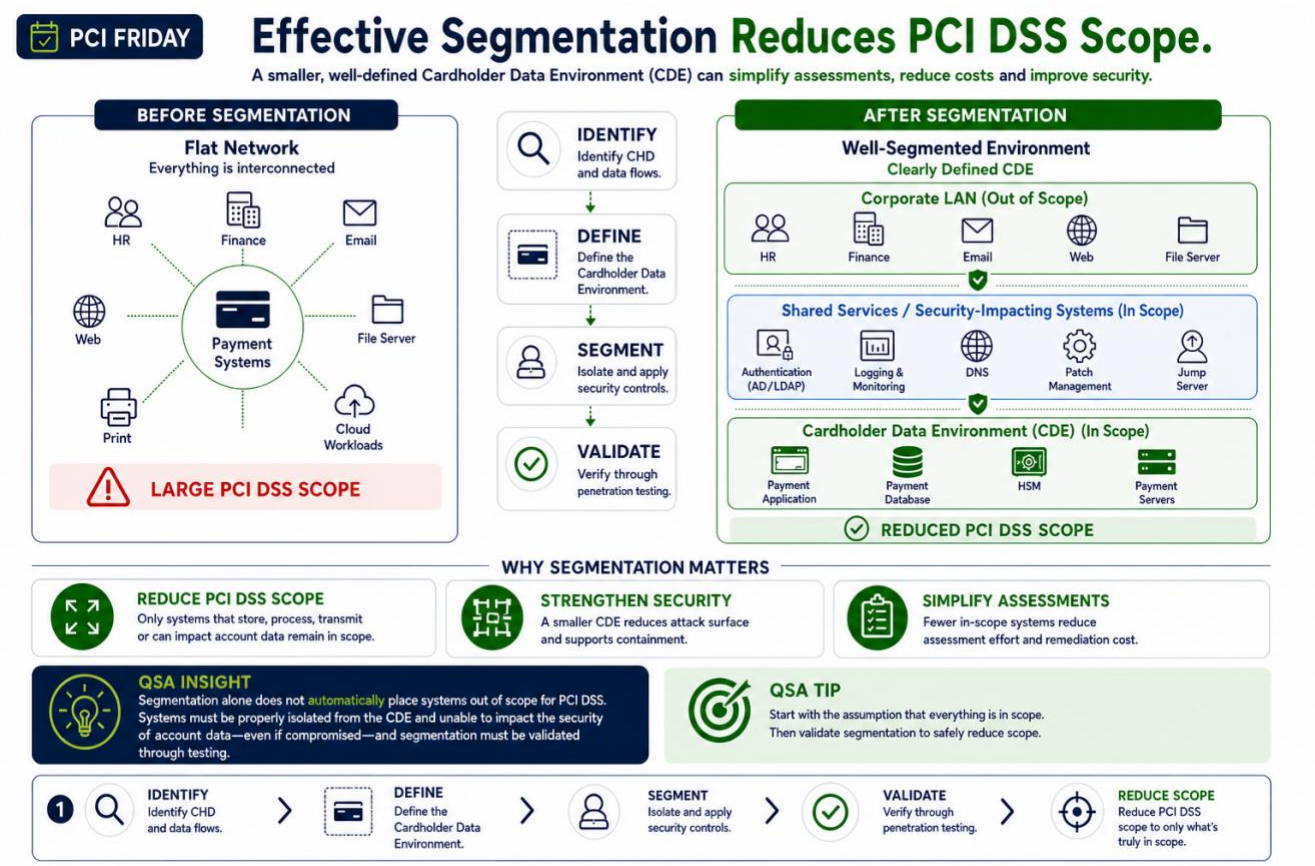
The real objective is protecting payment data every day. That means knowing where account data goes, limiting access, securing the systems around it, finding weaknesses early, and making sure the controls still work when nobody is preparing for an audit. The assessment should confirm that an effective security programme is already operating. It should not be the event that temporarily creates one.

