AuditKit

Multi-Cloud Compliance Scanner

SOC2 Compliance Report

49	13	26
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 33.3% is based ONLY on 41 automated technical checks (31.7% of automated checks passed).
The remaining 8 controls require manual documentation and cannot be automated.

What This Report Covers

Automated: 41 controls

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

Manual: 8 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 8 manual controls (policies, procedures, training records, etc.), your true compliance score could be significantly higher than 33.3%.

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 33.3%. Out of 49 controls evaluated, 13 passed and 26 failed. Immediate action is required on 5 critical issues.

Top Priority Actions

1. URGENT: Fix 5 CRITICAL issues immediately - these WILL fail your audit
2. CRITICAL: Enable MFA for root/admin accounts TODAY - auditors check this first
3. MEDIUM: Enable encryption on all storage - best practice
4. HIGH: Close management ports from internet - major security finding
5. HIGH: Rotate access keys/credentials older than 90 days - compliance requirement

SOC2 Critical Control Failures

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

1. [CC3.2] Risk Identification

Issue: GuardDuty not enabled - no automated threat detection

```
$ Enable GuardDuty for continuous threat monitoring
```

2. [CC6.1] Logical and Physical Access Controls

Issue: CRITICAL: 1 security groups with admin ports open to internet

```
$ Restrict SSH/RDP/database ports to specific IPs only
```

3. [CC7.1] Security Monitoring and Logging

Issue: No CloudTrail configured

```
$ Enable CloudTrail for comprehensive logging
```

4. [CC6.1] Logical and Physical Access Controls

Issue: 1 security groups have critical ports open to 0.0.0.0/0: sg-0ab56571076bcff37 (port 22/SSH open to world!) | Violates PCI DSS 1.2.1 (firewall config)

```
$ Close open ports on SG: sg-0ab56571076bcff37
Run: aws ec2 revoke-security-group-ingress
```

5. [CC7.1] Security Monitoring and Logging

Issue: CRITICAL: NO CloudTrail configured! Zero audit logging | Violates PCI DSS 10.1 (implement audit trails) & HIPAA 164.312(b)

```
$ aws cloudtrail create-trail --name audit-trail --s3-bucket-name YOUR_BUCKET && aws
cloudtrail start-logging --name audit-trail
```

Evidence Collection Guide

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

Failed Controls - Fix Then Screenshot (26 total)

1. CC1.1 - Organizational Governance

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

- 1. Go to AWS Organizations
- 2. Screenshot the organization structure
- 3. Document SCPs in place

2. CC1.2 - Board Oversight

3. CC1.4 - Commitment to Competence

4. CC2.2 - Internal Communication

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

- 1. Go to SNS Console
- 2. Create topics for SecurityAlerts, OperationalAlerts
- 3. Configure subscriptions

5. CC3.1 - Risk Assessment Process

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

- 1. Go to Security Hub
- 2. Enable with security standards
- 3. Document compliance scores

6. CC3.2 - Risk Identification

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

- 1. Go to GuardDuty
- 2. Enable for all regions
- 3. Configure threat intel feeds

7. CC3.3 - Risk Analysis

8. CC4.1 - Monitoring Activities

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

- 1. Go to AWS Config
- 2. Set up configuration recorder
- 3. Enable compliance rules

9. CC4.1 - Monitoring Activities

10. CC4.2 - Evaluation of Deficiencies

11. CC5.1 - Control Activities

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

- 1. Go to AWS Backup
- 2. Create backup plan
- 3. Assign resources

12. CC5.2 - Technology Controls

13. CC6.1 - Logical and Physical Access Controls

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

- 1. Go to EC2 -> Security Groups
- 2. Review inbound rules
- 3. Remove 0.0.0.0/0 from ports 22, 3389, 3306

14. CC6.3 - Encryption at Rest

- 1. Go to VPC -> Endpoints
- 2. Create endpoints for S3, DynamoDB
- 3. Route table associations

