PCI DSS v4.0.1 READINESS ASSESSMENT

Illustrative Sample Deliverable

SampleCompany.com

E-Commerce / Online Retail · Fictional Sample Report

FICTIONAL SAMPLE REPORT — DEMONSTRATION PURPOSES ONLY

This document is a simulated PCI DSS assessment created by TMG Security to demonstrate report structure, methodology, evidence handling, findings, and professional reporting standards. SampleCompany.com is fictional. No actual PCI DSS assessment, certification, Attestation of Compliance (AOC), or Report on Compliance (ROC) was performed.

Assessment Period	01 August 2026 – 21 August 2026	**Report Date**	25 August 2026
Report Version	1.0	**Classification**	**Confidential**
Service Provider	TMG Security	**Assessment Type**	Illustrative Readiness Assessment

CONFIDENTIALITY NOTICE

This document, including all findings and illustrative data herein, is provided by TMG Security strictly as a demonstration sample. Distribution outside its intended demonstration purpose without written consent is discouraged. This report does not constitute, and must not be represented as, an actual PCI DSS Report on Compliance, Attestation of Compliance, or certification of any kind.

01 DOCUMENT CONTROL

Document Owner	TMG Security — Governance, Risk & Compliance (GRC) Practice
Prepared By	TMG Security Assessment Team
Reviewed By	TMG Security Quality Assurance Lead
Version	1.0
Issue Date	25 August 2026
Classification	CONFIDENTIAL — SAMPLE / DEMONSTRATION
Assessment Type	Fictional PCI DSS Assessment / Illustrative Readiness Assessment
Assessment Period	01 August 2026 – 21 August 2026
Client	SampleCompany.com (Fictional Entity)
Service Provider	TMG Security

Document Change History

Version	Date	Description	Author
1.0	25 Aug 2026	Initial issue of sample report	TMG Security Assessment Team

Distribution List

Name / Role	Organization	Purpose
Chief Information Security Officer (Fictional)	SampleCompany.com	Primary recipient
Compliance Officer (Fictional)	SampleCompany.com	Compliance oversight
Engagement Lead	TMG Security	Quality assurance / archival

TABLE OF CONTENTS

02 IMPORTANT DISCLAIMER

FICTIONAL SAMPLE REPORT — DEMONSTRATION PURPOSES ONLY

This report has been produced solely for demonstration and portfolio purposes on behalf of TMG Security. It is intended to illustrate the structure, depth, and professional standard of a PCI DSS compliance assessment deliverable. To ensure there is no ambiguity regarding the nature of this document, TMG Security sets out the following clarifications:

- SampleCompany.com is a fictional entity. It does not correspond to any real business, and any resemblance to an actual organization is purely coincidental.
- No actual PCI DSS assessment, gap analysis, or readiness review was performed against any real environment, system, or organization.
- No certification, attestation, or compliance determination has been issued to any party as a result of this document.
- This report does not represent, reference, or substitute for an official Report on Compliance (ROC) or Attestation of Compliance (AOC) as defined by the PCI Security Standards Council.
- All findings, risk ratings, evidence references, control statuses, and remediation timelines contained in this report are illustrative and fictional. They were constructed to demonstrate realistic reporting conventions and do not describe any actual security condition.
- All evidence artifacts referenced (policies, configurations, scan results, interview notes, and similar items) are representative examples only. No actual client evidence was collected, reviewed, or retained.
- Technical examples, control descriptions, and architecture diagrams are representative of common industry patterns and do not describe any specific, real system.
- TMG Security is not representing, and this document must not be interpreted as representing, that TMG Security acted as a Qualified Security Assessor (QSA) engaged by SampleCompany.com.

Intended Use

This sample report may be shared with prospective clients, partners, and other interested parties to illustrate TMG Security's assessment methodology, documentation standards, and reporting quality. It should not be relied upon for any compliance, legal, contractual, or risk decision. Organizations seeking an actual PCI DSS assessment should engage a PCI SSC-listed Qualified Security Assessor (QSA) company.

PCI DSS Assessment Types — Terminology

TMG Security uses the following terms precisely and does not use them interchangeably. This sample report is formatted as an illustrative PCI DSS Readiness Assessment and is not, and does not claim to be, any of the formal validation outputs listed below.

PCI DSS Compliance Assessment	A formal assessment against all applicable PCI DSS requirements, typically performed by a QSA for entities required to validate via a ROC.
PCI DSS Readiness Assessment	A gap-analysis-style engagement (as illustrated by this sample report) performed ahead of a formal assessment to identify and remediate gaps; it does not itself produce a ROC or AOC.
Self-Assessment Questionnaire (SAQ)	A validation tool completed by the entity itself, used by eligible merchants and service providers in lieu of a full on-site assessment.
Report on Compliance (ROC)	The detailed report documenting an entity's PCI DSS assessment results, prepared by a QSA (or internal assessor, where eligible).
Attestation of Compliance (AOC)	A formal declaration, based on a ROC or SAQ, that an entity has validated its PCI DSS compliance status.
QSA Assessment	An assessment performed by an individual and company certified by the PCI Security Standards Council as a Qualified Security Assessor. TMG Security does not represent itself as a QSA company in this document.
ASV Scanning	Quarterly external vulnerability scanning performed by a PCI SSC-Approved Scanning Vendor, required under PCI DSS Requirement 11.3.2.
Penetration Testing	Manual, methodology-driven testing of network and application-layer controls, required under PCI DSS Requirement 11.4.

03 EXECUTIVE SUMMARY

TMG Security has prepared this fictional, illustrative PCI DSS v4.0.1 Readiness Assessment sample to represent SampleCompany.com, a hypothetical e-commerce and online retail organization. This section presents a fictional executive-level summary of the simulated assessment results, prepared in the style and format TMG Security would use for an actual engagement.

ALL METRICS ON THIS PAGE ARE FICTIONAL SAMPLE DATA

Overall Illustrative Assessment Status

PARTIALLY IN PLACE

SampleCompany.com's simulated environment substantially aligns with PCI DSS v4.0.1 requirements, with a defined set of fictional gaps requiring remediation. This illustrative status reflects a sample readiness assessment and does not represent an official PCI DSS compliance determination, ROC, or AOC.

Fictional Sample Metrics

12	8	3	1
Requirements Assessed	In Place	Partially In Place	Not In Place

Executive Risk Summary

The fictional assessment identified one high-severity sample finding related to vulnerability remediation tracking under Requirement 6, alongside a small number of medium and low-severity observations distributed across network security, data protection, and access management domains. No critical findings were recorded in this illustrative scenario. TMG Security's simulated recommendation is that SampleCompany.com prioritize closure of the high-severity item within 30 days, with remaining items addressed across a 90-day remediation roadmap (see Section 23).

This summary, and every figure on this page, is entirely fictional and constructed for demonstration purposes only. It does not describe the security posture of any real organization.

04 PCI DSS V4.0.1 — ILLUSTRATIVE ASSESSMENT DASHBOARD

FICTIONAL SAMPLE DASHBOARD — ILLUSTRATIVE DATA ONLY, NOT AN OFFICIAL COMPLIANCE DETERMINATION

Overall Illustrative Assessment Status

PARTIALLY IN PLACE

Requirements Assessed — Illustrative Status Breakdown

12	8	3	1	0
Requirements Assessed	In Place	Partially In Place	Not In Place	Not Applicable

Total Findings — Illustrative Severity Breakdown

10	0	1	3	3	3
Total Findings	Critical	High	Medium	Low	Observations

Illustrative Status by Domain

PCI DSS v4.0.1's twelve requirements are grouped below into their six control-objective domains. Status shown reflects the least-favorable illustrative status of any requirement within that domain; finding counts match the Detailed Findings and Finding Register sections exactly. Two additional findings (PCI-TLS-004, PCI-TST-009) are internal security observations not mapped to a PCI DSS requirement and are therefore excluded from the domain table below, though both are included in the Total Findings count above.

Domain	Illustrative Assessment Status	Findings
Build and Maintain a Secure Network and Systems (Req. 1–2)	Partially In Place	2
Protect Account Data (Req. 3–4)	Partially In Place	1
Maintain a Vulnerability Management Program (Req. 5–6)	Not In Place	2
Implement Strong Access Control Measures (Req. 7–9)	Partially In Place	1
Regularly Monitor and Test Networks (Req. 10–11)	In Place	1
Maintain an Information Security Policy (Req. 12)	In Place	1

05 MANAGEMENT OVERVIEW

Business Environment

SampleCompany.com (fictional) is presented as a mid-market online retailer offering direct-to-consumer e-commerce across web and mobile channels. The organization's simulated environment processes card-not-present transactions through a hosted storefront, a public-facing API layer, and an integration with a third-party payment gateway. This narrative is illustrative and constructed solely to give context to the sample findings that follow.