> **The lesson: Compliance is a milestone. Protecting payment data and maintaining trust is the continuing responsibility.**

From the QSA's Notebook

The healthiest PCI DSS programmes do not suddenly become busy when the assessor arrives. Their normal operations already produce the control evidence the assessment needs.

LESSON 02



Segmentation is often discussed as an easy way to reduce scope: place the Cardholder Data Environment on a separate network and keep everything else outside it.

In practice, it is rarely that simple.

Shared authentication, logging, administrative access, monitoring, patching, DNS, remote support, and other connected or security-impacting services can affect the CDE even when they do not store cardholder data themselves.

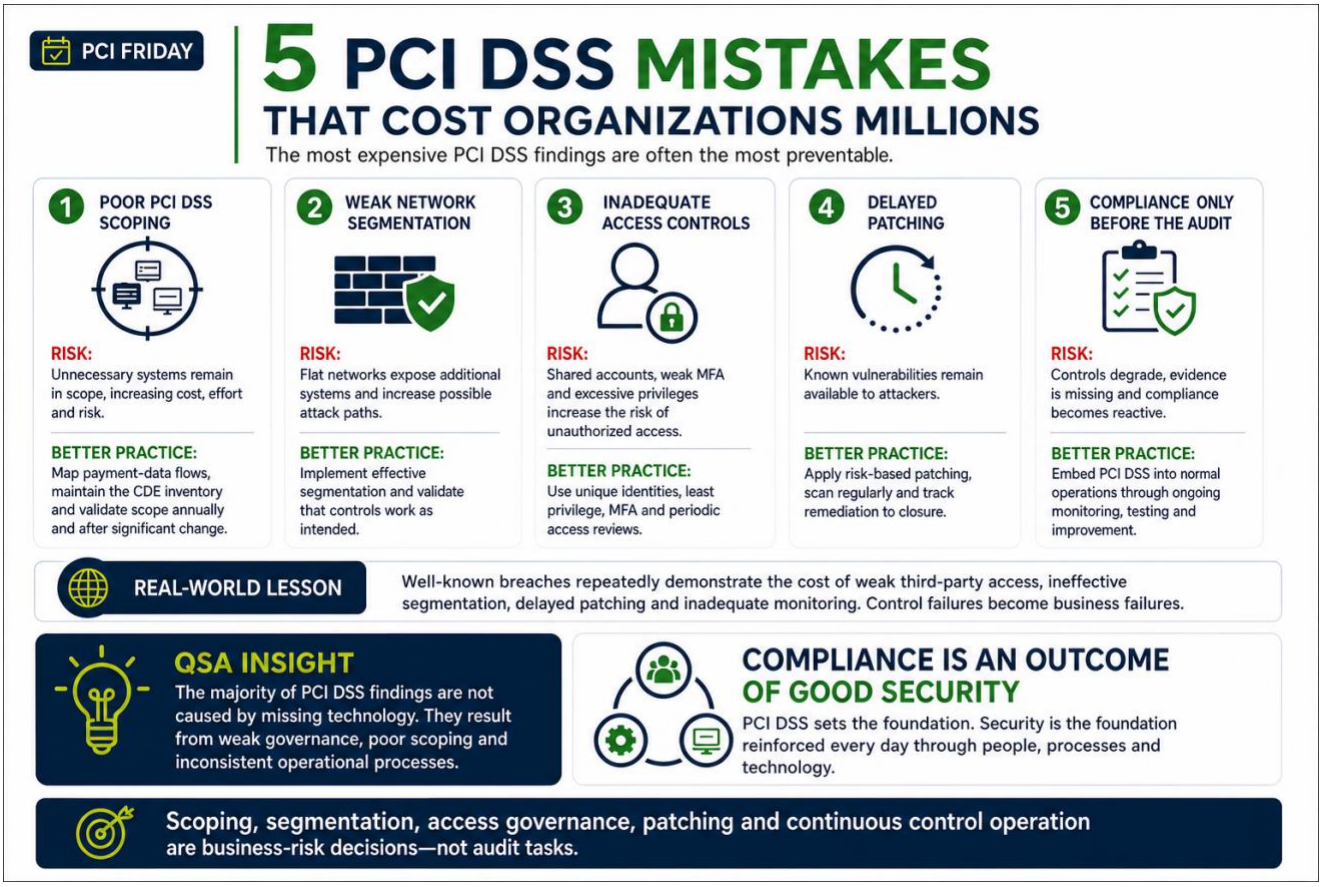
A separate VLAN or a line on a network diagram does not prove isolation. If segmentation is being used to reduce scope, it must be properly designed, maintained, and validated as effective.

