PCI DSS Control Mapping

What PCI DSS Is (Context)

PCI DSS (Payment Card Industry Data Security Standard) is a **risk-based security framework** designed to protect cardholder data. It applies to **any system that stores, processes, or transmits cardholder data**, including cloud-based infrastructure.

PCI DSS v4.0 emphasizes:

- Continuous security (not point-in-time)
- Strong access controls
- Evidence-based validation
- Risk-driven implementation

Requirement 1

Install and Maintain Network Security Controls

What this means
You must restrict network access so only approved traffic can reach systems in scope for cardholder data.

In cloud environments

- Security Groups, NSGs, firewalls, routing tables, peering, and load balancers replace traditional firewalls
- Misconfiguration is the #1 cause of violations

Common failures

- Internet-facing resources unintentionally in scope
- Flat networks without segmentation
- Overly permissive inbound rules (0.0.0.0/0)

Why auditors care
They want proof that **only explicitly allowed traffic** can reach CDE systems.

Requirement 2

Apply Secure Configurations to All System Components

What this means
Systems must follow secure configuration standards, and insecure defaults must be removed.

In cloud environments

- Managed services ship with defaults that are often insecure
- Configuration drift happens continuously

Common failures

- Public storage buckets
- Default encryption disabled
- Insecure service settings not reviewed post-deployment

Why auditors care
Misconfigurations are silent, persistent risks and frequently exploited.

Requirement 3

Protect Stored Account Data

What this means
If cardholder data is stored, it must be:

- Minimized
- Encrypted
- Properly protected with key management

In cloud environments

- Object storage, databases, snapshots, backups
- Cloud-native encryption and KMS usage

Common failures

- Encryption disabled or improperly configured
- Poor key rotation practices
- Unclear data location visibility

Important note
PCI does **not** want card data stored unless absolutely necessary.

Requirement 4

Protect Cardholder Data in Transit

What this means
Cardholder data must be encrypted when transmitted over open or public networks.

In cloud environments

- TLS configuration
- Load balancers, APIs, service endpoints

Common failures

- Legacy TLS versions
- Services allowing plaintext communication
- Internal traffic assumed to be “trusted”

Requirement 5

Protect Systems from Malware

What this means
You must deploy anti-malware controls appropriate to the system.

In cloud environments

- Often shifts to cloud-native services or EDR tools
- Less relevant for fully managed PaaS but still assessed

Key takeaway
Auditors want **coverage justification**, not just tools installed.

Requirement 6

Develop and Maintain Secure Systems and Software

What this means
Systems must be hardened, patched, and securely configured.

In cloud environments

- Managed services still require secure configuration
- Infrastructure-as-Code drift creates risk

Common failures

- Unpatched services assumed “managed means secure”
- No visibility into configuration changes

Requirement 7

Restrict Access by Business Need to Know

What this means
Access must be limited to what is required for a user’s job role.

In cloud environments

- IAM roles, policies, service accounts
- Identity sprawl is common

Common failures

- Wildcard permissions (*:*)

- Shared service accounts
- No periodic access review

Why auditors care
Most breaches involve **excessive or misused permissions**.

Requirement 8

Identify Users and Authenticate Access

What this means
Every user must be uniquely identifiable and strongly authenticated.

In cloud environments

- MFA enforcement
- Privileged role protections
- Federated identity via SSO

Common failures

- MFA not enforced for privileged users
- Local cloud accounts left active
- Shared credentials

Requirement 9

Restrict Physical Access to Cardholder Data

Cloud impact
Mostly inherited from the cloud service provider.

Customer responsibility
Document reliance on cloud provider controls.

Requirement 10

Log and Monitor All Access

What this means
You must log and monitor access to systems and data and retain logs.

In cloud environments

- Cloud-native audit logs
- Centralized logging pipelines

Common failures

- Logging disabled or partially enabled
- Logs not retained long enough
- No visibility across multiple accounts/subscriptions

Why auditors care
Without logs, incidents cannot be investigated.

Requirement 11

Test Security of Systems and Networks

What this means
Regular testing proves controls are actually working.

Includes

- Vulnerability scanning
- Penetration testing
- Change detection

Cloud nuance
Continuous configuration monitoring increasingly satisfies parts of this requirement.

Requirement 12

Support Security with Organizational Policies and Programs

What this means
Security must be governed, documented, and continuously managed.

In practice

- Defined roles and responsibilities
- Risk management processes
- Continuous compliance visibility

Why PCI v4.0 emphasizes this
Compliance must be **operational**, not just documented.

How Auditors Think About PCI Now

Auditors increasingly ask:

- “How do you know this control is still working?”
- “What changed since the last review?”
- “Show me evidence over time, not screenshots”

This is why **continuous monitoring and historical evidence** matter more in PCI v4.0 than ever before.

Executive Summary (One Sentence)

PCI DSS is no longer about passing an annual audit; it is about **proving, at any time, that security controls protecting cardholder data are continuously enforced and monitored**.