Payment Processing Model

In this fictional scenario, cardholder data is captured through a client-side integration with the payment gateway's tokenization service, with account data transmitted directly from the customer's browser to the third-party processor. SampleCompany.com's own infrastructure is represented as handling transaction metadata, order records, and tokenized references rather than full Primary Account Numbers (PAN), reducing — but not eliminating — the scope of the illustrative cardholder data environment (CDE).

Security Maturity (Illustrative)

The simulated environment reflects an organization with an established security program, formal policies, and defined ownership of key controls, but with inconsistent operational follow-through in select areas such as vulnerability remediation tracking and access recertification. This fictional maturity profile is representative of many mid-market e-commerce organizations preparing for a first or renewal PCI DSS assessment.

Major Strengths (Fictional)

- Documented information security policy suite reviewed on an illustrative annual cycle.
- Network segmentation separating the simulated cardholder data environment from general corporate systems.
- Centralized identity and access management with multi-factor authentication enforced for administrative access.
- Managed detection and response (MDR) coverage across illustrative endpoints and cloud workloads.

Major Gaps (Fictional)

- Inconsistent documentation of vulnerability remediation timelines and ownership (see Finding PCI-SD-006).
- Periodic user access reviews not consistently evidenced for all sampled system components.
- Legacy firewall rules identified during sampling without current documented business justification.

Immediate Priorities (Fictional)

- Remediate and formally close the high-severity sample finding related to vulnerability tracking within 30 days.
- Complete a full recertification of privileged and administrative access across in-scope systems.
- Review and retire undocumented legacy firewall rules identified during the illustrative sampling exercise.

Strategic Recommendations (Fictional)

TMG Security's simulated recommendation is that SampleCompany.com formalize a centralized GRC tracking capability spanning vulnerability management, access governance, and remediation reporting, supported by quarterly management review of control performance ahead of any future formal PCI DSS assessment engagement.

06 SCOPE & ENVIRONMENT

The table below presents the fictional scope boundary defined for this sample assessment. Scope determinations shown are illustrative and follow the general structure TMG Security uses to document environment boundaries during an actual engagement.

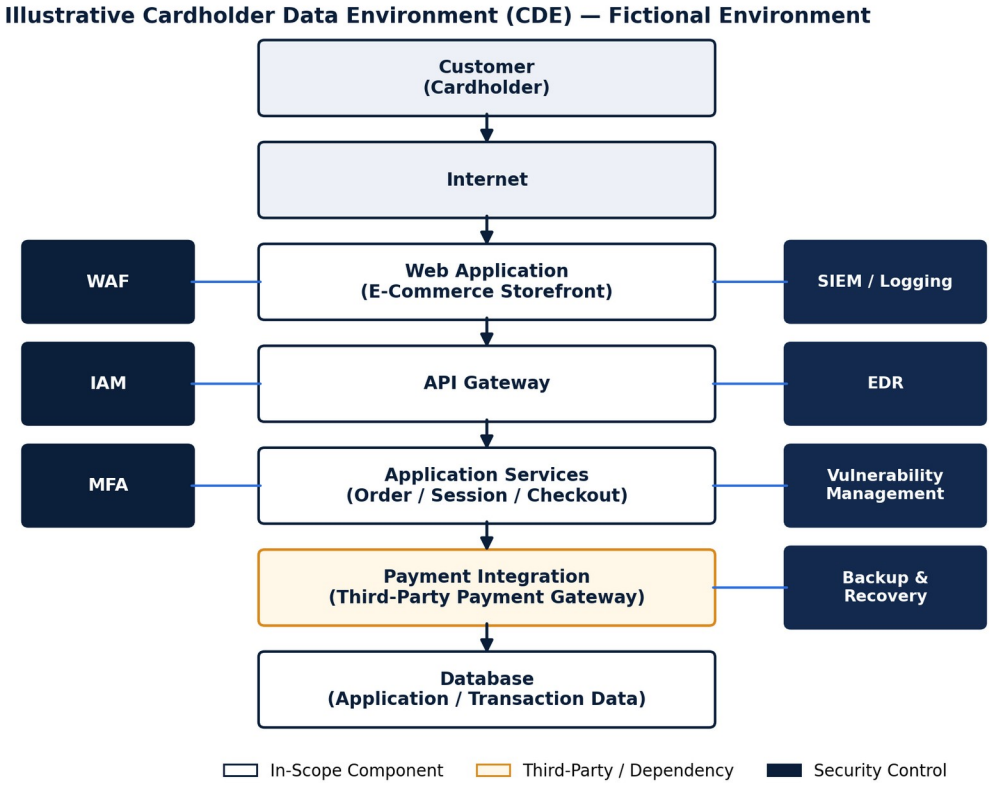
Component	Description	Scope Determination
Internet-Facing E-Commerce Platform	Customer storefront, checkout, and account management functions.	IN SCOPE
Web Application	Front-end and server-side application logic supporting the storefront.	IN SCOPE
API Layer	REST APIs supporting order, session, and checkout services.	IN SCOPE
Database	Application, order, and transaction metadata stores.	IN SCOPE
Cloud Infrastructure	Illustrative cloud compute, storage, and networking supporting the CDE.	IN SCOPE
Administrative Access	Privileged / administrative access paths to in-scope systems.	IN SCOPE
Logging Infrastructure	Centralized log aggregation and SIEM supporting in-scope systems.	IN SCOPE
Vulnerability Management Program	Scanning, tracking, and remediation processes for in-scope assets.	IN SCOPE
Payment Integration	Third-party hosted payment gateway and tokenization service.	DEPENDENCY / THIRD PARTY
Security Monitoring (SOC/MDR)	Illustrative outsourced monitoring and detection service.	DEPENDENCY / THIRD PARTY
Employee Access	Corporate workstation and internal business-system access.	OUT OF SCOPE
Corporate HR / Payroll Systems	Human resources platforms with no CDE connectivity.	OUT OF SCOPE

Scope Validation Approach

Scope was fictionally validated through a combination of simulated network diagram review, data flow analysis, and personnel interviews, consistent with PCI DSS requirements to confirm the accuracy of the defined cardholder data environment prior to control testing.

07 ILLUSTRATIVE ARCHITECTURE DIAGRAM

The diagram below presents a fictional, representative architecture for SampleCompany.com's simulated cardholder data environment. It is provided to illustrate how TMG Security documents environment architecture and control placement in an actual assessment deliverable.



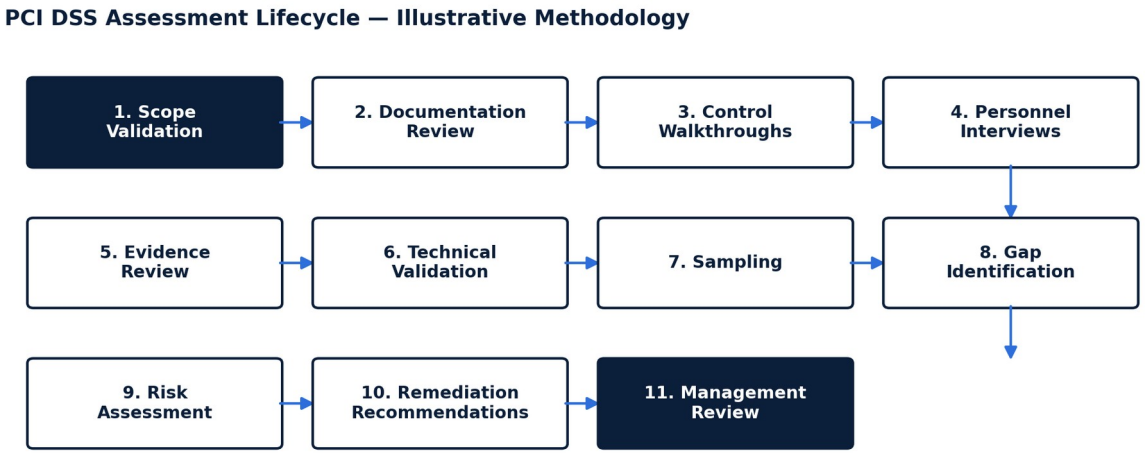
Illustrative Architecture — Fictional Environment. Not representative of any real system.

Diagram Notes

- WAF: Web Application Firewall positioned in front of the customer-facing web application.
- IAM / MFA: Identity and access management with multi-factor authentication for administrative paths.
- SIEM / Logging: Centralized log aggregation supporting Requirement 10 monitoring objectives.
- EDR: Endpoint detection and response deployed across illustrative servers and workloads.
- Payment Integration is shown as a third-party dependency outside SampleCompany.com's direct operational control.

