AuditKit

Multi-Cloud Compliance Scanner

CMMC Level 1 Compliance Report

17	4	3
Total Controls	Passed	Failed

Generated: October 11, 2025 at 6:52 PM
Provider: AWS | Account: 405894844061

IMPORTANT: COMPLIANCE DISCLAIMER

Automated Technical Checks Only

This compliance score of 57.1% is based ONLY on 7 automated technical checks (57.1% of automated checks passed).
The remaining 10 controls require manual documentation and cannot be automated.

What This Report Covers

Automated: 7 controls

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

Manual: 10 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 10 manual controls (policies, procedures, training records, etc.), your true compliance score could be significantly higher than 57.1%.

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 57.1%. Out of 17 controls evaluated, 4 passed and 3 failed. Immediate action is required on 0 critical issues.

Top Priority Actions

1. Enable continuous compliance monitoring
2. Document your security policies and procedures
3. Set up automated alerting for security events
4. Schedule quarterly access reviews

CMMC Level 1 Critical Findings

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

[PASS] No critical issues found - excellent work!

Evidence Collection Guide

C3PAO assessor requires evidence for ALL CMMC Level 1 practices:

Failed Controls - Fix Then Screenshot (3 total)

1. AC.L1-3.1.2 - Security Control

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

- AWS Console -> IAM -> Policies -> Create policy -> Screenshot custom policies

2. IA.L1-3.5.2 - Security Control

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

- AWS Console -> IAM -> Users -> Security credentials -> Screenshot MFA devices

3. SC.L1-3.13.1 - Security Control

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

- AWS Console -> VPC -> Security Groups -> Screenshot showing restricted inbound rules

Passed Controls - Collect Evidence (4 total)

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

1. AC.L1-3.1.1 - Security Control

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

- AWS Console -> IAM -> Users -> Screenshot user list showing authorized access

2. IA.L1-3.5.1 - Security Control

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

- AWS Console -> IAM -> Users -> Screenshot showing unique user identities

3. SC.L1-3.13.16 - Security Control

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

- AWS Console -> S3 -> Properties -> Screenshot showing encryption enabled

4. SC.L1-3.13.11 - Security Control

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

- AWS Artifact -> Screenshot showing FIPS 140-2 compliance documentation

Manual Documentation Required (10 total)

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

1. [INFO] MP.L1-3.8.3 - Security Control

Documentation Required: MANUAL: Document media sanitization procedures for EBS volumes and S3 objects

- Documentation -> Screenshot showing media sanitization procedures | AWS Console -> S3 -> Lifecycle rules

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

2. [INFO] PE.L1-3.10.1 - Security Control

Documentation Required: MANUAL: AWS data centers have physical controls (inherited control)

- AWS Artifact -> Screenshot SOC 2 report showing physical controls

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

3. [INFO] PE.L1-3.10.3 - Security Control

Documentation Required: MANUAL: AWS data centers escort visitors (inherited control)

- AWS Artifact -> Screenshot showing visitor management procedures

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

4. [INFO] PE.L1-3.10.4 - Security Control

Documentation Required: MANUAL: AWS maintains physical access logs (inherited control)

- AWS Artifact -> Screenshot showing physical access logging

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

5. [INFO] PE.L1-3.10.5 - Security Control

Documentation Required: MANUAL: AWS controls physical access devices (inherited control)

- AWS Artifact -> Screenshot showing physical access device management

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

6. [INFO] PS.L1-3.9.1 - Security Control

Documentation Required: MANUAL: Document personnel screening procedures for CUI access

- HR Documentation -> Screenshot showing personnel screening procedures and background check records

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

7. [INFO] PS.L1-3.9.2 - Security Control

Documentation Required: MANUAL: Document authorization process for CUI access

- Documentation -> Screenshot showing CUI access authorization procedures and approval records

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

8. [INFO] SI.L1-3.14.1 - Security Control

Documentation Required: MANUAL: Document flaw identification and remediation processes

- AWS Console -> Systems Manager -> Patch Manager -> Screenshot compliance dashboard

Console: https://console.aws.amazon.com/systems-manager/patch-manager

9. [INFO] SI.L1-3.14.2 - Security Control

Documentation Required: MANUAL: Document malicious code protection mechanisms

- AWS Console -> GuardDuty -> Screenshot showing malware detection enabled

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

10. [INFO] SI.L1-3.14.4 - Security Control

Documentation Required: MANUAL: Document malicious code protection update procedures

- AWS Console -> GuardDuty -> Settings -> Screenshot showing automatic updates enabled

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

CMMC Level 1 Evidence Checklist

Check off each item as you collect evidence for your audit

- [ ] Access Control Policy (AC.L1-3.1.1 - 3.1.2)
- [ ] Identification and Authentication (IA.L1-3.5.1 - 3.5.2)
- [ ] Media Protection (MP.L1-3.8.3)
- [ ] Physical Protection (PE.L1-3.10.1 - 3.10.5)
- [ ] Personnel Security (PS.L1-3.9.1 - 3.9.2)
- [ ] System and Communications Protection (SC.L1-3.13.1 - 3.13.16)
- [ ] System and Information Integrity (SI.L1-3.14.1 - 3.14.5)

For CMMC Level 2 (CUI Protection - 110 additional practices):
Visit auditkit.io/pro