The lesson: Do not assume segmentation reduces scope. Be ready to demonstrate that it does.

From the QSA's Notebook

Good segmentation can reduce risk and assessment effort. Weak segmentation creates false confidence—and may leave far more of the environment in scope than expected.

LESSON 03



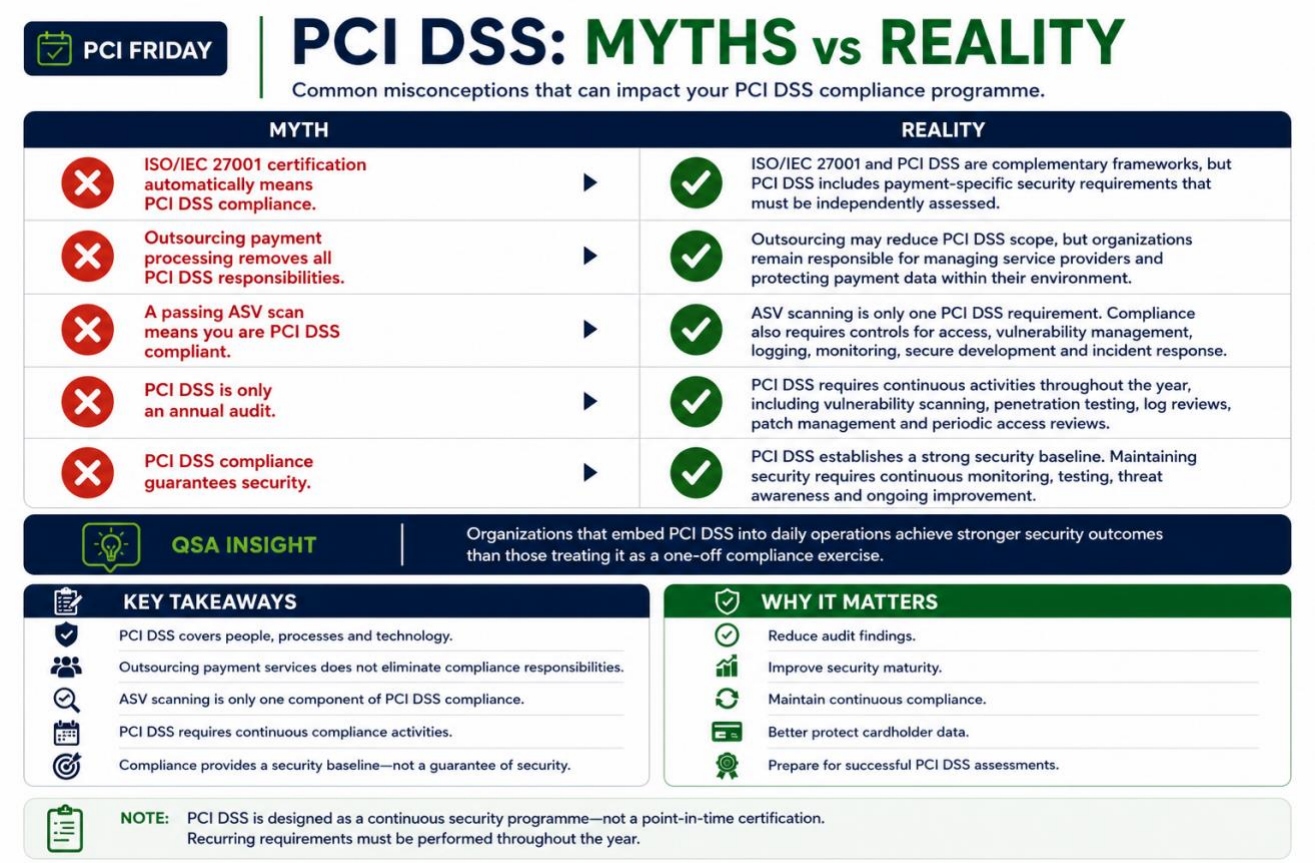
Some PCI DSS problems are expensive because they create both security exposure and unnecessary operational effort.