08 ASSESSMENT METHODOLOGY

TMG Security applies a structured, repeatable methodology across every engagement. The eleven-stage lifecycle below (illustrated here in a fictional context) reflects the general approach TMG Security follows when performing a PCI DSS compliance or readiness assessment.



PCI DSS Assessment Lifecycle — Illustrative Methodology

Methodology Stages

1. Scope Validation	Confirm the boundary of the cardholder data environment and any connected systems.
2. Documentation Review	Review policies, standards, network diagrams, and data flow documentation.
3. Control Walkthroughs	Observe and walk through key controls with system and process owners.
4. Personnel Interviews	Interview control owners across IT, security, and business functions.
5. Evidence Review	Collect and evaluate artifacts supporting each control objective.
6. Technical Validation	Perform configuration reviews and technical checks against sampled systems.
7. Sampling	Apply a representative sampling methodology across system components and locations.
8. Gap Identification	Identify and document control gaps relative to PCI DSS v4.0.1 requirements.
9. Risk Assessment	Assign risk ratings to identified gaps based on likelihood and impact.
10. Remediation Recommendations	Develop actionable, prioritized remediation guidance for each finding.
11. Management Review	Present findings to management and align on ownership and timelines.

09 EVIDENCE & SAMPLING METHODOLOGY

ILLUSTRATIVE EVIDENCE EXAMPLES — NOT ACTUAL CLIENT EVIDENCE

The categories below represent the fictional classes of evidence referenced throughout this sample report. Each evidence identifier (EV-xxx) is used solely to demonstrate TMG Security's evidence referencing convention and evidence register structure; no actual documents or artifacts were collected.

Reference	Illustrative Evidence Category
EV-001	Information Security Policies
EV-002	Standard Operating Procedures
EV-003	Network & Data Flow Diagrams
EV-004	Asset Inventory Records
EV-005	User Access & Recertification Records
EV-006	Multi-Factor Authentication Configuration
EV-007	Vulnerability Scan Reports
EV-008	Penetration Test Reports
EV-009	Firewall & Network Security Control Configuration
EV-010	Logging & SIEM Configuration
EV-011	Incident Response Records
EV-012	Security Awareness Training Records
EV-013	Change Management Records
EV-014	Backup & Recovery Records

Sampling Approach

Where full-population testing was not practicable, a representative sampling methodology was applied consistent with common assessment practice: samples were selected to reasonably represent the population of in-scope system components, locations, and time periods, with sample sizes adjusted based on population size and control criticality. All sampling described in this report is fictional and provided to illustrate TMG Security's documented sampling approach.

10 PCI DSS REQUIREMENT OVERVIEW

The table below presents a fictional, sample-level summary of illustrative assessment status across all twelve PCI DSS v4.0.1 requirement areas. Detailed narrative for each requirement follows in Sections 11 through 20.

#	Requirement / Control Objective	Control Objective Summary	Assessment Focus	Illustrative Status
1	**Install and Maintain Network Security Controls**	Firewalls, network segmentation, and boundary defenses	Network security control configuration and rule review	Partially In Place
2	**Apply Secure Configurations to All System Components**	Hardened baselines and elimination of default settings	Configuration standards and default credential controls	In Place
3	**Protect Stored Account Data**	Minimization, encryption, and protection of stored data	Data retention, encryption, and key management practices	Partially In Place
4	**Protect Cardholder Data with Strong Cryptography During Transmission**	Encryption of cardholder data in transit over open, public networks	TLS configuration and certificate management	In Place
5	**Protect All Systems and Networks from Malicious Software**	Anti-malware and endpoint protection controls	EDR / anti-malware deployment and alerting	In Place
6	**Develop and Maintain Secure Systems and Software**	Secure SDLC, patching, and vulnerability management	Change management, code review, and vulnerability remediation	Not In Place
7	**Restrict Access to System Components and Cardholder Data**	Least privilege and role-based access control	Access provisioning, RBAC, and periodic access review	Partially In Place
8	**Identify Users and Authenticate Access to System Components**	Unique identities and strong authentication	Authentication mechanisms, MFA, and password controls	In Place
9	**Restrict Physical Access to Cardholder Data**	Physical safeguards over in-scope facilities and media	Physical access controls, CCTV, and visitor management	In Place
10	**Log and Monitor All Access to System Components and Cardholder Data**	Centralized logging, monitoring, and audit trails	Logging configuration, retention, and SIEM alerting	In Place
11	**Test Security of Systems and Networks Regularly**	Ongoing vulnerability and penetration testing	Scanning cadence, penetration testing, and segmentation testing	In Place
12	**Support Information Security with Organizational Policies and Programs**	Governance, risk management, and security awareness	Policy framework, risk management, and incident response program	In Place

11 REQUIREMENT 1 — INSTALL AND MAINTAIN NETWORK SECURITY CONTROLS

Objective

To evaluate whether network security controls (NSCs), including firewalls and equivalent technologies, are implemented and maintained to protect the fictional cardholder data environment from untrusted networks, consistent with PCI DSS v4.0.1 Requirement 1.

Controls Reviewed

- Firewall and network security control rule sets protecting the simulated CDE boundary.
- Network segmentation controls separating the CDE from the corporate network.
- Change control process governing modifications to network security control rules.
- SampleCompany.com's internal NSC rule review cadence (performed quarterly).

Sample Evidence Referenced

EV-003 Network & Data Flow Diagrams; EV-009 Firewall & Network Security Control Configuration; EV-013 Change Management Records. (Illustrative Evidence Reference — No Actual Client Evidence)

ILLUSTRATIVE ASSESSMENT STATUS: PARTIALLY IN PLACE

Observations

- SampleCompany.com has defined a quarterly internal NSC rule review cadence, which is stricter than the PCI DSS v4.0.1 minimum periodic review expectation of once every six months (Requirement 1.2.7). A sample of firewall rules reviewed, however, included entries without a clearly documented business justification or defined owner, indicating that the internal quarterly review was not consistently evidenced for all sampled rule sets.
- Network segmentation testing evidence was available for the primary CDE boundary; however, evidence of segmentation testing frequency aligned to the organization's defined testing methodology was incomplete for one sampled connection point.

Related Finding

PCI-NSC-001 — Network Security Control Rule Set Contains Undocumented Legacy Rules

PCI DSS Reference: Requirement 1.2.5 / 1.2.7 | Illustrative Assessment Status: Partially In Place

Risk

Undocumented or unjustified NSC rules increase the risk of unintended network access paths into the cardholder data environment and complicate ongoing rule set maintenance and review.

Recommendations

- Formally evidence each internal quarterly NSC rule review, including documented business justification and a defined owner for every active rule.
- Remove or formally re-justify legacy rules identified as lacking current business need.
- Extend segmentation testing evidence to cover all defined CDE boundary connection points on the documented testing cadence.

12 REQUIREMENT 2 — APPLY SECURE CONFIGURATIONS TO ALL SYSTEM COMPONENTS

Objective

To evaluate whether system components are configured and managed securely, including the elimination of vendor-supplied default accounts, passwords, and unnecessary services, consistent with PCI DSS v4.0.1 Requirement 2.

Controls Reviewed

- Documented secure configuration standards for sampled system component types.
- Vendor-supplied default account and password elimination process.
- System hardening baselines applied to in-scope servers and network devices.
- Configuration management and drift-detection tooling.
- Administrative access configuration for in-scope system components.

Sample Evidence Referenced

EV-002 Standard Operating Procedures; EV-004 Asset Inventory Records; EV-009 Firewall & Network Security Control Configuration. (Illustrative Evidence Reference — No Actual Client Evidence)

ILLUSTRATIVE ASSESSMENT STATUS: IN PLACE

Observations

- Secure configuration standards were current and mapped to CIS-aligned baselines for the majority of sampled system types.
- A single fictional cloud service deployed during the assessment period was not yet reflected in the current configuration standard, though compensating hardening had been applied manually.

Related Finding

PCI-CFG-002 — Secure Configuration Standard Not Updated for Newly Deployed Cloud Service

PCI DSS Reference: Requirement 2.2.1 | Illustrative Assessment Status: Partially In Place

Risk

Configuration standards that lag newly deployed technology increase the likelihood of inconsistent hardening being applied to new system components over time.

Recommendations

- Update the secure configuration standard library to formally include the newly deployed cloud service category.
- Incorporate a configuration-standard-update checkpoint into the change management process for new technology deployments.

