CMMC 2.0 Level 1 Compliance Report

Report Generated: August 11, 2025

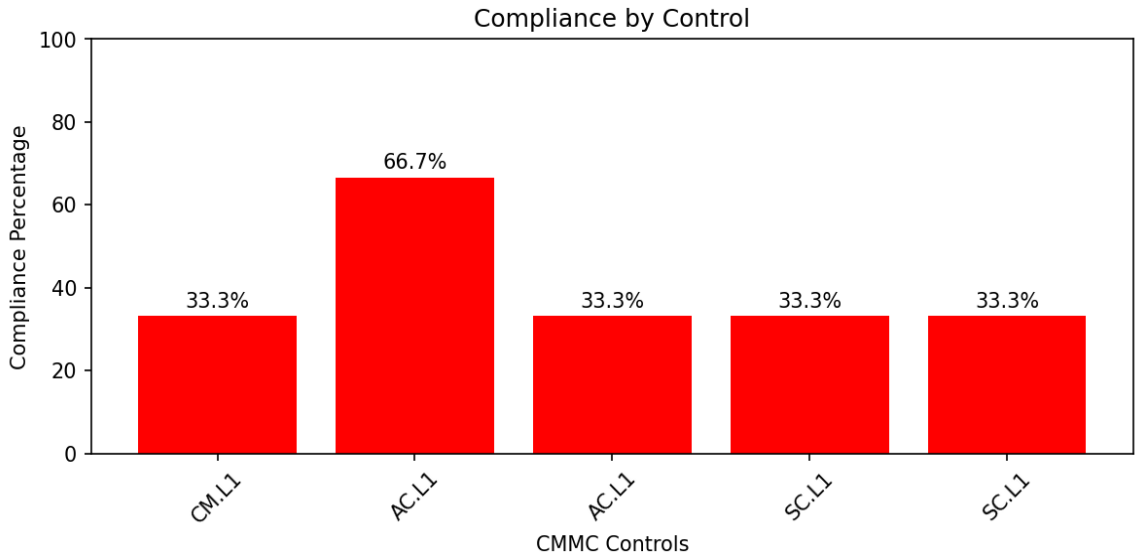
Compliance Framework: CMMC 2.0 Level 1

Assessment Type: Network Device Configuration Review

Executive Summary

This report presents the results of a CMMC 2.0 Level 1 compliance assessment conducted on 3 network devices. The overall compliance rate is 0.0% (0 out of 3 devices). The assessment evaluated five critical security controls: • CM.L1-3.4.1: Baseline Configuration Management • AC.L1-3.1.1: Authorized User Control • AC.L1-3.1.2: Transaction Limitation • SC.L1-3.13.1: Boundary Protection • SC.L1-3.13.5: Public Access Point Separation

Compliance Overview



Detailed Findings

Device: CoreSwitch01

Status: NON-COMPLIANT

Control	Status	Details
CM.L1-3.4.1	PASS	Configuration baseline check
AC.L1-3.1.1	PASS	AAA: Yes, TACACS Servers: 2
AC.L1-3.1.2	PASS	Enable Secret: Yes, No Telnet: Yes
SC.L1-3.13.1	PASS	SSH Management: Yes, ACLs Applied: Yes
SC.L1-3.13.5	FAIL	DMZ Interfaces Missing ACL: 3

Device: DMZFirewall01

Status: NON-COMPLIANT

Control	Status	Details
CM.L1-3.4.1	FAIL	Configuration baseline check
AC.L1-3.1.1	PASS	AAA: Yes, TACACS Servers: 2
AC.L1-3.1.2	FAIL	Enable Secret: No, No Telnet: Yes
SC.L1-3.13.1	FAIL	SSH Management: No, ACLs Applied: Yes
SC.L1-3.13.5	FAIL	DMZ Interfaces Missing ACL: 2

Device: EdgeRouter01

Status: NON-COMPLIANT

Control	Status	Details
CM.L1-3.4.1	FAIL	Configuration baseline check
AC.L1-3.1.1	FAIL	AAA: No, TACACS Servers: 0
AC.L1-3.1.2	FAIL	Enable Secret: No, No Telnet: Yes
SC.L1-3.13.1	FAIL	SSH Management: No, ACLs Applied: Yes
SC.L1-3.13.5	PASS	DMZ Interfaces Missing ACL: 0

Recommendations

1. Implement AAA authentication on 1 devices. Configure TACACS+ servers with local fallback for centralized user management.

2. Configure enable secret on 2 devices to protect privileged access mode.

3. Apply ACLs to DMZ interfaces on 2 devices to properly separate public-facing services.