1. **Poor scoping** — bringing unnecessary systems into the PCI DSS environment, or overlooking systems that can affect it.
2. **Weak segmentation** — increasing the number of systems exposed to the CDE and widening possible attack paths.
3. **Inadequate access controls** — allowing shared accounts, excessive privileges, weak authentication, or poorly governed administrative access.
4. **Delayed patching** — leaving known vulnerabilities available to attackers while remediation waits for the next assessment cycle.
5. **Preparing only for the audit** — allowing controls and evidence to deteriorate during the rest of the year.

These are not isolated compliance problems. They influence the cost of the programme, the size of the attack surface, and the organization's ability to respond when something goes wrong.

> **The lesson: The most expensive PCI DSS failures often begin with weak fundamentals, not obscure technical issues.**

LESSON 04



“We are ISO/IEC 27001 certified, so we are already PCI DSS compliant.”

The two can complement each other, but PCI DSS contains payment-specific requirements that still need to be evaluated.

“We outsourced payments, so PCI DSS is no longer our responsibility.”

Outsourcing can reduce scope, but the organization still needs to understand its remaining responsibilities and manage the service-provider relationship.

“Our ASV scan passed, so we are compliant.”

An ASV scan validates only one part of a much broader PCI DSS programme.

“PCI DSS is an annual audit.”