13 REQUIREMENT 3 — PROTECT STORED ACCOUNT DATA

Objective

To evaluate whether stored account data is protected through data minimization, organization-defined retention and disposal, strong cryptography, and appropriate key management, consistent with PCI DSS v4.0.1 Requirement 3.

Controls Reviewed

- Data retention and disposal policy applicable to stored account data.
- Encryption methodology applied to any stored sensitive authentication or account data.
- Cryptographic key management lifecycle, including generation, rotation, and retirement.
- Access restrictions limiting stored account data visibility to authorized roles.

Sample Evidence Referenced

EV-001 Information Security Policies; EV-005 User Access & Recertification Records. (Illustrative Evidence Reference — No Actual Client Evidence)

ILLUSTRATIVE ASSESSMENT STATUS: PARTIALLY IN PLACE

Observations

- PCI DSS v4.0.1 Requirement 3.2.1 requires the organization to define and implement data retention and disposal based on legal, regulatory, and business need; PCI DSS does not itself specify a universal maximum retention period. SampleCompany.com has defined its own retention policy; however, a sample of archived transaction records was found to exceed that organization-defined retention period prior to disposal.
- Encryption of data at rest for in-scope data stores was confirmed as implemented using industry-standard algorithms.

Related Finding

PCI-DAT-003 — Archived Account Data Retained Beyond Organization-Defined Retention Period

PCI DSS Reference: Requirement 3.2.1 | Illustrative Assessment Status: Partially In Place

Risk

Retaining account data beyond the organization's own defined business need unnecessarily expands the data footprint available to a potential attacker and increases the impact of any future data exposure event.

Recommendations

- Implement an automated data lifecycle and disposal process aligned to SampleCompany.com's documented retention policy.
- Perform a one-time cleanup of archived records currently exceeding the defined retention period.
- Add retention-period compliance as a recurring item in the quarterly data governance review.

14 REQUIREMENT 4 — PROTECT CARDHOLDER DATA WITH STRONG CRYPTOGRAPHY DURING TRANSMISSION

Objective

To evaluate whether cardholder data is protected with strong cryptography during transmission over open, public networks, consistent with PCI DSS v4.0.1 Requirement 4.

Controls Reviewed

- TLS configuration for public-facing endpoints handling account data or session tokens.
- Certificate management process, including issuance, renewal, and revocation.
- Enforcement of secure protocol versions and disabling of deprecated protocols and cipher suites.
- Transmission encryption for internal traffic carrying account data between in-scope components.

Sample Evidence Referenced

EV-009 Firewall & Network Security Control Configuration; EV-010 Logging & SIEM Configuration. (Illustrative Evidence Reference — No Actual Client Evidence)

ILLUSTRATIVE ASSESSMENT STATUS: IN PLACE

Observations

- TLS 1.2 and above was enforced across all sampled primary customer-facing endpoints, with strong cipher suite configuration confirmed during technical validation.
- A legacy internal endpoint outside the cardholder data environment (CDE) was observed to permit an older cipher suite. Because the endpoint does not store, process, or transmit cardholder data, it falls outside the scope of this requirement and is tracked separately as an internal security observation, not a PCI DSS Requirement 4 gap (see Section 22).

Risk

No PCI DSS Requirement 4 risk was identified; all sampled CDE-connected transmission paths enforced TLS 1.2 or higher with approved cipher suites.

Recommendations

- As a general hardening practice outside the PCI DSS scope, update the legacy internal endpoint's TLS configuration to the organization's approved standard.
- Consider extending the internal (non-CDE) configuration review cycle to cover this endpoint category.

15 REQUIREMENT 5 — PROTECT ALL SYSTEMS AND NETWORKS FROM MALICIOUS SOFTWARE

Objective

To evaluate whether systems are protected from malicious software through anti-malware and endpoint detection and response (EDR) controls, with appropriate monitoring and alerting, consistent with PCI DSS v4.0.1 Requirement 5.

Controls Reviewed

- EDR / anti-malware deployment coverage across in-scope servers and endpoints.
- Malware signature and detection-engine update frequency.
- Alerting and escalation workflow for detected malicious activity.
- Anti-malware audit log retention configuration, consistent with Requirement 10.5.1.

Sample Evidence Referenced

EV-010 Logging & SIEM Configuration; EV-011 Incident Response Records. (Illustrative Evidence Reference — No Actual Client Evidence)

ILLUSTRATIVE ASSESSMENT STATUS: IN PLACE

Observations

- EDR coverage was confirmed across 100% of sampled in-scope servers and endpoints, with centralized alerting integrated into the SOC monitoring workflow.
- A sample review of EDR / anti-malware audit log configuration found that logs for a subset of sampled endpoints were not retained for the full period required under Requirement 10.5.1.

Related Finding

PCI-MAL-005 — Anti-Malware Audit Logs Not Consistently Retained in Accordance with Requirement 10.5.1

PCI DSS Reference: Requirement 5.3.4 | Illustrative Assessment Status: Partially In Place

Risk

Insufficient anti-malware audit log retention could limit the organization's ability to investigate and reconstruct malicious activity following a suspected incident.

Recommendations

- Extend anti-malware audit log retention configuration to align with Requirement 10.5.1 across all in-scope endpoints.
- Add anti-malware log retention verification to the periodic SIEM health review.

16 REQUIREMENT 6 — DEVELOP AND MAINTAIN SECURE SYSTEMS AND SOFTWARE

Objective

To evaluate whether SampleCompany.com develops and maintains secure systems and software through a secure development lifecycle, structured change management, and timely vulnerability remediation, consistent with PCI DSS v4.0.1 Requirement 6.

Controls Reviewed

- Secure software development lifecycle (SDLC) process, including security requirements and code review.
- Change management process governing production application and infrastructure changes.
- Vulnerability management program, including scanning cadence and remediation tracking.
- Patch management process for operating systems, application frameworks, and third-party dependencies.
- Application security testing coverage for in-scope, customer-facing applications.
- Third-party and open-source dependency management practices.

Sample Evidence Referenced

EV-007 Vulnerability Scan Reports; EV-008 Penetration Test Reports; EV-013 Change Management Records. (Illustrative Evidence Reference — No Actual Client Evidence)

ILLUSTRATIVE ASSESSMENT STATUS: NOT IN PLACE

Observations

- A secure SDLC process and peer code review requirement were documented and evidenced for sampled application changes.
- A fictional sample review identified that remediation tracking for certain vulnerabilities was not consistently documented against defined remediation timelines, with several sampled findings lacking clear ownership or current status.

Related Finding

PCI-SD-006 — Incomplete Vulnerability Remediation Tracking

PCI DSS Reference: Requirement 6.3.1 / 6.3.3 | Illustrative Assessment Status: Not In Place

Risk

Potential exposure to known vulnerabilities and increased risk of compromise due to inconsistent tracking of remediation activity against defined, risk-based timelines.

Recommendations

- Implement centralized vulnerability remediation tracking with defined ownership, risk-based remediation timelines, validation, and management reporting.
- Establish a recurring management review of open vulnerabilities aged beyond their defined remediation timeline.
- Validate closure evidence (e.g., rescan confirmation) for all vulnerabilities marked as remediated.

17 REQUIREMENTS 7 & 8 — ACCESS CONTROL & AUTHENTICATION

Objective

Requirement 7 evaluates whether access to system components and cardholder data is restricted to only those individuals with a legitimate business need. Requirement 8 evaluates whether each user is assigned a unique identity and access is authenticated through appropriately strong mechanisms. Both are evaluated against PCI DSS v4.0.1.

Control Matrix

Control Area	Requirement 7 — Restrict Access	Requirement 8 — Identify & Authenticate
Role-Based Access Control (RBAC)	Formal RBAC model defined for in-scope systems	N/A
Least Privilege	Access provisioned per defined job role	N/A
Multi-Factor Authentication	N/A	MFA enforced for all administrative and remote access
Privileged Access Management	Privileged accounts inventoried and reviewed	Privileged session activity logged
Password Controls	N/A	Password policy aligned to PCI DSS v4.0.1 minimums
User Lifecycle Management	Joiner / mover / leaver process defined	Account deactivation within defined SLA
Service Accounts	Service account inventory maintained	Service account credentials rotated periodically

Sample Evidence Referenced

EV-005 User Access & Recertification Records; EV-006 Multi-Factor Authentication Configuration. (Illustrative Evidence Reference — No Actual Client Evidence)

ILLUSTRATIVE ASSESSMENT STATUS: PARTIALLY IN PLACE

Observations

- MFA enforcement was confirmed for 100% of sampled administrative and remote access accounts, consistent with the documented policy.
- SampleCompany.com performs access reviews on a quarterly internal cadence, which is stricter than the PCI DSS v4.0.1 minimum of once every six months (Requirement 7.2.4). Recertification sign-off documentation was, however, incomplete for a subset of sampled application accounts during the most recent quarterly cycle.

