AuditKit

Multi-Cloud Compliance Scanner

PCI Compliance Report

44%

Compliance Score

21	7	9
Total Controls	Passed	Failed

Generated: October 11, 2025 at 6:52 PM
Provider: AWS | Account: [redacted]

IMPORTANT: COMPLIANCE DISCLAIMER

Automated Technical Checks Only

This compliance score of 43.8% is based ONLY on 16 automated technical checks (43.8% of automated checks passed).
The remaining 5 controls require manual documentation and cannot be automated.

What This Report Covers

Automated: 16 controls

- Infrastructure configuration
- Access controls (IAM/RBAC)
- Encryption settings
- Network security rules
- Logging and monitoring
- Security group rules

Manual: 5 controls

- Policies and procedures
- Training records
- Incident response plans
- Business continuity plans
- Third-party assessments
- Physical security controls

Your Actual Compliance May Be Higher

If you already have documentation for the 5 manual controls (policies, procedures, training records, etc.), your true compliance score could be significantly higher than 43.8%.

This tool identifies technical gaps but cannot verify your documentation. Both are required for certification.

THIS IS NOT A CERTIFICATION
This tool assists with compliance but does not replace formal third-party assessment

Executive Summary

Your AWS environment requires immediate attention with a compliance score of 43.8%. Out of 21 controls evaluated, 7 passed and 9 failed. Immediate action is required on 5 critical issues.

Top Priority Actions

1. PCI-DSS URGENT: Fix 5 CRITICAL issues - QSA will fail your assessment
2. Document cardholder data flow and network segmentation
3. Enable continuous compliance monitoring
4. Document your security policies and procedures
5. Set up automated alerting for security events

PCI-DSS Critical Violations

These issues must be resolved before your audit. Each failure represents a significant compliance gap.

1. [PCI-1.2.1] Network Segmentation

Issue: PCI-DSS Req 1.2.1 VIOLATION: Only 1 VPC found - PCI requires isolated network for cardholder data environment (CDE)

```
$ Create separate VPC for CDE
```

2. [PCI-1.3.1] No Direct Public Access

Issue: PCI-DSS Req 1.3.1 VIOLATION: 1 security groups allow 0.0.0.0/0 access: sg-0ab56571076bcff37 (port 22)

```
$ Remove all 0.0.0.0/0 rules immediately
```

3. [PCI-8.2.4] Password Rotation

Issue: PCI-DSS Req 8.2.4 VIOLATION: No password policy configured - PCI requires 90-day rotation

```
$ Set password expiry to 90 days MAX
```

4. [PCI-8.3.1] MFA for All Access

Issue: PCI-DSS Req 8.3.1 VIOLATION: 1 users with console access lack MFA - PCI requires MFA for ALL: auditkit-test

```
$ Enable MFA for ALL users with console access
```

5. [PCI-10.1] Audit Trail Implementation

Issue: PCI-DSS Req 10.1 VIOLATION: No CloudTrail configured - PCI REQUIRES comprehensive audit trails

```
$ Enable CloudTrail immediately
```

Evidence Collection Guide

Your auditor requires evidence for ALL controls. Follow these steps:

Failed Controls - Fix Then Screenshot (9 total)

1. PCI-1.2.1 - Network Segmentation

Console: https://console.aws.amazon.com/vpc/

- VPC Console -> Show all VPCs -> Screenshot showing CDE VPC separated

2. PCI-1.3.1 - No Direct Public Access

Console: https://console.aws.amazon.com/ec2/v2/home#SecurityGroups

- EC2 -> Security Groups -> Each group -> Inbound rules -> No 0.0.0.0/0

3. PCI-2.2.2 - Default Configuration Changes

Console: https://console.aws.amazon.com/ec2/v2/home#SecurityGroups

- EC2 -> Security Groups -> Filter by 'default' -> Show empty rule sets

4. PCI-4.1.1 - Security Control

5. PCI-8.2.4 - Password Rotation

Console: https://console.aws.amazon.com/iam/home#/account_settings

- IAM -> Account settings -> Password policy -> Must show 90 days or less

6. PCI-8.3.1 - MFA for All Access

Console: https://console.aws.amazon.com/iam/home#/users

- IAM -> Users -> Show MFA enabled for ALL users with console access

7. PCI-10.1 - Audit Trail Implementation

Console: https://console.aws.amazon.com/cloudtrail/

- CloudTrail -> Dashboard -> Show trail enabled for all regions

8. PCI-11.5.1 - Security Control

Console: https://console.aws.amazon.com/config/

- AWS Config -> Settings -> Show recorder enabled

9. CC6.7 - Password Policy

Console: https://console.aws.amazon.com/iam/home#/account_settings

- 1. Go to IAM -> Account settings
- 2. Screenshot 'Password policy' section
- 3. Must show all requirements enabled
- 4. PCI DSS requires minimum 7 chars, we recommend 14+

Passed Controls - Collect Evidence (7 total)

These controls passed automated checks. You still need screenshots for audit evidence.

1. PCI-3.4 - Encryption at Rest

2. PCI-4.1 - Encryption in Transit

3. PCI-8.2.4-keys - Security Control

4. CC6.6 - Authentication Controls

Console: https://console.aws.amazon.com/iam/home#/security_credentials

- 1. Go to IAM -> Security credentials
- 2. Screenshot MFA section showing device configured

5. CC6.8 - Access Key Rotation

6. CC6.7 - Password Policy

7. CC6.1 - Logical and Physical Access Controls

Manual Documentation Required (5 total)

These controls require manual documentation or policy evidence that cannot be automated.

1. [INFO] PCI-7.1.2 - Security Control

Documentation Required: MANUAL REVIEW REQUIRED: Verify separation between development, operations, and security roles

2. [INFO] PCI-8.1.8 - Session Timeout

Documentation Required: PCI-DSS Req 8.1.8: Verify console timeout is set to 15 minutes or less

- IAM -> Account settings -> Show 15-minute session timeout configured

3. [INFO] PCI-11.2.2 - Quarterly Vulnerability Scans

Documentation Required: PCI-DSS Req 11.2.2: PCI requires QUARTERLY vulnerability scans by Approved Scanning Vendor (ASV)

- Document ASV scan reports dated within last 90 days

4. [INFO] PCI-11.3.1 - Security Control

Documentation Required: PCI-DSS Req 11.3.1: PCI requires ANNUAL penetration testing of CDE

5. [INFO] PCI-11.5 - Security Control

Documentation Required: PCI-DSS Req 11.5: Deploy file integrity monitoring on critical systems

PCI-DSS Evidence Checklist

Check off each item as you collect evidence for your audit

[ ] Cardholder Data Environment (CDE) Network Diagram
[ ] Firewall Configuration Screenshots (Requirement 1)
[ ] User Access Control Matrix (Requirement 7)
[ ] MFA Configuration for All Admin Access (Requirement 8.3)
[ ] Password Policy Settings (Requirement 8.2)
[ ] Access Key Rotation Report (< 90 days)
[ ] Encryption Settings for Data at Rest (Requirement 3.4)
[ ] Audit Log Configuration (Requirement 10)
[ ] Log Retention Settings (90+ days minimum)
[ ] Vulnerability Scan Results (Requirement 11)
[ ] Security Patch Documentation (Requirement 6.2)
[ ] Incident Response Plan (Requirement 12.10)