AuditKit

Multi-Cloud Compliance Scanner

CMMC Level 1 Compliance Report

17	4	1
Total Controls	Passed	Failed

Generated: October 11, 2025 at 9:55 PM

Provider: AZURE | Account [redacted]

IMPORTANT: COMPLIANCE DISCLAIMER

Automated Technical Checks Only

This compliance score of 80.0% is based ONLY on 5 automated technical checks (80.0% of automated checks passed).
The remaining 12 controls require manual documentation and cannot be automated.

What This Report Covers

Automated: 5 controls

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

Manual: 12 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 12 manual controls (policies, procedures, training records, etc.), your true compliance score could be significantly higher than 80.0%.

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 AZURE environment is in good standing with a compliance score of 80.0%. Out of 17 controls evaluated, 4 passed and 1 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 (1 total)

1. IA.L1-3.5.1 - Security Control

Console: https://portal.azure.com/#blade/Microsoft_AAD_IAM/UsersManagementMenuBlade/AllUsers

- Azure Portal -> Azure AD -> Users -> Screenshot user list

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://portal.azure.com/#blade/Microsoft_Azure_Billing/SubscriptionsBlade

- Azure Portal -> Subscriptions -> IAM -> Screenshot showing role assignments

2. AC.L1-3.1.2 - Security Control

Console: https://portal.azure.com/#blade/Microsoft_Azure_Billing/SubscriptionsBlade

- Azure Portal -> Subscriptions -> IAM -> Screenshot role assignments

3. SC.L1-3.13.1 - Security Control

Console: https://portal.azure.com/#blade/HubsExtension/BrowseResource/resourceType/Microsoft.Network%2FnetworkSecurityGroup

- Azure Portal -> NSGs -> Screenshot monitoring controls

4. SC.L1-3.13.16 - Security Control

Console: https://portal.azure.com/#blade/HubsExtension/BrowseResource/resourceType/Microsoft.Storage%2FStorageAccounts

- Azure Portal -> Storage -> Screenshot encryption status

Manual Documentation Required (12 total)

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

1. [INFO] IA.L1-3.5.2 - Security Control

Documentation Required: MANUAL: Verify Azure AD MFA is enabled for all users via Conditional Access

- Azure Portal -> Azure AD -> Security -> MFA -> Screenshot MFA status | Conditional Access -> Screenshot MFA policies

Console: https://portal.azure.com/#blade/Microsoft_AAD_IAM/MultifactorAuthenticationMenuBlade/GettingStarted

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

Documentation Required: MANUAL: Document media sanitization procedures for Azure Storage and compute resources

- Documentation -> Screenshot sanitization procedures | Azure Storage -> Lifecycle -> Screenshot

Console: https://portal.azure.com/#blade/HubsExtension/BrowseResource/resourceType/Microsoft.Storage%2FStorageAccounts

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

Documentation Required: Azure inherited: Microsoft data centers limit physical access (documented in SOC 2)

- Azure Trust Center -> Compliance -> Screenshot physical security documentation

Console: https://servicetrust.microsoft.com/

4. [INFO] PE.L1-3.10.2 - Security Control

Documentation Required: Azure inherited: Microsoft data centers have physical protection

- Azure Trust Center -> Screenshot physical protection controls

Console: https://servicetrust.microsoft.com/

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

Documentation Required: Azure inherited: Microsoft data centers escort all visitors

- Azure Trust Center -> Screenshot visitor procedures

Console: https://servicetrust.microsoft.com/

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

Documentation Required: Azure inherited: Microsoft maintains physical access logs

- Azure Trust Center -> Screenshot access logging

Console: https://servicetrust.microsoft.com/

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

Documentation Required: Azure inherited: Microsoft controls physical access devices

- Azure Trust Center -> Screenshot device controls

Console: https://servicetrust.microsoft.com/

8. [INFO] PE.L1-3.10.6 - Security Control

Documentation Required: Azure inherited: Microsoft enforces physical safeguards

- Azure Trust Center -> Screenshot safeguarding controls

Console: https://servicetrust.microsoft.com/

9. [INFO] SC.L1-3.13.5 - Security Control

Documentation Required: MANUAL: Verify Azure VNet subnets separate public and private systems

- Azure Portal -> Virtual networks -> Subnets -> Screenshot subnet separation

Console: https://portal.azure.com/#blade/HubsExtension/BrowseResource/resourceType/Microsoft.Network%2FvirtualNetworks

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

Documentation Required: MANUAL: Verify Azure Update Management identifies system flaws

- Azure Portal -> Update Management -> Screenshot compliance | Defender -> Screenshot vulnerabilities

Console: https://portal.azure.com/#blade/Microsoft_Azure_Automation/AutomationMenuBlade/updateManagement

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

Documentation Required: MANUAL: Verify malicious code protection via Defender for Cloud

- Azure Portal -> Defender for Cloud -> Screenshot malware protection

Console: https://portal.azure.com/#blade/Microsoft_Azure_Security/SecurityMenuBlade/0

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

Documentation Required: MANUAL: Verify automatic updates for malicious code protection

- Azure Portal -> Defender -> Settings -> Screenshot automatic updates

Console: https://portal.azure.com/#blade/Microsoft_Azure_Security/SecurityMenuBlade/0

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