Related Finding

PCI-IAM-007 — Quarterly User Access Review Evidence Incomplete for Sampled Accounts

PCI DSS Reference: Requirement 7.2.4 | Illustrative Assessment Status: Partially In Place

Risk

Incomplete access review evidence increases the likelihood that access no longer aligned with an individual's current job role goes undetected, contrary to the principle of least privilege.

Recommendations

- Formalize a documented sign-off workflow for each quarterly access recertification cycle, retained as auditable evidence.
- Extend recertification tracking to cover 100% of in-scope application and system accounts.

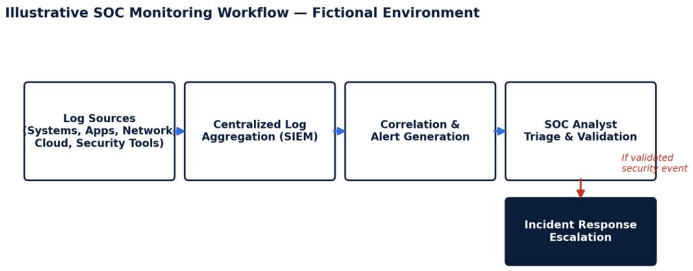
18 REQUIREMENTS 9 & 10 — PHYSICAL ACCESS & LOGGING

Objective

Requirement 9 evaluates physical access restrictions over facilities, media, and devices associated with the cardholder data environment. Requirement 10 evaluates whether access to system components and cardholder data is logged and monitored. Both are evaluated against PCI DSS v4.0.1.

Controls Reviewed

- Physical access controls (badge access, visitor management, CCTV coverage) for the illustrative data center facility.
- Media handling and destruction procedures for physical assets containing sensitive data.
- Centralized log aggregation (SIEM) covering in-scope system components.
- Audit log retention configuration and alerting rule coverage.



Illustrative SOC Monitoring Workflow — Fictional Environment

Sample Evidence Referenced

EV-010 Logging & SIEM Configuration; EV-011 Incident Response Records. (Illustrative Evidence Reference — No Actual Client Evidence)

ILLUSTRATIVE ASSESSMENT STATUS: IN PLACE

Observations

- Physical access to the illustrative primary facility was appropriately restricted, with CCTV retention and visitor logging confirmed for the sampled period.
- PCI DSS v4.0.1 Requirement 10.5.1 requires audit log history retained at least 12 months, with the most recent 3 months immediately available. SampleCompany.com's internal policy separately targets 12-month retention for all in-scope systems; retention configuration was, however, inconsistent across a small number of sampled components relative to both the PCI DSS minimum and internal policy.

Related Finding

PCI-LOG-008 — Audit Log Retention Configuration Inconsistent Across Sampled Systems

PCI DSS Reference: Requirement 10.5.1 | Illustrative Assessment Status: Partially In Place

Risk

Inconsistent log retention reduces the organization's ability to support a full forensic investigation window, or immediate access to the most recent three months of activity, in the event of a suspected security incident.

Recommendations

- Standardize log retention configuration across all in-scope system components to meet both the PCI DSS v4.0.1 minimum and the organization's internal policy.
- Include log retention configuration as a checkpoint within the periodic SIEM health review.

19 REQUIREMENT 11 — TEST SECURITY OF SYSTEMS AND NETWORKS REGULARLY

Objective

To evaluate whether SampleCompany.com regularly tests security systems, processes, and network segmentation to identify and remediate vulnerabilities in a timely manner, consistent with PCI DSS v4.0.1 Requirement 11.

Controls Reviewed

- Internal and external vulnerability scanning cadence and remediation follow-through.
- Annual internal and external penetration testing coverage and scope.
- Segmentation testing methodology and frequency for the CDE boundary.
- Intrusion detection / prevention system (IDS/IPS) coverage and validation.

Sample Testing Schedule (Fictional)

Testing Activity	Frequency	Last Performed (Fictional)	Status
Internal Vulnerability Scanning	Quarterly	Jul 2026	On Schedule
External Vulnerability Scanning (ASV)	Quarterly	Jul 2026	On Schedule
Internal Penetration Testing	Annual	Mar 2026	On Schedule
External Penetration Testing	Annual	Mar 2026	On Schedule
Segmentation Testing	At least every 12 months	Feb 2026	On Schedule
IDS / IPS Validation	Annual	Jan 2026	On Schedule

Sample Evidence Referenced

EV-007 Vulnerability Scan Reports; EV-008 Penetration Test Reports. (Illustrative Evidence Reference — No Actual Client Evidence)

ILLUSTRATIVE ASSESSMENT STATUS: IN PLACE

Observations

- Vulnerability scanning and penetration testing were performed on schedule and covered the defined in-scope population.
- Segmentation testing was completed within the PCI DSS v4.0.1 Requirement 11.4.5 testing frequency. Formal management review and sign-off of the results had not yet occurred at the time of sampling; because Requirement 11.4.5 does not itself require management sign-off, this is tracked separately as an internal governance observation, not a Requirement 11.4.5 gap (see Section 22).

Risk

No PCI DSS Requirement 11 risk was identified; all sampled scanning, penetration testing, and segmentation testing activity was completed within the required PCI DSS v4.0.1 testing frequency.

Recommendations

- As a general governance practice outside the PCI DSS scope, formalize a management review and sign-off step following each segmentation test.

20 REQUIREMENT 12 — SUPPORT INFORMATION SECURITY WITH ORGANIZATIONAL POLICIES AND PROGRAMS

Objective

To evaluate whether SampleCompany.com maintains an organization-wide information security policy and supporting program, including risk management, security awareness, incident response, and third-party risk oversight, consistent with PCI DSS v4.0.1 Requirement 12.

Controls Reviewed

- Information security policy suite, ownership, and annual review cycle.
- Enterprise risk management process and risk register.
- Security awareness training program, content, and completion tracking.
- Incident response plan, including defined roles and tabletop exercise cadence.
- Third-party / service provider risk management program.
- Annual PCI DSS scope confirmation and program governance review.

Sample Evidence Referenced

EV-001 Information Security Policies; EV-011 Incident Response Records; EV-012 Security Awareness Training Records. (Illustrative Evidence Reference — No Actual Client Evidence)

ILLUSTRATIVE ASSESSMENT STATUS: IN PLACE

Observations

- The information security policy suite was current, formally approved, and reviewed within the defined annual cycle.
- Security awareness training completion was confirmed for sampled personnel; however, completion tracking was maintained manually rather than through a centralized learning management system.

Related Finding

PCI-GOV-010 — Security Awareness Training Completion Not Centrally Tracked

PCI DSS Reference: Requirement 12.6.3 | Illustrative Assessment Status: Observation

Risk

Manual tracking of training completion increases administrative burden and the risk of incomplete population coverage going undetected.

Recommendations

- Adopt a centralized learning management system to track security awareness training completion and automate reminder escalation.

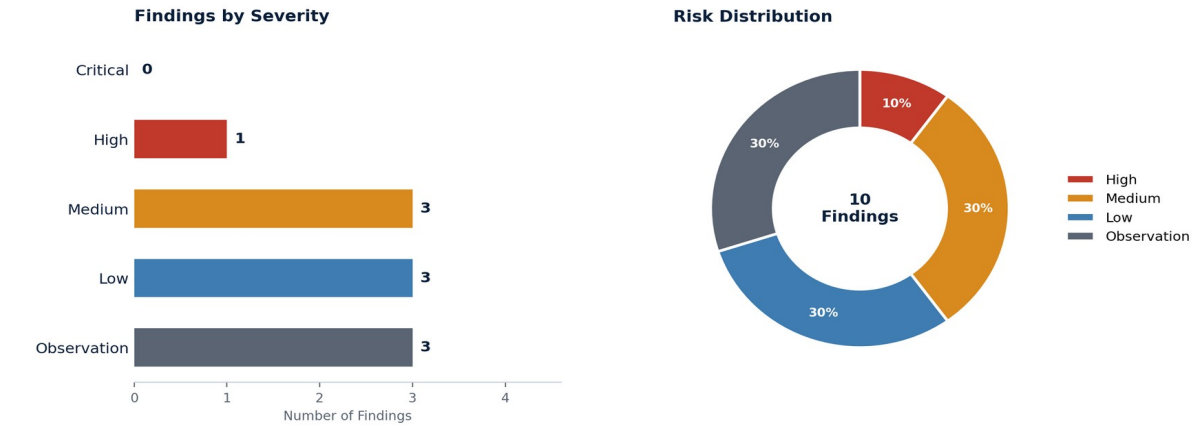
21 FINDINGS SUMMARY

FICTIONAL SAMPLE RESULTS — ILLUSTRATIVE DATA ONLY

This fictional sample assessment produced a total of 10 illustrative findings across the twelve PCI DSS v4.0.1 requirement areas assessed. The dashboard below summarizes findings by severity for demonstration purposes; illustrative assessment status by requirement domain is presented in Section 4.

