



CMMC
Simplified



AG GRACE INC

Simplify Your CMMC Journey



Protecting Remote Access – Meeting CMMC AC.L2-3.1.13 with Strong Cryptographic Controls

The Role of Cybersecurity Tools: Employing Cryptography to Ensure Confidentiality in Remote Access Sessions

Understanding AC.L2-3.1.13 In today's hybrid and remote work environments, remote access is both a necessity and a vulnerability. The Cybersecurity Maturity Model Certification (CMMC) requirement AC.L2-3.1.13 specifically focuses on safeguarding remote sessions by employing cryptographic mechanisms to maintain confidentiality.

According to NIST SP 800-171A, the assessment objectives for AC.L2-3.1.13 are:

- **[a]** Determine if cryptographic mechanisms to protect the confidentiality of remote access sessions are identified.
- **[b]** Determine if those cryptographic mechanisms are effectively implemented.

In essence, organizations must use approved encryption standards to secure remote communications and demonstrate that these protections are not only planned but also functioning as intended.

Why It Matters Remote access creates opportunities for cyber attackers to intercept sensitive information if communications are not properly encrypted. Unsecured connections can expose Controlled Unclassified Information (CUI), leading to compliance violations and potential data breaches.

Tips for Implementing AC.L2-3.1.13 Compliance To meet this requirement, here are some actionable steps:

1. **Use Strong, Approved Encryption Protocols:**
 - Implement cryptographic mechanisms such as **TLS 1.2 or higher, IPsec, or SSL VPNs** to protect data in transit.
 - Ensure encryption libraries and tools are **FIPS 140-2 validated**, aligning with federal standards.
2. **Secure Remote Access Solutions:**
 - Use secure gateways like **VPNs, Zero Trust Network Access (ZTNA)** tools, or **cloud-based remote access platforms** that offer built-in encryption.
 - Enforce **multi-factor authentication (MFA)** for all remote sessions.
3. **Document Cryptographic Mechanisms:**
 - Clearly identify all cryptographic tools and protocols in use for remote access in your **System Security Plan (SSP)**.
 - Maintain an up-to-date inventory of encryption technologies and configurations.
4. **Regularly Audit and Monitor Access Logs:**
 - Set up **SIEM tools** or endpoint logging to monitor remote session activity.
 - Investigate anomalies and unauthorized access attempts in real time.
5. **Train Users and Update Policies:**
 - Educate employees on the importance of secure remote access.

- Regularly review and update your **remote access policy** to reflect current threats and compliance standards.

Maintaining and Monitoring Compliance

- **Review Cryptographic Standards Regularly:** Stay informed of changes to federal cryptographic guidelines and update configurations accordingly.
- **Test Configurations:** Periodically test remote access systems to confirm encryption is enforced.
- **Conduct Internal Assessments:** Regularly assess whether cryptographic protections are not only in place but effective.

Final Thoughts Meeting the CMMC requirement AC.L2-3.1.13 is not just about installing VPNs—it's about ensuring all remote sessions are encrypted using validated cryptographic tools and proving that these tools are active and effective. Implementing these best practices will help secure sensitive communications, protect CUI, and position your organization for successful CMMC assessments.

Need help implementing secure remote access solutions? Contact us today for expert advice on CMMC readiness.



5257 Buckeystown Pike, Suite 206, Frederick, MD 21704
Copyright © 2025 All rights reserved

No longer want to receive these emails? [unsubscribe](#)
AG Grace, Inc. www.aggrace.com