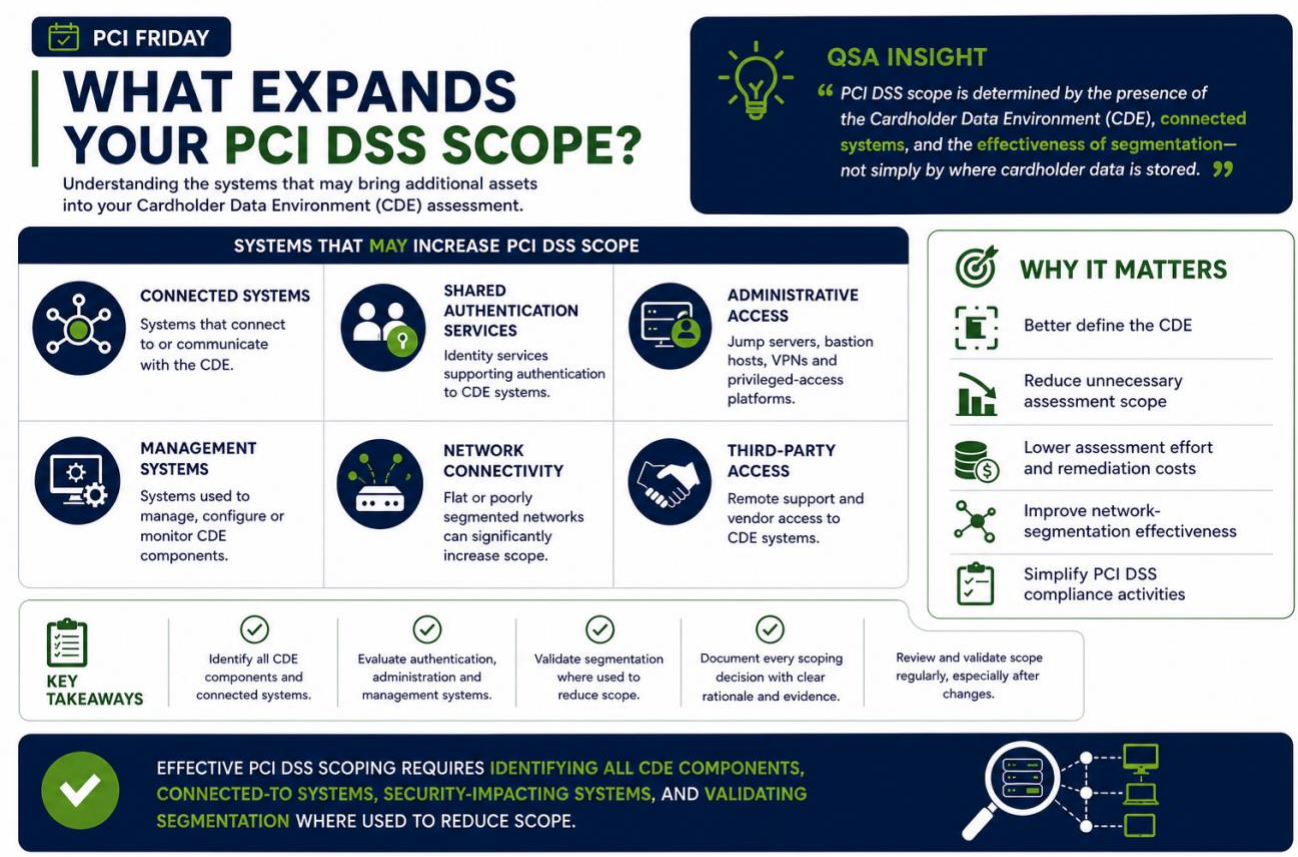
Many controls and activities must operate throughout the year.

“PCI DSS compliance means we are secure.”

PCI DSS provides an important baseline. It does not replace continuous monitoring, testing, risk management, and improvement.

> **The lesson: Compliance provides structure and assurance, but it should never create complacency.**

LESSON 05



One of the easiest scoping mistakes is to ask only whether a system stores cardholder data.

PCI DSS scoping also considers systems that connect to the CDE or can affect its security. Depending on the environment, that can include:

- Shared authentication and identity services
- Jump servers, bastion hosts, VPNs, and privileged-access platforms
- Logging, monitoring, and security-management systems
- Connected networks and shared infrastructure
- Administrative workstations
- Third-party support and remote-access paths

This is why the CDE often becomes larger than teams initially expect. The relationships around payment systems matter as much as the obvious systems inside them.

> **The lesson: Start with payment-data flows and trust relationships—not just a list of systems known to store cardholder data.**

From the QSA's Notebook

A system does not need to hold cardholder data to influence PCI DSS scope. The more useful question is: "Could its compromise affect the security of the CDE?"

LESSON 06

PCI DSS Requirement 12 is titled **"Support Information Security with Organizational Policies and Programs."** It covers the organizational disciplines needed to keep technical controls working, including policies, responsibilities, acceptable-use expectations, risk activities, security awareness, incident response, scope management, and third-party service-provider governance.

Firewalls, encryption, MFA, and logging all matter. But somebody must own them, review them, respond when the environment changes, and retain evidence that they continue to operate.

This is why PCI DSS cannot belong to IT alone. Security, Infrastructure, Cloud, Development, Operations, Risk, Compliance, Procurement, HR, and business teams may all have responsibilities within the programme.

The lesson: Technology enables PCI DSS compliance. Governance is what sustains it.

