CMMC 2.0 Level 1 Compliance Report

Cybersecurity Maturity Model Certification Assessment Report

Generated on August 19, 2025 at 03:13 PM
33.3% Compliant - POOR

■ Executive Summary

This report presents the results of a comprehensive CMMC 2.0 Level 1 compliance assessment conducted on 3 network devices. The assessment evaluated compliance against seven critical cybersecurity controls. **Key Findings:**
• Overall compliance rate: 33.3%
• Compliant devices: 1 of 3
• Risk level: Critical
• Priority remediation items: 7

■ Compliance Statistics

Metric	Value	Status
Total Devices	3	Assessed
Compliant Devices	1	Passing
Non-Compliant Devices	2	Failing
Compliance Rate	33.3%	Critical
Risk Level	Critical	Immediate Action

■■ CMMC 2.0 Level 1 Controls Assessment

CM.L1-3.4.1 - Configuration Management - NON-COMPLIANT

Description: Establish and maintain baseline configurations and inventories of organizational systems.

Purpose: Configuration baselines ensure that systems are built and maintained according to approved, documented standards.

Results: 0 passing, 3 failing (0% compliant)

Business Impact: Without proper configuration management, organizations face increased security risks, system instability, and difficulty in troubleshooting.

Common Issues:
• Missing baseline configurations: 2 items (2 devices)
• Missing baseline configurations: 1 items (1 devices)

AC.L1-3.1.1 - Access Control Policy - NON-COMPLIANT

Description: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices.

Purpose: This fundamental access control ensures that only legitimate users, processes, and devices can access network systems.

Results: 2 passing, 1 failing (67% compliant)

Business Impact: Failure to properly control access can result in data breaches, intellectual property theft, regulatory fines, and loss of customer trust.

Common Issues:
- AAA authentication not configured (1 devices)
- No TACACS+ servers configured (1 devices)

AC.L1-3.1.2 - Transaction and Function Control - COMPLIANT

Description: Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

Purpose: This control prevents privilege escalation and ensures users can only perform actions appropriate to their role.

Results: 3 passing, 0 failing (100% compliant)

Business Impact: Without proper transaction controls, users might accidentally or intentionally perform actions beyond their authority.

IA.L1-3.5.1 - User Identification - NON-COMPLIANT

Description: Identify information system users, processes acting on behalf of users, or devices.

Purpose: User identification is the foundation of accountability and audit trails.

Results: 2 passing, 1 failing (67% compliant)

Business Impact: Poor user identification makes forensic investigations difficult, reduces accountability, and may violate regulatory requirements.

Common Issues:
- Individual user accounts not configured (1 devices)

IA.L1-3.5.2 - User Authentication - NON-COMPLIANT

Description: Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Purpose: Authentication ensures that users are who they claim to be before granting access to sensitive systems and data.

Results: 2 passing, 1 failing (67% compliant)

Business Impact: Weak authentication mechanisms can lead to unauthorized access, data breaches, and compliance violations.

Common Issues:
- Authentication mechanisms insufficient (1 devices)

SC.L1-3.13.1 - Boundary Protection - COMPLIANT

Description: Monitor, control, and protect organizational communications at the external boundaries and key internal boundaries of the information systems.

Purpose: Boundary protection controls network traffic flow and prevents unauthorized access from external threats.

Results: 3 passing, 0 failing (100% compliant)

Business Impact: Without proper boundary protection, organizations are vulnerable to external attacks, data exfiltration, and lateral movement by attackers.

SC.L1-3.13.5 - Public Access Point Controls - NON-COMPLIANT

Description: Deny network communications traffic by default and allow network communications traffic by exception.

Purpose: This control ensures that publicly accessible systems are properly isolated and controlled.

Results: 2 passing, 1 failing (67% compliant)

Business Impact: Improperly secured public access points can provide attackers with entry into internal networks.

Common Issues:
- DMZ interfaces without ACL protection: 1 (1 devices)

■■ Device Compliance Status

Device Name	Vendor	Score	Status	Risk Level	Issues
CoreSwitch01	Generic Switch	85%	COMPLIANT	Medium	1 issues
DMZFirewall01	Generic	71%	NON-COMPLIANT	High	2 issues
EdgeRouter01	Cisco IOS	42%	NON-COMPLIANT	Critical	5 issues

■ Device Issues Details

DMZFirewall01 (Generic)
- DMZ interfaces without ACL protection: 1
- Missing baseline configurations: 2 items

EdgeRouter01 (Cisco IOS)
- AAA authentication not configured
- No TACACS+ servers configured
- Individual user accounts not configured
- Authentication mechanisms insufficient
- Missing baseline configurations: 1 items

■ Priority Remediation Recommendations

1. DMZ interfaces without ACL protection: 1 - High PRIORITY

Control: DMZ/Public Access Separation (SC.L1-3.13.5)
Impact: 1 devices (33.3%)

Recommended Actions:
- Address within 1-2 weeks
- Implement automated monitoring
- Update configuration baselines

2. Authentication mechanisms insufficient - High PRIORITY

Control: User Authentication (IA.L1-3.5.2)
Impact: 1 devices (33.3%)

Recommended Actions:
- Address within 1-2 weeks
- Implement automated monitoring
- Update configuration baselines

3. AAA authentication not configured - High PRIORITY

Control: Authorized Access Control (AC.L1-3.1.1)
Impact: 1 devices (33.3%)

Recommended Actions:
- Address within 1-2 weeks
- Implement automated monitoring
- Update configuration baselines

4. No TACACS+ servers configured - High PRIORITY

Control: Authorized Access Control (AC.L1-3.1.1)
Impact: 1 devices (33.3%)

Recommended Actions:
- Address within 1-2 weeks
- Implement automated monitoring
- Update configuration baselines

5. Missing baseline configurations: 2 items - High PRIORITY

Control: Baseline Configuration (CM.L1-3.4.1)
Impact: 2 devices (66.7%)

Recommended Actions:
- Address within 1-2 weeks
- Implement automated monitoring
- Update configuration baselines

6. Individual user accounts not configured - High PRIORITY

Control: User Identification (IA.L1-3.5.1)
Impact: 1 devices (33.3%)

Recommended Actions:
- Address within 1-2 weeks
- Implement automated monitoring
- Update configuration baselines

7. Missing baseline configurations: 1 items - High PRIORITY

Control: Baseline Configuration (CM.L1-3.4.1)
Impact: 1 devices (33.3%)

Recommended Actions:
- Address within 1-2 weeks
- Implement automated monitoring
- Update configuration baselines