0	1	3	3	3
Critical	High	Medium	Low	Observations

Fictional Sample Findings Dashboard — Illustrative Data Only



Fictional Sample Findings Dashboard — Illustrative Data Only

Interpretation

No critical-severity findings were recorded in this fictional scenario. One high-severity finding was identified relating to vulnerability remediation tracking (Requirement 6). Medium-severity findings were distributed across network security, data retention, and access review domains. Low-severity findings and observations reflect minor process and documentation gaps that, while not urgent, warrant remediation to strengthen overall control maturity.

22 DETAILED FINDINGS

Every fictional sample finding is presented below in full consulting-format detail: control objective, criteria, condition, cause, risk/business impact, evidence reference, recommendation, management response, owner, target date, and status. All findings, evidence, and management responses on this page are entirely fictional.

ILLUSTRATIVE EVIDENCE REFERENCE — NO ACTUAL CLIENT EVIDENCE

PCI-SD-006 — Incomplete Vulnerability Remediation Tracking	HIGH
PCI DSS Requirement: Requirement 6.3.1 / 6.3.3	**Illustrative Assessment Status: Not In Place**
Control Objective	Security vulnerabilities affecting in-scope system components are identified, ranked by risk, and remediated within defined timeframes.
Criteria	PCI DSS v4.0.1 Requirement 6.3.1 requires that security vulnerabilities be identified, evaluated, and assigned a risk ranking. Requirement 6.3.3 requires that applicable security patches/updates be installed within defined timeframes based on that risk ranking: patches/updates addressing critical vulnerabilities must be installed within one month of release, while all other applicable security patches/updates must be installed within a timeframe appropriate to the organization's risk assessment.
Condition	A fictional sample review of vulnerability scan output found that remediation activity for several sampled vulnerabilities was not consistently logged against a defined remediation timeline.
Cause	No centralized, single system of record existed for vulnerability remediation tracking; ownership and due dates were maintained inconsistently across teams.
Risk / Business Impact	Potential exposure to known, exploitable vulnerabilities for longer than the organization's intended remediation window, increasing the likelihood of compromise.
Evidence Reference	*EV-007 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Implement centralized vulnerability remediation tracking with defined ownership, risk-based remediation timelines, closure validation (e.g., rescan confirmation), and recurring management reporting.
Management Response	*Agreed. Vulnerability remediation tracking will be centralized in the GRC platform with defined SLAs and monthly management reporting.*
Owner / Target Date / Status	**Application Security Lead** | 24 Sep 2026 | **Open**

PCI-NSC-001 — Network Security Control Rule Set Contains Undocumented Legacy Rules	MEDIUM
PCI DSS Requirement: Requirement 1.2.5 / 1.2.7	**Illustrative Assessment Status: Partially In Place**
Control Objective	Network security control (NSC) rule sets permit only necessary, documented, and business-justified traffic into and out of the cardholder data environment.
Criteria	PCI DSS v4.0.1 Requirement 1.2.5 requires all services, protocols, and ports allowed to be identified, approved, and have a defined business need; Requirement 1.2.7 requires NSC configurations to be reviewed at least once every six months to confirm they remain relevant and effective.
Condition	A sample of NSC rules reviewed included entries without a documented business justification or defined owner.
Cause	SampleCompany.com has defined a quarterly internal NSC rule review cadence, which is stricter than the PCI DSS v4.0.1 minimum six-month review expectation; however, this internal review was not consistently evidenced for all sampled rule sets, allowing legacy entries to persist.
Risk / Business Impact	Undocumented or unjustified rules increase the risk of unintended network access paths into the cardholder data environment and complicate ongoing rule set maintenance.
Evidence Reference	*EV-009 (Illustrative Evidence Reference — No Actual Client Evidence)*

Recommendation	Formally evidence each internal quarterly NSC rule review, including documented business justification and owner for every active rule. Remove or re-justify legacy rules lacking current business need.
Management Response	*Agreed. Legacy rule cleanup will be completed and the quarterly internal review will be formally documented and retained as evidence.*
Owner / Target Date / Status	**Network Engineering Lead** | 24 Sep 2026 | **Open**

PCI-DAT-003 — Archived Account Data Retained Beyond Organization-Defined Retention Period	**MEDIUM**
PCI DSS Requirement: Requirement 3.2.1	**Illustrative Assessment Status: Partially In Place**
Control Objective	Storage of account data is minimized to what is required for legal, regulatory, and business purposes, with data securely disposed of once no longer needed.
Criteria	PCI DSS v4.0.1 Requirement 3.2.1 requires the organization to define and implement data retention and disposal policies, procedures, and processes based on legal, regulatory, and business requirements; PCI DSS does not itself define a universal maximum retention period.
Condition	A sample of archived transaction records was found to exceed SampleCompany.com's own documented retention period prior to disposal.
Cause	The automated disposal job supporting the archival data store was not consistently executed, allowing records to persist beyond the organization's defined retention window.
Risk / Business Impact	Retaining account data beyond the organization's own defined business need unnecessarily expands the data footprint available to a potential attacker and increases the impact of any future exposure event.
Evidence Reference	*EV-001 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Implement an automated, monitored data lifecycle and disposal process aligned to SampleCompany.com's documented retention policy, and perform a one-time cleanup of records currently exceeding the defined window.
Management Response	*Agreed. Automated data lifecycle management will be implemented and monitored, with a one-time cleanup of aged records.*
Owner / Target Date / Status	**Security Manager** | 22 Oct 2026 | **Open**

PCI-IAM-007 — Quarterly User Access Review Evidence Incomplete for Sampled Accounts	**MEDIUM**
PCI DSS Requirement: Requirement 7.2.4	**Illustrative Assessment Status: Partially In Place**
Control Objective	User accounts and associated access privileges are periodically reviewed to confirm continued alignment with job function and business need.
Criteria	PCI DSS v4.0.1 Requirement 7.2.4 requires that all user accounts and related access privileges be reviewed at least once every six months to ensure access remains appropriate.
Condition	SampleCompany.com performs access reviews on a quarterly internal cadence, which is stricter than the PCI DSS v4.0.1 minimum; however, recertification sign-off documentation was incomplete for a subset of sampled application accounts during the most recent quarterly cycle.
Cause	The access recertification workflow relied on manual email sign-off rather than a tracked, auditable workflow, resulting in incomplete record-keeping for some reviewers.
Risk / Business Impact	Access no longer aligned with an individual's current job role may go undetected, weakening enforcement of least privilege.
Evidence Reference	*EV-005 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Formalize a documented, system-tracked sign-off workflow for each quarterly access recertification cycle, retained as auditable evidence, and extend coverage to 100% of in-scope accounts.
Management Response	*Agreed. Access review sign-off will be formalized within the IAM platform's certification workflow.*
Owner / Target Date / Status	**IT Operations** | 22 Oct 2026 | **Open**

PCI-CFG-002 — Secure Configuration Standard Not Updated for Newly Deployed Cloud Service	LOW
PCI DSS Requirement: Requirement 2.2.1	**Illustrative Assessment Status: Partially In Place**
Control Objective	Configuration standards are developed, maintained, and applied to all system component types to address known security parameters.
Criteria	PCI DSS v4.0.1 Requirement 2.2.1 requires configuration standards to be developed, implemented, and maintained to cover all in-scope system component types.
Condition	A newly deployed cloud service category was not yet reflected in the current secure configuration standard, though manual compensating hardening had been applied.
Cause	The change management process did not include a checkpoint requiring the configuration standard library to be updated when a new technology category is introduced.
Risk / Business Impact	Increased likelihood of inconsistent hardening being applied to future deployments of the same service type.
Evidence Reference	*EV-002 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Update the configuration standard library to formally include the new cloud service category, and add a standard-update checkpoint to the change management process for new technology deployments.
Management Response	*Agreed. The configuration standard library will be updated and the change process amended.*
Owner / Target Date / Status	**IT Operations** | 22 Oct 2026 | **Open**