From the QSA's Notebook

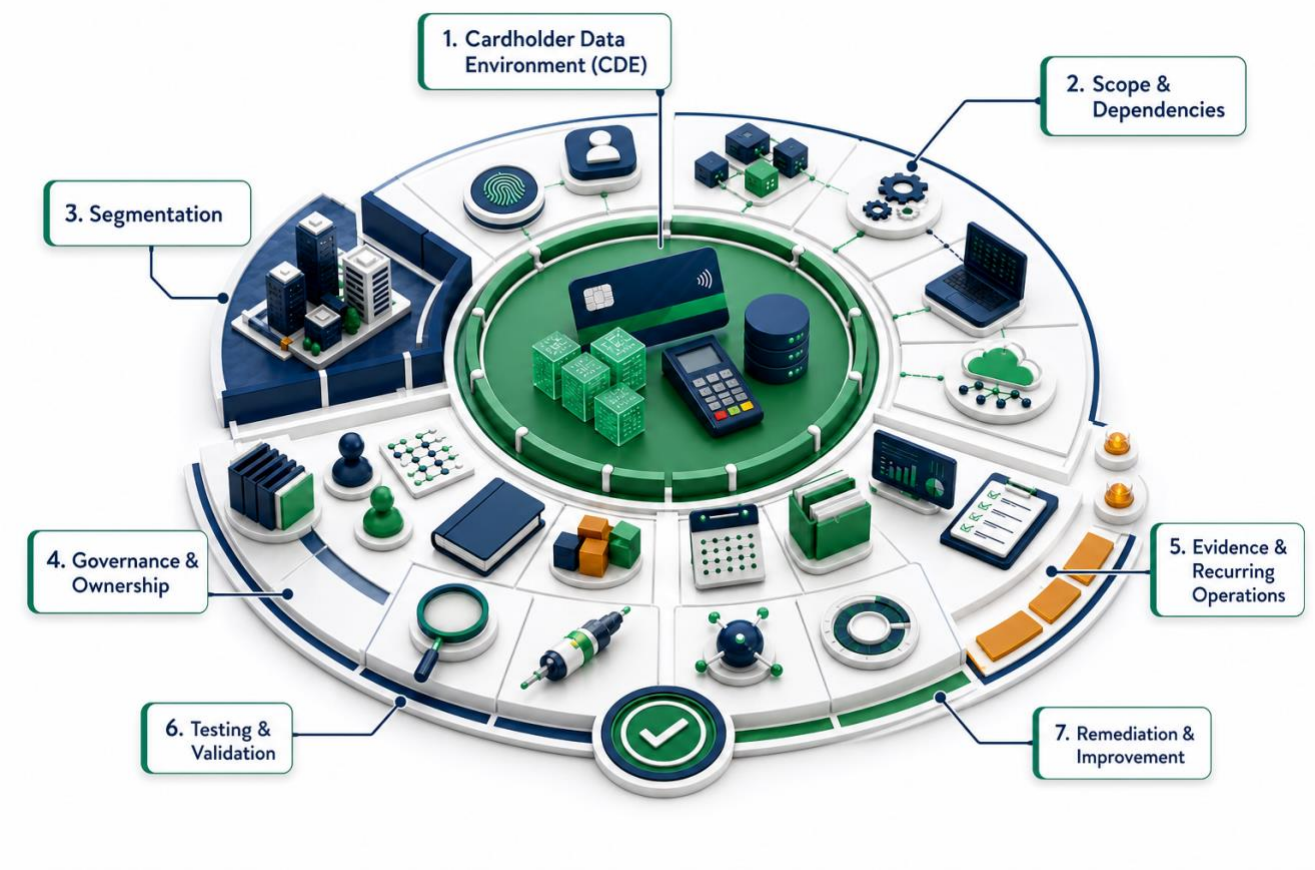
Assign one person to coordinate the PCI DSS programme, but give each control a genuine operational owner. The programme owner should not spend the year chasing responsibilities that were never clearly assigned.

THE COMBINED PERSPECTIVE

What Connects These Lessons?

Although each lesson approaches PCI DSS from a different angle, together they describe the foundations of a sustainable PCI DSS programme.

