AiVRIC

Sample ROC evidence export

Document Purpose

This document describes how **AiVRIC** is used to align cloud and infrastructure controls with **PCI DSS v4.0 requirements** and generate **assessor-ready evidence artifacts** that support a formal **Report on Compliance (ROC)** conducted by a Qualified Security Assessor (QSA).

Included is a **Sample ROC Evidence Export**, representative of what AiVRIC produces to support PCI DSS assessments for cloud-based and hybrid environments.

Role of AiVRIC in PCI DSS Compliance

AiVRIC supports PCI DSS compliance by providing:

- Continuous technical validation of PCI DSS requirements
- Automated mapping of findings to PCI DSS controls
- Evidence collection across cloud services, identity, network, and storage
- Historical scan results to demonstrate control operation over time

AiVRIC **does not replace** the QSA or the official ROC.
Instead, it acts as a **continuous assurance and evidence-generation layer** that dramatically reduces assessment effort and audit friction.

PCI DSS Alignment Model

AiVRIC aligns to PCI DSS v4.0 across the following domains:

PCI DSS Requirement	AiVRIC Coverage
Req 1 – Network Security Controls	Firewall configs, segmentation, security group analysis
Req 2 – Secure Configurations	Baseline config validation, drift detection
Req 3 – Protect Stored CHD	Storage exposure, encryption validation
Req 4 – Protect CHD in Transit	TLS enforcement, insecure protocol detection

PCI DSS Requirement	AiVRIC Coverage
Req 5 – Protect Systems	Vulnerability discovery, misconfiguration detection
Req 6 – Secure Development	Cloud service configuration & exposure checks
Req 7 – Access Control	IAM permissions, least privilege enforcement
Req 8 – User Identification	MFA, credential hygiene, identity controls
Req 9 – Physical Security	Scope confirmation (process-based)
Req 10 – Logging & Monitoring	Log configuration validation
Req 11 – Testing	Continuous testing & historical evidence
Req 12 – Governance	Risk inputs into policy and oversight

Sample ROC Evidence Export

PCI DSS v4.0 – Supporting Documentation

Classification: Internal / Assessor Review
Generated By: AiVRIC Continuous Compliance Platform
Purpose: Support QSA-led ROC

---

1. Assessment Overview

Entity Name: Global Payments Corp
PCI Level: Level 1 Merchant
Assessment Standard: PCI DSS v4.0
Assessment Period: December 1–5, 2025
Evidence Export Date: December 9, 2025
QSA Firm: SecureAudit Partners LLC
ROC Reference ID: ROC-2025-GP-001247

Scope Summary

- Cardholder Data Environment (CDE)
- Supporting cloud infrastructure
- Network segmentation controls
- Identity and access management
- Logging and monitoring services

2. Executive Summary (ROC Support)

AiVRIC continuous scanning and validation confirmed that all **12 PCI DSS requirements** and **363 applicable sub-requirements** were:

- **In Place**
- **Operating Effectively**
- **Supported with verifiable technical evidence**

High-Level Metrics

Metric	Result
PCI Requirements Assessed	12 / 12
Sub-Requirements Validated	363 / 363
Locations Assessed	24 (Cloud & Physical)
Annual Transactions Supported	8.7M+

---

3. Detailed Requirement Evidence (Sample)

Requirement 1

Install and Maintain Network Security Controls

Status: ✅ In Place

AiVRIC validated network security controls protecting the CDE by analyzing firewall rules, cloud security groups, routing configurations, and segmentation boundaries.

1.1 – Processes for Network Security Controls

Sub-Requirement 1.1.1
Security policies and procedures are documented, approved, and communicated.

AiVRIC Evidence

- Policy references mapped to technical enforcement
- Configuration alignment validation

✅ Status: In Place

Sub-Requirement 1.1.2
Roles and responsibilities for network security are assigned.

AiVRIC Evidence

- IAM role analysis
- Ownership mapping to cloud accounts and services

✅ Status: In Place

Supporting Evidence Artifacts

The following artifacts were generated automatically or collected through AiVRIC scanning:

- network_security_groups.csv
- cloud_firewall_rules.json
- segmentation_validation_report.pdf
- iam_role_assignment_export.csv

Each artifact includes:

- Timestamp
- Resource identifier
- Region and account scope
- Scan reference ID

---

4. Scan Results Summary (Extract)

Resource	Control Area	Result	Severity
AWS VPC	Segmentation	Pass	Informational
IAM Policy	Access Control	Pass	Informational
Load Balancer	TLS Config	Pass	Informational
S3 Storage	Data Protection	Pass	Informational

No critical, high, or medium findings impacting PCI DSS scope were identified during the assessment window.

5. Evidence Handling & Traceability

All evidence produced by AiVRIC includes:

- Immutable scan timestamps
- Control mapping references (PCI Requirement & Sub-Requirement)
- Resource-level traceability
- Historical scan retention

This enables QSAs to:

- Perform walkthroughs efficiently
- Validate operating effectiveness
- Sample controls across time (v4.0 continuous requirements)

6. QSA Review & Attestation Support

This Evidence Export is intended to be reviewed by the assigned QSA and used as **supporting documentation** for:

- ROC completion
- Control validation
- Sampling confirmation
- Ongoing compliance assurance

Final compliance determination and attestation remain the responsibility of the QSA.

7. Continuous Compliance Advantage with AiVRIC

Using AiVRIC for PCI DSS enables organizations to move from:

Point-in-time PCI validation → Continuous PCI assurance

Key benefits include:

- Reduced assessment prep time
- Early detection of non-compliance drift
- Stronger v4.0 alignment
- Lower audit fatigue year-over-year

Document Control

- **Document Type:** ROC Supporting Evidence Export
- **Standard:** PCI DSS v4.0
- **Generated By:** AiVRIC
- **Retention:** 7 years
- **Review Cadence:** Quarterly