PCI-MAL-005 — Anti-Malware Audit Logs Not Consistently Retained in Accordance with Requirement 10.5.1	LOW
PCI DSS Requirement: Requirement 5.3.4	**Illustrative Assessment Status: Partially In Place**
Control Objective	Anti-malware mechanisms generate audit logs that are enabled and retained consistent with Requirement 10.5.1, supporting detection and forensic analysis of malicious activity.
Criteria	PCI DSS v4.0.1 Requirement 5.3.4 requires that audit logs for anti-malware mechanisms be enabled and retained in accordance with Requirement 10.5.1.
Condition	A sample review of EDR / anti-malware audit log configuration found that logs for a subset of sampled endpoints were not retained for the full period required under Requirement 10.5.1.
Cause	Anti-malware audit log retention settings were not included in the same retention-configuration baseline applied to centralized SIEM logs, resulting in a shorter retention window on a subset of endpoints.
Risk / Business Impact	Insufficient anti-malware audit log retention could limit the organization's ability to investigate and reconstruct malicious activity following a suspected incident.
Evidence Reference	*EV-010 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Extend the anti-malware audit log retention configuration to align with Requirement 10.5.1 across all in-scope endpoints, and add retention verification to the periodic SIEM health review.
Management Response	*Agreed. Anti-malware audit log retention will be aligned to the Requirement 10.5.1 standard across all in-scope endpoints.*
Owner / Target Date / Status	**SOC Manager** | 21 Nov 2026 | **Open**

PCI-LOG-008 — Audit Log Retention Configuration Inconsistent Across Sampled Systems	LOW
PCI DSS Requirement: Requirement 10.5.1	**Illustrative Assessment Status: Partially In Place**

Control Objective	Audit log history is retained for a period sufficient to support incident response and forensic analysis.
Criteria	PCI DSS v4.0.1 Requirement 10.5.1 requires audit log history to be retained for at least 12 months, with logs for the most recent three months immediately available for analysis. SampleCompany.com's internal logging policy separately specifies a 12-month retention target for all in-scope systems.
Condition	Log retention configuration was inconsistent across a small number of sampled system components relative to both the PCI DSS v4.0.1 minimum and the organization's internal 12-month policy.
Cause	A subset of systems onboarded to the SIEM after the initial logging standard was published had not been reconciled against the current retention configuration baseline.
Risk / Business Impact	Reduced ability to support a full 12-month forensic investigation window, or immediate access to the most recent three months of activity, in the event of a suspected incident.
Evidence Reference	*EV-010 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Standardize log retention configuration across all in-scope components to meet both the PCI DSS v4.0.1 minimum and SampleCompany.com's internal policy, and add retention verification to the periodic SIEM health review.
Management Response	*Agreed. Log retention will be standardized and added to the recurring SIEM health check.*
Owner / Target Date / Status	**SOC Manager** | 21 Nov 2026 | **Open**

PCI-TST-009 — Internal Security Observation — Segmentation Test Governance	**OBSERVATION**
PCI DSS Requirement: Not directly applicable — Informational	**Illustrative Assessment Status: Observation**
Control Objective	Segmentation testing results are formally reviewed, documented, and tracked through management governance processes to ensure identified issues are appropriately addressed.
Criteria	The segmentation penetration test itself was completed within the required PCI DSS testing frequency. PCI DSS Requirement 11.4.5 does not specifically require management sign-off of test results. The lack of formal management review is therefore treated as an internal governance and security-maturity observation rather than a PCI DSS compliance gap.
Condition	The most recent fictional segmentation test results had not yet been formally reviewed and signed off by management at the time of sampling, although the segmentation test itself had been completed within the required testing period.
Cause	No defined internal governance workflow or SLA existed for management review and sign-off following completion of segmentation testing.
Risk / Business Impact	Delayed management review may slow prioritization, ownership, and remediation of any issues identified through segmentation testing.
Evidence Reference	*EV-008 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Formalize a management review and sign-off step following each segmentation test, with documented ownership, review timelines, and tracking of any resulting remediation actions.
Management Response	*Agreed. A management review and sign-off step will be added to the segmentation testing governance workflow.*
Owner / Target Date / Status	**Security Manager** | 21 Nov 2026 | **Open**

PCI-TLS-004 — Internal Security Observation — Legacy TLS Configuration	**OBSERVATION**
PCI DSS Requirement: Not directly applicable — Informational	**Illustrative Assessment Status: Observation**
Control Objective	Internal, non-cardholder-data-environment endpoints are maintained on current, supported transport security configurations as a matter of general security hygiene.
Criteria	This item is not mapped to a specific PCI DSS v4.0.1 requirement. The affected endpoint does not store, process, or transmit account data and falls outside the cardholder data environment (CDE) and connected-systems scope; it is reported as an internal security observation to demonstrate security maturity beyond the defined PCI DSS assessment scope.

Condition	A legacy, non-customer-facing internal endpoint was observed to permit an older TLS cipher suite outside SampleCompany.com's approved internal standard. The endpoint does not store, process, or transmit cardholder data.
Cause	The endpoint was provisioned prior to the current internal TLS standard and had not been captured by the recurring external-facing TLS review scope, which is scoped to CDE-connected systems.
Risk / Business Impact	Minimal risk given the endpoint's non-critical role and its position outside the CDE; represents a general configuration hygiene item rather than a PCI DSS control gap.
Evidence Reference	*EV-009 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Update the endpoint's TLS configuration to the organization's approved internal standard and consider extending the internal (non-CDE) systems inventory to periodic configuration review.
Management Response	*Agreed. Endpoint TLS configuration will be updated as a general hardening item outside the PCI DSS assessment scope.*
Owner / Target Date / Status	**Network Engineering Lead** | 21 Nov 2026 | **Open**

PCI-GOV-010 — Security Awareness Training Completion Not Centrally Tracked	**OBSERVATION**
PCI DSS Requirement: Requirement 12.6.3	**Illustrative Assessment Status: Observation**
Control Objective	Personnel receive security awareness training and their completion is tracked to confirm full population coverage.
Criteria	PCI DSS v4.0.1 Requirement 12.6.3 requires personnel to receive security awareness training upon hire and at least once every 12 months, with content addressing relevant threats and acceptable use.
Condition	Security awareness training completion was confirmed for sampled personnel; however, completion tracking was maintained manually rather than through a centralized learning management system (LMS).
Cause	No centralized LMS had been procured; tracking relied on spreadsheet-based reporting maintained by HR and Compliance.
Risk / Business Impact	Increased administrative burden and risk that incomplete population coverage could go undetected.
Evidence Reference	*EV-012 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Adopt a centralized LMS to track training completion and automate reminder escalation for outstanding personnel.
Management Response	*Agreed. Centralized LMS evaluation will be completed and adopted.*
Owner / Target Date / Status	**Compliance Officer** | 21 Nov 2026 | **Open**

23 REMEDIATION ROADMAP

The fictional remediation roadmap below sequences remediation activity across a 90-day window, prioritizing the High- and Medium-severity sample findings for early closure.

Illustrative 90-Day Remediation Roadmap — Fictional Timeline

0–30 Days

- Remediate the High-severity finding: implement centralized vulnerability remediation tracking (PCI-SD-006).
- Complete recertification of privileged and administrative access across in-scope systems.

30–60 Days

- Complete logging and alerting configuration improvements across all sampled systems.
- Update information security policy and configuration standards to reflect current environment.
- Refresh security awareness training content and completion tracking approach.

60–90 Days

- Execute segmentation and network security control testing, including formal management review.
- Conduct an incident response tabletop exercise validating updated escalation procedures.
- Complete third-party / service provider risk review and annual governance program assessment.

24 MANAGEMENT ACTION PLAN

SampleCompany.com's fictional management team has reviewed and formally accepted each sample finding below, with defined ownership and target remediation dates. This table is synchronized with the Detailed Findings section (Section 22) and the Finding Register (Section 25).