Protecting payment data begins with understanding where it flows and which people, processes, technologies, connections, and third parties can affect its security. That understanding creates the foundation for accurate PCI DSS scoping and helps organizations distinguish the systems that genuinely belong within the environment from those that can be safely separated.



Effective segmentation can then reduce unnecessary exposure and compliance effort, but only when it is properly designed, maintained, and validated. Assumptions about outsourcing, certifications, network boundaries, or passing security scans cannot replace a clear understanding of how the environment actually operates. The programme also needs governance. Every control should have an accountable owner, recurring activities should operate throughout the year, and evidence should be retained as part of normal business processes. Technical safeguards remain essential, but policies, responsibilities, risk management, awareness, and third-party oversight are what keep those safeguards effective as systems and organizations change.

Finally, organizations need to test their assumptions. Scanning, penetration testing, segmentation validation, access reviews, monitoring, and remediation should demonstrate that controls are not merely documented or configured, but are genuinely reducing risk to the payment environment.

> **PCI DSS becomes easier to manage when it stops being an annual audit project and becomes part of normal business operations.**

PRACTICAL TAKEAWAY

Six Habits of a Sustainable PCI DSS Programme

Looking across the lessons in this volume, six practical habits stand out. Together, they help organizations maintain PCI DSS compliance while strengthening payment security throughout the year.

1. Keep scope alive

PCI DSS scope is not something you define once and forget. New systems, integrations, service providers, network connections, and administrative tools can change the environment. Keep payment-data flows, inventories, dependencies, and CDE boundaries current—and review them whenever something significant changes.

2. Give every control an owner

A control without a clear owner eventually becomes nobody's responsibility. Each recurring PCI DSS activity should have someone accountable for performing it, retaining the evidence, addressing exceptions, and ensuring there is backup coverage when that person is unavailable.

3. Capture evidence as you work

Do not wait for the assessment to start searching through emails, tickets, and shared folders. Access reviews, scans, approvals, training, risk analyses, and remediation activities should produce and retain evidence as part of the normal process.

4. Put change through a PCI lens

A new application, vendor, cloud service, firewall rule, or authentication platform may affect PCI DSS scope or control effectiveness. Ask about the PCI DSS impact before the change goes live—not after it has already altered the environment.

5. Test whether controls work

A documented or configured control is not necessarily an effective control. Scanning, penetration testing, segmentation testing, access reviews, monitoring, and other validation activities should confirm that controls operate as intended and genuinely reduce risk.

6. Remediate, retest, and improve

Finding a weakness is only the beginning. Assign remediation, track it to closure, and retest the fix. When the same issue appears repeatedly, look beyond the individual finding and address the underlying process, ownership, or governance problem.

Sustainable PCI DSS compliance is built through everyday operational habits—not through a once-a-year assessment exercise.

COMPANY PROFILE

About Haumaru Whānau

Haumaru Whānau is a **PCI DSS Qualified Security Assessor (QSA) Company**, helping organizations protect payment data and build sustainable PCI DSS programmes.

Our services include PCI DSS assessments, readiness and advisory support, payment-security assurance, penetration testing, cybersecurity assurance, governance, risk, and compliance. We combine assessor insight with practical technical experience to help organizations move beyond audit preparation and maintain effective security controls throughout the year.

www.haumaru.org
info@haumaru.org
+971 50 269 1596

Securing Trust. Protecting Data. Enabling Growth.

Important Notice

This publication provides general educational and professional guidance. It is not a substitute for the official PCI DSS standard, applicable PCI SSC programme documentation, payment-brand requirements, acquirer instructions, or a formal assessment by an appropriately qualified assessor. Organizations should refer to current PCI SSC documentation when determining their obligations. PCI DSS v4.0.1 is the active version of the standard at the time of publication.

Official References

PCI Security Standards Council, PCI DSS v4.0.1 and supporting documents: www.pcisecuritystandards.org
PCI SSC, Guidance for PCI DSS Scoping and Network Segmentation: www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1_1.pdf