15. CC6.6 - Authentication Controls

16. CC6.7 - Password Policy

17. CC6.8 - Access Key Rotation

18. CC7.1 - Security Monitoring and Logging

19. CC7.3 - Security Event Analysis

20. A1.2 - Backup and Recovery

Console: https://s3.console.aws.amazon.com/s3/buckets/auditkit-test-public-1759976302?tab=properties

- 1. Open S3 Console
- 2. Click bucket 'auditkit-test-public-1759976302'
- 3. Go to 'Properties' tab
- 4. Screenshot 'Bucket Versioning' showing 'Enabled'

21. 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+

22. CC6.1 - Logical and Physical Access Controls

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

- 1. Go to EC2 -> Security Groups
- 2. Click on the flagged security group
- 3. Go to 'Inbound rules' tab
- 4. Screenshot showing NO rules with Source '0.0.0.0/0' for ports 22, 3389, or databases
- 5. Critical: SSH/RDP must never be open to internet
- 6. For PCI DSS: Document business justification for any public access

23. CC7.1 - Security Monitoring and Logging

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

- 1. Go to CloudTrail Console
- 2. Click 'Create trail'
- 3. Enable for all regions
- 4. Screenshot showing trail is 'Logging' status
- 5. This is MANDATORY for SOC2, PCI, and HIPAA!

24. CC7.1 - Security Monitoring and Logging

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

- 1. Go to AWS Config Console
- 2. Click 'Get started'
- 3. Enable recording for all resources
- 4. Screenshot showing 'Recorder is ON'

25. CC7.2 - Incident Detection and Response

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

- 1. Go to GuardDuty Console
- 2. Click 'Get Started'
- 3. Enable GuardDuty
- 4. Screenshot showing 'GuardDuty is ENABLED'

26. CC7.1 - Security Monitoring and Logging

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

- 1. Go to VPC Console
- 2. Select your VPC
- 3. Go to 'Flow logs' tab
- 4. Screenshot showing flow logs enabled

Passed Controls - Collect Evidence (13 total)

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

1. CC2.3 - External Communication

2. CC6.4 - Security Control

3. CC6.5 - Security Control

4. CC9.2 - Vendor Management

5. CC6.2 - Network Security

Console: https://s3.console.aws.amazon.com/s3/buckets

- 1. Open S3 Console
- 2. Click any bucket
- 3. Go to 'Permissions' tab
- 4. Screenshot showing all 'Block public access' settings ON

6. CC6.3 - Encryption at Rest

7. CC7.1 - Security Monitoring and Logging

8. 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

9. CC6.8 - Access Key Rotation

10. CC6.7 - Password Policy

11. CC6.3 - Encryption at Rest

12. CC6.1 - Logical and Physical Access Controls

13. CC7.2 - Incident Detection and Response

Manual Documentation Required (8 total)

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

1. [INFO] CC1.5 - Accountability

Documentation Required: No explicit deny policies found

2. [INFO] CC3.2 - Risk Identification

Documentation Required: Inspector v2 status checked - manual review required

3. [INFO] CC3.4 - Risk Management

Documentation Required: Manual review required: Verify change management process includes risk assessment

4. [INFO] CC5.3 - Policy Implementation

Documentation Required: Manual review required: Verify security policies are documented and enforced

5. [INFO] CC6.2 - Network Security

Documentation Required: 2 users created in last 30 days - verify approval process

6. [INFO] CC7.2 - Incident Detection and Response

Documentation Required: No automated anomaly detection functions found

7. [INFO] CC7.4 - Performance Monitoring

Documentation Required: Manual review required: Verify incident response procedures are documented

8. [INFO] CC8.1 - Change Management Process

Documentation Required: No custom AMIs found - consider creating golden images

SOC2 Evidence Checklist

Check off each item as you collect evidence for your audit

- [ ] AWS Account Summary Page
- [ ] IAM Dashboard showing MFA status
- [ ] Password Policy Settings
- [ ] S3 Bucket Encryption Settings
- [ ] CloudTrail Configuration
- [ ] Security Groups Configuration
- [ ] Access Key Age Report
- [ ] VPC Flow Logs Configuration
- [ ] AWS Config Dashboard