Finding ID	Management Response	Owner	Target Date	Priority	Status
PCI-SD-006	Agreed. Vulnerability remediation tracking will be centralized in the GRC platform with defined SLAs and monthly management reporting.	Application Security Lead	24 Sep 2026	Priority 1	Open
PCI-NSC-001	Agreed. Legacy rule cleanup will be completed and the quarterly internal review will be formally documented and retained as evidence.	Network Engineering Lead	24 Sep 2026	Priority 2	Open
PCI-DAT-003	Agreed. Automated data lifecycle management will be implemented and monitored, with a one-time cleanup of aged records.	Security Manager	22 Oct 2026	Priority 2	Open
PCI-IAM-007	Agreed. Access review sign-off will be formalized within the IAM platform's certification workflow.	IT Operations	22 Oct 2026	Priority 2	Open
PCI-CFG-002	Agreed. The configuration standard library will be updated and the change process amended.	IT Operations	22 Oct 2026	Priority 3	Open
PCI-MAL-005	Agreed. Anti-malware audit log retention will be aligned to the Requirement 10.5.1 standard across all in-scope endpoints.	SOC Manager	21 Nov 2026	Priority 3	Open
PCI-LOG-008	Agreed. Log retention will be standardized and added to the recurring SIEM health check.	SOC Manager	21 Nov 2026	Priority 3	Open
PCI-TST-009	Agreed. A management review and sign-off step will be added to the segmentation testing governance workflow.	Security Manager	21 Nov 2026	Priority 4	Open
PCI-TLS-004	Agreed. Endpoint TLS configuration will be updated as a general hardening item outside the PCI DSS assessment scope.	Network Engineering Lead	21 Nov 2026	Priority 4	Open
PCI-GOV-010	Agreed. Centralized LMS evaluation will be completed and adopted.	Compliance Officer	21 Nov 2026	Priority 4	Open

25 FINAL ASSESSMENT & APPENDIX

Overall Assessment Conclusion

Based on the fictional evidence and simulated procedures described in this report, SampleCompany.com's environment is presented with an overall Illustrative Assessment Status of PARTIALLY IN PLACE for demonstration purposes.

This status is illustrative only. It is not an official PCI DSS compliance determination and does not constitute or substitute for a Report on Compliance (ROC) or Attestation of Compliance (AOC).

This conclusion, and every element of this report, is fictional and produced solely to demonstrate TMG Security's assessment methodology and reporting standards. It does not describe the actual security or compliance posture of any real organization.

Evidence Register (Illustrative)

ILLUSTRATIVE EVIDENCE REFERENCE — NO ACTUAL CLIENT EVIDENCE

Reference	Evidence Description	Type	Illustrative Owner
EV-001	Information Security Policies	Policy	Compliance Officer
EV-002	Standard Operating Procedures	Procedure	IT Operations
EV-003	Network & Data Flow Diagrams	Diagram	Network Engineering Lead
EV-004	Asset Inventory Records	Register	IT Operations
EV-005	User Access & Recertification Records	Access Records	Security Manager
EV-006	Multi-Factor Authentication Configuration	Configuration Export	IT Operations
EV-007	Vulnerability Scan Reports	Scan Report	Application Security Lead
EV-008	Penetration Test Reports	Test Report	Security Manager
EV-009	Firewall & Network Security Control Configuration	Configuration Export	Network Engineering Lead
EV-010	Logging & SIEM Configuration	Configuration Export	SOC Manager
EV-011	Incident Response Records	Program Records	Security Manager
EV-012	Security Awareness Training Records	Training Records	Compliance Officer
EV-013	Change Management Records	Change Tickets	IT Operations
EV-014	Backup & Recovery Records	Operational Records	IT Operations

Finding Register (Illustrative)

Illustrative Assessment Status reflects the sampled control condition underlying each finding; Remediation Status reflects fictional tracking of the corrective action itself. Both are synchronized with Section 4, Section 22, and Section 24.

ID	Title	Severity	PCI DSS Requirement	Illustrative Assessment Status	Remediation Status
PCI-SD-006	Incomplete Vulnerability Remediation Tracking	HIGH	Requirement 6	Not In Place	Open
PCI-NSC-001	Network Security Control Rule Set Contains Undocumented Legacy Rules	MEDIUM	Requirement 1	Partially In Place	Open
PCI-DAT-003	Archived Account Data Retained Beyond Organization-Defined Retention Period	MEDIUM	Requirement 3	Partially In Place	Open
PCI-IAM-007	Quarterly User Access Review Evidence Incomplete for Sampled Accounts	MEDIUM	Requirement 7	Partially In Place	Open
PCI-CFG-002	Secure Configuration Standard Not Updated for Newly Deployed Cloud Service	LOW	Requirement 2	Partially In Place	Open
PCI-MAL-005	Anti-Malware Audit Logs Not Consistently Retained in Accordance with Requirement 10.5.1	LOW	Requirement 5	Partially In Place	Open
PCI-LOG-008	Audit Log Retention Configuration Inconsistent Across Sampled Systems	LOW	Requirement 10	Partially In Place	Open

ID	Title	Severity	PCI DSS Requirement	Illustrative Assessment Status	Remediation Status
PCI-TST-009	Internal Security Observation — Segmentation Test Governance	OBSERVATION	Not Applicable	Observation	Open
PCI-TLS-004	Internal Security Observation — Legacy TLS Configuration	OBSERVATION	Not Applicable	Observation	Open
PCI-GOV-010	Security Awareness Training Completion Not Centrally Tracked	OBSERVATION	Requirement 12	Observation	Open

Assessment Limitations

This entire report — including its scope, methodology, evidence, findings, and conclusions — is a fictional construct created solely to demonstrate TMG Security's report structure, methodology, and reporting standards. The following limitations apply specifically to this sample document and distinguish it from an actual PCI DSS engagement deliverable:

- SampleCompany.com is a fictional organization. It does not correspond to any real company, and no real entity was assessed in the production of this document.
- No production environment, system, or network of any kind was accessed, scanned, or tested in the creation of this report.
- No actual evidence — including policies, configuration exports, screenshots, logs, or records — was collected, reviewed, or relied upon. All evidence references (EV-xxx) are illustrative placeholders only.
- No actual interviews or control walkthroughs were conducted with any personnel.
- No actual vulnerability scanning, configuration scanning, or automated technical testing was performed.
- No actual penetration testing or segmentation testing was performed.
- No formal PCI DSS validation activity — of any type, and by any assessor — was undertaken in connection with this document.
- No Report on Compliance (ROC), Attestation of Compliance (AOC), Self-Assessment Questionnaire (SAQ), or other PCI DSS validation artifact was issued, and this document does not constitute or substitute for one.
- TMG Security does not represent itself as a PCI SSC-certified Qualified Security Assessor (QSA) company in connection with this sample document unless separately and explicitly stated in writing.
- All findings, severities, illustrative assessment statuses, evidence references, dates, and management responses appearing in this report are fictional and illustrative, constructed to demonstrate TMG Security's reporting format and are not reflective of any real assessment outcome.

In an actual engagement, TMG Security would additionally disclose engagement-specific limitations such as sampling boundaries, reliance on client-provided information, and the point-in-time nature of assessment conclusions. This sample report is provided purely to illustrate that disclosure practice and carries no assurance value of its own.

Glossary of Terms

CDE	Cardholder Data Environment — the people, processes, and technology that store, process, or transmit account data.
PAN	Primary Account Number — the unique payment card number identifying the cardholder and issuer.
QSA	Qualified Security Assessor — an individual certified by the PCI Security Standards Council to perform PCI DSS assessments.
ROC	Report on Compliance — the detailed report documenting an entity's PCI DSS assessment results.
AOC	Attestation of Compliance — a formal declaration of an entity's PCI DSS compliance status.
SAQ	Self-Assessment Questionnaire — a validation tool for entities not required to undergo a full on-site assessment.
ASV	Approved Scanning Vendor — an organization approved by the PCI Security Standards Council to perform external vulnerability scanning.
SIEM	Security Information and Event Management — a platform for centralized log aggregation, correlation, and alerting.
EDR	Endpoint Detection and Response — technology that monitors and responds to threats on endpoint devices.
WAF	Web Application Firewall — a control that filters and monitors HTTP traffic to and from a web application.
MFA	Multi-Factor Authentication — authentication requiring two or more independent verification factors.
RBAC	Role-Based Access Control — an access model that assigns permissions based on defined organizational roles.

TLS	Transport Layer Security — a cryptographic protocol used to secure data in transit.
SOC	Security Operations Center — the function responsible for continuous security monitoring and incident response.
NSC	Network Security Control — a technology (e.g., firewall) that enforces network traffic policy.

"Offensive Security | GRC | SOC/MDR | vCISO | AI Security"

Web: www.tmgsec.com **Email:** security@tmgsec.com

USA Office: 117 South Lexington Street, STE 100, Harrisonville, MO 64701

Support: support@tmgsec.com | **Phone:** +1 (816) 793-1929 | **WhatsApp:** +1 (480) 680-0342

FICTIONAL SAMPLE REPORT — NOT AN ACTUAL PCI DSS CERTIFICATION OR ATTESTATION

This document was created by TMG Security to demonstrate report structure, methodology, and reporting standards. SampleCompany.com is fictional; no real assessment, certification, AOC, or ROC was performed or issued.